Mobile Integrated Conditional Access System (MICAS)

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 design of a novel security architecture integrating mobile and broadcasting technologies in the Pay-TV system. The security architecture proposed herein is a state-of-the-art solution to tackle well-known problems challenging current Pay-TV systems including but not limited to interoperability amongst service providers, relatively high cost of the service deployment, the security compromise, limited interactivity and bespoken services offered to subscribers. It also proposes the Follow-me service that enables subscribers to access their entitlements via an arbitrary set-top box.[1]**

***Index Terms*—Conditional Access (CA) System, Set-top Box (STB), Pay-TV, Mobile, SIM-Card**

I. Preface

The security consideration is an essential part of any business especially in Pay-TV and hence it is critical for the development of successful digital television businesses. Europe and USA were among the fist countries that realised the necessity of Conditional Access (CA) systems to prevent unauthorised users to gain access to the contents in Pay-TV services. The CA system consists of technical (i.e. encoding, decoding, scrambling, descrambling, and transmission techniques) and administrative services (i.e. subscription management and service deployment) [2].

There have been commercial issues concerning with the implementation of open standard CA system, control of the specification, distribution and use of STB containing the CA functions. 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 [5], [6]. Nevertheless, none of them provides an interactive, resilient, scalable, updatable and cost-effective solution for CA system, 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. In DVB system, for instance, the content is scrambled by the Control Word (CW), which is included in the Entitlement Control Message (ECM) to be broadcast to receivers' population. The ECM is encoded using the Service Key (SK), which is associated with the service and is valid for a period of time depending on the subscription type. The information of SK is included in the Entitlement Management Message (EMM). The EMM itself is encoded using the Master Key (MK) shared with the service provider and security module resided at the receiver side. The ECM and EMM are broadcast along with contents to all receivers. Each receiver filters its corresponding EMM messages (EMMs are addressed to the individual receiver) and decrypts ECMs using information inserted into the EMM and 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 [3]. Fig. 1 (next page) shows the general block diagram used in DVB Conditional Access system [7].

The paper is organized as follows. In Chapter 2, the current system is analysed and consequent requirements are elicited, followed by high-level descriptions of the Mobile Integrated Conditional Access System (MICAS) proposed herein. In Chapter 3, the MICAS design and architecture is illustrated and analysed. Finally, the paper is concluded in the Chapter 5.

[1] Manuscript received March 30, 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, UK (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, UK (email: David.cutts@s-and-t.com; nick.birch@s-and-t.com; paul.daly@s-and-t.com)

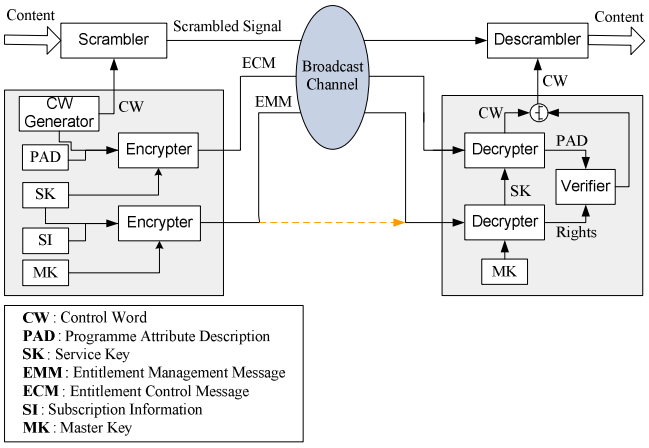

Figure 1: DVB Condition Access System.

II. REQUIREMENT ELICITATION

In the current Conditional Access systems, the security-related data (i.e. ECM and EMM messages) needed for descrambling TV contents are broadcast to receivers' population operating in the operator's coverage area. This method of delivering sensitive data is neither secured nor bandwidth efficient.

In addition, the current business model used in Pay-TV systems follows a circle of dependency, wherein service provider, CA provider and STB producer have to work in a restricted vertical market. In this model, a STB producer needs to pay licence fee in order to use CA system in his STB and sign a non-disclosure agreement (NDA) with the CA system provider in order to enable his STB products to work under security considerations adopted by this CA system. 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 substantially 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 contents, which would result in revenue loss for the service provider [9].

Furthermore, in case of security flaws, due to lack of interaction between receiver and transmitter head-ends, the service provider can not distinguish compromised security keys and identify the corresponding subscriber quickly. Eventually, revoking and substituting the compromised keys and security algorithms would impose additional costs to the service provider.

Additionally the subscriber is compelled to be bound to one specific STB pre-determined by the service provider; as such he can not access his entitlements via an arbitrary STB or receive contents from any other service providers [1].

The abovementioned issues are well-known in Pay-TV systems. There have been various activities to resolve them from very beginning of ratifying the CA system in the DVB group. However, an effective solution has not yet been suggested to provide a platform whereby not only current issues but also long term demands of the market can be satisfied effectively.

Herewith, taking into account the current research and industrial activities regarding the convergence of services and networks, we are introducing new elements from mobile technology into the traditional Pay-TV system to ultimately transfer this system to a more flexible, intelligent, scalable, interoperable and ubiquitous system. The following chapter treats the abovementioned requirements through employing various security architectures.

III. SYSTEM DESIGN

The Mobile Integrated Conditional Access System (MICAS) introduces new subsystems into the current Pay-TV system which are explained as follows.

It is postulated that the STB located at the vicinity of the subscriber supports Bluetooth and/or GSM communications and has a unique universal identity (STB-ID), which is recognizable by the service provider in the network. It is also assumed that the subscriber runs an application (Follow-Me application) on his/her mobile phone to generate subscription requests. This application can be installed in the form of a MIDlet on subscriber's Java-enabled mobile phone by mobile phone manufacturers, service providers or by subscriber itself.

The MICAS is described by explaining a general use case scenario where a subscriber would like to view a programme (or a channel) included in his/her subscription package, from an arbitrary STB. The subscriber needs to run the Follow-Me application to discover the available Bluetooth devices operating at the vicinity of the subscriber. After selecting the intended STB, the pairing process is performed between subscriber's mobile phone and STB. The STB-ID is then transferred to the mobile through Bluetooth channel. The Follow-Me application provides the subscriber with a list of Follow-Me service providers followed by associated services. After selecting the service provider and desired service(s), the Follow-Me application generates a subscription request message, which includes the service description, subscriber's International Mobile

Subscriber Identity (IMSI), STB-ID and subscriber's register code that shows whether the subscriber's mobile phone is compliant with service provider's security and privacy policy. The Follow-Me application then sends the subscription request to the service provider.

At the transmitter head-end, Message Handling Subsystem (MHSS) handles subscribers' requests received from its GSM interface. It processes subscription requests and checks if subscriber and STB are presenting valid identities (ID). If the identity check process succeeds, the MHSS will contact the Subscriber Handling Subsystem (SMS). The SMS checks the subscriber's records and entitlements, and accordingly instructs Subscriber Authorisation Subsystem to generate corresponding entitlement message (Security Object). The SAS returns the associated Security Object to the MHSS to be encoded and sent to the subscriber's mobile phone. The MHSS checks the subscriber's register code before transmitting the Security Object. If the register code is not complied with service provider's security policy, the MHSS (re)initialise the subscriber's SIM card using requisite Key information and security algorithms [13]. These information should be transferred securely and stored in a privileged domain on the SIM card, where is solely accessible to the Follow-Me service provider and/or mobile provider. This information should be treated as the same way as the GSM SIM treats GSM cipher keys. The Security Object processing can be shared between the SIM card and STB. Hence, the mobile phone can be as the main security elements or be an intermediary means to deliver the Security Objects to the STB to descramble contents. The security information encapsulated into the Security Object can convey any information regarding the Key hierarchical system [8].

Fig. 2 shows the data flow in the system where Security Object (i.e. Master Key and rights) delivered to the STB via mobile phone, and EMM and ECM messages are broadcast to all receivers' population.

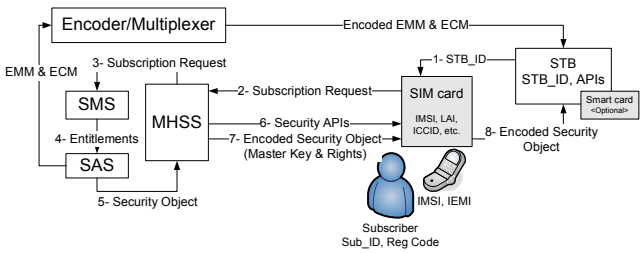

Figure 2: Delivery of security objects to the STB via mobile phone.

The service provider might adopt additional security mechanisms to guarantee the integrity and confidentiality of the Security Objects. Therefore, in addition to the Follow-Me application, there might be other application(s) (SIM applet) running on the SIM card responsible for executing service provider's specific security sensitive algorithms. The SIM applets can be designed to run encryption and decryption algorithms based on Key information provided by service provider. Moreover, these applications can provide the service operator with insight into subscribers' behaviour [14]. This would generally improve the level of security and services offered to customers.

The underlying protocol used to transfer data across GSM network can be Short Message Service (SMS) or Wireless Application Protocol (WAP) [12]. On the other side, the mobile phone may communicate with the STB through GSM or Bluetooth channel, depending on STB capabilities. The STB also needs to be equipped with standard Application Programme Interfaces (APIs) to handle I/O and possibly some security activities over interaction channel (i.e. GSM). These APIs shall be installed by STB manufacturer on secure domains (flash memory or smart card) to perform security-related algorithms and fulfil authentication, decryption and descrambling processes.

There might be some concerns about exposing security information on Bluetooth channel. However, this issue can also be addressed using security services offered by Bluetooth technology [10], [11] and adopting additional cryptosystems and techniques to ascertain that data is not exposed and the security architecture fails gracefully.

Fig. 3 shows the deployment diagram of the MICAS system presenting the correlation amongst security elements in the system.

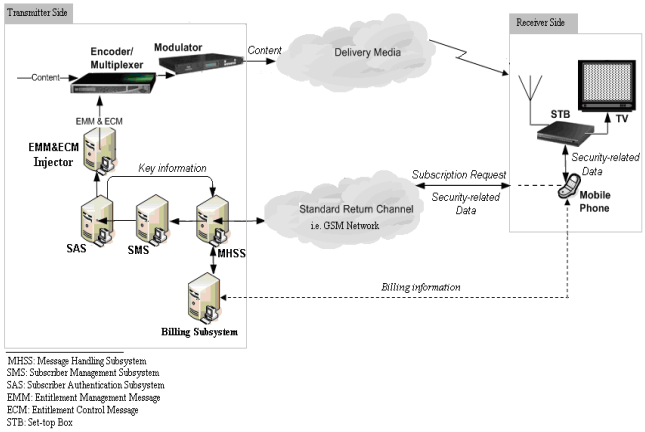

Figure 3: Overall layout of the system.

IV. CONCLUSION

In this document, the high-level security architecture for provisioning of a horizontal market in Pay-TV industry and for establishing interoperability amongst various CA systems was proposed. The Mobile Integrated Conditional Access System (MICAS) was explained. 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 MICAS would reduce service deployment costs and subscription fees for service provider and end-users respectively. It is also equally beneficial for end-users as there would be no need to have additional receiver(s) to join the other service providers; as the proposed system provides a dynamic platform which affords interoperability amongst service providers. Moreover, it improves the overall security in the system by interacting with receiver head-end and downloading new security mechanisms on the fly as and when it is needed. Furthermore, the functions of revoking the compromised keys and monitoring the contractual behaviour of subscribers are performed automatically and cost-effectively through GSM (or its descendants like UMTS, 3G and etc) interaction channel. Other advantages of such interactions would be emergence of wider range of personalised services as well as ubiquitous access to them which comes with the 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 ensure that security requirements are met by proposed security architectures. Therefore, analysing security threads and introducing security counter-attacks play great role in success of the proposal. Our research which we are in the process of conducting, addresses the above mentioned concerns and also the effect of GSM network performance on the proposed system, the security measurements, the implementation and finally thorough analysis of the related subsystems.

REFERENCES

[1] 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

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

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

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

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

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

[7] ITU-R Rec. BT.810: "Conditional-access Broadcasting Systems", 1992.9

[8] Zhu M., Zhang M., Chen X., Zhang D., Huang Z., "A Hierarchical Key Distribution Scheme for Conditional Access System in DTV Broadcasting", CIS 2006, LANI 4456, pp. 839-846, 2007

[9] Xie Q., Zheng S., Yu X., "A Smart-Card-Based Conditional Access Subsystem Separation Scheme for Digital TV Broadcasting", IEEE Transaction on Consumer Electronics, vol. 51, no. 3, August 2005

[10] Karygiannis T., Owens L., "Wireless Network Security 802.11, Bluetooth and Handheld Devices", National Institute of Standards and Technology, Special Publication 800-48

[11] Lamm G., Falauto G., Estrada J., Gadiyaram J., Cockerham D., "Bluetooth Wireless Networks Security Features", ISBN 0-7803-9814-9, IEEE 2001

[12] Jorstad I., Dustdar S., Do T. V., "An Analysis of Current Mobile Services and Enabling Technologies", International Journal of Ad Hoc and Ubiquitous Computing, Vol. 1, Nos 1/2, 2005

[13] MacDonald J. A., Sirett W., Mitchell C. J., "Overcoming Channel Bandwidth Constraints in Secure SIM Applications", 20th IFIP International Information Security Conference (Sec 2005) - Small Systems Security and Smart cards, Makuhari-Messe, Chiba, Japan, 31 May 2005.

[14] Wright T., "Security Considerations for Broadcast Systems", Information Security Technical Report 11 (2006) 137 - 146