Journal of Zhejiang University SCIENCE A
ISSN 1009-3095 (Print); ISSN 1862-1775 (Online)
www.zju.edu.cn/jzus; www.springerlink.com
E-mail: jzus@zju.edu.cn

A smartcard conditional access interface scheme for conditional access subsystem separation in digital TV broadcasting*

XIE Qiang†, ZHENG Shi-bao, YU Xiao-jing
(*Institute of Image Communication and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China*)
†E-mail: qxie@sjtu.edu.cn

Received Aug. 15, 2005; revision accepted April 18, 2006

Abstract: Conditional access system (CAS) is a key technical component in digital TV broadcasting through which TV operators manage the appropriate rights of different subscribers in order to protect their commercial benefits. The normal digital TV receiver can only receive and decode the pay TV programs scrambled by one specific CAS. In this paper, the authors proposed a smartcard conditional access interface (SCAI) scheme in order to make the digital TV receiver be a common receiving platform independent of any specific CAS employed at the broadcasting head-end. As a result, it only needs to include a common conditional access software package (CCAP) without any requirement of hardware modification in the receiver. Comparison between the two mentioned DVB-CI-based schemes showed that the cost of such kind receiver is greatly reduced. The main design points of the proposed scheme and its reference implementation's architecture are presented in this paper. This scheme is also one of the candidate national standards for Chinese digital TV broadcasting industry.

Key words: Digital TV broadcasting, Conditional access subsystem separation, Smartcard interface
doi:10.1631/jzus.2006.A1008 **Document code:** A **CLC number:** TN931.2

INTRODUCTION

With the introduction of digital TV broadcasting in China, TV operators can deliver their TV programs and value-added services to their subscribers more efficiently and conveniently than the analog counterpart. Most main technical components of digital TV broadcasting have been adopted by the Chinese government as the de facto national standards. For example, the standards relating to the programs' source coding are MPEG-2 (ISO/IEC 13818, 1996~2004) or MPEG-4 (ISO/IEC 14496, 2001~2005) series international standards. For the aspects relating to digital TV program transmission, there are DVB (Reimers, 2001), ATSC (Whitaker, 2001) and ISDB (Asami and Sasaki, 2006) series international standards. The method of terrestrial transmission has not yet been standardized for China, while the most often used method of cable transmission is DVB-C (Reimers, 2001), as the de facto industry standard. In order to control the subscriber's access to these standardized digital TV programs broadcasted by various TV operators to ensure that only those authorized subscribers who have paid the corresponding fees can watch these programs, the technique of conditional access (CA) has been created and it has also experienced a long evolution history just as TV broadcasting (Macq and Quisquarter, 1995). Due to the consideration of system security and market competition, most current commercially available conditional access systems (CASs) have not been standardized, which means they are not compatible with each other. The conditional access subsystem (CASS), which is a necessary part of CAS at the broadcasting receiving end, is also not compatible with each other. This is the underlying reason why the digital TV receiver equipped with one CASS cannot receive and decode the programs scrambled by other CASs. If one sub-

* Project (No. 200442) supported by the Electronics Development Foundation for the Key Industrialization Project of the Ministry of Information Industry, China

scriber wants to watch those programs scrambled by different CASs, he/she has to purchase additional receiver equipped with the corresponding CASS. Thus, the CAS is at the technical core of the whole digital pay TV business (Mooij, 1994).

Let us take a brief overview of the most current commercially available CASSs. Most of these CASSs can be classified into two categories according to the different locations of the interface between the digital TV receiver and the CA security module (CAM). These two possible locations are illustrated in Fig.1 as *I*1 and *I*2.

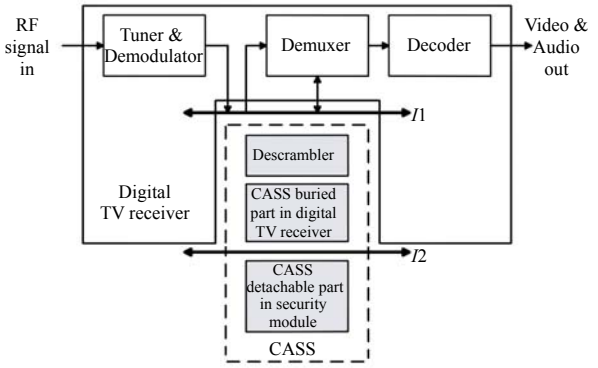

Fig.1 Two possible locations of the interface between the digital TV receiver and the CA security module

When this interface is located at *I*2 as indicated in Fig.1, which is the most common case for those CASs already deployed in China, the whole CASS is composed of two parts: the CASS buried part in digital TV receiver and the CASS detachable part in security module. For this kind of CASs, the often-used security module hardware is a smartcard using 8-bit CPU with dedicated cryptographic coprocessor. Smartcard is cheap and has mature hardware and software security mechanisms to ensure the confidentiality and integrity of the CASS detachable part. This detachable part contained in smartcard is the most security critical part of the whole CASS. It often contains many proprietary cryptographic algorithms, various CA related functions, such as authentication and pairing-up algorithms to bind up the digital TV receiver and the smartcard, subscriber personal distribution key, subscriber entitlement files, subscriber consuming history files, etc. (Zheng and Zheng, 2004). The corresponding CASS buried part provides the necessary support needed by the detachable part in order to correctly provide many CA related functions as a whole CASS. Such support usually contains the operating system (OS) related functions, MPEG transport stream (TS) or packetized elementary stream (PES) demuxing and descrambling, on screen display (OSD), program loader, the possible bidirectional communication channel support through the cable, etc. Because the buried part is provided by one specific CAS supplier, who provides the CAS at the broadcasting head-end, the digital TV receiver equipped with this CASS is bound with this CAS and can only receive and decode the programs scrambled by this CAS. In order to provide such digital TV receivers, the receiver manufacturer has to bid the order of receivers from one TV operator first, and then pay expensive license fee to the CAS supplier in order to use its CASS in their receivers. After signing a non-disclosure agreement (NDA) with the CAS supplier, the manufacturer gets the technical specification needed to port the CASS buried part to its receivers. The last step before shipping the receivers to the TV operator is a completion of a compliance test conducted by the CAS supplier in order to get the certification. Because such kind of digital TV receivers are not compatible with those using different CASSs, the TV operator has to provide the digital TV receivers directly to its subscribers in order to deliver its scrambled pay TV programs. This kind of receiver is tailored to one specific TV operator, especially to the CAS employed by this TV operator (Kamperman and Rijnsoever, 2001). If one subscriber wants to watch the TV programs scrambled by other CASs, he/she has to purchase additional corresponding receivers. It is obviously an unnecessary waste of investment for the subscriber. Especially at present in China, most local city TV operators have the freedom to choose any CAS they think appropriate, and in the mean time it often has only several thousand digital TV subscribers. For all these TV operators, one receiver manufacturer has to design and produce the specific model required by one TV operator. Thus, the receiver manufacturer has to pay expensive CASS license fee for each CASS it used and pay for the costly research and development (R&D) expense, in the mean time loses the commercial scale. The resulted receivers are quite expensive for common customers in a developing country like China. The Chinese government has realized this problem and made efforts to make the CASS separation as a technical

policy from Chinese digital TV broadcasting industry. Considering the tremendous expense of transformation from analog to digital TV broadcasting, we propose this smartcard conditional access interface (SCAI) scheme for CASS separation in this paper, which is significantly cost efficient compared to the other two schemes mentioned in the later part of this paper.

VARIOUS CASS SEPARATION SCHEMES

The effort to make the digital TV receiver be a common receiving platform independent of any specific CAS has experienced a long history. Various CASS separation schemes have been proposed throughout the world and some of them have already been standardized.

The DVB project initialized in Europe has already realized the deleterious results caused by the incompatibility problem between different CASs. Two methods have been proposed to reach the target of making the receiver be a common receiving platform. These two methods are Simulcrypt and Multicrypt (Cutts, 1997). In Simulcrypt, different CASs can exist concurrently in one broadcasting head-end with one common receiving platform. The distinctive characteristic of Simulcrypt is that all CASs in one broadcasting network share the same descrambling key and use the standardized common scrambling algorithm (CSA) specified by DVB (DVB Blue Book A011, 1996). To realize Simulcrypt, a common interface and common scrambling module are needed at the broadcasting head-end between different CASs. It is obviously not an easy task to reach the above stated condition considering the competition among CAS suppliers. Additionally, in the perspective of system security, the whole broadcasting network's security level is aligned with the weakest CAS deployed in this network (Giachetti *et al*., 1995). Another negative effect caused by Simulcrypt is that the bandwidth used to transport all CA messages used by all deployed CASs is greatly increased compared to the case of using just one CAS, which is a great waste of bandwidth. The advantage of Simulcrypt is that the subscriber can use cheap smartcard as CAM to watch pay TV programs scrambled by the corresponding CAS using one common receiver.

Considering the difficulty of reaching an agreement to use Simulcrypt, the Multicrypt scheme was proposed to allow different CASs exist concurrently and scramble the pay TV programs independently at the broadcasting head-end. At the receiving end, the CASS resides as a whole part in one CAM and the interface between the digital TV receiver and the CAM is located at *I*1 as depicted in Fig.1. The *I*1 interface is often stipulated as a common interface used by different CASs. There are many standardized common interface schemes, such as the most popular DVB-CI (CENELEC En 50221, 1997), OpenCable (Adams and Dulchinos, 2001), NRSS-B (EIA 679-B, 1999) and DAVIC CA0 (DAVIC 1.4 Specifications Part 10, 1998). Due to the high communication data rate between the receiver and the CAM, all these schemes use PCMCIA (PCMCIA, 2001) card, whose cost is much higher than the smartcard.

There is also one smartcard-based common interface scheme, DAVIC CA1 (DAVIC 1.4 Specifications Part 10, 1998), which locates the interface at *I*2 and makes it a common interface. However, DAVIC CA1 stipulated a detailed specification on how to implement this common interface in a way like ISO/IEC 7816-4 (ISO/IEC 7816-4, 1997). In this specification, detailed data objects used by this scheme are defined and the smartcard file system used to store these data objects is also specified. However, most CAS suppliers are reluctant to reveal any implementation details about the CASS detachable part in smartcard because it is the security core of the whole CASS. As a consequence, DAVIC CA1 has not been widely used by CAS suppliers.

Currently, three schemes have been proposed in China to reach the target of CASS separation. Two of them use revised DVB-CI technical specification based on PCMCIA card or USB 2.0 (Compaq *et al*., 2000) card as the CAM hardware, respectively. As DVB-CI, these two schemes locate the interface between the digital TV receiver and CAM at *I*1 as illustrated in Fig.1. The third one is our proposed SCAI scheme using smartcard as the CAM hardware. The first two schemes basically have not much difference because the DVB-CI specification was designed to be able to support any physical interface only if this physical interface can satisfy the required communication data rate. For these two schemes, a demuxer, a descrambler and a multiplexer have to be included in the CAM because the input and output of the CAM

are at the MPEG TS level. This is an unnecessary duplication because most current commercially available digital TV receiver decoder chips have already included these components as standard components. To ensure the CAM's security, a smartcard is often still needed because only the smartcard has intrinsic security-related capabilities as we have mentioned in the introduction. The need of smartcard in one CAM which locates the interface at *I*1 can also be proved in schemes using OpenCable architecture (Song *et al*., 2003), which is the digital cable TV (CATV) standard in North America areas. In addition, a content protection (CP) or digital right management (DRM) mechanism has to be employed to effectively protect the descrambled MPEG TS transported over this common interface being pirated. However, such mechanism is far from mature at present.

The CAM hardware used in these two DVB-CI-based schemes is much more expensive than the smartcard used in SCAI scheme. The license fees for using DVB-CI, PCMCIA and USB 2.0 related patents have not yet been decided and it is quite possible that these fees are quite expensive when these two schemes are widely used—the DVD player is one typical example. In addition, most sold receivers (especially the set-top boxes) produced in China are designed to receive and decode standard definition TV (SDTV) programs as the equipments used for the transformation from analog to digital TV broadcasting. Most of these receivers have no PCMCIA or USB 2.0 physical interface slot. Often there is only one or two smartcard slots that have been installed because most SDTV decoder chips have embedded the ISO/IEC 7816-3 (ISO/IEC 7816-3, 1997) physical interface (smartcard interface) I/O ports. In order to use the two DVB-CI-based schemes, all sold receivers have to be discarded and new models of receivers equipped with PCMCIA or USB 2.0 slots have to be produced. It is a great infrastructure investment waste for the TV operators or the subscribers.

PREVIOUS SMARTCARD-BASED SCHEMES

Because of the above stated obvious high cost-efficiency of using smartcard as the CAM hardware, many smartcard-based CASS separation schemes have been proposed, such as the DAVIC CA1 and the scheme proposed in (Zheng and Zheng, 2004).

We have already stated the reasons why DAVIC CA1 has not been widely adopted by CAS suppliers. As for the scheme proposed in (Zheng and Zheng, 2004), the authors suggested to implement the whole CASS in one smartcard using a high-performance 32-bit reduced instruction set computer (RISC) CPU as the CAM hardware. A downloadable common CA module (DCCAM) has to be included in both the digital TV receiver and the smartcard. This scheme has several commercial and technical shortcomings which make it a quite unpractical proposition in the real world. First, most current 32-bit RISC CPUs are not designed for security purpose, which means they are not equipped with a cryptographic coprocessor to assist the computation intensive operations related to the data encryption and decryption frequently encountered in CASS. If we use a 32-bit RISC CPU equipped with cryptographic coprocessor, the cost of the CAM will greatly increase. In addition, using 32-bit CPU means the CAS supplier has to re-cast the whole CASS software which formerly runs on 8-bit~32-bit CPU. This is obviously not an easy task considering the complexity and security requirement of CASS. Thus, this scheme obviously loses the advantage of low cost alleged by Zheng and Zheng (2004). Second, the middleware has not been standardized and thus is not widely used in China, and as the direct consequence, most digital TV receivers cannot support platform-independent software programs, such as codes written in Java. Without middleware, all codes must be written in native program languages, such as C, C++ or assembly language. The codes written in these program languages must be compiled and linked as a whole, or pre-compiled as a dynamically linked library (DLL) if the receiver's OS supports DLL. Considering the abundance of receiver decoder chips available, obviously DCCAM and any such kind of schemes using download are unrealistic for the current mainstream decoder chips. Third, due to the considerations about the intelligent property and system security of the CAM, most CAS suppliers are possibly unlikely to accept a common module, such as the DCCAM, in (Zheng and Zheng, 2004)'s CAM software, which is the secure core of the whole CASS. We have already noted that DAVIC CA1 has not been accepted by CAS suppliers due to the same reason.

PROPOSED SCAI SCHEME

The proposed SCAI scheme for CASS separation locates the interface between the digital TV receiver and the CAM at *I*2 and makes it a standardized common interface. Fig.2 outlines the reference system model for this scheme from the perspective of data streaming path between the receiver and the smartcard. As shown in Fig.2, at the digital TV broadcasting receiving end, the previously wholly proprietary CASS is divided into two parts. The CASS buried part in receiver, which provides the necessary data and function support needed by the CASS buried part in smartcard, becomes a common part for all CASs. The buried part is under the complete control of CAS suppliers and is still proprietary. Both parts interact with each other through the standardized SCAI interface. The detailed interaction protocols of this interface are stipulated in the SCAI interface technical specification and will be formulated as a standard. For the initial design of the proposed SCAI interface scheme as a scheme using smartcard as CAM hardware, please see (Xie *et al.*, 2005).

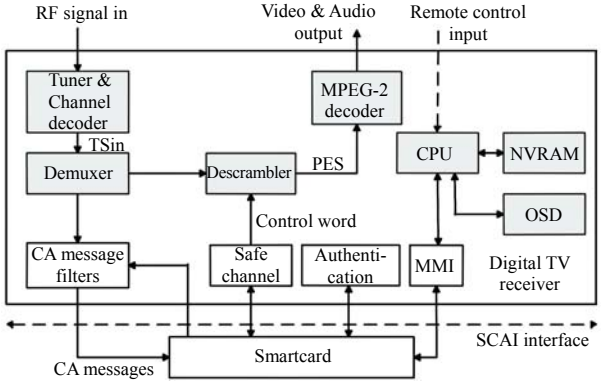

Fig.2 Reference system model for the proposed SCAI scheme in the perspective of data streaming path

The SCAI interface is designed following the ISO OSI layered protocol model in order to keep its extendibility because of possible future expansion of CA functions. Considering that most receivers will only be equipped with one smartcard slot, there is no session layer designed in the SCAI interface (compared to the DVB-CI-based schemes or the OpenCable specification) in order to reduce the complexity of the whole scheme and its implementation cost. Fig.3 illustrates the detailed layers in the SCAI interface.

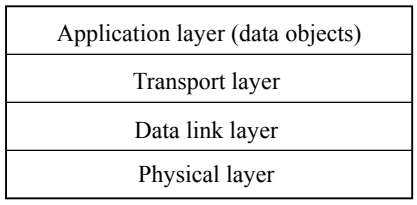

Fig.3 Protocol layers in the SCAI interface

All application layer data are defined as data objects which are coded by means of basic encoding rule Tag-Length-Value (BER-TLV) derived from that used to code ASN.1 syntax (ISO/IEC 8825-1, 2002).

All data objects are contained in the *data* field of the application protocol data unit (APDU) commands and the corresponding responses as stipulated in ISO/IEC 7816-4. These APDUs are passed into the transport layer (using ISO/IEC 7816-3 *T*=1 transmission protocol) or directly into the data link layer (using ISO/IEC 7816-3 *T*=0 transmission protocol) and then transported over the ISO/IEC 7816-3 physical interface (i.e. smartcard interface). Only five APDU commands have been defined in the proposed SCAI interface compared to the ISO/IEC 7816-4 specification to assist the interactions between the receiver and the smartcard. These APDU commands include: *Get_data_more*, *Get_data_last*, *Put_data_more*, *Put_data_last*, and *Get_response*. For simplicity in transmitting related software program implementation and the support of those smartcards using small transmission buffer, all these APDU commands and the corresponding responses are designed to be able to support data object partitioning and combining. Each APDU command and its response are mapped into the transport protocol data unit (TPDU) using different transmission protocol, *T*=0 or *T*=1 in SCAI interface, as indicated by the smartcard. Each APDU and its response are stipulated not to exceed 255 bytes because of the above stated reasons. This stipulation is reasonable because most CA messages that must be transported over this interface are often no longer than 255 bytes, thus extra protocol overhead is avoided.

Among these 5 APDU commands, *Get_data_more* and *Get_data_last* are used to enquire and retrieve one or more data objects from the smartcard. *Get_data_more* is used to inform the smartcard that there are still more data needed to be transported until receiving *Get_data_last*, from that time the process-

ing of the transported data object(s) can be started in the smartcard. *Put_data_more* and *Put_data_last* are used to send one or more data objects to the smartcard for processing, such as data encryption, data decryption, data storage and so on. *Put_data_more* is used to inform the smartcard that there are sill more data needed to be transported until receiving *Put_data_last*, from that time the processing of the transported data object(s) can be started. *Get_response* is used to retrieve the response from the smartcard when the smartcard needs long time to process the data object(s) sent by the receiver and this processing period has exceeded the interaction time-limit specified in ISO/IEC 7816-3. Another case when receiver needs using *Get_response* is when there are several parts of data needed to be retrieved since each response should not exceed 255 bytes. It should be emphasized here that all protocol interactions using these APDU commands have to follow the Request-Answer pattern because the smartcard should always be passive and never start a protocol interaction first as stipulated in ISO/IEC 7816-4. Fig.4 illustrates one data exchanging course example using these APDU commands and the corresponding responses. The value of the *SW*2*_field* in different cases is presented in Fig.4 to emphasize its new usage compared to ISO/IEC

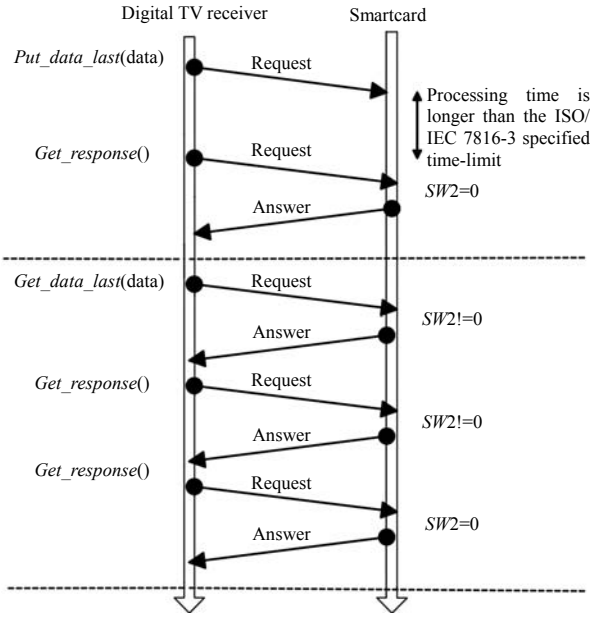

Fig.4 One example data exchanging course between the receiver and the smartcard using the APDU commands and the corresponding responses defined in the SCAI interface

7816-4 specification. Interested readers are encouraged to read the ISO/IEC 7816-4 specification to better understand the basic concept of APDU commands and responses.

Digital TV broadcasting related applications can be classified into 4 types using SCAI interface. To support these applications, various data objects have been defined to support the needed protocol interactions between the receiver and the smartcard.

The first data object type is related to the common security mechanism of the SCAI interface. This is the security core of the SCAI interface. Because this scheme is designed to be a standard, the detailed specification of this scheme will finally be open and available to the public, which is contrary to the practice of CAS suppliers. The detailed protocol interactions are stipulated in the SCAI interface technical specification and are open, which will potentially endanger the security level of the whole CASS using the SCAI interface. The previous wholly proprietary CASS does not open any interaction details between the receiver and the smartcard, so the vulnerability of the proposed scheme to potential malicious attacks is obviously greater than the proprietary one. In order to ensure the security level of the proposed scheme will not be reduced as an open standard compared to the previous wholly proprietary CASS, a common security mechanism has been devised and stipulated in the SCAI interface. This security mechanism uses a bilateral authentication algorithm to ensure the legitimacy of the smartcard inserted into the receiver and vice versa. After passing the authentication, a safe channel is set up between the receiver and the smartcard to safely transport data over the smartcard interface and prevent the data from interception and tampering. The authentication algorithm is based on digital certificate issued by a third part independent of the CAS supplier and the receiver manufacturer. The safe channel uses a set of symmetric encryption algorithms, such as DES, Triple-DES and AES (Stinson, 2002). The actual used encryption algorithm is chosen by the smartcard according to its encryption capability. Whether the data objects transported over the smartcard interface are encrypted or not can be identified by the *CLA* field of the APDU command and the *flag* field of the response (its first byte). The authentication process and safe channel set-up process are designed to be unified algorithm in order to improve

the security mechanism's security level. This unified algorithm has been carefully designed to be an unbalanced and light-weight one which is suitable for the resource-constrained 8-bit smartcard and the computation-power-limited normal receiver decoder chip. This unified algorithm can prevent the SCAI interface from the following typical attacks: Attacks of Oracle type, Replay attack, Attacks of Sign type, Substitution attack and Partial Chosen Key attack (Stinson, 2002).

The second data object type is related to the unified CA message filtering and its corresponding processing mechanism. Thanks to a series of international standards adopted by the digital TV broadcasting industry in China, the SCAI interface can stipulate a unified CA message filtering mechanism to satisfy the data support needed by most CAS suppliers in the receiver. The MPEG-2 part 1 (ISO/IEC 13818, 1996~2004) has stipulated how private data other than the video and audio data bits and other necessary standard tables being multiplexed into the MPEG-2 TS or PES through *private_section* mechanism. DVB-CA (ETSI ETR 289, 1996) also has described the minimum set of common CA elementary to achieve the interoperability between different CASs. With these standards, a unified CA message filtering field and the acquiring of the corresponding filtering conditions from the smartcard are stipulated in the proposed SCAI scheme. This unified filtering field is shown in Fig.5. The digital TV receiver also needs to obtain the conditional access table (CAT) of the current TS and the program map table (PMT) of the current playing program in order to extract the *CA_system_ID* and the *CA_PID* from the *CA_descriptor* contained in these two tables. The most often filtered CA messages are the entitlement management message (EMM) and the entitlement control message (ECM). The interactions between the TV watcher and the smartcard, when the program entitlement related interactions are necessary, are communicated through the high-level man machine interface (MMI) data objects similar to DVB-CI, which include *text*, *enquiry*, *answer*, *menu* and *menu_ans*.

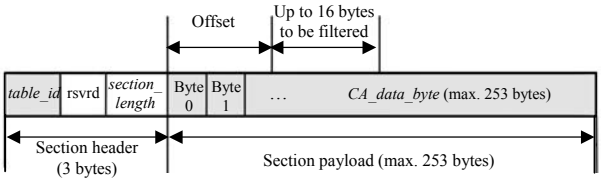

Fig.5 Unified filtering field of CA messages (CA related *private_section*)

The third data object type is related to the smartcard's properties and various value-added services provided by various CAS suppliers. The data objects defined as the smartcard's properties are used for the convenience of the smartcard's distribution management. The main properties include the smartcard's ID, the version of the SCAI interface specification the smartcard supports, its provider ID (same as *CA_system_ID*) and so on. The multifold value-added services provided by the various CAS suppliers result in the fact that the data objects related to this aspect are the most extendable part in the interface. The typical value-added services related data objects are electronic purse used in impulse pay per view (IPPV), pay per view (PPV), unidirectional e-mail, unidirectional short message, weather forecast, etc. Most of these data objects are defined as compound data objects containing MMI data objects and purpose-specific data objects in order to ensure the universality between different CASs. The display style and format of these data objects are at the control of the receiver manufacturers in order to keep their characteristics.

The fourth data object type is related to the possible existing bidirectional communication channel to the broadcasting head-end using the common program loader (CPL) through either the telephone-line modem or the cable modem. The common program loader is currently under consideration in order to facilitate the online upgrading of the receiver software either through the possible existing bidirectional communication channel or through MPEG TS. Because most current digital TV receivers are not equipped with modem and program loader is a quite difficult technology, these two classes of data objects have not yet been fully defined and they may be presented as the standard's appendix. The reference implementation discussed later does not include functions related to this type of data objects.

REFERENCE IMPLEMENTATION

In order to verify the feasibility of the proposed

CASS separation scheme using SCAI interface in the real broadcasting network and make preparation for the standard compatibility test when this scheme is submitted for examination and approval as a standard, we have developed a reference implementation of the proposed scheme on several set-top box platforms. This reference implementation includes two parts: the common part in the receiver and the cooperating smartcard compliant with the SCAI scheme which is provided by the CAS supplier. The common part in the receiver can be implemented as a pure software package and we call it common CA software package (CCAP) using ANSI C or C++ program language. Because the SCAI scheme has no detailed implementation specification on how the CAS supplier implements the CASS detachable part in smartcard except in compliance with SCAI interface specification, we will only present the system architecture and the logical constituent function modules of CCAP. We hope it can help the readers to better understand the working principle of the proposed scheme.

Following the reference system model illustrated in Fig.2, the CCAP in the receiver has no requirement of hardware modification for most currently available digital TV receivers by taking advantage of those already existing necessary hardware components in the receiver (components with shadow). The only requirement for one normal receiver to be a common receiving platform compliant with the SCAI interface specification is an inclusion of the CCAP (components without shadow).

CAAP is located under the digital TV receiver's application programs and above its OS and device drivers as for the CCAP's place in the receiver's whole software architecture. Like the previous wholly proprietary CASS buried part in the receiver, the CCAP also expresses it through two layers of interface which can be standardized as application program interface (API) functions. These two layers are: the "App layer" and the "Porting layer". All underlying support needed by the CCAP is defined in the Porting layer's API functions. The CA related functions provided by the CCAP are defined in the App layer's API functions. By doing so, the digital TV receiver manufacturer can follow the same developing flow as that using the previous proprietary CASS. This design can help the receiver manufacturer accelerate its product development and shorten the period of R&D before shipping their new products to the market. Fig.6 outlines the system architecture of the CAAP and its logical location in the receiver's software structure.

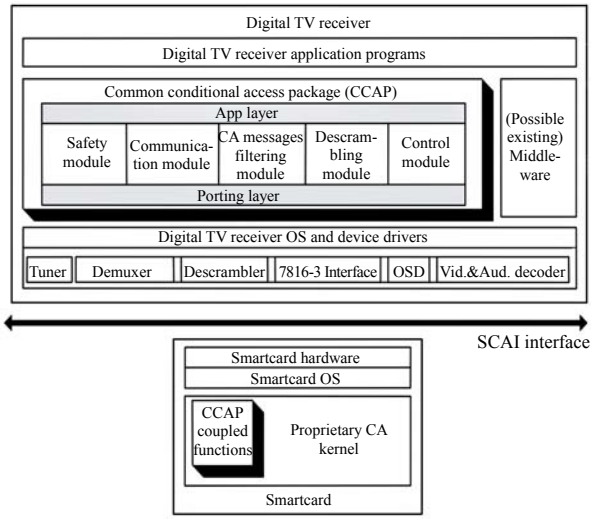

Fig.6 System architecture of the CCAP and its logical location in the receiver's software structure

In order to streamline R&D of the reference implementation and better illustrate the different types of data objects interacting between the digital TV receiver and the smartcard through SCAI interface, we divided the CCAP into several logical constituent function modules. Fig.7 outlines these function modules and the connections between them and the outer environment in the receiver.

In order to communicate with various kinds of smartcards used by different CAS suppliers as the

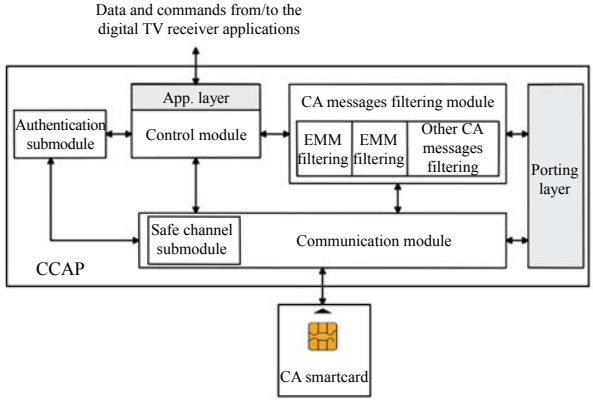

Fig.7 Logical constituent function modules of CCAP and the interconnections between them and the outer environment

CAM hardware which may have different communication data rate capability or transmission protocol (T=0 or T=1), CCAP utilizes the "Communication module" to deal with all aspects related to data communication between the receiver and the smartcard using SCAI interface. Any other function module of CCAP can interact with the smartcard without knowing the complex communication details on how to using the SCAI interface. This will greatly reduce the burden of the software developers who are in charge of other function modules.

The bilateral authentication algorithm and the setup of safe channel are parts of the common security mechanism of the CCAP and can be realized as the "Safety module". The software developer has to master some basic knowledge of cryptology to implement this module. Because the authentication process is only executed whenever the smartcard is inserted into the smartcard slot or the receiver is powered on, while the safe channel has to be sustained throughout the whole working phase of the receiver, thus the Safety module is separated into two submodules: the Authentication submodule and the Safe channel submodule as shown in Fig.7. The software developer of the Safe channel submodule can focus on the implementation of various symmetric encryption algorithm stipulated in the SCAI interface specification and simply use the key negotiated during the course of bilateral authentication as the safe channel's session key.

The main part of CCAP is about the unified CA message filtering and processing mechanism which is independent of any specific CAS. This part is implemented as the CA message filtering module which is in charge of the filtering out of various kinds of CA messages according to the filtering conditions given by the smartcard and the following processing.

The Control module provides the resources for CCAP to control the interaction between the receiver and the TV watcher. It receives data and commands from the receiver's application programs through the API functions defined in the App layer and also harmonizes the operations among other function modules of the CCAP in order to provide the CA related functions required by the receiver. The Control module is also in charge of the procedural execution sequence decision of the whole CCAP. As an example, when the Authentication submodule reports to the Control module that the receiver or the smartcard has failed the bilateral authentication, then any further interactions will be suspended by the Control module which then gives out indication to the TV watcher.

CONCLUSION

We presented an SCAI interface scheme for the CASS separation at the digital TV broadcasting receiving end in order to make the digital TV receiver a common receiving platform independent of any specific CAS deployed at the digital TV broadcasting head-end. The reference implementation of this scheme is also presented in this paper. This scheme strikes at the target of lowest cost among all the three CASS separation propositions in China. With our proposed scheme, there is no requirement of any hardware modification for the current widely used digital TV receivers (especially the set-top boxes) compared to the other two DVB-CI-based schemes. The only requirement is an inclusion of a CCAP in the receiver. The CASS detachable part is still under the complete control of the CAS suppliers. This makes the CAS suppliers have enough innovation space on how to implement the SCAI interface in their CAM and keep their product's characteristics. By this way, the CAS supplier's intelligence property and the system security of their CAM are efficiently protected.

Digital TV receiver manufacturers can easily change their current receivers to be the common receiving platforms required by the government using the proposed SCAI interface scheme. Furthermore, using the SCAI interface scheme they no longer need to pay the expensive license fee and royalty to the CAS suppliers. Thus, the cost of receivers using SCAI interface is greatly reduced compared to the two DVB-CI-based schemes.

Local city TV operators can freely choose CAS to scramble their pay TV programs. They can switch from one CAS to another at any time needed. The TV operators do not need complex trans-control technique (Macq and Quisquarter, 1995) to distribute the pay TV programs provided by other TV operators using different CASs, such as CCTV in China. The most significant benefit is that the TV operator need

not directly provide digital TV receivers free of charge or at low price to their subscribers in order to introduce digital TV broadcasting. This will greatly reduce the business risks for some small local TV operators to start digital TV broadcasting.

Government can realize the project of the whole transformation from analog to digital TV broadcasting more easily with low price receivers using the SCAI interface scheme.

Currently, prototype set-top boxes using the SCAI interface scheme have passed the initial certification test conducted by several CAS suppliers. These prototype digital TV receivers produced by several receiver manufacturers have been successfully exhibited on the 9th Beijing International Software Exhibition 2005 and the BIRTV Exhibition 2005. The following online field test will be conducted in Shanghai. The standardization of the proposed SCAI interface scheme is also under way.

References

Adams, M., Dulchinos, D., 2001. OpenCable. *IEEE Commu. Mag.*, **39**(6):98-105. [doi:10.1109/35.925676]

Asami, H., Sasaki, M., 2006. Outline of ISDB systems. *IEEE Proc.*, **94**(1):248-250. [doi:10.1109/JPROC.2005.859690]

CENELEC En50221, 1997. Common Interface for Conditional Access and Other Digital Video Decoder Applications. Comité Européen de Normalisation Électrotechnique CENELEC.

Compaq, Hewlett-Packard, Intel, Lucent, Microsoft, NEC, Philips, 2000. Universal Serial Bus Specification, Revision 2.0.

Cutts, D.J., 1997. DVB—conditional access. *IEEE Electronics & Communication Engineering Journal*, **9**(1):21-27. [doi:10.1049/ecej:19970104]

DAVIC 1.4 Specifications Part 10, 1998. Basic Security Tools. Digital Audio-Visual Council.

DVB Blue Book A011, 1996. Digital Video Broadcasting (DVB)—DVB Common Scrambling Distribution Algorithm. DVB Project.

EIA 679-B, 1999. National Renewable Security Standard (NRSS) Part B. Electronic Industries Association.

ETSI ETR 289, 1996. Digital Video Broadcasting (DVB)—Support for Use of Scrambling and Conditional Access (CA) within Digital Broadcasting Systems. DVB Project.

Giachetti, J.L., Lenoir, V., Codet, A., Cutts D., Sager, J., 1995. A common conditional access interface for digital video broadcasting decoders. *IEEE Trans. Consum. Elec.*, **41**(3):836-841. [doi:10.1109/30.468076]

ISO/IEC 7816-3, 1997. Information Technology—Identification Cards—Integrated Circuit(s) Cards with Contacts, Part 3: Electronic Signals and Transmission Protocols. International Organization for Standardization.

ISO/IEC 7816-4, 1997. Information Technology—Identification Cards—Integrated Circuit(s) Cards with Contacts, Part 4: Interindustry Commands for Interchange. International Organization for Standardization.

ISO/IEC 8825-1, 2002. Information Technology—ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). International Organization for Standardization.

ISO/IEC 13818, 1996~2004. Information Technology—Generic Coding of Moving Pictures and Associated Audio Information. International Organization for Standardization.

ISO/IEC 14496, 2001~2005. Information Technology—Coding of Audio-Visual Objects. International Organization for Standardization.

Kamperman, F., Rijnsoever, B.V., 2001. Conditional access system interoperability through software downloading. *IEEE Trans. Consum. Elec.*, **47**(1):47-64. [doi:10.1109/30.920419]

Macq, B.M., Quisquarter, J.J., 1995. Cryptology for digital TV broadcasting. *IEEE Proc.*, **83**(6):944-957. [doi:10.1109/5.387094]

Mooij, W.G.P., 1994. Conditional Access Systems for Digital Television. Int'l. Broadcasting Convention'94, p.489-491.

PCMCIA, 2001. PC Card Standard Release 8.0. Personal Computer Memory Card International Association (PCMCIA).

Reimers, U., 2001. Digital Video Broadcasting (DVB)—The International Standard for Digital Television. Springer-Verlag, Berlin.

Song, W.J., Kim, W.H., Kim, B.G., Kang, M.H., Choi, M., 2003. Contents protection system using smart card interface for digital CATV network based on the OpenCable specification. *IEEE Trans. Consum. Elec.*, **49**(3):693-702. [doi:10.1109/TCE.2003.1233806]

Stinson, D.R., 2002. Cryptography Theory and Practice, 2nd Ed. CRC Press, New York.

Whitaker, J., 2001. DTV Handbook: The Revolution in Digital Video, 3rd Ed. McGraw-Hill, New York.

Xie, Q., Zheng, S.B., Yu, X.J., 2005. A smart-card-based conditional access subsystem separation scheme for digital TV broadcasting. *IEEE Trans. Consum. Elec.*, **51**(3):925-932. [doi:10.1109/TCE.2005.1510505]

Zheng, M., Zheng, S.B., 2004. A common smart-card-based conditional access system for digital set-top box. *IEEE Trans. Consum. Elec.*, **50**(2):601-605. [doi:10.1109/TCE.2004.1309434]