

OMNICRYPT 200 Conditional Access System

1 OmniCrypt CAS Summary

1.1 Introduction

OMNICRYPT CAS is a high-security conditional access system. It has been used in more than 200 projects with over 5 million subscribers in 60 countries.

OMNICRYPT CAS has many secure techniques including high-security chipset solution, multi-layer keys, independent developed encryption algorithm, EAL 5+ level smart card and so on. It has obtained the class A certificate and is recommended by State Administration of Radio Film and Television (SARFT).

OMNICRYPT CAS can support DVB simulcrypt standard and lots of functions, such as PPV, IPPV, VOD, PUSH VOD, prepaid, multi-TV, region control, STB paring etc. It can provide a secure, stable, powerful, flexible and standard compatible conditional access system and billing solution for digital TV operators.

OMNICRYPT CAS includes:

Principal module:

- System Core Module (CAS)

Optional modules:

- Subscriber Management Module (SMS)
- Program Management Module (PMS)
- Short Message Payment Module (TVM)
- Bi-directional Enhanced Module (BCA)
- Pre-Encryption Module (PRCA)

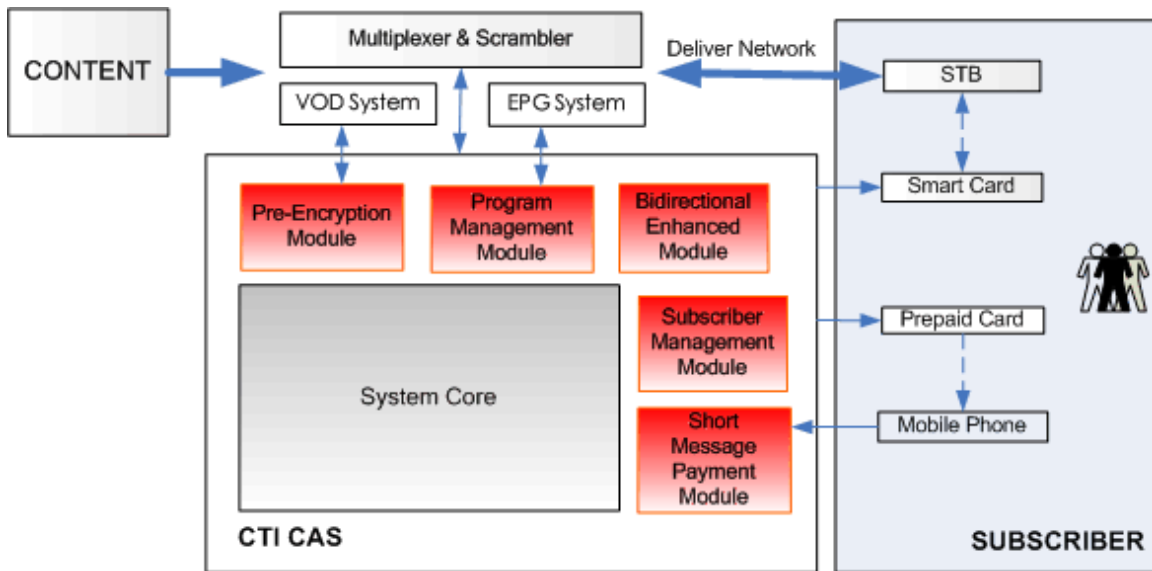


Chart 4-1-1 OMNICRYPT_CAS Architecture

The TVM module and PMS module can be considered for advanced functions such as prepaid or IPPV. If there is VOD or PVR application, the PRCA module will be needed. Moreover, the BCA module can protect the important message in the bidirectional network.

1.2 Components

System Core Module (CAS): It is the basic module of OMNICRYPT CAS including ECMG, EMMG, EIS and database which provides the normal functions such as register, entitlement, Bmail etc. System core is comprised by three parts: headend system, STB core, and smart card.

Subscriber Management Module (SMS): the processing, the maintenance and the management of the subscriber information, subscribers' equipments information, programs ordering information, subscribers' authorization information, and financial information, providing meanwhile the basic data of subscribers' authorization management for the other subsystem.

Program Management Module (PMS): As database application software, PMS links efficiently the description of digital TV operation (service), the description of digital TV program information (event), the scrambling control of digital TV and the definition of digital TV products, providing control data and management data for the function of CAS. In cooperation with the other systems, PMS helps to form one integrated operation process including: program scheme (program guide and management), control and management of authorization (conditional access) and charge management.

Short Message Payment Module (TVM): providing for the broadcasting operators a multitude of value-added services such as: charging by short message, balance query, product order, transition, customer complaints and service help through the short message gateway and short message server to transfer the short messages.

Bi-directional Enhanced Module (BCA): based on the function of the CAS core module, using the secure bidirectional information returning channel, the PKI technology and digital sign, digital certificate to improve the confidentiality, authentication and incontestableness and to provide for the operator a more reliable manner to ensure the security of online alternative operation such as: VOD, online game, puzzles and purchase etc.

Pre-Encryption Module (PRCA): The pre-encryption system scrambles the video and audio streaming files and multiplexes the key with the encrypted video and audio streams together. The STB must be online to receive authorization for watching. It is used for VOD, PUSH VOD, PVR applications.

1.3 OMNICRYPT CAS Features

- DVB Standard

OMNICRYPT CAS complies with DVB Simulcrypt standard. The CAT, ECM, EMM are supported and some interface is open to other DTV system. It could be integrated with all kinds of DVB products, including scrambler, SMS, STB, CAS, Middleware etc.

- Security

There are many advanced technique, such as multi-level encryption, self-developed

algorithm, operation system in card, EAL 5+ level smart card, security chipset for STB, etc.

- **High-Security Chipset Solution**

It is the newest secure method for client devices that prevents control word redistribution (CWR) and device software tempering. There is a secure channel between smart card and descrambling chipset where the CW is encrypted. Every chipset has a unique identifier and the public/private keys system protects the software in the STB's memory.

- **Multi TV**

The master / subsidiary cards are applied for multi TV and STB in home. Then the operator could provide different prices for the second or third STB in a family.

- **Region Control / Pairing of card and STB**

These functions can help the operator to manage subscribers in different regions.

- **EIS / PMS**

The EIS / PMS can exchange the event information with EPG system, and provide event database for ECM generator or other systems.

- **PPV / IPPV-T**

OMNICRYPT CAS supports OPPC, OPPV, and IPPV. Moreover, we created IPPV-T function by which subscribers can watch the unordered channel and pay by time.

- **Prepaid by mobile message**

OMNICRYPT CAS can support TV message system, which could send and receive short message with mobile phone. Then, operators can sale prepaid cards at shops or supermarkets, the subscriber can buy it and charge or order product via short message of handset.

- **Pre-Encrypt for VOD**

The Pre-Encryption is a new function for video on demand service. The program file could be encrypted and saved in the storage array of the VOD system. It could only be watched online and could not play without authorization.

- **Audience Statistics (rating)**

In bidirectional network, the STB could provide statistics information. So it will be easy to know the most popular program and the golden period in various channels for

advertisement.

- Redundant

The important servers in the system have hot-backup. The database could be updated to backup server automatically. So if there is any critical error, the system could be restored in short time.

- Local Program Insertion

If there are several local programs in the sub headend, these programs could be scrambled by the local scrambler or multiplexer or IPQAM device. Some important messages such as ECM / EMM can be transmitted between the CAS at main headend and the scramblers at sub headend by the VPN network.

2 System Core Module (CAS)

2.1 System Summary

The system core module (CAS) is a high-security DVB Simulcrypt conditional access system that supports DVB common scrambling equipments. It uses several standard encryption algorithms, OmniCrypt encryption algorithm and multi-layers encryption system. Moreover, it can support the high-security chipset solution and EAL5+ smart card.

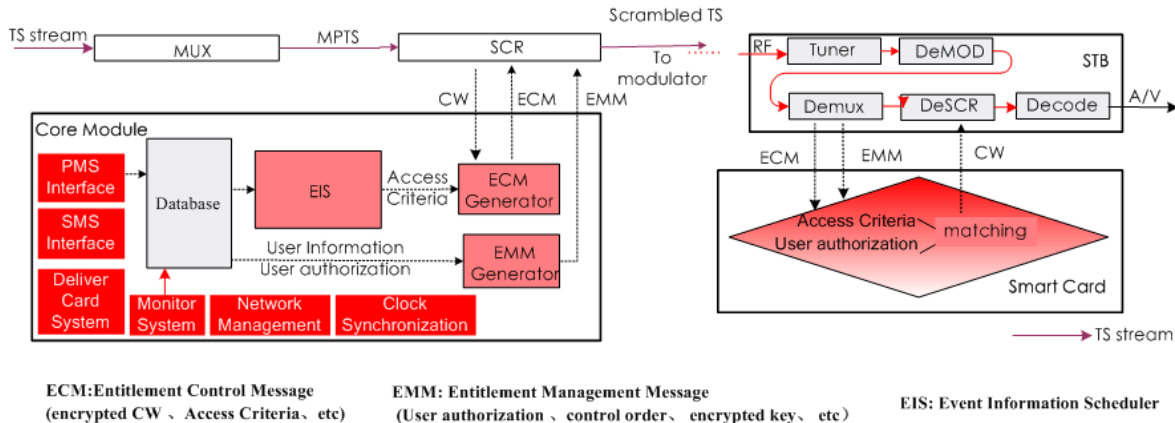


Chart 4-2-1 CA system core module structure

The system core module of OMNICRYPT_CAS is constituted of head end system, CA core software, smart card system.

- **Headend system**

It takes charge of scrambling control of digital video and audio programs by hardware and CAS software.

- **CA core software**

It is integrated on the chipset of certified STBs which get control word (CW) from smart card and descramble the TS stream.

- **Smart card system**

It includes smart card and distribution system. The smart card is different for every

subscriber of different TV network.

2.2 Main Functions

- The registration of new subscribers

The registration of new subscribers requires registering the basic information of the customers, such as the user name, address, contacting number, number of smart card, card address information and ordered product information etc. After registered successfully in the SMS module, the customer information will be transferred from the interface between SMS and CAS to CAS system, of which is partly broadcasted by CAS to the customer's smart card.

- suspending, resuming and cancellation of the subscribers

The operator can chose to suspend, resume or cancel the service which the subscribers have ordered according to their needs. The subscribers will not be able to watch the scrambled program after the operator suspends the authorization. If the subscriber is canceled, the smart card will not be available.

- Emergency authorization

The emergency authorization function is set for sending rapidly the authorization to the subscribers. The CAS system sends rapidly in a certain period the authorization information to the subscribers who can immediately receive the ordered program on the STB.

- Pre-authorize of program channel

The subscribers can reserve the program by the pre-authorization function of CAS. And the authorization will be invaluable after the program ends.

- Cancellation of the channel authorization

The reservation could be cancelled according to the demand of the subscribers. And

relevant scrambled channels will not be able to be watched after the annulment.

- OSD sending

CAS supports the information sending. The long text can be broadcasted as MAIL to the subscribers' STB and then be read on the TV. The subscribers can also receive the short message of the operators as OSD on the TV screen. The direct, convenient and non-traditional OSD mode saves largely the human and material resource.

- Multilevel CA technology

OMNICRYPT_CAS supports multilevel management by using one CA system. The chief authorization center is set in the main district where the unique CAS is installed. Every divisional district has its own SMS by which the SMS information is transferred to the authorization center of the main district. The authorization information is sent together by the center so that the authorization for the divisional districts is controlled by the main district as well as the divisional districts hold the right to the management of its own subscribers.

- Algorithm admitted by National Commercial code committee

The **OMNICRYPT_CAS** has complied with multi encrypt algorithm, such as: DES, 3 levels DES and **OMNICRYPT** developed independently algorithm which is admitted by National Commercial code committee.

- National Commercial code committee pointing manufacturer

The **OMNICRYPT** is on the examination for the pointing manufacture by National Commercial code committee.

- Mother and seed card control

To satisfy the needs of different favors for TV programs of family members, the powerful and flexible **OMNICRYPT_CAS** provides the function of mother and seed card control to ensure that the subscribers watch their favorite programs on different STB at the same times. Several smart cards can be distributed to one subscriber, one of which is mother card and the others are seed cards. The main difference between mother card and

seed card is that the available period of the seed card is limited. The duration can be configured according with the need of the operators from 1 min to 40 days. To receive normally the scrambled programs, the seed card should acquire the authorization from the mother card STB. During the operation, the property of mother card and seed card can be exchanged by sending EMM authorization information. However one mother card should be guaranteed.

- **Sharing group authorization**

The OMNICRYPT_CAS supports various addressing function, including personal addressing, sharing address and group addressing, and logistic addressing, by which the operators can configure different audience property, can authorize totally the subscribers group who have special connection and can sending information in best times.

- **PPV / IPPV / IPPV-T**

The OMNICRYPT_CAS provides various program ordering modes: PPV, IPPV, IPPV-T etc which the subscribers can self determinate. This function needs PMS module.

- **User card charge**

The OMNICRYPT_CAS provides user card charging function. The subscribers can charge in the operating hall and the charging information will be recorded by SMS and write to smart card by EMM. The short message charging is also supported.

- **Smart card deleting**

The smart card deleting function helps to protect the operators' profit and controls effectively the distribution of pirate cards. The operators can delete simply the number of smart card pirated to prevent unallowed subscribers from watching scrambled programs.

- **District control**

The OMNICRYPT_CAS can send different district codes to STB in different districts corresponding. Meanwhile the district codes will also be written into the smart card according with the subscribers' addresses. To watch normally the TV program, the district code in the smart card should match to the one sent by the system. The function enhances

the flexibility of selling strategy and ensures the security for the operators. The STB should bind with the smart card to prevent the circulation of smart card in current district.

- Machine and card match

The STB should bind with the smart card which means one STB supports only the matching smart card, protecting effectively the operators' profits.

- Key updating

On account of the periodic CW updating for 5 seconds to 10 seconds, the OMNICRYPT_CAS is able to keep high security. All keys update termly by sending renewed EMM information.

- Encryption algorithm selection

The common encryption algorithms, including DES and 3DES, and special OMNICRYPT encryption algorithm are used to ensure the high security of data and CAS.

- Anti- recording tag

The permission of program recording can be admitted or forbidden by configuring the transferring programs.

- Finger print technology

The electronic finger print technology of the CAS protects the copyright of valuable programs. The finger print information is stuck to the protected programs for copyright tracking to protect the operators' profits.

- Parents level control

The OMNICRYPT_CAS can set level limited information for broadcasting programs to allow the subscribers to use password for different level programs depending on family members' situation which prevent the minors from watching inappropriate programs.

- TVM interface

The TVM module is one of the most important extended modules of CAS, which

supports account querying, charging, purchasing and annulling operations by sending messages.

- Card number control

The card numbers can be updated by CAS while the operation is extending. The subscribers will not be able to watch normally the scrambled programs if their cards are not updated. This function protects effectively the operators' profits.

- Obligated programs switching

The programs switching function can oblige the subscribers to change to the special channel which broadcasts important information as earthquake, flood or international affairs etc.

- TV watching period control

The subscriber can set the watching time on the STB according with his own need. This function enhances the controllability to the programs of the subscribers.

- Redundancy system

The redundancy system contains two parts, one of which is for the application program backup of CAS by using special software which ensures that one of the servers will keep corresponding to the accessing and that the application program of CAS works uninterruptedly. The other part takes charge of the backup for database. Once the fault is detected, the accessing will be switched automatically to the backup database server to ensure the security of the data in the server.

2.3 Highlights

- Complying with DVB simulcrypt standard
- The first CAS provider in China
- Technique criterion and structure complying with relevant international and national standard
- Supporting scrambling and encryption technology integrating

- DVB-CA and IP-CA technology experiences
- Firstly simulcrypt with other CAS in China
- Integrated with a lot of scrambling products in the world
- Lots of application cases of CAS in cable, satellite and IP Ethernet environment, plenty of experiences on the construction of CAS and digital TV platform.
- Complying with international and national relevant standards
- Supporting over 10 million subscribers and 2048 services
- Great working efficiency, capable to authorize rapidly even on the condition of small bandwidth
- Strict anti-hacks security technique to protect the operators' profits
- Multi technologies as: smart card technique, security algorithms and CW loop encryption etc to ensure normal receiving of legal subscribers and to prevent the illegal receiving
- The subscribers' authorization information and programs accessing information are always encrypted to transit to prevent the illegal monitoring.
- Machine and card matching function allows unique card to work on one STB.
- Valuable period for authorization information to prevent the subscribers from receiving programs over the valuable authorization duration
- Developed independently COS smart card to guarantee the security
- Standard system structure convenient for updating
- Supporting redundancy system to ensure the resuming of system from serious errors
- Supporting distributed system structure
- Supporting multi-SMS
- Remote system management tool to help detecting the situation of system and each component
- Satisfying bidirectional mutual functions
- Supporting lots of programs packing and selling modes, including products selling, PPV, VOD etc.
- Flexible price modes which allows to sell one program in different product packs
- Several addressing function, including: individual addressing, group addressing and

logistic addressing

- Districts control or other control modes according to addressing manner
- Data information displaying function as B_MAIL and OSD
- Supporting mutual and data operations
- Supporting OPPV selling in manner of event
- Supporting IPPV, IPPV-T
- Supporting broadcasting in turn mode NVOD operation
- Supporting Cable Modem back transmission mode
- Supporting a lot of scrambling equipments, SMS and STB to provide more choices for the operators
- Complying with DVB Common Scrambling algorithm
- Multi-levels key for protecting the transmission of ECM and EMM information
- Sending information in the air periodically to change the subscribers' multi-levels key, conversation key or authorization information in order to strengthen the capability of anti-attack
- Based on Ethernet head end system developing, flexible use and configuration in the Ethernet environment
- Parents levels control: capable for parents to set password for programs accessing control
- Anti-recording: anti-recording tag to control programs recording by receiving equipment
- STB programs downloading or smart cards encryption algorithms downloading: downloading application programs to STB or smart card to change the function of receiving and control
- supporting obliged channels switching
- supporting watching period control
- Providing TVM platform interface

2.4 Headend System

The headend system includes OmniLynx CAS software and third party devices such as PC servers, workstations, network switchers, KVM, smart card readers etc.

Here are the OmniLynx CAS softwares below.

- ECMG
- EMMG
- EIS
- Clock synchronization processing
- License control
- AC_EDIT
- SI processing
- Encryption control system
- CAS control commands editing
- PMS interface
- SMS Interface
- CAS Event Interface System
- CAS Cache Monitor System
- Database management system
- Network Management System

2.5 CA core software

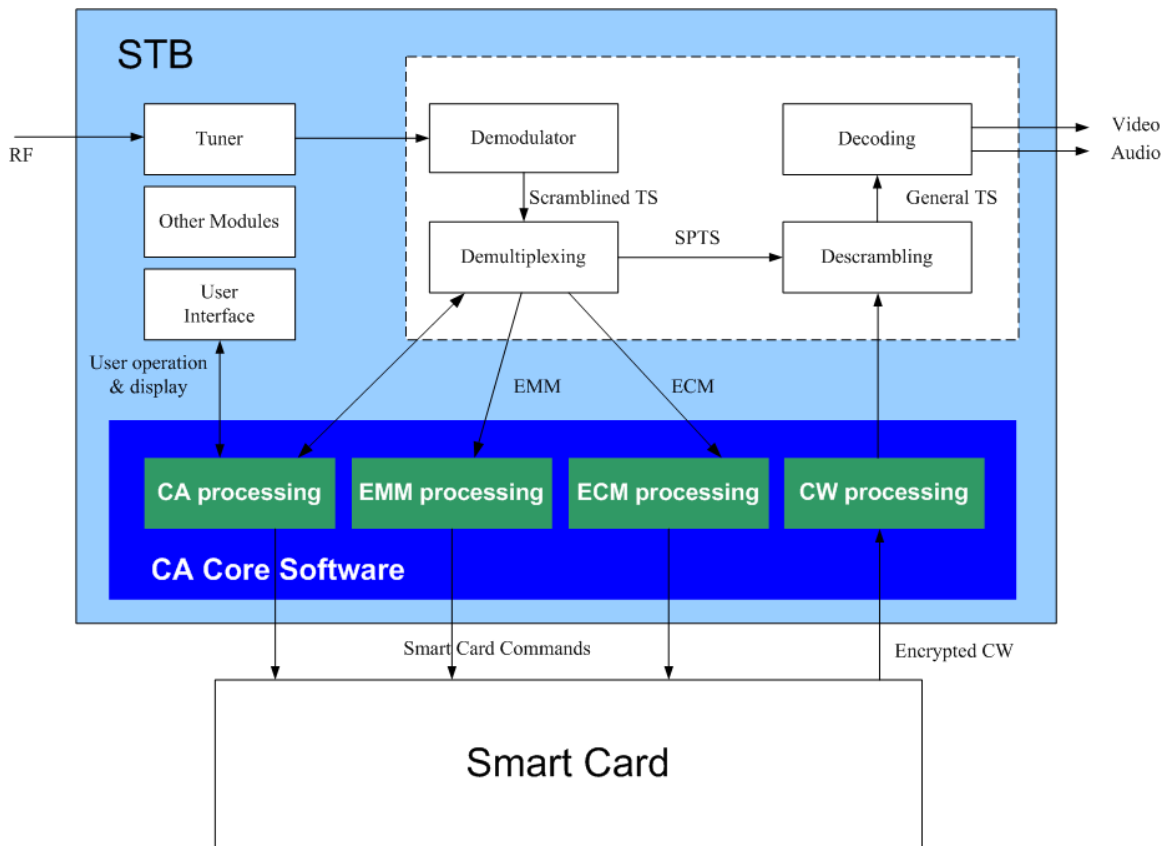


Chart 4-2-2 CA core software

STB receives scrambled TS and filters out the ECM and EMM information, then sends it to smart card by means of the CA core software. There are special regulars and commands between the STB and the smart card that is already integrated inside the CA core software.

After receiving the ECM, EMM information, by interrelated processing, the smart card will write the authorization information into the subscribers' authorization data area, and unscrambles CW in accordance with the authorization condition and pointing key, and send it to STB. Then STB will pass CW to descramblers. The program can be normally watched only if the descrambling CW is correct. If the high-security chipset is used in STB, the CW will only appear inside the chipset.

The CA Core software system receives and processes ECM, EMM information sent by CAS, obtains descrambling CW and sends it to descramblers. It provides meanwhile the additional information related to CAS for receiving devices for displaying.

2.6 Smart Card System



Chart 4-2-3 OMNICRYPT Smart Card

2.6.1 Smart Card

The smart card contains hardware and software. The hardware is a smart chipset on a plastic card. The software is the card operating system (COS) and private applications developed by OMNICRYPT.

Several smart cards are used in CAS, including: system mother card, system control card, system key card, terminal users' cards. The system mother card is system total control card which takes responsibility of generating other card and provides basic data. System control card is used to control the license right and relevant basic parameters of each module. The system key card is startup key for all types of cards to ensure the validity of card uses. Terminal users' card which is for uses of the subscribers, can provide authorization of televuew for them and make sure that the legal subscribers watch normally the paying programs.

The smart card, which is a plastic card, has an embedded IC chip containing CPU and

ROM, EPROM, RAM EEPROM. This embedded chip, which maintains hardware and software protecting and secrecy processing technique, connects externally through asynchronism bus interfaces and uses CPU for serial I/O link control. To prevent effectively the illegal attacks, the memorizer embedded in the chip can not be accessed externally. The main features are as the following:

- Storage capacity: its internal storage capacity from a few dozen to a few dozen bytes K bytes
- Complicated security algorithms: hardware supporting symmetrical DES accelerated algorithms, maximally supporting 2 random data generator, capable for high level self encryption function.
- High level security: special hardware logistic design for encrypted IC card, the configurations of reading and writing feature in several areas of IC card are controllable, which is to ensure unchangeableness of the information in IC before the password is checked. The IC will lock automatically to prevent the writing operation if the password is wrong. The matching of entering password and system setting password is obligatory for system accessing. At present, OMNICRYPT smart card has obtained EAL5+ certificate.
- High reliability: IC card Magnetically-shielded, anti-static, anti-interference capability and more reliable than magnetic card. Information can be read and written 10-500,000 times, use time from 10 to 100 years.
- Low requirement for network: the absolute security reliability of IC card allows the lower demand for real-time and sensitivity of network during the application which enable to apply the system in lower network environment.
- The reading and writing structure of IC card is simpler, more reliable, cheaper, and easier for extending than magnetic card. Simple maintenance.



BSI-DSZ-CC-0340-2005
Infineon Smart Card IC (Security Controller)
SLE66C168PE/m1530-a25,
SLE66C84PE/m1538-a25,
SLE66C44PE/m1539-a25 and
SLE66C24PE/m1563-a25
with specific IC Dedicated Software
from
Infineon Technologies AG



The IT products identified in this certificate have been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Part 1 Version 0.6, Part 2 Version 1.0* extended by advice of the Certification Body for components beyond EAL4 and smart card specific guidance for conformance to the *Common Criteria for IT Security Evaluation, Version 2.1 (ISO/IEC 15408:1999)* and including final Interpretations for compliance with Common Criteria Version 2.2 and Common Methodology Part 2, Version 2.2.

Evaluation Results:

PP Conformance: Protection Profile **BSI-PP-0002-2001**
Functionality: **BSI-PP-0002-2001 conformant plus product specific extensions**
Common Criteria Part 2 extended
Assurance Package: **Common Criteria Part 3 conformant**
EAL5 augmented by:
ALC_DVS.2 (Life cycle support - Sufficiency of security measures),
AVA_MSU.3 (Vulnerability assessment - Analysis and testing for Insecure states),
AVA_VLA.4 (Vulnerability assessment - Highly resistant)

This certificate applies only to the specific version and release of the products in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 30. September 2005
The President of the Federal Office
for Information Security



Dr. Helmbrecht

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 • D-53175 Bonn • Postfach 20 03 63 • D-53133 Bonn
Phone +49 228 9582-0 • Fax +49 228 9582-455 • Infoline +49 228 9582-111

Chart 4-2-3 EAL5+ level certificate for smart card

2.6.4 Distribution System

OMNICRYPT smart card distribution and management system is specially designed for pay-TV and digital broadcasting. The special layered smart card distribution and management is designed according to CAS operations regulars and to ensure the security of pay-TV. Based on different levels and different uses, the smart cards will be divided into the mother cards, key cards, system control cards, terminals users' cards etc. The data structure and application programs are different. The whole distribution and management is divided into several layers including: mother cards distribution and management, system control cards distribution and management, users' cards distribution and management. The smart cards of each layer manage and restrict the distribution work of next layer. At the same time, the improved key generation system, mature encryption algorithm and smart card matching to key card technique can be fully verified to ensure the security of each layer.

3 SMS module

3.1 System Summary

OMNICRYPT_CAS SMS module is an integrative operation management platform by which the operators can provide multi-services to the subscribers. It can send authorization data to CAS according with the ordering situation of subscribers and charge meanwhile. Utilizing the bank network characteristic as secrecy, security and rapid fund circulation etc, it can implement the charging function by cooperating with bank system and monitor and analysis function through the interface with bank system.

As the pioneer SMS developed independently in China, **OMNICRYPT_CAS** SMS module already has mature system structure and product module, complies with EUROCRYPT standard made by European Electronic Standards Committee and all the standard made by State Admission of Radio, Film and Television.

3.2 Main Features

- Managing subscribers' information about paying, recharging, installation, change (returning) IC card/STB/service etc
- Sending authorization data to CAS according with subscribers' ordering, paying situation
- Managing automatic bank recharging, charging by card
- Surveying, querying function (which provides effective ways for report form statistic, analysis forecast, finance management etc)

3.3 System Characteristic

- Supporting multi-levels system management, router exchanging technology for multi-layers network
- Adapting to the complex condition of required network

- Based on large-scale network database system, constituting client/server or web/server network structure
- Running on various databases platforms as Oracle, Sybase, and SQL Sever etc

3.4 System Structure

According with the different management function, SMS module is divided into five standard modules and three selectable modules. 5 standard modules are general management module, querying management module, control management module and statistic report forms management module (gift); 3 selectable modules are bank management module, charging card management module and short message management module.

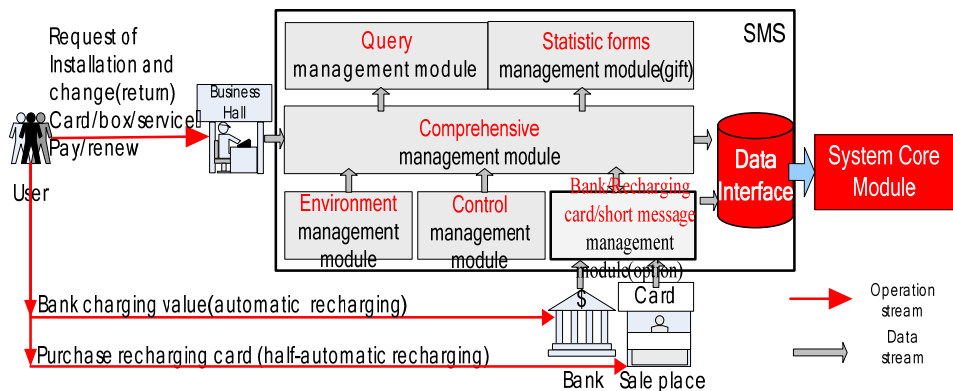


Chart 4-3-1 SMS system structure

4.4.1 General Management Module

The general management module possesses the functions as subscribers paying and recharging, programs ordering/canceling, service suspending / resuming, returning / changing STB and IC card (the model of invoice can be modified according with customers' needs in different areas).

4.4.2 Environment Management Module

Environment management module manages mainly the basics data for management

system running, as area codes, products information, departments, personnel, function authorizing, operating password and operating rights etc.

4.4.3 Control Management Module

Control management module is mainly for the management of system running environment, subscribers' serial numbers generating regular, products selling regular and time displaying modes etc.

4.4.4 Querying Management Module

This module supports various convenient querying manner and combines with operating right to provide advantaged supporting to concentrated database and multi-levels management.

4.4.5 Statistic Report Form Management Module

Statistic report forma management module supports diverse report forms/figures (subscribers' distribution, subscribers reserving/canceling details, subscribers' card/STB time information etc). The report form and figure can be designed according with users' demands. It contains business report forms of each time period, subscribers' information report forms, subscribers' ordering collecting forms and relevant figures in order to reflect directly the diverse system parameters and operating management status of programs providers.

4.4.6 Bank Management Module

Using fully the bank system technology and the effective, exact and safe devices, bank management module controls charging, credit and profits distribution.

The subscriber signs contract with the programs providers to reserve some or all the channels and audience time which is minimally by month. The programs provider informs the bank monthly to transit the fund from the subscriber's account to its own account and sends programs authorization to allow the subscriber to receiving programs.

4.4.7 Charging Card Management Module

This module supports charging account by charging card, provides a simple paying mode for the subscribers.

4.4.8 Short Message Management interface

Short message management interface connects with short message payment module (TVM) of OMNICRYPT-CAS. The subscribers can query account, charging and ordering products by sending short message. The interface between the short message management module and short message payment module processes the subscribers' information and stores it to the database of SMS module.

4 Short Message Payment Module

4.1 System Summary

Short message payment module, namely TVM platform, provides short message center for TV station and Network Company. By the short message transferring through short message gateway and server, it provides diverse value-added businesses for the broadcasting TV operators as short message charging, short message querying, products ordering, fund transition, services complaints and services helps etc.

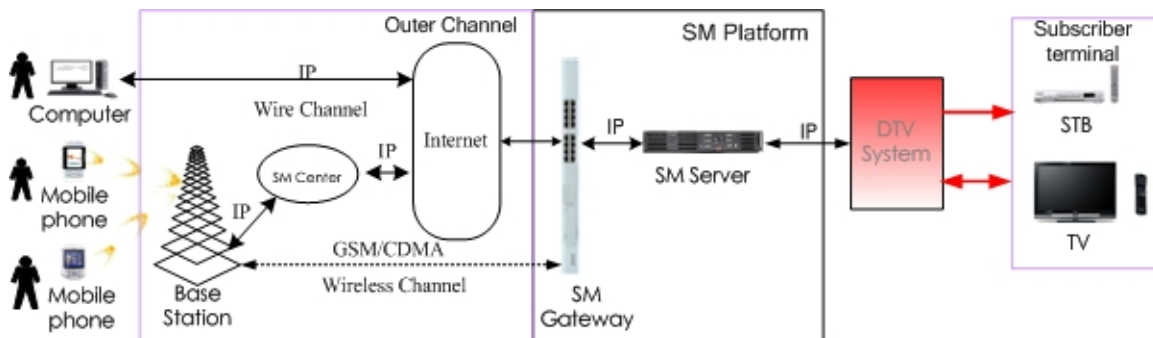


Chart 3-4-1 Short Message Payment Module System Structure

4.2 Main Features

- Supporting remote charging function for digital TV account by mobiles
- Supporting balance querying, products ordering and fund transition etc
- Supporting diverse value-added services

4.3 System Characteristic

- Modularization design, supporting flexibly various head end system, terminals, mobile operators, value-added operator and diverse new services
- Supporting OMNICYPT_CAS core module and bidirectional enhanced module, supporting common STB and bidirectional STB
- Flexible, improved billing system and working process, supporting various billing and sharing profits modes
- Short message server provides database and HTTP services, stores all the information, supports clients browsing
- GSM/CDMA modem supports several local SIM card and supports also the TV users to query account by short message.

4.4 System Structure

Short message payment module is mainly composed by short message gate way, WEB server, database server, network management working station and GSM/CDMA modem.

- Short message gateway: connecting with network, being able to receive and transfer mobile short message. Connecting external with a Wi-Fi modem which has 8 interfaces for 8 SIM card. The short message sent by mobile phone is analyzed according to certain regulars for later balance querying and account charging functions. The environment for short message gateway is Windows 2003 server linking externally with GSM modem.
- WEB server: WEB server is a standard website server which provides to the

operators the functions as registering, logging, editing, sending, browsing, deleting, responding message etc by programs in background. The site has background management enter. The administrator can change system parameters or charging, deleting users, monitoring short message content etc. The running environment for WEB server is IIS 5.0/Windows 2003 Server.

- Database server: short message and subscribers' information is normally stored in database server for surveying and querying etc and also for the management of subscribers' account and right. The database server links effectively short message gateway, WEB server, terminals, CAS and SMS. Its running environment is Oracle 10g and Window 2003 Server.
- Network management work station: the configuration and management of subscribers billing/registering, database and gateway; accessing to short message server to examine stored information. Its main work is system background management and monitoring. The management work station, which does not have to run 24h/24h, could help the operators for various remote services, as opening an account, charging, querying etc. Its running environment is the network.
- GSM/CDMA Modem: capable for several local SIM card, responding the communication with outside

5 Technical Parameters

5.1 Head End Technical Parameters

- Maximal subscribers: over 10,000,000
- Maximal scrambling programs: 2048
- Maximal controllable class number: 256
- Maximal controllable PPV/IPPV programs number: 65535
- EMM processing and sending speed: 100-1500 packet/sec
- EMM sending authorization according to sharing address: 256 subscribers/packet
- Maximal programs providers number: 8
- Maximal TS supported: 1 ECMG for 20 TS (ECMS is expandable)
- Maximal products number: 2048
- CW changing frequency: 5-10 seconds once
- ECM bandwidth: 3k-7.5kbps (2-5 ECM packet per second for one channel)
- EMM bandwidth: 0.15-2.2Mbps

5.2 Smart Card Parameters

- CPU: enhanced 8 bit CPU with extended address mode
- RAM: 4 k bytes ; ROM:126 k bytes ; EEPROM:34 k bytes
- Communication interface: ISO 7816-1/2/3 standard
- Security protecting: memory firewall, EEPROM protecting
- Security: EAL5+
- Encryption algorithm: DES, Triple DES, OMNICRYPT algorithm etc
- Maximal sectors number: 4, each sector has independent key data, support multi-levels authorization

- Maximal programs providers number: 8
- Maximal scrambling services number: 2048
- Maximal programs category numbers: 256
- Maximal PPV programs number: 256, storing in loop the programs serial number in case of over 256
- Maximal PPV-P programs number: 256, storing in loop the programs serial number in case of over 256
- Maximal PPV-T programs numbers: unlimited, paying by time according to the electronic pocket in card
- Programs preview: counting by scrambling period or scrambling time, controlling the preview time when switching channels
- Channels pre-authorizing: defining pre-authorization for pointing channels, pre-authorization duration from 10 minutes to 454 days, charging from the first time to watch programs
- Maximal electronic pockets: 8