Cooperating Broadcast and Cellular Conditional Access System for Digital Television

A Thesis Submitted for the Degree of Doctor of Philosophy

by

Hamidreza Shirazi

Department of Electronic and Electrical Engineering

Brunel University

January 2009

Abstract

The lack of interoperability between Pay-TV service providers and a horizontally integrated business transaction model have compromised the competition in the Pay-TV market. In addition, the lack of interactivity with customers has resulted in high churn rate and improper security measures have contributed into considerable business loss. These issues are the main cause of high operational costs and subscription fees in the Pay-TV systems.

This paper presents a novel end-to-end system architecture for Pay-TV systems cooperating mobile and broadcasting technologies. It provides a cost-effective, scalable, dynamic and secure access control mechanism supporting converged services and new business opportunities in Pay-TV systems. It enhances interactivity, security and potentially reduces customer attrition and operational cost. In this platform, service providers can effectively interact with their customers, personalise their services and adopt appropriate security measures. It breaks up the rigid relationship between a viewer and set-top box as imposed by traditional conditional access systems, thus, a viewer can fully enjoy his entitlements via an arbitrary set-top box.

Having thoroughly considered state-of-the-art technologies currently being used across the world, the thesis highlights novel use cases and presents the full design and implementation aspects of the system. The design section is enriched by providing possible security structures supported thereby. A business collaboration structure is proposed, followed by a reference model for implementing the system. Finally, the security architectures are analysed to propose the best architecture on the basis of security, complexity and set-top box production cost criteria.

Acknowledgement

This thesis owns its existence to the help, support and inspiration of many people. In the first place, I would like to express my sincere appreciation and gratitude to Prof. J. Cosmas for his support and encouragement during the more than three years of this thesis' work. The mind-opening discussions and cooperation with my colleagues in the IST Projects - INSTINCT and PLUTO - have contributed significantly into broadening my knowledge and experience.

I am really indebted to David Cutts and grateful to his group at the Strategy and Technology for funding the project and providing me with constructive technical support and resources. Their expertise in the field of interactive TV has furthered my technical and commercial understandings throughout the thesis' work.

Also, I would like to express my thankfulness to Prof. M. Ghanbari, Prof. M. Merabti and Dr. M. Hadjinicolaou who kindly accepted to be my examiners. I also would like to thank Dr. Thomas Owens, Professor Andy Valdar from the UCL University, Emeritus Professor Nimal Nissanke from the Southbank University, Tony Reed from the BT consultancy group and Peter Croonen from the Testronic Labs for their valuable support and comments.

Finally, I owe special gratitude to my wife and indeed to my family for continuous and unconditional support of all my undertakings, scholastic and otherwise that I am veritably unable to mention them all.

I wish them all the best and I hope that hereby I could reward a part of their efforts.

Hamidreza Shirazi

TABLE OF CONTENTS

FIGURES

TABLES

ABBREVIATIONS

For the purpose of the present document following abbreviations apply.

3GPP	3rd Generation Partnership Project
AAA	Authorisation, Authentication and Accounting
AES	Advanced Encryption Standard
AIPN	All IP Network
AIT	Application Information Table
APDU	Application Protocol Data Unit
ARIB	Association of Radio Industries and Businesses
ATM	Asynchronous Transfer Mode
ATSC	Advanced Television Systems Committee
AVC	Advanced Video Coding
BCC	Bluetooth Control Centre
BCH	Bose-Chaudhuri-Hocquengham
BIP	Bearer Independent Protocol
BK	Broadcast key
BSC	Base Station Controller
BTS	Base Transceiver Station
CA	Conditional Access
CAT	Conditional Access Table
CATV	Cable TV
CDC	Connected Device Configuration
CDMA	Code Division Multiple Access
CI	Common Interface
CLDC	Connected Limited Device Configuration
CoD	Class of Device
COFDM	Coded Orthogonal Frequency Division Multiplexing
CPCM	Content Protection and Copyright Management
CPRM	Content Protection for Recordable Media
CW	Control Word
DAB	Digital Audio Broadcasting
DAM	Digital Audio Broadcasting
DARS	Digital Audio Radio Satellite
DBS	Direct Broadband Satellite
DCCAM	Downloadable Common Conditional Access Module
DCE	Data Communication Equipment

DES	Data Encryption Standard
D-H	Diffie-Hellman
DMB	Digital Multimedia Broadcasting
DMUX	De-Multiplexer
DTCP	Digital Transmission Content Protection
DTE	Data Terminal Equipment
DTMB	Digital Terrestrial Multimedia Broadcasting
DVB	Digital Video Broadcasting
DVB-C	DVB Cable
DVB-CSS	DVB Common Scrambling System
DVB-RCG	DVB Return Channel for GSM
DVB-RCS	DVB Return Channel for Satellite
DVB-RCT	DVB Return Channel for Terrestrial
DVB-S	DVB Satellite
DVB-SI	DVB Service Information
DVB-T	DVB Terrestrial
ECB	Electronic Codebook
ECM	Entitlement Control Message
EF	Elementary File
EK	Event key
EMM	Entitlement Management Message
EPG	Electronic Programme Guide
ETSI	European Telecommunications Standards Institute
FFT	Fast Fourier Transform
FTP	File Transfer Profile
GCF	Generic Connection Framework
GEM	Globally Executable MHP
GMSC	Gateway MSC
GPRS	General Package Radio Service
GSE	Generic Stream Encapsulation
GSM	Global System for Mobile Communication
HLR	Home Location Register
HMAC	Hash Message Authentication Code
IB	In-Band
ICCID	Integrated Circuit Card Identification
IETF	Internet Engineering Task Force
IIM	Interactive Interface Module
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity

INA	Interactive Network Adapter
IP	Internet Protocol
IRD	Integrated Receiver/Decoder
ISDB	Integrated Service Digital Broadcasting
ISDN	Integrated Services Digital Network
J2ME	Java 2 Micro Edition
JABWT	Java APIs for Bluetooth Wireless Technology
JCA	Java Cryptography Architecture
JCE	Java Cryptography Extension
JCRMI	JavaCard Remote Method Invocation
JSR	Java Specification Request
L2CAP	Logical Link Control and Adaptation Protocol
LAI	Location Area Identity
LPDC	Low Density Parity Check
LTE	Long Term Evolution
MAC	Medium Access Layer
MAC*	Multiplex Analogue Components
MAP	Mobile Application Part
MCF	Monitoring and Control Functions
MCP	Multimedia Car Platform
MCPA	Multi Channel Power Amplifier
ME	Mobile Equipment
MHEG	Multimedia & Hypermedia information coding Expert Group
MHP	Multimedia Home Platform
MHSS	Message Handling Subsystem
MICAS	Mobile Integrated Conditional Access System
MIDP	Mobile Information Device Profile
MIMO	Multiple Input Multiple Output
MK	Master Key
MPEG	Moving Pictures Experts Group
MPEG-PSI	MPEG Programme Specific Information
MS	Mobile Station
MSC	Mobile Switching Centre
MSISDN	Mobile Station ISDN Number
MUX	Multiplexer
NCC	Network Control Centre
NCR	Network Clock Reference
NIU	Network Interface Unit
NSAP	Network Service Access Point

OBEX	Object Exchange
OCAP	OpenCable Application Platform
OCF	Open Card Framework
OFDM	Orthogonal Frequency Division Multiplexing
OOB	Out-Of Band
PAL	Phase Alternating Line
PCMSIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant
PES	Packetised Elementary Stream
PID	Packet Identification
PKI	Public key Infrastructure
PLMN	Public Land Mobile Network
PPP	Point to Point Protocol
PPV	Pay-Per View
PRBS	Pseudo-Random Bit Stream
PRNG	Pseudo-Random Number Generator
PSM	Protocol Service Multiplexer
PSTN	Public Switched Telecommunication Network
QAM	Quadrature Amplitude Modulation
QPSK	Quadrature Phase Shift keying
RAM	Remote Application Management
RCBC	Reverse Cipher Block Chaining
RCST	Return Channel Satellite Terminal
RCTT	Return Channel Terrestrial Terminal
RFCOMM	Radio Frequency Communication
RFM	Remote File Management
RISC	Reduced Instructions Set Computer
RUIM	Removable User Identity Module
SAP	SIM Access Profile
SAS	Subscriber Authentication System
SAT	Subscription Association Table
SATSA	Security and Trust Services API
SDDB	Service Discovery Database
SDP	Service Discovery Protocol
SFN	Signal Frequency Network
SGSN	Serving GPRS Support Node
SI	Service Information
SK	Service Key
SMATV	Satellite Master Antenna Television

SMPTE	Society of Motion Picture and Television Engineers
SMS	Subscriber Management System
SMS	Short Message Service
SMSC	Short Message Service Centre
SMSC	Short Message Service Centre
SPI	Security Parameter Indicator
SPP	Serial Port Profile
SS7	Signalling System 7
STB	Set-Top Box
TAF	Terminal Adaptation Function
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TLS	Transport Layer Security
TMSI	Temporary Mobile Subscriber Identity
TM-T2	Technical Module on next generation DVB-T (DVB-T2)
TPDU	Transport Packet Data Unit
TS	Transport Stream
UHF	Ultra High Frequency; 470- 862 MHz, television
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
VHF	Very High Frequency; 47 – 300 MHz, television
VLR	Visiting Location Register
VSB	Vestigial Sideband Modulation
WAP	Wireless Application Protocol
Wi-Fi	Wireless Fidelity
WMA	Wireless Messaging APIs
XAIT	Extended Application Information Table

1 INTRODUCTION

1.1 Overview

Media contents are made available in various ways including direct broadcasting to fixed/portable receivers, Internet multicasting or point-to-point delivery and selling contents at the downloading points in the shops. Nevertheless, the great demand is still dedicated to the traditional direct broadcasting whereby people can benefit from wider range of programmes especially in cases of broadcasting via satellite and cable media. The revenue in this business usually flows from viewers' payment and advertisements. The viewers' payment can be in the form of a license fee (in case of national TV) or subscription fee, which can occur once (i.e. Pay-Per-View, etc.) or in number of instalments spread across a predetermined period of time. The Pay-TV is a business model which adopts the latter in which contents are directly funded by the viewers. The access control is the key to secure the revenue in this model. The Conditional Access (CA) technique is an access control mechanism to ensure that only authorised viewers, who have subscribed to a service, can view the paid content. The technique tends to be proprietary thereby indicating known commercial issues such as interoperability, high subscription fees and so on and so forth.

In the next sections, the scope and objectives of the thesis' work are discussed, followed by explaining the methodology used and contribution made to the knowledge herein. Finally, the structure of thesis is provided.

1.2 Scope and Objectives

The thesis is aimed at investigating the viable solutions whereby the security and interactive services can be enhanced in the Pay-TV systems. The technical and commercial needs in cutting the cost and increasing the potential revenue across the Pay-TV platform have been the main factors to driving the project. The scope and objectives of the project are specified as follows.

1.2.1 Project Justification

The main players in the Pay-TV system are the service provider (i.e. network provider), CA provider, set-top box producer and TV consumers (viewers). The current business model forms a restricted circle of dependency amid the players. The service provider governs a vertical market such that the rest of the players ought to operate confidentially under the service provider's influence. Such restriction owes to the importance of security in the success of the Pay-TV business model. Evidently, this discipline scales down the business opportunities for new broadcasters or set-top box producers, introduces higher operation/deployment costs to service providers and ultimately offers expensive products to the TV consumers. These pitfalls have resulted in a great demand amongst the key players in the Pay-TV to operate under a horizontal transaction model wherein viewers can freely make their own choice from the wide range of services and set-top boxes in the market. This requirement has been partly distinguished for the viewers' convenience since the CA system has been introduced, though it has not been truly practiced to date due to the lack of interoperability between Pay-TV systems. Indeed, the interoperability itself can be rooted to the fact that service providers are reluctant to share any part of their system with others'.

The said issues are addressed in the thesis by proposing an end-to-end cooperative Broadcast and cellular access control whereby the GSM mobile phone (i.e. SIM card and mobile equipment) is used to implement the Pay-TV security module. The pervasive support for Java technology (i.e. JavaCard, J2ME), standardised communication and security protocols (i.e. SATSA) in mobile technology ensure that an application centric model can be deployed in the mobile network. In such a platform, given the service provider has an appropriate download certificate, the service provider may benefit from the flexibility of software applications to enhance security and introduce personalised/targeted services. Such a security deployment shift from set-top box to the mobile phone not only reduces the service deployment costs (i.e. eliminating the smartcard) but also introduces new types of interactive services. Moreover, it can encourage a horizontal transaction model for the Pay-TV market wherein all players can variably enjoy the following advantages.

The system introduces higher level of flexibility in the implementation of a software-based CA system as TV viewers can enjoy their entitlements via any set-top box and switch to any service provider with no need to change the set-top box. In fact, the system uses the mobile systems (i.e. GSM) and proposes a comprehensive solution to control the access and identity of viewers in a way that a viewer can concurrently benefit from services offered by different service providers via an arbitrary set-top box. Ultimately, viewers may be able to shop from range of multimedia services offered by different vendors (service providers) via arbitrary but standardised terminals. In other words, the security features in the mobile phone and SIM card (i.e. data encapsulation, application firewall, etc.) enable the co-existence of different vendors at the same time at receiver-end and/or head-end.

The proposed access control mechanism can help service providers constructively interact with their customers to realise their needs and improve their convenience and satisfaction level. This would at least reduce the viewers' churning rate and security costs as imminent threats and security breaches can be identified via constant interactions with viewers and monitoring their contractual behaviour.

1.2.2 Project Product and Objectives

The marriage of telecommunication (i.e. Internet, mobile network) and broadcasting networks not only can extend the coverage (i.e. global coverage) and range of services but also resolve most of the issues known in the traditional Pay-TV systems. This advantage has been realised in the thesis to derive benefits from the convergence of mobile and broadcasting systems which results in a flexible and dynamic platform. In this platform, a Pay-TV service provider can generate more revenue by employing the interaction channels to remotely deploy the access control subsystem in the field and enhance the security and interactive services. Some of the great advantages of the proposed system can be catalogued as follows:

- Lower deployment cost: no need to commission third-party engineers to attend the customer's premises and install the access point equipment;
- Cheaper set-top boxes: the price can be subsidised as the set-top box producers can operate in a wider market. Also, the security module in the set-top box can be possibly replaced by GSM SIM card;
- Lower security flaws cost: communication channels can be effectively used for point-to-point delivery of the keys and also to report back the customers' contractual behaviour;

- Higher revenue: lower deployment, operational and production costs can stimulate the Digital-TV (DTV) market and emerge more affordable services and products for the TV consumers. Moreover, interaction with viewers can improve their satisfactory level and thus revenue.

The worldwide popularity of the mobile phone, low deployment cost and enriched features of the mobile technologies (i.e. security, communication, etc.) can be seen as key forces to the success of the proposal particularly in the emerging Pay-TV markets (i.e. African countries).

The proposed CA system exploits the mobile technology to enhance personalisation concept and interactive services in the Pay-TV systems. The MICAS enables service providers to introduce new type of services like 'Follow Me' service which adds mobility to the conditional access system enabling the service provider to identify a viewer and issue necessary licenses to let the viewer access his entitlements even if he is away from his home. Other advantages of using the mobile phone include, but are not limited to, locate and realise the need of viewers and provide them with appropriate data (i.e. local information, advertisement, services of interest, etc.) In addition, introducing the mobile technology into the broadcasting systems will enhance not only the interaction between a service provider and viewers but also viewers with viewers in that they can share each others' opinion with respect to an event, a service or a programme.

The networking and personalisation can be offered via the Internet too, but nevertheless the mobile technology is considered as a core solution here. The main reason to such an adoption is that the mobile phone has proved that it is more personal and available to people than other technologies. Thus, it has attracted huge investments on expanding the mobile features. Today, mobile

phones support range of PC-like applications support and connectivity features to personal or local area networks.

As mentioned before, the proposed CA system can potentially break the current monopoly Pay-TV business model and advocates a competition model in that Pay-TV service providers can enter into the market and coexist at both head-end and receiver-end. The service provider needs to directly cooperate with a conditional access provider and deal with mobile network operator(s) to deploy his CA system. A mutual agreement between a service provider and mobile operator(s) is necessary to enable the service provider use the mobile technologies (i.e. network, privileged domains in the mobile phone or SIM card) for his added value services, access control and security mechanisms. Additionally, a regulator is able to govern the market and introduce standards for interoperability of applications and devices across the service providers' boundaries and a means of providing for inter-provider settlement. Last, but not least, is to establish a central database that can be managed for instance by the regulator to provide adequate information to service providers for identity and compliance checking. The service providers can therefore ensure that their services will be interoperable with valid terminals (i.e. mobile phone, set-top box).

Identifying the full technical and regulatory challenges faced in the real implementation of the cooperative Broadcast and cellular CA system in the field demands collaboration of various groups of experts, which falls outside the project scope due to the project restrictions (i.e. man-hour, financial and technical resources, etc.) Clearly, implementing the proposed system also demands the government's incentive on obliging the market players to comply with regulations and standards that are needed for ensuring the interoperability amidst applications, services and devices in the platform.

1.2.3 Methodology

The thesis' work is a research-based project which aims to investigate on potential techniques to evolve the traditional Pay-TV system particularly with respect to the transaction model, costs (i.e. deployment, operational and set-top box production costs) and revenue making schemes (i.e. new services, security and interactivity).

In line with the project objectives, various technologies which are currently integrated into the broadcasting systems, especially Pay-TV systems, were considered. Among them are the broadcasting systems, interactive channels and conditional access systems. Considering the current trend in communication systems, the popular Internet, mobile and wireless technologies (i.e. Bluetooth, WiFi) are reviewed aiming at finding an integrated solution to the current Pay-TV system which could potentially satisfy the said project objectives.

After having studied the involved technologies, a set of viable solutions are delivered ending in a novel solution with higher technical and commercial implications. The system architecture and requirement analysis reflected in various use-case scenarios are discussed followed by proposing a possible implementation model to prove the concept and endorse the solution. Finally, a thorough analysis is given to compare various solutions that can be deployed within the proposed framework.

1.3 Contribution to Knowledge

The thesis' work proposes the Mobile Integrated Conditional Access System (MICAS) as a state-of-the-art cooperative Broadcast and cellular access control solution to the Pay-TV system. The MICAS introduces a new GSM-based CA system which can be integrated into a set-top box either internally or externally [98].

It introduces a new Message Handling Subsystem (MHSS), which operates at the head-end and interfaces with viewers, Subscriber Management Subsystem, Subscriber Authorization Subsystem and Billing Subsystem for interaction, access control and billing processes. It handles all the input/output (I/O) processes taking place over the GSM interaction channel [98].

The thesis identifies various use-case scenarios (i.e. subscription via mobile phone, amendment, etc.), security architectures and services (i.e. Follow Me) which can be defined within the MICAS framework [97].

A new competitive transaction model for the Pay-TV system is identified. In this model, service providers, CA providers, STB producers, mobile phone operators cooperate with each other under a regulator's umbrella to deliver an open and standardised platform. The TV viewers can enjoy the flexibility and diversity of services in this system.

A reference model is specified to implement one of the possible security architectures that can be defined in the MICAS. In the reference model, a model for the software protocol stack taking into account underlying agents is presented. Having considered the possible use case scenarios, the format of the message employed in the MICAS for interaction purposes are determined within. Finally, the determined security architectures are analysed versus pre-deployment criteria (i.e. security, cost and complexity) to distinguish the pros and cons of the architectures.

1.4 Research Activities and Publications

The thesis is a result of extensive research on DVB systems conducted on the following projects:

- The Interactivity, Personalisation and Access Control Enhancement in Pay-TV (iPACE-TV) project was an industry-led project to investigate the

potential solutions for well-known Pay-TV issues namely lack of interactivity, low range of services, security and interoperability amid service providers.

- The IST-Physical Layer DVB Transmission Optimization (PLUTO) project [87] was centred on investigating the effect of the diversity techniques (Multiple Input Multiple Output - MIMO) on the Quality of Experience at the receiver-end through exhaustive measurements in the laboratory and field. The design of a central measurement and monitoring centre taking into account all the configuration and processing parameters required to establish the MIMO performance in the DVB-T system was part of the cooperation. Following papers and deliverables have been published during the work in the PLUTO project:
- The IST-IP-based Services & Terminals for Converging Systems (INSTINCT) project [55] were focused on the Quality of the Service (QoS) monitoring and control in the converged IP and DVB systems.

The contributions in the said projects have been published in the following transactions, conference and white papers.

- **Transactions**

[1] Shirazi H., Cosmas J., Owens T., Song Y-H, Centonza A., "A QoS Monitoring System in a Heterogeneous Multi-domain DVB-H Platform", IEEE Transactions on Broadcasting Mar 2009, vol. 55, Issue 1, pp. 124-131;

[2] Di Bari R., Bard M., Zhang Y., Nasr K.M., Cosmas J., Loo K.K., Nilavalan R., Shirazi H., Krishnapillai K., "Laboratory Measurement Campaign of DVB-T Signal with Transmit Delay Diversity", IEEE Transactions on Broadcasting Sep 2008, vol. 54, Issue 3, Part 2, pp. 532-541;

- **Conference Papers**

[3] Shirazi H., Cosmas J., Cutts, D., Birch N., Daly P., "Security Architectures in Mobile Integrated Pay-TV Conditional Access System", 13th IEEE International Telecommunications Network Strategy and Planning Symposium, Network 2008, Sep 2008, pp. 1-15;

[4] Shirazi H., Cosmas J., Cutts, D., Birch N., Daly P., "Mobile Integrated Conditional Access System (MICAS)", IEEE International Symposium on Consumer Electronics, ISCE 2008, Apr 2008, pp. 1-4;

[5] Shirazi H., Di Bari R., Cosmas J., Nilavalan R., Zhang Y., Loo K.K., Bard M., "Test-bed Development & Measurement Plan for Evaluating Transmit Diversity in DVB Networks", 16th IST Mobile and Wireless Communications Summit Jul 2007, pp. 1-5;

[6] Shirazi H., Cosmas J., Krishnapillai K., Di Bari R., Bard M., Bradshaw D., "Evaluating Existing Set-top Boxes Versus Transmit Diversity Schemes", IEEE International Symposium on Consumer Electronics, ISCE 2008, Apr 2008, pp. 1-4;

[7] Di Bari R., Cosmas J., Bard M., Loo K.K., Nilavalan R., Shirazi H., "Measurements, Processing functions and Laboratory test-bench Experiments for Evaluating Diversity in Broadcast Network", IEEE International Symposium on Broadband Multimedia Systems and Broadcasting Mar 2007, Florida, USA;

[8] Di Bari R., Bard M., Cosmas J., Nilavalan R., Loo K.K., Shirazi H., Krishnapillai K., "Field Trials and Test Results of Portable DVB-T/H Systems with Transmit Delay Diversity", IEEE International Symposium on Consumer Electronics, ISCE 2008 Apr 2008, pp. 1-4

[9] Di Bari R., Bard M., Cosmas J., Nilavalan R., Loo K.K., Shirazi H., Krishnapillai K., "Measurement Results of Transmit Delay Diversity for DVB-T Networks", IEEE International Symposium on Broadband Multimedia Systems and Broadcasting Apr 2008, pp. 1-7;

- **White Papers**

[10] Shirazi H., Cosmas J., Di Bari R., Krishnapillai K., Bard M., "Simulation Lab Facility and Test Report", PLUTO IST-026902-Brunel/WP03/Del3.1, Sep 2006;

[11] Shirazi H., Krishnapillai K., Cosmas J., Bard M., Bradshaw D., "Backwards Compatibility Testing", PLUTO IST-026902/Brunel/WP03/Del3.2 Annex for DTG testing, Apr 2007;

[12] Shirazi H., Krishnapillai K., Di Bari R., Cosmas J., Bard M., Masse D., Oksanen M., Raynal C., Defee I., Kasser P., "Pilot Trial Facilities including Service Creation System", PLUTO IST-026902/Brunel/WP03/Del3.3, January 2008;

[13] Cosmas J., Bard M., Shirazi H., "Report on Field Testing on Channel Repeater and MCPA", PLUTO IST-026902/Brunel/WP01/Del5.4, Jun 2008;

- **Submitted Papers**

[14] Shirazi H., Cosmas J., Cutts, D., Birch N., Daly P., "MICAS - A Conditional Access solution to Pay-TV systems", IEEE Transactions on Broadcasting, submitted Aug 2009;

1.5 Thesis Structure

The thesis is organised to give an overview of the existing technologies used in the DTV and Pay-TV systems. With respect to the network convergence and technology integration, the well-known telecommunication and wireless technologies are then detailed in terms of their architecture and underlying

security mechanisms. The literature review on the conditional access systems is provided next to highlight the current state and state-of-art-solution proposed herein as the MICAS. The thesis then concentrates on the design, implementation and analysis of the MICAS. The details of the chapters are as follows:

Chapter 2 presents an overview of the existing broadcasting systems covering DTV standards and technologies used in the Europe and rest of the world such as North America, Japan, Korea and China. The broadcasting standards ratified by the European Digital Video Broadcasting (DVB) project for satellite, cable, terrestrial, mobile and Internet media are briefly discussed followed by standards used in other regions which are enjoying almost similar specifications. The Interactive TV is then explained elaborating return channels in telecommunication and broadcasting networks mainly standardised by the DVB project. The satellite, cable and terrestrial systems are among the broadcasting return channels considered and the mobile network (i.e. GSM) and Internet are popular telecommunication networks which afford bi-directional communications. Apart from communication aspects of the DTV, the Middleware embedded in the digital TV receivers are equally important to deliver digital and interactive services. Therefore, the chapter is extended to cover various Middleware standards including private, open and portable solutions.

Chapter 3 provides an insight to the technologies that might be employed at the access network and in-house (personal) communications. Amid various mobile and wireless solutions, the GSM and Bluetooth technologies are discussed due to their successful business model, worldwide availability and popularity. The structure of the GSM network is provided together with transport protocols and services (i.e. SMS, WAP) supported in the GSM network. The core technologies and protocol stack of a Bluetooth-enabled device are then detailed.

Chapter 4 explains the security architecture of the GSM and Bluetooth technologies considering that they can imply security concerns for Pay-TV service providers. The chapter continues to describe security primitives that can be implemented by service providers to add more security within the MICAS when exchanging data (i.e. privacy and integrity), establishing a session (i.e. authorisation and authentication) and dealing with an order (i.e. non-repudiation).

Chapter 5 provides an in-depth overview of conditional access systems since the technique has been defined by the DVB project. The chapter describes the Pay-TV systems and gives a general model for conditional access systems. It then presents the evolution of conditional access system in response to technological and commercial needs.

Chapter 6 analyses the current state of the Pay-TV system in terms of the commercial success and customers' satisfaction factors. The issues of the common business model of Pay-TV systems are highlighted concerning the transaction model, interoperability amid service providers, costs and security defects while appreciating the presence of personalisation and enhanced interactive services. The chapter provides a set of high-level solutions taking into account the technological trends in the market. It narrows down the solutions to the Mobile Integrated Conditional Access System (MICAS) due to the popularity of the GSM network and enhanced features supported by mobile technologies. It is also believed that the GSM network is a basis for updated mobile technologies and given a viable solution based on the GSM technology, it would be applicable to next mobile generations with minimum modifications. The chapter then defines the design aspects of the MICAS. It provides a thorough requirement analysis using various scenarios identifying use cases and underlying functions that shall be supported in the MICAS. It is followed by introducing possible

security architectures supported within the MICAS framework. The security architectures are differentiated from each other based on where and how security keys and access control messages are delivered and processed.

Chapter 7 highlights the implementation aspects of MICAS security architecture. It provides the MICAS protocol stack and details the underlying agents, which shall be deployed in the MICAS to satisfy the requirements. The chapter is continued by providing an overall analysis on MICAS security architectures with respect to the security, complexity and set-top box cost model. The overall pre-deployment performance of the security architectures is then derived to conclude the chapter.

Chapter 8 concludes the thesis by succinctly describing the solution statement taking into account the results of the literature and technology review and current Pay-TV issues. Finally, potential future works and research opportunities are proposed to pave a way for related research or commercial activities.

2 DIGITAL TV SYSTEMS

2.1 Introduction

The digital TV (DTV) was introduced in late 1990s, in contrary to the analogue TV. The DTV has opened new business opportunities for TV broadcasting and consumer electronic industries. The TV consumers have also embraced the technology as it offers wider range of higher quality of services than the former system. The DTV has proved to be more bandwidth efficient and as such capable of offering more number of channels. The characteristic of digital signals depends on to the physical layer (medium) used for service delivery. The main medium used in the broadcasting systems are satellite, cable and terrestrial systems. With the technology growth and consumers' readiness, new type of added-value services (i.e. digital interactive services) has come out for attracting TV consumers. Traditionally interactive services were in the form of participation television incorporating random calls for polling or advertisement purposes. Today, the interactivity has different forms depending on features integrated in DTV receivers and supported by service providers. Employing bi-directional networks (i.e. telephone, internet, etc.) and embedding high-tech middleware in TV receivers would enable a service provider to offer enhanced and digital interactive services whereby consumers can realise local broadcasting services or interact with their service providers via a return channel. In the following sections, the DTV standards followed by underlying technologies in the digital interactive TV are discussed.

2.2 Digital TV Standards

The digitisation of the TV analogue signals has been considered as a new phase in the TV history which has opened new horizons in technical and commercial activities around the world. The EU, North America and Japan have pioneered in leading standardisation activities for different broadcasting medium like satellite, cable and terrestrial networks. The next sections describe some of these standards widely used nowadays.

2.2.1 European Standards

The Digital Video Broadcasting (DVB) Project [23] was established in 1993 as an alliance of about 300 companies originally from Europe, but now is worldwide. The DVB project has been focused at defining specifications for digital media delivery systems, including broadcasting.

At the beginning of the 1990s, change was coming to the European satellite broadcasting industry, and it was becoming clear that once the state-of-the-art Multiplex Analogue Components (MAC*) systems would have to give way to all-digital technologies due to the more effective compression and modulation techniques to utilise available bandwidth with more flexibility. It became clear that satellite and cable would deliver the first broadcast digital television services. Fewer technical problems and a simpler regulatory climate meant that they could develop more rapidly than terrestrial systems. Market priorities meant that digital satellite and cable broadcasting systems would have to be developed rapidly. Terrestrial broadcasting would follow.

2.2.1.1 DVB-S

The DVB-S system for digital satellite broadcasting was developed in 1993 [25], [103]. It is a relatively straightforward system using the QPSK modulation. The

specification described different techniques for channel coding and error protection which were later used for other delivery media systems.

The satellite television is mainly broadcast in South and North Africa, Canada, Latin American, United States, and Asia in countries like Malaysia, Japan and India. Also it is used in Middle East, Australia, New Zealand, Europe including Italy, Northern, Western and Central Europe and it could be received as far as Cyprus. Russian Federation, United Kingdom and Nordic countries are the pioneers of using Direct Broadcast Satellite (DBS) intended for home reception. The term DBS or Direct-to-Home (DTH) services are used to distinguish satellite services from Telco-satellite services.

In Africa, satellite television has been far more successful than cable, mainly due to the lack of infrastructure for cable television and the high cost of installation. Furthermore, the cable network maintenance is expensive in Africa because of the need to cover larger and more sparsely populated areas. The majority of Africans cannot afford paid cable television though there are some terrestrial Pay-TV and Multi-channel Multi-point Distribution Service (MMDS) operators.

In Russia, thanks to the Moskva Global'naya system (or Moscow Global 1989), TV signal could be received in any country except Canada and North-West of the USA. Modern Russian satellite broadcasting service based on powerful geostationary satellites provides mostly free-to-air television channels to millions of householders. Pay-TV is still not popular among Russian TV viewers and only the NTV Russia news company broadcasts a few encrypted channels via its own communications satellite constellation.

According to the www.Fact-Archive.com (online encyclopaedia), the overall market share of DBS satellite services was 21.4% of all TV homes in Europe in 2004; however, this highly varies from country to country. For example, in

Germany, with many free-to-air TV-stations, DBS market share is almost 40%, and in Belgium and the Netherlands, it's only about 7%, due to the widespread cable networks with exclusive content.

2.2.1.2 DVB-C

The DVB-C system for digital cable networks was developed in 1994 [26]. It uses the 64-Quadrature Amplitude Modulation (QAM) scheme, and for the European satellite and cable environment can, if it is needed, convey a complete satellite channel multiplex on a cable channel. The DVB-CS specification described a version which can be used for Satellite Master Antenna Television (SMATV) distribution systems [27].

Recently, following the ever increasing hunger for bandwidth for broadcast and narrowcast services, the DVB Project conducted study on a new standard incorporating enhanced coding and modulation techniques for cable systems. DVB was able to identify several cutting edge technology candidates for a second generation cable transmission system (DVB-C2). The commercial requirements set out by DVB challenged engineers to create a transmission system that combined a high degree of efficiency and flexibility. The target set was to achieve at least 30 percent more spectrum efficiency and to provide the technical flexibility needed to transmit present and future services. The development of the specification is almost finalised and the DVB-C2 group plans to present their draft specification to the DVB Technical Module in March 2009 [24].

The Cable-TV (CATV) provides television or radio services through fibre optic networks or coaxial cable. It has been widely deployed in many countries for distribution of broadcast programmes. It is deployed in more than 50 million cable tuners worldwide mostly located in North America, Europe (esp. Switzerland and UK), Australia, Canada and East Asia. However, CATV has a

little success in Africa because of that laying the cable in that sparsely populated area is not cost effective.

2.2.1.3 DVB-T

The digital terrestrial television system (DVB-T) is more complex than former systems; due to noise, bandwidth environment, and multi-path situations in the terrestrial channel [28]. The system has several dimensions of receiver 'agility', where the receiver is required to adapt its decoding according to signalling. The key element is the use of Orthogonal Frequency-Division Multiplexing (OFDM). There are two modes in the DVB-T system: 2K carriers plus QAM, 8K carriers plus QAM. The 8K mode allows more multi-path protection, but the 2K mode offers Doppler advantages where the receiver is moving. The 8K mode can be used for both single transmitter operation and small/large SFN networks, but 2K mode is suitable for single transmitter operation and for small SFN networks with limited transmitter distance.

The digital TV world is mainly broadcast through satellite or cable. However some plans have been adopted towards increasing the terrestrial broadcast system in the world. Fig. 1 shows the worldwide coverage of digital TV terrestrial (DTT) services, according to the www.aquivo.co.uk.

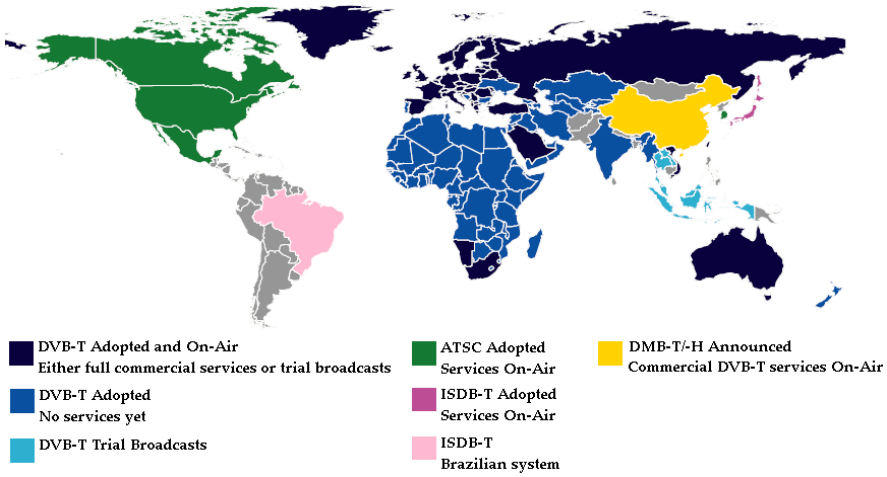


Fig. 1: Worldwide coverage map for terrestrial services

2.2.1.4 DVB-H or Personal TV

This is a more flexible and robust digital terrestrial system, which has recently been developed [31]. The system is intended to be receivable on handheld receivers and thus includes features which will reduce battery consumption (time slicing) and operates on the 4K OFDM mode, together with other measures. DVB-H services will probably use more efficient video compression systems such as MPEG-4 Advanced Video Coding (AVC) or SMPTE VC1.

DVB-H has been commercially launched in some European countries like Finland, Switzerland, Netherlands, Italy, Austria and Albania. In the UK, two trails were launched in Oxford and Cambridge which presented promising results.

2.2.1.5 DVB-S2

This is a higher efficiency digital satellite broadcasting system, which has recently been developed [32], [105], [109]. It has both DVB-S backwards-compatible and non-backwards-compatible versions. The non-compatible version allows almost 30% more data capacity for the same receiving dish size compared to DVB-S. It uses 8-Phase Shift keying (PSK) and Low Density Parity Check (LDPC) code to achieve higher efficiency. The DVB-S2 is likely to be used for all future new European digital satellite multiplexes, and satellite receivers will be equipped to decode both DVB-S and DVB-S2.

2.2.1.6 DVB-SH

The DVB-S service to handheld devices (DVB-SH) was standardized by DVB Project in February 2007 [110]. It is a physical layer standard for delivering IP-based media content to handheld terminals (i.e. mobile phones, PDAs, etc.) It is based on a hybrid satellite or terrestrial downlink and a mobile-based uplink (i.e. GPRS). It has been designed for frequencies below 3 GHz, supporting Ultra High

Frequency (UHF) band, Low Band or Satellite band. It complements and improves the existing DVB-H physical layer standard. Similar to the DVB-H, it is based on DVB-IP Datacast (IPDC) delivery, electronic service guides, and service purchase and protection standards. However, the DVB-SH offers a number of enhancements in comparison with the DVB-H:

- More alternative coding rates are available;
- The 64-QAM modulation scheme has been omitted;
- The support for 1.7 MHz bandwidth and 1K FFT;
- FEC using Turbo coding;
- Improved time interleaving;
- Support for antenna diversity in receivers.

DVB-SH specifies two operational modes:

- *SH-A*: specifies the use of COFDM modulation on both satellite and terrestrial links with the possibility of running both links in SFN mode.
- *SH-B*: uses Time-Division Multiplexing (TDM) on the satellite link and COFDM on the terrestrial link.

2.2.1.7 DVB-T2

In March 2006 DVB decided to study options for an upgraded DVB-T standard. In June 2006, a formal study group named Technical Module on next generation DVB-T (TM-T2) was established by the DVB Group to develop an advanced modulation scheme that could be adopted by a second generation digital terrestrial television standard, named DVB-T2. The European Telecommunications Standards Institute (ETSI) has received the DVB-T2 draft standard from DVB Project on June, 2008. The standard will be known as ETSI "EN 302 755". However, from the DVB-T2 fact sheet published by the DVB Project, the DVB-T2 specifications can be summarised as follows.

- It is backward compatible with DVB-T, which is active on 35 countries;
- It can deliver multimedia contents to fixed, portable and mobile devices;
- It offers 30-50% more payload, which can be extended to 100%, if it adopts the Multiple-Input-Multiple-Output (MIMO) technique, but new aerial is needed;
- It has higher bit rate and improved spectral efficiency:
    - It implements the OFDM modulation with large number of subcarriers; i.e. 16K and 32K subcarriers in addition to 2K and 8K;
    - It uses a rotated constellation which provides robustness in difficult channels: 256-QAM in addition to QPSK, 16-QAM and 64-QAM;
    - It uses robust error correction techniques: Low Density Parity Checking (LPDC) combined with Bose-Chaudhuri-Hocquengham (BCH) error correction coding that employs turbo decoding principle;
    - It uses MPEG-4 H.264 video codec which is more efficient than the MPEG-2 video codec;
- It is flexible to adjust a signal for a specific transmission channel to meet the reception condition; i.e. Indoor antenna and roof-top antenna;
- It can reduce the power consumption at the receiver by tailoring the transmission to decode just a single programme rather than the whole multiplex programmes;
- It is IP ready as it implements the Generic Stream Encapsulation (GSE), which is an evolved version of the encapsulation of IP in MPEG TS over physical layer. The GSE provides more than 30% gain in capacity especially for IP-based services;
- It implements Future Expansion Frame that the standard can be compatibly enhanced in the future.

2.2.1.8 DVB-IPTV

The DVB-Internet Protocol TV (IPTV) is the collective name for a set of open, interoperable technical specifications, developed by the DVB Project [104], [107]. It facilitates the delivery of digital TV using Internet Protocol over bi-directional fixed broadband networks. The work is taking place in two phases: the first phase covers delivery over managed networks and the second phase covers Internet delivery. The objectives in the first phase can be listed as follows.

- Delivery of MPEG-2 over IP network
    - Including multicast (broadcast) video or Unicast services as part of the Triple-Play services (voice, video and data) being deployed on a converged IP-based network structure
- Connection of an IPTV-STB to an IP network
- Standardisation of the Broadband Content Guide and Service Discovery & Selection mechanism to recognise the unicast and multicast offerings of IPTV service operators on a broadband network
- Addressing issues like:
    - Content downloading
    - Retransmission
    - Profiling
    - Hybrid DVB broadcast and DVB-IPTV services

The challenges in the second phase can be categorised as follows:

- More flexible stream composition to enhance IPTV services;
- More straightforward interfaces to enhance n-Play solutions;
- Distribution of commercial contents over the Open Internet;

The key specifications already published in DVB-IPTV include:

- ETSI TS 102 034: Transport of MPEG-2 TS-Based DVB Services over IP Based Networks;

- ETSI TS 102 539: Carriage of Broadband Content Guide (BCG) Information over Internet Protocol;
- ETSI TS 102 824: Remote Management and Firmware Update System for DVB IP Services.

2.2.2 Other Digital TV Standards

The Advanced Television Systems Committee (ATSC) is the group, established in 1982, that developed the eponymous ATSC Standards for digital television in the United States, also adopted by Canada, Mexico, South Korea, and recently Honduras and is being considered by other countries. The ATSC systems will replace the NTSC analogue system in the United States in 2009 and in Canada in 2011. The ATSC uses the 188-byte MPEG-2 transport stream packets to carry data. It also supports H.264/MPEG-4 Advanced Video Coded (AVC). The ATSC signals have been designed to use the same 6 MHz bandwidth used in the NTSC. After the digital signal is compressed and multiplexed, the transport stream is modulated depending on the following standards.

- ATSC-T (Terrestrial): it uses 8-VSB modulation scheme that can transfer maximum data rate of 19.39 Mbps;
- ATSC-C (Cable): it operates at higher signal-to-noise ratio (SNR) and can use 16-VSB and 256-QAM modulation schemes to achieve a throughput of 38.78 Mbps using the same 6 MHz bandwidth;
- ATSC-M/H (Mobile): it uses 8-VSB modulation with 19.39 Mbps data rate.

Another family of digital TV standards is the Integrated Service Digital Broadcasting (ISDB) which has been originally adopted in the Japan and recently in the Brazil. The ISDB standards are maintained by Japanese Association of Radio Industries and Businesses (ARIB) [20]. The ISDB is based on MPEG-2

video and audio coding and transport stream described by the MPEG-2 standard. The core standards of ISDB are as follows.

- ISDB-S for satellite television which uses PSK modulation scheme on 12 GHz band;
- ISDB-T for terrestrial television which uses COFDM with PSK/QAM schemes on 5.6 MHz transmission bandwidth. The OneSeg is the name of an ISDB-T service for reception on mobile phones and portable devices. ISDB-T and ISDB-Tsb are for mobile reception in TV bands;
- ISDB-C is the cable digital broadcasting standard.

The Digital Multimedia Broadcasting (DMB) known as mobile TV is a South Korean technology which can operate on the satellite (S-DMB) and terrestrial (T-DMB) transmissions. DMB is based on the Eureka-147 Digital Audio Broadcasting (DAB) standard, and has some similarities with the main competing mobile TV standard - DVB-H. The China has then adopted the DMB-T/H or Digital Terrestrial Multimedia Broadcast (DTMB) standard for both fixed and mobile terminals.

2.3 DVB Return Channels

The interactivity between a service provider and viewers in DVB network is established via a return channel to the transmission system. The enhancement of the communication technology has influenced the ways whereby an end-user can communicate with the intermediate networks that connect to the service providers.

Solutions for interactive services incorporate of a set of specifications describing protocols and interfaces for all kind of transmission media and network scenarios. Interactive services refer to the services, which need to have

interaction between users and service providers. Currently the interactive TV services are offered in three main categories as follows:

- *Participation television* – predominantly in analogue services – where the viewer can participate to some degree in the programme through the use of a return channel such as the phone, SMS or e-mail;
- *Enhanced digital television* where the viewer has only local interactivity, as no return channel is available. It means that data belonging to a certain interactive service is transmitted over the broadcast network and stored in terminals;
- *Interactive digital television* on terrestrial, satellite, cable or broadband networks where the viewer has access to some kind of return channel(s);

According to the complexity level of the interaction and transmission capacity, the return channel from user to service provider could be either one-way narrow-band path, or bi-directional narrow/broadband path. The data rate in the return channel varies depending on the type of the channel. For instance, the data rate in terrestrial network is up to 20 Mbps per channel and in satellite or cable networks is up to 38 Mbps per channel or few Kbps in case of simple telephone modem.

The deployment of interaction channel is divided into two levels. First, the higher level design that is network independent and deals with the diverse applications interacting with the users. Second, the lower level design that is network dependent and provides the physical channel for interaction purposes. The following sections will explain the network-dependent design of some interaction channels in the DVB network.

2.3.1 DVB-S Return Channel

Currently, the scope of using satellite systems for the provision of DVB interaction channel is mainly limited to the business-to-business environment. However, with the growth of market, it is predicted that it will be introduced in a domestic environment too. In the specification of DVB-Return Channel for Satellite systems (DVB-RCS) the interactivity is achieved through the geostationary satellite interactive networks and fixed Return Channels Satellite Terminals (RCST). The main functional blocks in the DVB-RCS are as follows [30]:

- *Feeder*: It transmits the DVB-S/S2 forward signal (uplink signal) conveying the user data or control timing signal. The timing information is needed for the operation of the satellite interactive network and synchronisation between the uplink and downlink.
- *Network Control Centre (NCC)*: it provides Monitoring and Control Functions (MCF). It generates the control and timing signals for operation of satellite interactive network to be transmitted by Feeder station(s).
- *Traffic Gateway*: It receives RCST return signals and provides accounting, interactive services or connection to service providers;

The synchronisation between RCST and satellite interactive network is handled via the Network Clock Reference (NCR). The NCR is retrieved by RCST from MPEG-2 TS with a specific Programme Identifier (PID). The RCST reconstructs the reference clock from the received NCR and compensates the carrier frequency.

On the forward link the RCSTs should be uniquely identified by a physical MAC address and Logical address. The MAC address is a 48-bit value compliant with IEEE 802.3 standard that is stored in a non-volatile memory corresponding to a unique RCST physical identifier. The Logical address consists of two fields:

the Group ID and Log-on ID. The 8-bit Group ID corresponds to a group of logged on RCSTs. The 16-bit Log-on ID uniquely identifies the RCST within a Group ID.

Fig. 2 shows a reference model for the DVB-RCS. The download transmission (SAT FW) and the return channel uplink transmission (SAT RT) can be provided by two separate satellites or just one satellite, which is used for both down/up link purposes (as in reality).

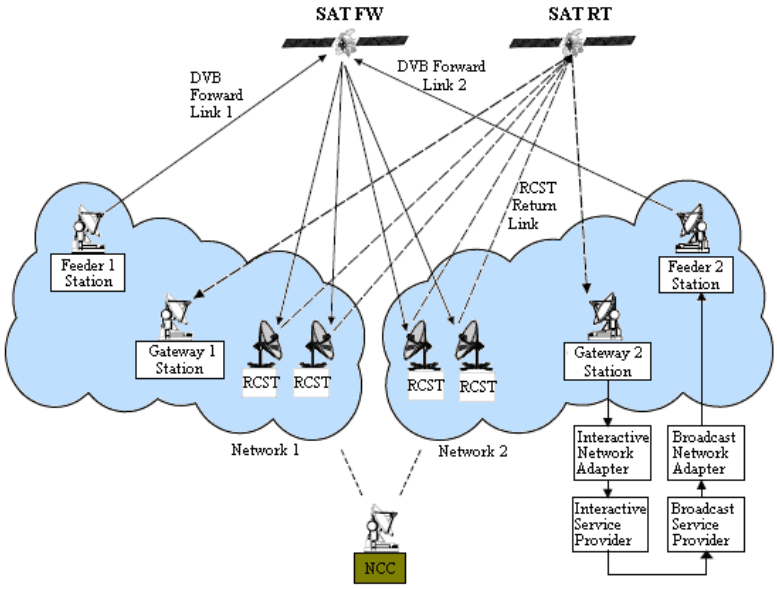


Fig. 2: A reference model for satellite interactive network

2.3.2 DVB-C Return Channel

The physical layer specifications, framing, slot timing assignment and MAC functionality of this system are well defined in the DVB Interaction Channel for Cable TV Distribution System (CATV) [35].

The Cable TV (CATV) supports a bi-directional path between a user terminal and service provider. The CATV interactive path consists of a Forward Interaction path (downstream) and a Return Interaction path (upstream). The downstream is used to send the synchronization and information from the Interface Network Adapter (INA) at the head-end to all Network Interface Units

(NIU) at receive-ends. This allows the NIUs to adapt themselves to the network and send synchronized information upstream.

An access control mechanism needs to be applied in CATV to manage the multiple accesses to a shared coaxial cable. The Time Division Multiple Access (TDMA) technique is used to divide the upstream transmission into time slots, which can be used by different end-users. One downstream channel is used to synchronize up to 8 upstream channels. A counter at the INA is sent periodically to the NIUs, so that all NIUs work with the same clock. This gives the opportunity to the INA to assign time slots to different users. The access modes adopted for this system can be based on contention or contention-less access, which vary in the level of congestion with the other users.

In order to synchronise and provide information to all units, two alternatives are defined: In-Band (IB) and Out-Of-Band (OOB) downstream signalling, albeit a set-top box which does not need to support both systems.

In OOB signalling, a Forward Interaction path is reserved for interactive data and control information. In this case, the presence of this path is mandatory. Also it is possible to send higher bit-rate downstream information through a DVB cable channel, whose frequency is indicated in the forward information path.

In the case of IB signalling, the Forward Information path is embedded into the MPEG-2 TS of a DVB cable channel. However, it is not mandatory to include the Forward Information path in all DVB cable channels.

Both systems can provide the same quality of service (QoS). However, the overall system architecture will differ between the networks which are using IB and OOB set-top boxes. Both systems may exist on the same networks, if different frequencies are assigned to each system.

Each set-top box has two addresses:

- *MAC address*: a 48-bit value representing the MAC address of the NIU that could be hard coded in the set-top box or provided by an external source;
- *NSAP address*: a 160-bit value representing the network address provided by the higher level during the communication.

The INA can establish a unicast communication with a particular user using set-top box addresses. Also, having the address of each set-top box, the upstream information can be differentiated at the INA.

For the interactive downstream OOB channel, a data rate of 1.544 Mbps or 3.088 Mbps may be used. There is no limitation for downstream IB channels; however, data rate shall be the multiple of 8 Kbps.

The INA specifies the rate of upstream transmission used by the NIUs, which may be 3.088 Mbps, 1.544 Mbps or 256 Kbps. Only the implementation of one of these bit rates would be mandatory. Upstream framing consists of packets of 512 bits (256 symbols), which are burst from the different users present on the network.

Fig. 3 presents a reference model for an interactive system in Cable TV (CATV).

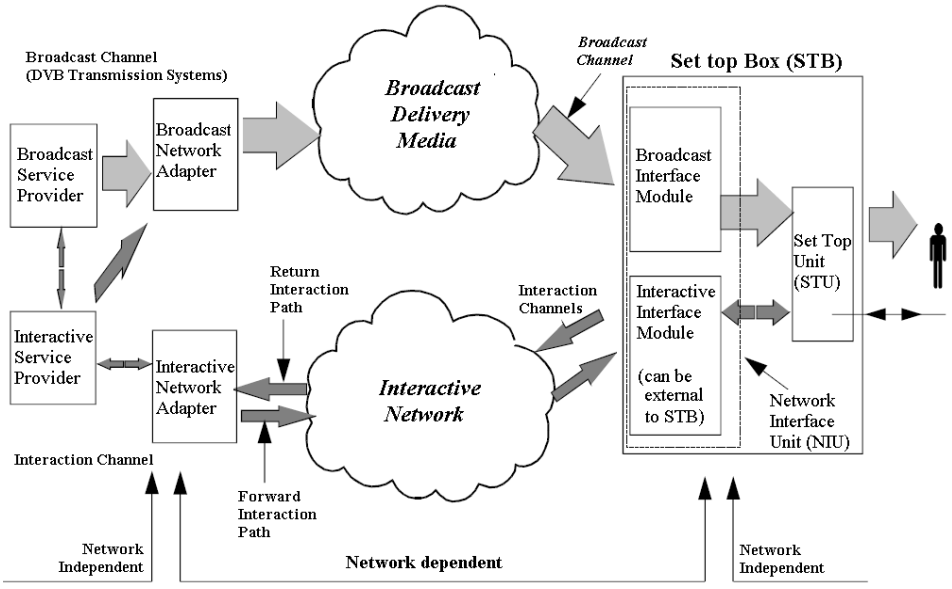


Fig. 3: The interactive CATV functional diagram

2.3.3 DVB-T Return Channel

The DVB Return Channel for Terrestrial system (DVB-RCT) is able to provide interactivity using existing infrastructure for digital terrestrial TV. It connects the Return Channel Terrestrial Terminals (RCTT) to an Interactive Network Adapter (INA).

The forward interaction path is embedded in the broadcast channel. As a result, the terrestrial interactive network consists of two unidirectional physical layers. The downstream direction is comprised of the broadcast plus forward interaction paths and the upstream direction is the return interaction path.

The downstream direction uses the DVB-T, which is based on MPEG-2 TS. A specific PID is assigned for signalling messages for interactive services. The application data and signalling messages in reverse are encapsulated in the Asynchronous Transfer Mode (ATM) cells to be mapped onto the physical bursts of a VHF/UHF transmission system. DVB-RCT offers a wireless interaction channel for interactive digital terrestrial television even in the congested UHF/VHF bands. The DVB-RCT is compatible with different DVB-T systems (6, 7 or 8 MHz) around the world.

The functional diagram proposed for the DVB-RCT is similar to what was presented in Fig. 2. The downstream transmission from base station (INA) provides synchronisation and management information to all RCTTs. This information is used by the RCTTs in order to access to the upstream channel and transmit synchronously to the base station. A single antenna at the remote station is sufficient to receive broadcast and forward interaction channels and send the information on the backward interaction channel. The multiple flexible OFDM system can manage cost-effectively the UHF/VHF spectra.

The main elements contributing into the service deployment cost in broadcasting systems are user terminals, bases station costs and indeed the cost

of the backhaul-linking network from the base stations to the service provider's main hub, which is normally valid on existing broadcasting networks. The DVB-RCT system is cost effective due to the single low cost receive system used at the base station, which can process up to 20k short interactions per second. Therefore, the deployment cost of DVB-RCT is considerably lower than any rival system like PSTN or GSM. In addition, the DVB-T and DVB-RCT networks can provide wire-free services for home reception. This results in enormous savings for service providers as they can launch new services and generate more revenue streams with minimal changes in the service delivery configuration.

2.3.4 GSM Return Channel

The Global System for Mobile Communication (GSM) infrastructure can provide interaction channel for broadcasting systems [29]. It provides a bi-directional wireless communication between the head-end and receiver-end. The GSM network can be whole or a part of the interaction network. It can connect to another network (i.e. PSTN, ISDN) to reach to the service provider.

At the receiver-end, the set-top box shall be equipped with a GSM Interactive Interface Module (IIM) to access to the GSM network. The interface between the set-top box and GSM network should be compliant with the standards on general Terminal Adaptation Functions (TAF) for mobile stations and for services using asynchronous bearer capabilities [48], [49]. Also the interface between the GSM network and the external network to provide the whole interaction channel shall be compliant with the general and signalling requirements on inter-working between the GSM Network and the ISDN or PSTN or any other GSM inter-working specifications [50], [51]. Depending on the external network, the mobile station should be configured to support the right bearer capabilities. When possible, it is preferential to implement GSM-ISDN

inter-working, which provides an end-to-end digital link between the IIM (i.e. set-top box) and the INA (i.e. service provider) with lower connection set-up times.

The physical interfaces vary depending on how the GSM mobile station is connected to the set-top box unit. The mobile station can be integrated with the set-top box as an internal or external module. The external mobile station should support the interface requirements between the set-top box as a Data Terminal Equipment (DTE) and the mobile station as a Data Communication Equipment (DCE) [38] and in the same way for the modem interface [33]. The internal (integrated) mobile station shall meet the same needs as external MS with the exception of providing the 9-pin interface connector.

New data services are becoming available with the evolution of GSM towards the third generation of mobile communication and in particular General Packet Radio Service (GPRS) offering a suitable interaction channel for the DVB service scenario with a similar reference model shown in Fig. 4.

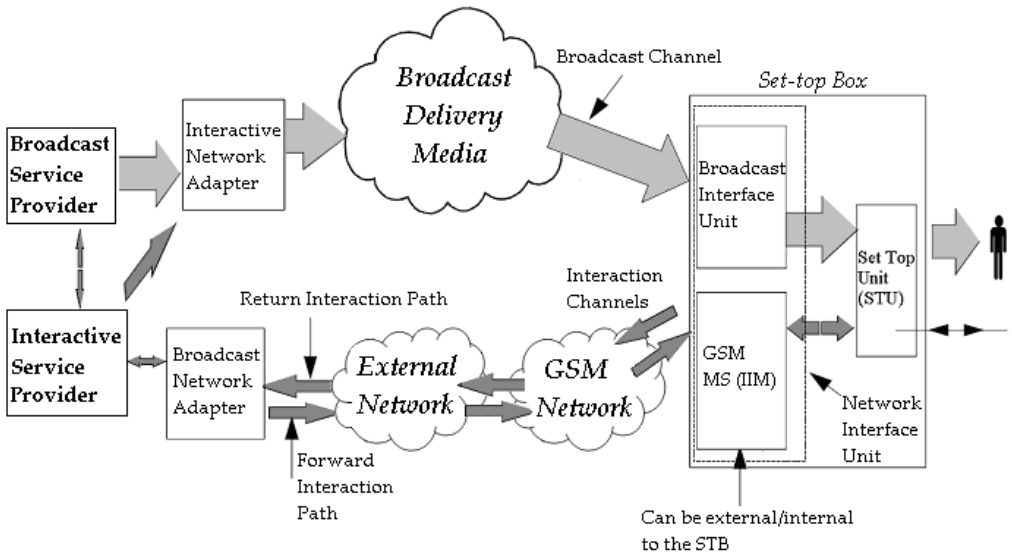


Fig. 4: System architecture when GSM is used as an interaction channel

In terms of popularity, GSM has been granted as the most popular technology by now spreading worldwide and attracting customers with a mix of services.

The GSM supports voice calls and data transfer speeds of up to 9.6 Kbps, together with the transmission of SMS (Short Message Service). The GSM operates in the 900 MHz and 1.8 GHz bands in Europe and the 850 MHz and 1.9 GHz bands in the US. The 850 MHz band is also used for the GSM and 3G in Australia, Canada and many South American countries.

By having a harmonised spectrum across most of the globe, the GSM international roaming capability allows users to access the same services when travelling abroad as at home. This gives consumers seamless and same number connectivity in more than 218 countries. The terrestrial GSM networks now cover more than 80% of the world's population (i.e. over 2 billion customers). The GSM satellite roaming has also extended service access to areas where terrestrial coverage is not available. Fig. 5 shows the GSM world coverage, Fig. 6-(a) reveals the technology market share and Fig. 6-(b) reveals the regional share of mobile subscribers [52].

Fig. 5: The GSM world coverage 2008

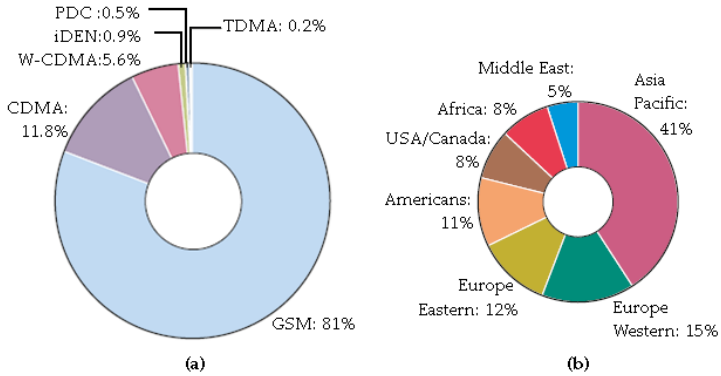


Fig. 6: (a) Mobile technology (b) regional market shares in global market

In terms of implementation and deployment costs, the GSM is more affordable and profitable (especially for developing countries) in comparison with the other technologies mentioned earlier. The features like mobility and roaming makes this technology outstanding among the rest. The GSM has been even more promoted with releasing the new data service scenarios – like GPRS – and converging to the Internet to form a global public network like Long Term Evolution (LTE) and All IP Network (AIPN).

2.3.5 Internet Return Channel

The return channel through IP network provides interactivity in TV specific services, interactive programming services and interactive services. The DVB-IPTV can be part of this declaration as well [104], [107]. In the IPTV both broadcast (constructed by multicast mode) and return channels (upstream) are implemented via Internet protocols. The IPTV performs better than DVB on interactive services, but traffic engineering for broadcasting services will be a big challenge for the current Internet architecture. The United States has announced that Internet operators are allowed to provide higher bandwidth service with two-tiered Internet architecture. This is promising news for IPTV operators to develop their businesses on the broadband Internet.

The Internet can be integrated into the DVB network to provide up/down interaction channels. In this view, the Internet protocols and web-based services can deliver a wide range of audio/video services to TV consumers. The Internet Engineering Task Force (IETF) has developed many networking protocols that make these services possible. On the other hand, the DVB IP Infrastructure has delivered the architectural framework for DVB Services on IP as a reference model for an end-to-end IP system [104]. In the architecture, the need for specifications of the transport of DVB Services over IP-based networks, service

discovery and selection, network provisioning, IP addressing and home network segments for Ethernet and IEEE 1394 has been identified. In addition, a network layer security needs to be applied based on the DVB Content Protection and Copyright Management (CPCM) [111]. The transport of DVB services over IP (i.e. MPEG-2/4 TS) was ratified by steering board. The DVB set of IP networking is network independent and it is accessible via DVB physical layers (i.e. DVB-S/-C/-T) in combination with appropriate return channels. The DVB-IP protocols are also intended for the home networking on wired and wireless physical layers. Adoption of the IP networking will greatly increase accessibility of real-time and storage-based video and audio services to consumers.

2.4 Interactive Middleware Standards

The middleware is an important component to construct embedded applications for set-top boxes, handsets for DVB-H, etc. This section will describe the middleware in the terminals used for the broadcasting services.

In the set-top box market, there are two main types of middleware: Proprietary and Open standards, which are explained as follows.

2.4.1 Proprietary Middleware

In the proprietary middleware, the following products are known as the main players in the market.

- *MediaHighway* is interactive television middleware software introduced in 1993 by Paris-based Canal+ Technologies SA, part of the Canal+ Group. It is currently owned and developed by the NDS Group, which acquired it from Thomson SA in 2003. According to the manufacturer it is (as of December 2007) used by 69 million set-top boxes in the world on every type of digital TV platform (i.e. cable, satellite, broadband, digital terrestrial networks, etc.) It has been deployed by more than 25 operators

worldwide including: France's Canal Satellite, Sky Italia, Sky Latin America, STAR and YES (Israel). It has also been selected by DIRECTV as the basis for their new interactive platform [79];

- *The Liberate* middleware solution is based on the HTML and JavaScript software engine, which is called Navigator Standard. The Navigator Standard is composed of a customisable component that is used to match the individual's needs of service provider and support a limited number of interactive applications like Interactive TV Sites. It has TV browser and rendering capabilities built-in to support the Interactive TV sites. The Liberate stopped operating in 2005 and it is no longer a reporting company under the Securities Exchange Act of 1934;
- *The Betanova* middleware developed by Beta Research is dependent on the D-Box set-top box platform. The Betanova and D-Box have been limited to the German market. The first version of the Betanova middleware was based on the C/C++ programming language. In 1999, BetaResearch deployed the world-wide and first Java-based middleware called Betanova 2.0. BetaResearch is committed to Multimedia Home Platform (MHP) now such that, the Betanova 2.0 is fully compliant with MHP [15], [16];
- *Microsoft TV* is a middleware developed by the Microsoft targeting both mid-end and high-end set-top-boxes. The Microsoft TV is a software platform designed specifically for today's cable architecture. It obviously runs on top of the Microsoft Windows operating system and can provide a number of DTV applications such as, Video-On-Demand, Electronic Programme Guide, PVR functionality and access to HDTV programmes [74];

- *Open TV Inc.* is a middleware provider with the largest number of deployments worldwide. At present, it is leading the middleware players in the vertical market, reaching over 27 million set-top-boxes produced by more than 30 worldwide suppliers [15]. The core middleware architecture of the Open-TV is said to be hardware independent, modular and extensible [89]. Due to the great number of set-top-box manufacturers and service providers employing Open-TV, different conditional access systems and wide range of interactive applications are needed. In this respect, Open-TV supports Near-Video-On-Demand, Pay-Per-View (PPV), EPG, PVR functionality and downloading of data and applications. The Open-TV applications are written in C-code by means of a virtual machine interpreter. The 'C' virtual machine is an execution environment that supports the Open-TV Software Developer's Kit (SDK) APIs, which allows content providers to create DTV applications in C-code. Apart from the C-code execution layer, the Open-TV provides compatibility with HTML and Java code applications, and hence extends Open-TV middleware to support DVB-MHP. Furthermore Open-TV offers a range of development tools for creating interactive TV applications for Open-TV middleware [83].

2.4.2 Open Standard Middleware

As part of Open standards, MHEG, MHP, OCAP and ACAP are the outstanding international standards.

2.4.2.1 MHEG

The MHEG-5 [56] has been created by the Multimedia and Hypermedia Experts Group. The MHEG-5 is a standard devised for the middleware of digital teletext services in the UK. The MHEG-5 applications need the MHEG-5 engine

to be run. The engine integrated into the set-top box presents the pictures to a TV viewer and handles the navigation and interaction between the pictures as requested by the viewer. The MHEG-5 was particularly designed to be supported by scarce resource systems, so it is ideal for low-end set-top boxes. The MHEG versions have been ratified as follows.

- MHEG-6 [57] is an extension to MHEG-5 allowing the creation of Java-based applications;
- MHEG-7 [58] defines test and conformance procedures of MHEG-5 applications;
- MHEG-8 [59] provides XML scripting for MHEG-5.

In the UK, the MHEG is the main middleware though it can exist with MHP through its plug in/out MHP [73].

2.4.2.2 JAVA TV - The Predecessor of MHP

Before the development of MHP, Java was mainly used as a scripting language or a plug-in extending other platforms. Some standard bodies, such as Digital Audio-Visual Council (DAVIC), who had defined several Java APIs for DTV, placed Java as an extension to current technologies like MHEG-6. The DAVIC is a non-profit organization established in Switzerland in August 1994 and folded five years later. The DAVIC 1.3.1 became an International Standard, closely associated with the DVB and several joint standards [19]. Nowadays, the Java TV is widely supported by the Sun Microsystems. The Java TV is a Java-based software framework designed for use on TV set-top boxes, based around components called Xlets. It is currently used only on the Connected Device Configuration (CDC), specifically for iTV applications development.

The API includes the Xlet classes in the package javax.tv.xlet. Other packages of the public API include:

- javax.tv.graphics - provides a simple rendering canvas;
- javax.tv.locator - provides a locator in the style of a URL for services and media, such as service:/SERV1;
- javax.tv.service - defines a mechanism for service information (SI) databases and APIs representing the SI elements, such as the TV channels and media available for playback.

2.4.2.3 MHP

In 1997, the DVB consortium decided to develop an open middleware system standard to resolve the issues of software and hardware interoperability. The approach to this end was to hide the hardware and operating system specifications from the actual iDTV applications.

The MHP specification version 1.0 was finalised by the DVB Project in February 2000 and published by ETSI in July 2000. In June 2003, MHP v.1.0.3 was released after removing many errors and ambiguities of its forerunner [36].

The MHP as an open middleware system standard defines a generic software interface (API) between interactive applications and the terminal on which those applications reside and execute. It enables the content provider to address various types of terminals, ranging from set-top boxes and integrated TV sets to multimedia PCs. As an "offspring" of the DVB project, the MHP extends all the DVB open standards and all transmission networks. MHP 1.1 defines the next generation of the Multimedia Home [86].

2.4.2.4 OCAP & ACAP

Following the development of MHP by DVB project in Europe, the standard organisations in the United States decided to develop open middleware solutions. The ATSC group defined the Advanced Common Application Platform (ACAP) middleware standard for the Terrestrial and Satellite TV,

whilst the CableLabs consortium developed the Open Cable Application Platform (OCAP) middleware platform for Cable systems.

At the time, MHP was under development and rather than reinvent the wheel, CableLabs decided to re-use elements of the MHP standard where it was appropriate.

The OCAP provides interactive TV service providers and application developers with a middleware software specification. This middleware enables them to design products that would be run successfully on any cable TV system in North America, independent of the set-top box, TV receiver hardware or operating system. Similar to the MHP, OCAP applications are categorised as:

- *Java-based* Applications also known as OCAP-J;
- *HTML-based* applications.

OCAP also supports three different models of applications:

- *Bound applications* are linked directly with the channel in which the user is currently tuned. So, it terminates when the viewer selects another channel;
- *Unbound applications* are independent from any particular channel. So, they remain operational even if the viewer selects another channel;
- *Native* are applications written for a specific host and are not related to a specific broadcast. These may be stored in the firmware of the set-top box [82].

The ACAP has been the result from collaboration between the CableLabs OCAP standard and the previous DTV Application Software Environment (DASE) specification of the ATSC. Similar to the OCAP, it is derived from the MHP however there are some differences between them. These include adopting a slightly modified version of the carousel system used by MHP, a mandatory return channel and support for independent applications, which can be run at any time without binding to a particular channel.

ACAP applications are also classified into categories depending upon the initial process of the application content, which can be based on a procedural or declarative language. These categories of applications are referred respectively to Procedural (ACAP-J) and Declarative (ACAP-X) applications [11].

2.4.3 Portable Digital-TV Middleware

Middleware like MHP has designed originally for a stationary living-room environment where there is no issue regarding power supply and processing power of the terminal. Nowadays, the Broadcast industry is facing a novel trend towards portability as a result of the telecommunication/mobile and broadcast networks convergence. In this case, Digital TV cannot be an exception and it ought to respond to this new type of demand. As such, the DVB project has defined a standard for the portable community of viewers, DVB-H, which deals extensively with the power consumption issue.

The applications running as part of the middleware in a set-top box are mainly resource greedy and need an acceptable level of accuracy at the information received through the air. In order for the applications to be run on the low processing power terminals under the error prone nature of the radio-based networks, a series of new standards needs to be developed to address the deployment of the middleware on the portable devices.

The Multimedia Car Platform (MCP) draws together a number of car and receiver manufacturers and network operators to define a specification for an open multimedia platform in the car. The MCP is based on the architecture of hybrid DVB-T/GSM networks, including service hand-over and interoperability between different networks. Therefore the errors occurred during the transmission could be recovered dynamically via the interaction channel. The MCP defines its own dedicated APIs and also recruits some MHP APIs for the in-

car systems; such as the Navigation API, Car Data API [12]. Some projects have implemented the platform, such as Dynamic Radio for IP-Services in Vehicular Environments (DRiVE) [21].

On the mobile-TV handset, the Java Specification Request (JSR) defines an optional package in J2ME/MIDP/CLDC environment to provide functionality to handle broadcast content for instance to view digital television and utilize its rich features and services [64].

Regarding the development of DVB-H, the handset of mobile TV must converge with mobile phone (2G/3G). Some convergence handsets have already been developed supporting GPRS/UMTS and Broadcast services. Also, the middleware on the handset needs to be the convergence of middleware of the DVB and mobile communication industry. The security and authentications of such handsets must be solved according to the 3GPP standards.

2.5 Summary

The digital TV (DTV) was introduced in the late 1990s, in contrary to the analogue TV. The DTV has opened new business opportunities for TV broadcasting and consumer electronic industries. The TV consumers have also embraced the technology as it offers wider range of higher quality of services than the former system. The DTV has proved to be more bandwidth efficient and as such capable of offering more number of channels. The characteristic of digital signals depends on the physical layer (medium) used for service delivery. The main medium used in the broadcasting systems are satellite, cable and terrestrial systems. It is predicted that the DTV will reach almost half a billion homes around the world by 2012 [54]. The report also forecasts 43% digital penetration by 2012, up from an estimated 264 million household by end of 2007. This

indicates that digital growth will accelerate as the decade progresses, especially in China, North America, Japan and India.

The digital Cable will be the main source of digital TV households, bringing in 249 million subscribers by 2012. The Direct-to-home (DTH) satellite will account for 23% of the global digital total by 2012; an overall decrease of 13% from 2007; due to the increase in Cable, IPTV and DTT. The IPTV will attract almost 37 million global subscribers by 2012. Although the IPTV will remain a niche platform but it will account for only 3% of global total by 2012. The digital terrestrial TV (DTT) homes on the other hand will witness a dramatic increase in number of subscribers; rose from 1.4 million in 2000 to 47.8 million in 2007 and then it is forecast to racket to 97.1 million global households by 2012. The digital growth is likely to extend away beyond the forecast period, since still 738 million homes would take analogue signals in 2012.

The interactive service support requires communication link and service enablers embedded at digital receivers. The communication link can be implemented either in the broadcasting or telecommunication networks. The cellular network (i.e. GSM) has nowadays gained worldwide popularity attracting media investors to deliver multimedia services via handheld terminals. Technologies like DVB-H and DVB-SH are of examples of such consideration. Nevertheless, the traditional TV viewing is yet recognised as the most important business model in the media industry; as such interactive product makers have been developing range of software applications to be run by a Middleware which sits on top of the hardware like a set-top box. The ACAP, MHEG and MHP (or Globally Executable MHP -GEM) are dominant Middleware standards operating in the North America, UK (recently in China, India and South Africa) and European countries.

The DVB-J or Xlet is the most popular type of MHP applications that is broadcast via an object carousel (i.e. DSM-CC) to MHP-enabled set-top boxes. The MHP application manager monitors, starts or stops the applications at the set-top box based upon information signalled via the Application Information Table (AIT) defined in the Service Information (SI) Table. The Java APIs are almost supported by the rest of Middleware standards too. They provide application programming interfaces like low-level MPEG access APIs, media control APIs, graphic APIs, application lifecycle APIs, communication APIs, etc. The broadcasting and managing applications in other Middleware standards are almost similar to what is briefly explained for the MHP standard.

The next Chapter is focused on wireless technologies that can be used for interaction between a service provider and an end-user and a set-top box. The GSM (WWAN) and Bluetooth (WPAN) are chosen here amid wireless technologies due to their popularity, connectivity and security features.

3 GSM AND BLUETOOTH TECHNOLOGIES

3.1 Introduction

The wireless technology has not only changed the way people communicate with each other but also eliminated the cable in many applications. The wireless communication encompasses various types of fixed, mobile and portable two way radios, mobile phones, etc. used for wireless networking or short-range communication. The GSM is the most known technology enabling the Wireless Wide Area Network (WWAN) configuration. According to the last statistics in 2008, it connects over 2.5bn people across the world and advances the personalisation concept. The Wi-Fi is another wireless technology enabling the Local Area Network (WLAN). It has been standardised under IEEE 802.11 family standard supporting different data rate, security feature and quality of service. Another popular wireless technology is the Bluetooth which has largely replaced the cable application for short-range connection. It is now integrated in almost any portable device like mobile phone, laptop, etc. It is considered as a technology enabler for Wireless Personal Area Network (WPAN) standardised under IEEE 802.15.

In this chapter the GSM network architecture and important functional elements of the network are thoroughly explained followed by providing an overview of the Bluetooth technology.

3.2 GSM Network

The primary aim of mobile systems is to extend the concept of personal communications in order to maintain the point of presence while travelling or roaming. This throws up two main challenges namely the location management

and call management with variable channel quality. The outstanding advantages of the GSM system are the mobility, roaming, ever increasing range of services and cost, which is affected from market competition and technology maturity. However there are some issues addressed to the GSM including limited bandwidth, high bit error rate (BER), security and health hazard concerns.

3.2.1 GSM Network Structure

Fig. 7 presents the key elements incorporated in a typical GSM network architecture. The elements and their relationships in the system are thoroughly discussed here.

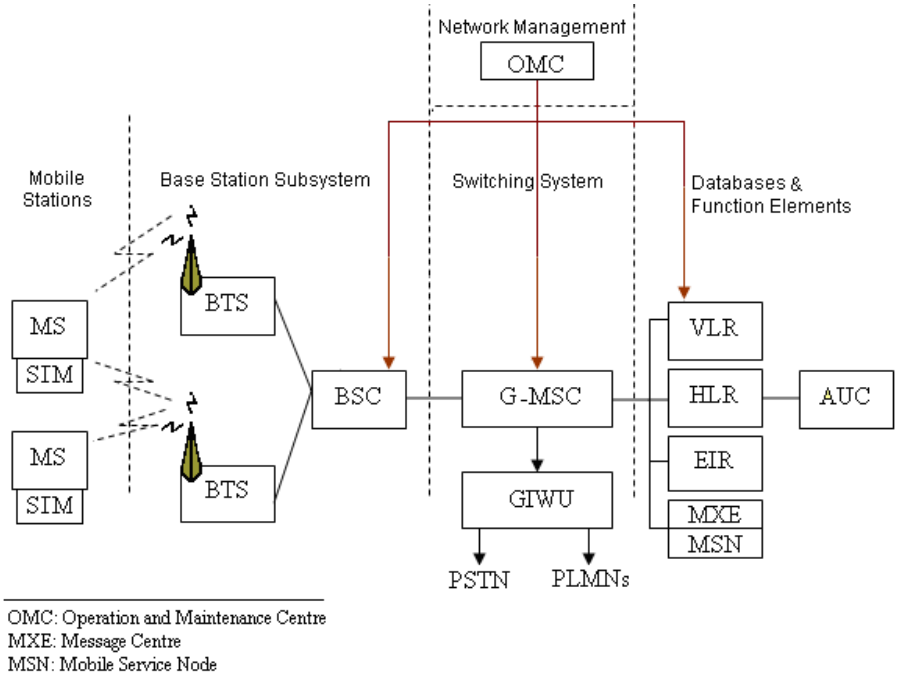


Fig. 7: The key elements of the GSM network architecture

The complexity of the GSM network is obscured from an end-user whose point of connection is only his mobile phone. Each mobile phone requires a detachable smartcard, which is called the Subscriber Identity Module (SIM) card, to connect to the network. With the evolution of technology, SIM cards are now having more storage and processing capacity offering more value-added services. One

of the technology enablers in the SIM card is the SIM Application Toolkit (SAT) to interact with the handset or mobile equipment via standard commands. The SAT applications must be small in size and developed in the SIM application development environment, which is costly and rigorously controlled by mobile operators. In light with these obstacles, Sun Microsystems has developed Java core technologies for both mobile equipment and SIM card. The J2ME profiles for resource-constrained devices together with the JavaCard technology have changed the mobile market and making them more application specific.

The SIM is the GSM security element which is deployed in the field and inserted into the mobile phone. The SIM and Mobile Station (MS) provide whole GSM services to GSM subscribers. The subscribers' data are stored in the SIM, Home Location Register (HLR) and Visitors Location Register (VLR). The Equipment Identity Register (EIR) blacklists the stolen/lost reported mobiles to prevent them from being used for any further business. The Authentication Centre (AUC) grants permission to SIM card in order to connect to the network and HLR.

The MXE is the message centre for voice, fax and data. It also handles the short message service (SMS), cell broadcast, voice/fax mail, e-mail, etc. The Mobile Service Node (MSN) is another functional element which handles the mobile intelligent network services.

The Operation and maintenance centre (OMC) connects to the elements residing in the switching system, base station and service subsystems. The Operation and support system (OSS) is the implementation of the OMC through which the network operator monitors and controls the system.

The HLR is considered as a database used in a Public Land Mobile Network (PLMN). It stores the details of each mobile phone subscriber, who is authorised to use the GSM core network. The details of every SIM card, which is issued by a

mobile phone operator, are saved in the HLR. One of the primary keys for each HLR record is the International Mobile Subscriber Identity (IMSI), which is used to uniquely identify the SIM. The telephone number known as Mobile Station ISDN number (MSISDN) is the next item associated to the HLR record. The remaining items stored in the HLR are namely service subscription details, updated location information, authentication and encryption keys. The HLR data is stored so long as a subscriber remains with the mobile phone operator.

The HLR is not just a database, but also it is a subsystem, which directly receives and processes Mobile Application Part (MAP) transactions and messages. It is worthwhile explaining that the MAP is a SS7 signalling protocol, which provides an application layer for various nodes in the GSM such as HLR, VLR, AUC, MSC, EIR and short message service centre (MXE). The main facilities provided by MAP are as follows: mobility services, operation and maintenance (i.e. retrieving a subscriber's IMSI), short message services. [106].

The GSM core network elements connected to the HLR are as follows:

- The Gateway Mobile Switching Centre (G-MSC) handles incoming calls;
- The VLR handles network access requests received from mobile phones;
- The Short Message Service Centre (SMSC) as part of the Message Centre (MXE) handles incoming SMSs;
- The Voice Mail System delivers notifications to a mobile phone that a message is waiting.

The procedures implemented in HLR are as follows:

- Mobility Management is the main function of the HLR. It updates the subscriber's position in the administrative area called as the 'location area'. The location area is obtained from the BSS as BSIC (cell identifier);
- Updating VLR by sending the subscriber data to a VLR (or SGSN in the GPRS network) when a subscriber first roams there;

- Interface between the GMSC or SMSC and the current VLR to allow incoming calls or text messages to be delivered;
- Removing the subscriber's data from the VLR from which the subscriber has just roamed.

The VLR is a temporary database, which stores information about all mobiles roamed to an area served by a particular Mobile Switching Centre (MSC). The most important information saved about the Mobile Station (MS) in the VLR is its current Location Area Identity (LAI). The LAI identifies which Base Station Controller (BSC) serves the MS. This information is vital in the call setup process. Whenever an MSC detects a new MS in its network, in addition to creating a new record in the VLR, it updates the HLR about the new location of that MS. Each Base Station in the network is served by exactly one VLR; hence a subscriber cannot be present in more than one VLR at a time. The data saved about each MS in the VLR are as follows:

- IMSI (subscriber's identity number);
- Authentication data;
- MSISDN (subscriber's phone number);
- GSM services that the subscriber is allowed to access;
- Access Point (GPRS);
- HLR address of the subscriber.

The Authentication Centre (AUC) is an intelligent database operating in the network to ensure that only authenticated users can access to the network (i.e. HLR) and GSM services. The AUC is usually co-located with the HLR.

The AUC is not directly involved in the authentication process. However, it generates and stores the security data known as 'Triplets' associated with each mobile phone (or SIM card). The Subscriber Authentication key (K_i) and Algorithm_ID are the most important data saved in the AUC. The K_i is a 128-bit

shared secret key between AUC and SIM. It is burned securely into the SIM during the manufacture and replicated on the AUC (via the HLR). It is used for the authentication of the subscriber by the operator. It is never transmitted into the air, but it is combined with the IMSI to create a challenge/response for identification purposes and an encryption key called K_c for all the wireless communications. The standard GSM security algorithms are A3, A5 and A8 and the proprietary ones which are discussed later.

The main security element in the GSM is the Subscriber Identity Module (SIM), which is technically a detachable smartcard containing the subscription and personal information (i.e. phone book) of a user. Some operators lock the mobile phones due to the fact that they subsidise the price of their own mobile phones. The lock is applied on the International Mobile Equipment Identity (IMEI) number, not to the account, which is identified by SIM card.

The SIM card retains not only the subscriber's personal information but also it has some critical data that are used by the network to identify the subscriber and SIM. The IMSI is stored in the SIM to uniquely identify the subscriber in the GSM network. The SIM itself is identified by its International Circuit Card ID number (ICCID). The equivalent to SIM in UMTS (3G) is USIM. The SIM is mandatory in the GSM network while the Removable User Identity Module (RUIM) is optional in the Carrier Division Multiple Access (CDMA) world.

The IMEI is a unique number allocated to each GSM mobile phone. The IMEI is 15 or 17 digits presenting the origin, model and serial number of the mobile phone. It is used to identify the valid devices and subsequently to stop stolen or lost ones connecting to the network. The number is linked to the device not to the subscriber. It is always printed on the phone underneath the battery. However, it is possible to link the subscriber and his device together offline.

The IMSI is a unique number associated with all the GSM and UMTS subscribers. It is stored in the SIM and sent to the HLR or VLR to acquire other details of the mobile phone. For the security reasons, the IMSI is occasionally sent over-the-air. Instead, a randomly generated number, which is called Temporary Mobile Subscriber Identity number (TMSI), represents the subscriber in the network. The IMSI is usually fifteen-digit long although in some regions a shorter IMSI is used (e.g. 14 digits in MTN South Africa). The first three digits are the mobile country code and the next two (in Europe) or three (North America) digits are the mobile network code (MNC). The remaining digits, up to maximum length, are the unique subscriber number (MSIN) within the network's customer base.

3.2.2 Short Message Service (SMS)

The Short Message Services (SMS) is available on the most of digital mobile phones, which can send text messages to mobile phones or hand-held devices or even land-line telephones. There are three types of SMS available in the GSM network [45]:

- Short message Mobile Terminated / Point-to-Point (SMS-PP) [46];
- Short message Mobile Originated / Point-to-Point (SMS-PP) [46];
- Short message Cell Broadcast (SMS-CB) [47].

The messages are sent to the Short Message Service Centre (SMSC) which operates based on either store-and-forward or forward-and-forget mechanism. The message delivery is best-effort. It means that there is no guarantee for message delivery neither for delay or loss. The protocols which are mainly used for text message transmission between SMSC and phones are SS7 and TCP/IP within the standard GSM MAP framework. The payload of the message is 140 bytes for 8-bit or 160 bytes for 7-bit or 70 for 16-bit characters. A long SMS or

concatenated SMS can be sent segmented over multiple messages. In this case, each message has a User Data Header (UDH), which is used at the receiver to assemble the segmented messages and present them as a one message. Having segmented the long messages and inserted UDH on the payload, the number of characters per segment is restricted to 153 for 7-bit, 134 for 8-bit and 67 for 16-bit encoding. Theoretically the number of segmentations can be up to 255 segments, although in practice it is restricted to 6 or 8 segment messages.

3.2.3 Wireless Application Protocol (WAP)

The Wireless Application Protocol (WAP) is an open international standard for applications using the wireless communication to access the internet. The WAP browser used in mobile phones has the application similar to the computer web browser but with limited features. The WAP is the main protocol to access to the mobile internet sites which are the web sites written in Wireless Markup Language (WML). It is used by the operators to provide different interactive data applications like E-mail. The WAP browser can be installed on the PC to enable the user to experience mobile sites and services like SMS and MMS from the PC. In order to keep WAP interoperable with the other network technologies (GSM and CDMA), the WAP Forum proposed WAP protocol suite detailed as follows.

Wireless Application Environment (WAE)
Wireless Session Protocol (WSP)
Wireless Transaction Protocol (WTP)
Wireless Transport Layer Security (WTLS)
Wireless Datagram Protocol (WDP)
*** Any Wireless Data Network ***

- *Wireless Session Protocol (WSP)*: It is a compressed version of the HTTP.
- *Wireless Transaction Protocol (WTP)*: It provides a reliable request/response transaction mechanism in the wireless communication. WTP is more effective than TCP on handling the packet loss issue, which is common in 2G wireless technologies.
- *Wireless Transport Layer Security (WTLS):* It is an optional security feature which performs a public-key cryptography-based security mechanism.
- *Wireless Datagram Protocol (WDP):* This is an adaptation layer used to make every data network look like UDP to the upper layers. It provides an unreliable transportation using two 16-bit port numbers including the origin and destination. It behaves exactly like UDP on top of the IP bearers such as GPRS and UMTS.

This protocol suite allows a terminal to send requests that have an HTTP or HTTPS (HTTP over encrypted secure socket layer or transport layer security) equivalent to a WAP gateway. The WAP gateway translates requests into the plain HTTP to be used by any HTTP server.

3.3 Bluetooth Technology

The Bluetooth is an industrial specification for Personal Area Networks (PAN) ratified under IEEE 802.15.1 standard. It is used for exchanging information between devices like mobile phones, computers, etc. via a secure, globally unlicensed short-range radio frequency (2.4 GHz). The basic design of the Bluetooth was for low power consumption with short range of coverage and low-cost transceiver microchips. The coverage range varies upon the transmitter power from 1 meter to 100 meters. The devices do not need to be in line of sight, so they even work in an office with multiple rooms as long as the received

transmission is powerful enough. Table 1 presents three classes of the Bluetooth devices differentiated from the radiation power and coverage area.

Table 1: The Bluetooth device classes

Class	*Maximum Permitted Power (mW)*	*Maximum Permitted Power (dBm)*	**Approximate Range (m)**
1	100	20	100
2	2.5	4	10
3	1	0	1

One of the Bluetooth applications is to transfer files and contact details, calendar appointments, etc. via the Object Exchange (OBEX) communication protocol. The Bluetooth specific architecture includes Bluetooth specific protocols and other adopted protocols like Wireless Application Protocol (WAP), Wireless Application Environment (WAE), etc. It also supports cable replacement protocols and telephony adapter protocols such as AT-commands. Fig. 8 shows the Bluetooth Protocol Stack.

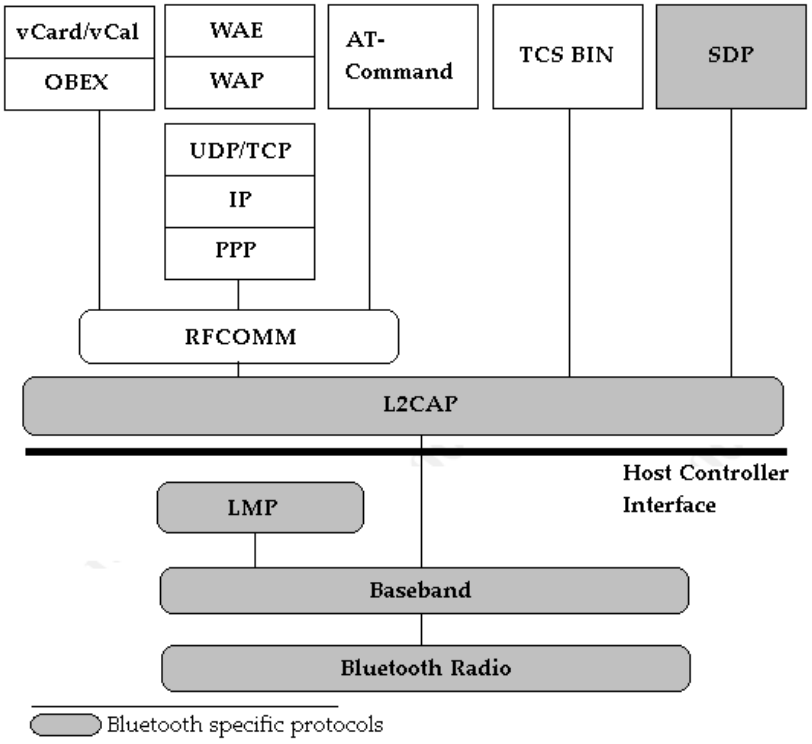


Fig. 8: The Bluetooth Protocol Stack

The Baseband provides physical RF connection between Bluetooth-enabled devices. The Logical Link Control Adaptation Protocol (L2CAP) adapts and controls the upper layer protocol over the Baseband. The Link Manager Protocol (LMP) works in parallel with L2CAP to set up the link between the two Bluetooth devices. It includes deciding and controlling the Baseband packet size, security services such as authentication and encryption using link and encryption keys. The Host Controller Interface (HCI) provides a command interface to Baseband controller, Link Manager and other hardware controllers. The Service Discovery Protocol (SDP) provides the Bluetooth-enabled devices with the information about device types, services and service specifications, so that a connection between devices can be set up. The RFCOMM is a cable replacement protocol. The AT-Command is a telephony control protocol to enable modems run over the Bluetooth. All the adopted protocols form the application oriented protocols that run over the Bluetooth specific protocols.

The first release of the Bluetooth was in 1994 as IEEE 802.15.1 which then followed by Bluetooth versions 1.0, 1.0 B, 1.1, 1.2 and 2.0. The early stage problem was interoperability between these standards, although this problem eased up with upgrading and revising the standards. In the Bluetooth 2.0, the data rate is 3 times more than previous versions (maximum 3 Mbps) within 100 meters range. It is fully compatible with 1.x. In addition, it consumes less power due to a reduced duty cycle and offers better Bit Error Rate (BER). The Adaptive Frequency Hopping Spread Spectrum (AFH) technique used in the earlier versions switches the channel into a less crowded one to reduce the electromagnetic interference. It supports neither IP nor the wireless applications since it is best suited for connecting PDAs, mobile phones and PCs in short distance. The next version of the Bluetooth technology is known as Lisbon in which the security and usability of the Bluetooth have increased. The new

features including the Atomic Encryption Change and Extended Inquiry Response add security to the Bluetooth link by, respectively, periodically changing the encryption keys and filtering devices before establishing any connection. The Simple Pairing is another option introduced in Lisbon to simplify and improve the pairing experience of the Bluetooth devices and also increase the use and strength of the security. Another upgraded version of the Bluetooth is known as Seattle, which is a code name for the merging of Bluetooth with WiMedia Ultra-wideband (UWB) radio technology. It improves the data rate while using very low power. More information can be found in the WiMedia website (www.wimedia.org).

The Bluetooth device (master) can communicate simultaneously with 7 Bluetooth devices (slave) in a master-slave mode. This ad hoc computer network of up to 8 devices is called Piconet. The number of computers in Bluetooth network is restricted by the length of the MAC address (3 bits). The piconets (2 or more) can connect together via a Bluetooth device as a bridge between two networks and form a Scatternet.

The following information is exchanged on demand at a time when a Bluetooth device tries to establish a connection with another: device name, device class, list of services and technical information (i.e. device features, manufacturer, Bluetooth specification, clock offset, etc.)

3.4 Summary

The GSM is the most popular standard for mobile phone in the world enabling the Wireless Wide Area Network (WWAN). According to the last statistics in 2008, it connects over 2.5bn people across the world. The main driving key in the GSM technology is the roaming feature, which enables users to ubiquitously retain their contact with the network. Additionally, it enables them to change

their service providers by just changing their SIM card and enables service providers to operate in an open market wherein many vendors are manufacturing mobile phones.

From the user point of view, the most known GSM element is the Subscriber Identity Module (SIM) card, which presents the subscriber to the network. The SIM can be considered as a secure platform which interacts with the network through mobile equipment using a limited range of APIs. It holds the subscriber's data and operator's data, which are mainly used for security purposes (i.e. authentication, encryption). The subscribers' data in the GSM network are stored in the distributed databases namely Home Location Register (HLR) and Authentication Centre (AUC) which are the first databases that any subscriber implicitly contacts prior to use the network. Another database is the Visiting Location Register (VLR), which serves each Base Station in the network, and so any subscriber, who is present on that service coverage area. It retains the data related to each subscriber including IMSI, MSISDN, authentication data, GSM services and the subscriber's address in the HLR. The IMSI number is unique in the network and mainly used to identify the subscriber. As its secrecy is important for the mobile operator, it is occasionally transmitted in the clear; instead, a temporary number, which is called TMSI, is used to present the subscriber in the network. The IMSI number is usually transmitted at the first time when a subscriber connects to the network. Then, the TMSI number is delivered to the SIM from the network to be used so long as the subscriber remains in that particular VLR zone. In addition to the private subscriber's numbers, which are solely used by the network operator, the subscriber has a public number, which is called MSISDN and that is the known subscriber's mobile number. The subscriber uses his mobile number to communicate with outside world through voice, SMS, MMS or E-mail communication services.

Amongst the GSM communication services, the SMS or text message is the most popular bi-directional communication service in the world. It is significantly cheaper than other GSM communication services especially voice and multimedia services. The GSM subscribers can also enjoy connecting to the mobile internet sites via the WAP browser, which has more limited features in comparison to normal PC browsers but it is secured and standardised. In practice, the subscriber sends an HTTP request to a WAP gateway and the gateway translates it into a conventional HTTP format understandable for any Web (HTTP) servers in the Internet.

Another popular wireless technology is the Bluetooth, which has largely replaced the cable application for short-range connection. It is now integrated in almost any portable device like mobile phone and laptop. The Bluetooth is considered as a technology enabler for Wireless Personal Area Network (WPAN) standardised under IEEE 802.15.

The Bluetooth-enabled devices usually support various services namely Service Discovery Protocol (SDP), RFCOMM which is a cable replacement protocol, file transfer and telephony adapter commands (AT commands). There are various Bluetooth versions in the market but the most popular one is the Bluetooth 2.0, which covers up to 100 meters with data rate of 3 Mbps. However, it does not support IP protocols as it is for connecting PDAs and mobile phones in short distance. Nevertheless, the next generations of Bluetooth can offer higher bit rate and more range of services.

Having considered the overall structure of the two most popular wireless technologies, the GSM and Bluetooth, the next section presents the security features in these technologies. Additionally, some well-known security primitives are also explained.

4 SECURITY REVIEW

4.1 Introduction

The security in information systems ensures the data integrity, confidentiality, users' authenticity and service availability. There are various ways to protect the security criteria in a system. Employing security primitives at each stage of the data communication, processing and storage ensures that the pirate attack will not take place easily. It has been proved that wireless communications are more prone to piracy than wired communication systems. Therefore, sophisticated authentication and encryption methods have been adopted in the wireless systems to guarantee such level of security that can be provided in the cable.

The security is relevant and it is mostly ensured by employing techniques and intelligently analyse transitions states in the system. Nevertheless, no system in the world is totally secure, which enlightens the fact that the security considerations have a life time which then need to be revised.

In this chapter, the security architecture in the GSM network is discussed followed by security mechanism adopted in the Bluetooth technology. Finally, some security methods, which are mainly used in the Pay-TV Conditional Access systems, are explained briefly.

4.2 GSM Security

The analogue based mobile phone systems were considerably vulnerable to fraudulent activities such as interception of telephone conversations, telephone cloning and monitoring the subscriber's location even if the call is not in progress. These issues are well addressed in the GSM network thanks to the

digital techniques used in speech coding, modulation plus the slow frequency hopping and the Time Division Multiplex Amplitude (TDMA) technique.

The GSM is one of the most secured telephone communication systems, which ensures the anonymity of the subscriber through the use of the temporary identification number, and confidentiality of the telephone conversation via encryption algorithms and frequency hopping.

In the cryptography, the symmetric algorithm takes the risk of key management since the same key is used for ciphering and deciphering. However, the public key algorithm, which is knows as asymmetric key cryptography, is characterised by two keys: public and private keys. The private key has the less relationship with the public key to not be deduced easily from the openly distributed public key. The data is encrypted using the recipient's public key and can only be decrypted by the corresponding private key. Thus, the security of this scheme depends on the security of the private key.

The one way hash functions are usually used for accessing data or for security reasons. The hash function outputs a fixed-length hash value from the input string of text. They are designed in a way that it is computationally unfeasible to determine the hash value or two inputs that share the same hash value. The famous example of the one-way hash functions are MD5 with 128-bit hash value and Secure Hash Algorithm (SHA) with 160-bit output.

A key-dependent one-way hash function verifies and computes the hash value with the key appended to the message. It is practical for authentication purposes, where a sender and receiver use a key-dependent hash function in a challenge/response mechanism. This method is used in the GSM authentication (A3) and ciphering key generating (A8) algorithms, which are simply implemented as a single algorithm called COMP128.

The highlights in the GSM security are subscriber identity authentication and confidentiality, signalling data confidentiality and user data confidentiality. The security mechanism of GSM is deployed in the three different system elements:

- Subscriber Identity Module (SIM): it holds the IMSI, K_i, ciphering key generating algorithm (A8), authentication algorithm (A3) and Personal Information Number (PIN) information;
- GSM handset or Mobile Station (MS): it contains the ciphering algorithm (A5);
- GSM network: it equips with the A3, ciphering algorithm (A5) and A8.

The IMSI, which uniquely identifies the subscriber, along with the individual subscriber authentication key (K_i), forms the sensitive identification credentials. The sensitive information is never (or rarely) transmitted over the radio channel; instead, a challenge/response mechanism performs the authentication process. The MS identifies itself by Temporary Mobile Subscriber Identification (TMSI), which is a temporary identifier produced periodically by the network. For further security, a random and temporary ciphering key (K_c) is used for encrypting the actual conversations.

In the GSM network, security information is distributed among the Authentication Centre (AUC), Home Location Register (HLR) and Visitor Location Register (VLR). The AUC, as part of the Operation and Maintenance Subsystem, is a database which contains the identification and authentication information corresponding to each subscriber. This information is IMSI, TMSI and LAI and K_i. The AUC also generates a set of triples (RAND, SRES and K_c) for authentication and privacy purposes for a particular IMSI which has requested to connect to the network. The IMSI request is first received by the MSC and then it forwards it to the AUC.

The K_i is a 128-bit individual subscriber authentication key which is used as a shared secret key between MS, and AUC. It is securely burned into the SIM during manufacture and is also securely replicated onto the AUC. It is never transmitted over the air but it is combined with IMSI to produce a challenge/response for identification process and the encryption key K_c. The RAND is a 128-bit random challenge generated by HLR. The SRES is a 32-bit signed response generated by the MS and Mobile Switching Centre (MSC). The K_c is a 64-bit ciphering key used as a session key for encryption of the over-the-air channel.

Fig. 9 shows the distribution of security information across different GSM elements.

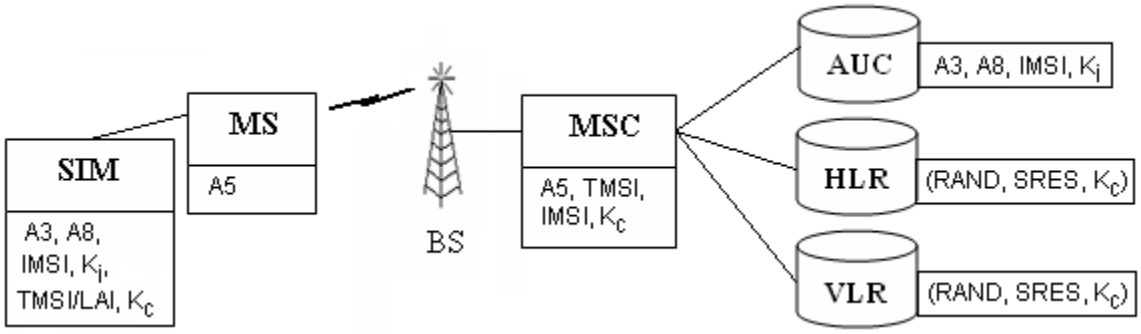


Fig. 9: The security elements in the GSM network

The A3 and A8 algorithms produce the SRES and K_c from K_i and RAND, respectively. The SRES is vital in the GSM authentication process. In order for MS to generate the SRES, the network sends the RAND to the MS to be encrypted with K_i and authentication algorithm (A3). The SRES is sent back to the network for verification. The subscriber is granted to join to the GSM network, if the SRES generated by MS and network are matched.

The MSC forwards the K_c to the BS upon success authentication. Therefore, the confidentiality in signalling and data can be achieved via encrypting data/voice exchanged between MS and BS. The K_c is calculated by feeding the ciphering key

generating algorithm (A8) with the RAND, which is presented by the network and subscriber authentication key (K_i) from the SIM. The ciphering algorithm (A5) then uses the K_c to encrypt/decrypt the data/voice communications. The encryption/decryption of data is started in the MS upon receiving the ciphering mode request command from the network.

The subscriber identity is protected in the GSM network via TMSI, which is used instead of IMSI. The TMSI is assigned to the MS when the IMSI is transmitted to the AUC upon switching on the phone for the first time. When the phone is switched off the TMSI is stored on the SIM card to be read next time. The VLR performs assignment, administration and update of TMSI. The TMSI is valid only on the network area in which it is issued and it is changed every time the location is updated.

Fig. 10 (see next page) presents the data exchange and control scheme used in the GSM authentication and encryption scheme. The security mechanisms specified in the GSM standard make it one of the most secure telecommunication systems available. The use of authentication, encryption and temporary identification numbers ensures the privacy of the users as well as safeguarding the system against fraudulent use.

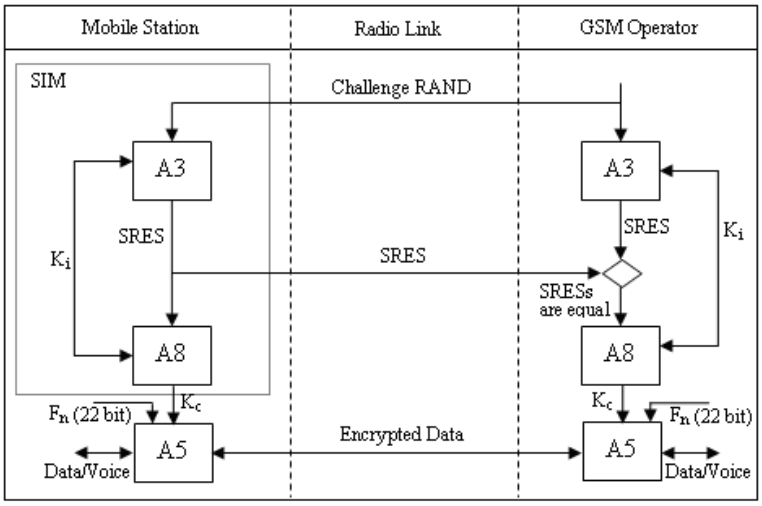


Fig. 10: The GSM authentication and encryption scheme

Both A3 and A8 algorithms are implemented on the SIM and operator can decide which of them becomes effective. The algorithm implementation is independent of hardware manufacturers and network operators. The COMP128, which is a keyed hash function, is the logical implementation of both A3 and A8 in most GSM networks. The A5 is a stream cipher and it is implemented efficiently on hardware although its design has never made public. There are three variations of A5 algorithm: A5/1, A5/2 and A5/3 where the first one is the strongest one. According to the compromise in 1993, A5/1 is allowed to be used in Western European nations and a few other specialised markets such as Hong Kong. The weaker version (A5/2) is allowed for export to most other countries like central and eastern European nations. Under the agreement, designated countries like Russia would not be allowed to receive any functional encryption technology in their GSM systems.

4.3 Bluetooth Security

This section provides an overview of the generic security levels and features that have been incorporated in the Bluetooth specifications. The Bluetooth-enabled devices can communicate with each other over a short range wireless link with range of about 10 meters to 100 meters. The wireless link is established on the heavily used unlicensed 2.45 GHz radio band while employing frequency hopping of 1600 times per second. This technique necessitates synchronisation between devices to be connected via Bluetooth and reduces the risk of eavesdropping while exchanging data. Every Bluetooth device has a 48-bit address allowing users to have some trust in the person at the other end of the transmission. When the requests are placed for connection establishment, the name of the Bluetooth device appears. The name is set to the manufacturer and model for the phone by default.

The Bluetooth-enabled devices can operate in one of three different security modes numerated as follows.

- *Security Mode 1*: a Non-secure mode where the device will not initiate any security procedures;
- *Security Mode 2*: it is the service-level security mode where the security procedures are initiated after channel establishment at the Logical Link Control and Adaptation Protocol (L2CAP) level. The L2CAP resides at the data link layer and can establish either connection-oriented or connection-less data services to upper layers. It is flexible and policy-based and provides encryption, authentication and authorisation;
- *Security Mode 3*: In this mode authentication and encryption security features are enforced at the Baseband level before setting up the connection. This is a built-in security mechanism that is independent of any application layer security. This mode is fixed and it provides authentication and encryption based on a secret key that is shared by paired devices.

The link key is generated during an initialisation phase, while two Bluetooth devices that are communicating are bound. The key is derived when a user enters an identical personal identifier (PIN) into both devices. After this stage, devices automatically and transparently authenticate and perform encryption of the link. The PIN code that is used in Bluetooth devices can vary between 1 and 16 bytes. The typical 4 digit PIN may be sufficient for some applications; however longer codes may be necessary [66].

In Bluetooth, the security levels can be applied on both devices and services. For devices there are two security levels, where the remote device is either a trusted device or untrusted device. The trusted device would be able to access to the specific services for which the trusted relationship is set up. On the other hand, the untrusted device has a restricted level of access to services.

For services, three levels of security have been defined:

- Authorisation and Authentication: automatic access is only granted for trusted devices. Other devices need a manual authorisation;
- Authentication-Only: authorisation is not necessary;
- None/Open to all: authentication is not needed; no access approval is required before service access is granted.

Associated with these levels are the following security controls to restrict access to the services:

- Authorization: it includes authentication and it is performed automatically for trusted devices;
- Authentication-Only: It enforces the authentication of the remote device before granting access to the device;
- Encryption: It encrypts the link between two devices before accessing the applications.

The Bluetooth authentication procedure is in the form of challenge-response scheme. The challenge-response protocol validates devices by verifying the knowledge of a secret key – a Bluetooth link key. In the authentication procedure the following parameters are used:

- 48bit Device Address (BD_ADDR): a public parameter;
- 128bit Random Challenge (AU_RAND): a public parameter and unpredictable;
- 32bit Authentication response (SRES): public parameter;
- 128bit Link key: secret parameter.

Fig. 11 presents the challenge-response verification scheme taken place in the Bluetooth Authentication process [66].

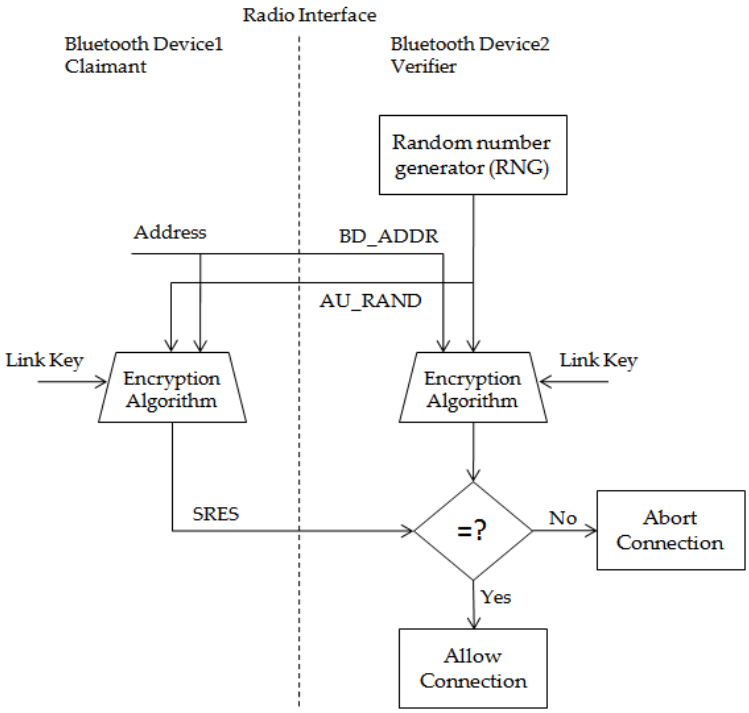


Fig. 11: The block diagram of Bluetooth Authentication process

In the authentication process, the Claimant is the device who is seeking permission to get access to the services available at the Verifier. First of all, the Claimant sends its 48-bit address (BD_ADDR) to the Verifier. The Verifier then sends the 128-bit random challenge (AU_RAND) to the Claimant. Then both sides calculate the authentication response (SRES) using the link key, address and random challenge as inputs. The Claimant sends its SRES to the Verifier. The connection is established only if the SRES calculated at the Claimant matches the SRES calculated at the Verifier.

The Authentication process, which is practiced in the Bluetooth core protocols, is device-based access control not user-based. However, the Bluetooth security architecture allows applications to enforce their own security policies. It means that it is possible to perform user-based authentication and fine grained access control within the Bluetooth security framework.

In a Bluetooth device, the security features and policies are enabled by the Security Manager. It may enforce the application level authentication, encryption of the session and many other specific access policies based on the device type (i.e. trusted, untrusted) and services. To grant any permission, the Security Manager needs to gather some information from two databases: Device and Service Databases. The Device Database stores information about the device type, trust level and length of the link key, which is used for encryption. The Service Database stores data about the authentication, authorisation and encryption requirements for the services. The typical process followed by the Security Manager in granting access to a remote device to connect to a particular service is as follows:

- First a remote device initiates an access request;
- The request comes to the L2CAP and passed to the Security Manager;
- Security Manager queries device and service databases;
- If the device is trusted, depending on the implementation, the Security Manager may or may not perform authorisation;
- If the device is untrusted, depending on the implementation, the Security Manager may terminate the connection or enforce authorisation (i.e. username/password application level security scheme);
- Security Manager decides if the link encryption is required. If so, keys will be exchanged at the L2CAP protocol level and the connection is then set up;
- Alternatively, if the device is in security mode 3, the Security Manager instructs the LMP to authenticate and encrypt the link prior to transmission.

The Security Manager acts as an interface between application level and core Bluetooth protocol level (link layer) security controls and thus provides an end-to-end security across the layers.

4.4 Security Primitives

The key exchange protocols and data stream encryption are based on a set of well-established security functions and cryptographic methods. The functions and their associated key sizes can be exchanged as the threat of brute-force attacks become realistic. The functions and the size of keys are negotiated between a service provider and an end-user at sign-on time. The common protocols supported at present are Diffie-Hellman, HMAC-SHA1 and DES. The following clauses give a brief overview of the cryptographic primitives.

4.4.1 Pseudo-Random Numbers

The protocols used for generating secret values are always dependent of the availability of Pseudo-Random Number Generator (PRNG) algorithm. It generates practically unpredictable, endless string of bytes. The unpredictable nature of the random input ensures that different secret values are produced each time, and also prevents replay of old intercepted messages. Indeed, initialising the PRNG with an unpredictable value is the hardest aspect of using the algorithm. The starting value should contain multiple high-granularity device-dependent time-samples as well as any other available pseudorandom material, like file allocation tables, etc. These random source values are then hashed together to squeeze out the entropy for the starting value [90].

Note that truly random sequences may nevertheless be predictable and so entirely useless for cryptographic purposes. There are many examples in cryptographic history of ciphers, otherwise excellent, in which random choices were not random enough and security was lost as a direct consequence.

Users and designers of cryptography are strongly cautioned to treat their randomness needs with the utmost care. Absolutely nothing has changed with the era of computerized cryptography, except that patterns in pseudorandom

data are easier to discover than ever before. Randomness is, if anything, more important than ever.

4.4.2 Public key Cryptography

The public key cryptography (exchange) allows a service provider to communicate securely with end-users without having prior access to a shared secret key. They simply agree on a secret key and communicate in public. This is done using a pair of cryptographic keys called public and private keys which are mathematically related to each other. The Public key (used as a lock) may be widely distributed but the Private Key must be kept secret to unlock a lock. The Private Key should not be deduced from its Public key.

The Asymmetric key Cryptography is somehow a synonym to the Public key cryptography but both keys must be kept secret, since both are private keys.

There are many forms of public key cryptography, including:

- Public key encryption: ensures the confidentiality by encrypting a message using a recipient's public key. The message can only be decrypted by who possess the corresponding private key;
- Public key digital signature: ensures authenticity by signing a message using a sender's private key. The message can only be verified by who possess the sender's public key;
- Key agreement: generally, allows two parties that may not initially share a secret key to agree on one.

Typically, public key techniques are much more computationally intensive than purely symmetric algorithms, but the judicious use of these techniques enables a wide variety of applications.

4.4.3 Diffie-Hellman

The Diffie-Hellman (D-H) key exchange is also known as: Diffie-Hellman key agreement, Diffie-Hellman key establishment, Diffie-Hellman key negotiation or exponential key exchange. The D-H key exchange is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure (but authenticated) communication channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

Although D-H key agreement itself is an anonymous (non-authenticated) key agreement protocol, it provides the basis for a variety of authentication protocols. It is used to provide a perfect forward secrecy in Transport Layer Security's (TLS) ephemeral modes [92].

In D-H, both parties must select firstly a private key for themselves (i.e. a service provider selects 'a' and so does an end-user 'b'). The service provider then selects a prime number (P) and a small number (G) which is a generator modulo P (G is a primitive mod P).

Fig. 12 describes how D-H protocol provides exchanging key between two parties – a service provider and an end-user.

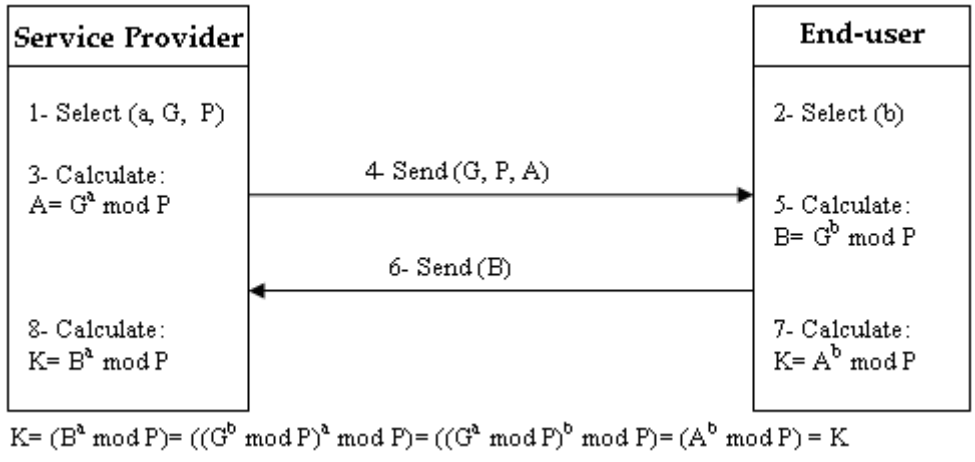


Fig. 12: The Diffie-Hellman key Agreement procedure

4.4.4 Encryption

In the Pay-TV conditional access system, the cryptographic keys are encrypted in the conditional access messages prior to the transmission. The actual encryption method uses proprietary algorithms, which are always shared in both analogue and digital TV signals. The encryption process determines the level of the security in a system. The encryption methods are typically based on the Data Encryption Standard (DES) functions. In generic terms, the encryption and decryption functions take two byte strings: the key and a data block. It then outputs another data block of the same length:

$$CipherText = E(Key, PlainText)$$
$$D(Key, CipherText) = PlainText$$

The key length and block length is specified by the cipher, and the payload stream processing logic will apply it as appropriate to data units of various sizes.

The specification currently supports the DES algorithm, which has a block size of 8 bytes, and various options for key length based on an 8-byte raw key block.

The DES is now considered to be insecure for many applications. This is mainly due to the size of the key (56-bit) which is too small - DES keys have been broken in less than 24 hours. There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES [14], although there are theoretical attacks such as chosen plaintext or known plain text attacks which are not practical till 2030. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES).

4.4.5 Hashing – Digital Signature

A Hash function (or hash algorithm) is a way of creating a small digital 'fingerprint' or 'Hash value' from any kind of data by a function called Hash

function. The hash value is commonly represented as a short string of random-looking letters and numbers.

One of the applications of the Hash function is in cryptography. In cryptography, a cryptographic hash function is a hash function with certain additional security properties to make it suitable for use as a primitive in various information security applications such as authentication and message integrity. A hash function takes a long string (or message) of any length as an input and outputs a fixed length string known as the message digest or digital fingerprint.

Generally, the keyed hash function takes two byte strings as input, the key and Data string to produce another string of bytes.

$$Digest = Hash(Key, Data)$$

The Hash function is designed to accept key and Data of any size whereas the protocol is designed to accept Digest of any size.

In various standards and applications, the two most-commonly used cryptographic hash functions are MD5, SHA1. The Hash Message Authenticating Code (HMAC) is a keyed hashing for message authentication which uses the said hash functions for message authentication [91].

4.5 Summary

The security in information system ensures the integrity, confidentiality, authenticity and service availability. In the GSM system, following elements are responsible to store and save security credentials and algorithms to handle such criteria: the subscriber's SIM card, subscriber's handset (mobile station) and network elements such as HLR, VLR and AUC. The credentials in the system can be categorised into user identification credentials, user authentication and confidentiality and network credentials. The identification credentials are IMSI

(or TMSI) and K_i which are stored securely in the SIM card. The former is used for identification and latter is used for authentication purposes.

The authentication in the GSM is a one way scheme where only the network authenticates the user. When a user tries to connect to the network through its IMSI number, the MSC requests the AUC to generate a triplet (RAND, SRES, K_c) and then forwards the RAND to the MS to calculate the SRES using the authentication algorithm (A3) and K_i. The authenticated user then can use the K_c and an encryption algorithm (A5) to ensure its privacy during the communication (i.e. voice, SMS) with the GSM network.

The security level in the GSM is attributed as moderate supporting one-way authentication, confidentiality, but limited authorisation and no non-repudiation schemes. It is secure enough for everyday use but it is not crack proof. For this reason, the next generations of the GSM have evolved to offer greater security by a set of new security methods supporting mutual authentication of the network and end-user.

Another popular wireless technology is the Bluetooth. It covers between 10 and 100 meters and enjoys high frequency hopping which together make eavesdropping rather difficult. The Bluetooth-enabled device can be recognised by its name, type and 48-bit address. It has a Security Manager, which is responsible for applying device and service level security measures based on the security information registered in the Service and Device databases. The default security includes authentication and encryption at the Baseband level using a shared-secret key, which is independent of any application level security. In addition, each service can enforce its own security measurement at the L2CAP level. It may include both authorisation and authentication or only authentication or none. The measurements may vary depending on the category

of a device, which can be either trusted or untrusted. The trusted device can only access to certain services, if it passes authorisation and authentication processes.

In both GSM and Bluetooth communications, the higher level of security can be achieved utilising security primitives at the application level. There are various security primitives that allow parties to establish reasonably secured communication links. In an unsecured environment such as wireless links, the key exchange algorithm (D-H) is usually used to establish a key agreement between parties. The cipher algorithms are used to transform messages before transmission. The digital signature can ensure authenticity and integrity of the messages. The digital signature can also provide non-repudiation.

Having considered the technologies which can be used in the DTV and Interactive-TV systems, the next chapter provides an in-depth overview of the typical Pay-TV systems and state-of-the-art CA systems defined for the Pay-TV systems.

5 PAY-TV CONDITIONAL ACCESS SYSTEMS

5.1 Introduction

The security is considered as the main factor to guarantee the revenue in Pay-TV businesses. Various techniques have been utilised for providing more secure and reliable infrastructure for both service providers and viewers. Changes in commercial and technological environments, widespread introduction to the digital TV, ever increasing risk of content piracy and vast improvements in silicon manufacturing capabilities emphasise on the security and protection of digital assets in broadcasting networks. The history of conditional access technology shows that the security techniques have been developed beside other technologies in the broadcasting industry.

The CA is a technique used in Pay-TV systems to protect payable contents from unauthorised viewing. The motivation for conditional access can be concluded to controlling costs, generating revenue and preventing commercial piracy. The technique was firstly used in the Europe and USA and is now spreading across the globe.

In this chapter a typical model of broadcast security architecture is presented and then state-of-the-art security techniques are described.

5.2 Pay-TV Business Models

One of the basic principles behind any Pay-TV system is that television programmes are financed directly by viewers through following business models.

The "Subscriber television" refers to all businesses providing television programming to consumers for a fee. It includes, but is not limited to, cable

television and satellite televisions. The Subscriber television often transmits special channels offering a variety of programming such as movies, sporting events, children's entertainment, news and other informational services to its customers. A potential customer purchases a programme for a given period of time (i.e. a month or a year) to become a legal subscriber. The fee is the subscription fee and it includes the amount paid by the subscriber to receive the television service. Generally, it is payable monthly and it covers installation, maintenance or service charges.

The Pay-Per-Order (PPO) defined in the Pay-TV as a business model in which a consumer pays once-off subscription fee for access to digital content. The popular PPO business models are Pay-Per-View (PPV), Pay-Per-Channel (PPC), Near-Video-On-Demand (NVOD) and Video-on-Demand (VOD). In both PPV and PPC, a piece of digital content (i.e. a sport events or movie) is offered by Pay-TV service provider for a fee based on pre-scheduled time and channel (service). In PPC, the receiving fee for each channel is counted with time unit (i.e. daily, weekly or monthly), while the receiving fee for PPV channel is counted with program unit (i.e. film or live match) [67]. In the NVOD a piece of digital content (i.e. a movie) is broadcast repeatedly on one or more services. Clearly, the maximum amount of time a consumer has to wait for the start of the event depends on the number of services allocated to it. For instance, a 2-hour movie can start every 15 minutes, if eight services are used exclusively for its repeated broadcast. The NVOD model is the content broadcast variant of the VOD model, in which a piece of digital content is unicast to a consumer immediately after his or her corresponding order is received. Therefore, the VOD requires a communication network with a significant amount of bandwidth compared to the content broadcast models [70].

Currently, Pay-TV systems follow a circle of dependency in which a service provider, CA system provider and set-top box producer have to operate together in a vertical market. In this cycle, the set-top box producer needs to bid for a set-top box order form from a Pay-TV service provider and pay a licence fee to use the service provider's CA system in his set-top boxes. He also needs to sign a non-disclosure agreement with the CA system provider. Therefore, the set-top box producer is bound to the CA system provider to deliver CA related functions in his set-top boxes. Consequently, set-top boxes will be exclusively tailored based on the CA system employed by the service provider. The service provider supplies the set-top boxes to his subscribers usually free of charge or at a subsidised price. Such a discount is usually offered in the Subscriber TV model, where a customer subscribes for a service.

The service provider usually schedules installation of customer premises equipment (CPE) and sends his engineer to the customer's premises (physical location). After the customer has become an authorised subscriber, the service provider posts a subscription card (i.e. smart card) to the subscriber. The engineer will ask the subscriber for the subscription card at the time of installing CPE (i.e. antenna, set-top box, cables, etc.) Typically, the subscription card is inserted into the set-top box and undergone a binding process, which allocates the card to the set-top box. The binding process needs to be done by an authorised engineer at the customer's premises and it is authorised by an Authorisation and Transaction Server (ATS). When a set-top box sends a binding request to the ATS through a return path (i.e. telephone line), the ATS connects to the set-top box to retrieve and verify the set-top box and subscription card identities. If the binding process succeeds, the ATS will send an activation code to the user smart card to enable the set-top box to operate under the employed CA system. The smartcard can be only used then on that particular set-top box.

The service provider stores various data associated to his subscribers in a database. The data is inserted upon receiving a subscription request and might include the customers' personal data, bank details, entitlements, subscription request history, associated set-top box identity, smart card identity and cryptographic keys.

Fig. 13 illustrates the relationship of external entities in the Subscriber Television model.

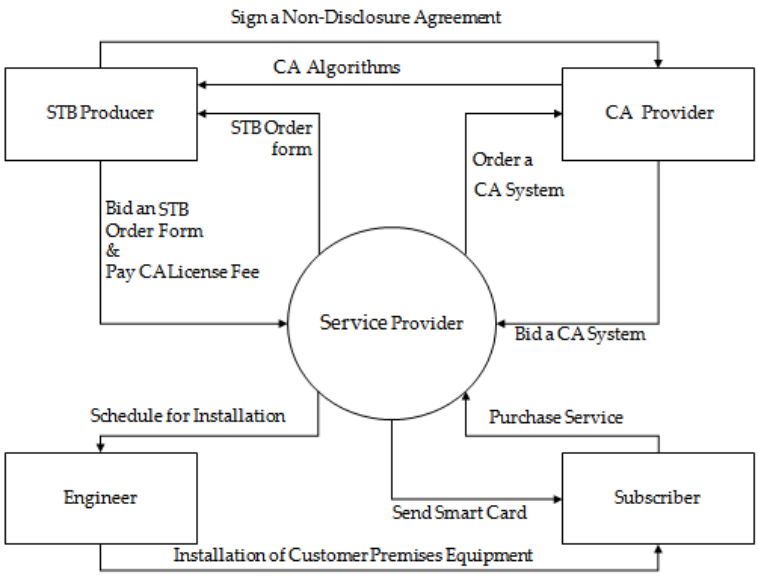


Fig. 13: Business cycle in typical Subscriber Television model

5.3 *General Pay-TV Conditional Access System*

The Pay-TV CA system usually consists of two following subsystems [76]:

- The Scrambling Subsystem: it is responsible for scrambling the signal at the head-end and descrambling it at the subscriber's receiver;
- The Control Access Subsystem: it processes access control messages to determine whether descrambling must be performed. The European Digital Video Broadcasting (DVB) project has defined two conditional access messages namely the Entitlement Control Message (ECM) and Entitlement Management Message (EMM) [78].

The DVB group has ratified a standard method for scrambling digital contents called the DVB Common Scrambling Subsystem (CSS). The details of the algorithm are held confidential to protect the system from making illegal descramblers. The CSS is a DVB standardised symmetric cipher, which is based on cascading of two ciphering procedures including a block cipher using a Reverse Cipher Block Chaining (RCBC) and a stream cipher. First, the data blocks consisting of 8 bytes, each one including 8 bits is scrambled, and then in the second round the resulting data are re-scrambled bit by bit. The 64-bit content encryption key, Control Word (CW), is used to drive the scrambling method. It is generated and updated periodically (i.e. every 5-10 seconds) by CW Generator. The CW Generator supplies the CWs to the content packager and ECM generator [37].

The first step in scrambling is to cipher a block code using a CW. The encoded data stream is then fed into the stream cipher mechanism, which operates with a pseudo-random operator. The output of the pseudo-random bit stream (PRBS) generator is added modulo-2 to the block ciphered data [89].

Fig. 14 presents the block diagram of the DVB common scrambling subsystem.

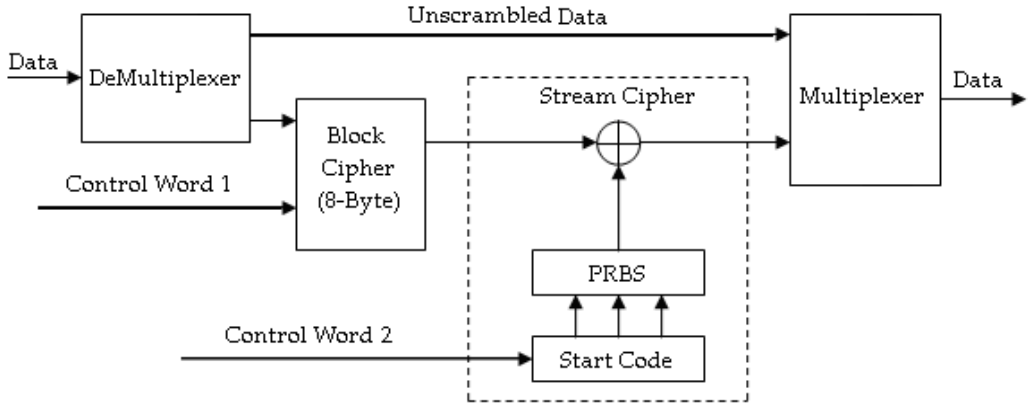


Fig. 14: Scrambling procedures for DVB systems

Considering that the DVB uses MPEG-2 compression method, the ciphering could happen in two following levels (one of them should be applied at a time):

- Packetized Elementary Stream (PES);
- Transport Stream (TS).

The MPEG-2 TS header is not ciphered and it contains special control bits listed in Table 2. The first bit specifies the status of the next block (coded, uncoded) and another shows which cipher used (even or uneven) for the packet. The control bits bear the same meaning on both levels of ciphering. The key, which represents the encryption of two CWs, is changed from time to time. The new key is transmitted within MPEG-2 stream and the second scrambling-control bit shows that everything following the block to which the header belongs is subject to the changed cipher [89].

Table 2: The scrambling control bits used by CA procedure.

Bit Values#	*Meaning in Transport Stream and Packet Elementary Stream, Respectively*
00	No Scrambling
01	(it is not used at the moment)
10	Scrambled with even code word
11	Scrambled with uneven code word

Two CWs are required at the receiver to descramble a programme. At the head-end, ciphering procedures are used to transform them into the ECM. One of the ECMs is used for descrambling the block-wise scrambling and another ECM enables the descrambling of the bit-by-bit scrambling. The descrambler acquires the conditional access table from the Service Information (SI). This table can contain the EMM and ECMs. The EMM is attached to the programme stream to ensure that the subscriber is supplied frequently (i.e. hourly or daily) with the new individually valid EMM.

The ECM Generator packages CW information together with other related service references (i.e. channel identifier, entitlements required for accessing the service, etc.) into a single ECM. The output of the ECM Generator is an ECM, which is a public message and identical to all subscribers within a Pay-TV

operator's population. The ECM Generator injects the ECM around ten times per second into its elementary steams (ES) to enable the subscriber quickly access to content after tuning to a service. In the meantime, the ECM Generator protects the authenticity of the ECM and confidentiality of the CW using cryptographic methods (i.e. AES-128 algorithm together with ECB mode of encryption). The corresponding cryptographic key is passed to the EMM Generator/Injector to be inserted into EMM elementary streams [67].

The ECM is restricted to 256 Bytes and consists of three fields. The first field contains the access parameters. The access parameters define the conditions under which access to a program is allowed. The service provider can use this field to leverage, for example, local control (i.e. using a parental rating system) and geographical black out (i.e. domestic channels). The second field contains an encrypted CW and the last field contains a data integrity check.

The EMM Generator compiles an EMM from authorisation data (i.e. service reference, entitlements, access-time/date schedule and cryptographic keys). The EMM Generator encrypts EMM before transmission using symmetric-key algorithms, which are shared with subscriber's smart card. The main objective of EMM will be to entitle a subscriber or a group of subscribers to access a specific piece of digital content.

The EMMs shall be transmitted in advance in order to give access to the authorised subscribers. In the broadcast-only environment, the transmission of a conditional access message needs to be repeated to make sure that set-top boxes will descramble contents on time and according to the subscriber's entitlement. It is worthwhile noting that set-top boxes are not receiving anything when they are switched off or, in some cases, when they are in the stand-by mode (i.e. for energy-saving reasons). Such requirements are handled by the EMM Injector, which schedules the EMMs to be transferred to the receivers in time before the

start of associated programmes. The EMMs are organized in a carousel model for broadcasting and is managed by a component to insert, move and remove an EMM when it is appropriate (i.e. no need to broadcast an EMM when its associated event is not broadcast). The EMMs are addressed to subscribers using their unique and group smart card addresses. The EMMs can be delivered either via broadcasting medium along with ECMs and digital contents or via interaction channels (i.e. phone line).

The size of EMM is restricted to 256 Bytes and usually consists of four fields. Each EMM starts with an address field associated to a specific set-top box. There are usually two addressing modes; one for an individual set-top box and one for a group of set-top boxes. The second field is the subscriber's entitlements and the third field is encrypted service keys. The last field is for the data integrity check.

There may be different applications for the EMMs. For instance, it can also be used to send a command to set-top boxes. Additionally, it can be used as a 'Unique EMM' to send activation and key update messages to a single subscriber or it can be used as a 'Group EMM' to send a cryptographic key associated to an event (i.e. tennis match) to a group of subscribers, who have paid for the event.

The MPEG Multiplexer multiplexes the output of the content packager (i.e. scrambled video, audio and data elementary streams) and conditional access messages (i.e. ECM, EMM) into a single transport stream. Typically, the MPEG-2 transport stream contains up to 8 services, one EMM elementary stream and small number of ECM elementary streams.

The subscriber is identified using its smart card unique address (typically 4 Bytes) or group address. The size of the group address varies based on the number of subscribers and grouping size. For instance, when a service provider has about one million subscribers, a 3 Byte group address can be used to address groups of 1024 subscribers. The user smart card presents its address to the set-

top box during initialisation. The set-top box uses this address to filter and acquire corresponding EMMs. The EMMs are then delivered to the user smart card. The user smart card decrypts the EMMs and updates its memory based on the information conveyed by the EMMs. This information is used at the user smart card to decrypt the ECMs and retrieve CWs. The user smart card delivers the CWs and initiates the descrambling of contents.

Fig. 15 and Fig. 16 present the processes that usually take place, respectively, at the transmitter and receiver sides in a general Pay-TV system.

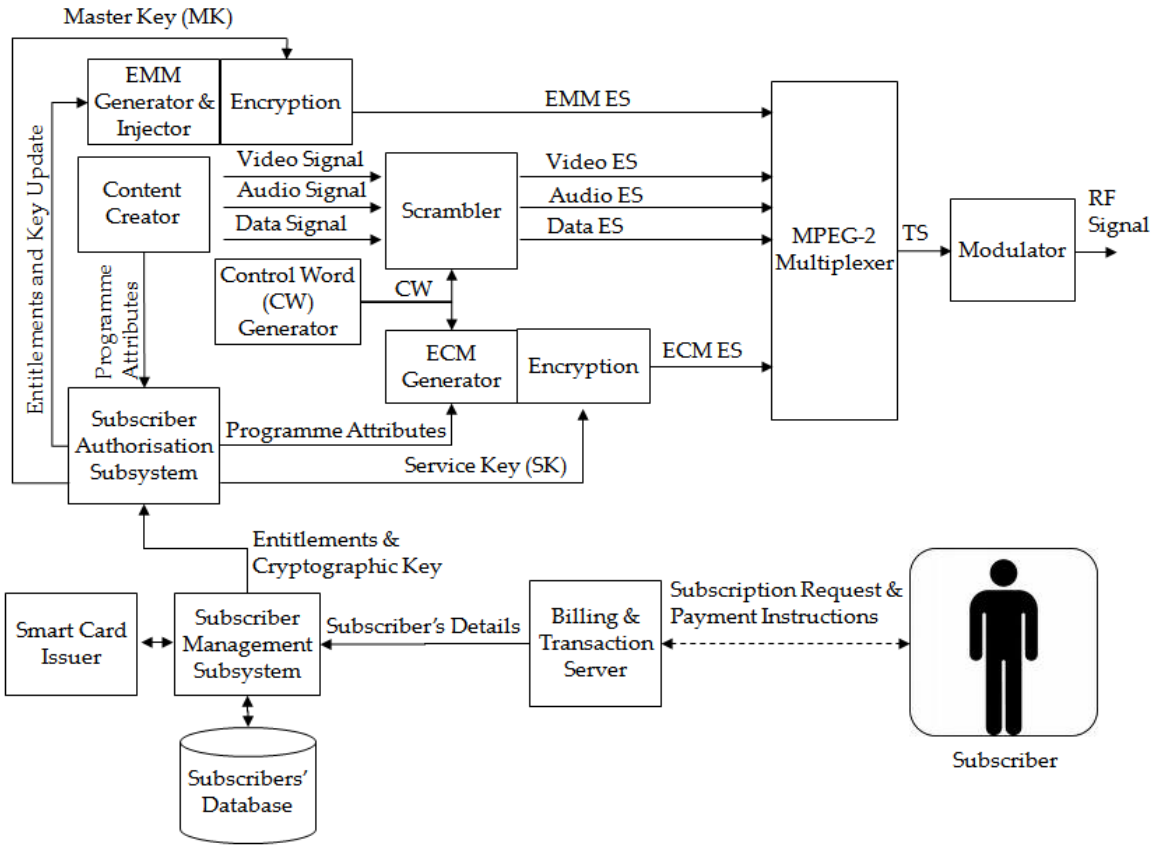


Fig. 15: The head-end structure in a general Pay-TV system

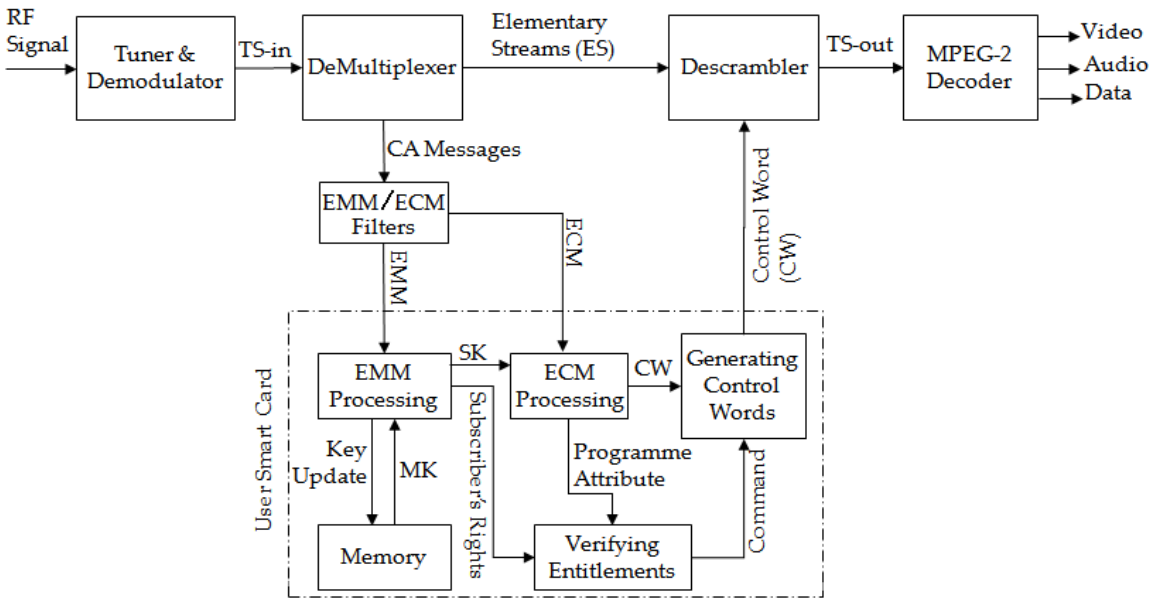


Fig. 16: The receiver-end structure in a general Pay-TV system

5.4 Pay-TV Conditional Access (CA) Solutions

The Conditional Access System (CAS) plays an essential role in the success of any Pay-TV business model. The key requirement for Digital-TV CAS is to enhance the security and effectively support the advanced features of the DTV business concepts (i.e. bandwidth efficiency, interactivity). These aspects have put the CAS at the technical core of the Pay-TV business and attracted a large number of academia and industrial groups to develop solutions to match the evolving commercial requirements. The technical analysis of the requirements resulted in formulating common elements in CA systems [102]. The need of common elements in the CA systems has been chiefly driven by following commercial issues [76].

- Supporting of Pay-TV signals by only a receiver and a single smart card;
- Possibility of changing the CA control data at delivery media boundaries;
- Interoperability and minimising the amount of differences in consumer receivers for the support of different CA systems.

Next sections highlight some important conditional access techniques proposed to Pay-TV systems since adopting the CA technology by European DVB group.

5.4.1 Eurocrypt CA System

The Eurocrypt is a result of research on conditional access system carried out by the CCETT (France Telecom) since 1979. With the emergent of Pay-TV systems in Europe, France Telecom was mandated to define an open conditional access system (Eurocrypt) for all broadband networks in 1989. In 1995, the European Economic Community (EEC) ruled on incorporating the D2-MAC decoder in the TV receivers which had the Eurocrypt CA system to make service available to only legitimate users who had previously subscribed [39]. It was stipulated that the Eurocrypt should fulfil the following requirements:

- Provisioning of high-security;
- Offering greater range of services;
- Capability to encrypt each of services separately;
- Being managed via an open system organisation (i.e. be as standard as possible).

In the system proposed by the France Telecom, the Eurocrypt system can support following business transactions:

- Subscription: customers purchase a programme for a given period;
- Pay-Per-View: customers purchase the programme when viewed and it can be an advanced purchase or impulse purchase;
- Pay-Per-Time: the fee is based on the length of the session

Additional features like maturity rating for the programme, blackout of geographical areas, replacement of services for blacked out receivers, transmission of personalised messages and local viewer control of the security

device using PIN number are included in the system. Some characteristics of the Eurocrypt system are as follows [69].

- It is a unified CA system and compatible with all broadband networks and broadcasting standards;
- It is a hierarchical system organisation with three levels of decision:
    - Issuing authority that is responsible for the security of the system and issuing the PC2 smartcards. It allocates a service field to the programme provider, who inserts his conditional information to the field;
    - Programme provider that manages its resources and customers with full autonomy. A technical management centre, which is shared by several programme providers, will manage the entitlement functionality with total commercial independency;
    - User that subscribes to a programme and enjoys various services, local control and rapid update of entitlements thanks to the broadcasting network and efficient grouped user addressing system;
- It broadcasts entitlement management messages to entire group or individuals using over-the-air addressing methods;
- It utilises the PC2 smartcard which increases the security and potentially reduces the set-top box cost as it reserves the use of a standardised descrambler in the system. In addition, it supports high change rate of control word (i.e. every 10 seconds) and the entitlement message which can increase the security in the system. The control word is delivered by the entitlement message to be used for content descrambling, if the entitlement matches the programme's parameters. However, the downside of the system has been attributed to the scrambler, which is

based upon a stream cipher technique [118] protected by Jennings' pseudo random generator [61]. Analysis revealed that the generator has great deviations from typical pseudo random generators with regards the important parameters like complexity or correlation. It has also been cryptanalysed during the Linear Consistency Test [18];

- It is user-friendly and ergonomic since most programme parameters are broadcast and stored in clear. The users can navigate through parameters and read entitlements, if the receiver is equipped by a simple firmware;
- It is scalable meaning that the system evolution for adding new functionality and upgrading security mechanism is possible;

5.4.2 DVB Protocols - Simulcrypt & Multicrypt

Following series of discussions held by the DVB project over the conditional access system since 1993, a common scrambling system was agreed to be used in the system. The decision implies the need of a common set-top box that can descramble all scrambled programmes given right ECMs and EMMs. The issue regarding the access of pay programmes using a common receiver however needs further agreements between service providers. One solution could be a consensus amid Pay-TV providers on using a unified conditional access system, which is unrealistic for commercial reasons. The other solutions defined under DVB standardisation system were Simulcrypt [112] and Multicrypt [34] protocols. They were adopted to make decoders more universally usable.

The Simulcrypt allows multiple parallel CA system to share the head-end and scrambler feeding multiple receiver population. This enables the subscribers to use a uniform receiver to receive any entitled services. It also enables service providers operate more conveniently on the same geographical area based on an agreed framework. The Simulcrypt technique is a shared scrambling system. It

encrypts the main service by a common scrambling algorithm with a certain CW, which is used in different conditional access systems. Each system then encrypts the CW by its own proprietary scheme and the resulting data is inserted into the broadcast signal. The SimulCrypt provides a flexible way to offer different products to subscribers by simply changing the conditional access data stream. It is bandwidth inefficient. Even if service providers agree on sharing the overall cost of operating the head-end or uplink (i.e. cost of transponder, support for the head-end, promotions, etc), still commercial and technical issues like implementation of head-end, synchronisation of ECMs and CW and timing of ECMs need to be addressed [99]. Most of CA subsystems implementing the Simulcrypt use an 8-bit smartcard. Although the smartcard based set-top boxes are cheaper, they limit viewers to a specific service provider who supports the Simulcrypt; since the smartcard-based set-top boxes are usually dedicated to one conditional access system. Therefore, the viewer needs to change his set-top box if the new service provider does not support the Simulcrypt. This issue has been addressed in the Multicrypt enabling a set-top box to support multiple CA systems.

The Multicrypt introduces the Common Interface (CI) to be used in set-top boxes. The CI has a slot that supports CA modules from different service providers. Each module has a CA subsystem, which is managed by the set-top box. Thus, all CA related proprietary hardware and software components are concentrated into the security module. This simplifies the set-top box function and makes it more affordable due to its wider applications. The Multicrypt allows multiple service providers to co-exist at the receiver and enable them update their CA subsystem more conveniently. The interfaces which are mainly used in the Multicrypt are as follows [42].

- The PC-card-based interface supporting the PC card standard – Personal Computer Memory Card International Association [85]: DVB Common Interface [34], Digital Audio-Visual Council (DAVIC) CA0 [19] and National Renewable Security Standard (NRSS)-B [81]. All of them are essentially the same. The MPEG-2 TS passes from set-top box to the module and back, as the descrambling is performed by the module;
- The DAVIC CA1 [19] - the smartcard-based interface, which is based on ISO/IEC 7816-x smartcard specification [60]: only CA-messages pass this interface. The MPEG-2 TS remains in the set-top box where the descrambler function is located;

In brief, the Simulcrypt chooses low-cost smartcard-based CA subsystem at the sacrifice of interchange-ability while the Multicrypt with PC-card-based CA subsystem achieves high interchange-ability at the expense of high-cost PC card module.

5.4.3 JavaCard-based CA System

The JavaCard was first demonstrated by Schlumberger, a smartcard manufacture, and then the Sun Microsystems specified the JavaCard (JC) specification in 1996. The specification described JavaCard general goals and architecture to support a Java language subset and APIs for smartcard specific functions (i.e. cryptography). The JavaCard extends the Java technology into the smartcard, which adds more portability comparing to the old assembly based smartcards used in the Simulcrypt. The JavaCard has been accessible to a wide community of Java programmers and it shows great success due to the light weight Java byte-code, which breaks the memory bottleneck in the smartcard. A JavaCard like smartcards has a Central Processing Unit (CPU) and memory unit(s) (i.e. ROM, RAM, EEPROM). The operating system consists of the

JavaCard Virtual Machine (JCVM), which executes Java applications (i.e. Cardlet or Applet). Fig. 17 presents a common JavaCard architecture.

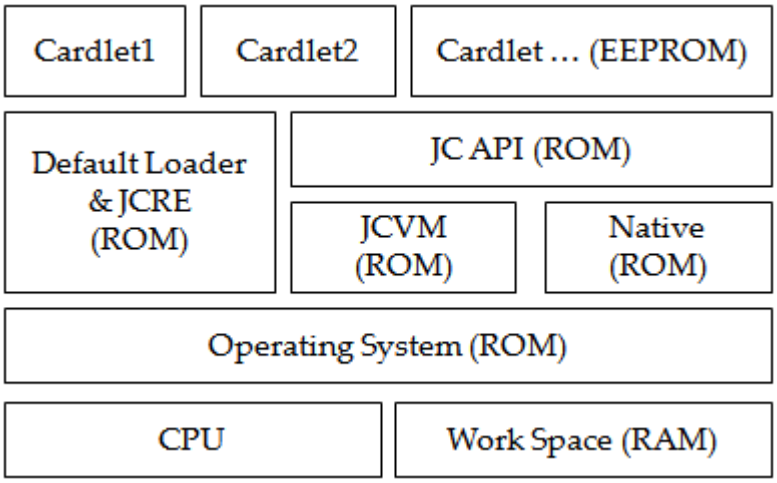


Fig. 17: The JavaCard architecture

The most important objective of the JavaCard is providing data security, which can be achieved by various aspects of this technology categorised as follows:

- Data Encapsulation: data is stored within applications which are run in an isolated environment (JCVM) separated from underlying OS and hardware;
- Applet Firewall: isolates applications and checks access of data elements of one applet to another;
- Cryptography: supports commonly used encryption techniques such as DES, 3DES, AES, RSA, Signing, key generation and key exchange.
- Applet: is a state machine, which only processes incoming requests and sends back data to the interface.

Employing the JavaCard technology in the Simulcrypt CA system can add more flexibility in management and provide wider range of value-added services and higher level of security [88].

5.4.4 Downloadable CA System

For security and business reasons, the service providers usually prefer to run and enforce their own security mechanism. As such, they provide set-top boxes directly to end-users. The DVB protocols, NRSS and DAVIC solutions are aimed to break such a transaction model and prepare an infrastructure where higher level of interoperability can be achieved between CA systems and set-top boxes. However, issues like the need for an agreement amongst service providers to use each others' system, inefficient bandwidth usage, high cost, lack of flexibility and functionality are yet to be addressed. In response, a software downloading scheme [65] was proposed to enhance Multicrypt in 2000 followed by standardisation of downloading interoperable Java APIs on set-top boxes by DVB and DAVIC. It has been claimed that higher flexibility and interoperability can be achieved via running interoperable applications on different types of set-top boxes. The scheme requires defining platform abstraction runtime engines (i.e. MHEG-5, Java Virtual Machine - JVM) into the set-top box software stack and standardised APIs for set-top box functions [19]. The OPTIMA is an abstract example of the downloadable CA system [84].

The downloadable applications can be downloaded from the security module or coupled with MPEG-2 TS or downloaded from a server though a telephone line. The interoperability can be realised in three following levels:

- Application-CA interoperability which can be achieved via downloading CA-related APIs into a STB to enhance the standard CA interfaces (i.e. CA0, CA1). The API provides low-level access to standard security modules (i.e. PC Card, Smartcard) to handle CA functions associated to services and read/change CA-related settings. An example is the CA API defined in the DAVIC [19];

- CA-STB interoperability which covers entire CA functionalities of a STB. It is particularly suitable for the Smartcard-based CA system though a PC-Card-based CA system may benefit too. It requires an open access to the set-top box functions and security module using corresponding low-level APIs. The APIs replace standard CA interfaces and make accessible the basic set-top box functions (i.e. filtering, descrambling, etc.), which are needed by the downloaded CA system;
- Copy right protection can be achieved via enhancing the native applications in the set-top box to support a native cryptographic API, which provides access to common mathematical operations of cryptographic algorithms.

Fig. 18 shows the software stack proposed for a downloadable CA system.

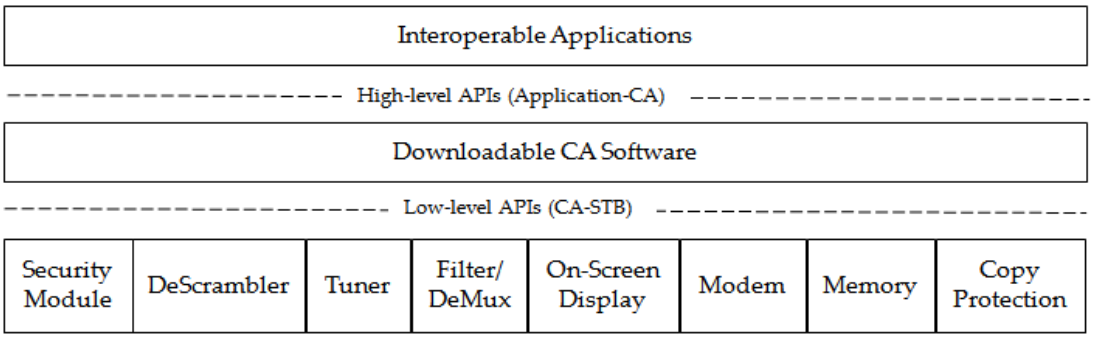


Fig. 18: The software stack operating in a downloadable CA system

5.4.5 Common Smartcard-based CA System

In response to the limitations such as interoperability, control relationship (between a set-top box and smartcard) and encouraging private CA system, a common smartcard-based CA system has been proposed in China. The common smartcard-based CA system can be considered as a smartcard-based implementation of the Multicrypt replacing the PCMCIA-based implementation. The private components of the CA subsystem will move to high performance 32-bit CPU smartcard while common components (i.e. descrambler) are still located

in the set-top box. The interactions between the set-top box and smartcard are handled by a Downloadable Common CA Module (DCCAM) via an ISO 7816 interface. The DCCAM adds more flexibility to the CA system. It is a software module located in the set-top box and smartcard.

There are four components defined as part of the STB-DCCAM to mainly handle communication with the smartcard across the ISO 7816 interface, perform authentication, protect the sensitive data exchanged across the interface and control the relationship between the set-top box and smartcard.

There are two ways of implementing the DCCAM which were suggested in the proposal as the common and proprietary smartcard CA platforms. The former provides a common platform where the DCCAM is developed by a set-top box producer or third party and inserted into the set-top box and smartcard. The CA vendor can download his CA system into the smartcard, which communicates with the smartcard using standardised protocols over ISO 7816 interface. In the proprietary approach both DCCAM and smartcard are provided by a CA vendor. Thus, the DCCAM needs to be developed platform-independently, based on standard APIs and using widely accepted languages. The DCCAM can be downloaded to the set-top box via the smartcard or over broadcasting medium or through a return path [119]. The common smartcard-based platform might have reduced the overall cost and improved the interchange ability in the system; however, due to the technological and commercial problems attributed to the Chinese market, it was not accepted for China. The immaturity of 32-bit RISC smartcards to perform cryptographic and real-time operations, lack of standardised middleware to support DCCAM and cost of replacing the 8-bit CA subsystem were amid the main problems attributed to the common smartcard-based CA system.

In response, a smartcard-based separation scheme was proposed to the Pay-TV conditional access system in China. The separation scheme makes the set-top box or digital TV receiver a common platform independent of any specific CA system. The separation scheme is very similar to the Multicrypt but replaces the PCMCIA with an 8-bit smartcard. The common part of the CA resides in the set-top box to support the proprietary part of the CA subsystem located in the smartcard. The communication between the set-top box and smartcard is handled by a common software package called Common CA Package (CCAP) which is hosted in both set-top box and smartcard. Fig. 19 presents the reference model of the smartcard-based separation scheme [116].

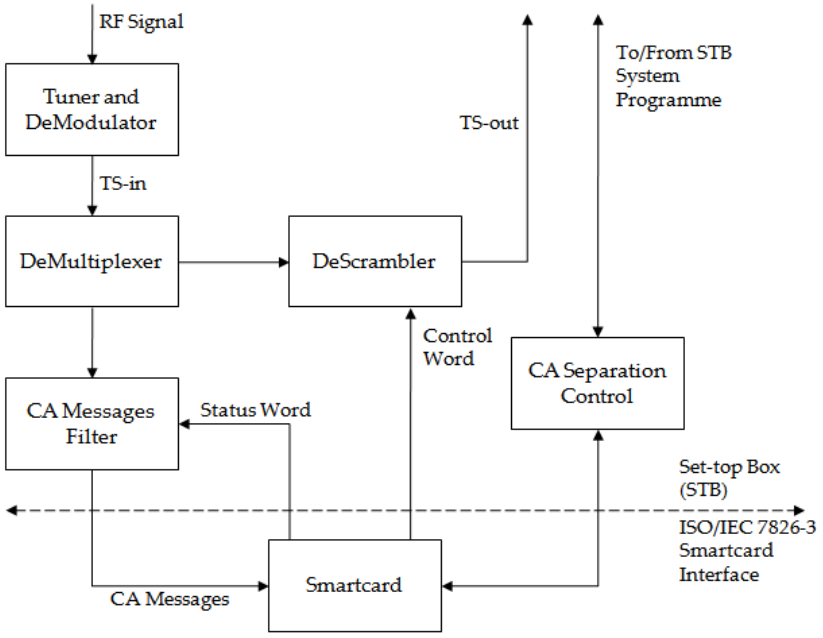


Fig. 19: A reference model for the smartcard-based separation scheme

The standardisation of such a separation scheme was encouraged by the Chinese government as it has managed to satisfy following promises required by DTV players in China (i.e. DTV service providers, CA providers, STB producers, etc.) [116].

- The deployment cost of the scheme is relatively cheaper than formerly explained schemes (i.e. Multicrypt, Simulcrypt, Common smartcard-based CA systems);
- It is more secure at the receiver-ends than the previous schemes;
- It does not imply any significant changes at the broadcasting head-end;
- It can accommodate most CA systems existed at the time;
- It does not stipulate any implementation detail for implementing the proprietary parts of the CA system;
- It will be able to use the cheap 8-bit smartcard as the security module to achieve both low cost and high interoperability.

5.4.6 Metadata-based CA System

New services like digital broadcasting receivers using metadata (DBRM) [75], which have the capacity for recording programmes and internet connectivity are becoming so popular. These services allow viewers to watch programmes out of normal broadcasting hours and view programme highlights using metadata.

It is important to protect stored contents from unauthorised use and viewers from malicious metadata that can be reconstructed from original metadata. Therefore, an access control technique is required to enable service providers protect their revenue stream. The content protection techniques including content protection for recordable media (CPRM) [10] and digital transmission content protection (DTCP) [22] can not provide any conditional access mechanism. The conditional access techniques do not provide any mechanism for handling complex use-cases introduced by the metadata such as the playback for only certain scenes. A distribution control technique for content and metadata was proposed using management information [117]. However, it does not provide any access control to content through metadata. Therefore, an advanced

conditional access system for digital broadcasting receivers using metadata has been proposed [80].

The metadata is described in the XML description scheme [112] to ensure the interoperability amid receivers. It is transmitted to DBRM via broadcasting medium or internet connections and classified in four major types as follows.

- Content description metadata which describe general content information (i.e. title and genre);
- Instance description metadata which describe content transmission parameters (i.e. channel name);
- Segmentation metadata which describe scenes in the content (i.e. scene grouping);
- User metadata which are descriptions created by the user (i.e. book marks).

The metadata can be created by a content creator, service provider or viewers. There is a concern that authorised metadata might be maliciously falsified or created with malicious intentions. Thus, the CAS for DBRM has been proposed to satisfy the following requirements:

- Metadata should be tamper-proof;
- Metadata creators should be certified;
- Access control to stored content through segmentation metadata should be possible under the control of broadcasters;

The advanced CA system for DBRM prevents metadata tampering and unauthorised access to the contents stored on DBRM using the digital signature and authentication techniques. The metadata is sent as an encrypted document or as a plain text protected by a digital signature. The access control for receiving and playback are usually handled via content encryption and entitlement messages (i.e. license information) [13], [112]. The proposed CA system for

DBRM uses license information, which includes a content key and metadata access control descriptors indicating metadata creators, who are permitted access to content. The service provider sends the license information required to access the content and the digitally signed metadata to legitimate viewers.

5.5 Summary

The CA is a technique used in Pay-TV systems to protect payable contents from unauthorised viewing. The motivation for conditional access can be concluded to controlling costs, generating revenue and preventing commercial piracy. The technique was firstly used in the Europe and USA and is now spreading across the globe.

In this section a typical model of Pay-TV systems was presented followed by business criteria set by the Eurocrypt. Then, the advancements in the access control mechanisms since the Digital Video Broadcasting (DVB) group suggested a CA technique to guarantee revenue in the Pay-TV systems were described.

The very early versions of the CA system were Simulcrypt and Multicrypt – the protocols defined by the DVB group. The DVB protocols were defined to encourage interoperability between CA systems in the Pay-TV system. The former adopts a smartcard-based CA system where various service providers can co-exist at the head-end sharing a common scrambler. The latter adopts a PC-Card-based CA system supporting multiple CA systems via a common interface at the receiver-end.

The Simulcrypt offers cheap smartcard-based set-top boxes which are dedicated to a single CA system; as such it limits end-users to Simulcrypt-enabled service providers. In practice, it requires an agreement amid service providers to use a shared scrambling system, multiplexer and each others' set-top boxes, which are not welcomed by service providers. Moreover,

Nowadays, digital broadcasting receivers using metadata (DBRM) with recording and internet connectivity has become so popular. These services allow viewers to watch programmes out of normal broadcasting hours and view programme highlights using metadata. It is important to protect stored contents from unauthorised use and viewers from malicious metadata that can be reconstructed from original metadata. The content protection techniques can not provide any conditional access mechanism and conditional access techniques do not provide any mechanism for handling complex use-cases introduced by the metadata; such as the playback for only certain scenes. Thus, a distribution control technique for content and metadata was proposed using management information. However, it does not provide any access control to content through metadata. Therefore, an advanced conditional access system for digital broadcasting receivers using metadata has been proposed. It prevents metadata tampering and unauthorised access to contents stored on DBRM using the digital signature and authentication techniques. The access control for receiving and playback are usually handled via content encryption and entitlement messages.

The CA systems discussed above mainly address the interoperability and interchange-ability issues between CA systems. They are not suitable for handling new challenges arisen by converging networks and emerging of convergent services. They are not concerned with interactivity and

personalisation concepts. Moreover, they are although a little but not addressed high cost of operation and security flawed in Pay-TV systems.

The next chapter thoroughly analyses requirements and new use-cases that should be properly addressed in this era of technology. It then proposes novel security architectures to meet these requirements.

6 ENHANCED CA SOLUTIONS AND DESIGN

6.1 Introduction

The network convergence as a new phenomenon has opened new business opportunities for network operators and service providers. This has already emerged in the mobile and Internet based platforms and to some extent in the DTV. The content delivery through the Internet is now being offered in the DTV and standards like DVB-T/-H also enable broadcasters to reach the hand-held devices. The range of services has been diversified although there are still fundamental issues in the Pay-TV systems yet to be resolved. Some of the inherited issues include the improper business models, lack of interoperability, high administration and operational costs. Considering that the viewers are financing the Pay-TV business, the overall costs are transferred to them. This needs to be controlled to compete effectively in an increasingly price-driven market.

The convergence of the Internet, Mobile and DTV platforms can be utilised to tackle the inherited issues in the Pay-TV system. The converged platforms also enables the service providers to keep up with the next generation multimedia services offering enhanced interactivity, personalisation and higher security. Considering the novelty and market penetration criteria, this chapter proposes high level convergence solutions to the inherited issues, elaborates the Mobile Integrated Conditional Access System (MICAS) and elicits the non-functional and functional requirements through various use case scenarios. It is followed by detailing possible security architectures in the proposed system.

6.2 Inherent Issues in Pay-TV Systems

The overall expectation of TV consumers has now evolved dramatically compared to the analogue TV arena thanks to the technology boost and implementation of the digital and interactive TV. Nowadays Internet service providers, mobile operators and broadcasters tend to diversify their services and are merging with each other to expand their businesses. In this competitive environment, the broadcasters and in particular Pay-TV service providers need to fully revise their system structure and adapt it to a dynamic and scalable platform. Such platform shall rectify well-known issues and welcome new technologies and services for the next generation of TV consumers. These issues together with potential solutions are explained in this section.

6.2.1 Transaction Models and Interoperability

Two business models are usually incorporated in the CA broadcasting system: the vertically-integrated CA system and advanced CA system.

The vertically-integrated CA system has been more popular in cable systems. It consists of a service provider who also controls the network, designs the CA system, supplies and owns decoders. The tailored decoders are carefully integrated by a set-top box producer into his set-top boxes. The set-top box producer needs to compete for an order for his set-top boxes from the service provider. He also needs to sign a non-disclosure-agreement to use the service provider's tailored CA system in his set-top boxes. The service provider usually employs a single proprietary CA system that does not share any part with other competitors' CA system. Thus, this model compromises the interoperability between various CA systems. It also scales down the business, in particular for newcomers and set-top box producers. Furthermore, it impedes the

implementation of the horizontally integrated business model in CA broadcasting systems.

The advanced CA system is more popular in analogue satellite systems. It rather mitigates the interoperability issue amongst service providers. In this model a common delivery system or CA system, which is owned and operated by different third parties, is shared amongst service providers. This however implies that the CA system provider shall have full access to all viewers' details (i.e. names, addresses, entitlements status) to carry out all billing transactions. This model is not as popular as vertically-integrated CA system model due to the fact that the service providers are reluctant to reveal any sensitive information about their system and customers. To date, most of commercially available CA systems are not compatible to each other at the receiver-end. Thus, it is fair to conclude that a shared CA system is not a desirable solution for encouraging a fair competition in an open and horizontal market where security and commercial requirements of service providers are satisfied.

A truly interoperable CA system does not seem to be a practical solution for CA broadcasting systems. However, a platform that enables the service providers to openly advertise and deliver their services based on their own proprietary CA system without imposing additional costs to the viewers might be a viable solution for transforming the traditional transaction models to a more open and flexible one. This model requires a security architecture that allows service providers to deploy their proprietary security cost effectively as and when it is needed. Such a solution may not completely resolve the interoperability issue, but it can establish an open Pay-TV market for service providers, set-top box producers, CA providers and TV consumers. In this utopia, a viewer can also enjoy a range of TV services offered by service providers who are accessible via an arbitrary set-top box.

6.2.2 System and Bandwidth Requirements

The nature of the communication network has an impact on the complexity and bandwidth requirements in the design of CA security architecture. The most challenging type of the network is a broadcast-only environment (i.e. satellite and terrestrial communication networks), where there is no return channel between viewers and the service provider. Hence, the service provider cannot ascertain whether the viewer has received the conditional access message. This is particularly the case when most of the set-top boxes are not receiving anything when they are switched-off or in the stand-by mode (i.e. for energy saving). Thus, the transmission of a conditional access message needs to be repeated to ensure that authorised viewers can access to contents that they have paid for. This ultimately implies large overhead in data transmission.

A transport stream (TS) consists of small numbers of Entitlement Control Message (ECM) elementary streams (ES), one Entitlement Management Message (EMM) ES and (up to) eight services. The ECM, as a global message, is broadcast to all viewers in a service provider's population. It is inserted into its elementary stream about 10 times per second to enable quick access to contents after tuning to a service. Given the maximum size of an ECM (256 Bytes), the maximum bit rate required to transmit one ECM would be about 20 Kbps. This is rather negligible comparing to several bit rates required for transmitting video streams.

The EMM is broadcast for each event (i.e. sport matches or films) and it is usually intended for a single or group of viewers. It is restricted to 256 Bytes for synchronisation and smart-card processing reasons at the receiver end. The maximum bandwidth required to transmit EMMs mainly depends on the number of subscribers and the broadcast encryption scheme, which is used to broadcast secrets to authorised viewers. Generally one bit per second per subscriber is considered high in a broadcasting-only environment. It corresponds

to upper-bound bandwidth of 1 Mbps per transport stream for a service provider comprising of one million subscribers. The lower-bound can be derived from Binary Entropy Function ($-P\log_2^{(P)}-(1-P)\log_2^{(1-P)}$) [96], where viewers place independently their orders with probability of P. Thus, when P equals to 0.5 (unbiased bit), at least one bit of information per combination of the subscriber and event needs to be broadcast.

The complexity of the system mainly regards to the design of the EMM Injector and set-top box architecture (i.e. filter spacing, smart-card processing). At the head-end, the EMM injector repeatedly injects EMM elementary streams into a MPEG-2 multiplexer to be inserted into the corresponding TS. The TS is broadcast to a single or group of subscribers participating into an event. At the receiver-end, the EMM filters (unique or group based filters) integrated into the set-top box pick up corresponding EMMs and deliver them to the attached smart card for decryption. The synchronisation of EMM injection at the head-end and EMM processing (from filtering to releasing control words) at the receiver-end is crucial to the success of the CA broadcasting system. Failing to deliver control words in time prevents authorised subscribers access to the contents of the paid events, which would result in degradation of customer satisfaction level and revenue.

The high channel costs (bandwidth deficiency) and system complexity in CA broadcasting systems are mainly due to the lack of communication and inefficient interactions between head-end and receiver-ends. For instance, if access control messages are sent to individuals from a return channel (i.e. GSM network) then more bandwidth will be freed for commercialisation purposes. In addition, exchanging information over the return channel using hand-shake protocols can ascertain higher level of security with lower complexity in the CA

system, as there will be no need to design the EMM Injector based on queuing models [44] and repeating EMMs in a data (object) carousel.

6.2.3 Administration and Operational Costs

As mentioned before, in the vertically integrated CA transaction model, the service provider supplies and owns decoders. The set-top box producer needs to sign non-disclosure agreements to integrate the service provider's decoders into his set-top boxes to function under the service provider's CA system. Such exclusivity in the market would reduce commercial scale of service providers and set-top box producers. Hence, resultant products will be too expensive to be attractive for normal TV consumers. Ultimately, the service provider has to subsidise or in some cases provide his tailored receivers free of charge [116].

Apart from providing the receiver, there is another cost for installing the subscriber access equipment (i.e. satellite dish, set-top box, phone sockets, etc.) Service providers usually contract out the installation of the access equipment to trained and trusted contractors to reduce the security risks and maintenance costs. The engineers need to go to the customer's premises to install access equipment and activate the customer's account. Such a procedure tends to be very costly for service providers so that the deployment cost has been constantly attributed as the highest cost beside the contents in CA broadcasting systems.

The deployment cost can be cut down by adopting an automated system to monitor and download the CA system to an arbitrary set-top box over broadcasting or return channels. In this case, customers will be responsible for buying and installing the TV access equipment. Such reduction in the deployment cost would potentially relieve subscription fees and indirectly compensate customers for installation costs. In addition, in this business model set-top box producers can compete in a wider price-driven market and

potentially attract more revenue. That would ultimately result in emerging wider range of products with different features and competitive prices.

6.2.4 Security Flaw Cost

The Pay-TV system is commercially oriented which provides TV services to subscribers in return of a subscription fee. The CA system is the security technology adopted in the Pay-TV system to prevent illegal access to contents. The CA system is supposed to only let legitimate subscribers enjoy their paid services. As TV consumers are reluctant to pay for subscription fees, there have always been various types of piracy in Pay-TV systems. Nowadays, the Internet communication provides a platform wherein pirates with various levels of expertise can collude and grow up in 'black communities'. Such piracy threats can cast a shadow over billions of pounds taking into account world-wide providers [41]. The underlying costs can be broken down into several sections including illegal access to TV programmes, operating costs (i.e. investigating for crime and piracy in the Pay-TV and replacing compromised security elements) and corresponding administration costs. The customised receivers and tailored CA system are amongst the counter measures employed by service providers to protect their investment and revenue streams. However, these solutions, as mentioned earlier, limit the service provider's business scale, lead to less choice and duplication of access equipment at the receiver-end, and yet, do not ease off the operating costs.

Employing advanced security techniques is necessary but it is not enough to prevent pervasive and advanced attacks like card-sharing by which one legitimate user colludes to provide protected content to a larger group of illegitimate users [41]. In addition to encryption and authentication techniques, effective usage guidelines must be enforced upon which service providers

monitor and control behavioural contracts through effective interactions with subscribers at the receiver-ends. In case of detecting any illegal activities, the service provider shall adopt effective counter measures and replace the compromised security keys or algorithms cost effectively (i.e. on-line over interaction channels). Security mechanisms such as detecting, revoking and replacing compromised security elements, would possibly increase the security level and reduce security flaws associated costs if they are executed automatically over secure channels (i.e. GSM network).

6.2.5 Interactivity and Personalisation

From the technical perspective, the interactive TV can be introduced in following categories:

- The Interactive Digital TV on terrestrial, cable, satellite or broadband network where a return channel is available to end-users;
- The Enhanced Digital TV where end-users have local interactivity only, as no return channel is available;
- The Participation TV which is common in analogue TV where end-users can participate to some degree in programmes through a return channel such as phone, SMS or email.

The Interactive DTV has been mainly targeted by independent developers and academic researchers so far, while Enhanced DTV and Participation TV have been more widespread and indeed of greater economic significance. Nevertheless, looking at the prospective of the DTV (i.e. shifting from consuming media to creating media, emergence of broadcast media and data cast services) and considering on-going plans for the transition from analogue to digital transmission, it is likely that the Interactive DTV will take over other traditional business models.

The Interactive DTV can introduce a wider range of features, which will ultimately facilitate the trade-offs in bandwidth requirements for broadcast media in standard definition, high definition and Datacast services. It is also worthwhile noting that the interactivity can play an important role besides providing more choice, technical enhancements and personalisation features in assuring the take-up of the digital television, so that the analogue-switch-off phase will take place with the least problem.

The personalisation emphasises on "Anything, Anytime and Anywhere" paradigm which potentially results in the decline of social viewing and increase of number of television sets per household [71]. Such a trend would justify the emergence of technologies like Mobile-TV and IPTV which have been already announced to keep up with new consumption patterns and adjust the mobility and personalisation features for TV-like services.

The traditional platform of TV services does not allow operators to ubiquitously offer mobility and personalised services. Nevertheless, value-added services like electronic programme guides, enhanced background information on programmes, internet access, video on demand, near video on demand have certain business value. The mobility in Pay-TV and improved personalised services require a platform with at least the support of bi-directional communication. Such a platform shall provide service providers with adequate information to strengthen their customer relationship and with technologies to enable customers to submit their request(s) at anytime and anywhere with an expectation of a prompt service delivery at lowest cost and highest quality. Such quality and cost criteria can be well satisfied in a broadcasting network using TV service access equipment. However, it is required to integrate another technology such as mobile technology into the Pay-TV system in order to add mobility and

personalisation services (i.e. targeted marketing) to the traditional Pay-TV system.

As discussed in Chapter 3 and 4, the mobile technology, which is widely available today and uniquely bound to individuals as a personal possession, offers a secure platform (i.e. SIM card), connectivity features and protocols (i.e. Bluetooth, SMS and WAP). Hence, it can be utilized by service providers to recognise their customers and provide them with related information. Such information would enable them to make the most of their entitlements and available services. These would ultimately improve customer relationship management, decrease the customer churn rate and increase profits.

6.2.6 Subscription Fees and Convenience for Viewers

The lack of interoperability amid service providers in vertical transaction model together with its corresponding administration, operation and security flaw costs would result in relatively high subscription fees. The key point is that TV consumers are seeking low cost services comparable to Free-To-Air (FTO) or Free-View services. Therefore, it is essential for Pay-TV operators to reduce their costs, diversify their services and keep the subscription fees as low as possible.

In addition, viewers should benefit from wide choice of set-top boxes produced by various manufacturers competing in an open market. Also, the viewers should be provided with multiple services readily available by various service providers via any standardised receiver. In such an open market, service providers can fairly compete with each other to deliver services cost-effectively using leading-edge technologies. On the other hand, viewers will benefit from a range of services, quick service delivery, low subscription fees and multiple choices of services and receivers.

These requirements can be met by standardising some parts of DTV receivers in a way that service providers can deploy their tailored conditional access subsystem on-line into a security element (i.e. smartcard or SIM card). The list of available services and service providers should be provided with viewers to freely choose their favourite services at anytime and anywhere via an established return channel.

6.3 Solution Statement

There have been various activities in resolving some of the inherited issues discussed above during the earlier stages of introducing the CA technique. However, no effective solution has yet been suggested to address present and future demands. Nowadays, communication boundaries have been shifted so that broadcasters are more inclined to diversify their services via utilizing the Internet and mobile platforms. Such convergence can be effectively used to establish an end-to-end CA system offering a more flexible, intelligent, scalable, interoperable and ubiquitous security system in Pay-TV systems.

The marriage of broadcasting and telecommunication networks can widen the range of bespoke services and extend the concept of personalisation. As a result, the rigid one-to-one relation between a viewer and set-top box in the Pay-TV system can be mitigated using an intermediary that uniquely represents the viewer in that platform.

The following subsections consider the abovementioned issues and propose state-of-the-art solutions to resolve mobility and interoperability in the Pay-TV system. The solutions are elaborated using simple real-life scenarios where John, who usually travels around, is an authorised subscriber of the service provider called SP.

John would like to enjoy his subscription or amend it to watch his favourite programmes (i.e. local news, sport events or premier films) whenever he wishes to. At the moment, he can not have access to his subscription when he is not at the vicinity of his set-top box provided by the SP. However, services like pay-per-view, near-video-on-demand and video-on-demand may enable him to buy programmes via a once-off payment. In fact, when he stays at a hotel, he will be bound to TV services offered by the hotel. A desirable business model can be that Pay-TV subscribers can access their subscriptions through any certified set-top boxes; resembling the ATM machines in the banking system where customers can have access to their bank accounts through any ATM machine.

In light of that need, the following solutions are proposed based on popular technologies which are widely available to establish an interaction channel between John and SP.

6.3.1 Cooperating Broadcast and Internet CA System

The Internet is a worldwide and publicly accessible series of interconnected computer networks connecting large geographical areas together. Therefore, it can be effectively used to connect service providers and viewers together. In this case, the requisite information that helps the SP to identify John and his set-top box can be sent over the Internet. The set-top box can be identified via its secured and unique identity number (i.e. MAC address or IP address) and, John can be identified either through a challenge/response process or through his public digital signature. The SP can put John's signature or any security related information in a secure website in the Internet domain. John then can log into his account for instance via his set-top box and download his signature to sign the subscription request(s).

The proposed solution needs a set-top box with Ethernet connectivity, a valid IP-address and requisite APIs to handle data communication, security functions and subscription processes. The APIs can be downloaded and updated by the SP for instance through the broadcasting network or interaction channels such as the Internet. At the head-end, John's subscription request shall be validated before granting any content access keys.

Fig. 20 shows the overall architecture of the internet integrated Pay-TV conditional access system.

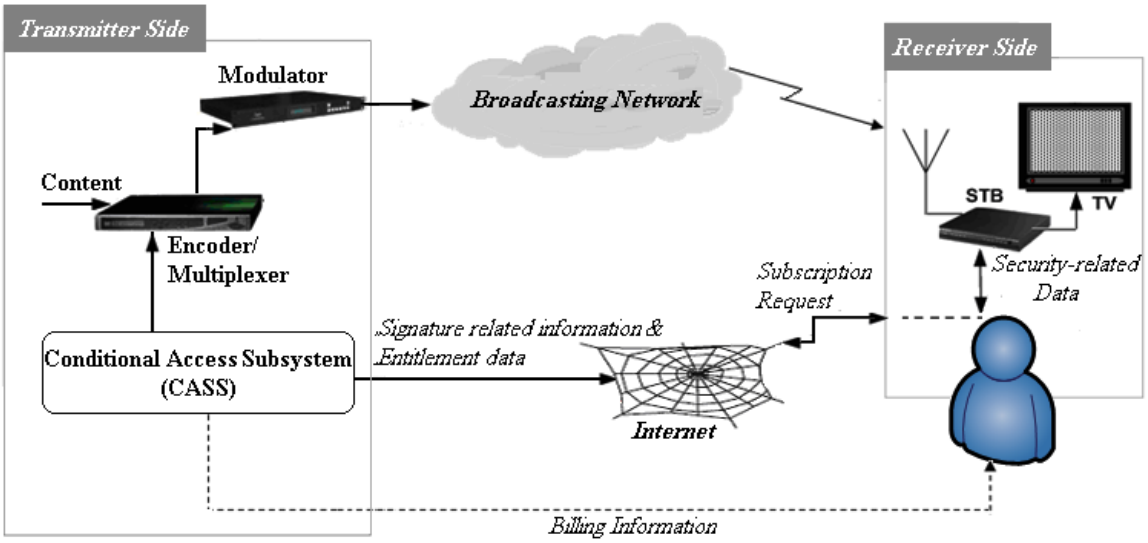


Fig. 20: The reference model of Internet integrated CA System

6.3.2 Cooperating Broadcast and GSM CA System

The GSM network with billions of subscribers is a popular and secure network which has been recognised as a potential return channel in broadcasting systems (i.e. DVB). Every GSM subscriber has a mobile phone operating with a SIM card. The SIM card which is bound to the subscriber provides a secure, programmable and remotely accessible platform. If the mobile operate grants the permission, it can be used to store and deploy conditional access mechanisms. Hence, it can be considered as an alternative to the smartcard technology. A result of this replacement could be the emergence of more affordable set-top boxes.

In addition, incorporating mobile technologies can also extend mobility features in broadcasting systems, it means that the subscriber no longer needs to be at home at the vicinity of the pre-selected set-top box to enjoy his/her entitlements. The one-to-one rigid relationship between an authorised subscriber (like John) and his set-top box can be adjusted, if SP could uniquely identify John, his set-top box and ultimately prevent any anticipatory repudiation and piracy. In this approach, John can be identified through a challenge/response authentication process or based on his IMSI or mobile number stored at his SIM card. His mobile phone can be identified by its IMEI and his location can be recognised by LAI stored in the SIM card. His set-top box can be identified for instance using a unique identity number assigned by its manufacturer. It is worthwhile mentioning that the set-top box identity number and smartcard unique (or group) addresses are already used by service providers for authentication and access control purposes.

The proposed solution needs a set-top box with wireless connectivity (i.e. GSM, Wi-Fi, Bluetooth or IR) and a class of APIs to handle security functions as well as subscription processes. As mentioned before, the required APIs can be downloaded or updated by SP through any available communication link (i.e. broadcasting medium). The APIs installed in the set-top box shall provide John with a request submission wizard to select his favourite service(s) and the mobile phone from the list of, for instance, nearby Bluetooth devices discovered by set-top box. The set-top box then signs the request using its identity number and sends it through a wireless link (i.e. Bluetooth) to the selected device (i.e. John's mobile phone). The request may be then digitally re-signed at the SIM card using John's signature (i.e. using his IMSI number or a private key provided by SP) and then forwarded to the CASS using transport protocols such as the Short Message Service (SMS) or Wireless Application Protocol (WAP). Once the message is

received at the head-end, the sender, set-top box and subscription request are validated. If the validation process succeeds, requisite credentials shall be transferred to the set-top box either through the broadcasting network or the GSM network utilising John's mobile phone as an intermediary device between SP and set-top box.

Fig. 21 shows the architecture of the mobile integrated conditional access system (MICAS) in Pay-TV systems.

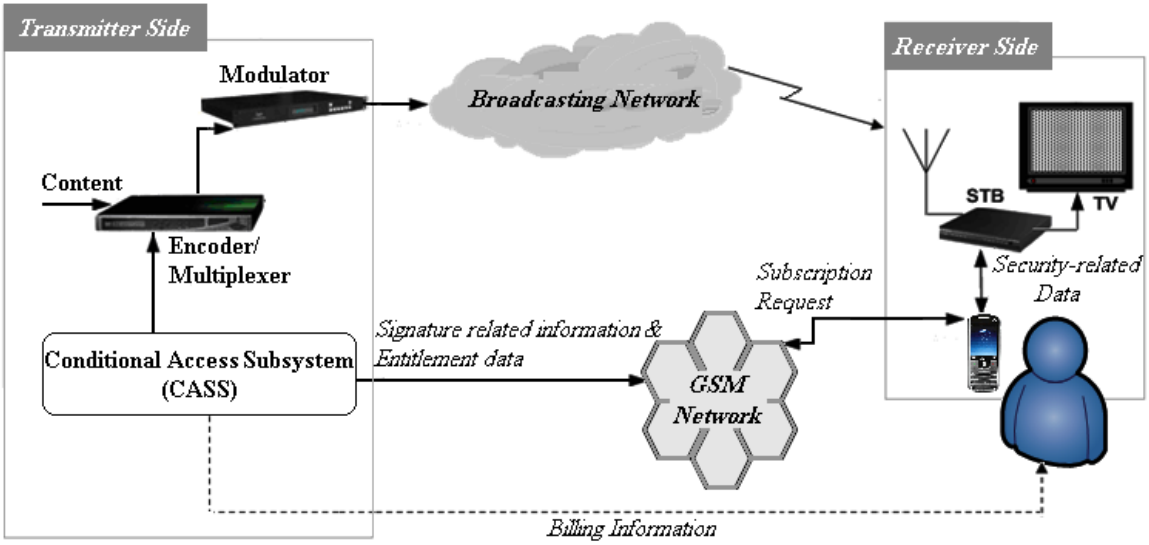


Fig. 21: The reference model of GSM integrated CA system

6.3.3 Cooperating Broadcast and GPRS CA System

In the next generations of GSM technology (i.e. GPRS, UMTS, EDGE, etc.), services like WAP access, SMS and Internet communication services such as email and web access are available to mobile users. Therefore, the previous solutions can be amalgamated together to form a GPRS integrated CA system in the broadcasting system. Its great advantage is the higher security level that can be established for instance through the WAP protocol and IP-Sec.

Similar to the previous approaches, the subscriber can be identified through his mobile phone's IMSI number or IP address and, the set-top box can be identified via its unique IP address and/or its equipment identity number. The registration

and identification processes can also be executed in the same way explained before.

6.3.4 CA System for Multi-domain Pay-TV Systems

In the described integrated systems, the possible approaches for eliminating the rigid one-to-one relationship between TV subscribers and service providers were addressed. The proposed systems can offer various services like Subscription and Pay-Per-View. However, delivery of TV services to subscribers, who are in a geographical area beyond service provider's service coverage, is not possible. For instance, when John travels to another country, the local TV programmes will not be accessible; as such he cannot enjoy his subscription where SP does not have any service coverage. Such a shortfall in coverage is chiefly attributed to the technical limitations of the terrestrial, satellite or cable technologies.

The GSM (2G) network, although, it is becoming more popular, it does not meet bandwidth requirement for multimedia delivery. The next generation of the mobile network like 4G and LTE, on the other hand, provide robust platform for delivery of multimedia services to mobile users enjoying the quality of TV-like services. Nevertheless, problems like bad reception, short battery life and low resolution display units in hand-held devices are yet to be resolved.

The Internet with worldwide coverage and sufficient bandwidth (at least in the core network) can be leveraged for establishing a global service delivery in Pay-TV system (i.e. Internet Television, IPTV). The bandwidth, quality of experience (QoE) and security constraints have been well addressed and standardised in IP-based networks. The mobile and Internet conditional access systems proposed earlier need to be enhanced though to support cross-border multimedia service delivery and corresponding access control mechanism.

The globalised Pay-TV system can also benefit from IP Datacast (IPDC). In the IPDC various IP streams (i.e. audio and video streams) are generated by the Service Subsystem (SS) to be distributed over a multicast intranet to IP-Encapsulator(s) [40]. The IP-Encapsulator will feed the video/audio/data elementary streams to a multiplexer which forms transport streams, and then, broadcasts them over satellite, cable or terrestrial medium. The CASS manages subscribers' account, subscription requests, billing processes and controls access to contents.

In the global zone interconnected by IP-based networks, a viewer (or an existing subscriber) can send a subscription request to a particular service provider regardless of time and location. Similar to the previous models, the request should enable the service provider to identify the subscriber, his set-top box, location and full specification of requested services. The locale of the subscriber can be identified from subscriber's LAI number saved in the subscriber's SIM card or roughly via the set-top box IP address. After having recognised the subscriber, set-top box and his location, the remote service provider will notify a local service provider of the subscriber's request. The remote service provider then forwards the encoded services (i.e. data, video, audio IP streams plus temporarily entitlement messages) to the subscriber either directly through the local service provider or the Internet connection. Considering that service providers are usually reluctant to reveal their control access mechanisms, hence any security functions or subscribers' related information, which needs to be provided to other service providers must be only valid temporarily. The security mechanisms (i.e. for authentication, encoding/decoding purposes) can be installed into the set-top box either through the broadcasting networks, Internet or GSM via subscriber's mobile phone. The remote service provider can send the key information to the subscriber (or

directly to the set-top box) through the Internet or GSM network. Fig. 22 shows overall architecture of the globalise Pay-TV system.

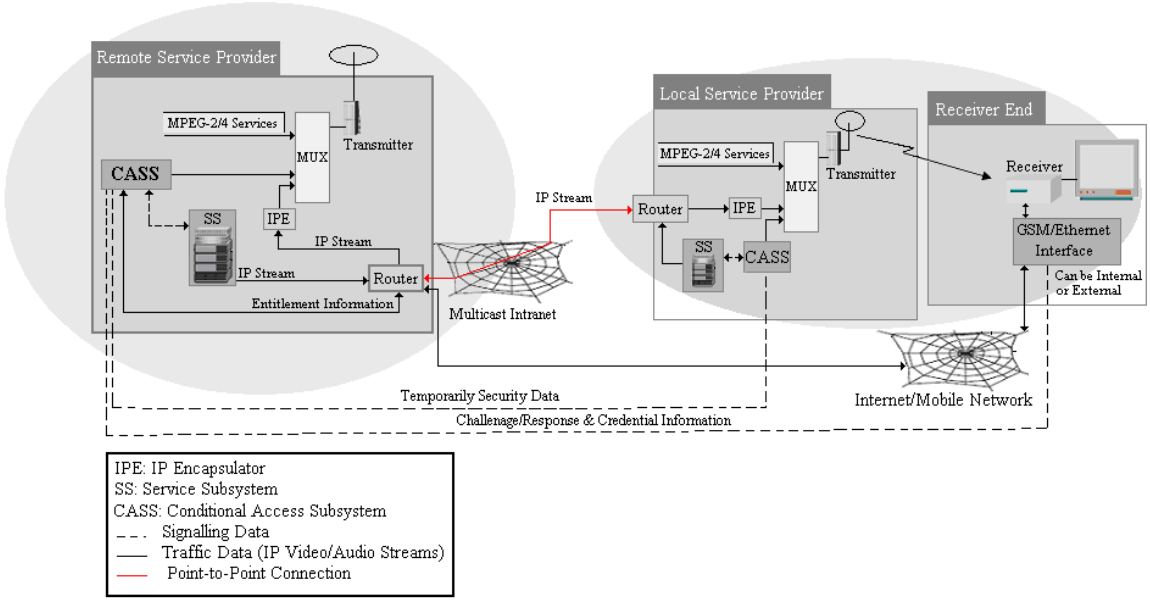


Fig. 22: An access control system for multi-domain Pay-TV systems

In this architecture, the dynamic allocation of bandwidth for multimedia services requested by random groups of TV consumers can be one of the most challenging issues for service providers (network operators). The analogue switch-off might ease up the situation in the broadcasting networks, but thorough resource management needs to be planned for delivery of high quality multimedia services over heterogeneous IP-based networks.

At this moment, with exception of some developed countries (North America, Europe and Asia Pacific) that offer broadband services using diverse technologies (i.e. fibre optic communication, 3G mobile networks, Wi-MAX and power-line), the rest of the world is still using low bandwidth Internet connections on the access network (i.e. dial-up of 56 kbps). As presented in Chapter 2, the cable or satellite technologies are more available and effective to be used for delivery of multimedia services across various regions, due to their

worldwide presence and the amount of bandwidth that they can provide. Nevertheless, upon availability of technology at each region, the method of service delivery (physical layer) can vary.

The Internet-only architecture will neither decrease the overall production cost of the set-top box nor improve mobility nor the level of personalisation in the Pay-TV system. Moreover, the emergence of PC-based access to IPTV services possibly compromise commercial take-up of the proposed architecture. On the other hand, the mobile-based solutions (GSM or GPRS solutions) can reduce the overall cost of the set-top box by replacing the smartcard in the set-top box with the SIM card in the mobile phone. They will also provide a flexible platform to improve mobility and personalised services in the Pay-TV system. Therefore, amid the proposed architectures, the mobile integrated solution is considered herewith as a primary approach to be analysed further. The functional and non-functional requirements are elicited through various use-cases, followed by describing diverse architectural models of the system.

6.4 Mobile Integrated CA System Design

The Mobile Integrated Conditional Access System (MICAS) introduces a new mobile application in the Pay-TV CA systems. It supports various security architectures and data flow models concerning the distribution of entitlements and access key information to the viewers. It also adds mobility features to the traditional Pay-TV system and as such services like 'Follow Me', which is detailed hereby, can be offered to the Pay-TV subscribers. Such mobility features, however, require implementing subsystems like Message Handling Subsystem (MHSS) operating at the transmitter and deploying some APIs at the receiver sides (i.e. set-top boxes and/or mobile phone). The MHSS will deal with subscribers' requests and establish a secure access control subsystem by

proactively monitoring end-users' behaviour and updating security mechanisms. The APIs used at the receiver-end provide various functionalities with proper user-interfaces enabling viewers to navigate through available services including online subscription, Pay-Per-View and Follow Me.

Following a brief description of design scale and pre-requirements (assumptions), the behaviour of the system is fully described using the Unified Modelling Language (UML) use case diagrams.

6.4.1 Scope and Assumptions

The goals and scale of the MICAS design are as follows:

- Enhance security and promote Know-Your-Customer (KYC) concept by enabling service providers to effectively interact with subscribers and update their security mechanism(s) via available mobile technologies;
- Extend personalised services and enabling viewers to effectively utilise their mobile phone(s) to interact with the set-top box and service provider;
- Provide viewers with user-friendly interfaces to manage their subscriptions using their mobile phone(s);
- Extend mobility features and let viewers enjoy their subscription via an arbitrary set-top box;

The MICAS design is based upon following assumptions:

- The GSM network is secure and both the mobile phone and set-top box, would support the Bluetooth connectivity at its highest security level;
- The Pay-TV service provider has a mutual agreement with mobile phone operator upon accessing to privileged domains in SIM cards or mobile phones population of the mobile operator;

- The subscriber's mobile phone would support Java technology and its subsequent standards such as Bluetooth connection (JSR-82) and security features - Security and Trust Services API (SATSA);
- The set-top box has a registered unique identifier and supports security technologies like hash function.
- The set-top box has a tamper resistant built-in memory (i.e. flash memory) beside an optional smartcard compatibility feature;

6.4.2 Stockholders and Actors

The main actors interacting with the MICAS are as follows.

1) The subscriber (viewer): an existing or new customer who pays for the service and wants to receive Pay-TV services over an arbitrary set-top box;

2) The Pay-TV service provider: it manages subscribers' accounts, grants content access permission, monitors activities in the field, delivers multimedia services and possibly owns the broadcasting network;

3) The conditional access provider: it can act as the service provider but to establish a security platform to ensure that only authorised subscribers can access to contents, security mechanisms are downloaded securely, updated regularly and compromised keys are revoked immediately;

4) The set-top box producer: it produces standardised set-top boxes with connectivity and security features;

5) The mobile network operator: it establishes an interaction channel amid Pay-TV subscribers and service provider, grants permission to Pay-TV service provider to access the privileged memory domains in SIM cards, provides short-message-service and wireless-application-protocol, possibly provides the Pay-TV service provider with geographical information of the subscriber and/or adequate

information to verify the identity of the subscriber based on subscriber's IMSI number;

6) The SIM/Smart card issuer: it produces SIM cards and/or Smart cards respectively used in mobile phones and set-top boxes. The card issuer shall publish the specifications of his cards (i.e. memory size and processor power, RAM etc.)

7) The set-top box certifier: it certifies the set-top box, assigns and registers the set-top box identifier (i.e. STB-ID, STB MAC address, STB IP address);

6.4.3 Non-functional Requirements

Some non-functional requirements of the MICAS are as follows.

1) Usability: a normal TV and mobile consumer should be able to perform the tasks; The set-top box shall be running a multi-language user interface; full instructions should accompany the set-top box or shall be found in the Internet in the service provider's (or set-top box producer's) web site;

2) Reliability: the set-top box should drive Bluetooth adapter making minimum inconvenience; the set-top box shall update the information of paired devices; the set-top box should handle well known and un-known Bluetooth and Graphical User Interface (GUI) related exceptions and the viewer should be able to restart the box in the event of failure; both set-top box and mobile phone should adopt maximum Bluetooth security service at the time of opening the connection;

3) Performance: the set-top box should respond to any viewer's query within one minute, the operation time related to decoding the content (i.e. Filtering, decoding access control messages like EMM and ECM) should be as low as possible to present pictures in real-time, the Bluetooth discovery process should be accomplished within 10 seconds, the set-top box can only respond to one Bluetooth connection at a time, the size of the data stored in the set-top box shall

be at least 1MB and in the SIM card should be at least 1KB, depending on the available memory size (i.e. SIM memory size varies from 2KB to 514KB), the worst latency acceptable for the viewer is considered as 30 seconds;

4) Supportability: the set-top box could be featured with GSM connectivity with a built-in SIM card or having a SIM card reader to read the viewer's SIM card. The set-top box producer and mobile phone operator shall provide effective troubleshooting, pre-/post- sale and support services;

5) Implementation: the set-top box and mobile phone shall be featured with appropriate software platform to support GUI, interactivity, Bluetooth connectivity and security related APIs; both set-top box and mobile phone are limited resource devices; as such Java based software configurations like CLDC (or CDC for set-top box) and MIDP profile supporting Wireless Toolkit APIs might be needed;

6) Interface: the set-top box needs to interact with the viewer and viewer's mobile phone, respectively through remote control and Bluetooth connection. The service provider interacts with the viewer through the viewer's mobile phone;

7) Operation: the initial interaction between the viewer and the service provider is managed via standardised APIs pre-installed in the set-top box and mobile phone by set-top box producer and mobile phone operator, the access control operations are managed by Pay-TV service provider;

8) Packaging: the set-top box (including all standardised APIs) is installed by set-top box producer, the viewer might be involved in installing some APIs in the set-top box downloaded off-air or in the mobile phone from certified sources, the Pay-TV service provider remotely (or mobile operator) installs the tailored conditional access subsystem in the viewer's mobile phone (i.e. SIM card);

9) Legal: Pay-TV service providers should reach a commercial consensus on multiple existence of service providers at transmitter (SIMULCRYPT) and

receiver (MULTICRYPT) sides, commercial agreement needs to be signed between the Pay-TV service providers and mobile operators;

In the next section the functional and user requirements are described through various use case models and scenarios defined in the MICAS.

6.4.4 Functional Requirements - Use Case Scenarios

The Pay-TV service provider can leverage diverse features of the MICAS to introduce new trends of consuming in Pay-TV system. The MICAS requires new type of standardised set-top boxes. In addition, the service provider and mobile phone operators need to be consolidated or at least have an agreement on sharing SIM cards inserted in their mobile phones. It is also desirable to establish an authority (a trustee) to certify set-top boxes and also manage set-top box identities. As mentioned before, the set-top box identity (STB-ID) can be used by the service provider to authenticate the set-top box and recognise the model and specifications of the set-top box. The viewer on the other hand has to set up his TV services' access point in order to benefit from the services offered in the MICAS. Given that the set-top box is receiving encoded streams, the viewer can subscribe to any available services using an arbitrary set-top box and his mobile phone, if they are properly paired together. The corresponding service provider will manage the subscriber's account and provide him with a proper mechanism to decode the paid contents.

Fig. 23 presents possible use case packages defined in the MICAS concerning the viewer and service provider's functionalities. Each package is separately treated in the following sections.

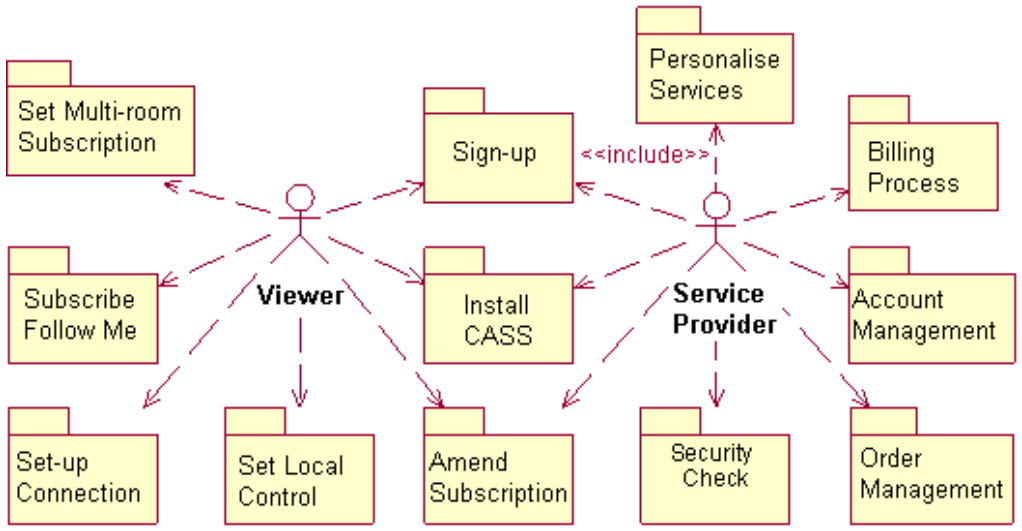


Fig. 23: The use-case packages defined in the MICAS

6.4.4.1 Set-up Connection

The digital TV viewer who is at the vicinity of a digital receiver should be able to opt for Pay-TV services as and when he wants. Thus, the standardised set-top box shall be featured with interactive menus to enable the viewer to bind his mobile phone to the set-top box and subscribe to available Pay-TV services. The viewer's mobile phone plays an important role to access to the MICAS services.

Table 3 describes the Set-up Connection use case in details.

Table 3: The Set-up Connection use case

Use case name	*Set-up Connection*
Participating actor:	Initiated by a TV viewer;
Flow of events:	1. The viewer turns Bluetooth radio on in his set-top box and mobile phone; 2. The set-top box provides an interactive window to the viewer on the TV screen to configure the Bluetooth and starts discovering nearby Bluetooth devices; 3. The set-top box then lists the detected Bluetooth-devices and prompting the viewer to select his mobile phone; 4. The set-top box attempts to connect to the selected

	device and discover its services (i.e. file transfer service); 5. For security reason , both mobile phone and set-top box may authenticate each other for instance using a PIN number; 6. The set-top box then requires the mobile phone to fulfil the pairing sequence; 7. Once the viewer's mobile phone is registered as a paired device, next time, the set-top box will automatically connect to the mobile phone without checking the security phrases, if its Bluetooth is on;
Entry Condition:	1. The viewer opts for Pay-TV services; 2. The set-top box is a MICAS approved receiver 3. The set-top box and mobile phone both have Bluetooth connectivity feature offering file transfer service;
Exit Condition:	1. The viewer disables the Bluetooth radio from either sides ; 2. The viewer can disconnect the link from either side; 3. The viewer's mobile phone and set-top box are beyond the Bluetooth coverage area (i.e. over 10m distance);
Quality Requirements:	1. The interaction windows shall be informative and be presented quickly within one second after the viewer demands; 2. The Bluetooth discovery task should be accomplished not more than 30 seconds;

Fig. 24 presents the Unified Modelling Language (UML) use case diagram for the Set-up Connection use case.

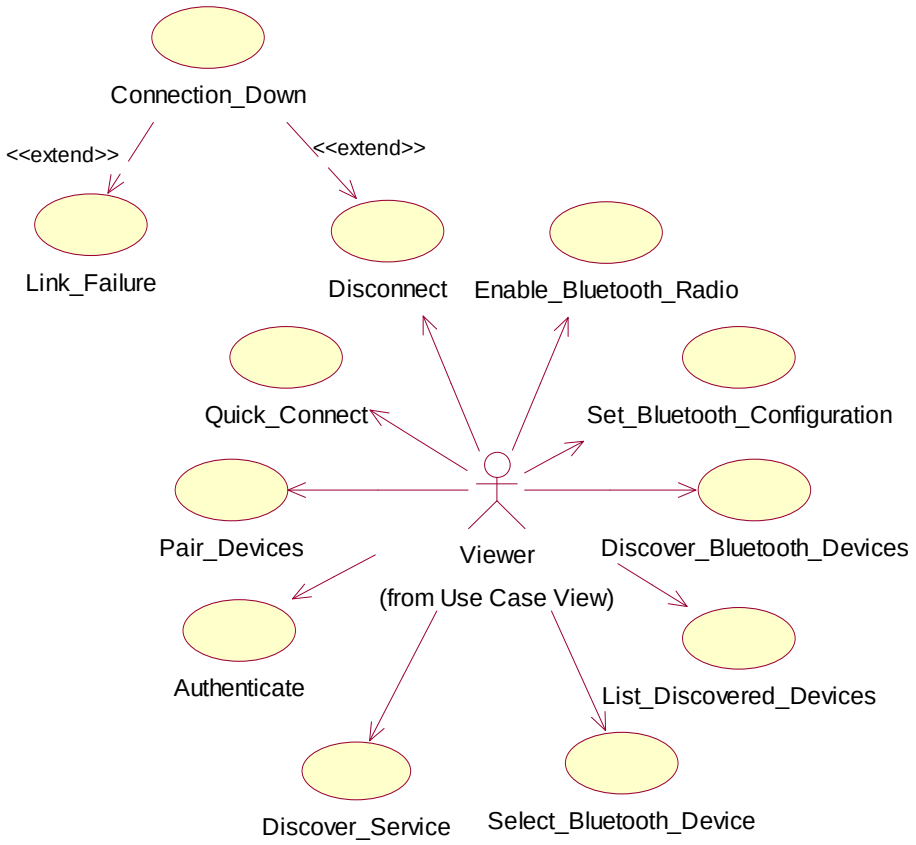


Fig. 24: The Set-up Connection use case diagram

The level of the security adopted by Bluetooth manager in the set-top box and mobile phone can vary from PIN authentication method to rather complicated session-based authentication and encryption methods.

The Disconnect and Link_Failure use cases are extended from Connection_Down use case. The Disconnect use case enables the viewer to disable the Bluetooth radio at the set-top box (or mobile phone). The Link_Failure handles all the connection exceptions raised for instance due to the bad reception.

The described use cases may be initiated from set-top box. Nevertheless, both sides – set-top box and mobile phone - shall be capable of driving the Bluetooth adapter.

6.4.4.2 Sign-up

The viewer should be able to sign-up for Pay-TV services (i.e. subscriber TV, pay-per-view) through an arbitrary set-top box as and when he desires. A viewer can purchase a range of services whose suppliers are different. Thanks to the MICAS architecture, multiple service providers can co-exist at both the transmitter (like DVB Simulcrypt protocol) and the receiver sides (like DVB Multicrypt protocol) and yet, each supplier can deploy its own proprietary access control system.

The first step to enjoy Pay-TV services is to sign-up for a service. The set-top box shall display the list of discovered TV services (i.e. Electronic Service Guide) for the viewer and enable the viewer to browse and select them via the sign-up wizard. After the set-up process, the viewer can place his order by following the wizard. Similar to the conventional registered delivery, a unique identity shall be used to identify and authenticate the recipient in the Pay-TV system.

Table 4 details the Sign-up use case identifying the participant actor(s) and describing the sequence of interactions of the use case.

Table 4: The Sign-up use case

Use case name	*Sign-up*
Participating actor:	Initiated by a TV viewer and communicates with Pay-TV service provider;
Flow of events	1. The viewer selects the sign-up service by for instance pressing the 'Service' button on the set-top box remote control and selecting the 'Sign-up' from the menu; 2. The set-top box compiles off-air electronic programme/service guide (EPG/ESG) and displays available services (i.e. subscriber TV, pay-per-view, pay-per-time) to be selected by the viewer; 3. The viewer can cancel the operation at any time by pressing for instance 'Exit' button on the set-top box

	remote control; 4. After selecting a service, the set-top box presents available packages to the viewer (i.e. programmes or channels); 5. After selecting a package, the set-top box presents a window to the viewer to set-up the period of the contract (i.e. from a few hours to one year depending on the requested service and package); 6. After setting up the period of the contract, the set-top box presents additional preferences to the viewer including the local control preference (i.e. parental control, family package, personal choice), the multi-room subscription (i.e. register another receiver) and Follow Me service; 7. The set-top box then requires the viewer to enter his details (i.e. first name, last name, address, username, password and a memorable phrase) and specify the payment method in a window using the remote control keys or set-top box emulated key-board; 8. The viewer can revise the order at any time for instance by selecting the 'Order Preview' option using the set-top box remote control; 9. The se-top box presents a window asking the viewer if he wishes to receive local advertisements and, if so, how often (i.e. daily, weekly or on event basis); 10. The set-top box then presents 'terms and conditions' corresponding to the viewer's order; 11. If the viewer accepts the conditions, the set-top box then registers the viewer's mobile phone by acquiring its IMSI or IMEI numbers over Bluetooth connection (i.e. the number of mobile phones that can be registered under one account may vary upon the viewer's or service provider's preference); 12. The set-top box then attaches its identity number (STB-

	ID) to the order and then digitally signs the order; 13. The set-top box sends the order to the service operator through the viewer's mobile phone for instance using the SMS protocol; 14. The service provider verifies the order, manages the viewer's account and update/create corresponding billing statements;
Entry Condition	1. Performing the Set-up Connection process; 2. The set-top box shall be able to process the ESG/EPG; 3. The viewer opts for Pay-TV services;
Exit Condition	1. The viewer presses the 'Cancel' button on the set-top box remote control; 2. The viewer submits the subscription request;
Quality Requirements	1. The ESG/EPG shall be continuously broadcast and updated regularly at least in daily basis; 2. The set-top box shall present the most updated service information received off-air; 3. The set-top box shall operate very smoothly and respond quickly to any viewer's request; 4. The set-top box shall save the viewer's preferences as he progresses in sign-up wizard; 5. The sign-up wizard shall enable the viewer to revise the selected options any time before placing the order; 6. The service provider shall respond to the 'Subscriber TV' request by maximum 30 minutes; 7. The service provider shall respond to the 'Pay-Per-View' request including 'advance purchase', 'impulse request' at least 10 minutes prior to the ordered event;

Fig. 25 present the UML Use Case diagram for the Sign-up use case.

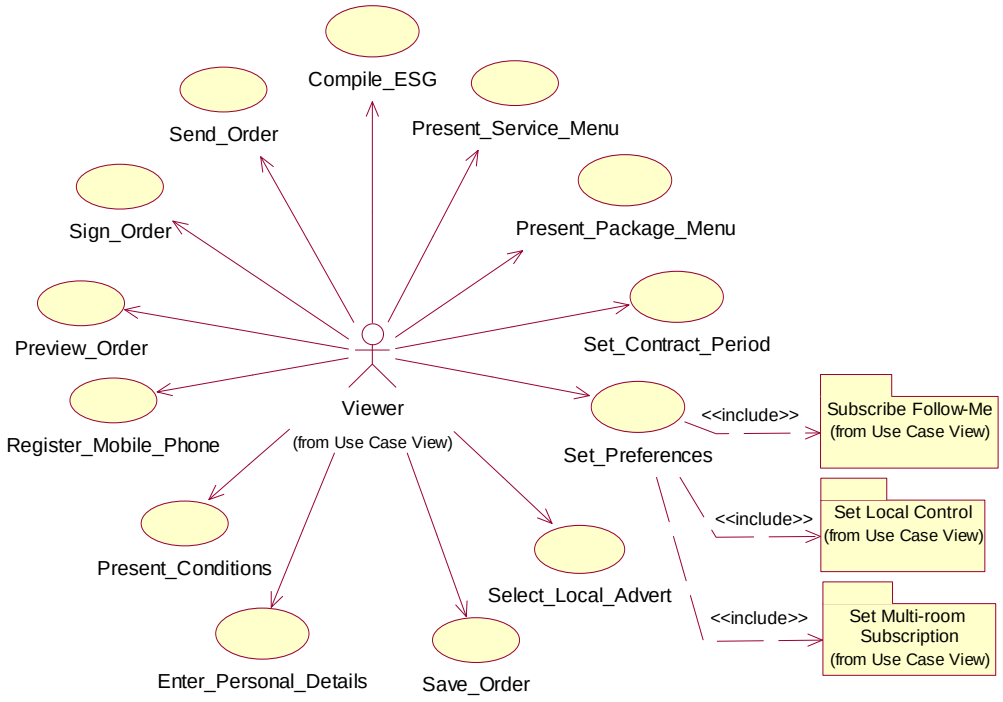


Fig. 25: The Sign-up use case diagram

6.4.4.3 Set Local Control

The local control option will enable the viewer to control the access to programmes. The viewer may consider his criteria to filter some channels (programmes) which are unsuitable for the rest of the family (i.e. children). For instance, some parents may consider to not allowing the children to watch any movies after a certain time.

The local control preferences can be set (reset) during or after the subscription process. The local control preferences can be set in two following levels.

- '*Rating-based Control*': complies with the motion picture rating system. The motion picture rating system categorizes a film with regard to suitability for audiences in terms of issues such as sex, violence, substance abuse, profanity, impudence or other types of mature content. A particular issued rating is called a certification. This helps parents decide whether a

movie is suitable for their children. Different countries have adopted different rating systems. In the UK, the British Board of Film Classification (BBFC) rates both motion pictures and videos. The local authorities are responsible for accepting and enforcing the BBFC's recommended ratings for cinema showings, whereas those for videos are legally binding. The current BBFC system certifies the programmes as 'Uc (Universal - Children)': suitable for pre-school children; 'U (Universal)': suitable for audiences aged 4 years and over; 'PG (Parental Guidance)': general viewing but might be harmful to a sensitive child aged around 8 or older; '12 or 12A (12 Accompanied/Advisory)': suitable for 12 years and over; '15': suitable only for 15 years and over; '18': suitable only for adults; 'R18 (Restricted 18)': to be shown only in specially licensed cinemas, or supplied only in licensed sex shops and to adults of not less than 18 years;

- '*Service-based Control*': allows the viewer to set a password on the purchased services (channels or programmes) based on the personal or family criteria. In this case, when the viewer orders a service, he shall specify whether the service is authorised for social viewing (all family members) or whether it is a personal choice protected for instance by a password (i.e. PIN number).

Table 5 describes the details of the Local Control use case.

Table 5: The Set Local Control use case

Use case name	*Set Local Control*
Participating actor:	Initiated by a TV viewer;
Flow of events:	1. The viewer selects the 'Local Control' preference option in the 'Service' menu; 2. The viewer selects the 'Preferences'; 3. The set-top box presents local control, Follow Me and

	multi-room preferences; 4. The viewer selects the local control menu; 5. The set-top box presents the control options; the Rating-based Control or Service-based Control; 6. The viewer is asked to enter a security (PIN) number to block programmes, if Rating-based Control option is selected; 7. The viewer is asked to tag each ordered service as Personal or Family categories. The control can be applied through a security (PIN) number; 8. The viewer may select both options; in this case the Service-based Control will be in force when a service personalised; 9. The viewer confirms the set-up; 10. The set-top box saves the control preferences and enforces the setting;
Entry Condition:	Performing the Sign-up use case prior to set the Service-based Control;
Exit Condition:	1. The viewer sets the control options and saves the setting; 2. The viewer presses the 'Cancel' or 'Exit' button in the set-top box remote control at any time;
Quality Requirements:	1. The set-top box needs to provide the viewer with a standard GUI to set the local control preferences; 2. The set-top box needs to apply local control preferences once the viewer confirms the setting; 3. The set-top box needs to save the settings and allow the authorised viewer change them as and when it is called; 4. The set-top box needs to protect the setting using the selected PIN code; 5. The set-top box may send the preferences to the service provider through the interactive channel;

Fig. 26 presents the UML Use case diagram for the Set Local Control use case.

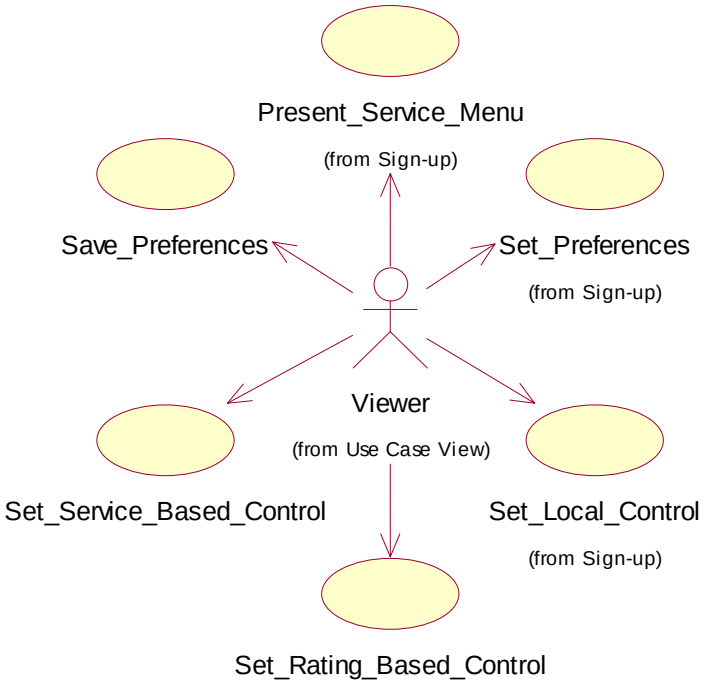


Fig. 26: The Set Local Control use case diagram

6.4.4.4 Subscribe to Multi-room Service

The viewer may subscribe to the multi-room service and watch TV programmes through multiple TV receivers (personalisation concept). In this case, the viewer has to choose one of his set-top boxes as a server and initiate the Sign-up process. The viewer then needs to physically connect (i.e. through USB or Serial interface or Bluetooth in the piconet topology) and register the rest of his set-top boxes (as clients) with the server. Once all the set-top boxes are registered, the viewer may place the order.

The multi-room subscription wizard running in the server will allow the viewer to register a set-top box (i.e. client) with the server. In the wizard, the viewer is asked to specify the port to which the client receiver has been connected. The server then starts searching for the connected device. Once the

viewer confirms the device, the server retrieves the Client Identifier (Client-ID) and saves it into an internal tamper-resistant memory type device (i.e. flash memory) for future use. Once the process is accomplished, the Server will present the outcome of the process and prompts the viewer if he wishes to register another receiver. A similar procedure is repeated to register a certain number of set-top boxes (i.e. up to 7 clients in the Bluetooth mode). At the end, the list of Clients will be shown to the viewer and enclosed to the viewer's order to keep the service provider updated about the receiver side configuration.

To prevent piracy, the server might use the Client-ID and a security function to generate a key to encode TV streams and/or security data exchanged between the server and each client. It is also possible to utilise the viewer's mobile phone to grant the clients with appropriate key information provided by the service provider for decoding the contents. All in all, sufficient Digital Right Management (DRM) techniques need to be carefully adopted by service providers and set-top box producers to secure contents in the said Client-Server configuration. Notwithstanding, the DRM consideration and multi-room topology variations are out of the scope of this project. Table 6 details the Multi-room Subscription use case.

Table 6: The Multi-room Subscription use case

Use case name	*Multi-room Subscription*
Participating actor:	Initiated by a TV viewer;
Flow of events:	1. The viewer selects the 'Local Control' preference option in the 'Service' menu; 2. The viewer selects the 'Preferences'; 3. The set-top box presents 'Local Control', 'Follow Me' and 'Multi-room' preferences; 4. The viewer selects the 'Multi-room' subscription menu; 5. The set-top box launches the subscription wizard;

	6. The set-top box (server) prompts the viewer to connect another set-top box (client) for instance to its serial port; 7. The viewer confirms the message for instance by pressing the 'OK' button in the set-top box remote control; 8. The set-top box start searching for the connected client set-top box; 9. The set-top box presents the search result to the viewer; 10. The viewer confirms the result and goes to the next stage or run the search again in case of receiving an unexpected result; 11. When the search result is confirmed, the set-top box retrieves the client identifier (Client-ID) and shows a successful message to the viewer; 12. If the Server fails to retrieve the Client-ID, an error message is came up prompting the user to either connect an MICAS approved set-top box or instruct the Server to try again; 13. When the viewer confirms the message, the set-top box saves the Client-ID in a secure memory; 14. The set-top box prompts the viewer whether there is another set-top box to be registered as a client - procedures numbered from 4 to 14 can be repeated for a certain number of time; 15. The set-top box presents the list of Clients connected to the Server and prepares the viewer's order to be submitted, as explained in the Sign-up use case;
Entry Condition:	1. The viewer needs to perform the Set-up Connection process; 2. The viewer needs to perform the Sign-up use case;
Exit Condition:	1. The viewer successfully submits the multi-room subscription request; 2. The viewer may cancel the order by pressing the

Quality Requirements:	'Cancel' or 'Exit' button in the set-top box remote control at any time before finalising the order; 1. The set-top box shall provide the viewer with an easy-to-use subscription wizard to register his set-top boxes; 2. The set-top box needs to effectively interact with the viewer at any stage of subscription process; 3. The identifiers of the client set-top boxes need to be securely saved within the server set-top box;

Fig. 27 presents the UML Use case diagram for the Multi-room Subscription use case.

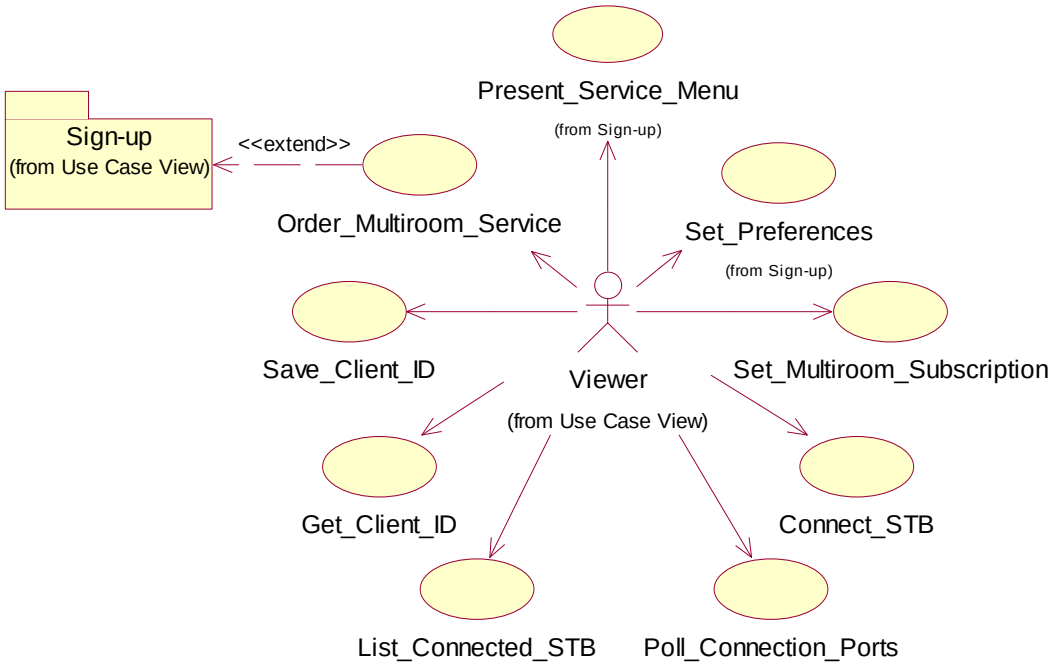


Fig. 27: The Multi-room Subscription use case diagram

The Order_Multiroom_Service is instantiated from the Sign-up use case. Thus, the service provider will validate the order and if it is appropriate, he will amend the viewer's subscription and update the billing statement accordingly.

6.4.4.5 Subscribe to Follow Me Service

The implementation of a downloadable conditional access system (DCAS) [65] together with utilising mobile technologies allow the Pay-TV service provider to offer his subscriber(s) ubiquitous access to TV contents. This phenomenon would push the boundary in the Pay-TV system to support the 'Anything, Anytime and Anywhere' paradigm. This model is expected to be demanded mostly by the viewers who spend most of their time in travelling and tend to have the habit of targeted viewing (i.e. sport or news programmes). This service, called herein as the 'Follow Me' service, enables the viewer to access to contents based on his subscription profile via an arbitrary set-top box located within the service provider's service coverage area.

The viewer can sign up for the Follow Me service through an arbitrary set-top box connected to a viewer's registered mobile phone for instance through the Bluetooth connection. The set-top box needs to be equipped with pre-defined service menus and a wizard to allow the viewer to request for the Follow Me service. The set-top box generates the Follow Me activation message upon the viewer's request and then sends the message to the service provider through the viewer's mobile phone. The message shall specify the viewer's demand for a temporary access arrangement. In addition, it shall bear sufficient information to enable the service provider to identify the viewer, set-top box and the CASS already deployed in his mobile phone. The GSM unique identifiers (i.e. IMSI and IMEI numbers) and set-top box identity (STB-ID) can be respectively used to identify the viewer, his mobile phone and the set-top box. The service provider can then enquire the viewer's account to learn more about the deployed security subsystem associated to the viewer. After all, the service provider shall set the security requirements and supply the viewer with a temporary CASS (security keys and APIs) to enable his set-top box to decode the paid contents. For security

reasons, the CASS shall be working for a short while, although the viewer may request to extend it with an extra payment.

Table 7 details the Follow Me service use case.

Table 7: The Follow Me service use case

Use case name	*Follow Me Service*
Participating actor:	Initiated by a TV viewer and communicates with the service provider;
Flow of events:	1. The viewer selects the service menu of the set-top box and opts for the 'Follow Me' service; 2. The viewer will be then prompted to either 'Cancel' or 'Activate' the service; 3. If the viewer opts for 'Activate' option, the set-top box starts generating the Follow Me activation message; 4. It connects to the viewer's mobile phone for instance through the Bluetooth connection and retrieves the IMSI and/or IMEI numbers; Note that the security functions in the viewer's mobile phone may exchange unique numbers associated to the viewer and recognisable by the service provider instead of exposing the actual IMSI or IMEI numbers. These numbers can be regarded to the session held for that particular time and request; 5. It extracts the STB-ID or its representative number; 6. It then generates the Follow Me activation message; 7. If the message is successfully generated, the set-top box prompts the viewer to confirm the request; 8. Then, the set-top box signs the message and sends it to the mobile phone; 9. In the mobile phone, the message might be digitally re-signed and then sent to the service provider for instance over SMS bearer; 10. The service provider verifies the order, updates the viewer's account and deploy a temporary access control

	solution; 11. If the viewer decides to leave earlier, he shall cancel the service by selecting the 'Cancel' option under the 'Follow Me' menu; 12. Upon cancellation, the Follow Me cancellation message is then sent to the service provider and the CASS will self-destruct;
Entry Condition:	1. The viewer needs to perform the Set-up Connection process; 2. The viewer needs to perform the Sign-up process; 3. The viewer's mobile phone needs to be pre-registered with the service provider;
Exit Condition:	1. The Activation message is successfully generated and sent to the service provider; 2. The viewer may cancel the order by pressing the 'Cancel' or 'Exit' button in the set-top box remote control at any time before submitting the order; 3. The viewer may cancel the service by selecting the 'Cancel' option under the 'Follow Me' menu;
Quality Requirements:	1. The set-top box needs to provide the viewer with an easy-to-use subscription wizard to activate and cancel the Follow Me service; 2. The set-top box needs to effectively interact with the viewer at any stage of subscription process; 3. The temporary CASS shall self-disable for security purposes; 4. The viewer will be allowed to enjoy his subscription for instance for a period of one day, then the access permission will be expired;

Fig. 28 presents the UML Use case diagram for the Follow Me service use case.

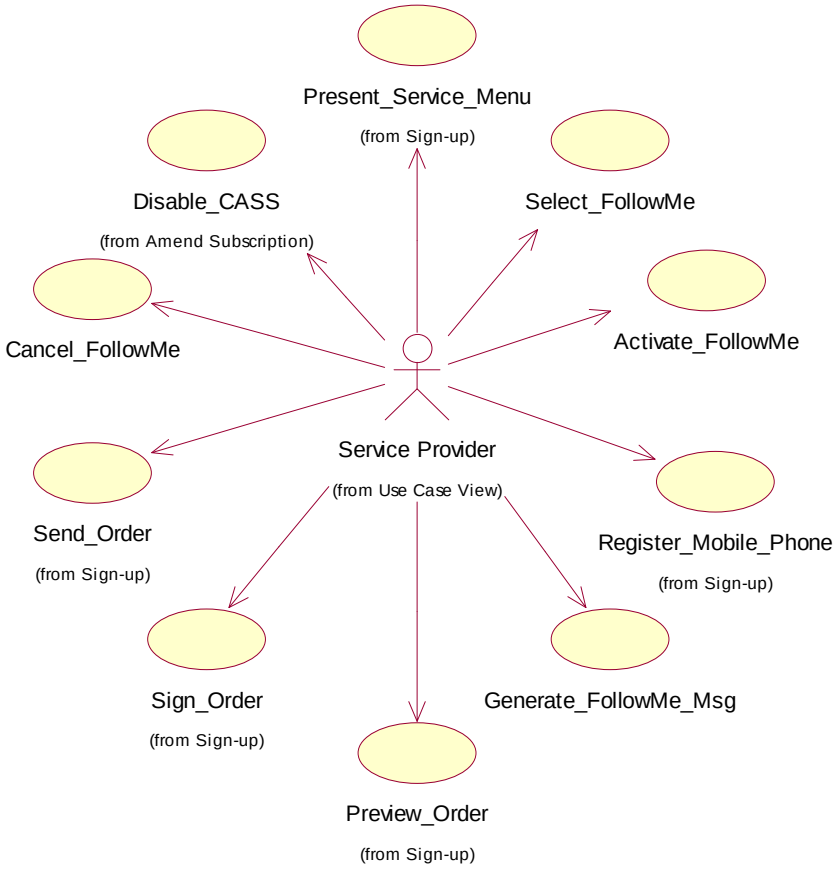


Fig. 28: The Follow Me service subscription use case diagram

6.4.4.6 Amend Subscription

Once a viewer has subscribed to a service, the service provider will deploy his conditional access system and consequently grant him with proper key information to access to the paid contents. The viewer may be allowed to amend or cancel his subscription profile, subject to the terms and conditions stipulated by the service provider.

When a viewer applies for amendment or cancellation of his subscription, the security applications installed in the viewer's mobile phone and/or set-top box will transit to the suspension state, waiting for the service provider's command to function. In case of amendment, the service provider may penalise the viewer,

update the viewer's subscription profile and send the new key information to the viewer. If the viewer cancels the policy, the service provider may penalise the viewer for leaving the contract early. It is followed by disabling the viewer's associated conditional access subsystem by sending a deactivation code to the viewer's mobile phone and/or set-top box. The security applications installed in the viewer's mobile phone or set-top box will for instance self-destruct after compiling the code.

The amendment process shall be pursued in the so-called server set-top box, albeit it might be possible for the viewer to amend his subscription via an arbitrary set-top box. In this case, the set-top box shall send a request to the service provider to get and display the viewer's subscription profile.

Table 8 details all the necessary actions need to be taken in order for the viewer to amend or cancel his subscription.

Table 8: The Amend Subscription use case

Use case name	*Amend Subscription*
Participating actor:	Initiated by a Pay-TV viewer and communicates with a Pay-TV service provider;
Flow of events:	1. The viewer selects the 'Service' menu and then 'Amend Subscription' option in his so-called server set-top box; 2. The set-top box brings up the terms and conditions prior to apply any changes in the subscription; 3. If the viewer agrees upon the conditions and wishes to pursue the amendment, the set-top box presents two options for the viewer: Cancellation and Amendment; 4. If the viewer opts for the 'Cancellation', a new message will prompt the viewer confirming the action; 4.1. If the viewer confirms the cancellation warning message, the Cancellation code will be generated; 4.2. The set-top box then opens a link to the viewer's mobile phone and sends the code across;

	4.3. The code is digitally signed in the viewer's mobile phone and sent to the service provider for instance using the GSM SMS bearer; 4.4. Upon transferring the code to the service provider, the deployed conditional access mechanism in the viewer's set-top box and mobile phone will be halted till receiving further control signal from the service provider; 4.5. The service provider verifies the request, updates the viewer's account and billing statements; 4.6. The service provider then sends an Acknowledgment code to the viewer's mobile phone; 4.7. The mobile phone compiles and executes the code to disable the deployed conditional access subsystem in the mobile phone and set-top box; 5. If the viewer selects the 'Amendment' option, a new message will pop-up in the TV screen prompting the viewer to confirm the action; 5.1. If the viewer confirms the amendment warning message, the viewer's subscription saved in the Server set-top box will be presented in the next screen; 5.2. The viewer is asked whether he confirms the subscription. Otherwise, the set-top box will send a message to the service provider through viewer's mobile phone to download the latest subscription profile (i.e. an updated EMM message); 5.3. The set-top box compiles the subscription message and lists the subscribed services enabling the viewer to amend the policy associated with each subscribed service (i.e. cancel or change the subscription period); 5.4. The set-top box also enables the viewer to add new

	services to his subscription that leads the viewer to the Sign-up use case; 5.5. Having done the amendment, the set-top box enables the viewer to preview the revised subscription and prompts the viewer to either confirm the changes or cancel the operation; 5.6. Having confirmed the new changes, the set-top box halts the conditional access subsystem and sends the revised subscription message to the viewer's mobile phone; 5.7. The message is then compiled and signed in the mobile phone; 5.8. The conditional access subsystem located in the mobile phone is also halted till receiving further notice from the service provider; 5.9. The signed message is sent to the service provider for instance through GSM SMS bearer; 5.10. The service provider compiles the message and identifies the subscriber; 5.11. Based on the policy, the service provider updates the subscriber's profile and bill statement; 5.12. The service provider then sends the Acknowledgement message (i.e. new EMM message) to the viewer's mobile phone and/or set-top box to decode the contents accordingly;
Entry Condition:	The viewer has to place an order through the Sign-up use case;
Exit Condition:	1. The viewer may successfully cancel his subscription; 2. The viewer may successfully amend his subscription; 3. The viewer may cancel the operation any time before submitting the request by pressing the 'Exit' or 'Cancel' button in the set-top box remote control;
Quality	1. The user interface implemented in the set-top box for

Requirements:	local interactivity shall be simple, comprehensive and instructive to enable a normal TV viewer to readily place his request; 2. Whilst the set-top box is waiting to receive the service provider's code, the viewer should be able to enjoy at least the Free-view programmes;

Fig. 29 presents the UML Use Case diagram concerning the receiver side functionalities for Amend Subscription use case. The operator side functionalities are similar to the Sign-up use case presented in Fig. 25.

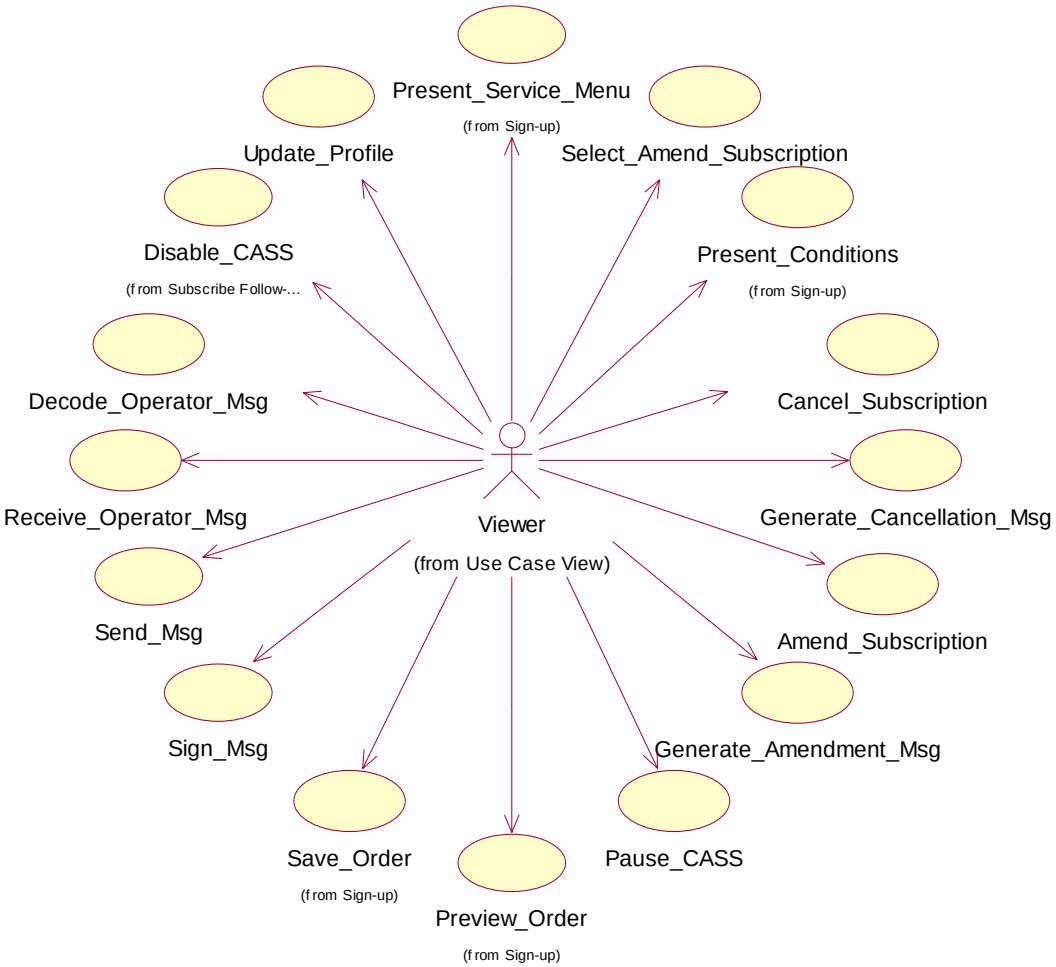


Fig. 29: The Amend Subscription use case diagram

6.4.4.7 Order Management

In today's business climate, the order management is crucial to corporate success as the demand for perfection increases and flexibility and tolerance for errors decreases. Superior order management can provide a competitive edge across the board for improving business performance as well as customer satisfaction and retention. Thus it is very important to consider an automatic order management subsystem in the MICAS platform.

In the MICAS, when the service provider receives a viewer's subscription request, he first decodes the message and fulfils the validation process. The service provider shall recognise the viewer using his unique ID (i.e. IMSI and IMEI number). His set-top box can be recognised by its unique ID (i.e. STB-ID or STB address, which can be assigned to the set-top box by its producer).

The service provider may crosscheck the validity of IMSI number, IMEI number and STB-ID with a central database, which can be developed by various parties like Pay-TV service providers, mobile phone operators and set-top box producers. The central database can be managed by a trusted third party. It can provide the service providers with customers' history records (i.e. customer payment history, customer criminal history, etc.) and valid set-top box and GSM identities deployed in the field. The customer history record aids the service provider to validate the viewer's request, calculate viewer's risk factor and appreciate viewer's needs (i.e. Know-Your-Customer rule).

In the MICAS, the order management is an intricate and automatic process subject to the successful validation of the order and involved entities (i.e. viewer, mobile phone and set-top box). The service provider will create or update the viewer's account wherein all the information concerning the viewer is saved. In addition, the viewer's billing statement will be issued on the basis of his order and service provider's tariff. If banking transactions are authorised successfully,

the service provider will process the viewer's order and take appropriate action to satisfy the viewer's order. If it is needed, the service provider will tailor his conditional access system too. The service provider shall keep the viewer advised of his order progress at any stage of the process.

Table 9 details the Order Management use case.

Table 9: The Order Management use case

Use case name	*Order Management*
Participating actor	Initiated by the Pay-TV service provider;
Flow of events	1. The service provider receives the viewer's request (order) through the GSM interface; 2. The service provider confirms the receipt of the message by sending back the Acknowledgement message; 3. The service provider decodes the subscription request; 4. The service provider validates the viewer, set-top box and order; 5. The service provider sends the order status to the viewer via the SMS protocol; 6. The service provider then generates/updates the viewer's account, processes the billing statements and starting deploying the conditional access system;
Entry Condition	A viewer sends a request (order) to the Pay-TV service provider;
Exit Condition	1. The service provider receives a cancellation request right after receiving the order; 2. The validation process fails;
Quality Requirements	1. The service provider shall send the Acknowledgment message right after receiving the order; 2. The service provider shall respond to the order within the contracted period (i.e. maximum one hour after receiving the order);

	3. For security reasons, the service provider may consider to send a confirmation letter to the viewer's address; 4. The service provider shall set up a dedicated telephone line or email address to respond to any viewer's query/complaint; 5. The service provider shall set up a support line for pre/post sale services;

Fig. 30 presents the UML Use Case diagram for the Order Management use case.

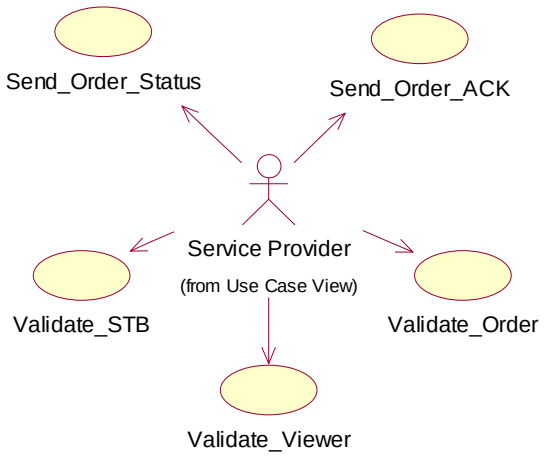


Fig. 30: The Order Management use case diagram

6.4.4.8 Subscriber Account Management

Managing of the subscribers' account is critical for customer based businesses such as Pay-TV. In the conditional access system implemented in DVB project, the Subscriber Management Subsystem (SMSS) is responsible for managing subscribers' information. The SMSS usually includes a user interface and a series of functions to enable the operator to administrate the subscribers' account saved in a repository such as an Oracle or SQL database. The SMSS may offer added-valued features such as remote account management, or being compatible with

various platforms or backing-up the data automatically at specified time intervals.

The MICAS will remain compatible with the traditional Pay-TV systems while mitigating the overall responsibilities of the operator and improving the information management system. In the MICAS, the Information System (IS) is semi-automatic as a great part of the viewer-related data is acquired through the GSM interface. Other parts are developed as the viewer builds up his history in the system. The viewer's data shall consist of viewer's personal details (i.e. full name, address and bank account information), GSM identity (i.e. IMSI and IMEI), STB-ID, subscription, preferences, payment history, etc. The data saved in the viewer's account will be used by the service provider for security, finance and marketing purposes.

Table 10 details some aspects of the Subscriber Account Management use case.

Table 10: The Subscriber Account Management use case

Use case name	*Subscriber Account Management*
Participating actor:	Initiated a Pay-TV service provider;
Flow of events	1. The service provider enquiries the subscriber account database about a specific viewer; 2. The service provider may just read through the saved records in the database; 3. If it turns out that the viewer is an existing customer, the service provider updates the account: 2.a. The service provider may read or write on a specific account in the database; 2.b. The service provider may perform update, delete or other commands on the database; 4. Otherwise, the service provider creates an account in the database;

	5. The service provider may block reading and/or writing on the database for anyone or a group of users; 6. The service provider may share the database with a group of users (internal or external sources); 7. To speed up transactions (i.e. search) on the database, the service provider may index the subscribers' account in the database;
Entry Condition	The service provider shall perform the Order Management use case;
Exit Condition	1. The service provider cancels the operations; 2. The service provider performs the database transaction successfully;
Quality Requirements	1. The subscribers' account database needs to be indexed and normalised with minimum redundancy; 2. The transactions need to be done quickly and securely; 3. The required channel(s) to exchange data with the database needs to be allocated on demand and released as soon as the job is done; 4. The access to the database shall be solely granted for authorised users;

Fig. 31 presents the UML Use Case diagram for the Subscriber Account Management use case.

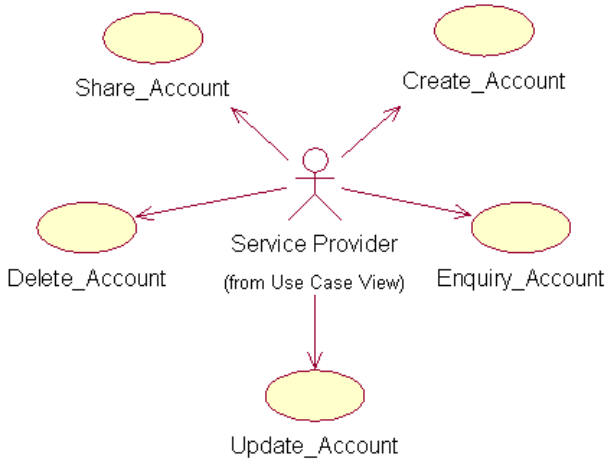


Fig. 31: The Account Management use case diagram

6.4.4.9 Billing Process

The heart of the financial activities in the Pay-TV system is processing and issuing invoices or bills for every individual subscriber based on their subscription and outstanding requests (orders). Each service provider has to provide the viewer with a tariff presenting his available services and corresponding subscription fees. The services may vary from subscription services, pay-per-view, video-on-demand, near-video-on-demand, multi-room subscription, Follow Me services etc. As mentioned earlier, once the viewer sends his order, the service provider dedicates an account to the viewer wherein the viewer's personal information, bank account and order (subscription profile) are saved. The service provider issues the bill based on of the viewer's subscription profile and contracted tariff. The bill is usually issued prior to the service and if there is any change of fee, the service provider shall inform the viewer in advance. When the viewer pays the fee, the service provider and viewer are legally bound. At this point, the service provider shall grant the viewer with proper key to access the service with the quality contracted in the Service Level Agreement (SLA) and Service Level Specification (SLS).

The statement itself or statement notification shall be sent to the viewer either electronically or paper-based, for instance, on monthly basis. This would help the viewer tracking TV corresponding transactions on his bank account. The service provider may facilitate various ways for the viewer to pay and manage his bills for instance through the phone or internet. The viewer can log in to his on-line account within the service provider's website and set-up various ways of payment (i.e. direct debit, credit card, sending cheque or postal order). In the MICAS, the viewer can also set-up the payment method while signing up for the service through the set-top box. At any stage, if the payment fails, the service

provider shall warn the viewer to settle the payment in a certain period of time before stopping the service.

Table 11 details the Bill Processing use case.

Table 11: The Bill Processing use case

Use case name	*Billing Process*
Participating actor:	Initiated by a Pay-TV service provider;
Flow of events	1. The service provider compiles the viewer's order; 2. The service provider saves the viewer's order in the viewer's account; 3. The service provider generates the viewer's bill based on his tariff and viewer's order; 4. The service provider sends the bill or a notification to the viewer's address; 5. The service provider refers to the viewer's account to acquire viewer's banking information; 6. The service provider charges the viewer according to the issued bill; 7. If the viewer's bank authorises the payment, the service provider continues to serve the viewer; 8. Otherwise, the service provider flags the viewer's account for the bad payment and sends a warning to the viewer; ultimately the service can be stopped, if the subscription fee is not received within a specific period of time;
Entry Condition	1. The service provider shall perform the Account Management use case; 2. The service provider shall perform the Order Management use case;
Exit Condition	1. The viewer withdraws the order; 2. The service provider cancels the service; 3. The subscription fee is not received; 4. The fee is paid utterly;

Quality Requirements	1. The bill shall be issued transparently based on the contract; 2. The bill shall be delivered to the viewer regularly; 3. The record of payment shall be saved in the viewer's account; 4. The service provider shall set-up a direct line to reply to viewers' concerns or complaints raised upon the bills and/or payment issues;

Fig. 32 shows the UML Use Case diagram for the Billing Process use case.

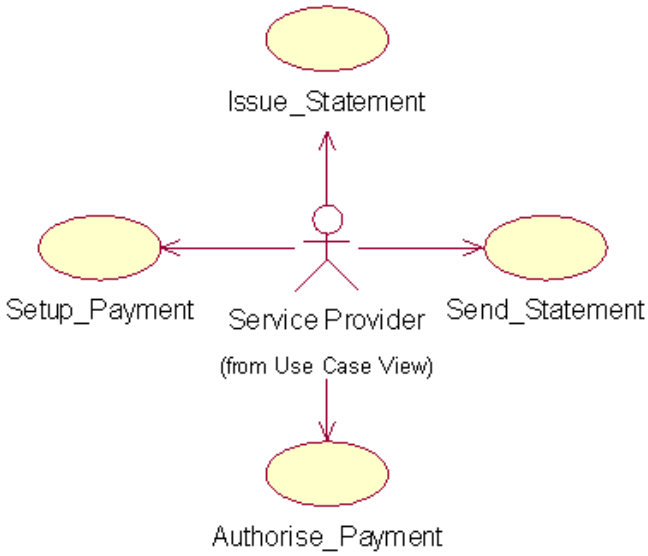


Fig. 32: The Billing Process use case diagram

6.4.4.10 Download CASS

Given that all validation processes on the viewer identity and requested set-top box succeed, the service provider starts deploying his tailored conditional access subsystem in the viewer's SIM card and/or set-top box through the GSM network [100]. The conditional access subsystem (CASS) shall at least consist of cryptographic keys and a series of security software applications (APIs).

The key information sent to the viewer side corresponds to the service provider's control and key hierarchy system. It shall satisfy the confidentiality for any interactions between the viewer and service provider.

The security applications shall satisfy interactivity and security criteria like identification, authentication, integrity and confidentiality for instance using symmetric or asymmetric cryptographic techniques. The security applications may be transferred to the viewer's mobile phone or set-top box through both or either of the broadcasting or GSM communication links. In addition, they may be installed in both or either of the viewer's mobile phone and set-top box depending on the system architecture adopted by the service provider. Nevertheless, there will be common procedures that all service providers need to pursue prior to enforcing their conditional access subsystem.

The service provider needs to decide on how to deploy his conditional access subsystem in the field. If the Pay-TV service provider decides to interact with his subscribers and deploy his conditional access subsystem over the GSM network, a proper commercial agreement between the Pay-TV service provider and mobile phone operator(s) needs to be drawn up. Such an agreement should facilitate provision of convergence services and also certify the service provider to reach his individual subscriber's SIM card (or a secure domain in the mobile phone) over a secure channel in the GSM network [72]. The applications are owned by the service provider and they shall be installed in a specific memory address (domain) pre-allocated in the SIM card (or mobile phone) by the mobile phone operator. The applications need to be certified by the mobile operator; as such, an operator Certificate needs to be transferred to the SIM card to verify the applications prior to installation. The installation of the security applications can take place over the air with or without the viewer intervention.

There are several ways to remotely install applications in the SIM card or in a secure domain in the mobile phone. The SIM Application Toolkit (SAT) ratified as a standard in the GSM enables the mobile phone operator or a certified Pay-TV operator to remotely install, control, monitor and manage over-the-air applications on the SIM card [3]. In addition, the WebSIM, which integrates the GSM SIM into the Internet, enables communications in TCP/IP using HTTP requests. The Internet connectivity of the SIM inside a mobile phone can be achieved by having a proxy host tunnel IP packets to the SIM over SMS [53]. Moreover, a secure data channel can be established between service provider and viewer's SIM card using Java technologies (J2SE, J2EE, J2ME and JavaCard) to securely exchange large volume of data files [72]. In this case, the credential data (i.e. operator domain Certificate and cryptographic keys) shall be saved in the SIM card (tamper resistant device) and security applications shall be installed in the secure operator domains as introduced in the MIDP 2.0 specifications [63]. The security applications shall be checked upon the SIM card resident root Certificate prior to installation. The security applications can access to the security information stored in the SIM card for instance using Java Specification Request (JSR) documents to develop Security and Trust Services APIs (SATSA) [62] in Java platform.

The GSM SMS protocol can be used to exchange credential data between the service provider and viewer. The key information can be used by the security applications to fulfil the authentication, digital signature, decoding and encoding processes. Most of the security processes will be pursued in an obscure manner though in some cases, while and/or after the installation, the viewer might be prompted to take action. In this case, the SAT features can be used to control the man-machine interface, menu management, application control and handle communication services.

Table 12 details the deployment of the Conditional Access Subsystem (CASS) use case when SAT and MIPD 2.0 features are used to install and access data stored in the viewer's SIM card.

Table 12: The Download CASS use case

Use case name	*Download CASS*
Participating actor:	Initiated by a Pay-TV service provider and communicates with viewer;
Flow of events:	1. The service provider checks if the viewer's mobile phone or set-top box are compatible with his CASS; 2. The service provider decides the possible conditional access system architecture (explained later); 3. The service provider generates the cryptographic keys to be transferred to the viewer side; 4. The mobile phone operator generates the operator Certificate; 5. The service provider signs the security applications using the Certificate; 6. The service provider transfers the key information and Certificate to the viewer's mobile phone using the GSM SMS bearer; 7. The service provider transfers the security applications over-the-air to the viewer's mobile phone; 8. The applications are checked upon the Certificate and installed in a pre-allocated operator domain in the mobile phone; 9. The mobile phone shall inform the service provider and viewer of the successful CASS installation;
Entry Condition:	1. The viewer has to place an order as explained in the Sign-up use case; 2. The service provider shall perform Billing process;
Exit Condition:	1. The viewer's mobile phone may be turned off during the CASS deployment;

	2. The GSM communication link may be cut off for instance due to the bad reception; 3. The viewer may cancel the contract explained in the Amend Subscription use case; 4. The service provider successfully deploys the CASS;
Quality Requirements:	1. The deployment should be pursued with minimum involvement of the viewer; 2. Should the CASS locates in the mobile phone SIM card (i.e. JavaCard), the limitation of SIM card has to be considered by the service provider prior to deployment; 3. The size of the security applications shall be proportionate to the memory size available in the limited resource devices like mobile phones; 4. The security application shall not introduce any degradation or interruption to the normal mobile phone operations (i.e. voice or video call); 5. For security reasons, the CASS shall only operate when the mobile phone is in the phone mode attached to the GSM network;

Fig. 33 presents the UML Use Case diagram for the Download CASS use case.

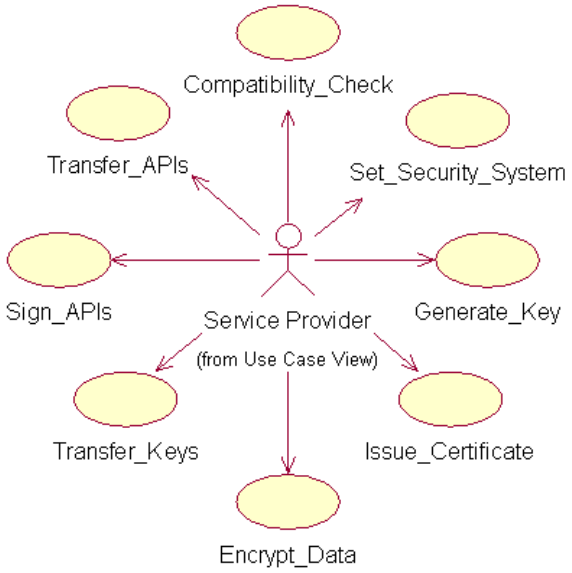


Fig. 33: The Download CASS use case diagram

6.4.4.11 Security Check

The main objective of the design and implementation of the conditional access techniques is to prevent pirates from illegal access to encoded contents. The threat of piracy in the Pay-TV system is now evolving with the growth of the Internet. The black market communities across the globe can now easily collude and share the secret knowledge across in the Internet. One of these sorts of attack is key Sharing attack where the legitimate users collude in a community and provide the key information to the illegitimate users. To tackle the issue, the service provider needs to penetrate to the black market communities (i.e. on-line or in the social places like pubs) and identify the compromised keys to be revoked. Nevertheless, proving that a viewer has breached the contract is not an easy task and requires concrete evidence. As such in most of the cases, the service provider cannot penalise the viewer to compensate part of his security flaw costs. Solutions like monitoring the viewer's contractual behaviour throughout the term of the contract as well as improving the interactivity and security implementation in the system can mitigate the issue.

In the MICAS, the service provider, set-top box producer together with the mobile phone operator can limit the capability of the end-user in terms of accessing, inserting and installing new keys or APIs into the security sensitive domains (SIM card or set-top box). Moreover, the service provider can effectively interact with receiver-end and monitor the viewer's behaviour throughout the contract. To monitor the viewer's contractual behaviour, the service provider needs to deploy a security agent to the viewer's mobile phone and set-top box. The agent can be a software application which guards the protected domains and monitors any piracy at the receiver-end (i.e. mobile phone and set-top box). The agent may reflect the security status at the receiver-end in the value of the security data which are shared between the agents and service provider.

Therefore, the service provider can realise the situation by polling the data from the agent (mobile phone agent). Analysing the security data will also enable the service provider to evaluate the viewer's risk (i.e. user modelling techniques). In addition, the agent may trigger an encoded alarm message in case that the threat is imminent. In this case, the CASS operating in the mobile phone and/or set-top box is automatically halted from operation. The service provider evaluates the situation and may send a formal warning to the viewer and ask for clarification. After logging the situation, the service provider may update the key and re-activate the CASS. If the threat persists, the service provider may ultimately revoke the key and dismiss the viewer for voiding the contract, given that he is in charge of his mobile phone and set-top box (not stolen).

There are many more monitoring techniques available to the service provider to establish whether a user is abusing the system. For instance, in the MICAS, the service provider can always monitor the location of the viewer and identification of the viewer by reading the value of the LAI, IMSI and IMEI numbers saved in the viewer's SIM card. Hence, the service provider can be alerted if the key associated to a specific viewer is also being used in a different area from where the viewer is living or in a different mobile phone that registered under the viewer's account. Albeit no system is utterly safe, but the MICAS can substantially reduce the risk of piracy attack in the Pay-TV system through effective interactions, which enable the service provider to detect the threat and act cost-effectively to destabilise the threat.

Table 13 details the Security Check use case.

Table 13: The Security Check use case

Use case name	*Security Check*
Participating actor:	Initiated by a Pay-TV service provider;

Flow of events	1. The service provider pings the viewer's mobile phone; 2. If the viewer's mobile phone is active, the service provider polls the monitoring data from the viewer's SIM card; 3. The security agent running on the viewer's SIM card or mobile phone will send an encoded alarm message to the service provider in case that the viewer attempts to read/write from/to the operator's domain; 4. The CASS running on the mobile phone and/or set-top box is halted from operation till receiving further notice from the service provider; 5. The service provider decodes and complies the security data; 6. The service provider decodes and compiles the alarm based on the value of the security data; 7. The service provider analyses the data to evaluate if there is any security risk involved; 8. In case of security breach, the service provider logs the alarm in the viewer's account; 9. The service provider may send a warning message to the viewer's mobile phone and update the key; 10. In more serious cases, the service provider may revoke the key(s) and disable the conditional access associated to the viewer;
Entry Condition	Performing the Install CASS use case;
Exit Condition	1. The viewer cancels his subscription or his subscription expires; 2. The service provider interrupts the operation;
Quality Requirements	1. The security monitoring data and alarm messages shall be encrypted/encoded before transmission; 2. The security check operation shall not interrupt or affect other mobile related operations; 3. The viewer's subscription can be de-activated if the

	service provider can not poll the data in a retention period;

Fig. 34 presents the UML Use Case diagram for the Security Check use case;

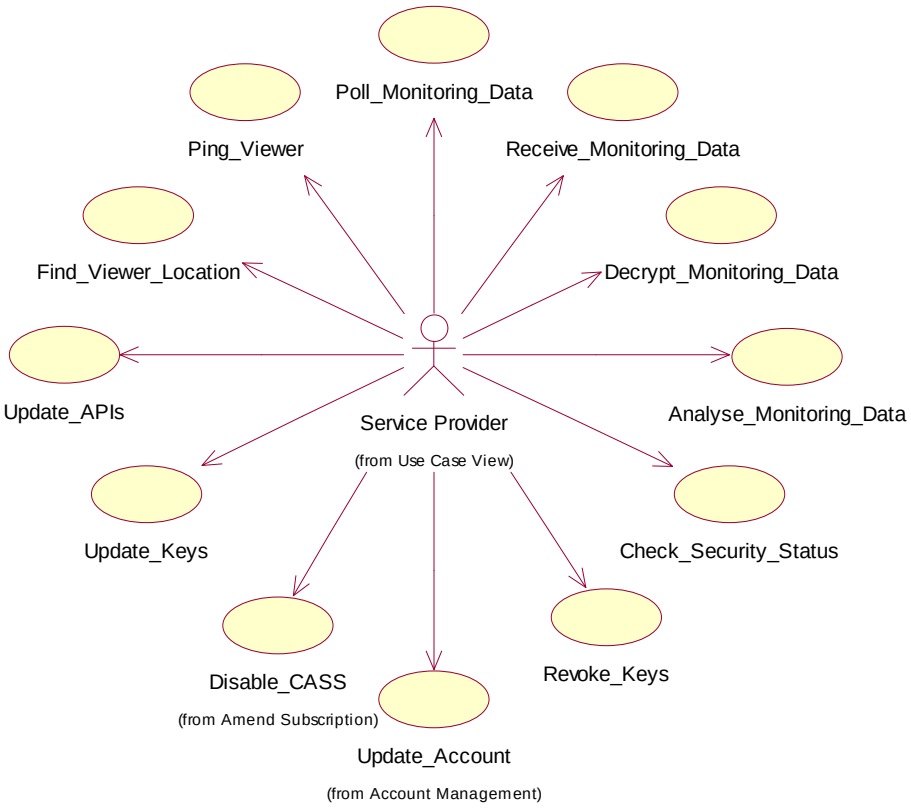


Fig. 34: The Security Check use case diagram

6.4.4.12 Personalised Services and Advertisement

The marketing and sales techniques have evolved in the digital communication arena. Putting on iron-made shoes to stroll across streets and knocking people's door are traditional techniques which are still practiced today. Recently making targeted phone calls to known customers has become more common, although receiving unexpected phone calls from salesmen is not usually welcomed by the public. It is important to recognise that people are more interested in receiving relevant and genuine offers corresponding to their interests and needs. Thus, conducting customer-based researches (i.e. psychological study and modelling

customers' behaviour) to closely understand customers' needs are strongly suggested.

In the Pay-TV system, practicing targeted advertisement and offering personalised services can be readily implemented via considering the viewer's profile. In the MICAS, the sales and marketing can become more intelligent. The service provider can interact with viewers on their mobile phones for instance to gather viewer's preferences. The service provider can process such personalisation information using various individual or social modelling techniques (i.e. cognitive modelling and social interaction) to diversify his services for individuals or group of viewers. The MICAS can even afford the location-based services based on the LAI stored in the viewer's SIM card.

The service provider shall keep the viewer's account updated in terms of viewer's location and preferences. The service provider can develop personalised ESG and send them to the viewer's mobile phone. The service provider may also download a cognitive agent to the viewer's mobile phone to improve the service provider's knowledge regarding the viewer's behaviour. This agent can be implemented as part of the security agent that has been described earlier, but it shall be activated upon the viewer's consent. The viewer can activate the personalised and targeted services while signing up to the contract. The viewer shall be able to cancel the service anytime at his will.

Table 14 details the Advertise Service use case.

Table 14: The Advertise Targeted Services use case.

Use case name	*Advertise Services*
Participating actor:	Initiated by a Pay-TV service provider;
Flow of events	1. The service provider updates the viewer's account on Polling or Interruption bases – in the Polling the service provider calls the cognitive agent to provide the most

	updated personalisation information, while in the Interruption mode the agent sends preference information (i.e. LAI number) automatically as it changes; 2. As receiving the message, the service provider decodes and compiles the message and updates the viewer's account; 3. The service provider categorises the viewer taking into account the viewer's profile and preferences; 4. The service provider generates personalised advertisements (i.e. ESG) based on available services and the viewer's need and interests; 5. The service provider circulates advertisement messages regularly according to the viewer's wish;
Entry Condition	Performing the Sign-up use case and opting for the Targeted Advertisement service;
Exit Condition	1. The viewer may cancel the service by simply sending a text message; 2. The service is automatically cancelled if the viewer's account is deactivated;
Quality Requirements	1. The offered services shall match the viewer's preferences; 2. The information should be presentable in the set-top box; 3. The size of the advertisement messages shall be kept small; 4. The information shall be succinct and preferably in text format unless WAP protocol is used for communication which in this case the set-top box shall be equipped with a web-based content parser or browser; 5. The viewer shall be able to cancel the service in a simple and cost-free way like sending a 'stop' text message to a free number;

	6. The viewer's preferences should be kept at the head-end and readily accessible so when the viewer's mobile is stolen, the viewer can still enjoy from the service;

Fig. 35 presents the UML Use Case diagram for the Advertise Targeted Services use case.

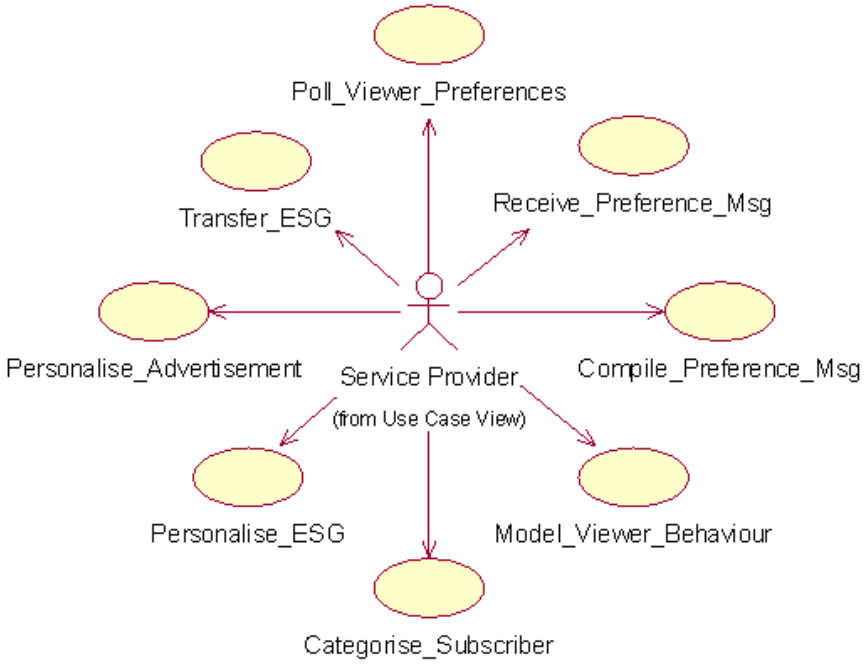


Fig. 35: The Advertise Targeted Services use case diagram

Having described various use case models, the possible security architectures concerning the key exchange schemes and underlying CA processing in the MICAS are elaborated as follows.

6.4.5 System Architecture

For implementing a federated identity management system in the converged networks, a third party data manager needs to work closely with various service providers and parties operating in the field. In fact, in the MICAS, the data manager plays an intermediary role between the Pay-TV service provider, mobile phone operator, set-top box and mobile phone certificate issuer.

The data manager manages silos of information regarding the in-field mobile and set-top box specifications, software/hardware certifications, identities, etc. It stores all the information regarding the valid SIM cards and GSM subscribers' identity (i.e. IMSI) in the database. It also keeps the track of valid certificates, which might be used to install new applications in the operator domain of the viewer's mobile phone or SIM card. On the other hand, to ensure that the operating set-top boxes are compliant with standards enforced by an authority (regulator), all the set-top boxes shall be tested by a certificate issuer agency. The agency then registers the approved set-top boxes with the data manager to be accessed by service providers. All of the data are stored in a central database, which are regularly updated by the data manager.

Fig. 36 shows an overall model of the external relationship of the service provider in the MICAS.

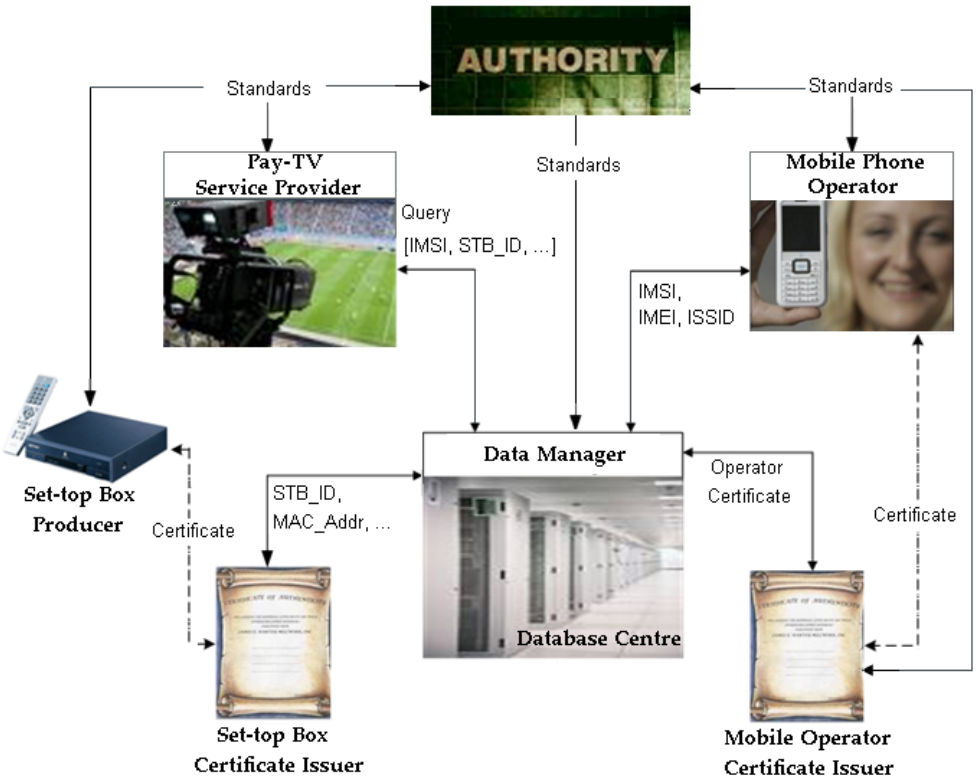


Fig. 36: The MICAS business circle

In the internal view of the MICAS, the service provider interacts with the viewer using the viewer's mobile phone over the GSM network. At the receiver-end, the viewer (subscriber) also establishes a connection between his mobile phone and set-top box for instance over the Bluetooth channel. During the interaction course, the viewer may place an order for a service or exchange his preferences to personalise services. At the head-end, the Message Handling Subsystem (MHSS) deals with all interactions and CASS installation processes in the field. It encodes/decodes outgoing/incoming messages and verifies the viewer's identity upon receiving the subscription request through either local or central database. It also updates the customer's accounts for instance regarding the personalisation information. The MHSS forwards the successfully verified subscription requests to the Subscriber Management Subsystem (SMSS). The SMSS enquiries, generates or updates the viewer's account based on the subscription request, instructs the SAS to decide on the CA mechanisms and instructs the Billing Subsystem to pursue the financial transactions. If the payments are authorised, the SAS starts responding to the CA instruction. The SAS may forward the key information as the Security Object to the MHSS or as the CA Message to the Multiplexer depending on the security architecture, as described later. The SMSS and SAS functionalities defined in the MICAS overlap with their counterparts defined in the DVB system except for interfacing with SMSS.

Fig. 37 (see next page) depicts the internal relationship and data flow amongst subsystems in the MICAS.

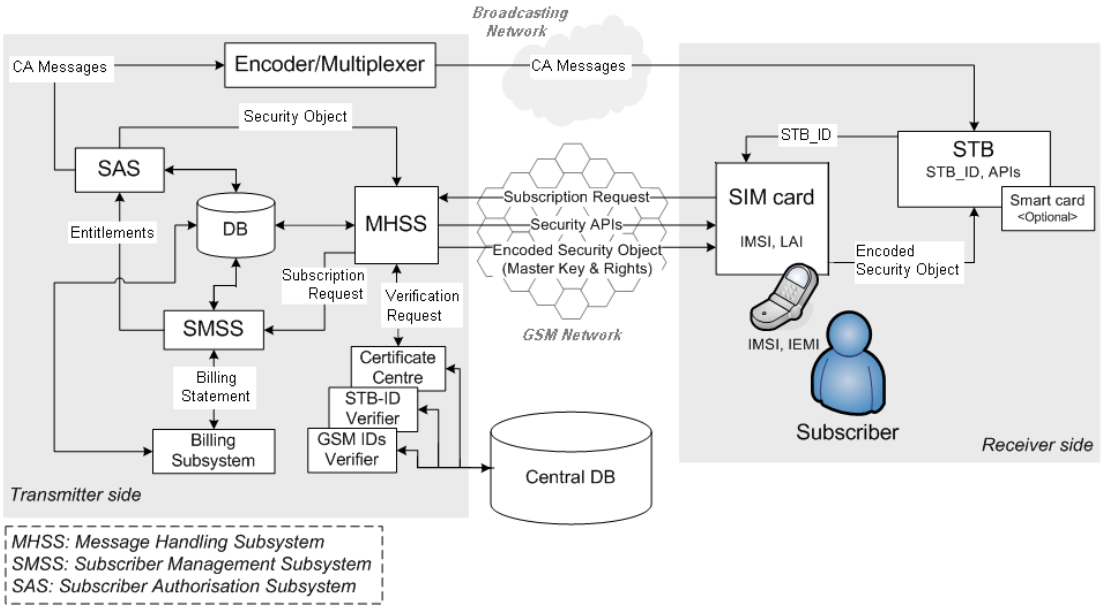


Fig. 37: An overall MICAS architecture

The APIs which need to be developed and installed to facilitate the control access system and communications across the MICAS are explained in the next section. It is followed by succinct description of possible security architectures in the MICAS.

6.4.5.1 Underlying Agents

The Subscription Sender agent can be implemented as a MIDLet running at the receiver-end (i.e. set-top box, mobile phone). It provides a comprehensive graphical interface and requisite functionalities specified in the Sign-up use case. It navigates the viewer through the sign-up wizard, generates and sends viewer's subscription request to the Subscription Manager which operates at the service provider.

After the viewer selects his list of services to subscribe, the set-top box Subscription Sender agent connects to the mobile phone Subscription Sender agent to acquire its IMSI and/or IMEI numbers. It then generates a message containing those numbers and the STB-ID and sends the message to the

Subscription Manager. For security reasons, the service provider may consider to not expose the STB-ID and IMSI number over the air. Instead, the set-top box temporary identifier (STB-TID) and Temporary Mobile Subscriber Identity (TMSI) can be used for identification purposes.

The Subscription Manager performs the verification processes, updates the viewer of the verification progress, updates the viewer's account, instructs the SMS for provisioning the CA system and issuing billing statements. It uses the IMSI, IMEI and STB-ID (or any temporary number derived from those) to respectively identify the viewer, his mobile phone and set-top box. For security reasons, it may crosscheck the identifiers with the data manager to ascertain that they are genuine, not reported stolen or used by another viewer in the network.

The Security agent operates at the receiver-end (i.e. set-top box, mobile phone) and it interacts with the Security Manager agent running at the head-end. The Security agent together with Security Manager guarantee the security aspects like authentication, identification, privacy, integrity and non-repudiation in any correspondence occurred amongst the entities in the MICAS. They can be an implementation of the digital signature scheme where three algorithms are required to generate a key, sign the message and verify the signature. In addition, they may incorporate the Hash function to encode the message. The Security agent is also responsible to monitor the viewer's contractual behaviour and alert the Security Manager in case that any illegal activity is detected. In case of piracy, the Security agent would halt the CA functions till receiving a notification message from Security Manager. The Security Manager compiles the alert and may ignore the event or automatically revoke/update the key information or inform the operator of the event.

The CA agent operates at the receiver-end (i.e. set-top box, mobile phone). The CA agent must have an Operator Certificate to be run on the privilege domain(s).

It is managed and downloaded by the CA Manager (also called MHSS CA Agent) operating at the head-end. The main duty of the CA agent lies in the control and execution of the CA functions (i.e. decoding or encoding the messages). The CA functionalities may vary depending on the security architecture explained later.

The Communication agent is running on the head-end and receiver-end and is responsible to implement the transportation protocols for exchanging the data across the channel. The interaction channel can be established through Bluetooth between the set-top box and mobile phone, and GSM network between the mobile phone and service provider. The underlying transmission protocols between the mobile phone and service provider can be the GSM Short Message Service (SMS) or Wireless Application Protocol (WAP).

The 'initialisation step' is a procedure conducted in all security architectures presented herein. It refers to the pairing sequence incurred between the mobile phone and set-top box, submitting the subscription request through subscriber's mobile phone, authorising the request, identification of subscriber, validation of the set-top box, and finally sending and installing security applets in a secure domain(s) in the subscriber's SIM card.

The possible data flow diagrams and processing model containing set-top box, mobile phone (SIM card) and service provider are presented in the following security architectures sections.

6.4.5.2 Security Architecture (1)

This model is an implementation of a simple 3-level key hierarchical conditional access system where the Master Key (MK) is used to decrypt the EMM. The decrypted EMM will provide the Service Key (SK) which is used to decode the ECM message and extract CWs for decoding the contents.

In the conceptual model, the CA Manager delivers the MICAS Security Objects (MKs and viewer's entitlements) to the mobile CA agent via the GSM network. The CA messages (i.e. EMM and ECM) are also broadcast to the set-top box operating in the field. The CA agent in the mobile phone fully transfers the credentials to the CA agent in the set-top box through the secure channel established by the Communication agent. At the set-top box, the CA agent invokes the underlying security algorithms to decrypt the EMM and extract the SK to decrypt the ECM. The subscriber's entitlements (rights) are checked against the rights associated to the content (as inserted in the ECM). If the condition is satisfied, the CWs are released to descramble the content.

Fig. 38 shows the interaction between the head-end and receiver-end in this security architecture where the mobile phone plays an intermediary role between the service provider and set-top box.

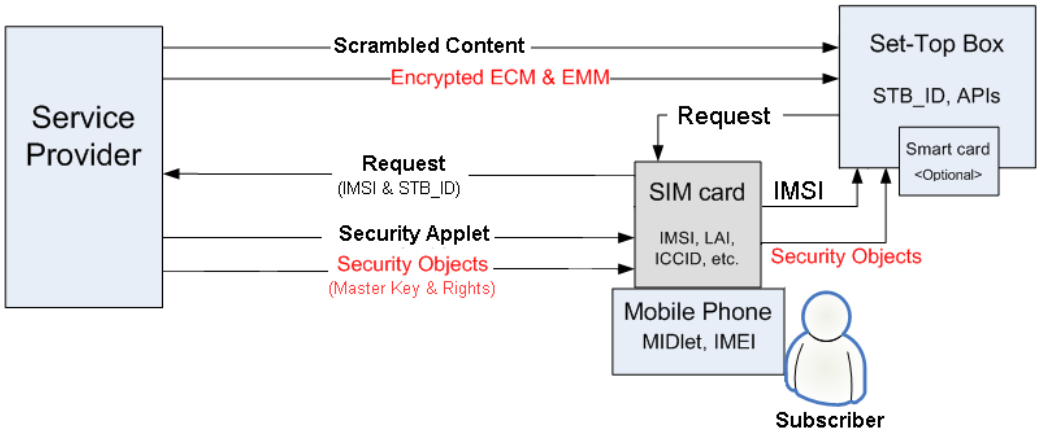


Fig. 38: The data flow diagram of security architecture (1)

6.4.5.3 Security Architecture (2)

This architecture is another model of the previous architecture where a 3-layer security is adopted and the CA messages (EMM and ECM) are delivered through broadcasting medium.

After having established the initialisation step, the set-top box CA agent forwards the EMM to the mobile CA agent. The mobile CA agent decrypts the

EMM and extracts the SK using the MK delivered with the Security Object (MK and Subscriber's rights) via the GSM channel. The mobile CA agent then forwards the extracted SK as well as subscriber's rights to the set-top box CA agent to be used for content decryption processes.

Fig. 39 shows the data flow diagram when EMM is broadcast over-the-air to the set-top box and delivered to the subscriber's mobile phone for processing.

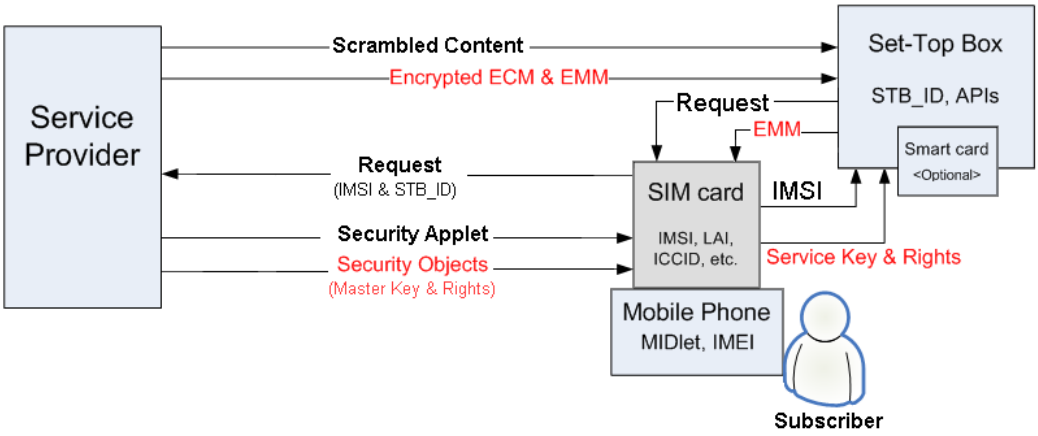


Fig. 39: The data flow diagram of security architecture (2)

6.4.5.4 Security Architecture (3)

Similarly, a 3-level key hierarchical security system is adopted in this model. The CA messages are broadcast to the receiver population in the field. The EMM and ECM processing is mainly pursued in the viewer's mobile phone.

In this architecture, after initialisation step, the set-top box CA agent forwards the CA message (i.e. EMM and ECM) to the mobile CA agent over the Bluetooth link established by the Communication agents. The mobile CA agent decrypts the EMM and extracts the SK using the knowledge of the Security Objects (MK and Subscriber's rights) delivered by the service provider through the GSM network. The extracted SK is then used for decoding the ECM and extracting the CWs. The mobile CA agent transfers back the extracted CWs to the set-top box CA agent for descrambling the content.

Fig. 40 shows the data flow diagram where the EMM and ECM are delivered to the mobile phone through the set-top box. The decoding processes mainly take place in the subscriber's mobile phone (SIM card) and the descrambling takes place in the set-top box.

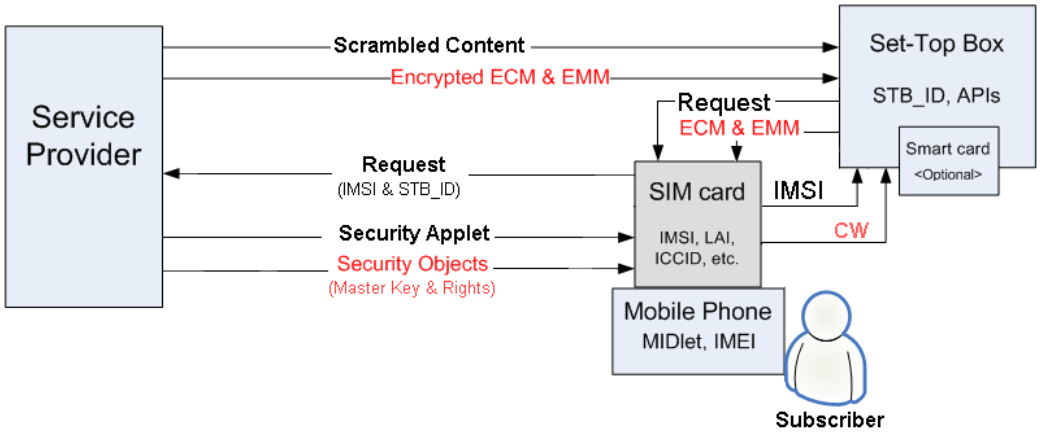


Fig. 40: The data flow diagram of security architecture (3)

In pervious proposals, the CA messages (i.e. ECM and EMM) are broadcast to the receivers. On the other side, the key information is delivered through the return channel (GSM network) to open the encrypted EMM. The decoding process can take place either in the set-top box or viewer's mobile phone.

6.4.5.5 Security Architecture (4)

This architecture models a 3-level key hierarchical security system where the ECM message is broadcast over-the-air to receivers and EMM message is unicast to the individual viewer's mobile phone.

After the initialisation step, the CA Manager transfers the EMM message to the mobile CA agent. The EMM may contain the SK and subscriber's rights. The mobile CA agent transfers the EMM to set-top box CA agent. The set-top box CA agent processes the EMM message using the Security Objects (i.e. MK and entitlements). The Security Objects can be pre-stored into a smartcard or delivered over-the-air through the GSM channel to the set-top box. Given the SK,

the ECM can be decoded and CWs can be extracted for descrambling the content. The CWs are released if the viewer has sufficient permission to watch the content. All the control actions are conducted in the set-top box.

Fig. 41 shows the data flow diagram where the viewer's mobile phone as an intermediary hands over the EMM to the set-top box. The set-top box then decodes the EMM and ECM to get the CWs for descrambling the content.

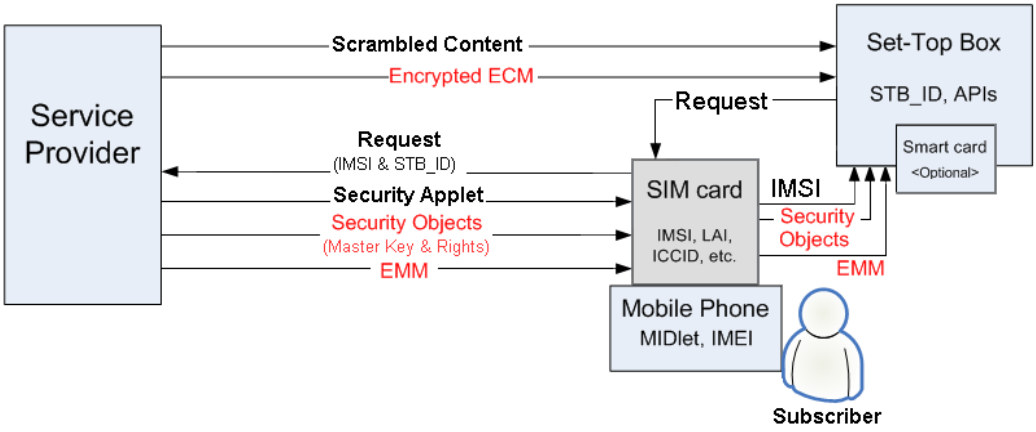


Fig. 41: The data flow diagram of security architecture (4)

6.4.5.6 Security Architecture (5)

In this model, the broadcasting network is used to transfer one part of the CA message (i.e. ECM) and GSM network is used to transfer another part of the CA message (i.e. EMM) to the receiver end. The EMM processing takes place in the viewer's mobile phone and ECM processing takes place in the set-top box.

After the initialisation step, the CA Manager at the head-end transfers the EMM to the mobile CA agent. The EMM message is decoded using the MK, which can be burnt into by the SIM card issuer or delivered by the service provider to the SIM card prior to the EMM delivery. The SK and subscriber's rights are then extracted to be transferred to the set-top box CA agent. The set-top box CA agent then decrypts the ECM message which is received from the broadcasting medium. If the subscriber's right matches the programme right, the CWs are released to descramble the content.

Fig. 42 shows the data flow diagram when the EMM is processed at subscriber's mobile phone (SIM card) and the SK and entitlements are sent to the set-top box for decoding ECM and descrambling contents.

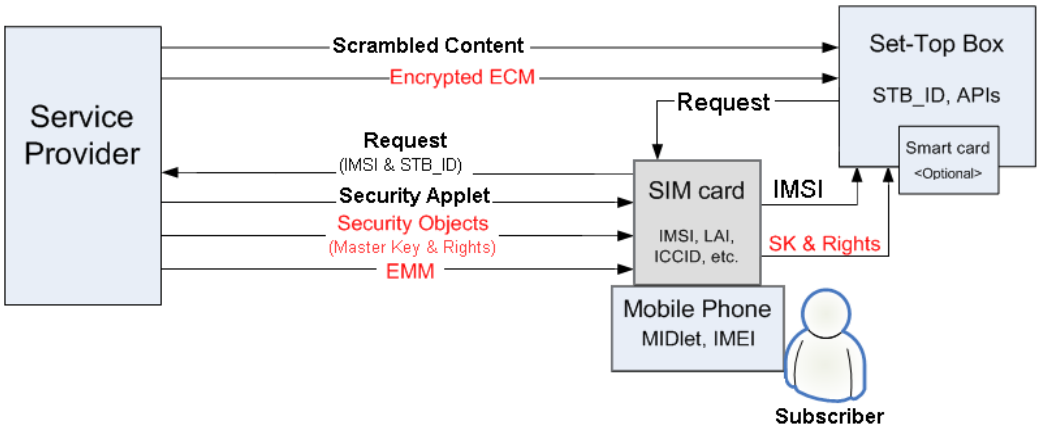


Fig. 42: The data flow diagram of security architecture (5)

6.4.5.7 Security Architecture (6)

Similar to the previous model, the ECM is broadcast to the field and EMM is unicast to the viewer's mobile phone through GSM network. But, in this model, the set-top box is an intermediary to deliver the ECM to the mobile phone where CA messages are processed and the CWs are extracted.

After the initialisation, the CA Manager transfers the EMM message to the mobile CA agent. The set-top box CA agent also transfers the ECM to the mobile CA agent to decrypt ECM using the knowledge of the SK conveyed with EMM and extract CWs if subscriber's rights match the programme right inserted into the ECM message. The mobile CA agent passes the CWs to the set-top box CA agent to descramble the content.

Fig. 43 shows the data flow diagram where the EMM and ECM are transferred to the viewer's mobile phone, respectively from the GSM and broadcasting networks, using the set-top box as an intermediary device.

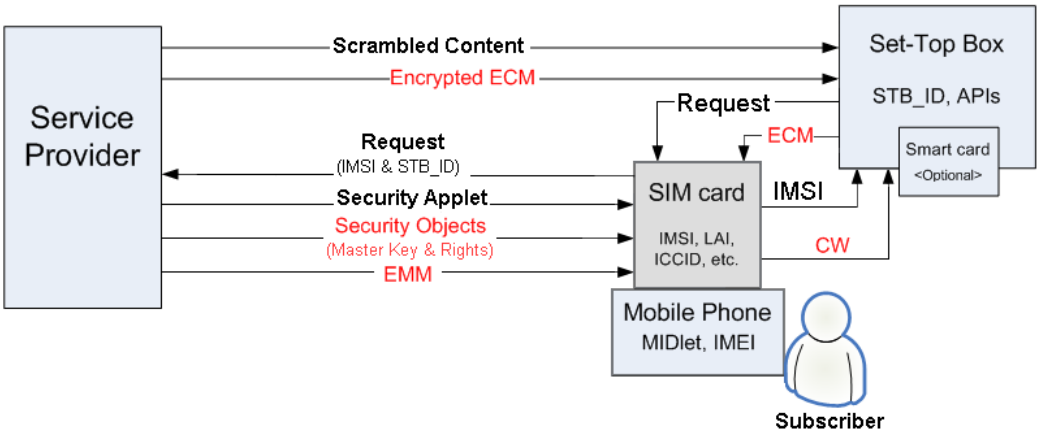


Fig. 43: The data flow diagram of security architecture (6)

6.4.5.8 Security Architecture (7)

This model represents an architecture wherein a 2-level key hierarchical security system is used. As the key information is unicast to the receiver-end, the MK used to decrypt the EMM message may be eliminated from the key hierarchy. As a result, the only key to transfer will be the SK which is used to decrypt the ECM message. Depending on the processing model, the security architecture may vary as follows.

After initialisation step, the CA Manager transfers the SK and subscriber's rights (Security Objects) to the mobile CA agent. The mobile CA agent then transfers the Security Objects to the set-top box CA agent. The SK and subscriber's rights may be used by the set-top box CA agent or any security algorithms embedded in the set-top box to decrypt the ECM message. The CWs are released to descramble the content only if the subscriber's rights match the access right of the content.

Fig. 44 presents the data flow diagram where the SK and viewer's rights from GSM side and ECM message from broadcasting medium side are delivered to the set-top box. The mobile plays an intermediary role and whole conditional access processing is hosted in the set-top box.

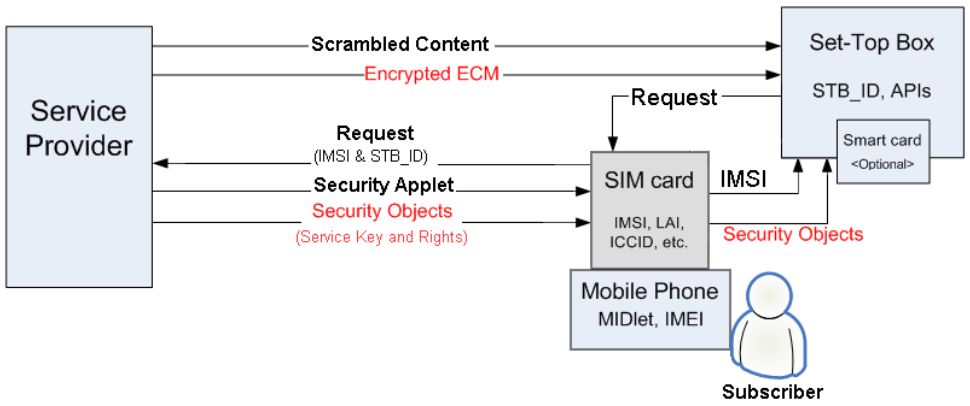


Fig. 44: The data flow diagram of security architecture (7)

6.4.5.9 Security Architecture (8)

This model is another type of the 2-level key hierarchical security system. In this model, the entire CA processing takes place in the mobile phone and the extracted CWs are delivered to the set-top box for the descrambling process.

After the initialisation step, the CA Manager transfers the Security Objects (SK and subscriber's rights) to the mobile CA agent. The set-top box CA agent transfers the ECM to the mobile CA agent to decrypt the ECM using the SK. If the viewer's rights match the conditional access criteria, the extracted CWs are then sent to the set-top box CA agent for descrambling.

Fig. 45 shows the data flow diagram where the ECM message is processed in the viewer's mobile phone based on the delivered Security Objects. The extracted CWs are then delivered to the set-top box for descrambling the content.

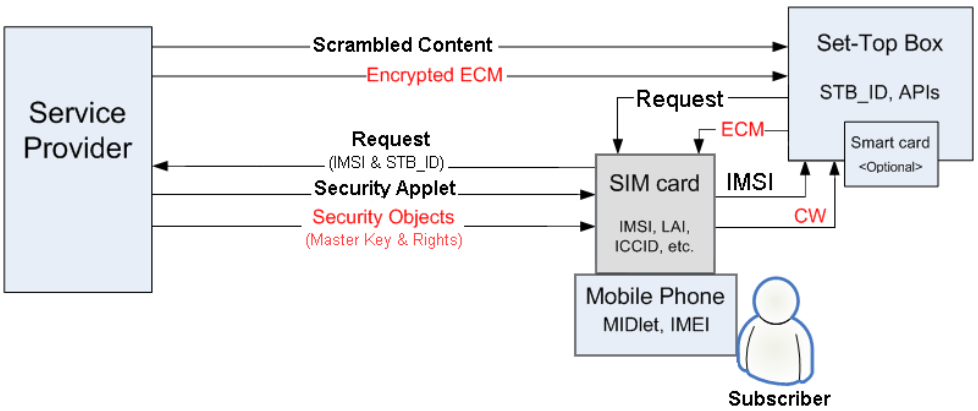


Fig. 45: The data flow diagram of security architecture (8)

6.4.5.10 Security Architecture (9)

This model presents the full application of the mobile phone in the CA message processing and descrambling the content. Regardless of the level of the key hierarchy used in the security system, the descrambling process fully takes place in the mobile phone. The ultimate goal is to fully shift the CASS to the mobile phone while enjoying the resolution of the TV-set. In order to achieve this goal, all the CA messages and Security Objects shall be delivered to the viewer's mobile phone. The content can be delivered to the mobile phone either over the mobile network (i.e. 4G, LTE) or over the broadcasting medium via the set-top box. The former is attributed with lower bit rate (i.e. 30Kbps – 512Kbps) suitable for scarce resource devices like mobile phones, while the latter is attributed with higher qualitative contents (i.e. 2Mbps - 60Mbps) suitable for TV screens.

For delivery of the CA messages, a possible approach is to unicast EMM to the viewer's mobile phone and broadcast the ECM message over-the-air to the set-top box. The set-top box then transfers the ECM and/or content to the mobile phone. The descrambled content may then transfer to the set-top box to be displayed on the TV screen.

The CA Manager may transfer the Security Objects and/or CA message (i.e. EMM) to the mobile CA agent. The set-top box CA agent receives transport streams (incl. ECM and content) and delivers them to the mobile CA agent. The mobile CA agent processes the ECM based on the received key and entitlements data and extracts the CWs. The mobile CA agent descrambles the content and transfers it to the set-top box to be displayed on the TV screen. The communication link between the set-top box and mobile phone shall be fast enough to display the content with no perceivable delay. Thus, popular Bluetooth adapters (1-3Mbps) do not seem to be a suitable choice of connectivity. Instead, the high speed interfaces like High Speed USB 2.0 (480Mbps), IEEE 1394

WireFire-400 or -800 (800Mbps), Ethernet 100Base-T (10-100Mbps) ATA-133 (1064Mbps) and ATA-300 (1200Mbps) can be used. Nevertheless, recently proposed versions of the high speed Bluetooth (Bluetooth V3.0) integrating the Ultra Wide Band (UWB) technology would potentially enable the high data rate transfers of up to 480Mbps.

Fig. 46 shows the data diagram in a 2-level key hierarchy security architecture where the ECM and digital content are delivered to the mobile phone for decoding and descrambling processes. The contents are then transferred to the set-top box for further encoding.

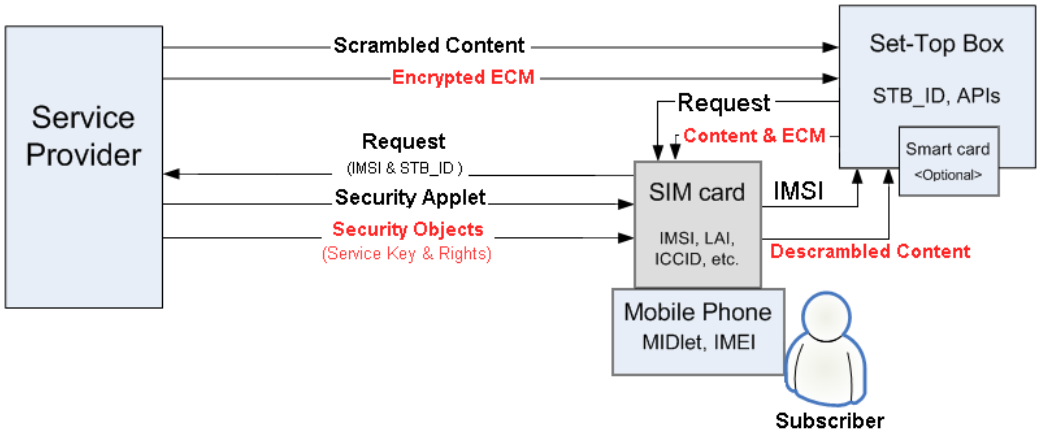


Fig. 46: The data flow diagram of security architecture (9)

6.4.5.11 Security Architecture (10)

In this model the GSM network is used for the delivery of the key information and CA messages (i.e. ECM and EMM) to the viewer's mobile phone. The decryption of the messages may take place at the mobile phone and/or set-top box. Considering all the combinations, the mobile phone may play an intermediary role to deliver both messages and viewer's rights to the set-top box to perform full CA processing. It may also process the EMM message and deliver the SK to the set-top box for ECM processing. Moreover, the mobile phone can be used to process EMM and ECM messages. In more advanced situations, the

mobile may be considered as the CA subsystem processing the CA messages and descrambling the content.

Fig. 47 presents a simple model of the security architecture where the CA messages are delivered to the receiver-end through the GSM network. In this architecture, the descrambling sequence takes place in the set-top box.

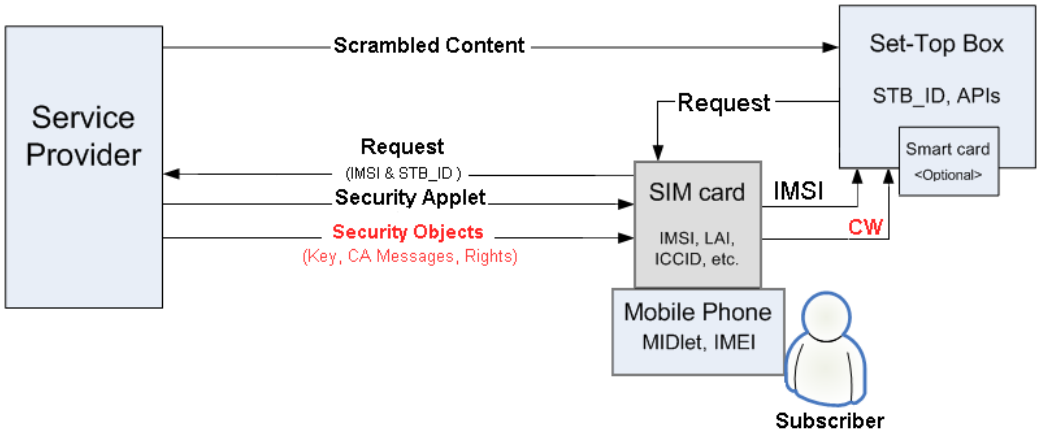


Fig. 47: The data flow diagram of security architecture (10)

Following points are supported in all security architectures explained above.

- The smart card is considered as an option; this will enable Free-view boxes to be used for Pay-TV services;
- The mobile phone can be replaced by any device offering similar features in connectivity and security (i.e. a STB with GSM connectivity);
- The service provider can update and/or revoke the compromised security key(s) and/or algorithms online through the GSM network;
- Implementing encryption, session key, digital signature and mutual authentication techniques are viable in the MICAS and will improve the security;
- Service provider(s) can download their own security algorithms into the subscriber's SIM card through GSM network followed by delivery of requisite key information to enable authorised people access to contents.

On the other hand, the platform enables service providers to monitor the behaviour of the subscriber which results in improving the security mechanism and enriching the range of bespoke services. One of the services that can be introduced in this platform is the 'Follow Me' service, which enables the subscriber to access the content upon his entitlement without the requirement of being bound to a specific set-top box. The service would give freedom of choice to the subscriber and offers ubiquitous access to the entitlements through an arbitrary set-top box. The Follow Me service can be applicable in the existing broadcast infrastructure. However, a mechanism should be adopted to eliminate the rigid and pre-defined one-to-one relationship between subscriber and STB. The approach is to identify both elements (subscriber and STB) based on the unique identities such as that which is used in mobile networks to identify the subscriber (IMSI) and identify the mobile device (IMEI). Such conditions are met by proposed architectures wherein a proper infrastructure can be established to offer the 'Follow Me' type of services to the viewers.

6.5 Summary

The network convergence as a new phenomenon has opened new business opportunities for network operators and service providers. This has already emerged in the mobile and Internet based platforms and to some extent in the DTV. The content delivery through the Internet is now being offered in the DTV and family standards like DVB-T/-H also enable broadcasters to reach hand-held devices. The range of services has been diversified although there are still fundamental issues in the Pay-TV systems yet to be resolved. These inherited issues can be categorised as follows:

- Lack of interoperability between CA systems and vertically integrated transaction model which scales down the business for a newcomer either as a service provider, set-top box producer or CA provider;
- Inefficient usage of bandwidth for transferring CA messages and high complexity of the system due to the synchronisation issues and nature of the network used in the traditional broadcasting systems;
- High administration and operational and high security flaw costs will result in more expensive subscription fees and together with lack of interactivity and personalised services will decrease the subscribers' satisfaction.

Such inherited issues can be routed to the commercial requirements and technologies used in the traditional Pay-TV and broadcasting systems. Nowadays, with the advent of the technology especially in the digital communication systems, interactivity, mobility and personalisation features can be added to Pay-TV services. The Internet and mobile networks are now widely available connecting the whole world together. Therefore, it is expected that information and multimedia services are delivered ubiquitously. This requirement has been addressed here via Internet, GSM and GPRS based solutions which can potentially resolve the mobility and interoperability issues in Pay-TV systems.

The GSM-based solution demonstrates novel features that can reduce the overall production cost of the set-top box, improve mobility and level of personalisation in the system. Therefore, amid the proposed architectures, the Mobile Integrated CA System (MICAS) solution was designed and analysed through various use case scenarios and security architectures.

The MICAS subscriber needs to set up his receiver equipment and bind his mobile phone to the set-top box in order to start using the MICAS services.

Having received proper service information, the subscriber may sign up for a service and place his order. The subscriber can set his local control criteria while signing up. It is also possible to set multi-room services via multiple set-top boxes. During the sign-up process, the viewer may activate the Follow Me service to enjoy his subscription via any set-top box. The MICAS would enable the subscriber to amend his subscription at any time.

In the MICAS, the service provider may interact with the viewer at any stage during the sign-up and subscription amendment processes. The service provider deals with the viewer's requests, manages his account and issues statements as part of the billing process. Furthermore, the service provider regularly checks the security level in the system, downloads CA subsystem or update patches to the viewer's set-top box or mobile phone depending on the security architecture. The service provider shall also offer personalised services, relevant advertisement and take appropriate security actions based on thorough analysis of viewer's behaviour and choices.

In the MICAS, the mobility feature is based upon the unique viewer's GSM identities (i.e. MSISDN, IMSI) and unique identity burned to the standardised set-top box. The in-field information of subscribers and authenticated set-top boxes are all managed and provided to service providers by a third party data manager. To ensure that operating set-top boxes are compliant with standards enforced by an authority (regulator), all the set-top boxes shall be tested by a certificate issuer agency. The agency then registers the approved set-top boxes with the data manager to be accessed by service providers. The service provider shall contact the data manager during the validation process to identify whether the viewer and his set-top box are genuine.

The MICAS is utilises the mobile platform in the traditional Pay-TV system. The mobile and broadcasting networks can be both used to deliver multimedia

services, CA messages, APIs and interactions. The mobile phone and set-top box can be used for hosting access control mechanisms and credentials. The combination of the message delivery routes and entity which hosts and deals with the CA-related processes leads to different security architectures. These architectures are attributed with different level of security, complexity and performance supporting different level of key hierarchy and CA messages.

The next chapter describes a prototype of the system and some aspects of the implementation using the UML Class diagrams. It is followed by thorough analysis of described security architectures against the non-functional requirements including the security, complexity, cost and performance.

7 MICAS IMPLEMENTATION AND ANALYSIS

7.1 Introduction

The MICAS incorporates different software applications to expand interactivity and security across the platform. The main focus of this chapter is on the software side of the MICAS. The hardware specifications, although is still important, but it is postulated that the most of the existing mobile handsets and set-top boxes can meet the minimum requirements of the MICAS. It is worthwhile noting that a full demonstration of the MICAS requires a close collaboration with a mobile operator to get trial access permission to the Operator domain in the mobile phone. The same problem applies to the set-top box, as the MICAS demands for a new type of set-top box with special connectivity and middleware specifications. As such, the receiver-side in the MICAS is prototyped in a controlled environment (i.e. PC) wherein the scarce devices like mobile phones and set-top box performance are emulated in the J2ME Connected Limited Device Configuration (CLDC) and/or Connected Device Configuration (CDC) platforms, respectively. At the head-end, only the newly introduced Message Handling Subsystem (MHSS) is prototyped where its interactions with other existing parts in the DVB system are not accounted. The MICAS prototype is described using the UML Class diagrams followed by some sample codes demonstrating the set-top box and mobile communications in the MICAS. The chapter is followed by providing thorough analysis of the MICAS security architectures described in Chapter 6.

7.2 MICAS Implementation

In Chapter 6, the behaviour of the system was explained using the UML Use Case diagrams and functional requirements. In addition, the possible interaction with each Use Case and flow of events were also described within each Use Case scenario. The APIs that run in the set-top box, mobile phone and head-end were also briefly discussed. Moreover, various security architectures were presented to highlight the possible data flow diagrams and security implementations which can be deployed in the MICAS. In this chapter, the structure of the system is presented in a programmable security platform supporting most of the described security architectures. The platform is not considered as an absolute solution, as requirements may vary from one security architecture to another. Thus, a Pay-TV service provider may wish to engineer his requirements and deploy an optimum security solution in a platform that satisfies his security criteria.

The design of the system will be Object Oriented wherein each entity in the MICAS is considered as an object with attributes (i.e. properties and functions) and relationships between other objects inside and outside of the MICAS scope. The objects are presented using the UML Class Diagram. Finally, some sample codes are presented to elaborate some practical aspects of the MICAS.

7.2.1 MICAS Protocol Stack

The static view of the MICAS is presented here using the UML Class Diagram. In this structure, a 4-layer protocol stack is defined in the MICAS to handle all interactions between the entities in the MICAS. The first layer is responsible for establishing the communication link, the second layer is the security or authentication layer, the third layer is the conditional access layer and the forth layer is the application layer. The implementation of the protocol stack in the mobile phone and set-top box very much depends on the security architecture

and the role wherein the said entities are playing. Nevertheless, the 3 layers - communication, authentication and application – must be adopted in any implementation.

Each underlying agent described in Chapter 6 forms a layer in the MICAS protocol stack. For instance, the Communication agent operating at both mobile phone and set-top box is responsible to establish a link between set-top box and mobile phone. The Security agent at the receiver side and Security Manager at the head-end together perform the Authorisation, Authentication and Accounting (AAA) processes. The CA Agent and CA Manager perform conditional access functions via exchanging Security Objects (i.e. security Applets, key, etc.) across the network. Finally, at the application layer, objects like Subscription Sender and Subscription Receiver facilitate the subscription processes (i.e. sign-up, amendment, cancellation, etc.). Monitoring the subscriber's behaviour to improve security and personalised services will be other instances operating in the application layer. Each agent is implemented as an object (class) and attributed with specific functions and relationships with other objects in and outside the MICAS to ultimately generate appropriate messages to be exchanged across the platform amid MHSS, mobile phone and set-top box. The messages can be of type the subscription, amendment, acknowledgment, monitoring or conditional access messages that the involved parties may send together; as explained in the use case models in Chapter 6.

The main hardware platforms in the MICAS are the Mobile phone and Set-top box at the receiver-end and a server (MHSS) at the head-end. Each of them can be run by different operating systems, but it is postulated that they will all support the fundamental Java technologies (i.e. Java Virtual Machine, communication and security APIs), as required by the MICAS.

Fig. 48 presents the Java platforms and APIs required in the MICAS. The Wireless Messaging APIs (WMA) can be replaced by a short message commands made available in the JavaCard and a server application (tailored application), which is connected to a SMS Service Centre (SMSC) to exchange text or binary messages (i.e. SMS). The relationship amid entities and the use of Java APIs are detailed later.

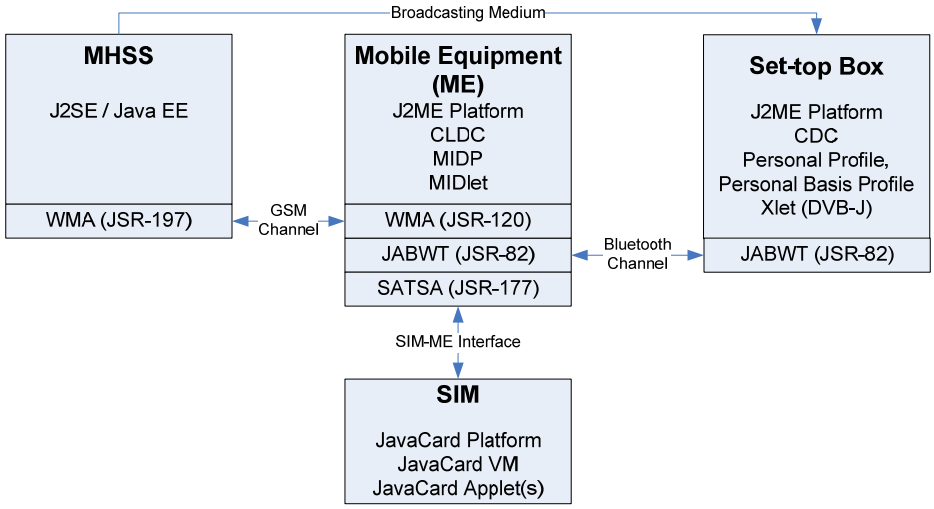


Fig. 48: The MICAS software architecture

Fig. 49 presents a static view of the interactive protocol stack used in the MICAS.

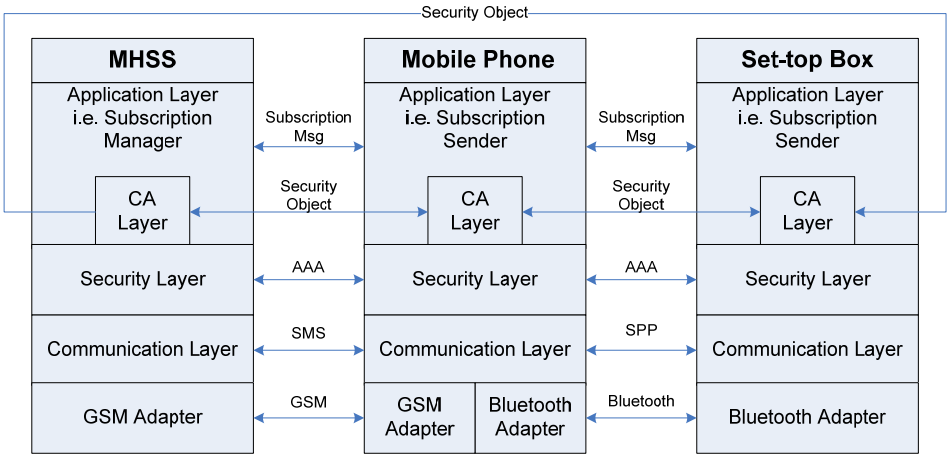


Fig. 49: The interactive protocol stack in the MICAS

It is worthwhile noting that two ways of implementation can be considered in the MICAS: 1) mobile centric [97] and 2) set-top box centric implementations. The former implements all the interactive use cases (i.e. signing-up, amending or subscribing for preferences) in the mobile phone. Thus, all the interactions are initiated from the mobile phone; as such the mobile phone shall present the EPG or ESG information and navigate the user to settle a specific request; such as subscription request explained in the sign-up use case. The latter, on the other hand, is based on the set-top box and all the interactions are initiated and managed through the set-top box and TV screen rather than the mobile phone. This is more analogous to the existing broadcasting platform and therefore it has been adopted in the design of the MICAS.

7.2.1.1 Communication Layer

The Communication agent in the mobile phone communicates with its counterparts residing at the set-top box and MHSS respectively via Bluetooth transport and GSM protocols. The mobile Communication agent can be implemented as a J2ME MIDlet in the Mobile Equipment (ME). It acts as an intermediary between the SIM and outside world. It communicates with applet(s) installed on the SIM based on Application Protocol Data Unit (APDU) commands through ME-SIM interface. The applet(s) can be considered as the implementation of Security and CA agents defined in the MICAS protocol stack.

Fig. 50 presents an abstract of the attributes and operations associated with the Communication agents in the MICAS. The Bluetooth-related operations are common between set-top box and mobile Communication Agent, but other operations are solely called by the mobile Communication agent to interact with the SIM and MHSS. Due to the potential interest in the commercialisation of the MICAS, only the main implementation aspects are discussed herein.

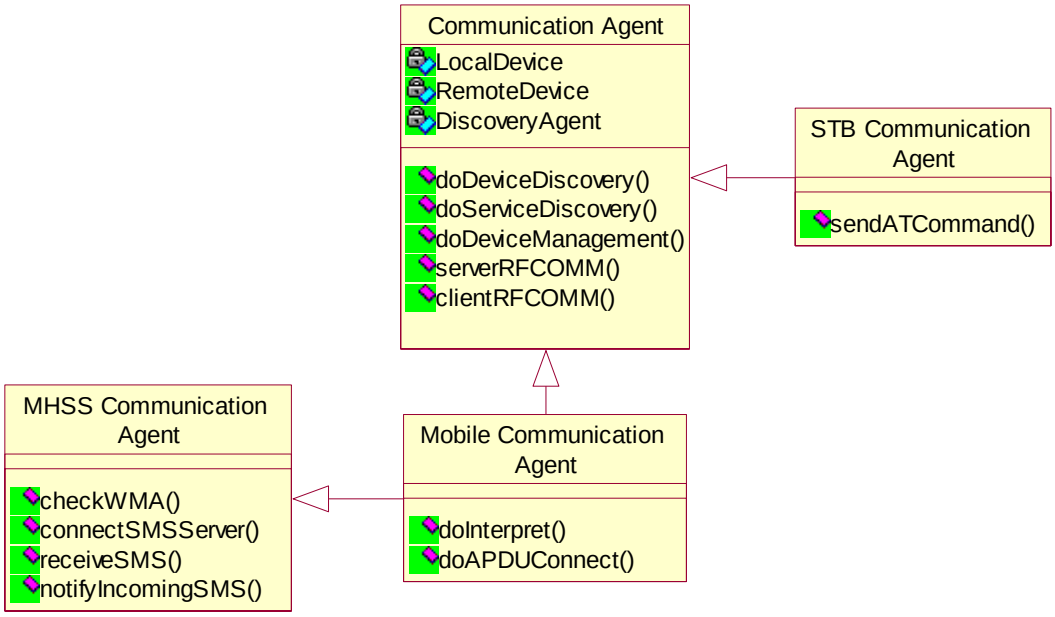


Fig. 50: The Communication agent class diagram

The Bluetooth profiles ensure the cross platform interoperability and consistency requirements. Bluetooth devices can offer additional functionalities, given that paired devices support similar profiles. Thus, the Bluetooth profiles such as the Serial Port Profile (SPP), File Transfer Profile (FTP), SIM Access Profile (SAP) can be employed for transferring file(s)/data between the mobile phone (or SIM) and set-top box. Alternatively, a new Bluetooth profile can be developed using Java technologies to handle all the transactions between the set-top box and mobile phone defined in the MICAS. The matter needs close cooperation with Bluetooth and mobile application developers, Bluetooth manufacturer, mobile manufacturer, set-top box manufacturer and finally network provider. Nevertheless, the Java APIs, which can be used for implementing the Communication agent in the set-top box and mobile phone, are explained as follows.

The Communication agent can be either a client or server in the MICAS Bluetooth software architecture. The server always advertises its services and

client initiates the connection request to consume the services. The Communication agent has to first initialise the Bluetooth stack. Then, it may inquire nearby devices (discovery), manage devices and establish communication link.

The Bluetooth stack is a vendor-based firmware that controls the Bluetooth device. Therefore, in order to work on a specific Bluetooth device, a developer needs to know the APIs defined by the associated vendor. However, if the device supports the Java platform, the developer can benefit the JSR-82 - Java APIs for Bluetooth Wireless Technology (JABWT). The JSR-82 APIs provides classes and interfaces to simplify the device discovery, device management and communication steps in the developing of Bluetooth-enabled applications.

The JSR-82 APIs have been defined in two optional packages: 1) the core Bluetooth APIs (*javax.bluetooth*) and 2) the Object Exchange APIs (*javax.obex*), which are both supported by any J2ME configurations such as Connection Limited Device Configuration (CLDC) supporting the Mobile Information Device Profile (MIDP). If the Communication agent is implemented as a MIDlet, it has to extend the *javax.microedition.midlet.MIDlet* and implement the *javax.microedition.lcdui.CommandListener* to listen for command input from the user interface. The details of the said classes can be found in the Sun Microsystems' website (java.sun.com).

For Bluetooth-related functions, the Communication agent has to use the *DiscoveryAgent* class and implements the *DiscoveryListener* interface to get the discovery notification when a nearby device and/or service is discovered. It is worthwhile noting that at the centre of the service discovery are Service Discovery Database (SDDB) maintained by the Bluetooth implementation and Service Discovery Protocol (SDP), which is transparent to applications based on the JABWT.

For device management, the Communication agent has to use the LocalDevice, RemoteDevice and DeviceClass classes. The LocalDevice provides methods to retrieve information about the local device and get access to the Bluetooth manager. Similar methods have been defined in the RemoteDevice class to enable the local device to retrieve remote device's information before consuming its services. Additional security related methods have also been defined in the RemoteDevice class which enable the local device to perform authentication, authorization, encryption functions. These security functions may also used by the Security agent in the MICAS protocol stack. The DeviceClass object presents the device's Class of Device (CoD) for example a phone. Hence, when a device is discovered, its class is discovered as well. This object can be used to verify the class of device (mobile phone and set-top box) supposed to be used in the MICAS.

The JABWT uses the Generic Connection Framework (GCF) when creating connection and performing I/O over Bluetooth link. The GCF is defined in the *javax.microedition.io* API. The JABWT extends the GCF by adding L2CAP and RFCOMM (OBEX) support, respectively through connection-oriented JSR-82 *L2CAPConnection* and *javax.microedition.io StreamConnection* types. Nevertheless, the *javax.microedition.io.Connector* is used to establish a Bluetooth connection in all GCF connection types. The URL passed to the Connector determines the type of GCF connection. For instance, the URL used for a L2CAPConnection is: "*btl2cap://hostname: [PSM | UUID]; parameters*" and the URL used for RFCOMM StreamConnection is: "*btspp://hostname: [CN | UUID]: parameters*". If the connection string starts with "*btgoep*", the OBEX is used for communication. The OBEX is a good choice for sending an object data like a file and RFCOMM, which is emulating the Serial port, is a good choice for sending stream data. In the URL, the hostname can be defined as the word "*localhost*" for a server connection or a

Bluetooth address (*ServiceRecord.getConnectionURL*) for a client connection. The Protocol Service Multiplexer (PSM) and Channel Number (CN) values are used by a client connection to a server. The parameter can be the name of a service and/or security parameters for authentication, authorization and encryption. While requesting for the URL, the security options can be set by *RequiredSecurity* argument required by the *getConnectionURL()* method. The *RequiredSecurity* can be *ServiceRecord.NOAUTHENTICATE_NOENCRYPT* indicating that the optional security parameters for authentication and encryption are not required. However, as mentioned earlier, the connection can be set to be secured after that it has been established. This can be done by calling *RemoteDevice*'s *authenticate ()*, and then *authorize ()* and *encrypt ()* security methods.

The Communication agent can also use the vendor's specific APIs to control the device via the Bluetooth Control Centre (BCC). The BCC provides an interface to change local Bluetooth settings, resolve conflicting requests between applications and handle security operations that require user interactions. In short, turning on/off the Bluetooth radio, changing the name of the device, device's discovery mode, setting PIN numbers and default security attributes are part of the BCC tasks. The BCC is part of the JABWT specifications but its details have been left to the implementation and there is no method within the JABWT that allows direct modification of a device's properties [68]. The following code snippets present how to perform device and service discovery and establish an RFCOMM link between a client and server over the Bluetooth link.

```
public class CommunicationAgent extends MIDlet implements CommandListener,
DiscoveryListener {

// Extending MIDlet related methods
public void startApp() {doDeviceDiscovery();}
public void pauseApp() {…}
public void destroyApp(boolean unconditional) {…}
```

```
public void commandAction(Command c, Displayable d) {…}
/* Implementing the CommandListener and DiscoveryListener interfaces
public void deviceDiscovered(RemoteDevice remoteDevice, DeviceClass deviceClass) {…}
public void inquiryCompleted(int param) {…}
public void servicesDiscovered(int transID,ServiceRecord[] serviceRecord) {…}
public void serviceSearchCompleted(int transID, int respCode) {…}
```

```
private void doDeviceDiscovery() {
try {
local = LocalDevice.getLocalDevice();
}
catch (BluetoothStateException bse) {…}
agent = local.getDiscoveryAgent();
devicesFound = new Vector();
try {
// Start discovering a device by calling its General Inquiry Access Code (0x9e8633)
if (!agent.startInquiry(DiscoveryAgent.GIAC,this)) {…}
}
catch(BluetoothStateException bse) {…}
}
```

```
private void doServiceDiscovery(RemoteDevice device) {

//  Service search will always give the default attributes:
// ServiceRecordHandle (0x0000), ServiceClassIDList (0x0001),
// ServiceRecordState (0x0002), ServiceID (0x0003) and
// ProtocolDescriptorList (0x004).
// Additional attributes may be required like ServiceName (0x100),ServiceDescription (0x101) and
 // ProviderName (0x102) which must be supplied through an int array

int [] attributes = {0x100,0x101,0x102};

// Each service is identified by an UUID. Supplying UUIDs in an UUID array enables searching
// for specific services. PublicBrowseRoot (0x1002) is used here. This will return any services that
// are publicly browse-able. When searching for a specific service, the service's UUID should be
// supplied here.

UUID[] uuids = new UUID[1];
uuids[0] = new UUID(0x1002);
try {
agent.searchServices(attributes,uuids,device,this);
}
```

```
catch (BluetoothStateException e) {…}
}
```

```
// Setting up an RFCOMM server
public void serverRFCOMM() {
LocalDevice local = null;
StreamConnectionNotifier server = null;
StreamConnection conn = null;

// Service name is 'FCOMM Server' and Service record (UUID) is  393a84ee7cd111d89527000bdb544cb1
// created in the Linux by 'uuidgen –t' function which calculates the UUID based upon the hardware
// address of the machine and time. No authentication and encryption is set.

String connectionURL =
"btspp://localhost:393a84ee7cd111d89527000bdb544cb1;"
+ "authenticate=false;encrypt=false;name=RFCOMM Server";

// The server should be discoverable, else clients cannot find our service
try {
local = LocalDevice.getLocalDevice();
local.setDiscoverable(DiscoveryAgent.GIAC);
} catch (BluetoothStateException e) {…}

// First get a StreamConnectionNotifier to get the service record and manipulate it.
try {
server = (StreamConnectionNotifier)
Connector.open(connectionURL);
} catch (IOException e1) {…}
// acceptAndOpen() will register the service record in the Bluetooth SDDB and block it until a client
// connects to the service.
try {
conn = server.acceptAndOpen();
} catch (IOException e2) {…}
}
```

```
// Setting up an RFCOMM client
public void clientRFCOMM() {

// The requested service has been found earlier (by service discovery) and the service record is
// referenced through the object named: service (of type ServiceRecord)
StreamConnection conn = null;
```

```
// The connection URL is extracted from the service record. Authentication and encryption is disabled. The
// client does not require to be the master of the connection (the false parameter)
String connectionURL = service.getConnectionURL(
ServiceRecord.NOAUTHENTICATE_NOENCRYPT, false);
// A StreamConnection is obtained from the connection URL
try {
conn = (StreamConnection) Connector.open(connectionURL);
} catch (IOException e) {…}
// The conn object is now a working StreamConnection, from which input/output streams can be obtained,
// enabling communication.
}
```

The set-top box Communication agent can use the Extended AT commands to interact directly with the SIM from outside world [4], [5]. The AT commands has to be sent through the RFCOMM-SPP over the Bluetooth link. They can be exploited to write/read data to/from the SIM. Some of the standardised commands are as follows:

- *AT*: to test the connection and if the GSM modem returns 'Ok', it means that the connection between two entities is fine;
- *AT+CMGF= ?*: to check what type of SMS is supported by the GSM modem (0 = PDU mode, 1= text mode) ;
- *AT+CMGW="recipient's phone number"*: to write a message which is intended to be sent to recipient's phone number. The command returns a prompt line to enter the message text. The message is saved in the SIM card and the address of the message is returned after writing the message;
- *AT+CMSS = "address of the message"*: to send a SMS message saved in a specific location in the SIM. The modem then returns a reference number assigned to the sent message;
- *AT+CMGR*: to read the content of a specific SMS record in the SIM and return the record in APDU format;

- *AT+CMGD*: to delete a specific SMS record in the SIM. The command will return an error code upon unsuccessful operation [53];
- *AT+CIMI*: to acquire IMSI, this is used to identify the individual SIM card or active application in the SIM attached to mobile terminal [5].

The following code snippets present how to exchange data over the Serial port emulated in the Bluetooth communication.

```
// Sending AT Command to acquire IMSI number through the Bluetooth Serial port - COM14
   public void sendATCommand (String) throws IOException, NoSuchPortException, PortInUseException, UnsupportedCommOperationException, InterruptedException{
  // Acquiring list of available ports
   Enumeration ports = CommPortIdentifier.getPortIdentifiers();
    while (ports.hasMoreElements()) {
     CommPortIdentifier PID = (CommPortIdentifier) ports.nextElement();
     String portName = PID.getName();
     if (portName.equals("COM14")) {
// Open the Bluetooth Serial Port
       SerialPort SP = (SerialPort)PID.open("Bluetooth Serial Port", 3000);
                        SP.setSerialPortParams(9600,SerialPort.DATABITS_8,SerialPort.STOPBITS_1,_
SerialPort.PARITY_NONE);
         int rosStatus = 0;
// Writing and reading from the Serial port
       OutputStream output = SP.getOutputStream();
       InputStream input = null;
       input = SP.getInputStream();
// Get the IMSI
       String cmd = "AT+CIMI"+ '\r'+'\n';
       byte[] cmdByte = cmd.getBytes();
       byte[] rspByte;
       try {
          output.write (cmdByte);
       } catch (IOException e) {…}
       try {
          int imsi = 0;
          while (imsi!=75){
             imsi = input.read();
             if ((imsi>=48) && (imsi<=57)) IMSI += ((char)imsi);
          }
       } catch (IOException e) {…}    }
```

The SMS protocol can be used as a data bearer between the mobile phone and MHSS for Remote Application Management (RAM) and Remote File Management (RFM) [2]. The MHSS can send a SMS to the SIM directly by setting the SMS protocol identifier (PID) to 0x7F. This method though is practiced by network operators to update and/or install SIM applications, but could be very slow for transferring a large volume of data. The maximum SMS size is 160 characters (each character is encoded using the GSM-7 bits alphabet) and 800 characters in concatenated mode (5 concatenated SMS messages) commonly supported by network operators [72]. However, the concatenation of maximum 255 SMS has been standardised to support the larger payload in the SMS messages [1]. When higher bandwidth is available (3G, UMTS, EDGE), the Bearer Independent Protocol (BIP) can be used to quickly exchange large volume of data with the SIM without any intervention. The RFM is a kind of service that can be transferred via BIP. The BIP compliant phones have to support class 'e' and 'f' commands to perform operations like open, close and get the status of the channel [108]. Further study on the BIP is left to the reader as the focus of the MICAS is on the GSM network, so the SMS is considered as a primary data bearer across the GSM network in the MICAS. The following code snippet shows how to send and receive SMS messages in J2ME using the Wireless Messaging API (WMA).

```
// Check if Wireless Messaging API is present
public static boolean isWMAPresent(){
  try {
     Class.forName("javax.wireless.messaging.MessageConnection");
    return true;
  }
  catch( Exception e ){
    return false;
  }
}
```

```
// Make a connection
public boolean connectSMSServer()
{
  try {
    messageConnection messageConnection =
// Make a SMS connection to a specific phone number
     (MessageConnection)Connector.open("sms://+447833656548");
    messageConnection.setMessageListener(this);
  }
  catch (Exception e) {
  }
}
```

```
// Send text message
public void sendTextmessage(String address,String message)
{
  try {
    //creates a new TextMessage
    TextMessage textMessage = (TextMessage)messageConnection.newMessage(
      MessageConnection.TEXT_MESSAGE, address);
      textMessage.setPayloadText(message);
      messageConnection.send(textMessage);
  }
  catch (Exception e) {…}
}
```

```
// Recieve text message
public void receiveTextMessage()
{
  try {
    Message message = messageConnection.receive();
    if (message instanceof TextMessage)
    {
      TextMessage textMessage = (TextMessage)message;
    }
    else
    {
    // Message can be binary or multipart
    }
  }
  catch (Exception e) {…}
}
```

```
// Notify Incoming Message
public synchronized void notifyIncomingMessage(MessageConnection conn)
{
 // Notify thread of incoming message
 synchronized (this) {notify();}
}
```

```
// Close Connection
public void closeConnection()
{
  if (messageConnection != null) {
    try {
      messageConnection.setMessageListener(null);
      messageConnection.close();
    }
    catch (Exception e) {…}
    }
  }
}
```

There are two ways that the mobile Communication agent can communicate with JavaCard applets resided on a smart card (SIM):

- *The APDU message passing* which requires the Communication agent to know the APDU instructions implemented in the applets on the SIM. The communication will be based on APDU logical data packets complaint with ISO/IEC 7816-3 and 7816-4 standards.
- *The JavaCard Remote Method Invocation (JCRMI)* which is a subset of J2SE RMI distributed object-model. It provides a distributed object model mechanism on top of the APDU-based messaging model. More information about the schemes can be found in the Sun Microsystems' website (java.sun.com/javacard/).

The major APIs which facilitate the communication between JavaCard applets and applications hosted for instance on mobile phones are:

- *The Security and Trust Services API (SATSA) for J2ME*, which extends the security features for the J2ME platform, through the addition of cryptographic APIs, digital signature service and user credential management. The SATSA is based on GCF and also defines the methods to communicate to the SIM card by leveraging the APDU protocol and JCRMI. The SATSA defines the apdu URL scheme and the *javax.microedition.io.APDUConnection* package to support the message passing scheme. It also defines the jcrmi scheme and the *javax.microedition.io.JavaCardRMIConnection* to support JCRMI. The SATSA-JCRMI consists of several packages that can be found in the Sun Microsystems' website (java.sun.com/products/satsa/);
- *The OpenCard Framework (OCF)*, which is a smart card middleware implemented in Java. The framework allows a smart card aware application to access contact/contact-less cards that implement commands using APDUs as defined by ISO/IEC 7816-4, -8 and -9 (www.openscdp.org/ocf/);
- *The JavaCard RMI Client API*, which depends on the OCF for card management and communications. It is used when the JavaCard applet is JCRMI-based (java.sun.com/javacard).

The MICAS is implemented based on the Java platform and as the J2ME is now widely adopted in new devices, the SATSA will be the most popular choice for the mobile Communication agent to use. On the other hand, the APDU protocol is fairly simpler and less resource intensive to implement. Thus, the mobile Communication agent uses the APDU protocol to communicate with the SIM applet(s). In this mode of communication, the mobile Communication agent needs to interpret APDU commands/responses to the conventional format(s) acceptable for JavaCard applet(s) and set-top box MIDlet(s). The SATSA

APDUConnection defines the following methods to interact with the ISO-7816 compliant cards using GCF:

- *enterPIN():* prompts the user for the Personal Identity Number (PIN)
- *exchangeAPDU():* exchanges an APDU with the SIM and it block until receiving an APDU response;
- *getATR():* returns the Answer-To-Reset (ATR) message sent by the SIM in the response to the reset operation;

As SATSA is based on the GCF, the *Connector.open()* method can be used to open a GCF connection. One of the arguments to *Connector.open()* is a URL that indicates the type of connection to create. The CLDC GCF defines the format of the SATSA URL as: *protocol: [slotID]; AID*. The *protocol* is either *apdu* for an APDU-based connection or *jcrmi* for a JCRMI-based connection. The *slotID* is the number that indicates the slot into which the card is inserted. It is optional and by default 0. The *AID* is the application identifier for a SIM card application. It is a string of 5 to 16 hexadecimal byte values separated by periods; for example, "A0.0.0.67.4.7.1F.3.2C.3". The following code snippet shows how the Communication agent opens and closes an APDUConnection.

```
public void doAPDUConnect() {
try {
// Create an APDUConnection
String url = "apdu:0;AID=A1.0.0.67.4.7.1F.3.2C.5";
APDUConnection ac = (APDUConnection) Connector.open(url);

// Send a command APDU and receive a response APDU
byte[] responseAPDU = ac.exchangeAPDU(commandAPDU);

// Close connection
ac.close();
} catch (IOException e) {…}
}
```

7.2.1.2 Security Layer

The Security agents are responsible to ascertain that the confidentiality, integrity and availability (known as the CIA Triad) criteria are guaranteed across the MICAS platform.

The authentication, authorisation and accounting (AAA) can be defined as a security protocol in the MICAS. The mutual authentication process determines who are involved in an interaction. An entity can be identified using a digital identity and credential. In the case that a mobile phone is involved, the IMSI number (phone number) and Bluetooth address can be used to identify the mobile phone. In the case that a set-top box is involved, the STB-ID (or MAC address) and its Bluetooth address can be used for the authentication. The mobile phone can also authenticate the MHSS server using an Operator-ID and his associated credential, which can be burnt into the SIM card by its manufacturer. In general, the authorisation ensures that the entity has adequate privilege to access a specific service. The authorisation can be restricted to different criteria such as time, location, number of requests to use, etc. The authorisation depends on the authentication but it concerns about the access permission. It ensures that only a trusted device (set-top box) can use the functionalities that the viewer's mobile phone offers. The authorisation process at this level is different from the Conditional Access measures, though together they will guarantee that only legitimate viewers can enjoy the MICAS services. The accounting enables the service provider to track the consumption and ensure that bills are issued correctly. The accounting process takes place at the head-end where the MHSS forwards consumption reports to the billing system. It is especially essential for handling the account for impulse viewers by keeping their identity, service requested and service schedule.

In addition to the triple-A processes, cryptographic techniques can be employed to provide higher security level. These techniques can include but are not limited to message digests (hash functions), digital signature and encryption. They can be also used to establish integrity, authenticity and non-repudiation.

Moreover, the session management can be used to prevent any repetition in security processes, for instance when the communication link is disconnected. The session management can be used to keep track of activities and session state. The session state is attributed by a session identifier (i.e. session ID, encryption key), which is created upon initiating any connection request. It shall be kept secret and frequently updated during transactions.

Fig. 51 presents some attributes and functions that can be defined in the general Security agent class from which set-top box (STB), mobile and MHSS can extend required functions.

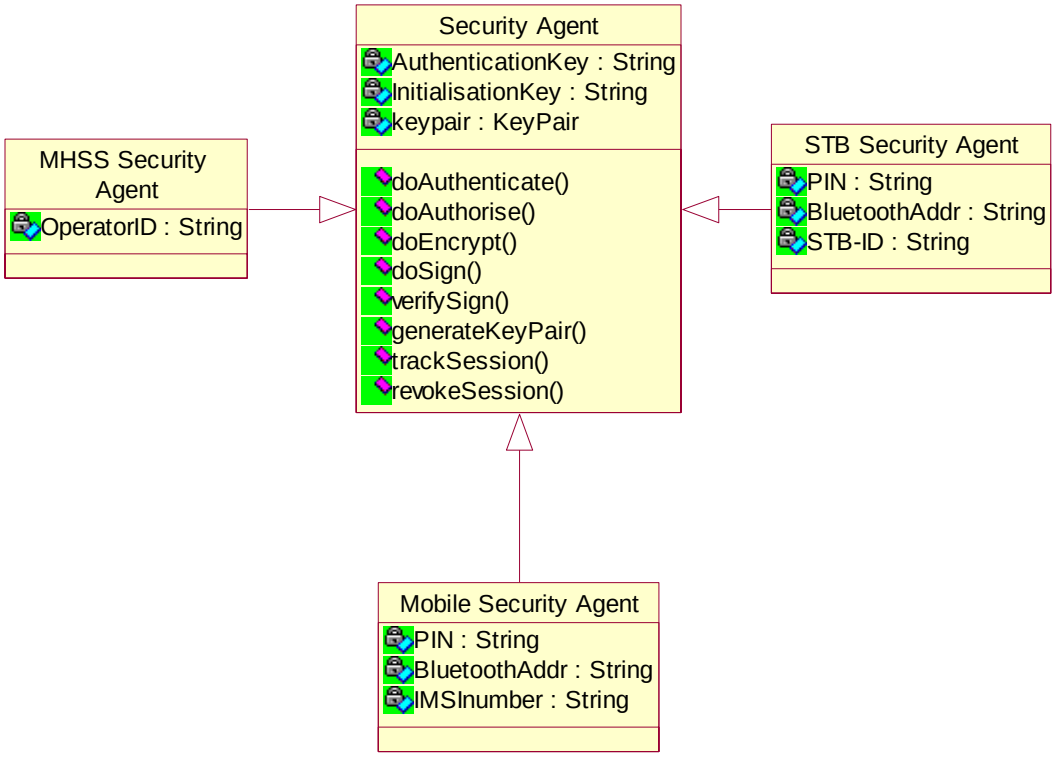


Fig. 51: The Security agent class diagram

In addition to the link-level security, the service-level security defined by developers can be used to enforce the most appropriate security mechanism(s) in the Bluetooth domain [66]. In the GSM domain, methods like the Extensible Authentication Protocol for GSM Subscriber Identity [95] can be used for authentication and session key distribution. Moreover, tougher security measures can be enforced by adopting sophisticated methods within the GSM and Bluetooth domains to ensure authenticity and non-repudiation. Nonetheless, ultimately the security protocol can be implementation dependent. It means that each service provider can have his own end-to-end security solution(s) based upon his security priorities. However, the interoperability and service availability has to be guaranteed when new Security agents are deployed to the field.

The set-top box and mobile Security agents can authenticate each other using a symmetric cryptographic algorithm, as defined in the Bluetooth specification [66]. The authorisation process will ensure that only trusted devices can access to services. The authorisation depends on the authentication process, which is called bonding, depends on a shared authentication key. If the devices are not sharing any authentication key, initialisation and authentication keys shall be generated during the pairing process. The initialisation key depends on a user input (PIN code or passkey), random number and Bluetooth physical address of one of the devices. The PIN code is used to generate a 128-bit secret key shared between the set-top box and mobile phone. The initialisation key is used for the encryption of data exchanged between parties to create the authentication key and it is thereafter discarded. The authentication key is based upon a random number and Bluetooth physical address. The authentication key then can be saved at both sides for a swift authentication at the bonding phase with no need to enter to the pairing process.

The authentication (pairing and bonding), confidentiality (encryption for instance via hardware support in Bluetooth module) and authorisation (trusted devices) security measures have already implemented in the Bluetooth technology. The integration and non-repudiation can be also added if the digital signature and hashing functions are implemented. The implementation of the Bluetooth security modes is not in the scope of the thesis, though some J2ME functions that enforce the authentication and authorisation in the Bluetooth communication are briefly introduced.

The Bluetooth security can be specified while the Communication agents attempt to open a connection string by setting optional parameters of the *Connector.open()* method. Parameters in the connection string can be used to setup the security measures (i.e. authentication, encryption, authorization and master/slave role switch) at the time that the connection is established. As mentioned, the authentication is based on the PIN code entered at both Bluetooth devices. The PIN code is used to generate a 128-bit shared key. The encryption depends on the authentication and as such only certain combinations of parameter setting are valid in the connection string.

- *authenticate = true* and *encryption = true*
- *authentication = true* and *encryption = false*
- *authentication = false* and *encryption = false*
- *encryption = true* is interpreted as equivalent to authenticate = true

The implementation of the authorisation involves prompting the server user to allow the client device to access the service. It may also require consulting the list of 'trusted' devices registered in the server device. The trusted devices are fully authorised to access services made available in the server device. Similar to the encryption, the authorisation depends on the authentication, as such following security settings are recognised as valid combinations in the connection string:

- *authenticate = true* and *authorisation = true*
- *authentication = true* and *authorisation = false*
- *authentication = false* and *authorisation = false*
- *authorisation = true* is interpreted as equivalent to authenticate = true

It is worthwhile noting that not all Bluetooth devices support the abovementioned security settings. Even if they are supported, it is possible to set the security settings using the BCC. Hence, the *BluetoothConnectionException* may be thrown by the *Connector.open()* method, if the security settings are not supported or conflict with the current security settings for the device.

The following code snippets present how security optional parameters (i.e. authentication, encryption) can be defined in the connection string set between server and client devices and over a serial port connection.

```
// Setting up a Serial Port connection Server
public void SerialPortServer () {

// Define the connection string used by this serial port server. The Server uses optional
// parameters to request that connections to this service are authenticated and encrypted. The
// default value ("false") will be used for authorize and master.

String serversConnString =
"btspp://localhost:3B9FA89520078C303355AAA694238F07; authenticate=true;encrypt=true";

try {
StreamConnectionNotifier notifier =
(StreamConnectionNotifier)Connector.open(serversConnString);

// Wait for a client to connect. If the client cannot be authenticated or if the link to the client
// cannot be encrypted, the connection attempt is refused by the API implementation without the
// server application even being aware of it.

StreamConnection rfconn =
(StreamConnection)notifier.acceptAndOpen();
} catch (IOException e) {…}
….}
```

```
// Setting up an Serial Port connection Client to send an encrypted message
public void SerialPortClient (String encryptedMsg) {

// When connecting to a server using Connector.open(), the client uses optional parameters in the
// connection string to set up authentication and encryption.

OutputStream os = null;
StreamConnection con = null;
ServiceRecord record;

// Use the SDP Client methods to obtain a ServiceRecord from a SDP Server.
// Define a String requesting that this client's connection to the service described by record be
// authenticated and encrypted.
// The false argument means that the client does not need the master role.

String clientsConnString =
record.getConnectionURL(ServiceRecord.AUTHENTICATE_ENCRYPT, false);
try {
con = (StreamConnection)
Connector.open(clientsConnString);

// If we reach this point, then the server device has been authenticated, and all communications between the
// client device and this server device over con are being encrypted.

os = con.openOutputStream();

// Send encrypted data to the server device
os.write(encryptedMsg.getBytes());
os.close();
} catch (BluetoothConnectionException e1) {
// If the server cannot be authenticated or the connection cannot be encrypted then this exception
// will be thrown.
return;
} catch (IOException e) {…}
finally {
if (con != null) {
try {
con.close();
} catch (Exception e) {…}
}
}
```

The *javax.bluetooth.RemoteDevice* class defines similar security methods to those defined in the CLDC *javax.microedition.io.Connector* class. However, the RemoteDevice security methods can be enforced at any time by set-top box and mobile phone Security Agents. Some of these methods take an instance of *javax.microedition.io.Connector* as an argument. This generic argument type is used in the methods so that they can apply to serial port connections, RFCOMM connections and OBEX connections. The following code snippets present how to add/remove security settings (i.e. authentication, encryption) to an already established serial port connection and send data across.

```
// Encrypting an unencrypted connection
// This function can be implemented at both client and server sides
public void doEncrypt() {
String encryptedMsg = "This message will be sent encrypted";
String clearMsg = "This message will be sent unencrypted";
OutputStream os = null;
StreamConnection con = null;
RemoteDevice remDev;
ServiceRecord record;
// Use the SDP client methods to obtain a ServiceRecord from an SDP server.
// Create a connection string requesting no security.
String clientsConnString =
record.getConnectionURL(ServiceRecord.NOAUTHENTICATE_NOENCRYPT,
false);
try {
// Establishing a connection to a service without requesting any Bluetooth security features.
con = (StreamConnection)
Connector.open(clientsConnString);
remDev = RemoteDevice.getRemoteDevice(con);
if (!remDev.isEncrypted()) {
// The connection to remDev is not currently encrypted, so authenticate and then turn on encryption
// The authenticate() is redundant as the encrypt statement ensures that the connection is authenticated
// before beginning the encryption.
if (!remDev.authenticate() || !remDev.encrypt(con, true)) {
// quit since unable to turn on encryption
return;
}
```

```
}
// At this point, the server device has been authenticated, and all communications
// between the client device and the server device over con (or any other connection) are being encrypted.
os = con.openOutputStream();
sendData(os, encryptedMsg, clearMsg);
}
}
```

```
// Send encrypted/clear data to the server device
void public sendData (Output Stream os , String encryptedMsg, String clearMsg) {
Try {
os.write(encryptedMsg.getBytes());
// Withdraw the request for encryption
if (remDev.encrypt(con, false)) {
// Send unencrypted data to the server device since successful in turning off encryption.
os.write(clearMsg.getBytes());
} else {
// Send encrypted data to the server device since unable to turn off encryption.
os.write(encryptedMsg.getBytes());
}
os.close();
} catch (IOException e) {…} finally {
if (con != null) {
// Closing the connection.
try {
con.close();
} catch (Exception e) {…}
}
}
}
```

In addition to the above security measures defined in the JABWT package, the SATSA API can be also satisfy integrity, non-repudiation and authenticity. The SATSA defines a security element (SE) which can be implemented in software or hardware platforms. It defines security related packages namely SATSA-PKI and SATSA-CRYPTO which can be used in the MICAS to improve security in both Bluetooth and GSM domains. The former generates the digital signature from the SIM card and the latter provides basic support for encryption, computing

digests, verifying signatures and accessing public keys without interacting with the SIM card.

The SATSA-PKI generates a signature based on a key pair (a public and a private key) and digital identity certificate. The public key is freely distributed whereas the private key is stored on the SIM Card and used to sign a message. The public key is usually tied to a user using the certificate issued by a certificate authority. The certificate is associated to the user information like name, address, etc. The package *javax.microedition.pki* consists of two following classes: *UserCredentialManager* and *UserCredentialManagerException*. The former provides methods for managing a user's certificates. The class allows adding certificates, removing certificates and generating requests for new certificates. In this context, certificates represent keys and link keys to specific people. keys are stored on the SIM card permanently and it is not possible to add, change, or remove them. The *javax.microedition.securityservice* package consists of *CMSMessageSignatureService* class that provides digital signature given the availability of the digital identity certificate and key pair. The *CMSMessageSignatureService* ensures the integrity and non-repudiation in transactions via *sign()* and *authenticate()* methods. The signing options supported are enumerated as follows.

- *SIG_INCLUDE_CONTENT:* It indicates that the formatted signature should include the content that was signed (an opaque signature). The absence of this option tells the implementation to create a detached signature.
- *SIG_INCLUDE_CERTIFICATE: It* controls whether the signer's certificate is included in the formatted signature.
- *Combined option:* The above options can be combined using the bitwise OR operator (|).

A call to authenticate() or sign() returns a formatted digital signature, which is essentially the signature itself plus information about the signer and the data that was signed. The CMSMessageSignatureService produces formatted digital signatures that conform to the Cryptographic Message Syntax (CMS) [93], [94]. The following code snippets present the syntax of sign() and authenticate() methods which might be used in the implementation of doAuthenticate() method.

```
// Sign a string message using options: SIG_INCLUDE_CONTENT or SIG_INCLUDE_CERTIFICATE
// and identity certificate. If it fails, a message is shown to the user
public static final byte[] sign(String MsgToSign, int options, String[] caNames, String
PromptingMsg)
throws CMSMessageSignatureServiceException, UserCredentialManagerException
```

```
// Authenticate a string message using options: SIG_INCLUDE_CONTENT or
// SIG_INCLUDE_CERTIFICATE and identity certificate. If it fails, a message is shown to the user
public static final byte[] authenticate(String MsgToAuthenticate, int options, String[] caNames,
String PromptingMsg)
throws CMSMessageSignatureServiceException, UserCredentialManagerException
```

```
// Authenticate a byte  message using options: SIG_INCLUDE_CONTENT or
// SIG_INCLUDE_CERTIFICATE and identity certificate. If it fails, a message is shown to the user
public static final byte[] authenticate(byte[] byteArrayToAuthenticate, int options, String[]
caNames, String PromptingMsg)
throws CMSMessageSignatureServiceException, UserCredentialManagerException
```

The classes and interfaces of SATSA-CRYPTO are located in the same packages as the J2SE platform JCE: *java.security*, *java.security.spec*, *javax.crypto*, and *javax.crypto.spec*. The SATSA-CRYPTO provides an API for three cryptographic tools as follows.

- *Ciphers - javax.crypto.Cipher* class: to encrypt and decrypt data using a mathematical algorithm such as Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES) and RC4. Other factors required to be specified in the ciphering are key type (symmetric or

asymmetric – see *java.security.key* and *java.security.spec.keySpec* interfaces), stream or block ciphers, mode and padding schemes associated with the block ciphers [17].

- *Message digests:* to create fingerprints of data to identify communication errors. The message digest algorithm used in SATSA-CRYPTO is SHA-1;
- *Digital signatures - java.security.Signature class:* to verify data integrity, using a private key. They are like message digests but much harder to forge. In SATSA-CRYPTO, A Signature object can be used to generate and verify digital signatures. It resembles the *MessageDigest* except that it is initialised like Cipher. The signature algorithm can be, among others, the DSA, using DSA and SHA-1. The DSA algorithm using the SHA-1 message digest algorithm can be specified as *SHA1withDSA*. In the case of RSA, there are multiple choices for the message digest algorithm, so the signing algorithm could be specified as, for example, *MD2withRSA*, *MD5withRSA*, or *SHA1withRSA*. The algorithm name must be specified, as there is no default.

The following code snippets show how to implement the encryption, signing, verification and key pair generation functions using the *java.security* package in a MIDP application.

```
// Encrypt using symmetric cipher DES and asymmetric cipher RSA
public void doEncrypt (String mode, String text, keyPair keypair) {
byte[] plaintext = text.getBytes();
…
If ( mode.equials("DES/ECB/NoPadding")) {
// Create a cipher based on the DES algorithm in Electronic Code Book (ECB) mode, with no padding. The
// cipher is initialized for encryption using the secret key.
byte[] ciphertext = new byte[];
// Create a cipher instance of the DES/ECB/NoPadding algorithm
Cipher cipher = Cipher.getInstance("DES/ECB/NoPadding");
// Get the private key
```

```
Privatekey key = getPrivate (keypair);
// Initialise the cipher for encryption process
cipher.init(Cipher.ENCRYPT_MODE, key);
// Feed data to the cipher using update() method
// Send the last data to the cipher using doFinal() method
int count = cipher.doFinal(plaintext, 0, plaintext.length, ciphertext, 0);
…}
elseif ( mode.equials("DES/CBC/NoPadding")) {
// DES cipher in Cipher Block Chaining (CBC) mode, in which the previous block of cipher text is
// combined with the current block of plaintext before encryption. For the first block of plaintext,
// there is no previous cipher text block, so an initialisation vector is needed.
….
// Define an initialisation vector
byte[] ivBits = {
(byte)0x01, (byte)0x02, (byte)0x03, (byte)0x04,
(byte)0x05, (byte)0x06, (byte)0x07, (byte)0x08
};
byte[] ciphertext = new byte[];
// Get the private key
Privatekey key = getPrivate (keypair);
// Pass an initialization vector to a cipher using one of its init() methods.
IvParameterSpec iv = new IvParameterSpec(ivBits, 0, ivBits.length);
// Create a cipher instance of the DES/CBC/NoPadding algorithm
Cipher cipher = Cipher.getInstance("DES/CBC/NoPadding");
// Initialise the cipher for encryption process
cipher.init(Cipher.ENCRYPT_MODE, key, iv);
// Feed data to the cipher using update() method
// Send the last data to the cipher using doFinal() method
int count = cipher.doFinal(plaintext, 0, plaintext.length, ciphertext, 0);
…}
elseif ( mode.equials("RSA")) {
// Encrypt data using the public key of an RSA key pair.
// keyFactory class is used to extract a public key from an encoded representation.
byte[] ciphertext = new byte[128];
Public key publickey = getPublic (keypair);
Cipher cipher = Cipher.getInstance("RSA");
cipher.init(Cipher.ENCRYPT_MODE, publickey);
int count = cipher.doFinal(plaintext, 0, plaintext.length, ciphertext, 0);
…}
…
}
```

```
// Verify a signature created by SHA-1 and RSA algorithms
public static boolean verifySign (byte[] kData, byte[] KSignature, , String algorithm, Publickey publickey) {
byte[] publickeyBits;
If (algorith.equals("SHA1withRSA")) {
// Create a Signature object from message digest algorithm SHA-1 and encryption algorithm RSA
Signature signature = Signature.getInstance("SHA1withRSA");
// Initialise Signature for verification using a public key
signature.initVerify(publickey);
// Process the byte data that is to be verified
signature.update(kData, 0, kData.length);
// Verifying signature on all updated bytes
boolean pass = signature.verify(kSignature);
return pass;
}
…
}
```

```
// Sign data using a Private key and SHA1 with DSA algorithms
public static byte[] doSign(byte[] data, Privatekey key) throws Exception {
Signature signer = Signature.getInstance("SHA1withDSA");
signer.initSign(key);
signer.update(data);
return (signer.sign());
}
```

```
// Generate a pair of public and private keys
public static keyPair generatekeyPair(long seed) throws Exception {
// Generate a key pair (public and private keys) using the Data Signature Algorithm (DSA) algorithm
keyPairGenerator keyGenerator = keyPairGenerator.getInstance("DSA");
// The DSA usually uses Hash functions from the SHA family
// Create a random number using algorithm (SHA1PRNG) and package provider (SUN)
SecureRandom rng = SecureRandom.getInstance("SHA1PRNG", "SUN");
rng.setSeed(seed);
// In the DSA algorithm the key size corresponds to the module size which is 512,768, 1024
keyGenerator.initialize(1024, rng);
return (keyGenerator.generatekeyPair());
}
```

7.2.1.3 Conditional Access (CA) Layer

The role of the CA agents depends on the implementation scheme. The MHSS CA agent can communicate with the set-top box CA agent and mobile CA agent

respectively through broadcasting and GSM channels. The MHSS CA agent (CA Manager) can transfer Security Objects (i.e. CA-related functions, credentials) either directly or through an intermediary to each CA agent. The intermediary can be either the mobile CA agent or set-top box CA agent. If the broadcasting medium is solely used to transfer security objects, the set-top box CA agent will be an intermediary who transfers requisite security data to the mobile phone over Bluetooth channel. This scenario is rather insecure due to the broadcasting of Security Objects to all the receivers in the field. Another scheme is to use the mobile CA agent as an intermediary between the MHSS CA manager and set-top box CA agent. The latter will be more secure due to the GSM security features [7], [8] and point-to-point connection established between the MHSS and SIM. However, there may be some concerns regarding the exposure of Security Objects over the Bluetooth channel. Hence, the easier and safer scheme, which is considered herein, is to employ both broadcasting and GSM channels to deliver a confident CA mechanism to the receiver-end. In this case, the MHSS CA agent will broadcast the set-top box CA agent and/or CA-related credentials (i.e. EMM, ECM) to set-top boxes deployed in the field using an object carousel. It also loads the mobile CA agent and/or CA credentials (i.e. MK) on the SIM card using the Over-the-Air technology in the GSM network.

It is worthwhile noting that generating conditional access management and control messages (EMM and ECM) and broadcasting DVB-J applications like set-top box CA agent lay into the responsibility of the Subscriber Management Subsystem, Subscriber Authorisation Subsystem and object carousel. Therefore, the MHSS CA agent functionalities considered here may overlap with CA-related functions defined in the said entities. Nevertheless, the MHSS CA agent is generally referred to the conditional access mechanism implemented at the head-

end regardless of its physical implementation. Fig. 52 presents a brief list of functions that can be defined in the CA layer in the MICAS protocol stack.

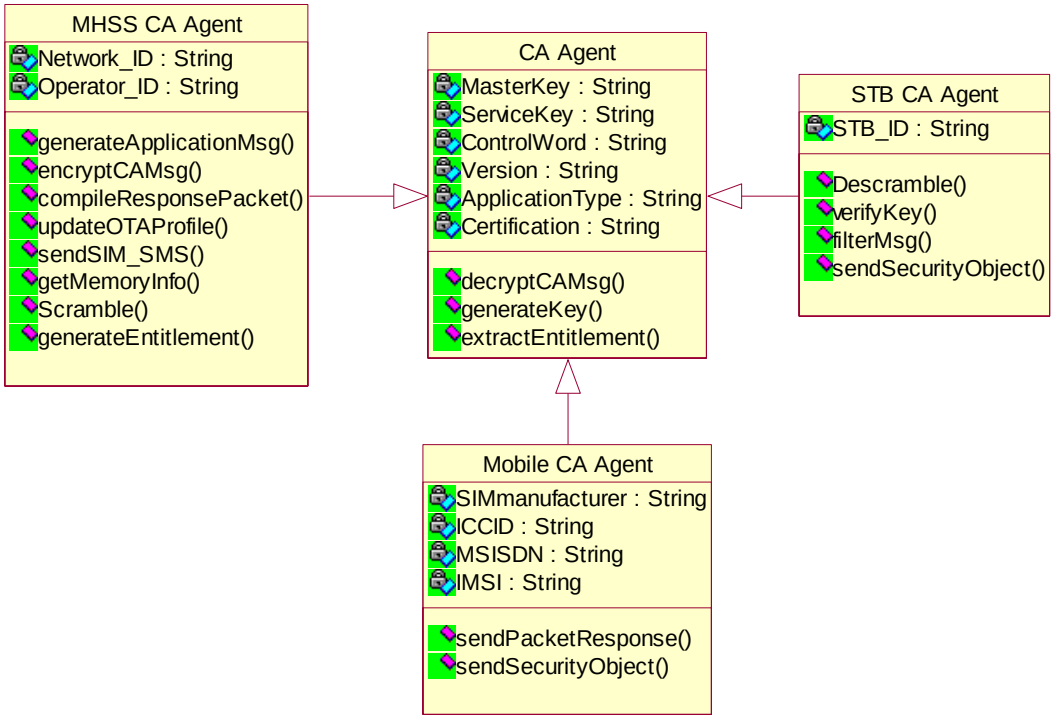


Fig. 52: The CA Agent class diagram

The service provider can use the OTA technology to update or change data in SIM card or Universal Integrated Circuit Card (UICC). Therefore, the service provider can introduce new services to modify content of SIM cards in a rapid and cost-effective way without having to reissue new cards. The technology is based on the client-server architecture wherein the MHSS CA agent shall send the Service-Requests (application message) to an OTA Gateway that transforms the requests into a Short Messages (SMS) or concatenated messages to be sent to a SIM card in the point-to-point or bulk of SIM cards in the cell broadcast mode. The Service-Requests may contain a secured command packet (i.e. LOAD, MODIFY, ACTIVATE FILE, DEACTIVATE FILE), the subscriber targeted and data to perform the service. The service provider can set the Security Parameter

Indicator (SPI) in the command packet to get a direct acknowledgement from the recipient (SIM card). The response will be sent back within a secured response packet which conveys a Status Code indicating if the packets have been received intact. Similarly, the service provider can retrieve data (application) from the SIM card(s) indicating a viewer's behaviour for security or personalisation purposes [2].

At the moment, in the mobile network, the main transport bearer is the SMS bearer but in a near future, the Circuit Switched Data (CSD) or GPRS can be used in conjunction with Card Application Toolkit – Transport Protocol / Bearer Independent Protocol (CAT-TP/BIP) or JSR-177 mechanisms to perform the OTA operations. The implementation of the OTA Gateway is not in the scope of this thesis, although some underlying technologies in this context will be discussed as follows.

The OTA Gateway in the mobile network (i.e. GSM network) receives Service-Requests through a Gateway API that will indicate the actual card to perform the requested operation (i.e. modify, update, activate). In fact, the OTA Gateway shall use a card database that indicates for each card the card manufacturer vendor, integrated circuit card identification number (ICCID), IMSI and MSISDN. The second step is to format the requested service into a message that can be understood by the recipient card. To achieve this, the OTA Gateway has a set of libraries that contain the formats to use for each brand of smart cards. The OTA Gateway then formats the message differently depending on the recipient card. The third step is to send a formatted message to the SMSC using the right set of parameters [2]. Then, the OTA Gateway issues as many SMS as required to fulfil the Service-Request. In this step, the OTA Gateway is also responsible for the integrity and security of the process. Regarding the OTA services, the mobile equipment has to be SIM Toolkit compliant.

It is worthwhile noting that it is not mandatory for smart cards to support OTA specifications, but the majority of existing cards are supporting the secured packets over SMS for Remote File Management and application download. Only very low cost cards may not support the OTA. The Remote Application Management (RAM) is generally supported by JavaCards. Nevertheless, a JavaCard needs to be personalized with an "OTA profile" to be updated via the OTA. The "OTA profile" enables the UICC to retrieve and execute the OTA command sent by the OTA Gateway.

The SMS messages with protocol identifier shall be set to "SIM DATA DOWNLOAD" to be delivered by the ME to the SIM card (i.e. ENVELOPE or UPDATE RECORD commands) [6]. When the GSM application receives the secured command packets, it shall call the OTA layer to check the messages. Each secured packet may contain one or more APDUs commands dedicated to RFM or RAM or SIM Toolkit.

The RFM enables to execute Elementary File (EF) management commands (i.e. SELECT, UDPATE BINARY, UPDATE RECORD, SEEK, VERIFY PIN, READ BINARY, READ RECORD, GET RESPONSE). The RAM can handle series of operations such as package loading, applet installation, package (applet) removal, applet parameters retrieval, etc. For instance, the package loading process allows the service provider to load new packages onto the SIM (or UICC). The service provider manages the loading of a package through a loading session with the card. The loading session may consist of a sequence of commands such as INSTALL and LOAD commands. Depending on the applet size, several SMS might be used for the package loading. The RAM fulfils these operations by executing applet management input and output commands (i.e. LOAD, INSTALL, DELETE, PUT KEY, SET STATUS, GET STATUS, GET DATA) [9].

The memory size is an important factor that has to be taken into account while adding data onto SIM card during the OTA operations. The OTA Gateway is aware of this information during the configuration and provisioning of the card. Furthermore, using Open Platform commands and OTA SMS, the OTA Gateway can retrieve the memory information of each card in the field [2], [43].

In addition to the GSM-based interactions using the OTA technology, the MHSS may use the broadcasting medium (i.e. cable, satellite, terrestrial, etc.) to deliver CA agent (CA-related APIs) to a specific set-top box in the field. The set-top box CA agent shall be downloaded on the viewer's set-top box when the receiver is connected to the service provider's network for the first time. The CA agent shall be started automatically when the receiver starts, until it is upgraded or the receiver is connected to a different network. The CA agent can be broadcast as an unbound application in OCAP-compliant network or a stored application in MHP-compliant network. It can be developed as an Xlet (applet for consumer systems) which forms the basis for all systems based on JavaTV including Multimedia Home Platform (MHP) and OCAP. The Xlet interface can be used by the service provider to control the agent's life-cycle.

The interface for an Xlet is defined in the *javax.tv.xlet* package. It provides interfaces used by applications and the application manager to communicate. This package defines two entities: the *Xlet* and the *XletContext*. The central function of this set of interfaces is to model and manage the states an application can be in. The Xlet is an interface that must be implemented by the primary class of the CA agent. When the set-top box CA agent is loaded, one instance of this primary class is created. The set-top box CA agent is controlled via method calls on this instance. Methods of Xlet are used by the application manager to deliver state change requests to the agent. The set-top box CA agent is provided with an instance of XletContext to deliver state change notifications to the application

manager. Each Xlet receives its own instance of XletContext. The following is the description of the methods defined in the Xlet interface.

```
public interface Xlet {
// Initialisation: Start an Xlet automatically (by service provider) or manually (by user)
  public void initXlet(XletContext ctx) throws XletStateChangeException;
// Execution: moving the Xlet from paused state into the Started state
  public void startXlet() throws XletStateChangeException;
// Application manager may change the Xlet state from Started state to Paused state. This may happen
several time during the execution
   public void pauseXlet();
// Termination: the user or service provider can kill the Xlet and move it to the Destroyed state.
// The application will remain in this state temporarily before moving back to the Not Loaded state.
   public void destroyXlet(boolean unconditional) throws XletStateChangeException;
}
```

The set-top box CA agent needs to implement the Xlet interface in conjunction with the functions required to fulfil the conditional access system. The CA-related functions can benefit from the Java Cryptography Architecture (JCA) and Java Cryptographic Extension (JCE) APIs. The security-APIs are part of the *java.security* package in the J2ME CDC profiles (JSR-216: personal profile; JSR-217: personal basis profile). However, the service provider may implement proprietary cryptographic algorithm (symmetric or asymmetric encryption algorithm) to encode/decode CA messages. The (de)scrambler can be also implemented in a software package (i.e. FreeDec) stored securely on the persistent storage (i.e. flash memory) in the set-top box as long as it is connected to the service provider's network [115].

The OCAP object carousel or MHP Digital Storage Media-Command and Control Object Carousel (DSMCCObject; *dvb.org.dsmcc* that extends *java.io.File*) broadcast multimedia applications to set-top boxes deployed in the field. In the MHP, applications can be loaded asynchronously from the carousel. The *AsynchronousLoadingEventListener* is notified when the file is fully loaded. In

order to instruct set-top boxes on when and how to launch applications, the signalling tables are included in the transport streams. The application signalling table describes bound and unbound applications and enables the service provider to remotely control the behaviour of each application. It is also used to ensure that only trusted applications are run in the set-top box (signing procedure). Currently, the Globally Executable MHP (GEM), MHP and OCAP standards use the Application Information Table (AIT) to describe bound applications or eXtended AIT (XAIT) to describe stored or unbound applications. The application can also be described in an XML format understandable to receivers [77]. The CA agent is an unbound application since it is not bounded to any services therefore in OCAP-compliant systems it needs to be described in an XAIT table. Nevertheless, the following description fields have least to be specified for each unbound (stored) applications [82].

Application name	*CA agent*
Application version	*v.1.0*
ID of application and associated organisation	*Application ID = 1, Organisation ID = 1; the combination of the application ID and organisation ID is unique to every application*
Application status	*AUTOSTART; in MHP the status can be AUTOSTART, PRESENT, DESTROY, KILL, REFETCH, REMOTE*
Application type	*Java; it can be of other sources like HTML*

In addition to the XAIT, the Conditional Access Table (CAT) needs to be modified to determine the used encryption method(s), conditional access management and entitlements (i.e. EMM). In a basic model, the EMM is decrypted using the MK delivered through the GSM network. The EMM itself contains the SK to decrypt the ECM. Here, higher security can be applied if the CAT conveys key information that together with key information delivered through the GSM form the MK. In Short, as the Security Objects can be delivered

from two separate media (broadcasting and GSM networks), the set-top box CA agent can use them to authenticate senders and also verify the integrity of the key information (i.e. MK, SK).

7.2.1.4 Application Layer

The highest level in the MICAS protocol stack is the Application layer. It handles all interactions that may take place between a viewer and set-top box (local interaction) or between a viewer and service provider (interaction over return channel). Use cases like Set-up Connection or Set Multi-room Subscription previously explained are mainly deal with the local interactions. This is while use cases such as Sign-up, Amend Subscription and Security Check require interactions between a viewer and service provider over the return channel (i.e. GSM). In both cases, native or stored (unbound) applications, which are broadcast and/or downloaded to a set-top box, will be used to handle interactions.

The range of TV applications that can be downloaded to the viewers' set-top boxed is rapidly increasing thanks to the JavaTV APIs and interactive standards (i.e. MHP, OCAP). Nevertheless, the MICAS platform employs technologies to enable TV consumers and service providers to readily manage their accounts and interests. Therefore, the main use cases (i.e. Sign-up, Subscribe Follow Me) defined in the MICAS are chiefly considered hereinafter.

In the MICAS, some APIs (i.e. native applications) need to be developed by set-top box manufacturers to provide viewers with appropriate user interfaces to settle their subscription request(s). Once the set-top box is connected to a service provider's network, the rest of APIs (i.e. unbound applications) need to be downloaded by the service provider to the set-top box. Such APIs are responsible to fulfil specific tasks such as security or personalisation-related tasks. The

unbound APIs are categorised as assumable modules in the OCAP-compliant systems, which are vendor-specific and usually taken over by the Monitor Application in the set-top box. The Monitor Application is downloaded from service providers (network operators) and stored on receivers' persistent memory. It takes over some functionalities of the Executive Module such as navigation, EPG functionalities, control over downloaded applications, handling CA messages, customising many aspects of the user experience, etc. Such functionalities lay into the Navigator's specification within MHP-compliant systems [77].

In the MICAS, it is assumed that each set-top box has a built-in navigator as of MHP-compliant systems or Monitor Application or Execution Engine as of OCAP-compliant systems. The navigator will enable a viewer to control the set-top box and set-up a Bluetooth connection between the set-top box and his/her mobile phone. It also displays a list of available service providers and their associated channels (services) as advertised by EPG, MPEG-2 and DVB-Service Information (SI) tables. Thus, the viewer can browse the list of programmes and build up his subscription request(s). After fulfilling the subscription process, the service provider may download a tailored navigator and/or module(s) (i.e. for handling the CA messages) to the viewer's set-top box.

The data conveyed in transport streams (TS) as MPEG-PSI and DVB-SI tables generally describe the network (Network Information Table, network_ID), multiplexes (TS_ID, network_ID, Programme Association Table), services (service_ID, Programme Map Table) and associated components (component_tag, Programme_ID) included in elementary streams. Such data together with EPG services provide all programming information and broadcasting content in real-time. However, in the MICAS, additional data are required to enable viewers to subscribe on-line through their set-top boxes. Such

extra data, which is called Subscription Association Table (SAT) hereinafter, shall advertise available service providers and their packages (products) to which TV consumers can subscribe. The subscription viewing packages can be played out in the form of XML files wherein the network, service provider and its packages are described. The navigator in the set-top box needs to parse the XML file and display subscription data in a user friendly fashion. Fig. 53 exemplifies a SAT table by identifying some fields and their associated values displayed to the viewer. It specifies the service provider, its service policies and subscription packages to which a viewer can subscribe through his set-top box. Each package is identified by an identifier (ID), a name, tariff and may include various packs. Each pack has also an ID, name, tariff and a bouquet of TV channels. Each TV channel has also an ID, name and tariff. Therefore, a viewer can subscribe to a package as for subscription services or purchase a programme or channel as for Per-Per-View (PPV) or Video-on-Demand (VoD) services. When a viewer selects the Sign-up service under the Service menu in the set-top box, the SAT shall be displayed for instance in a cascading form as shown below. The viewer will be able to build up his subscription request composed of one or more package(s) or pack(s) or channel(s).

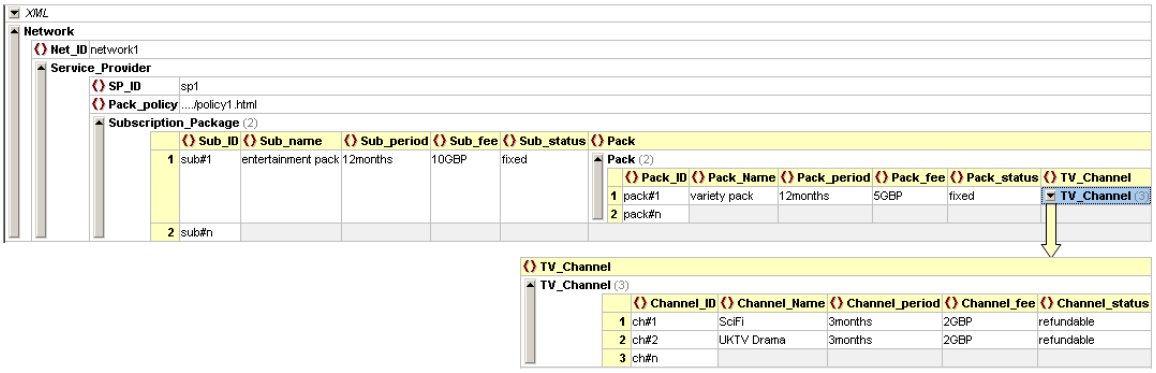


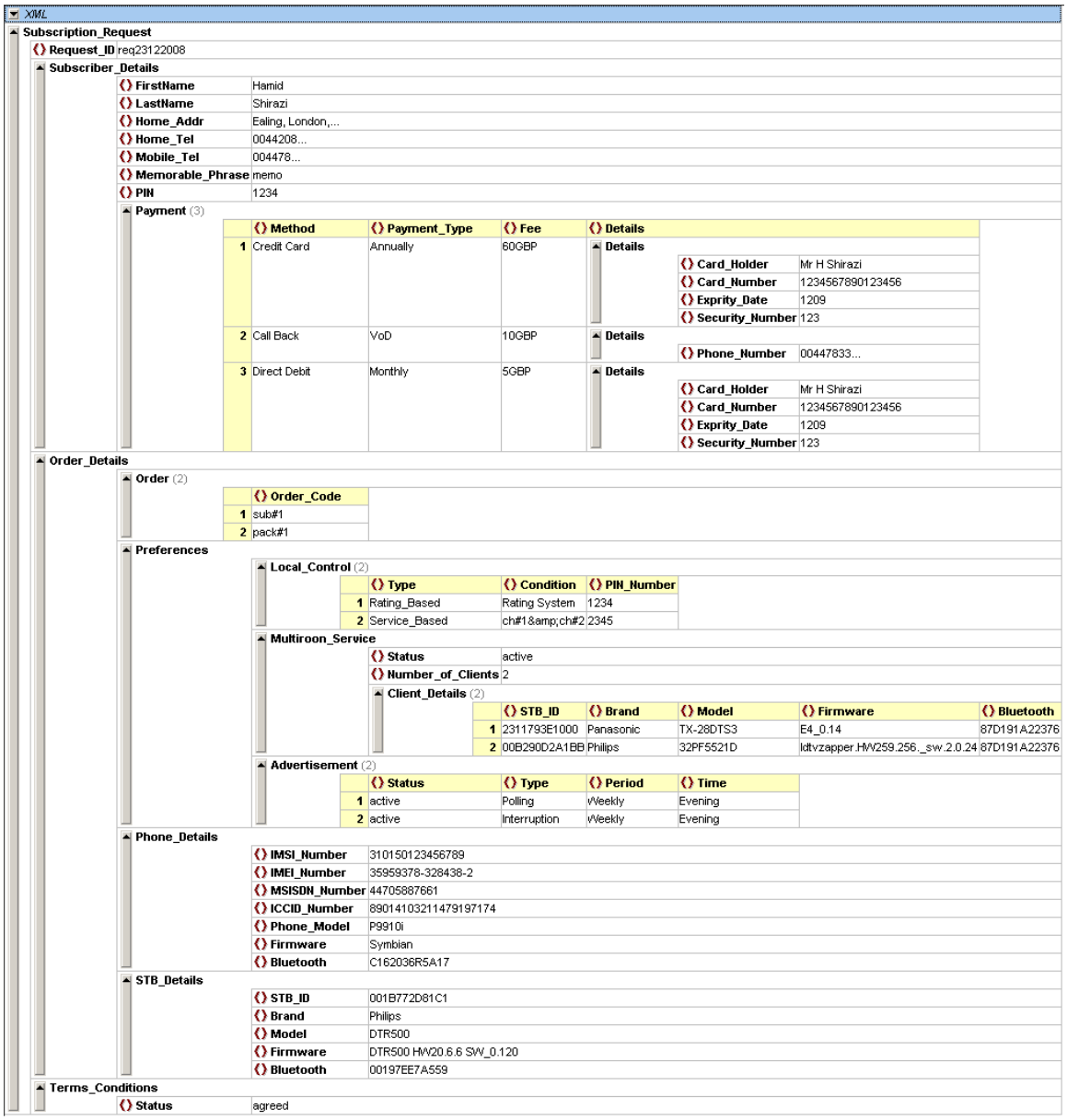
Fig. 53: The Subscription Association Table (SAT) in the XML format

The viewer needs to provide the service provider with certain information in order to place his order properly. As explained in the Sign-up use case, the subscription request is saved and sent to the service provider for instance in a XML format using SMS protocol. The format of the data very much depends on the security protocol standardised by the MICAS standardisation group. Nevertheless, some data that need to be delivered to the service provider to properly identify the viewer, his set-top box and proceed with billing sequence are shown using an XML structure in Fig. 54. The subscription request shall contain three sections as follows.

- *Subscriber details* which include the personal and account information of the subscriber. The payment method can vary depending on the service provider's facilities and available technologies. Nevertheless, three types of payment have been identified in the example below;
- *Order details* which includes the requested package/pack/channel(s) code(s), preferences in the local control, multi-room services and receiving advertisements, mobile phone and set-top box details;
- *Terms and conditions* which indicates the consent of viewer to the terms of the contract specified by the service provider.

The set-top box details can be deducted to the set-top box identification number as explained earlier. The number will be sufficient to query the rest of set-top box information from a central database. This can be the case for the mobile phone too. However, viewer's related data in the GSM network like IMSI and IMEI numbers can be retrieved by different ways such as using the AT commands of CIMI and CGSN, respectively. Then, the service provider can work out the MSISDN number mapped to the IMSI and IMEI number in the network and other information related to the device and its firmware. The Bluetooth

address of both devices can also be retrieved during the Bluetooth pairing sequence.



XML

- Subscription_Request
  - Request_ID: req23122008
  - Subscriber_Details
    - FirstName: Hamid
    - LastName: Shirazi
    - Home_Addr: Ealing, London,...
    - Home_Tel: 0044208...
    - Mobile_Tel: 004478...
    - Memorable_Phrase: memo
    - PIN: 1234
    - Payment (3)

	Method	Payment_Type	Fee	Details
1	Credit Card	Annually	60GBP	Card_Holder: Mr H Shirazi; Card_Number: 1234567890123456; Exprity_Date: 1209; Security_Number: 123
2	Call Back	VoD	10GBP	Phone_Number: 00447833...
3	Direct Debit	Monthly	5GBP	Card_Holder: Mr H Shirazi; Card_Number: 1234567890123456; Exprity_Date: 1209; Security_Number: 123

  - Order_Details
    - Order (2)

	Order_Code
1	sub#1
2	pack#1

    - Preferences
      - Local_Control (2)

	Type	Condition	PIN_Number
1	Rating_Based	Rating System	1234
2	Service_Based	ch#1&ch#2	2345

      - Multiroon_Service
        - Status: active
        - Number_of_Clients: 2
        - Client_Details (2)

	STB_ID	Brand	Model	Firmware	Bluetooth
1	2311793E1000	Panasonic	TX-28DTS3	E4_0.14	87D191A22376
2	00B290D2A1BB	Philips	32PF5521D	ldtvzapper.HW259.256._sw.2.0.24	87D191A22376

      - Advertisement (2)

	Status	Type	Period	Time
1	active	Polling	Weekly	Evening
2	active	Interruption	Weekly	Evening

    - Phone_Details
      - IMSI_Number: 310150123456789
      - IMEI_Number: 35959378-328438-2
      - MSISDN_Number: 44705887661
      - ICCID_Number: 89014103211479197174
      - Phone_Model: P9910i
      - Firmware: Symbian
      - Bluetooth: C162036R5A17
    - STB_Details
      - STB_ID: 001B772D81C1
      - Brand: Philips
      - Model: DTR500
      - Firmware: DTR500 HW20.6.6 SW_0.120
      - Bluetooth: 00197EE7A559
  - Terms_Conditions
    - Status: agreed

Fig. 54: The subscription request in the XML format

The viewer's details shall be kept secret during the transition and processing in the MICAS, as such some or whole part of the subscription message (or any message of this type) shall be encoded. The XML encryption and digital signature technique provide long-term authenticity as well as data integrity and

non-repudiation [114]. The content itself can be transformed via encoding algorithm such as the Base64. The Base64 content transfer encoding method is used as a generic term for any similar encoding scheme that encodes binary data by treating it numerically and translating it into a base 64 representation and character set of ISO-8859-1. The 1Kbyte subscription request after Base64 transformation will become as large as a 5Kbyte text file. A part of the transformed file is shown as follows.

Transforms	PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4NCjwhLS0gZWRpdGVkIHdpdGggWE1MU3B5IHYyMDA4IHJlbC4gMiBzcDIgKGh0dHA6Ly93d3cuYWx0b3ZhLmNvbSkgYnkgSCAoSCkgLS0+DQo8U3Vic2NyaXB0aW9uX1JlcXVlc3Q+DQoJPFJlcXVlc3RfSUQ+cmVxMjMxMjIwMDg8L1JlcXVlc3RfSUQ+DQoJPFN1YnNjcmliZXJfRGV0YWlscz4NCgkJPEZpcnN0TmFtZT5IYW1pZDwvRmlyc3ROYW1lPg0KCQk8TGFzdE5hbWU+U2hpcmF6aTwvTGFzdE5hbWU+DQoJCTxJb21lX0FkZHI+RWFsaW5nLCBMb25kb24sLi4uPC9Ib21lX0FkZHI+DQoJCTxJb21lX1RlbD4wMDQ0MjA4Li4uPC9Ib21lX1RlbD4NCgkJPE1vYmlsZV9UZWw+MDA0NDc4Li4uPC9Nb2JpbGVfVGVsPg0KCQk8TWVtb3JhYmxlX1BocmFzZT5TdHVkZW50PC9NZW1vcmFibGVfUGhyYXNlPg0KCQk8UEluY29tZV9CRDYXJkPC9NZXRob2Q+DQoJCQk8UGF5bWVudF9UeXBlPkFubnVhbGx5PC9QYXltZW50X1R5c …

After transformation, the resulted file can be compressed up to 40% for instance using Zip or arithmetic compression methods. The digest value is then calculated using the SHA1 algorithm.

SHA1 digest value	2330A8547FB968E7937BA9982A390653F4661486

The digest value needs to be signed (encoded) for instance using the RSA encoding method. The output of the signature will vary depending on the private key and size of the key (i.e. 2048, 1024, 512 bits). The signature based on a 512-bit private key will be as follows.

Signature value	340dab480b0b88443662b218f624698f8ff6aeebeb2c1300972417d24766f476 05c4a71d7f3cb7dd774810634cb674e30cec203ba938ba5a194ba43efea2833f
Private key	7cd1745aec69096129b1f42da52ac9eae0afebbe0bc2ec89253598dcf454960e 3e5e4ec9f8c87202b986601dd167253ee3fb3fa047e14f1dfd5ccd37e931b29d
Public key	10001

The public key and/or certification number will be known to the recipient to re-calculate the digest value and decode the subscription request. The signed subscription request can be structure as shown in Fig. 55 using the XML format.

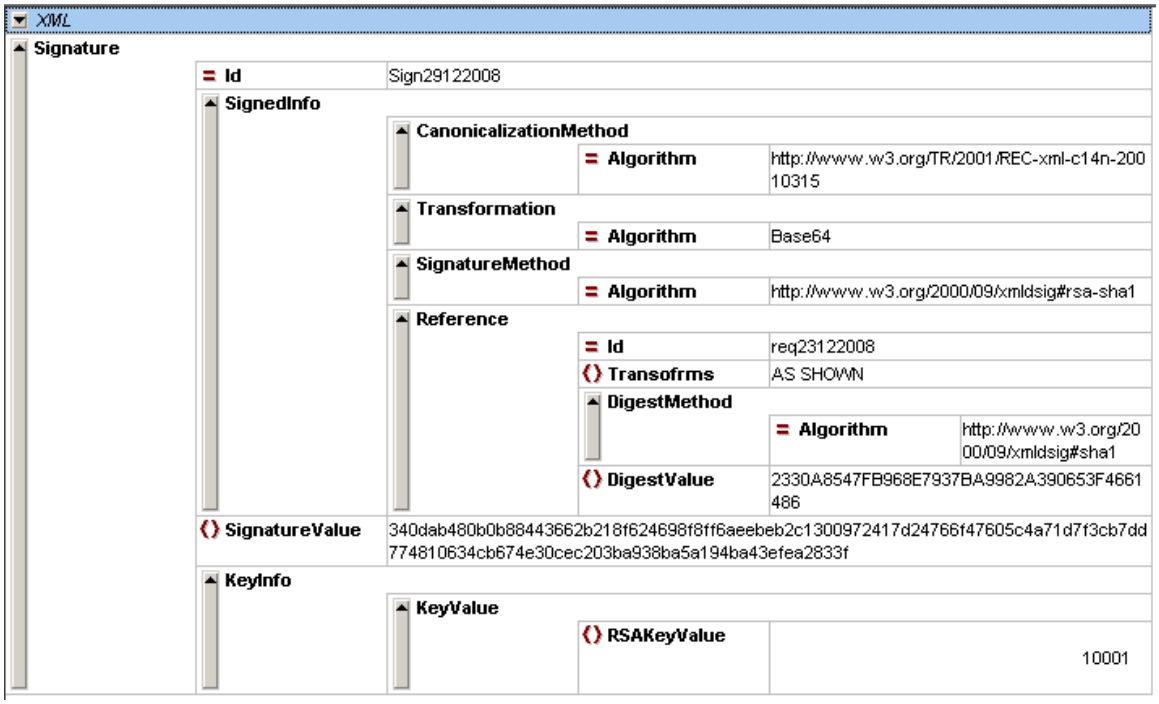


Fig. 55: The signed subscription request in the XML format

The signed subscription request can be sent by several SMS messages (i.e. 5 concatenated SMS messages); each SMS can only bear 160 7-bit characters. When the viewer's subscription request is granted, the service provider will send back an acknowledgement together with the viewer's identification number which may be calculated based on viewer's GSM and set-top box related data. The viewer's ID can be saved in the viewer's SIM card to be used in the future corresponding.

The Amendment request is similar to the Subscription request especially when a viewer wishes extending his entitlements by adding more channels or services into his subscription profile. However, it may include a cancellation request

concerning some or all parts of his subscription profile in that the requested channels or services needs to be specified clearly as shown in Fig. 56.

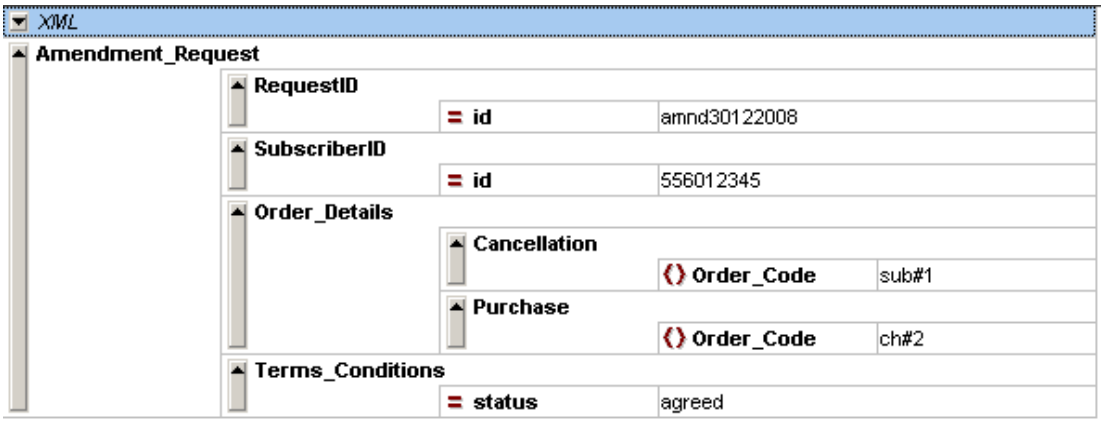


Fig. 56: The amendment request in the XML format

In the Follow Me activation request, the viewer needs to introduce himself, his set-top box and optionally determine the activation period. Given that the viewer has a valid identification number, the service provider can identify the viewer. The activation period can be pre-determined by the service provider (i.e. one day) and then extended on demand. The Follow Me service will be automatically cancelled when it is due or upon the viewer's cancellation request or when the service provider detects that the viewer is no longer using the set-top box for viewing (i.e. when he logs into another set-top box or changes his location). Fig. 57 presents the structure of the Follow Me activation request in the XML format.

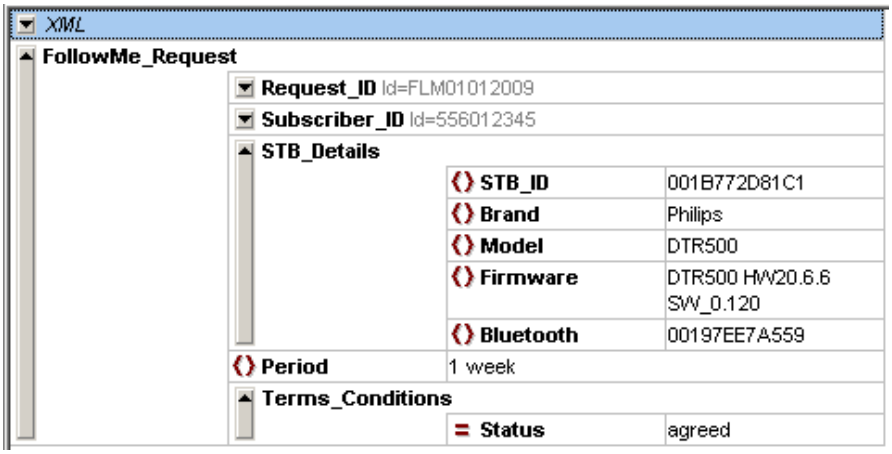


Fig. 57: The Follow Me activation request in the XML format

One of the cross-platform solutions to implement MICAS-related interactive applications is employing the JavaTV APIs (i.e. *javax.tv.carousel, javax.tv.xlet, etc.*) The JavaTV is compatible with other standards and provide high degree of control and flexibility over functionalities unique to television receivers. The *javax.xml.crypto* package also provides sufficient APIs to create and sign XML formatted messages. More information can be found in the Sun Microsystems' website (java.sun.com).

In the next section, the MICAS security architectures are briefly analysed versus security and performance related parameters.

7.3 MICAS Security Architectures Analysis

The MICAS architectures are analysed here based on the factors, which played important role in developing a comprehensive business case. The factors are quantified to provide a clear insight into the MICAS security architectures.

7.3.1 Security

The purpose of this step is to assess the level of risk to the various MICAS architectures. The determination of risk for a particular threat-vulnerability pair can be expressed as a function of the likelihood of a given threat-source's attempting to exercise a given vulnerability [101]:

- The magnitude of the impact should a threat-source successfully exercise the vulnerability;
- The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact.

To measure risk, a risk scale and risk-level matrix are developed. The standard risk level matrix includes the threat likelihood and impact of the threat. In order to determine the likelihood of exercising a potential vulnerability in a given security architecture, following factors can be taken into account:

- Threat-source motivation and capability;
- Nature of the vulnerability;
- Effectiveness of possible controls.

The threat likelihood can be measured in three levels: High (1.0); Medium (0.5) and Low (0.1). Table 15 presents the risk measurement criteria considered in the MICAS.

Table 15: Definitions of the Risk Scale.

Risk level	*Risk description and necessary action*
High	The system may continue to operate, but a corrective action plan must be put in place as soon as possible
Medium	Corrective actions are needed and a plan must be developed to incorporate these actions within a reasonable period of time
Low	The service provider must determine whether corrective actions are still required or decide to accept the risk

In general, depending on the mission of a system, criticality and sensitivity of data in the system, results of the impact analysis could vary. Therefore, the adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The impact is measured in three levels of High (10), Medium (5) and Low (1). Table 16 presents the impact measurement criteria considered in the MICAS.

Table 16: Definitions of the Impact Magnitude.

Magnitude of impact	*Impact definition*
High	Exercise of the vulnerability (1) may result in the highly costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede a Pay-TV service provider's objective, reputation, or interest

Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede a Pay-TV service provider's mission, reputation, or interest
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect a Pay-TV service provider's mission, reputation, or interest

As discussed previously, there are three different platforms (head-end, mobile phone and set-top box) in the MICAS. The communications between the head-end and receiver-end may take place either through broadcasting medium or GSM network. At the receiver-end, the set-top box and mobile phone communicates with each other through Bluetooth radio channel(s). The security data are saved either in the mobile phone or set-top box. Thus, attacks may take place on data stored at the head-end, mobile phone or set-top box or on transmission lines or on servers operating at the head-end.

One of the popular attacks in Pay-TV systems is the key piracy. The performance of a Pay-TV service provider depends on the security of key information used to protect contents. A direct attack may take place right at the head-end or mobile phone or set-top box. The impact of attacks can be controlled by adopting an effective distribution mechanism, key hierarchy system and key updating policy. At the head-end following actions can be taken to significantly reduce the risk of attack: 1) insertion of a highly secured firewall at the head-end and 2) storing data in an encrypted format during the data life cycle.

In addition, adopting some security measurement during the manufacturing of mobile phones or set-top boxes and transferring data over-the-air would reduce risk of the attack. For instance, the key can be protected more if it is: 1)

provisioned on a SIM/Smartcard during the manufacture, 2) delivered to a SIM/Smartcard over-the-air under protection of a key provisioned on the SIM/Smartcard during manufacture, 3) provisioned on a terminal during manufacture or 4) delivered to a terminal over-the-air under protection of a key provisioned on the terminal during manufacture. The security mechanism such as encryption, digital signature and session management techniques mentioned earlier can also guard the data from any piracy.

Moreover, adopting an effective distribution mechanism can also reduce the risk of the attack. Following counter-measurements can help a system fail gracefully in case of attack:

1) Minimising number of viewers who can use a common key to view programme(s) (i.e. reducing size of viewer group size);

2) Tailoring keys for individuals (i.e. unicast instead of broadcast);

3) Utilising both communication channels (i.e. broadcast medium and GSM network) to deliver valid key(s) to a set-top box;

4) Making sure that a certified and standardised set-top box can operate in the MICAS.

Last but not the least; the key hierarchical system can improve resistance of the MICAS against the attack. A three-level standard key hierarchical system has been proved higher security. It includes the MK, SK and CW to protect the digital contents. However, in other hierarchical systems a service provider may add a Broadcast Key (BK) or an Event Key (EK) to the standard security system to respectively classify viewers and provide more security for highly appreciated events (i.e. premier films). In addition, the service provider may frequently update the security keys. For instance, in some traditional broadcasting systems, ECM messages are updated in every 2 seconds and EMMs are updated in every

10 seconds. The key hierarchy and change rate, together, provides more protection against attacks.

There may various attacks to acquire key security information. Nowadays legitimate users collude to share the keys to a large group of illegitimate users. Adopting of some counter-measures like key provisioning during manufacturing of SIM or set-top boxes will be an obstacle for pirates from extraction of keys from a paying user's mobile phone or set-top box. Ultimately, pirates need to distribute key information to non-paying users. Thus, changing key with frequency of seconds instead of minutes, hours or days would obsolete compromised keys and makes the piracy more difficult. On the other hand, a non-paying user requires inserting the compromised keys into his set-top box or mobile phone, which can be stopped if manufacturers cooperate on counter-measurements. For instance, they shall not expose APIs or other programming mechanism(s) which could be used to re-insert keys or allow a programme emulating smartcard or SIM card to be loaded onto their devices. In addition, in case of re-broadcasting of contents, compliant set-top boxes shall not allow to move the contents off the set-top box. The service provider shall be able to prevent non-compliant set-top boxes from receiving contents in the first place.

The extraction of the MK is rather difficult if it is saved on a SIM card, given that algorithms using the key do not reveal anything about the key. It is not trivial to extract the MK when it is stored in the hardware or firmware on a robust platform like mobile terminal or set-top box, which supports hardware security methods. Although it is known to be less secure than SIM (or smartcard) technology and implying higher risk of cloning. However, extraction of the MK will be simple when the key or keys used to encrypt it are held in the clear or software. In case of the MK distribution, it is worthwhile noting that the MK is usually not changed at all or very infrequently and small amount of data needs

to be transmitted, thus the distribution of the MK is not difficult. However, constant monitoring of viewers' behaviour and black communities, who are advertising the keys, gives the service operator a chance to identify and revoke the compromised keys. After extraction and distribution, an illegal user needs to insert the keys into his mobile phone or set-top box. If the keys are inserted during manufacture, re-insertion is difficult unless there are serious bugs in the implementation of the SIM card, mobile phone or set-top box. To prevent such attacks, a secure boot mechanism should be in place that only allows the authorised versions of the operating system to be loaded into the terminal at the boot time. In addition, following counter-measures might be considered to protect the MK:

- Examining the records for entitlements and realising that a single terminal (i.e. SIM, mobile phone or set-top box) has been used on more occasions than should have occurred;
- The cloned terminals used in different broadcast system will be discovered if there is some forms of data sharing between operators;
- All mobile phones can have SIM-lock and IMEI protection broken. So, the MK can be extracted simply, however it is less likely that the key is extracted from a SIM:
    - Distribution of the key is trivial aside from keeping this information secret from service providers;
    - Insertion the key into a terminal needs programming the terminal which is not trivial;
    - Revoking the compromised MK by the operator motivates the users to use the key to extract service keys and distribute service key instead of the MK.

The SK, which is encrypted by the MK, stands at the second in the 3-level key hierarchical system. However, in a 4-level key hierarchical system, the SK is encrypted using a BK to save the bandwidth in the broadcast bearer. The BK is then encrypted using the MK. Therefore, the MK has to be attacked first in order to intercept and extract messages which convey the SK. The attack on SK might take place while it is in storage or used on the terminal or it can be obtained while being transferred in the clear. In addition, the SK might be intercepted from SIM-Mobile Equipment (ME) interface. Thus, transferring the SK encrypted from the SIM to the ME although helps but would not add that much security to prevent the illegally extraction of the SK. However, the encryption key of the SK must not be publicly or easily obtainable. It is worthwhile noting that the SK is not changing frequently enough to make distribution hard though advertising the compromised SK would give chance for the operator to take action. In order to tackle the key distribution problem, manufacturers must not expose any APIs used to inject SKs or expose data streams. The following counter-measures can also be considered versus the attack on the SK:

- Measures to protect SK and MK at the terminal (i.e. SIM, ME, set-top box);
- Just in time delivery of SK before starting the event;
- Diversity of SK and reducing the number of viewers who can receive security messages (i.e. unicast instead of broadcast EMM);
- Storing the SK on a SIM and extracting it using a key on the SIM would mitigate the risk of attack;
- The risk will be lessened if the SK is held in the terminal and delivered to the terminal using a key provisioned in the terminal during manufacture;
- The SK will be more vulnerable, if it is held in the terminal and delivered in the clear over SIM-ME or smartcard-STB interfaces and likewise the keys and/or any parameters from which SK is obtained.

The last key in the Pay-TV hierarchical security systems is the CW, which is usually obtained in the clear and distributed to the unauthorised receivers to re-insert. In the MICAS, it is more likely that CWs are obtained from Bluetooth radio link and/or broadcast bearer than a terminal, unless, the method of storing them in the terminal was so poor. Another way to extract the CWs is to use the already extracted SK in an emulator to decrypt the ECM messages and get the CWs. In the mobile phone platform, attack will be much simpler if the CWs are delivered in the clear through SIM-ME interface. Thus, it is better to encrypt interface messages using a key stored in the SIM rather than the ME. Having extracted the CWs, the pirates have to distribute the keys. Considering the changing rate of CWs (i.e. about seconds), distribution of CWs would be difficult. Thus, the CWs must have a period close to the time taken for their illegal redistribution. This enforces fraudsters to buffer the content at the receiver. The size of buffer is related to the frequency of CWs and the whole operation can be costly. Moreover, the insertion of CWs can be controlled too. The insertion would be very easy if CWs are delivered in the clear to the terminal. Therefore, the complaint terminals shall not accept CWs for instance in a clear text form. It shall be either encrypted by the SK held in the terminal or by a terminal specific key. In case of using the SIM card as a security entity, the CWs delivered to the SIM shall be encrypted using the SK and then from SIM to the terminal using a terminal-specific key. The SK and terminal-specific key shall be unique to the terminal. Non-compliant terminals, which accept CWs in clear, will be likely laptops or programmable mobile phones using open APIs. Following counter-measures can be considered to reduce the vulnerability of CWs in the security structure.

- Increasing frequency of CW change as it makes the redistribution difficult but it results in using more bandwidth for transmission of keys in broadcast layer;
- Encrypting CWs delivered to terminals using either SK or a terminal-specific key.

All in all, with regards the key extraction, the most likely attack would be against the MK to be used on an emulator or set-top box or SIM to obtain the SK. However, advertising the MK would reveal the identity of the compromised terminal and lead to revocation of that set-top box or mobile phone (or SIM card). With regards the reinsertion of extracted keys, the following points can be made:

- Given reinsertion of keys is very difficult, the non-compliant terminals will be an alternative; so the relevant APIs must not be exposed in mobile phones or set-top boxes;
- Manufacturers must ensure that extracted keys can not be extended into unauthorised receivers or emulators;
- Distribution of the MK and SK is not difficult especially when they are stored in terminals, while the distribution of CWs can be difficult especially when the changing rate of CWs is a few seconds;
- Re-insertion needs significant programming or physical attack upon terminals which is not too simple to attract great number of users;
- Using a software emulator requires the pirate to carry a portable PC to access the content illegitimately, which is another disincentive to attack;
- Downloading security agents in the terminals would facilitate monitoring of viewers' contractual behaviour.

Table 17 summarises the risk assessment of key piracy in the MICAS security architectures (see Chapter 6). The assessment is based upon the vulnerabilities

explained in the extraction, distribution and insertion of the MK, SK and CWs in the Pay-TV systems.

Table 17: Risk assessment of key piracy in the MICAS security architecture

	Risk Scale	*Impact Significant*
Architecture #1	1	1
Description	The ECM and EMM are broadcast and Security Objects (i.e. MK, entitlements) are delivered to each set-top box via the GSM network. The MK, which tends to be updated infrequently, is exposed in the rather insecure Bluetooth link. Extracting and sharing the MK may result in loss of tangible service provider's interests thus a corrective action plan must be put in place as soon as possible. For example, the service provider must revoke and replace the compromised MK and possibly look at other options as the MK can identify the viewer and security mechanism used on viewer's terminals. Given access to the MK, a pirate still needs to distribute, insert and also work out the SK and CWs. The Bluetooth link is likely the most vulnerable security zone here, unless Security Objects are encrypted for instance using a set-top box specific key. The MK can also be viewer/terminal-specific to be functional in a certain terminal. Moreover, the MK can be calculated at the set-top box using data delivered along with the EMM and Security Objects from both delivery routes.	
Architecture #2	0.5	5
Description	The EMM and ECM are broadcast and MK is stored in the viewer's SIM card. The MK is exposed in the GSM while EMM, SK and/or entitlements are exposed in the Bluetooth link. Subjecting the Bluetooth link to a successful attack, the pirate still needs to work out the CWs, which will be a trivial task, if the SK is appeared in clear and ECM is encrypted using known encryption algorithms. Therefore, the service provider has to take an immediate action (i.e. revoking the MK and replacing the SK) to tackle the problem and prevent from further loss in the revenue. Considering that the SK is not associated to a particular viewer so there will be no lead	

	to the compromised MK. The significance of the impact can be reduced by classifying viewers, allocating SK for each class of viewers and increasing the SK change rate. In addition, the attack will be more difficult if data which is exchanged over Bluetooth link is encrypted for instance using a terminal-specific key. Moreover, the terminal (i.e. set-top box, mobile phone) can be configured to just accept an encrypted form of the Security Objects (i.e. SK, entitlements, EMM) necessitating the confidentiality of security algorithms used in terminals. For prevention of the key insertion to the set-top box, the set-top box and mobile phone shall implement a session-based (state-full) hand-shaking mechanism to exchange the EMM and Security Objects.
Architecture #3	0.1 5
Description	The EMM, ECM and MK are ultimately delivered to the viewer's mobile phone (SIM card). The CWs which are used to descramble the contents are exposed in the Bluetooth link. However, the high change rate of the CWs will make the piracy difficult and in addition, if the CWs are transferred encrypted and accepted encrypted by the set-top box, the risk of exercising the vulnerability will be even more reduced. In the case that the CWs are extracted as a result of exercising the vulnerability of the Bluetooth link, the service provider must determine whether corrective actions are required or decide to accept the risk. The corrective actions can be the renewal of the SK and/or MK randomly or configuring the set-top box and mobile phone to implement a strict session management mechanism to exchange data over the Bluetooth link. In addition, the set-top box shall be programmed to not let any unencrypted keys be inserted into the set-top box out of the MICAS framework.
Architecture #4	1 1
Description	The ECM is broadcast to set-top boxes while EMM and MK are unicast to each STB through GSM and Bluetooth channel. The point-to-point delivery of the EMM reduces the risk scale. However, the extraction of the MK and decryption of

	the EMM can reveal the SK and entitlements needed to extract CWs. Considering that the EMM and MK are likely to be tailored for a specific viewer, advertising them will not be of interest to pirates, but sharing the compromised SKs can potentially damage the service provider's interest. Thus, the service provider shall immediately restore security level in the field, for instance by revoking the compromised MK and increasing the changing rate of SK. The impact of attack can be costly unless the MK and EMM are encrypted for instance using the terminal-specific key provisioned to the terminal during the manufacture. It is also important that service providers do not expose encryption algorithms as it helps pirates extract SKs. Implementing a session management technique in terminals and prevent the insertion of out of context keys would lessened the risk impact.
Architecture #5	0.5 5
Description	The ECM is broadcast whereas EMM and Security Objects are delivered to each viewer's mobile phone. The ECM is then delivered from the set-top box to the SIM over the Bluetooth channel to extract the SK. Next, the Security Objects (i.e. SK and entitlements) are delivered to the STB via Bluetooth link to extract CWs and descramble the contents. Exposing the SK on the vulnerable Bluetooth channel can endanger the service provider's mission and so the service provider shall plan to redeem the situation (i.e. increasing the changing rate of SK). However, the impact is less significant due to the point-to-point delivery of the EMM. The extraction of SK and entitlements can reveal the CWs too. However, encrypting the Security Objects and configuring the set-top box to prevent illegal insertion can reduce the risk.
Architecture #6	0.1 5
Description	The ECM is broadcast and then delivered to the mobile phone whereas the EMM and MK are directly delivered to the mobile phone. The exposure of CWs could endanger the service provider's assets however the high change rate of CWs would make the piracy rather difficult. Encrypting the CWs using a terminal-specific key and implementing a

	session-management technique in terminals would increase the security. The set-top boxes shall be configured to not accept any keys unencrypted and out of the managed session.
Architecture #7	0.5 5
Description	In this 2-level key hierarchy, the only conditional access message is ECM and Security Objects (i.e. SK and entitlements) are delivered to the STB through GSM and Bluetooth radio link. Compromising the SK would potentially impede the service provider's interest. The SK is likely associated to the services rather than viewers. Therefore revoking compromised keys is a great task as it may hit the whole receivers' population. However, the encryption of Security Objects using a terminal-specific key and increasing the changing rate of SK would mitigate the risk scale and impact. It is also important that the SK is not similar to previous SKs or does not lead to any knowledge to work out any upcoming SK. The set-top boxes operating in the field can also be configured to tackle illegal key insertion as explained earlier.
Architecture #8	0.1 5
Description	The ECM is broadcast to the set-top box and then delivered to the mobile phone (i.e. SIM card) via the Bluetooth channel. The Security Objects (i.e. SK and entitlements) are also delivered directly to the SIM. The CWs are then calculated in the SIM and delivered to the set-top box over the Bluetooth radio link. The exposure of the CWs can result in loss of service provider's revenue. However, the high frequency of CWs makes the extraction and distribution of the keys very difficult and so reduces the risk scale and impact. With a proper encryption technique and configuration policy, the extraction and insertion can also be more challenging.
Architecture #9	1 10
Description	The Security Objects are transferred over-the-air to the viewer's SIM card. The GSM is considered as a fairly secured network and the SIM card provides various means of security too. However, the Bluetooth channel is attributed as the weakest link in the MICAS. Thus, exposing the actual assets

	(contents) on the Bluetooth would potentially cause a large shadow over the service provider's interest. Adopting some sort of encryption technique may help but it is not sufficient.
Architecture #10	0.1 5
Description	In this model, there is no conditional access message that is broadcast. The MK is provisioned to the SIM by manufacture or over-the-air with absolute secrecy. The required Security Objects and/or CA message(s) are then delivered to the SIM through GSM network to calculate the CWs. The CWs are then delivered to the set-top box over the Bluetooth channel. The point-to-point delivery of CA messages and Security Objects to the SIM card provides a higher level of security. A GSM oriented attack may lead to the extraction of the SK, but such an attack is difficult to conduct due to the high security level of the GSM network. However, the vulnerability of the Bluetooth link can be exercised to extract CWs though high frequency of CWs makes the extraction and distribution difficult. Other said counter-measures can also degrade the scale and impact of the risk.

The risk assessment is calculated by multiplying the risk scale and impact significant. The risk of compromising the security of the system can vary from 0.5 to 10. The attack implies the least impact in the architectures 3, 6, 8 and 10 where the MK and SK are stored in the SIM and only CWs are exposed on a less secure Bluetooth link. However, the high frequency of CWs makes the piracy difficult. On the other hand, the architecture numbered 9 is attributed as the riskiest architecture as it exposes the actual contents on the Bluetooth channel. Fig. 58 presents the tendency of risk assessment in the MICAS security architectures.

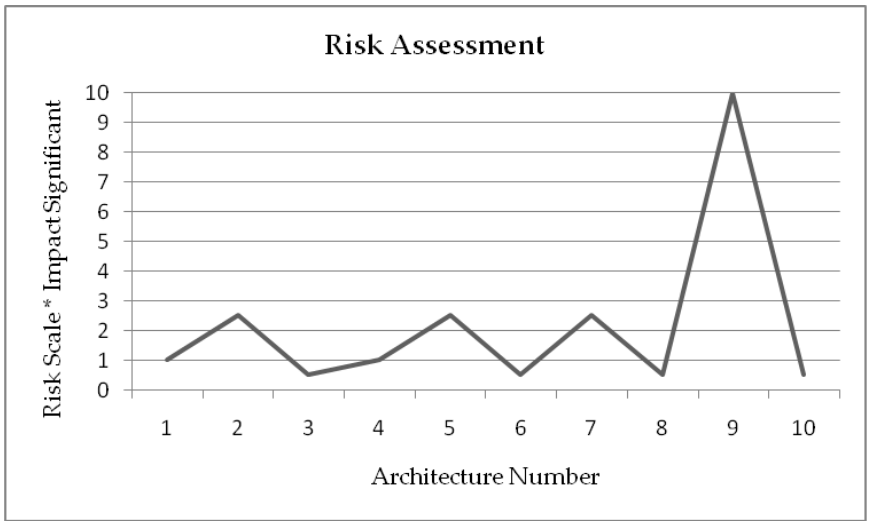


Fig. 58: The risk analysis of MICAS security architectures

7.3.2 Complexity

In broadcast-only Pay-TV systems, the complexity of the conditional access system lies chiefly in the CA message handling used at the head-end and receiver-end. The design of the EMM injector at the head-end, synchronisation mechanisms, message filtering and processing at the receiver-end are some challenges of the kind [67]. Most of these challenges are also applicable to the MICAS architectures. However, integrating the mobile technology as a bi-directional channel in the MICAS can mitigate the complexity of CA message handling. Nevertheless, supporting advanced interactive services and enforcing an on-line security mechanism will potentially add more complexity at both ends which is very much related to the design and implementation of the firmware.

The overall complexity of the MICAS architectures is calculated based on the following measures ranked from 1 to 10.

- *Emergent complexity*: it depends on the observer, and as such it can be defined as the complexity of the system from a viewer's point of view. A survey was carried out on groups of people (i.e. 50 people) to evaluate the emergent complexity level. The survey was based on a questionnaire

focused on the use-cases explained in Chapter 6. The observers were from different groups of age (i.e. between 15 to 60 years) and high-tech literacy (i.e. mobile, computer) but their view was counted equally weighted. The emergent complexity of MICAS architectures was achieved by averaging the viewers' observation of the system. Each observer ranked his skill (i.e. high-tech literacy) according to the competency array of unfamiliar (1), low (2), familiar (5), expert (7), highly expert (10). The observer ranked the complexity of use-cases from 1 to 10. Table 18 shows a snap-shot of the results gathered in the survey for the security architecture (1).

Table 18: A complexity survey sample of MICAS architecture (1)

Arch#1 / *Observer*	*Age*	*Skill*	*Set -up*	*Sign -up*	*Install CASS*	*Follow Me*	*Multi -room*	*Local Control*	*Amend Profile*	*Average of Complexity*
1	35	5	4	5	6	3	7	3	3	4
2	55	2	7	8	8	5	9	5	5	7
3	17	5	5	5	4	3	6	4	3	4
4	22	5	5	4	6	4	6	5	4	5
5	22	2	6	7	6	5	8	4	5	6
6	30	7	4	3	4	2	4	2	2	3
Average	30	4	5	5	6	4	7	4	4	5

- *Interdependencies*: the complexity of architectures partially depends on the interdependency of the modules so that it makes the system partially decomposable;
- *CA message handling*: the complexity of CA systems chiefly depends on the design of EMM injector at the head-end and design of set-top boxes at the receiver-end.

Quantifying the last two criteria in complexity measurement remains indefinite herein as it mainly depends on the implementation (i.e. user interface) and algorithm used in the architecture. In a first layer of analysis, a simple comparison amid architectures can be deducted to realise which solution is less complex for implementation. For instance, the architecture which needs to inject

EMM messages in a strictly timely manner implies more complexity in design than the architecture which demands a point-to-point messages delivery. Nonetheless, concerns may remain for deeper complexity analysis of algorithms used for message processing, delivery, and so on and so forth in MICAS architectures which can be achieved in the future. Table 19 presents the first layer complexity assessment of the MICAS architectures based on complexity criteria explained earlier.

Table 19: The complexity assessment of MICAS security architectures

	Emergent Complexity	*Interdependency*	*CA-related Complexity*	*Average of Complexity*
Architecture #1	5	5	7	6
Description	- The main concerns amid all observers were about the Set-up, Sign-up and Multi-room use cases; - The CA elements (i.e. SMS, SAS, EMM/ECM injector, MHSS, mobile, set-top box) are responsible to deal with viewer's request and service delivery while restoring the security criteria. However, after delivery of the security mechanisms and/or objects to the set-top box, the mobile and MHSS can standby since the MK is not changed or changed rarely. In this model, the EMM and ECM are broadcast like the traditional broadcast-only Pay-TV systems; - The CA-related complexity at the head-end is similar to that of the traditional broadcasting system, although it is slightly different at the receiver-end. The set-top box still needs to filter the CA messages and in addition handle the Bluetooth interface, which potentially adds more complexity to the set-top box architecture. However, the CA processing will be simpler and quicker if the Security Objects are stored on a privileged memory within the set-top box rather than an attached smart card;			
Architecture #2	7	7	8	7
Description	- In addition to previous challenges, the observers have found it difficult to work with mobile phone and/or set-top box in order to deliver the SK and entitlements to the set-top box; - The mobile phone has to be at vicinity of the set-top box whenever			

	a SK needs to be delivered to the set-top box; - This model needs a more complex synchronisation method to tackle the delay introduced to the system by processing of EMMs in the mobile phone. The set-top box still needs to decode the ECM and descramble contents using the SK delivered via the Bluetooth link. The overall design of the set-top box can be simpler if the Security Objects are stored inside the set-top box and no further interfacing with a smart-card is required;
Architecture #3	7 9 8 8
Description	- The Follow Me and Multi-room Subscription use-cases were the most complex use-cases. There were also concerns about the delivery of security keys via the mobile phone to the set-top box; - The CWs are changing rapidly (i.e. every five to ten seconds) and so it is essential that the mobile phone remains close to the set-top box to receive CA messages and deliver CWs; - The complexity of the head-end is similar to the traditional broadcast-only Pay-TV systems. At the receiver-end, the set-top box does not require to process the EMM and ECM messages to extract CWs. However, managing the Bluetooth interface to continuously deliver CA messages and receive CWs while handling the synchronisation issue to restore viewers' satisfaction adds more complexity to the set-top box architecture;
Architecture #4	6 8 6 7
Description	- The results were similar to the first survey and there were also concerns about the binding of mobile phone and set-top box to deliver EMM messages; - The elements working on the return channel (i.e. MHSS, mobile and set-top box) shall remain in contact to deliver services to a viewer. Although the MK is changed rarely, the EMM is changing every 10 seconds in the traditional broadcasting systems which dictates the necessity of close and continuous cooperation of the said elements; - The EMM injector needs to feed the EMM into the GSM channel for a point-to-point delivery. Thus, a more complex and delicate synchronisation method is required to deliver just in-time services to viewers due to the delay introduced from the GSM and Bluetooth channel. The filtering process at the set-top box can be

	eliminated however the set-top box still requires to process CA messages to extract CWs;
Architecture #5	6 8 7 7
Description	- The observers were mostly concerned about the complexity of the sign-up, Follow Me and Multi-room use cases. They also expressed concern over the difficulty of binding their phone to the set-top box; - The return channel elements are bound to each other even more due to the higher frequency of the SK; - The MHSS has to deliver the EMM messages to each viewer in-time through the GSM network. The overall complexity of the system might be lower than that of traditional Pay-TV systems due to the point-to-point delivery of EMM messages. The set-top box design can be simpler as there will be no need for filtering of CA messages. However, handling the Bluetooth interface to receive the SK and entitlements might require more attention to meet the synchronisation criteria;
Architecture #6	7 9 7 8
Description	- The most complex use-cases were Sign-up and Install CASS. The observers also did not welcome the fact that their mobile phone might be needed to enable them watch TV; - The interdependency amid return channel elements is even higher here as the set-top box needs to exchange ECM and CWs with the mobile phone. The high frequency of CWs requires both elements to be continuously in the range of Bluetooth radio; - The complexity of the head-end is similar to the previous architecture but the set-top box design can be less complicated. Although the set-top box needs to manage the Bluetooth interface and signal synchronisation, but there will be no CA processing inside the set-top box;
Architecture #7	6 7 6 6
Description	- The Sign-up use-case was recognised as the most difficult task beside the Multi-room Subscription use-case. The constant need for the mobile phone in order to watch TV was not welcomed; - The return channel elements still needed to be fully in contact as it is dictated by high frequency of SK unless a series of SK is delivered occasionally (i.e. once a day);

	- The CA system at the head-end can be less complex as there is no need to generate EMM messages. The point-to-point delivery of Security Objects also reduces the complexity. At the receiver-end, the set-top box architecture can be less complex as there is no need for filtering and EMM processing. However, the synchronisation task can be more complex if the SK is changed in the system quickly;
Architecture #8	7 8 7 7
Description	- Similar to previous results, the result of the survey shows that there is a great concern amid observers about their mobile phone to be bound to the set-top box. The Sign-up was also the most complicated use case; - The mobile phone and set-top box will be more dependent on each other to deliver services to the viewer due to the high frequency of the ECM and CW which are exchanged across the Bluetooth link; - The head-end complexity is similar to the previous architecture. However, more complexity is added to the set-top box to work out the synchronisation (i.e. descrambling contents using CWs). The set-top box will be fully running to acquire ECMs and deliver them to the mobile phone. In return, the mobile phone sends back the CWs to be used for descrambling of contents. The high frequency of ECM and CWs introduce higher processing and more complexity to the system;
Architecture #9	7 9 6 7
Description	- The results of the survey remained almost as same as previously given observations. The strict requirement of engaging mobile phone in content delivery was not welcomed; - Higher interdependency is required especially between mobile phone and set-top box as the whole CA processing is carried out in the mobile phone. On the other hand, the MHSS has to keep updating the mobile phone about the new SK; - The overall CA-related complexity will be lessened at both sides as there no EMM injector that is required and the set-top box is not involved in filtering or CA processing. The set-top box architecture will be reduced to a simple DTV box (i.e. Free-view box) with Bluetooth capability;

Architecture #10	7	9	7	8
Description	- The observers recognised that the Sign-up and Multi-room use-case as the most complex use-cases. The constant requirement of mobile phone to be at the vicinity of the set-top box was also part of their concerns; - The return channel entities will be fully dependent to each other as the mobile phone needs to deliver CWs to the set-top box. The CWs are changing rapidly and that demands for constant communication of keys amid involved elements; - The CA-related complexity will be reduced by eliminating the ECM/EMM injector subsystem. Considering that the Security Objects are delivered to the set-top box through the GSM network, strict synchronisation technique needs to be implemented at the set-top box to tackle the synchronisation issue;			

The result of survey emphasises on implementing user-friendly set-top box and mobile applications to enable viewers readily go through the MICAS use-cases. It also necessitates that the interdependency of return channel elements (i.e. MHSS, mobile phone, set-top box) needs to be mitigated to relieve the viewer from being bound to the set-top box. The interdependency strictly related to the key management and distribution schemes. The less frequent contact is made over the GSM route the less interdependency is required amidst the elements. Finally, the CA-related complexity at the head-end and receiver-end (i.e. set-top box) will be lessened by effectively shifting all/part of CA-related processes to the mobile phone. Considering that mobile phones are becoming more resourceful, therefore installing small sized applications on the SIM or ME will unlikely affect mobile phones' performance. Fig. 59 shows the tendency of complexity in the MICAS security architectures. The overall complexity simply represents the average of emergent, interdependency and CA-related complexity factors assessed above.

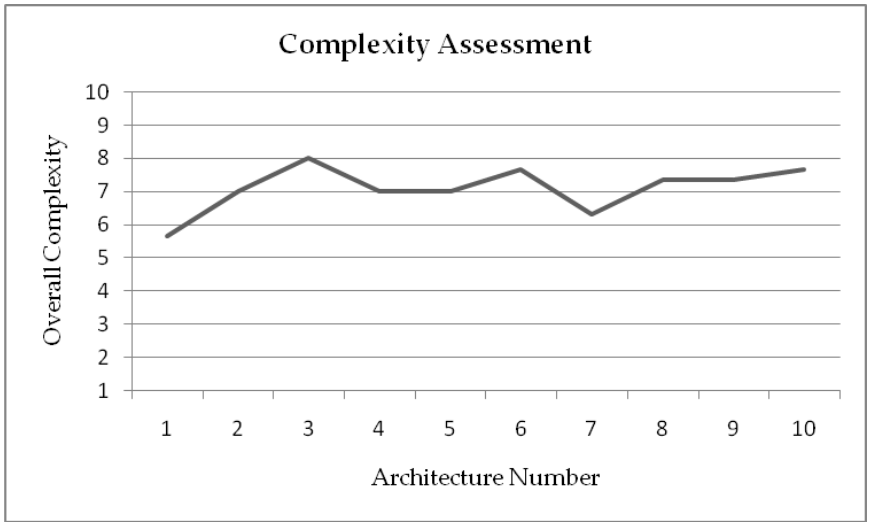


Fig. 59: The complexity assessment of MICAS security architectures

7.3.3 Set-top Box Production Cost Model

An important factor to take up of a technology is the rate of return and deployment cost which will attract stakeholders. The rate of return is very much related to customers' response to the technology. Thus, the survey which was presented earlier could be a starting point for further business analysis. Various factors can influence the overall deployment cost such as head-end development cost, transmission cost and transition cost to the MICAS. The set-top box cost is no longer counted as part of the deployment cost in the MICAS as it is paid by viewers. However, the additional cost of using the GSM services (i.e. send/receive SMS) might be added to the service provider's deployment cost.

A brief analysis of MICAS transaction model was given in Chapter 6 and more analysis of all business driven factors can be deferred to the future. Nevertheless, the overall cost of set-top boxes which might be attractive to the set-top box producers and viewers are briefly discussed here. A standard set-top box which is usually used in the Pay-TV system is considered as a reference for comparing the cost of the set-top boxes used in the MICAS security architectures. The overall production cost of a set-top box can be subdivided into the following

factors: the administration cost, labour cost, components cost, integration costs, tests, etc. The components (i.e. hardware and software) used in a set-top box are based on the design of the set-top box. A normal set-top box, which can be used in a Pay-TV system, usually has a CPU and memory (i.e. DRAM, Flash) to run the firmware and control the following hardware components.

- Tuner: converts RF-TV signals into a form suitable for further processing;
- De-Modulator: recovers original signals from modulated career waves;
- De-Multiplexer: decomposes the TS into CA messages and digital contents;
- Filter(s): separates EMM/ECM messages addressed to the set-top box;
- CA module: interfaces the set-top box to the smart card and/or processes the CA messages;
- Smart card: stores security sensitive data/algorithm and/or handles all CA processing;
- De-Scrambler: uses the CWs to descramble digital contents;
- Decoder: decodes the MPEG-2 signals into analogue signals (i.e. PAL);
- Common interfaces: provides interfaces to the outside world;
- Remote control handler: is used for remote operation via Infrared (IR) or radio signals;

The front-end components (i.e. tuner, demodulator, de-multiplexer) are the same in the most of set-top boxes. The CA subsystem (i.e. filter, CA module, Smartcard, descrambler) may differ depending on the CA system. The back-end components (i.e. decoder) are also similar to most of the set-top boxes working on the Pay-TV systems. The common interfaces (i.e. RJ-11, RS232, HDMI/DVI, 802.11, USB, etc) are not essential for non-interactive environment and in traditional Pay-TV systems are considered as optional features.

The production cost of the set-top box can be broadly analysed in MICAS security architectures based on the hardware components mentioned above. Table 20 presents a brief cost analysis of set-top boxes used in MICAS architecture. In the analysis, the cost differentiation in the hardware components integrated in the set-top box has not been considered. It has also been assumed that the firmware and memory differentiation cost is negligible amid security architectures, though it is appreciated that some architectures require more sophisticated firmware and memory resources to handle CA processing. As mentioned before, the Bluetooth interface is necessary in all architectures.

Table 20: The overall STB cost in the MICAS security architectures.

Architecture Number	*Cost (1-10)*		*Description*
	Min	*Max*	
1	9	10	Delivery of the MK over-the-GSM, can simplify set-top box design by eliminating the smartcard and/or CA module. The Security Objects can be stored in a secured memory (i.e. flash) and CA processing can be performed by CA-related applications downloaded into the set-top box;
2	8	9	The SIM card substitutes the smart card as it is used to store the MK and decode the EMM. The CA module might be used for decoding the ECM and extracting the CWs in the set-top box, however, it can be replaced by downloaded CA applications;
3	8	8	The SIM is used as a full security element to store Security Objects and process CA messages replacing the smartcard and CA module in the set-top box;
4	8	9	Delivery of EMM through the GSM channel will eliminate filters used in the set-top box. The smartcard and CA module may be used as the MK is delivered to the set-top box;
5	7	8	The EMM is delivered through the GSM and the SIM replaces the smartcard as it stores the Security Objects and decodes the EMM. The CA module can be used to

			decode the ECM using the SK delivered to the set-top box over the Bluetooth channel;
6	7	7	The point-to-point delivery of EMM eliminates the filters and SIM card replaces the smartcard and CA module in the set-top box;
7	8	9	The elimination of EMM in the system will simplify the set-top box by removing the filters. The use of high frequent SK can also eliminate the smartcard. However, the CA module might be still used for decoding the ECM;
8	7	7	The set-top box does not need to have filters, smartcard and CA module as whole CA-related processing is performed in the SIM card;
9	6	6	After de-multiplexing the TS, the set-top box sends contents and ECM to the mobile phone. The SIM card (i.e. SIM applications) replaces the CA module, smartcard and descrambler;
10	7	7	Adopting a one-level key hierarchy system and point-to-point delivery of Security Objects would eliminate the CA messages (i.e. ECM, EMM). The set-top box design will be simplified as there will be no need for filters, CA module and smartcard;

The analysis suggests that integrating the mobile phone in the traditional Pay-TV systems can potentially reduce number of hardware components used in the set-top box. The sophistication of the security mechanism (i.e. key hierarchy system) impacts on the set-top box cost. Fig. 60 depicts the average tendency of the set-top box production cost analysed for the MICAS security architectures.

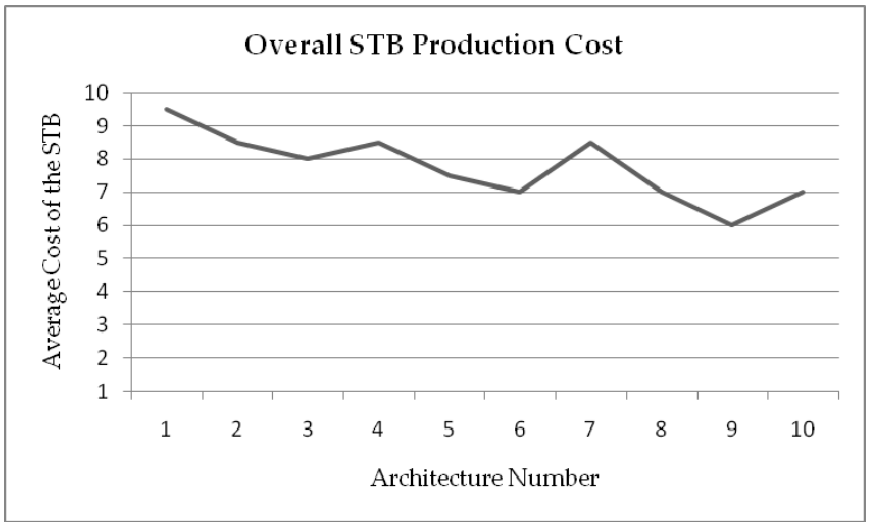


Fig. 60: The STB production cost analysis in MICAS security architectures

7.3.4 Deployment Analysis

Evaluating the performance of MICAS security architectures require the long-term monitoring of operations, costs, revenue and viewer's satisfaction level in the field. However, an evaluation of security risk analysis, complexity and cost model can help develop a more comprehensive business case for the MICAS security architectures.

The following formula can be used to present the Likely Deployment Success Rate (LDSR) based on the security risk, complexity and cost which have reverse impact on the performance of the MCIAS.

$$LDSR\% = \frac{1}{SecurityRisk \times Complexity \times Cost} \times 100$$

The performance percentage can be calculated based on the overall assessment presented previously. Table 21 provides an abstract of the assessment conducted so far and performance percentage calculated for the MICAS security architectures.

Table 21: The LDSR analysis of the MICAS security architectures

Architecture #	*Security Risk*	*Complexity*	*STB Production Cost*	*Performance%*
1	1	6	9.5	1.9
2	2.5	7	8.5	0.7
3	0.5	8	8	3.1
4	1	7	8.5	1.7
5	2.5	7	7.5	0.8
6	0.5	8	7	3.7
7	2.5	6	8.5	0.7
8	0.5	7	7	3.9
9	10	7	6	0.2
10	0.5	8	7	3.7
Average	**2.2**	**7.1**	**7.7**	**2.0**

Fig. 61 presents the likely deployment success rate of the MICAS security architectures.

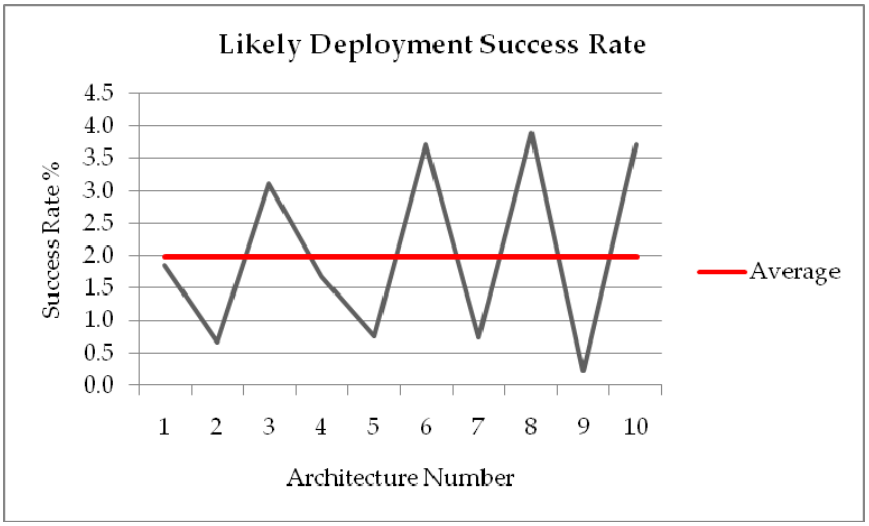


Fig. 61: The LDSR analysis of the MICAS security architectures

The security architecture numbered (9) is the poorest performer and (8) is the best. The architecture numbered (1) has the minimum deviation from the average performance and (8) has the maximum deviation; implying that the security architecture numbered (1) can be a conservative solution and numbered (8) can be the ideal solution.

7.4 Summary

The receiver-side in the MICAS has been prototyped in a controlled environment (i.e. PC) wherein the scarce devices like mobile phones and set-top box performance have been emulated respectively in the J2ME Connected Limited Device Configuration (CLDC) and/or Connected Device Configuration (CDC) platforms. At the head-end, the Message Handling Subsystem (MHSS) has been prototyped where its interactions with other existing parts in the DVB system have not been accounted.

In this chapter, a programmable security platform has been considered representing most of the MICAS security architectures. In this platform, a 4-layer protocol stack is defined to handle all interactions between the entities in the MICAS. Each layer is associated with an agent which deals with responsibilities encapsulated into its layer.

The Communication Agent in the mobile phone communicates with its counterparts residing at the set-top box and MHSS respectively via Bluetooth transport and GSM protocols.

The Security agents are responsible to ascertain that the confidentiality, integrity and availability (known as the CIA Triad) criteria are guaranteed across the MICAS platform. In addition to the triple-A processes (Authorisation, Authentication and Accounting), cryptographic techniques have been employed to provide higher security level. These techniques include message digests (hash functions), digital signature and encryption to establish integrity, authenticity and non-repudiation. Moreover, the session management mechanism can be used to prevent any repetition in security processes. The set-top box and mobile Security agents authenticate each other using a symmetric cryptographic algorithm.

The MHSS CA agent can communicate with the set-top box CA agent and mobile CA agent respectively through Broadcasting and GSM networks. The MHSS CA agent (CA Manager) can transfer Security Objects either directly or through an intermediary to each CA agent. The intermediary can be either the mobile CA agent or set-top box CA agent. The scheme, which has been considered in the MICAS, is to employ both broadcasting and GSM channels to deliver a confident CA mechanism to the receiver-end. In this case, the MHSS CA agent will broadcast set-top box CA agent and/or CA-related credentials (i.e. EMM, ECM) to set-top boxes using an object carousel. It also loads the mobile CA agent and/or CA credentials (i.e. MK) on the SIM card using the Over-the-Air technology in the GSM network. The CA agent is an unbound application since it is not bounded to any services therefore in OCAP-compliant systems it needs to be described in an XAIT table.

The highest level in the MICAS protocol stack is the application layer. It handles all interactions that may take place between a viewer and set-top box (local interaction) or between a viewer and service provider (interaction over return channel). The native or stored (unbound) applications, which are broadcast and/or downloaded to a set-top box, will be used to handle interactions.

In addition to the MPEG-PSI and DVB-SI tables, the MICAS employs the Subscription Association Table (SAT) which advertises available service providers and their packages (products) to which TV consumers can subscribe. The subscription viewing packages can be played out in the form of XML files where the network, service provider and its packages are described.

The reference model proposed for implementation can be tailored and applied to the MICAS security architectures. The architectures demonstrate different attributes with regards the security, complexity, cost and performance criteria.

In the MICAS security analysis, the adverse impact of a security event has been described in terms of loss or degradation of the following three security goals: integrity, availability, and confidentiality.

The most likely attack in the Pay-TV system has been against the key information and credentials. Consequently, in a 3-level key hierarchical system, the most likely attack would be against the MK to obtain the SK and CW. The risk of the key attack has been assessed in different security architectures by multiplying the risk scale and impact significant. The attack implies the least impact on the security architectures (3), (6), (8) and (10) where the MK and SK are stored in the SIM and only CWs are exposed on a less secure Bluetooth link. However, the high frequency of CWs makes the piracy difficult. On the other hand, the security architecture (9) is attributed as the most vulnerable architecture as it exposes the actual contents on the Bluetooth channel.

The complexity of the conditional access system lies chiefly in the CA message handling used at the head-end and receiver-end in the broadcast-only Pay-TV systems. The design of the EMM injector at the head-end, synchronisation mechanisms, message filtering and processing at the receiver-end are some challenges of the kind. Most of these challenges are yet applicable to the MICAS architectures. However, integrating the mobile technology as a bi-directional channel in the MICAS mitigates the complexity of CA message handling. Nevertheless, supporting advanced interactive services and enforcing an on-line security mechanism will potentially add more complexity at both ends which is very much related to the design and implementation of the firmware.

The overall complexity of the MICAS architectures has been calculated based on the following measures: the emergent complexity which depends on the observer and obtained via conducting a survey amid 50 people, interdependencies of the modules and CA message handling. Quantifying the

last two criteria in complexity measurement has remained indefinite as it mainly depends on the implementation and algorithm used in the architecture. In a first layer of analysis, a simple comparison amid architectures has been deducted to realise which solution is less complex for the implementation.

The result of survey emphasises on implementing user-friendly set-top box and mobile applications to enable viewers readily to go through the MICAS use-cases. It also necessitates that the interdependency of return channel elements (i.e. MHSS, mobile phone, set-top box) needs to be mitigated to relieve the viewer from being bound to the set-top box. The interdependency strictly related to the key management and distribution schemes. The less frequent contact is made over the GSM route the less interdependency is required amidst the elements. Finally, the CA-related complexity at the head-end and receiver-end (i.e. set-top box) will be lessened by effectively shifting all/part of CA-related processes to the mobile phone. Considering that mobile phones are becoming more resourceful, therefore installing small sized applications on the SIM or ME will unlikely affect mobile phones' performance. The overall complexity simply represents the average of emergent, interdependency and CA-related complexity factors. The security architecture (1) has been recognised as the least complex architecture and architecture (3) is the most complex one. The architecture (4) and (5) are recognised as fairly complex architectures.

The set-top box cost is no longer counted as part of the deployment cost in the MICAS as it is paid by viewers. However, the additional cost of using GSM services (i.e. send/receive SMS) might be added to the service provider's deployment cost. A standard set-top box which is usually used in the Pay-TV system has been considered as a reference for comparing the cost of set-top boxes which can be used in the MICAS security architectures. The production cost of the set-top box has been broadly analysed in MICAS security architectures based

on the minimum hardware components that a standard set-top box require to operate. In the analysis, the cost differentiation in the hardware components integrated in the set-top box has not been considered. It has also been assumed that the firmware and memory differentiation cost is negligible amid security architectures, though it is appreciated that some architectures require more sophisticated firmware and memory resources to handle CA processing. The Bluetooth interface is also necessary in all architectures. The analysis suggests that integrating the mobile phone in the traditional Pay-TV systems can potentially reduce number of hardware components used in the set-top box. The sophistication of the security mechanism (i.e. key hierarchy system) impacts on the set-top box cost. Thus, the security architecture (9) is attributed with the least expensive set-top box and the first architecture with the most expensive set-top box. The security architecture (5) is attributed with a fair set-top box.

The following formula has been used to present an overall pre-deployment measurement based on the security risk, complexity and cost which have reverse impact on the performance of the MCIAS.

$$LikelyDeploymentSuccessRate(LDSR)\% = \frac{1}{SecurityRisk \times Complexity \times Cost} \times 100$$

All in all, the security architecture (9) is attributed with the lowest and (8) with the highest LDSR. The security architecture (1) has the minimum deviation from the average LDSR and (8) has the maximum deviation implying that the security architecture (1) can be a conservative solution and (8) can be the ideal security architecture for deployment.

8 CONCLUSION & FUTURE WORKS

With the digital content market continuing to evolve, Telco and Broadcast service providers are no longer limited to a distinct number of services, starting to play each other's role in the market. The convergence of players and emergence of more bundled services imply that in today's climate market, service diversity and customer care are keys to success in the business. Offering more choice, flexibility and value to customers are important approaches to keeping consumers happy and growing a company's customer base. In addition, in such a competitive market that lines of the traditional services have been shattered, affording competitive prices are equally important. Thus, service providers shall improve their performance to operate cost-effectively and making higher net profit margin.

One of the successful business models in the digital content market is the Pay-TV model wherein contents are made solely available to authorised users by adopting the CA technique. Nowadays, with the convergence of players and exposure of digital contents in various technologies, the traditional CA technique needs to be revised and adapted to new commercial and technological requirements.

The TV consumption is very much transformed from a social viewing to a personal habit. The TV consumption is more objective now; as such viewers expect to ubiquitously access their favourite programmes. The TV viewers demand for range of services in competitive prices. The freedom of choice needs to be truly practiced in the Pay-TV systems so the viewers can switch to any programmes or service providers with the least cost, as and when they want to. All of these new trends can be abstracted in the following statement: The

interoperability, affordability, interactivity, personalisation and security have become the main key elements in the Pay-TV businesses model. These factors have been evolved with the technology and demand. Some of them have a long record in the history of the Pay-TV system (i.e. interoperability); as such some solutions have been proposed to address them. However, none of them have been able to fully satisfy the said criteria and future demands.

The stakeholders (i.e. service providers) have been always interested in proprietary solutions, when it comes to the security and commercial issues. The cost of operation and service deployment are also back broken in the Pay-TV systems. The service providers are interested in a cost-effective solution to regularly update the system, handle the installation process and promptly respond to malicious activities. On the other hand, any change in existing systems will imply transformation costs which need to be justified for involved parties. Therefore, the solution at least needs to appreciate trends of the market and utilise available technologies. Such requirements have been acknowledged in the thesis project and a systematic approach has been taken to highlight the current issues in the Pay-TV system in line with available communication systems, technologies and security primitives. Taking into account the state-of-the-art approaches and techniques used to tackle the inherited issues, the project proposes a novel end-to-end security architecture cooperating Broadcast and mobile technologies. The thesis is concluded into following sections.

8.1 Digital-TV Systems

The digital TV (DTV) was introduced in late 1990s, in contrary to the analogue TV. The DTV has proved to be more flexible, bandwidth efficient and as such capable of offering more number of channels. It is predicted that the DTV will reach almost half a billion homes around the world by 2012. The report also

forecasts 43% digital penetration by 2012, up from an estimated 264 million household by end of 2007. This indicates that digital growth will accelerate as the decade progresses, especially in China, North America, Japan and India.

The digital Cable will be the main source of digital TV households, bringing in 249 million subscribers by 2012. The Direct-to-home (DTH) satellite will account for 23% of the global digital total by 2012; an overall decrease of 13% from 2007; due to the increase in Cable, IPTV and DTT. The IPTV will attract almost 37 million global subscribers by 2012. Although the IPTV will remain a niche platform but it will account for only 3% of global total by 2012. The digital terrestrial TV (DTT) on the other hand will witness a dramatic increase in number of subscribers; rose from 1.4 million in 2000 to 47.8 million in 2007 and then it is forecast to racket to 97.1 million global households by 2012. The digital growth is likely to extend away beyond the forecast period, since still 738 million homes would take analogue signals in 2012.

The interactive service support requires communication link and service enablers embedded at digital receivers. The communication link can be implemented either in the broadcasting or telecommunication networks. The cellular network (i.e. GSM) has nowadays gained worldwide popularity attracting media investors to deliver multimedia services via handheld terminals. Technologies like DVB-H and DVB-SH are of examples of such consideration. Nevertheless, the traditional TV viewing is yet recognised as the most important business model in the media industry; as such the interactive TV industry has been developing range of software applications to be run by a Middleware which sits on top of the hardware like a set-top box. The OCAP, MHEG and MHP (or Globally Executable MHP -GEM) are dominant Middleware standards operating in the North America, UK (recently in China, India and South Africa) and European countries.

8.2 GSM and Bluetooth Technologies

The GSM is the most popular mobile standard in the world connected over 2.5bn people across the world in 2008. The main driving key in the GSM technology is the roaming feature, which enables users to ubiquitously retain their contact with the network. Additionally, it enables them to simply change their service providers, enjoy range of services and mobile phones exist in the market.

The most known GSM element is the Subscriber Identity Module (SIM) card. The SIM can is a secure platform which interacts with the network through mobile equipment using a limited range of APIs. It holds the subscriber's data and operator's data, which are mainly used for security purposes (i.e. authentication, encryption). The subscribers' data in the GSM network are stored on databases namely Home Location Register (HLR) and Authentication Centre (AUC). The Visiting Location Register (VLR) is a distributed database which serves each Base Station in the network. It retains any subscriber's data that is present on that service coverage area including IMSI, MSISDN, authentication data, GSM services and the subscriber's address in the HLR.

The IMSI number is unique in the GSM network and mainly used to identify the subscriber. As its secrecy is important for the mobile operator, it is occasionally transmitted in the clear; instead, a temporary number, which is called TMSI, is used to present the subscriber in the network. In addition to the private subscriber's numbers, which are solely used by the network operator, the subscriber has a public number, which is called MSISDN and that is the known subscriber's mobile number which is used for making call or sending text messages. The SMS or text message is the most popular bi-directional communication service in the world. The GSM subscribers can also enjoy

connecting to the mobile internet sites via the WAP browser, which is secured and standardised.

Another popular wireless technology is the Bluetooth, which has largely replaced the cable application for short-range connections. The Bluetooth is considered as a technology enabler for Wireless Personal Area Network (WPAN) standardised under IEEE 802.15. The Bluetooth-enabled devices usually support various services namely Service Discovery Protocol (SDP), RFCOMM which is a cable replacement protocol, file transfer and telephony adapter commands (AT commands). There are various Bluetooth versions in the market but the most popular one is the Bluetooth 2.0, which covers up to 100 meters with data rate of 3 Mbps. It does not support IP protocols, however the next generations of Bluetooth can offer higher bit rate and more range of services.

8.3 Security Review

In the GSM system, following elements are responsible to store and save security credentials and algorithms to handle such criteria: the SIM card, handset (mobile station) and network elements such as HLR, VLR and AUC. The credentials in the system can be categorised into user identification credentials, user authentication & confidentiality and network credentials. The identification credentials are IMSI (or TMSI) and K_i which are stored securely in the SIM card. The former is used for identification and latter is used for authentication.

The security level in the GSM is attributed as moderate supporting one-way authentication, confidentiality, but limited authorisation and no non-repudiation schemes. It is secure enough for everyday use but it is not crack proof. Therefore, the next generations of the GSM offer greater security by a set of new security methods supporting mutual authentication of the network and end-user.

Another popular wireless technology is the Bluetooth. It covers between 10 and 100 meters and enjoys high frequency hopping which together make eavesdropping rather difficult. The Bluetooth-enabled device can be recognised by its name, type and 48-bit address. It has a Security Manager, which is responsible for applying device and service level security measures based on that is registered in the Service and Device databases. The default security includes authentication and encryption at the Baseband level using a shared-secret key, which is independent of any application level security. In addition, each service can enforce its own security measurement at the L2CAP level. It may include both authorisation and authentication. The measurements may vary depending on the category of a device, which can be either trusted or untrusted. The trusted device can only access to certain services, if it passes authorisation and authentication processes.

In both GSM and Bluetooth communications, the higher level of security can be achieved utilising security primitives at the application level. There are various security primitives that allow parties to establish reasonably secured communication links. In an unsecured environment such as wireless links, the key exchange algorithm (D-H) is usually used to establish a key agreement between parties. The cipher algorithms are used to transform messages before transmission. The digital signature can ensure authenticity and integrity of the messages. The digital signature can also provide non-repudiation.

8.4 Pay-TV Conditional Access Systems

The CA is a technique used in Pay-TV systems to protect payable contents from unauthorised viewing. The motivation for conditional access can be concluded to controlling costs, generating revenue and preventing commercial piracy. The

technique was firstly used in the Europe and USA and is now spreading across the globe.

The very early versions of the CA system were Simulcrypt and Multicrypt – the protocols defined by the DVB group. The DVB protocols were defined to encourage interoperability between CA systems in the Pay-TV system.

The Simulcrypt offers cheap smartcard-based set-top boxes which are dedicated to a single CA system; as such it limits end-users to Simulcrypt-enabled service providers. In practice, it requires an agreement amid service providers to use a shared scrambling system, multiplexer and each others' set-top boxes, which are not welcomed by service providers. Moreover, implementing a Simulcrypt-enabled head-end and synchronising CA messages (i.e. ECM, CW) in this system are practically difficult. This can be a barrier for newcomers to enter the market too. In addition, sharing the CA system can increase the bandwidth usage since CA messages are duplicated for every CA system implicating scalability problem. The security of the Simulcrypt is also attributed to the weakest CA system. The Multicrypt improves the interoperability using PC-Cards which are more expensive than smartcards. However, the Multicrypt-enabled set-top boxes are cheaper than Simulcrypt-enabled set-top boxes due to the fact that CA functions are mainly hosted in the PC-Card. The Multicrypt is more interchangeable and updating the CA subsystem is more convenient than Simulcrypt, as it only costs the PC-Card replacement. Both protocols have been subjected to technology enhancements. For instance the JavaCard adds more portability to the smartcard as the widely accepted and light weight Java byte-code provides a common and memory efficient platform for smartcard API developers. On the other hand, the inflexibility and interoperability have been addressed in the Multicrypt via a downloadable CA system. Consequently, defining platform independent

Nowadays, digital broadcasting receivers using metadata (DBRM) with recording and internet connectivity have become so popular. These services allow viewers to watch programmes out of normal broadcasting hours and view programme highlights using metadata. It is important to protect stored contents from unauthorised use and viewers from malicious metadata that can be reconstructed from original metadata. The content protection techniques can not provide any conditional access mechanism and conditional access techniques do not provide any mechanism for handling complex use-cases introduced by the metadata; such as the playback for only certain scenes. Thus, a distribution control technique for content and metadata was proposed using management information. However, it does not provide any access control to content through

metadata. Therefore, an advanced conditional access system for digital broadcasting receivers using metadata has been proposed. It prevents metadata tampering and unauthorised access to contents stored on DBRM using the digital signature and authentication techniques. The access control for receiving and playback are usually handled via content encryption and entitlement messages.

The CA systems discussed above mainly address the interoperability and interchange-ability issues between CA systems. They are not suitable for handling new challenges arisen by converging networks and emerging of convergent services. They are not concerned with interactivity and personalisation concepts. Moreover, they are although a little but not addressed high cost of operation and security flawed in Pay-TV systems.

8.5 Enhanced CA Solutions and Design

The network convergence as a new phenomenon has opened new business opportunities for network operators and service providers. This has already emerged in the mobile and Internet-based platforms and to some extent in the DTV. The content delivery through the Internet is now being offered in the DTV and family standards like DVB-T/-H also enable broadcasters to reach hand-held devices. The range of services has been diversified although there are still fundamental issues in the Pay-TV systems yet to be resolved. These inherited issues can be categorised as follows:

- Lack of interoperability between CA systems and vertically integrated transaction model which scales down the business for a newcomer either as a service provider, set-top box producer or CA provider;
- Inefficient usage of bandwidth for transferring CA messages and high complexity of the system due to the synchronisation issues and nature of the network used in the traditional broadcasting systems;

- High administration and operational costs, high security flaw costs will cause more expensive subscription fees and together with lack of interactivity and personalised services will decrease satisfactory level of subscribers.

Such inherited issues can be routed to the commercial requirements and technologies used in the traditional Pay-TV and broadcasting systems. Nowadays, with the advent of the technology especially in the digital communication systems, interactivity, mobility and personalisation features can be added to Pay-TV services. The Internet and mobile networks are now widely available connecting whole world together. Therefore, it is expected that information and multimedia services are delivered ubiquitously. This requirement has been addressed here via Internet, GSM and GPRS based solutions which can potentially resolve the mobility and interoperability issues in Pay-TV systems.

The GSM-based solution demonstrates novel features that can reduce the overall production cost of the set-top box, improve mobility and level of personalisation in the system. Therefore, amid the proposed architectures, the Mobile Integrated CA System (MICAS) was designed and analysed or the first time herein through various use case scenarios and security architectures.

The MICAS subscriber needs to set up his receiver equipment and bind his mobile phone to the set-top box in order to start using the MICAS services. Having received proper service information, the subscriber may sign up for a service and place his order. The subscriber can set his local control criteria while signing up. It is also possible to set multi-room services via multiple set-top boxes. During the sign-up process, the viewer may activate the Follow Me service to enjoy his subscription via any set-top box. The MICAS would enable the subscriber to amend his subscription at any time.

In the MICAS, the service provider may interact with the viewer at any stage during the sign-up and subscription amendment processes. The service provider deals with the viewer's requests, manages his account and issues statements as part of the billing process. Furthermore, the service provider regularly checks the security level in the system, downloads CA subsystem or update patches to the viewer's set-top box or mobile phone depending on the security architecture. The service provider shall also offer personalised services, relevant advertisement and take appropriate security actions based on thorough analysis of viewer's behaviour and choices.

In the MICAS, the mobility feature is based upon the unique viewer's GSM identities (i.e. MSISDN, IMSI) and unique identity burned to the standardised set-top box. The in-field information of subscribers and authenticated set-top boxes are all managed and provided to service providers by a third party data manager. To ensure that operating set-top boxes are compliant with standards enforced by an authority (regulator), all the set-top boxes shall be tested by a certificate issuer agency. The agency then registers the approved set-top boxes with the data manager to be accessed by service providers. The service provider shall contact the data manager during the validation process to identify whether the viewer and his set-top box are genuine.

The MICAS is utilises the mobile platform in the traditional Pay-TV system. The mobile and broadcasting networks can be both used to deliver multimedia services, CA messages, APIs and interactions. The mobile phone and set-top box can be used for hosting access control mechanisms and credentials. The combination of the message delivery routes and entity which hosts and deals with the CA-related processes leads to different security architectures. These architectures are attributed with different level of security, complexity and performance supporting different level of key hierarchy and CA messages.

8.6 MICAS Implementation and Analysis

The receiver-side in the MICAS has been prototyped in a controlled environment (i.e. PC) wherein the scarce devices like mobile phones and set-top box performance have been emulated respectively in the J2ME Connected Limited Device Configuration (CLDC) and/or Connected Device Configuration (CDC) platforms. At the head-end, the Message Handling Subsystem (MHSS) has been prototyped where its interactions with other existing parts in the DVB system have not been accounted.

In this chapter, a programmable security platform has been considered representing most of the MICAS security architectures. In this platform, a 4-layer protocol stack is defined and prototyped to handle all interactions between the entities in the MICAS. Each layer is associated with an agent which deals with responsibilities encapsulated into its layer.

The Communication Agent in the mobile phone communicates with its counterparts residing at the set-top box and MHSS respectively via Bluetooth transport and GSM protocols.

The Security agents are responsible to ascertain that the confidentiality, integrity and availability (known as the CIA Triad) criteria are guaranteed across the MICAS platform. In addition to the triple-A processes (Authorisation, Authentication and Accounting), cryptographic techniques has been employed to provide higher security level. These techniques include message digests (hash functions), digital signature and encryption to establish integrity, authenticity and non-repudiation. Moreover, the session management mechanism can be used to prevent any repetition in security processes. The set-top box and mobile Security agents authenticate each other using a symmetric cryptographic algorithm.

The MHSS CA agent can communicate with the set-top box CA agent and mobile CA agent respectively through Broadcasting and GSM networks. The MHSS CA agent (CA Manager) can transfer Security Objects either directly or through an intermediary to each CA agent. The intermediary can be either the mobile CA agent or set-top box CA agent. The scheme, which has been considered in the MICAS, is to employ both broadcasting and GSM channels to deliver a confident CA mechanism to the receiver-end. In this case, the MHSS CA agent will broadcast set-top box CA agent and/or CA-related credentials (i.e. EMM, ECM) to set-top boxes using an object carousel. It also loads the mobile CA agent and/or CA credentials (i.e. MK) on the SIM card using the Over-the-Air technology in the GSM network. The CA agent is an unbound application since it is not bounded to any services therefore in OCAP-compliant systems it needs to be described in an XAIT table.

The highest level in the MICAS protocol stack is the application layer. It handles all interactions that may take place between a viewer and set-top box (local interaction) or between a viewer and service provider (interaction over return channel). The native or stored (unbound) applications, which are broadcast and/or downloaded to a set-top box, will be used to handle interactions.

In addition to the MPEG-PSI and DVB-SI tables, the MICAS employs the Subscription Association Table (SAT) which advertises available service providers and their packages (products) to which TV consumers can subscribe. The subscription viewing packages can be played out in the form of XML files wherein the network, service provider and its packages are described.

The reference model proposed for implementation can be tailored and applied to the MICAS security architectures. The architectures demonstrate different attributes with regards the security, complexity, cost and performance criteria.

In the MICAS security analysis, the adverse impact of a security event has been described in terms of loss or degradation of the following three security goals: integrity, availability, and confidentiality.

The most likely attack in the Pay-TV system has been against the key information and credentials. Consequently, in a 3-level key hierarchical system, the most likely attack would be against the MK to obtain the SK and CW. The risk of the key attack has been assessed in different security architectures by multiplying the risk scale and impact significant. The attack implies the least impact on the security architectures (3), (6), (8) and (10) where the MK and SK are stored in the SIM and only CWs are exposed on a less secure Bluetooth link. However, the high frequency of CWs makes the piracy difficult. On the other hand, the security architecture (9) is attributed as the most vulnerable architecture as it exposes the actual contents on the Bluetooth channel.

Integrating the mobile technology as a bi-directional channel in the MICAS mitigates the complexity of CA message handling traditionally used in the Pay-TV systems. Nevertheless, supporting advanced interactive services and enforcing an on-line security mechanism will potentially add more complexity at both ends which is very much related to the design and implementation of the firmware. The overall complexity of the MICAS architectures has been calculated based on the following measures: the emergent complexity which depends on the observer and obtained via conducting a survey amid 50 people, interdependencies of the modules and CA message handling. Quantifying the last two criteria in complexity measurement has remained indefinite as it mainly depends on the implementation and algorithm used in the architecture. In a first layer of analysis, a simple comparison amid architectures has been deducted to realise which solution is less complex for the implementation. The result of survey emphasises on implementing user-friendly set-top box and mobile

applications to enable viewers readily to go through the MICAS use-cases. It also necessitates that the interdependency of return channel elements (i.e. MHSS, mobile phone, set-top box) needs to be mitigated to relieve the viewer from being bound to the set-top box. Finally, the CA-related complexity at the head-end and receiver-end (i.e. set-top box) will be lessened by effectively shifting all/part of CA-related processes to the mobile phone. The overall complexity simply represents the average of emergent, interdependency and CA-related complexity factors. The security architecture (1) has been recognised as the least complex architecture and architecture (3) is the most complex one. The architecture (4) and (5) are recognised as fairly complex architectures.

The set-top box cost is not counted as part of the deployment cost in the MICAS as it is paid by viewers. However, the extra charge of using GSM services (i.e. send/receive SMS) might be added to the service provider's deployment cost. The production cost of the set-top box has been broadly analysed in the MICAS security architectures based on the minimum hardware components that a standard set-top box require to operate. In the analysis, the cost differentiation in the hardware components integrated in the set-top box has not been considered. It has also been assumed that the firmware and memory differentiation cost is negligible amid security architectures, though it is appreciated that some architectures require more sophisticated firmware and memory resources to handle CA processing. The analysis suggests that integrating the mobile phone in the traditional Pay-TV systems can potentially reduce number of hardware components used in the set-top box. The sophistication of the security mechanism (i.e. key hierarchy system) impacts on the set-top box cost. Thus, the security architecture (9) and (10) are attributed with the least expensive set-top box and the first architecture with the most expensive set-top box. The security architecture (5) is attributed with a fair set-top box.

The following formula has been used to present the likely deployment success rate of the MICAS security architectures based on the security risk, complexity and cost.

$$LikelyDeploymentSuccessRate(LDSR)\% = \frac{1}{SecurityRisk \times Complexity \times Cost} \times 100$$

The security architecture (9) has the lowest and (8) has the highest LDSR. The security architecture (1) has the minimum and (8) has the maximum deviation from the average LDSR implying that the security architecture (1) can be considered as a conservative solution and (10) as an ideal solution for deploying the MICAS.

In practice, MICAS implementation requires new set of regulations and agreements concerning active parties in the MICAS business cycle including the Pay-TV service providers, mobile operators and set-top box producers. However, the system itself has been emulated in the laboratory to do the feasibility study and prove the concept. The result of the emulation showed that it is possible to incorporate wireless technologies (i.e. mobile, Bluetooth) to enhance interactivity and security features in the Pay-TV systems. There might be some concerns about the available bandwidth, interoperability of mobile phones and applications, security over the Bluetooth which all can be nevertheless addressed in the said regulated market. With the current state and by minimum changes, only the mobile phone can be used as an intermediary to transfer the key information to the set-top box. The following remarks can be made about the MICAS advantages:

The MICAS is a novel end-to-end generic security solution for the Pay-TV system. It provides a seamless access control solution and it eliminates the need of smartcard by integrating both Broadcast and Mobile technologies for the first

time in the Pay-TV system. It provides a viable intelligent platform which supports both horizontally and vertically integrated transaction models. It incorporates the wide security features of the mobile phone and SIM card to deliver a platform wherein multiple service providers can co-exist without compromising each other's security guidelines.

Moreover, MICAS effectively addresses the inherited issues in the Pay-TV system including interoperability, mobility, personalisation, cost of operation and viewers' convenience. It employs the Java technologies embedded in the set-top box, mobile phone terminals to deliver a flexible, downloadable and programmable security platform. It enables the service provider to automatically download their own security mechanism into the viewer's set-top box or mobile phone. In addition, it enables the viewers to readily change their service providers without facing extra charge for purchasing new TV access equipment like set-top box or smartcard.

Thus, MICAS enables service providers to attract more revenue by reducing customer churn rate and operational expenses. It satisfies the set-top box producer as it makes the set-top boxes cheaper (no need for smartcard) and enables them to operate in an open market without being bound to a specific service provider. It also satisfies viewers as it enables them to freely choose/change the service provider and set-top box, enjoy a wider range of affordable services and benefit from enhanced interaction mechanisms enabling them to watch TV services from any set-top box based on their entitlements.

8.7 Future Works

The project appreciates the presence of multimedia services in the converged telecommunication and broadcasting systems to continue the research on the following concepts:

- A total convergent security solution satisfying access control and content protection in three screens (mobile, PC, set-top box);
- Expanding the personalisation concept in the MICAS using artificial intelligence (AI) techniques such as user profile modelling and recommendation systems;
- Security of the multimedia contents; i.e. copyright and data protection techniques and other security aspects to ensure data privacy, integrity and finally service availability;
- Extending the Mobile TV (i.e. delivery of multimedia contents to a mobile phone), security concepts (i.e. access control, descrambling, copyright and data protection, etc.) and power consumption (i.e. battery usage) to enable viewers utilise their mobile phone as a set-top box which can send multimedia contents to a TV screen through common interfaces.

BIBLIOGRAPHY

[1] 3GPP TS 03.40, "Technical realisation of the Short Message Service (SMS) Point-to-Point (PP)", v. 7.5.0, 1998

[2] 3GPP TS 03.48, "Digital cellular telecommunications system (Phase 2+); Security mechanisms for SIM application toolkit; Stage 2", v.8.9.0 Release 1999

[3] 3GPP TS 11.14, "Specification of the SIM Application Toolkit (SAT) for the Subscriber Identity Module – Mobile Equipment (SIM-ME) interface", v. 8.18.0, 1999

[4] 3GPP TS 27.005, "Use of Data Terminal Equipment – Data Circuit terminal Equipment (DTE - DCE) interface for Short Message Service (SMS) and Data Broadcast Service (CBS)", v.7.0, 2006

[5] 3GPP TS 27.007, "AT Command set for User Equipment (UE)", v.8.4.1, Release 8

[6] 3GPP TS 31.101, "Universal Mobile Telecommunications System (UMTS); UICC-terminal interface; Physical and logical characteristics", v.7.0.1, Release 7, 2006-07

[7] 3GPP TS 42.009, "Digital cellular telecommunications system (Phase 2+); Security aspects", v.4.1.0

[8] 3GPP TS 43.020, "Technical Specification Group Services and system Aspects; Security related network functions", Release 5, 2002-05

[9] 3GPP TS 51.011, "Digital cellular telecommunications system (Phase 2+); Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface", v.4.15.0

[10] "Content Protection for Recordable Media Specification", C4 Entity, DVD Book, Rev. 0.96, 2005 [online]. Available: www.4centity.com

[11] Advanced Television Systems Committee (ATSC) standard, Advance Common Application Platform Document A/101, 2 Aug 2005

[12] MCP: Multimedia Car Platform. Available: http://www.aramis-research.ch/e/7229.html

[13] Baba A., Nishimoto Y., Kurioko T., Namba S., "A digital rights management system for digital broadcasting based on home servers", IEEE Transactions on Broadcasting, Jun 2006, vol. 52, no. 2, pp. 167-172

[14] Barker W. C., "Recommendation for Triple Data Encryption (TDEA) Algorithm", Information Security, National Institute of Standard and Technology (NIST), Technology Administration, U.S. Department of Commerce, special publication 800-67 v.1, May 2004

[15] Benoit, H., "Digital Television: MPEG-1, MPEG-2 and Disciplines of the DVB System", 2nd Edition 2002, London, Focal Press, ISBN: 0240516958

[16] D-Box software Betanova v.1.0 [online]. Available:

http://alt.digitv.de/Hardware/betanova.shtml

[17] Bruce Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition, John Wiley & Sons, Inc., ISBN: 0-471-12845-7, 1995

[18] Cruselles E., Melus J. L., Soriano M., "An overview of security in Eurocrypt Conditional Access System", IEEE Global Telecommunications Conference, GLOBECOM '93, Huston, 1993, vol. 1, pp. 188-193

[19] Digital Audio-Visual Council (DAVIC), "DAVIC 1.4 specifications part 10", 1998

[20] Digital Broadcasting Expert Group (DiBEG). Available www.dibeg.org

[21] European DRiVE (Dynamic Radio for IP-Services in Vehicular Environments) Project, IST-1999-12515

[22] Digital Transmission Licensing Administrator (DTLA), "Digital Transmission Control Protection Specification", vol.1 (information version), Rev. 1.4, 2005 [online]. Available: www.dtcp.com

[23] Digital Video Broadcasting (DVB). Available www.dvb.org

[24] DVB SCENE, "Tune into Digital Convergence", Mar 2009, Edition no. 29, pp.04

[25] Digital Video Broadcasting (DVB); "Framing structure, channel coding and modulation for 11/12 GHz satellite services", ETSI EN 300 421, v1.1.2, 1997-8

[26] Digital Video Broadcasting (DVB); "Framing structure, channel coding and modulation for cable systems", ETSI EN 300 429, v1.2.1, 1998-04

[27] Digital Video Broadcasting (DVB); "Satellite Master Antenna Television (SMATV) distribution systems", ETSI EN 300 473, v1.1.2, 1997-8

[28] Digital Video Broadcasting (DVB; "Framing structure, channel coding and modulation for digital terrestrial television", ETSI EN 300 744, v1.5.1, 2004-06

[29] Digital Video Broadcasting (DVB); "Interaction channel through the Global System for Mobile communications (GSM)", ETSI EN 301 195, v1.1.1, 1999-02

[30] Digital Video Broadcasting (DVB); "Interaction channel for satellite distribution systems", ETSI EN 301 790, v1.3.1, 2003-03

[31] Digital Video Broadcasting (DVB); "Transmission system for handheld terminals", ETSI EN 302 304, v1.1.1, 2004-11

[32] Digital Video Broadcasting (DVB); "Second generation framing structure, channel coding and modulation systems for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications", ETSI EN 302 307, Draft v1.1.1, 2004-06

[33] CENELEC EN 50201: "Interfaces for Digital Video Broadcast Integrated Receiver Decoder (DVB-IRD)", 2001

[34] Digital Video Broadcasting (DVB); "Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications", ETSI EN 50221, CENELEC, Feb 1997

[35] Digital Video Broadcasting (DVB); "DVB interaction channel for Cable TV distribution systems (CATV)", ETSI ES 200 800, v1.3.1, 2001-10

[36] Digital Video Broadcasting (DVB); "Multimedia Home Platform (MHP) Specification 1.0.3", ETSI Specification ES 201 812, Dec 2003

[37] Digital Video Broadcasting (DVB); "Support for use of scrambling and conditional access within digital broadcasting systems", ETSI ETR 289, Oct 1996.

[38] GSM 07.06: "European digital cellular telecommunications system (Phase 2); Use of the V series Data Terminal Equipment - Data Circuit terminating Equipment (DTE - DCE) interface at the Mobile Station (MS) for Mobile Termination (MT) configuration", ETSI ETS 300 586, v2, 1995-07

[39] Clément J. P., Février P., "Eurocrypt, A Technical Approach", International Broadcasting Convention IBC 1990, 21-25 Sep 1990, pp. 278-281

[40] Faria G., Henriksson J. A., Stare E., Talmola P., "DVB-H: Digital Broadcast Services to Handheld Devices", Proc. of the IEEE Jan 2006, vol. 94, no. 1, pp. 194-209

[41] Francis L., Sirett W. G., Mayes K., Markantonakis K. "Countermeasures for attacks on satellite TV cards using open receivers", Third Australasian Information Security Workshop (AISW2005), Conference in Research and Practice in Information Technology 2005, vol. 108, pp. 153-158

[42] Giachetti J., Lenoir V., Codet A., Cutts D., Sager J., "A common conditional access interface for digital video broadcasting decoders", IEEE Transaction on Consumer Electronics Aug 1995, vol. 41, no.3, pp. 836-841

[43] GlobalPlatform, "Card Specification", The standard for global infrastructure, v.2.2, March 2006

[44] Gross D., Harris C. "Fundamentals of queuing theory", John Willey & Sons, New York, 1998

[45] Digital Cellular Telecommunications System (Phase 2+); "Teleservices supported by a GSM Public Land Mobile Network (PLMN)", ETSI GSM 02.03, v.6.0, 1997

[46] Digital Cellular Telecommunications System (Phase 2+); "Technical Realization of the Short Message Service (SMS) Point-to-Point (PP)", ETSI GSM 03.40, v.5.2.0, Jan 1996

[47] Digital Cellular Telecommunications System (Phase 2+) (GSM); "Technical realization of Short Message Service Cell Broadcast (SMSCB)", ETSI GS GSM 03.41, 1996

[48] Digital Cellular Telecommunications System (Phase 2+) (GSM); "General on Terminal Adaptation Functions (TAF) for Mobile Stations (MS)", ETSI GTS GSM 07.01, v.5.0.1, Apr 1996

[49] Digital Cellular Telecommunications System (Phase 2+); "Terminal Adaptation Functions (TAF) for services using asynchronous bearer capabilities", ETSI GTS

GSM 07.02, v.5.1.0, 1996-05

[50] Digital Cellular Telecommunications System – "Signalling requirements on inter-working between the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN) and the Public Land Mobile Network (PLMN)", ETSI GTS GSM 09.03, v.5.0.0, 1996-12

[51] Digital Cellular Telecommunications System (Phase 2+) (GSM); "General requirements on interworking between the Public Land Mobile Network (PLMN) and the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN)", ETSI GTS GSM 09.07, v.5.0.1, Mar 1996

[52] GSM World Coverage, GSM Association and Europa Technologies, Edition A, Jan 2008 [online]. Available: www.gsmworld.com

[53] Guthery S., Cronin M., "Mobile application development using SMS and the SIM toolkit", McGraw-Hill 2002, ISBN: 0-07-137540-6

[54] Informa Telecoms & Media, Global Digital TV, 7th Edition, Management Report, 2007

[55] EU-FP6 Integrated Project INSTINCT (IP-based Networks, Services and Terminals for Converging systems), IST2003-507014

[56] Information Technology, "Coding of multimedia and hypermedia information – Part 5: Support for base-level interactive applications", ISO/IEC International Standard ISO/IEC 13522-5, 1997

[57] Information Technology, "Coding of multimedia and hypermedia information – Part 6: Support for enhanced interactive applications", ISO/IEC International Standard ISO/IEC 13522-6, 1998

[58] Information Technology, "Coding of multimedia and hypermedia information – Part 7: Interoperability and conformance testing for ISO/IEC 13522-5", ISO/IEC International Standard ISO/IEC 13522-7, 2001

[59] Information Technology,"Coding of multimedia and hypermedia information – Part 8: XML notation for ISO/IEC 13522-5", ISO/IEC International Standard ISO/IEC 13522-8, 2001

[60] ISO/IEC 7816-x, "Identification cards – integrated circuit(s) cards with contacts", 1987

[61] Jennings S. M., "A Special Class of Binary Sequences", PhD Thesis, University of London, 1980, Chapter 2, pp. 57-61 & Chapter 4, pp. 156-161, United States Patent Number: 4748576

[62] JSR-117 JCP 2004, "Security and Trust Services API (SATSA) (JSR-117)", Sun Micorsystems [online]. Available: java.sun.com

[63] JSR-118 JCP 2002, "Mobile Information Device Profile, v.2.0 (JSR-118)", Sun Micorsystems [online]. Available: java.sun.com

[64] JSR 272: "Mobile Broadcast Service API for Handheld Terminals", Sun Micorsystems [online]. Available: java.sun.com

[65] Kamperman F., Rijinsoever B. V. "Conditional access system interoperability through software downloading", IEEE Transaction on Consumer Electronics Feb 2001, vol. 47, no. 1, pp. 47-54

[66] Karygiannis T., Owens L., "Wireless Network Security, 802.11, Bluetooth and hand-held devices", Computer Security Division, National Institute of Standards and Technologies (NIST), Special Publication 800-48, Nov 2002

[67] Kirkels B., Maas M., Roelse P. "A Security Architecture for Pay-Per-View Business Models in Conditional Access Systems", ACM Workshop On Digital Rights Management 2007, Virginia, USA, ISBN:978-1-59593-884-8

[68] Kumar C. B., Kline P. J., Thompson T. J., Thompson T. "Bluetooth Application Programming with Java APIs", Morgan Kaufman Publishers, Elsevier Inc. 2004, ISBN: 1-55860-934-2

[69] Lenoir V., "Eurocrypt, A successful Conditional Access System", IEEE Transactions on Consumer Electronics Aug 1991, vol. 37, no. 3, pp. 432-436

[70] Liu B., Zhang W., Jiang T. "A Scalable key Distribution Scheme for Conditional Access System in Digital Pay-TV System", IEEE Transaction on Consumer Electronics May 2004, vol. 50, no. 2, pp. 632-637

[71] Looms P. O. "Digital TV in Europe–How Important is Interactivity", Portuguese Association of Electrical Engineers, 9 Feb 2004, Lisbon, Portugal, pp. 1-12

[72] MacDonald J. A., Sirett W., Mitchell C. J., "Overcoming channel bandwidth constraints in secure SIM applications", 20th IFIP International Information Security Conference (Sec 2005) - Small Systems Security and Smart cards, Makuhari-Messe31 May 2005, Chiba, Japan, pp. 1-11

[73] Report on Technical Issues of Coexistence of MHEG-5 and MHP based services and enabling Migration to MHP, Written for UK DTI by Strategy & Technology Ltd. in conjunction with UK experts on MHEG and MHP, 8th May 2002

[74] The Microsoft TV Platform Microsoft Corporation. Available:
http://www.microsoft.com/tv/default.mspx

[75] Minami H., Baba A., Nishimoto Y., Kurioka T., Uehara T., "Study of integrated services with broadcasting, stored and internet contents", IEEE International Conference on Consumer Electronics, ICCE 2002, pp.116–117

[76] Mooji W. G. "Conditional Access System for Digital Television", IEEE International Broadcasting Convention, IBC Sep 1994, pp. 489-491

[77] Morris S., Chaigneau A. S., "Interactive TV Standards: A Guide to MHP, OCAP, and JavaTV", Contributor Anthony Smith-Chaigneau, Published by Focal Press, 2005, ISBN 0240806662

[78] Namba S. "Technologies and Services on Digital Broadcasting – Scrambling (Conditional Access System)", NHKS STRL, Broadcast Technology no.12, 2002

[79] NDS, MediaHighway Middleware Solution [online]. Available: www.nds.com/solutions/mediahighway.php

[80] Nishimoto, Y.; Baba, A.; Kimura, T.; Imaizumi, H.; Fujita, Y., "Advanced Conditional Access System for Digital Broadcasting Receivers Using Metadata", IEEE Transaction on Broadcasting Sep 2007, vol. 53, Issue 3, pp. 697-702

[81] "A guide to understanding NRSS parts A and B", SPECS International vol. 9, no. 7, Nov 1997

[82] OCAP 1.0 profile, "OpenCable™ Application Platform Specification", document control number OC-SP-OCAP1.0-I16-050803, Aug 2005

[83] Open TV [online]. Available: http://www.opentv.com

[84] Open Platform Initiative for Multimedia Access (OPTIMA), "OPTIMA 1.0 Specification", Oct 1999

[85] "PCMCI - Personal Computer Memory Card International Association, PC Card standard", vol. 2-4 Feb 1995

[86] Piesing J., Invited paper, "The DVB Multimedia Home Platform (MHP) and Related Specifications", Proc. of the IEEE Jan 2006, vol. 94, no. 1

[87] EU-FP6 Integrated Project PLUTO (Physical Layer DVB Transmission Optimisation), IST-4-026902, 2006-2008, http://www.ist-pluto.org

[88] Prasertsatid N., "Implementation Conditional Access System for Pay-TV based on Java Card", 3rd IEEE Conference on Computational Electromagnetic and its Application Nov 2004, pp. 399-402

[89] Ulrich Reimers, "DVB - The Family of International Standards for Digital Video Broadcasting", 2nd Edition, pp. 303-336, ISBN 3-540-43545-X Springer Berlin Heidelberg New York 2005

[90] "Randomness Recommendations for Security", IETF RFC 1750, Dec 1994

[91] "HMAC: Hash-keyed for Message Authentication", International Engineering Task Force (IETF), Request for Comments (RFC) 2104, Feb 1997

[92] T. Dierks, C. Allen., "The Transport Layer Security (TLS) Protocol v.1", IETF RFC 2246, Jan 1999

[93] Housley R., "Cryptographic Message Syntax", Network Working Group, Jun 1999

[94] Hoffman P., "Enhanced Security Services for S/MIME", Network Working Group, Jun 1999

[95] "Extendible Authentication Protocol method for Global System for Mobile communications (GSM) Subscriber Identity Module (SIM)", RFC-4186, Network Working Group, January 2006

[96] Shannon C. "A mathematical theory of communication", Bell System Technical Journal Jul/Oct, 1948, vol. 27, pp. 379–423, 623–656,

[97] Shirazi H., Cosmas J., Cutts D., Birch N., Daly P. "Security Architectures in Mobile Integrated Pay-TV Conditional Access System", 13th IEEE International Telecommunications Network Strategy and Planning Symposium, Networks

2008, Hungary, Sep 2008, pp. 1-15

[98] Shirazi H., Cosmas J., Cutts D., Birch N., Daly P. "Mobile Integrated Conditional Access System (MICAS)", 16th IEEE International Symposium of Consumer Electronics, Apr 2008, pp. 1-4

[99] "Technical Specification of DVB Simulcrypt", DVB Project Office, Apr 1997

[100] Sirett W. G., MacDonald J. A., Mayes K., Markantonakis K. "Secure Deployment of Applications to Fielded Devices and Smart Cards", 4th International Workshop on Security in Information System (WOSIS 2006), Institute for Systems and Technologies of Information, Control and Communication, ICEIS May 2006, Paphos, Cyprus, pp. 195-207

[101] Stoneburner G., Goguen A., Feringa A., "Risk Management Guide for Information Technology Systems", Recommendations of the National Institute of Standards and Technology (NIST), special publication 800-30, Jul 2002

[102] "Technical Report of the Conditional Access Specialist Group", EP-DVB document no. TM1244 Rev. 1, Geneva, 1994

[103] Digital Video Broadcasting (DVB), "Implementation of Binary Phase Shift keying (BPSK) Modulation in DVB satellite transmission systems", European Telecommunication Standards Institute (ETSI), TR 101 198, v.1.1.1, 1997-09

[104] Digital Video Broadcasting; DVB-Internet Protocol Infrastructure (DVB-IPI), Architectural Framework for the Delivery of DVB-Services over IP-based Networks. ETSI TS 102 033, Feb 2002

[105] Digital Video Broadcasting (DVB); "User guidelines for the second generation system for Broadcasting, Interactive Services, News Gathering and other broadband satellite applications (DVB-S2)", ETSI TR 102 376, v.1.1.1, 2002-05

[106] 3rd Generation Partnership Project; "Technical Specification Group Core Network; Mobile Application Part (MAP) specification (Release 1998)", 3GPP TS 09.02, v.7.15.0 (2003-04)

[107] Digital Video Broadcasting (DVB); "Transport of MPEG-2 Based DVB Services over IP Based Networks", ETSI TS 102 034, Mar 2005

[108] ETSI TS 102 223, "Smart cards; Card Application Toolkit (CAT)", Release 4

[109] Digital Video Broadcasting (DVB); "DVB-S2 Adaptive Coding and Modulation for Broadband Hybrid Satellite Dialup Applications", ETSI 102 441, v.1.1.1, 2005

[110] Digital Video Broadcasting (DVB); "System Specifications for Satellite services to Handheld devices (SH) below 3 GHz", ETSI TS 102 585, v.1.1.1, 2007

[111] Digital Video Broadcasting (DVB) Bluebook A129; "Content Protection and Copy Management Specification; Part 13: CPCM Compliance Framework", draft TS 102 825-13 v.1.1.1

[112] Digital Video Broadcasting (DVB); "DVB Simulcrypt, Part 1: Head-end architecture and synchronization", ETSI TS 101 197-1, Jun 1997

[113] TV-Anytime Forum, "Specification series: S-3 on Metadata (Normative)", SP0003, v.10, 2001

[114] IETF and W3C Recommendation, "XML-Signature Syntax and Processing", Feb 2002

[115] Wirt K., "Fault attack on the DVB Common Scrambling Algorithm", Springer-Verlag Berlin Heidelberg, ICCSA 2005, LNCS 3481, pp. 577–584

[116] Xie Q. Zheng S. "A Smartcard Conditional Access Subsystem Separation Scheme for Digital TV Broadcasting", IEEE Transactions on Consumer Electronics Aug 2005, vol. 51, no. 3, pp. 925-932

[117] Yamaguchi T., Matsumura H., Kawazoe K., "Distribution control technology using metadata for cooperative broadcasting and communication services", NTT Technical Review, vol. 2, no. 8, pp. 58-62, 2004

[118] Zeng K., Yang C-H, Wei D-Y, Rao T.R.N., "Pseudorandom Bit Generators in Stream-Cipher Cryptography", IEEE Transactions on Cryptography Feb 1991, vol. 24, Issue 2, pp. 8 – 17,

[119] Zheng M., Zheng S-B., "A Common Smart-card-based Conditional Access System for Digital Set-top Boxes", IEEE Transactions on Consumer Electronics May 2004, vol. 50, no. 2, pp. 601-605