A Cooperative Cellular and Broadcast Conditional Access System for Pay-TV Systems

Shirazi H., Cosmas J.[1], Cutts D.[2]

1- Brunel University, Uxbridge, Middlesex, UK; 2- Strategy & Technology Ltd. London, UK.

***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. As a result, this paper presents the Mobile Conditional Access System (MICAS) as an end-to-end access control solution for Pay-TV systems. It incorporates the mobile and broadcasting systems and provides a platform whereby service providers can effectively interact with their customers, personalise their services and adopt appropriate security measurements. This would result in the decrease of operating expenses and increase of customers' satisfaction in the system. The paper provides an overview of state-of-the-art conditional access solutions followed by detailed description of design, reference model implementation and analysis of possible MICAS security architectures.**

***Index Terms*— Pay-TV, Conditional Access System, Mobile, Set-top box.**

I. Introduction

THE consumption of TV is very much transformed from a social viewing to become more personalised. The TV consumption is more objective now; as such viewers expect to ubiquitously access their favourite programmes. The TV viewers demand for a range of services in the competitive prices and freedom of choice to switch to any programmes or service providers with the least cost, as and when they wish. Such trends can be abstracted in the following statement: the interoperability, affordability, interactivity, personalisation and security are becoming the main key elements in the Pay-TV business model. These factors have been evolved with the technology and demand.

The service providers on the other hand have been always interested in proprietary solutions when it comes to the security and commercial issues. They are interested in a cost-effective solution to regularly update the system, handle the installation process, promptly respond to malicious activities and interact effectively to retain their customers.

There has always been a trade-off between service providers' and viewers' expectations in the traditional Pay-TV systems. Tackling the interoperability issue has been the main objective in the Digital Video Broadcasting (DVB) conditional access protocols (Simulcrypt [2] and Multicrypt [3]), though owing to technical and commercial reasons, they have not gained wide acceptance in the DTV market. Issues like increasing the bandwidth requirement, security, sharing the platform in the Simulcrypt and higher cost and complexity in the Multicrypt are also amongst the pitfalls of DVB protocols. Nevertheless, solutions like downloadable CA system [4] or using a common smart-card-based CA system have been proposed to mitigate the inherent issues such as the control relationship and encouraging private CA systems. Introduction of more intelligent and resourceful smartcards (i.e. Java Card) has also evolved the DVB protocols supporting more dynamic features in the access control mechanism [5]. All the same, the solutions have not taken into account the actual requirements in the enhanced Pay-TV systems where ever evolving customers' interest shall equally be treated as service providers'. Such requirements necessitate a return channel in the DTV system architecture which is capable of promoting the personalisation concept. Thus, the best to-date bi-directional communication channel is the GSM network, which is not only secured, but also popular in the world. It owns a security element (SIM card) which can ultimately be considered as a replacement for the smartcard technology in the Pay-TV system. It supports various software and hardware features that are required to implement a scalable CA solution.

The cooperation of mobile technology with the broadcasting system is considered for the first time herein as an end-to-end access control solution in Pay-TV systems. The paper presents full aspects of the novel Mobile Integrated Conditional Access System (MICAS) to prove the concept that it can provide a scalable platform to offer interoperability, wider range of interactive services, higher security and more affordable services. Various use case scenarios and security structures are presented to highlight the design aspects of MICAS. A

Manuscript received June 16, 2009. This work was supported in part by Strategy & Technology (S&T) Ltd as the project iPACE-TV (Interactivity, Personalisation and Access Control Enhancement in Pay-TV Systems).

H. Shirazi, J. Cosmas are with the School of Engineering and Design, Brunel University, Uxbridge UB8 3PH, United Kingdom (e-mail: Hamidreza.shirazi@brunel.ac.uk; John.Cosmas@brunel.ac.uk)

D. Cutts is manager director and owner of S&T Ltd 4th Floor, 1 Benjamin Street, London, EC1M 5QG, UK (email: David.cutts@s-and-t.com)

business collaboration structure is proposed followed by a reference model implementation. Then, respective security architectures are analysed versus security vulnerabilities, system complexity and set-top box production costs. Finally, the conclusion is drawn out.

II. General Pay-TV System

The Pay-TV CA system usually consists of the two following subsystems:

1) The Scrambling Subsystem: This is responsible for scrambling the signal at the head-end and descrambling it at the receiver-end;
2) The Control Access Subsystem: This processes access control messages to determine whether descrambling must be performed. The DVB project has defined two conditional access messages namely the Entitlement Control Message (ECM) and Entitlement Management Message (EMM) [6].

The ECM is restricted to 256 Bytes and usually 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; such as local control (i.e. using a parental rating system) and geographical black out (i.e. domestic channels). The second field contains an encrypted Control Word (CW) and the last field contains a data integrity check.

The EMMs are transmitted in advance in order to give access to the authorised subscribers. In 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. Such a requirement is 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 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 the 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 subscriber is identified using its smart card unique address or group address. 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. 1 and Fig. 2 present the processes that usually take place at the transmitter and receiver sides respectively, in a general Pay-TV system.

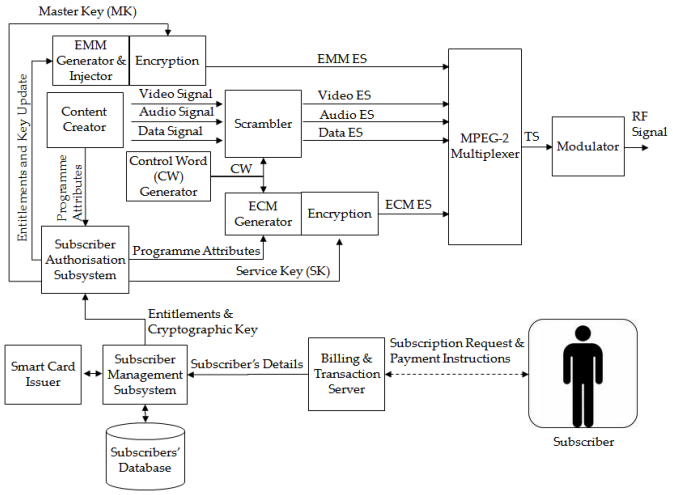

Fig. 1: The head-end structure in a general Pay-TV system

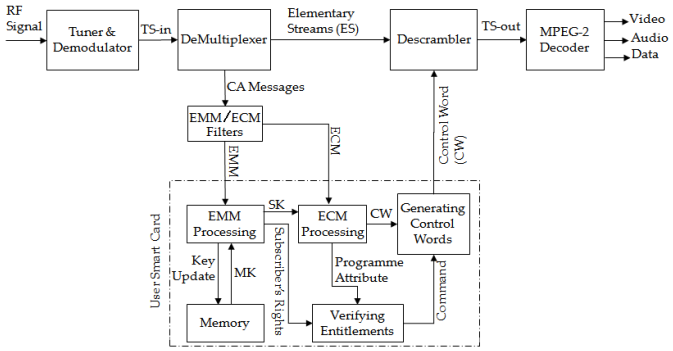

Fig. 2: The receiver-end structure in a general Pay-TV system

III. Enhanced CA Solutions

There are still fundamental issues in the Pay-TV systems yet to be resolved. These inherited issues can be categorised as follows:

1) 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;
2) Inefficient usage of bandwidth for transferring CA messages and high complexity of the system due to the synchronisation issues and nature of the network (unidirectional) used in the traditional broadcasting systems;
3) High administration and operational costs, and high security flaw costs will cause more expensive subscription fees and together with lack of interactivity and personalised services will decrease satisfaction level of

subscribers.

Such inherited issues can be expressed as 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 (i.e. convergence of telecom and broadcasting 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 can be delivered ubiquitously. The following subsections consider the abovementioned issues and propose high-level solutions to resolve the mobility and interoperability in the Pay-TV systems.

A. Cooperating broadcast and Internet CA system

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

Fig. 3 shows the overall architecture of the cooperating Internet and broadcast conditional access system.

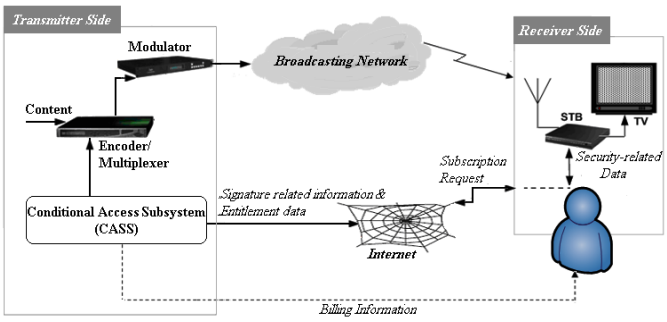

Fig. 3: The reference model for Internet integrated CA system

B. 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. 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 operator grants the permission, the SIM can be used to store and deploy conditional access mechanisms. Hence, it can be considered as an alternative to the smartcard. The 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 so that the subscriber no longer needs to be at home and at the vicinity of a pre-selected set-top box to enjoy his/her entitlements. The one-to-one rigid relationship between an authorised subscriber and his set-top box can be adjusted, if the service provider could uniquely identify the subscriber and his set-top box so to ultimately prevent any anticipatory repudiation and piracy. In this approach, the subscriber can be identified through a challenge/response authentication process or via his International Mobile Subscriber Identity Number (IMSI) or mobile number stored in his SIM card. His mobile phone can be identified by its International Mobile Equipment Identity (IMEI) and his location can be recognised by Location Identifier (LI) 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.

Fig. 4 shows the architecture of the mobile integrated conditional access system (MICAS) in Pay-TV systems.

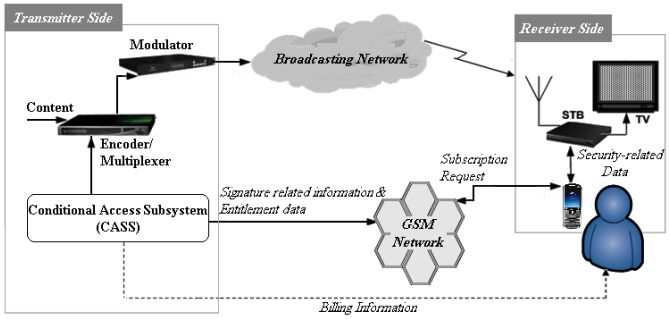

Fig. 4: The reference model for GSM integrated CA system

In the next generations of GSM technology (i.e. GPRS, UMTS, LTE and 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 or its equipment identity number or MAC address. The registration and identification processes can also be executed similarly.

All in all, the Internet-only architecture will neither decrease the overall production cost of the set-top box nor improve mobility, nor 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 solution (i.e. GSM or GPRS solutions) can possibly reduce the overall cost of the set-top box by at least replacing the smartcard in the set-

top box with the SIM card in the mobile phone. These solutions will also provide a flexible platform to improve mobility and personalised services in the Pay-TV system. Also, it distinguishes itself from Mobile-TV CA systems [20] as it cooperates with a set-top box to enable the viewer to watch TV programmes on a TV screen. Therefore, amid the proposed architectures, the mobile integrated solution is considered herewith as a primary and novel approach to be analysed further. The functional requirements are elicited in the next section, followed by describing various architectural models of the system.

IV. MICAS Design

The MICAS encompasses various security architectures concerning the distribution of entitlements and access key information to the viewers. Following a brief description of MICAS use-cases, the security architectures will be detailed.

A. *Functional requirements - Use case scenarios*

The service provider needs to provide the MICAS services on new type of set-top boxes and sign an agreement with mobile phone operators to use their SIM cards. The set-top box identity (STB_ID) can be used by the service provider to authenticate the set-top box and identify 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 the encoded streams, the viewer can subscribe to any available services using an arbitrary set-top box and his mobile phone. The corresponding service provider will manage the subscriber's account and provide him with a proper mechanism to decode the paid contents.

Fig. 5 presents possible use case packages defined in the MICAS. Each package is now briefly explained.

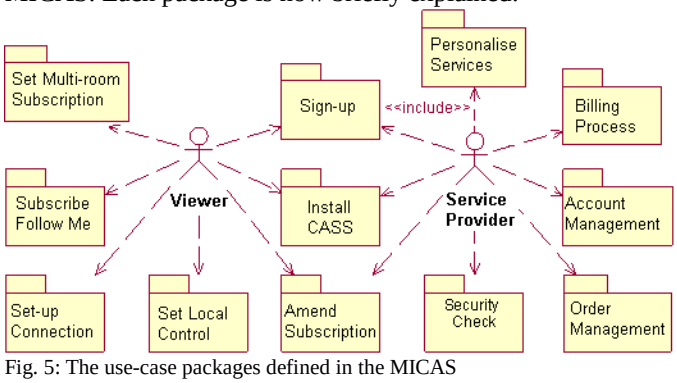

Fig. 5: The use-case packages defined in the MICAS

1) Set-up connection: the set-top box shall provide the viewer with appropriate service-menus to connect his mobile phone to the set-top box via the Bluetooth link. The viewer needs to activate the Bluetooth and bind his mobile phone to the set-top box for enjoying MICAS features.

2) Sign-up: The ultimate goal would be to enable the viewer to purchase a range of services (i.e. subscriber TV, pay-per-view) from different service providers.

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 on the TV screen using a remote control.

3) Set local control: The viewer may consider his criteria to filter some channels (programmes) which are unsuitable for the rest of the family (i.e. children). The local control preferences can be set (or 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 based on violence, substance abuse and etc.

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

4) Subscribe to multi-room service: It extends the personal viewing and 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) and register the rest of his set-top boxes (as clients) with the server. The registration can be pursued by retrieving the client identifier (Client-ID). In the end, the list of client(s) will be shown to the viewer and enclosed within the viewer's order to keep the service provider abreast of the receiver side configuration. The 'multi-room service' can be opted during the 'sign-up' procedure.

5) Subscriber to Follow Me service: This allows a subscriber to ubiquitously access his entitlements. This service will manifest the 'Anything Anytime Anywhere' paradigm. It is particularly suitable for viewers who spend most of their time in travelling and tend to have the habit of targeted viewing (i.e. sport or news programmes).

The viewer can sign up for the service through an arbitrary set-top box connected to the viewer's mobile phone for instance via the Bluetooth connection. The requested service message can be sent via the return channel to the service provider. The message shall include sufficient information to enable the service provider to identify the viewer, set-top box and the CASS already assigned to the viewer.

6) Amend subscription: When a viewer applies for the amendment or cancellation of his subscription, the security applications (if any) installed in the viewer's mobile phone and/or set-top box shall transit to the suspension state, waiting for the service provider's command to function. The service provider may react according to the contractual terms followed by updating the viewer's subscription profile. Updated Key information shall be sent to the viewer in case that he requests for subscription amendment and CA subsystem shall be disabled if he cancels the policy.

7) Subscriber account management: In the conditional access system proposed in DVB project, the Subscriber Management Subsystem (SMSS) is responsible for managing subscribers' information. The MICAS will remain compatible

with the SMSS 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 the 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 and etc.

8) Order management: 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. The order has to be forwarded to the billing section. If banking transactions are authorised successfully, the service provider will process the viewer's order.

9) Billing process: The service provider issues the bill based on the viewer's subscription profile and contracted tariff. The bill shall be issued prior to the service, and if there is any change of fee, the service provider shall inform the viewer in advance. The viewer can set-up the payment method during the 'signing up'.

10) Download CASS: Given that all validation processes on the viewer identity and set-top box succeeded, the service provider shall start deploying his tailored conditional access subsystem in the viewer's SIM card and/or set-top box through the GSM network [7]. The conditional access subsystem (CASS) shall at least consist of cryptographic Keys and a series of security software applications (APIs).

11) Security check: The service provider, set-top box producer together with the mobile phone operator shall 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 shall effectively interact with receiver-end and monitor the viewer's behaviour throughout the contract. Analysing the security data will also enable the service provider to evaluate the viewer's risk (i.e. user modelling techniques). In case that a threat is imminent, the CASS operating in the mobile phone and/or set-top box shall be automatically halted from operation. The service provider shall evaluate the situation and take appropriate action such as logging the situation, updating/revoking the Key and etc.

12) Personalised services and advertisement: in the MICAS, the sales and marketing can become more intelligent. The service provider can contact viewers on their mobile phones for instance to gather viewer's preferences and build up the viewer's profile online. The service provider can process such personalisation information using various individual or social modelling techniques (i.e. cognitive modelling and social interaction) to personalise his services for individuals or group of viewers. The service provider shall keep the viewer's account updated in terms of viewer's location and preferences. The viewer may opt for the personalised and targeted services while signing up to the contract. The viewer shall be able to cancel the service anytime at his will.

B. Underlying agents

The MICAS adopts an agent-based access control mechanism. The agents used to ascertain security and interaction across the MICAS are as follows.

The *Subscription Sender agent* is settled at the terminals (i.e. set-top box, mobile phone) and it provides a comprehensive graphical interface and requisite functionalities to satisfy the interactive use cases. For instance, it navigates the viewer through the sign-up wizard, generates and sends viewer's subscription request to the *Subscription Manager agent*, which operates at the head-end.

After the viewer generates his request to submit, the set-top box Subscription Sender agent connects to the mobile phone Subscription Sender agent to acquire its unique identities (i.e. IMSI 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, a set-top box temporary identifier (STB_TID) and Temporary Mobile Subscriber Identity (TMSI) may be used instead of STB_ID and IMSI numbers.

The Subscription Manager performs the verification processes, updates the viewer's account and instructs the SMSS 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, neither reported stolen nor used by another viewer in the network.

The *Security agent* operates at the terminals and it interacts with the *Security Manager agent* running at the head-end. They shall guarantee the security criteria like authentication, identification, privacy, integrity and non-repudiation in the MICAS. The Security agent is also responsible to monitor the viewer's contractual behaviour and alert the Security Manager in case any illegal activity is detected. In case of piracy, the Security agent shall halt the CA functions till receiving a notification message from the 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 *Conditional Access (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 agent* (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 responsible to implement the

transportation protocols for exchanging the data across the platform. The interaction channel is formed by the GSM network and Bluetooth link to connect the service provider to the set-top box through the viewer's mobile phone.

The 'initialisation step' is referred to the mobile phone and set-top box pairing sequence, submission of the subscription request through subscriber's mobile phone, authorisation of the request, identification of subscriber, validation of the set-top box, and finally provisioning of the security mechanism in the mobile phone and/or set-top box.

C. Overall system architecture

The MICAS proposes a federal identity management system wherein a third party data manager works closely with parties that operate in the system; including a Pay-TV service provider, mobile phone operator, set-top box and mobile phone certificate issuer. The data manager manages and stores silos of information regarding valid SIM cards, GSM subscribers' identity (i.e. IMSI), certified set-top boxes and Certificates, which authorise accessing to privileged locations in SIM cards or set-top boxes in a database. Fig. 6 presents an overall model of the external relationships between parties involved in the MICAS.

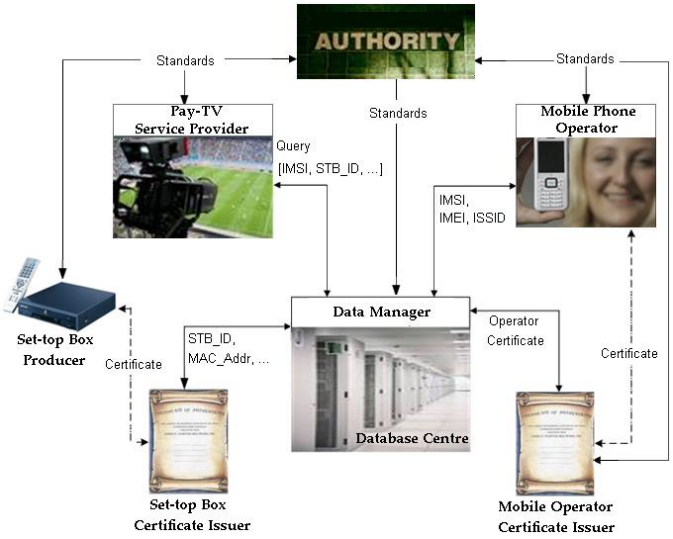

Fig. 6: The MICAS business circle

In the MICAS, the Message Handling Subsystem (MHSS) operates at the head-end and 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 the local or central database. It also updates the viewer's accounts for personalisation or security matters. The MHSS forwards the 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 conditional access (CA) mechanism 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 a Security Object to the MHSS or as a CA Message to the Multiplexer, depending on the security architecture described later. The SMSS and SAS functionalities defined in the MICAS are very similar to what has been defined in the DVB system, except for interfacing with SMSS. Fig. 7 depicts a general data flow diagram in the MICAS.

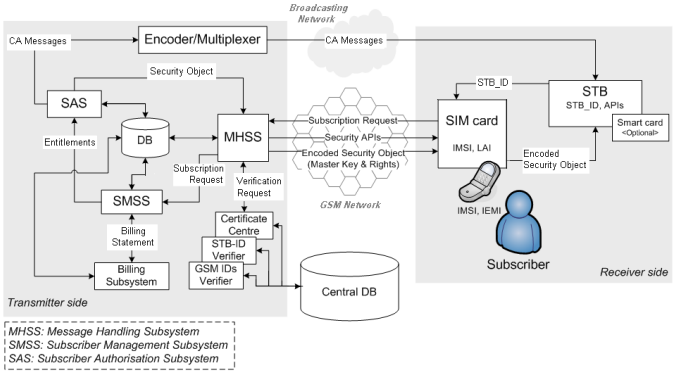

Fig. 7: The MICAS architecture

Depending on the data delivery route and the platform, wherein CA message processing and content descrambling take place, the following security architectures can be supported in the MICAS [8].

1) Security architecture (1): This is a simple 3-level Key hierarchical conditional access system where the Master key is used to encode the EMM and Service key is used to encode the ECM message containing the CWs. In this model, after the initialisation step, the CA Manager broadcasts the CA messages (i.e. EMM and ECM). It also delivers the Security Objects (i.e. Master key and rights) to the mobile phone CA agent via the GSM network. The mobile CA agent transfers the Security Objects to the set-top box CA agent through the secure channel established by the Communication agent. At the set-top box, the CA agent decodes the EMM and extracts the Service key. Having checked the subscriber's entitlements against the rights associated to the content (inserted in the ECM), the CWs are released to descramble the content.

2) Security architecture (2): This is similar to the previous model but the EMM processing takes place in the mobile phone. The EMM is delivered to the mobile CA agent via the set-top box. The mobile CA agent uses the Master key delivered from the GSM channel to decrypt the EMM and extract the Service key. The mobile CA agent then forwards the extracted Service key and subscriber's rights to the set-top box CA agent for ECM processing.

3) Security architecture (3): This is similar to the previous models but CA message processing wholly takes place in the mobile phone (SIM card). After initialisation step, the set-top box CA agent forwards the CA messages to the mobile CA agent over the Bluetooth link. The mobile CA agent decrypts the EMM and extracts the Service key using the Security Objects. The Service key is then used for decoding the ECM and extracting CWs. The CWs is sent back to the set-top box CA agent for descrambling the content.

4) Security architecture (4): This is a 3-level key hierarchical

security system where the ECM message is broadcast over-the-air and EMM message is sent to the subscriber's mobile phone along with the Security Objects (i.e. Master Key and rights) via GSM network. In this model, the mobile phone is an intermediary to deliver the EMM and Security Objects to the set-top box for CA processing.

5) *Security architecture (5):* This is similar to the previous model, but the EMM processing takes place in the subscriber's mobile phone. The mobile CA agent sends the extracted Service key and subscriber's rights to the set-top box CA agent to decode the ECM and descramble the contents.

6) *Security architecture (6):* This is similar to the previous model, but the CA message processing takes place in the subscriber's mobile phone. In this model, the set-top box plays an intermediary role to deliver the ECM to the mobile phone to extract the CW. The extracted CW is forwarded to the set-top box for descrambling the content.

7) *Security architecture (7):* This is a 2-level key hierarchical security system wherein the mobile is an intermediary to deliver Security Objects (i.e. Service Key and rights) to the set-top box. The set-top box receives the ECM from broadcasting network and deals with the CA processes and descrambling.

8) *Security architecture (8):* This is similar to the previous model, but the entire CA message processing takes place in the mobile phone. The set-top box delivers the broadcast ECM to the mobile phone. The mobile CA agent extracts the CW and sends it to the set-top box for content descrambling.

9) *Security architecture (9):* In this model, the CA message processing and content descrambling take place in the mobile phone. The content can be delivered to the mobile phone over either the mobile (i.e. 3G, UMTS, LTE) or broadcasting network via the set-top box. The communication link between the set-top box and mobile phone shall be then fast enough to display the content with no perceivable delay. Thus, popular Bluetooth adapters (1-3Mbps) do not seem to be suitable, 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, the recent high speed Bluetooth (Bluetooth V3.0) integrating the Ultra Wide Band (UWB) technology could be suitable as it would potentially enable the high data rate transfers of up to 480Mbps.

10) *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 CA 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 CA 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 Service key 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. A simple model of the security architecture is considered herein for analysis where the CA messages are processed in the mobile phone and descrambling sequence takes place in the set-top box.

In the security architectures explained above, the smart card is optional, replaced either by the viewer's SIM card or a flash memory integrated within the set-top box. The next section explains the implementation of the MICAS reference model.

V. Reference Model Implementation

The main components 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 run different operating systems, but they support the fundamental Java technologies (i.e. Java Virtual Machine, communication and security APIs). Fig. 8 presents the MICAS physical diagram highlighting core APIs needed in the MICAS. The Wireless Messaging APIs (WMA) can be replaced by short message commands to exchange text or binary messages (i.e. SMS) with MHSS through the SMS Service Centre (SMSC).

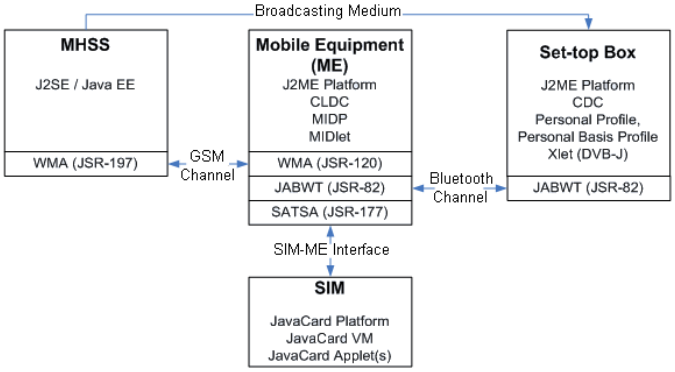

Fig. 8: The MICAS physical diagram

A 4-layer protocol stack is defined to handle all interactions between the entities in the MICAS. 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. Each agent 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 the 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 by exchanging Security Objects (i.e. security Applets, Key, etc.) across the network. Finally, at the application layer, objects like the 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 can be also defined as part of 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.

Fig. 9 presents a static view of the interactive protocol stack used in the MICAS.

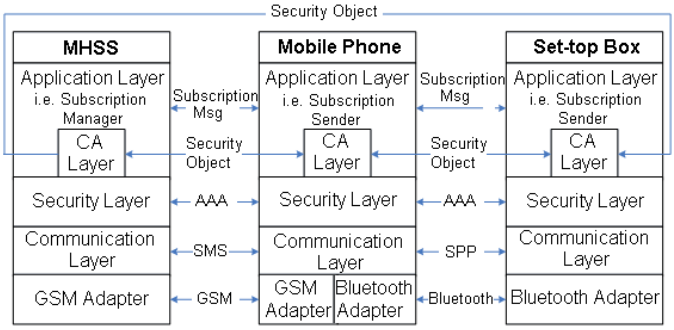

Fig. 9: The interactive MICAS protocol stack

Two ways of implementation can be considered in the MICAS: first, mobile centric [9] and second, set-top box centric implementations. In the former all the interactions are initiated from the mobile phone; as such the mobile phone presents the EPG-/ESG-like information and navigates the user to settle a specific request like sign-up request. 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. This is more analogous to the existing broadcasting platform, thus, it is considered herein.

A. Communication layer

The Communication agent in the mobile phone communicates with its counterparts residing at the set-top box and MHSS respectively via Bluetooth and GSM protocols.

The set-top box Communication agent uses the Extended AT Commands to interact directly with the SIM from outside world [10], [11]. The AT commands [12] are sent through the RFCOMM-SPP over the Bluetooth link. They are exploited to write/read data to/from the SIM.

The SMS protocol is used as a data bearer between the mobile phone and MHSS for the Remote Application Management (RAM) and Remote File Management (RFM) [13]. The MHSS sends 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. When a higher bandwidth is available (i.e. 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 [14].

The mobile Communication agent is implemented as a J2ME MIDlet. It acts as an intermediary between the SIM and the outside world. It can communicate with JavaCard applets resided on a smart card (SIM) using the Application Protocol Data Unit (APDU). The communication between JavaCard applets and applications, hosted for instance on the mobile phone, are handled by the Security and Trust Services API (SATSA), which extends the security support for cryptography, digital signature services, and user credential management.

B. Security layer

The authentication, authorisation and accounting (AAA) is defined as a security protocol in the MICAS. In case of mutual authentication when a mobile phone is involved, the IMSI number (or phone number) and Bluetooth address are used to identify the mobile phone. The STB_ID (or MAC address) and its Bluetooth address are used for the set-top box authentication. The MHSS server is authenticated using an Operator-ID and his associated credential, which can be made available to SIM cards during manufacturing. The authorisation is restricted to different criteria such as time, location, number of requests etc. The accounting process takes place at the head-end where the MHSS forwards statements to the billing system.

In addition to the triple-A processes, cryptographic techniques (i.e. hash functions, digital signature and encryption) are employed to provide a higher security level. Moreover, the session management mechanism is used to prevent any repetition in security processes, for instance when the communication link is disconnected. The session management is 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 is kept secret and frequently updated during transactions.

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 [15]. The Extensible Authentication Protocol method for GSM Subscriber Identity [16] can be used for authentication and session key distribution in the GSM domain. Nonetheless, the security protocol is implementation dependent. It means that each service provider can have his own security measures based upon his priorities.

C. Conditional Access (CA) layer

The role of the CA agents depends on the implementation scheme. The MHSS CA agent (CA Manager) can transfer Security Objects (i.e. CA-related functions, credentials) either directly or through an intermediary to the mobile or set-top box CA agents. The most suitable scheme, which is considered herein, is to employ both broadcasting and GSM channels. 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. Master Key) on the SIM card using the Over-the-Air (OTA) technology in the GSM network.

The MHSS CA agent sends Service-requests (application message) to an OTA Gateway that transforms the requests into Short Message Services (SMS) to be sent to a SIM card. The Service-requests contain a secured command packet (i.e. LOAD, MODIFY, ACTIVATE FILE, DEACTIVATE FILE), the targeted subscriber and data to perform the service. The service provider may set the Security Parameter Indicator (SPI) in the command packet to get a direct acknowledgement

from the recipient. 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 may retrieve data from the SIM card(s) for security or personalisation purposes [13].

The set-top box CA agent is downloaded to the viewer's set-top box when the receiver is connected to the service provider's network for the first time. The CA agent starts automatically as 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. Nevertheless, it is developed as an Xlet (applet for consumer systems) which forms the basis for all JavaTV-compliant systems including Multimedia Home Platform (MHP) and OCAP. The Xlet interface is used by the service provider to control the agent's life-cycle.

The signalling tables are included in the transport streams to instruct a set-top box on when and how to launch set-top box CA agent. Currently, the Globally Executable MHP (GEM), MHP and OCAP standards use eXtended AIT (XAIT) to describe stored or unbound applications [17]. The CA agent is described in an XAIT table as shown in Table 1.

TABLE 1
CA AGENT XAIT DESCRIPTION FIELD

Application name	CA agent
Application version	v.1.0
ID of application and associated organisation	Application ID = 1, Organisation ID = 1;
Application status	AUTOSTART
Application type	Xlet

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).

D. Application layer

This handles all interactions that take place between a viewer and set-top box (local interactions), and between a viewer and service provider (interactions over return channel). In both cases, native or stored (unbound) applications, which are broadcast and/or downloaded to a set-top box, will be used.

It is assumed that each set-top box has a built-in navigator or Monitor Application (or Execution Engine) as are usual for the MHP-compliant and OCAP-compliant systems, respectively. In the MICAS, the navigator enables a viewer to control the set-top box and set-up a Bluetooth connection between the set-top box and his/her mobile phone. Also, it displays a list of available service provider(s) and their associated services as advertised by EPG. 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.

In addition to the DVB-PSI/SI signalling tables and EPG, in the MICAS, additional data are required for online subscription, which is called Subscription Association Table (SAT). The SAT advertises available service provider(s) and their services to which TV consumers can subscribe. When a viewer attempts to sign-up, the SAT is displayed on the TV screen for instance in a cascading form.

The subscription request contains three sections: subscriber details, order details (i.e. order code, preferences, mobile phone and set-top box details) and terms and conditions. The subscriber's details are 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) is encoded. The content itself is transformed via the Base64 encoding algorithm. The 1Kbyte subscription request after Base64 transformation will become as large as a 5Kbyte text file. After transformation, the resulting file is compressed up to 40% using arithmetic compression methods. The digest value is then calculated using the SHA1 algorithm. The digest value needs to be signed 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 public key and/or certification number will be known to the recipient to re-calculate the digest value and decode the subscription request.

The Amendment request is similar to the Subscription request especially when a viewer wishes to extend his entitlements by adding more 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 services needs to be specified clearly.

The Follow Me activation request includes the viewer's identity (i.e. IMSI), the STB_ID and optionally the activation period. 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).

One of the cross-platform solutions to implement MICAS-related interactive applications is employing the JavaTV APIs (i.e. javax.tv.xlet) The JavaTV is compatible with other standards and provides 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.

VI. Analysis

The analysis pursued here is based on those factors, which play important role in developing a comprehensive business case for the MICAS. The factors are quantified to approximately identify the best MICAS security architecture.

A. Security

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 [19]:

1) The magnitude of the impact, should a threat-source successfully exercise the vulnerability;
2) The final determination of mission risk is derived by multiplying the ratings assigned for threat likelihood (e.g., probability) and threat impact.

To measure the 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, the following factors can be taken into account:

1) Threat-source motivation and capability;
2) Nature of the vulnerability;
3) Effectiveness of possible controls.

The threat likelihood can be rated in three levels: High (1.0); Medium (0.5) and Low (0.1). Table 2 presents the risk measurement criteria considered herein.

TABLE 2
RISK SCALE DEFINITIONS

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

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 rated in three levels of High (10), Medium (5) and Low (1). Table 3 presents the impact measurement criteria considered herein.

TABLE 3
IMPACT MAGNITUDE DEFINITIONS

Magnitude of impact	Definition of impact
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

Analysis reveals that the attack implies the least impact in the architectures 3, 6, 8 and 10 where the Master key and Service key are stored in the SIM and only CWs are exposed on the Bluetooth link. However, the high frequency of CWs makes the piracy difficult. But, the architecture numbered 9 is attributed as the most vulnerable architecture as it exposes the actual contents on the Bluetooth channel. Fig. 10 presents the tendency of risk assessment in the MICAS security architectures.

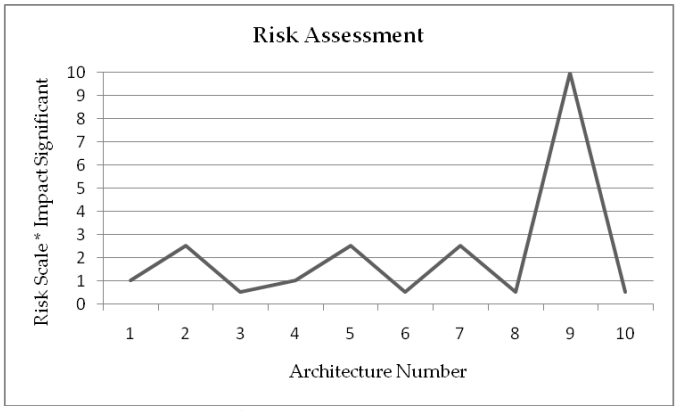

Fig. 10: The risk analysis of MICAS security architectures

B. Complexity

The overall complexity of the MICAS architectures is calculated based on the following measures:

3) *Emergent complexity:* This 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 in the MICAS based on the use case scenarios explained before. The observers were random from different ages (i.e. between 15 to 60 years) and high-tech literacy (i.e. mobile, computer) and their view was counted as equally weighted. Fig. 11 shows the emergent complexity index in the MICAS architectures based on the results of the survey.

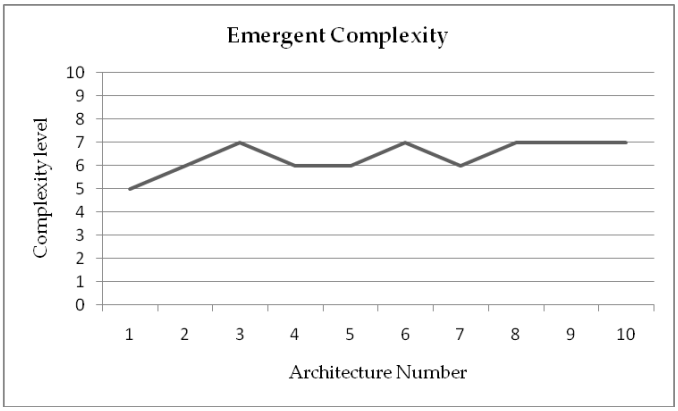

Fig. 11: The emergent complexity index in the MICAS security architecture

4) *Interdependencies:* The complexity of architectures partially depends on the interdependency of the modules so that it makes the system partially decomposable;
5) *CA message handling:* The complexity of CA systems chiefly depends on the design of EMM injector at the head-end and design of CA subsystem at the receiver-end.

In the first layer of analysis, a simple comparison amid architectures can be deducted to realise which solution is less complex for implementation. For instance, an architecture in which EMM messages must be broadcast timely in a uni-directional network is more complex than an architecture which adopts point-to-point message delivery method. In-depth analysis of algorithms is deferred to the future.

The result of the survey emphasises on implementing user-friendly interactive 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 or mobile phone. As 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 if the mobile phone is incorporated in CA processing. Fig. 12 shows the average of complexity in the MICAS security architectures considering the emergent, interdependency and CA-related complexity factors.

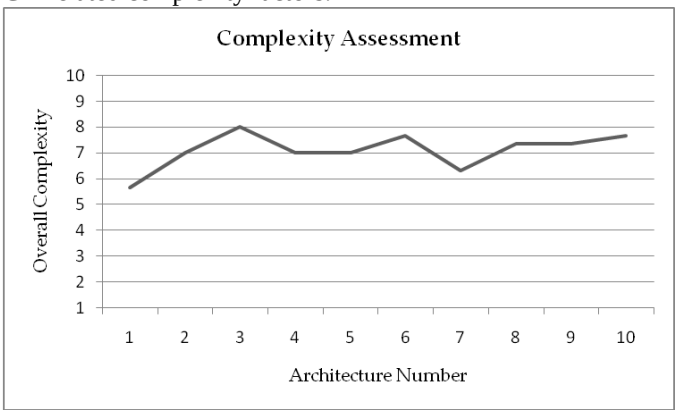

Fig. 12: The complexity assessment of MICAS security architectures

C. Set-top box cost model

An important factor to convince stakeholders to invest in a technology is the deployment cost and rate of return. The rate of return is very much related to customers' response to the technology. In-depth 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.

There are various factors that play a role in the total price of a set-top box, but we account the components cost as the basis for our analysis. The front-end set-top box components (i.e. tuner, demodulator, de-multiplexer) are required in all MICAS architectures. The CA subsystem (i.e. filter, CA module, smartcard, descrambler) may differ depending on the architecture. The back-end components (i.e. decoder) are also similar in all of the architectures. Amid the common interfaces (i.e. RJ-11, RS232, HDMI/DVI, 802.11, USB, etc), only Bluetooth is essential for all architectures.

It is appreciated that components like descrambler can be more expensive than others and also some architectures require more sophisticated firmware/memory resources to handle CA processing. But, the cost differentiation in the hardware components integrated in the set-top box, the firmware and memory differentiation costs are considered negligible amid security architectures here. Fig. 13 presents the cost analysis of the set-top box used in MICAS architecture.

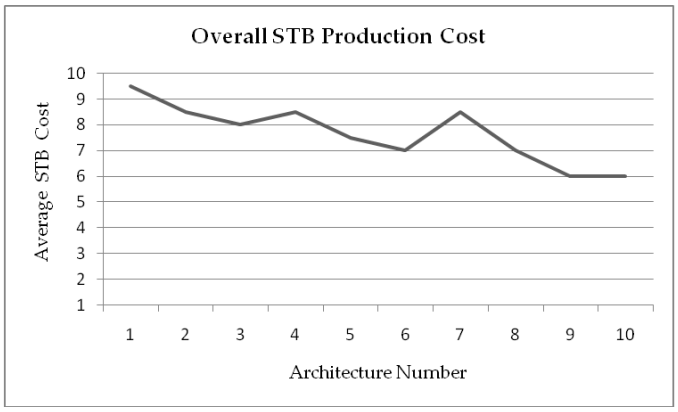

Fig. 13: The production cost analysis in the MICAS security architectures

The analysis suggests that incorporating the mobile technology into the Pay-TV system can potentially reduce number of the hardware components and overall cost of the set-top box.

D. Overall analysis

A pre-deployment evaluation of security risk analysis, complexity and set-top box cost model can help develop a more comprehensive business case for the MICAS security architectures. The following formula is used to present the overall pre-deployment measurement based on the security risk, complexity and cost.

$$Performance\% = \frac{1}{SecurityRisk \times Complexity \times Cost} \times 100$$

Fig. 14 presents the overall performance of MICAS security architectures based on the security, complexity and cost assessments.

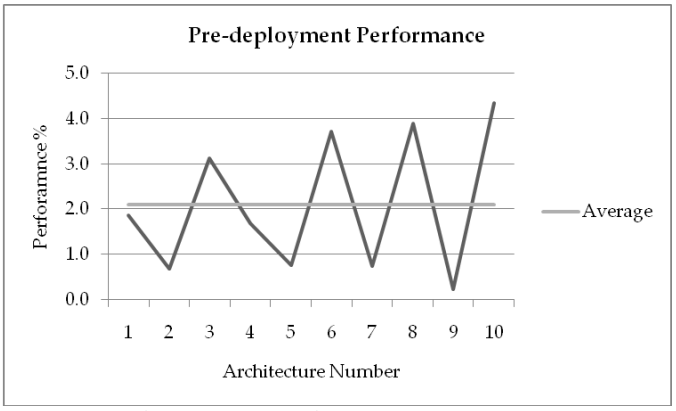

Fig. 14: The performance analysis of the MICAS security architectures

The security architecture numbered 9 is the lowest and 10 is the best performer. The architecture numbered 1 with minimum deviation from average performance can be a viable solution based on the said criteria.

VII. CONCLUSIONS

The utilisation of mobile technology in the Pay-TV system can enhance interactivity, security and potentially reduce customer attrition and operational cost. It breaks up the rigid relationship between a viewer and set-top box so that a viewer can fully enjoy his entitlements via an arbitrary set-top box.

Having thoroughly considered state-of-the-art communication and access control technologies, the paper presented a set of conventional use-cases to clarify the design and implementation aspects of the novel Mobile Integrated Conditional Access System (MICAS). The MICAS has been proposed to address the inherited issues in the Pay-TV mainly interoperability, mobility, personalisation, cost of operation, viewer's convenience by providing a viable and intelligent platform which supports a horizontal transaction model and can fulfil future demands in the Pay-TV and interactive-TV businesses. The MICAS design was enriched by providing possible security structures and data flow diagrams supported thereby. A business collaboration structure was proposed followed by an implementation reference model. Finally, the security architectures were analysed to propose the best architecture on the basis of the pre-deployment performance criteria namely the security, complexity and set-top box production cost. The analysis reveals that the best pre-deployment performance can be gained when the cellular network is used for CA message delivery (including ECM and EMM) and CA subsystem is shifted to the mobile phone from the set-top box; a SIM-based CA system for Pay-TV systems.

REFERENCES

[1] Digital Video Broadcasting (DVB). Available www.dvb.org
[2] Digital Video Broadcasting (DVB); DVB Simulcrypt, Part 1: Head-end architecture and synchronization, ETSI TS 101 197-1, June 1997.
[3] Digital Video Broadcasting (DVB); Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications, ETSI EN 50221, CENELEC, February 1997
[4] Kamperman F., Rijinsoever B. V. "Conditional access system interoperability through software downloading", IEEE Transaction on Consumer Electronics, Vol. 47, No. 1, pp. 47-54, February 2001
[5] Prasertsatid N., "Implementation Conditional Access System for Pay-TV based on Java Card", 3rd IEEE Conference on Computational Electromagnetic and its Application, 2004
[6] Namba S. "Technologies and Services on Digital Broadcasting – Scrambling (Conditional Access System)", NHKS STRL, Broadcast Technology no.12, Autumn 2002
[7] Sirett W. G., MacDonald J. A., Mayes K., Markantonakis K. "Secure Deployment of Applications to Fielded Devices and Smart Cards", The 4th International Workshop on Security in Information System (WOSIS 2006), Institute for Systems and Technologies of Information, Control and Communication, ICEIS 2006, Paphos, Cyprus, ISBN: 978-972-8865-52-8, pp. 195-207, May 2006.
[8] Shirazi H., Cosmas J., Cutts D., Birch N., Daly P. "Security Architectures in Mobile Integrated Pay-TV Conditional Access System", Networks 2008 – 13th IEEE International Telecommunications Network Strategy and Planning Symposium, Hungary, September, 2008
[9] Shirazi H., Cosmas J., Cutts D., Birch N., Daly P. "Mobile Integrated Conditional Access System (MICAS)", 16th IEEE International Symposium of Consumer Electronics, April 2008
[10] 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
[11] 3GPP TS 27.007, "AT Command set for User Equipment (UE)", v.8.4.1, Release 8
[12] Guthery S., Cronin M., "Mobile application development using SMS and the SIM toolkit", McGraw-Hill 2002, ISBN: 0-07-137540-6
[13] 3GPP TS 03.48, "Digital cellular telecommunications system (Phase 2+); Security mechanisms for SIM application toolkit; Stage 2", version 8.9.0 Release 1999
[14] ETSI TS 102 223, "Smart cards; Card Application Toolkit (CAT)", Release 4
[15] 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, November 2002
[16] RFC-4186, "Extendible Authentication Protocol method for Global System for Mobile communications (GSM) Subscriber Identity Module (SIM)", Network Working Group, January 2006
[17] 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, 9780240806662
[18] OCAP 1.0 profile, "OpenCable™ Application Platform Specification", document control number OC-SP-OCAP1.0-I16-050803, August 2005
[19] 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, July 2002
[20] Wright T., "Security considerations for broadcast systems", Information Security Technical Report 11 (2006) pp. 137-146

H. Shirazi (M'04) is expecting to receive his PhD in Multimedia Systems and Computer Science from the School of Engineering and Design, Brunel University, UK. He has received his MSc and BSc with honours in Data Communications Systems from School of Engineering and Design, Brunel University, UK in 2004 and Software Engineering from University of Science and Technology, Tehran, Iran in 2000, respectively.

He was the main researcher of the industry-led iPACE-TV project and contributed as a Research Assistant into European IST funded projects namely PLUTO and INSTINCT.

Mr. Shirazi has published over dozen papers in IEEE transactions and international conferences mainly on monitoring and improving of the QoS in

converged IP and DVB-T/H platforms. His research interests are focused on the quality of multimedia services and conditional access systems in converged broadcast, mobile and IP-based networks.