Security Architectures in Mobile Integrated Pay-TV Conditional Access System

Shirazi H., Cosmas J.[1], Cutts D., Birch N., Daly P.[2]

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

***Abstract*—This paper presents the design and describes the advantage of the state-of-the-art Mobile Integrated Conditional Access System (MICAS) concerning interoperability, personalisation, security and operational costs in Pay-TV systems. The Message Handling Subsystem is proposed and outlined together with 'Follow-Me' service, which proposed herewith to extend mobility and personalisation concepts on Pay-TV services[1].**

***Index Terms*—Conditional Access System (CAS), Pay-TV, DVB, GSM, Mobile Phone, Set-top Box (STB), SIM Card.**

I. Introduction

THE security consideration is an essential part of any business in Pay Television and hence critical to development of successful digital television businesses. Europe and USA were some of the fist countries that realised the necessity of Conditional Access (CA) systems to prevent unauthorised users to access to the contents in Pay-TV services. Conditional access system consists of technical services like coding, scrambling, and transmission and decoding, descrambling techniques as well as administrative services such as subscription management and STB deployment in the field and etc.

There have been commercial issues concerned with the implementation of open standard CAS and control of the specification, the distribution and use of STB containing the CA functions. As a consequence, a vertical market for Pay-TV industry has been generated that forms a business chain of service provider, CAS provider, STB manufacturer and subscriber. In this market, a proper interoperability between various CASs is compromised and as such, the operator and eventually the subscriber have to accept the consequent cost of service and STB deployment. It is worthwhile to mention that deployment cost is the highest cost for service provider beside the content itself. Techniques like common scrambling in conjunction with MPEG standard data transport mechanism used in Simulcrypt and common interface in Multicrypt, smart-card based solutions and downloadable conditional access systems have been proposed and, in some cases, deployed to satisfy the commercial requirements of broadcasters and operators. Nevertheless, none of them provides an interactive, standardised, resilient, scalable, updatable and cost-effective solution for CAS whereby service provider and subscriber in broadcasting systems can truly benefit [2].

The conditional access and service protection system commonly adopts a hierarchical system for security key management with response to scrambling and encoding purposes. For instance in DVB system, the content is scrambled by Control Words (CW), which are broadcast to the receivers via Entitlement Control Message (ECM). The ECM are encoded using the Service key that is associated with a service or programme or channel and is valid for a period of time depending on the type of subscription. The information of the Service key is included to Entitlement Management Message (EMM). The EMM itself is encoded using Master key shared with the service provider and security module available at the receiver. The ECM and EMM are broadcast along with the content to all the receivers. Each receiver filters its own messages (the messages are addressed to the individual receivers) and decrypts it using the information received by EMM and stored in the security module (i.e. smart-card). If the subscriber is authorised to access to the content, the CWs will be released to descramble the content. Figure below shows the block diagram used in DVB Conditional Access system [4]. Fig. 1 shows the data flow diagram of a typical hierarchical DVB conditional access system.

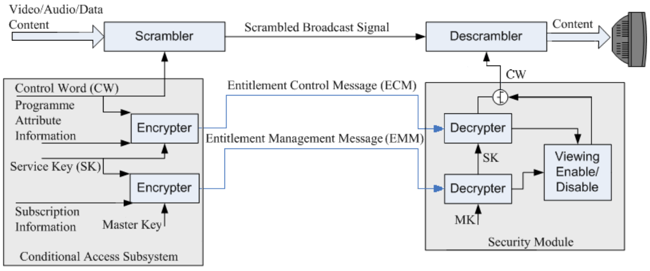

Fig. 1. A typical DVB Conditional Access System.

[1] Manuscript received February 28, 2008. This work was supported in part by Strategy & Technology (S&T) Ltd.

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, and N. Birch is director and D. Paul is general manager of clients systems at S&T Ltd. Strategy & Technology Ltd 4th Floor, 1 Benjamin Street, London, EC1M 5QG United Kingdom (email: David.cutts@s-and-t.com; nick.birch@s-and-t.com; paul.daly@s-and-t.com)

II. Analysis of Current System

The proprietary conditional access systems employed in broadcasting system contain specific security-related information and algorithms to scramble/descramble the content in order to be solely accessible for authorised subscribers via specific STBs. The challenges and pitfalls which are commonly observed in current Pay-TV systems are as follows.

Security-related information (i.e. ECM and EMM messages) that is needed to descramble the content is broadcast to all active receivers within the operator's coverage area. This method of delivery of sensitive information is not considered secure and bandwidth efficient.

The service provider must accept the deployment cost since the STBs and security module (smart-card) are delivered directly to its subscriber(s).

Moreover, a certified engineer needs to go to the site to install STB and undergo the binding process of STB and smart-card. This would prevent the smart-card being used in another STB. Such STBs are tailored to one specific service provider, especially to the CAS employed by this service provider. The STB producer also needs to pay licence fee in order to use the CAS in his STB and sign non-disclosure agreement with the CA provider to enable his STB products to receive and decode the pay-TV programmes scrambled by this CAS. This obvious loss of commercial scale and licence fee for CA subsystem make STBs quite expensive and since the public are reluctant to buy such kind of STBs, the operator has to provide them free of charge or indeed subsidise them. This contribution, however, will be eventually added to the subscription fee for the liable subscribers. Therefore, the high subscription fee would discourage public to subscribe to TV services and consequently encourage them to illegally attempt to access to the contents, which would result in revenue loss for service provider [1].

Furthermore, in case of security flaws, the service provider can not distinguish the compromised security keys and identify the corresponding subscriber, since he does not interact with the receiver end. Moreover, revoking the compromised keys and security algorithms and substituting them would impose additional cost to the service provider. Additionally, in this business case, the subscriber is compelled to bind to one specific STB pre-determined by the service provider, as such he can not access to his entitlements via an arbitrary certified STB when he is not home.

The CA architectures presented herein will address all of the concerns above and provide an infrastructure to offer the subscriber a Follow-Me service whereby subscriber's right will be recognised by his service provider. Hence, the subscriber can enjoy his entitlements via any STB receiving the service provider's content. The proposed architectures will enable the service provider to study his customers, improve the security and offer more personalised services based on the information received from the receiver end.

III. System Model & Architectures

In this section various security architectures are presented together with the details of the employed subsystems and their interactions. The architectures are elaborated and analysed with regards to possible key distributions and security processing needed in the typical Conditional Access system. The architectures mainly address issues imposed by traditional Pay-TV systems; interoperability, high cost of service deployment and revoking compromised keys, interactivity and binding customers to particular technologies and receivers.

Fig. 2 shows the system model of the GSM integrated Conditional Access system.

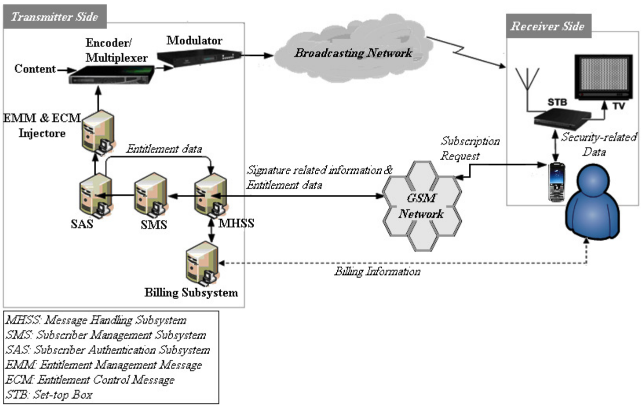

Fig. 2. The System model of GSM Integrated Conditional Access System.

The Message Handling Subsystem (MHSS), possible architectures of integrated STB and Mobile Phone CAS and Follow-Me service are detailed as follows.

A. *Message Handling Subsystem (MHSS)*

The Message Handling Subsystem (MHSS) is a subsystem operating at the transmitter side as an interface between subscriber and broadcaster in GSM network. It receives the subscriber's subscription request and performs mutual authentication along with initial tests to identify whether the request is made by valid sources (subscriber and STB). After having identified the subscriber and corresponding STB, it places requests with Subscriber Management Subsystem (SMS) and Billing Subsystem. It also downloads the security APIs (algorithms) to the SIM card in the mobile phone, if it is needed [6].

Upon receiving the request from MHSS, the SMS decides, based on criteria like customer product selection and payment status, if – and for which services – the user shall be authorised. The SMS requests the Subscriber Authorisation System (SAS) to generate EMMs and/or ECM. The key information used to generate entitlement messages are then sent to MHSS to be delivered to the mobile phone for security-related functions and descrambling processes. The MHSS also handles the transactions by forwarding the requests to the Billing system. The SMS and SAS, defined in this architecture, function similarly to what is defined in the broadcasting systems like DVB with the enhancement of capability to input and output from/to the MHSS.

The possible data flow diagrams and processing model containing STB, mobile phone (SIM card) and service provider or broadcaster are described as follows.

B. APIs used in MICAS

The requisite applications used in MICAS architectures are as follows.

- The *Subscription Request Handler* is a MIDLet running on the mobile phone that provides subscriber with an interface to select the service provider from a pre-defined list of service providers and generates and sends a subscription request to the service provider. The transmission protocol between mobile phone and service provider in for instance GSM technology may be Short Message Service (SMS) or Wireless Application Protocol (WAP).
- The *Mutual Authentication* communicates with MHSS to perform a mutual authentication process between subscriber and service provider. It might be implemented as a sub-function of Subscriber Request Handler described above.
- The *Conditional Access Handler* is an applet installed in SIM with access to privileged domains. It is downloaded to the SIM by MHSS and performs security-sensitive algorithms and communications. Its functionalities may vary at each proposal.
- The *Communication Daemon* is an application installed in STB. It interfaces the STB to the outside through interaction channel (i.e. GSM). It contains a series of APIs installed by STB manufacturer to access the privileged domains and performs security-related algorithms. It communicates with Conditional Access Handler to prepare a secure communication channel in pairing process. It provides Conditional Access Handler with the STB identity which must be obtainable solely to communication daemon privileged user by special rights.

The Conditional Access Handler generates a message containing International Subscriber Identity Number (IMSI) and/or International Mobile Equipment Number (IMEI) and STB Identity Number (STB ID) provided by Communication Daemon. It then sends the message to the MHSS to verify if subscriber and STB are valid and compliant to the standards.

The MHSS identifies the subscriber and his equipment using IMSI and IMEI and checks if they are valid and unique in the system. For security purposes, the Conditional Access Handler may check the number and origin of requests and also contact mobile network operator to ascertain the IMSI and IMEI numbers. The STB_ID indicates the type of STB, which is used to authenticate STB. The STBs may be registered with service provider or with a special agency to ensure that they are compliant to the standards for service and content protections and implement standard specifications. The MHSS transfers the Master key and subscriber's right (Security Objects) to the Conditional Access Handler in SIM card.

The 'initialisation step' is a procedure common in all security architectures presented herewith and refers to pairing of mobile phone and STB, submitting subscription request through subscriber's mobile phone, authorising the request, identification of subscriber, validation of STB, 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 STB, mobile phone (SIM card) and service provider or broadcaster are described as follows.

C. Decoding of EMM & ECM at STB using Security Objects delivered via mobile phone

The Conditional Access Handler delivers the credentials to the Communication Daemon in STB, where EMM and ECM are received. Communication Daemon provides the Security Objects to the security algorithms embedded in STB to decrypt EMM and extract Service key to decrypt ECM. The subscriber's rights are checked upon, the rights needed to watch the content (as inserted in ECM), and if the condition is satisfied, the CWs are released to descramble the content.

Fig. 3 shows the subsystems and data flow diagram when mobile phone plays an intermediary role to deliver Security Objects (Master Key and list of entitlements) to the STB. This information is used at STB to decode EMM and ECM and descramble digital contents.

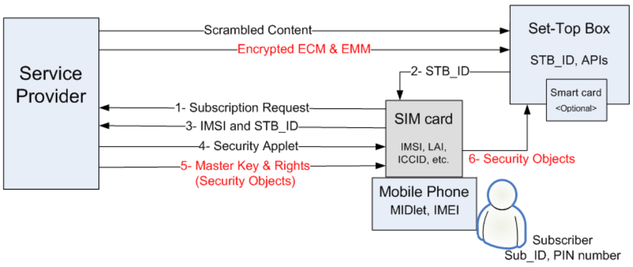

Fig. 3. The data flow of a 3-level hierarchical security architecture wherein all security functions take place in STB.

D. Decoding of EMM at SIM card and ECM at STB using Security Objects delivered to the SIM card

After having established the initialisation step, the Communication Daemon forwards the EMM to the Conditional Access Handler. The Conditional Access Handler decrypts EMM and extracts Service key using the knowledge of Master key obtained from Security Objects (Master key and Subscriber's rights) received from service provider. The Conditional Access Handler then forwards the Service key and subscriber's rights to the Communication Daemon to be used by security algorithms embedded in STB for decryption of ECM and extraction of CWs.

Fig. 4 shows the data flow diagram when EMM is broadcast on-air and delivered to the subscriber's mobile phone to be decoded.

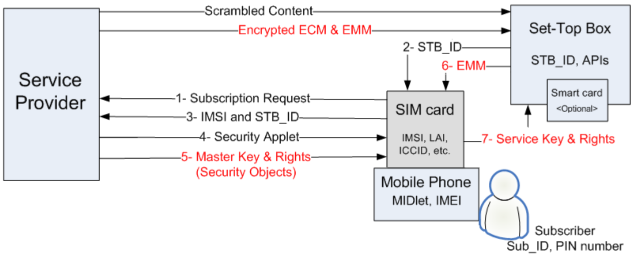

Fig. 4. The data flow of a 3-level hierarchical security architecture wherein EMM and ECM decoding is balanced between STB and mobile phone.

E. Decoding of EMM & ECM at SIM card using Security Objects delivered to the SIM card

In this architecture, after establishing the initialisation step, the Communication Daemon forwards the EMM and ECM to the Conditional Access Handler. The security algorithms placed in Conditional Access Handler using the Security Objects (Master key and Subscriber's rights) received from service provider decrypts the EMM and extracts the Service key to be used for decryption of ECM and extraction of CWs. The Conditional Access Handler then transfers the CWs to Communication Daemon for descrambling the content.

Fig. 5 shows the data flow diagram when all decoding processes concerning EMM and ECM messages take place in the subscriber's mobile phone (SIM card).

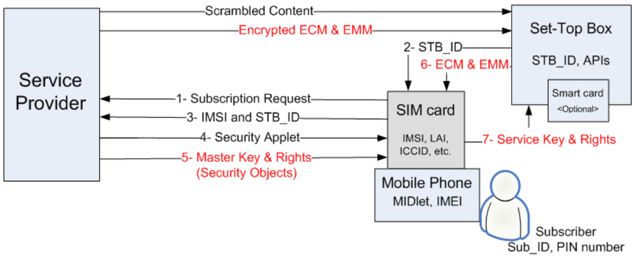

Fig. 4. The data flow of a 3-level hierarchical security architecture wherein EMM and ECM decoding takes place in the mobile phone.

In proposals C, D and E, the entitlements messages (ECM and EMM) are broadcast to the receivers and the key information to open the encrypted EMM is delivered through the return channel (GSM network).

F. Decoding of EMM & ECM at STB using EMM delivered via mobile phone

After having established the initialisation step, the MHSS transfers EMM message to the Conditional Access Handler. The EMM contains the information of Service key and subscriber's rights, but may not be limited. The Conditional Access Handler transfers the EMM to Communication Daemon. The Communication Daemon provides EMM message to the security-related algorithms to decrypt ECM (received from broadcast channel) and extract CWs for descrambling the content only if the subscriber is entitled to access to the content.

Fig. 6 shows the data flow diagram when EMM is delivered to the subscriber's mobile phone through GSM network. The mobile phone then forwards the message to the STB for decoding of ECM and descrambling contents.

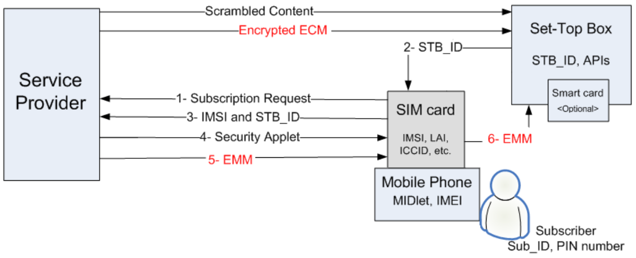

Fig. 5. The data flow of a 3-level hierarchical security architecture wherein EMM is transferred via mobile network and all security functions take place in the STB.

G. Decoding of EMM at SIM card and ECM at STB using EMM delivered to the SIM card

After having established the initialisation step, the MHSS transfers EMM message to the Conditional Access Handler. The EMM message is opened in SIM card and Service key and subscriber's rights are then extracted and transferred to the Communication Daemon. The Communication Daemon provides Service key and entitlements to the security algorithms embedded in STB to decrypt the ECM that is received from broadcast channel. If the subscriber is entitled to access to the content, CWs are used to descramble the content.

Fig. 7 shows the data flow diagram when EMM is delivered through GSM network and processed at subscriber's mobile phone (SIM card) to extract service key and entitlements sent to STB for decoding ECM and descrambling contents.

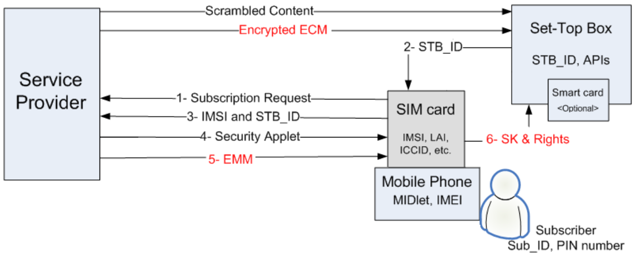

Fig. 6. The data flow of a 3-level hierarchical security architecture wherein EMM is transferred via mobile network and EMM & ECM decoding is balanced between STB and mobile phone.

H. Decoding of EMM and ECM at SIM card using EMM delivered to the SIM card

After having established the initiating, the MHSS transfers EMM message to the SIM card to the Conditional Access Handler. The Communication Daemon transfers the ECM to the Conditional Access Handler to decrypt ECM using the knowledge of Service key conveyed with EMM and extract CWs if subscriber's rights match the programme right inserted in ECM message. The Conditional Access Handler passes the CWs to the Communication Daemon to descramble the content.

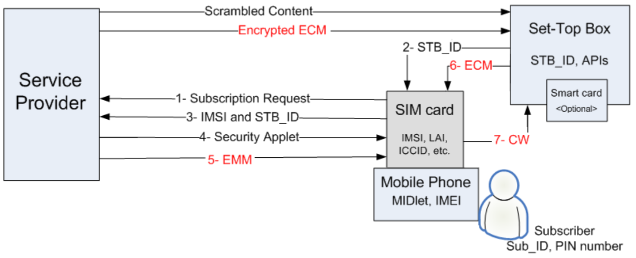

Fig. 7. The data flow of a 3-level hierarchical security architecture wherein EMM is transferred via mobile network and EMM & ECM decoding takes place in the mobile phone.

It is worthwhile noting that utilising GSM network to send EMM messages would save more bandwidth for the broadcaster.

I. Decoding of ECM at STB using the Security Objects delivered via mobile phone

Fig. 9 presents the data flow diagram when Master Key is not used in the key hierarchy. In this case, Security Objects including Service Key as the highest key in the key hierarchy together with entitlements are delivered through GSM network to the subscriber's mobile phone to be delivered to the STB. The ECM decoding and content descrambling processes take place in the STB.

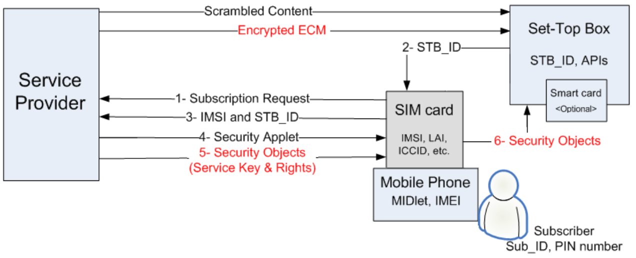

Fig. 8. The data flow of a 2-level hierarchical security architecture wherein all security functions take place in the STB.

After initialisation step, the MHSS transfers Service key and subscriber's rights (Security Objects) to the Conditional Access Handler to transfer the Security Objects to the Communication Daemon. The Service key and subscriber's entitlements may be used by Communication Daemon or security algorithms embedded in the STB to decrypt ECM broadcasted to the receivers. If subscriber is entitled to access the content, the CWs are released to descramble the content.

J. Decoding of ECM at SIM card using the Security Objects delivered to the SIM card

After having established the initialisation step, the MHSS transfers Service key and subscriber's rights (Security Objects) to the Conditional Access Handler. The Communication Daemon transfers the ECM to the Conditional Access Handler to decrypt the ECM using the Service key and extracts CWs if subscriber's right match the criteria set for the content. The Conditional Access Handler sends the CWs to the Communication Daemon to be used for descrambling of the content.

Fig. 10 shows the data flow diagram when Security Objects (Service Key and entitlements) and ECM messages are delivered to the subscriber's mobile phone respectively from GSM network and STB. The decoding process takes place in subscriber's mobile phone and the extracted CWs are delivered to the STB for descrambling process.

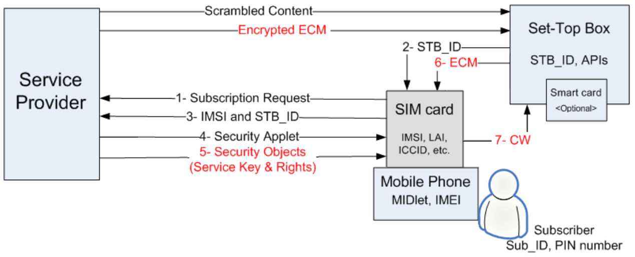

Fig. 9. The data flow of a 2-level hierarchical security architecture wherein ECM decoding takes place in the mobile phone.

Following remarks are valid for all proposed architectures.

- Making smart card an optional entity will enable free-viewers to benefit from Pay-TV services;
- Mobile phone can be replaced by any device with similar capability in communication and storing security-sensitive data (i.e. a STB with GSM connectivity);
- Service providers can update and/or revoke the compromised security key(s) and/or algorithms online through GSM network;
- The encryption, session key and digital signature techniques together with mutual authentication technique will enhance security of the system;
- 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 contents. In the other hand, the platform enables service providers monitor the behaviour of subscriber which results in enriching range of bespoke services and improving security mechanism. One of services that can be introduced in this platform is 'Follow-Me' service, which enables the subscriber to access to the content upon his entitlement without the requirement of being bound to a specific STB. The service would give freedom of choice to the subscriber with regards to the point of connection to the system and therefore enables subscription entitlements to follow the subscriber even when he travels. 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 is established to offer Follow-Me type of services to the customers.

IV. CONCLUSIONS & FUTURE WORKS

In this document, high-level security architectures for provisioning a horizontal market in Pay-TV industry and architectures for establishing interoperability amongst various CASs were provided. The Mobile Integrated

Conditional Access System (MICAS) was detailed considering various architectures to deliver key information that is needed to descramble requested contents at an arbitrary STB located at the vicinity of the subscriber. The main benefits and novel aspects of the system were fully outlined. Furthermore, the Follow-Me service and Message Handling Subsystem (MHSS) in the broadcasting system were also described.

The MHSS as a new entity in the broadcasting system operates at the transmitter side and handles communication between service provider and subscriber via cellular network. It interacts with subscriber via mobile phone and passes subscriber's subscription request to the existing Subscriber Management and Subscriber Authentication Subsystems to authorise corresponding rights. The authorised rights together with security key information will be sent by MHSS to the subscriber's mobile phone. Depending on the architecture, the decryption and descrambling process of security messages may take place in the SIM card of the mobile phone and/or in the trusted STB unit.

The system can reduce the cost for service provider and end-users by respectively cutting down the service deployment cost and eliminating the requirement of additional receiver as changing the service provider. Moreover, it can improve the overall security in the system by interacting with receiver and downloading new security mechanisms online as and when it is needed. Furthermore, the functions of revoking the compromised keys and monitoring the contractual behaviour of the subscriber can be performed cost-effectively through interaction channel provided by mobile network: GSM and its descendants like UMTS, 3G and etc. The Conditional Access system proposed here can improve the personalisation concept in broadcasting networks and provides subscriber with ubiquitous access to their entitlements as defined by Follow-Me service.

It is worthwhile noting that the concurrency between delivery and processing of entitlement messages are very important to the success of the proposed architectures. Failure to present digital contents shortly after a service being subscribed would likely cause customer dissatisfaction and raise complaints. Hence, implementation of underlying subsystems which are operating at transmitter side, mobile phone and STB and also considering appropriate transport protocols are of great importance. Least but not the last it is important to make sure that sufficient security requirements are guaranteed in architectures. Therefore, analysing security threads and introducing security counter-attacks play great role in success of the proposal too. Our research which we are in the process of conducting addresses, the above mentioned concerns thorough analysis of the message delivery latency introduced by GSM protocols, security measurements and implementation aspects of the subsystems.

REFERENCES

[1] 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

[2] Meng Z., Shi-bao Z., IEEE Transactions on Consumer 602 Electronics, "A Common Smart-card-based Conditional Access System for Digital Set-top Boxes", Vol. 50, No. 2, MAY 2004

[3] Cutts D. J., IEE Broadcasting Convention, Conference, "DVB Conditional Access", International publication No. 428, 1996

[4] Cutts D. J., Electronics & Communication Engineering Journal, "DVB Conditional Access", FEB-1997

[5] Hansvold O. Telektronikk 2/3.2002 "Conditional Access to Broadcasting Content"

[6] Kamperman F., Rijnsoever B. V., IEEE Transactions on Consumer Electronics, "Conditional Access System Interoperability through Software Downloading", Vol. 47, No. I, FEB-2001

[7] Prasertsatid N., 3"' International Conference on Computational Electromagnetics and Its Applications Proceedings Card, "Implementation Conditional Access System for Pay TV Based on Java", 2004

[8] 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, Vol. 50, No. 2, May 2004

[9] 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, Alexandria, Virginia, USA, ISBN:978-1-59593-884-8, 2007

[10] Mooji W. G. "Conditional Access System for Digital Television", International Broadcasting Convention, IEEE Conference Publications, No. 397, pp. 489-491 (1994.9)

[11] Xie Q. Zheng S. "A Smartcard Conditional Access Subsystem Separation Scheme for Digital TV Broadcasting", IEEE Transactions on Consumer Electronics, Vol. 51, No. 3, pp 925-932, August 2005

[12] 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