Sumavision CAS (V5.3) Description

Content

1 Introduction

As the entire DVB industry gradually transitions from card-based to cardless-based. Sumavision launched the new generation CAS (V5.3), which is designed to support both card-based and cardless-based scenarios at the same time. It helps operators to evolve from card-based network to cardless-based network smoothly.

Considering the card-based scenario, the product functions/features of CAS (V5.3) are the same with previous CAS product (StreamGuard CAS), so for the following parts, only focuses on the description of cardless CAS functions/features of the new generation CAS (V5.3).

Considering the cardless-based scenario, the terminal which has high security chip inside, and smart card is no longer required. By constantly updating keys and algorithms, with the features of high security chip in terminals, high security level of the system can be achieved.

CAS (V5.3) can be applied to one-way network (satellite/terrestrial, etc.), supporting up to 10 million terminals with security chip inside.

At present, the main manufacturers of security chip are ST, Broadcom, Hisilicon, ALI, Mstar, Montage, etc. The security chips are mainly divided into two types. Type one supports downloadable standard and type two does not support downloadable standard. There are two downloaded standards which are European "ETSI TS 103 162 V1.1.1 (2010-10)" and Chinese "Downloadable conditional Access System technical Specification GY/T 255-2012" (Sumavision is one of the

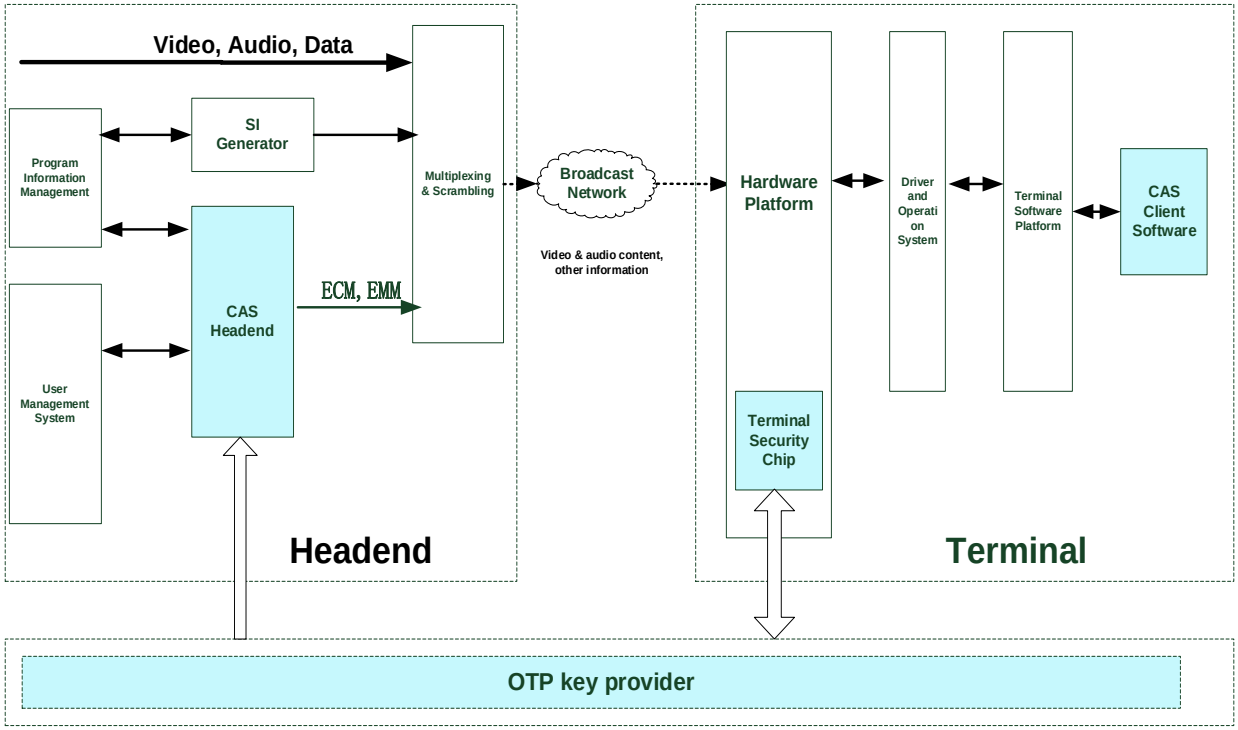
founders of Chinese standard). The two standards are consistent in the core hierarchy of keys. The difference is that Chinese standard is more operational which not only defined the standard of key hierarchy, but also the standard interface of terminal platform. The Chinese standard has refined the developing process, and the replacement verification with world famous CAS companies has already been done.

CAS (V5.3) supports two standards of downloadable high security chip and it also supports common security chips. The common security chips which have been verified are ALI and Montage.

CAS (V5.3) is developed on the basis of traditional CAS with smart card, therefore its operation interface is same as the traditional CAS and easy for the operator to control. CAS (V5.3) cardless function replaces smart card by virtual card, so it has similar external interface as traditional CAS with smart card, and BOSS needs no modification or a little modification to realize the connection. Virtual card is just a registration number of each terminal in the CAS (V5.3), and the terminal can only work by acquiring its registration number. The registration number is generated by the CAS vendor and it will be bound with the terminal number by the BOSS when open an account, then the BOSS will send the information to the CAS (V5.3) to generate the initialization data which is transmitted via one-way network to the terminal to complete the account open operation.

2 System Architecture

The system architecture is shown below.



CAS (V5.3) system is divided into headend system, terminal system and OTP key provider.

- Headend system is provided by CAS manufacturer which is connected to headend devices.
- Terminal system is provided by terminal manufacturer, which embed the 'CAS client software' by integration.
- OTP key provider is responsible to write the keys into the 'terminal security chip', and provide the keys to the CAS headend vendor.

The OTP key provider can be operator, third party, or CAS vendor.

3 Functions

- Open/stop account
- Authorization management
- OSD
- Email
- PIN code protection
- Program level control
- Working time control
- Regional lock
- Conditional broadcasting
- Advanced addressing
- Self-defined addressing
- Free period
- Free preview
- Set operator information
- STB localization control
- Suspend/resume STB
- Fingerprint tracing
- Emergency program broadcast
- Product management
- Simulcrypt
- Auto key cycle, update
- Encryption algorithm update
- Online update for STB software

3.1 Open/Stop Account

3.1.1 Open Account

Before using the terminal, the operator must open an account for it. The purpose of this operation is to initialize the terminal, the result of the operation: assign a number for the terminal in the CAS (V5.3) system, generate EMM information, the terminal receives the EMM, then open account operation is completed.

After open account operation, the terminal can receive further orders.

3.1.2 Stop Account

1. Clear terminal user information, authorization information, etc.
2. If the terminal is stopped, it must be open again to re-use.

3.2 Authorization Management

1. Support authorization and de-authorization for single terminal addressing.
2. Support authorization and de-authorization for all terminal addressing.
3. Supports a single command to clear all the authorizations in one terminal.
4. Supports BOSS query the interface of the authorization for single terminal.

3.3 OSD

CAS (V5.3) can display special words in terminals.

1. Operation method: send some words from CAS head-end system, then display these words on TV when STB receive them.
2. Display: scroll text string on the TV screen from right to left, or pop-up a text box
3. Command object:
   - One specific STB
   - All STBs
   - Under special conditions
4. Command processing: after the completion of the terminal display, the command will be deleted;

3.4 Email

CAS (V5.3) can display some words in terminal, and save these words in terminal.

1. Operation method: after sending some words from CAS headend system, terminal

will show these words.

2. Display: through remote control
3. Command object:
   - One specific STB
   - All STBs
   - Under special conditions
4. Command processing: TV mail can be deleted or kept, same as internet mail.

3.5 PIN Code Protection

PIN code is stored in the terminal, to protect terminal operation safety. The following operations need PIN code:

1) Modify the PIN code

2) Set working hours

3) Program level limit

When user do the operations above, after entering incorrect PIN code for three times, the PIN code will be locked, even if the user re-enter the correct PIN code, the terminal will not respond. CAS (V5.3) supports reset PIN code, which can modify the PIN code to default.

3.6 Program level Control

CAS (V5.3) can set the program level of each product, terminal user can set the watching level of the STB. The STB will prevent user from watching the program if the STB's watching level is lower than the program level. This function is mainly used to prevent children from watching certain adult-level programs. When user modify the watching level of the STB, PIN code will be required for verification.

3.7 Working Time Control

Terminal user can set the working time of the terminal. With this feature user can stop child from watching TV late at night. When user modify the working time of the terminal, PIN code will be required for verification

3.8 Regional Lock

Regional lock can prevent STB from moving among different regions. Operation scenario: there are many regions with different terminal prices, so the operator needs to use regional lock function to ensure the STB work in the appointed region.

3.9 Conditional Broadcasting

Conditional broadcasting can prohibit the eligible terminals from watching some programs, even the terminals have already been authorized.

3.10 Various Advanced Addressing

CAS (V5.3) supports 2 types of addressing. The first one is pre-defined by the CAS vendor while the second one is predefined by the operator. Operator can take the advantage of advanced addressing to enhance not only the utilization of EMM bandwidth significantly, but also the response speed of the CAS command.

3.10.1 Pre-defined Addressing

CAS vendor has pre-defined some addressing conditions to ensure an easy use for the operators, which include the most common situations and can be used by operators directly. The addressing conditions pre-defined by CAS vendor are listed below:

1. Terminal Registration Number
2. Region Code
3. Terminal CA Module Version
4. Terminal SN

5. Terminal Software Version
6. The product is authorized or not
7. The specific operator's product is authorized or not
8. The product which is being watched
9. The DVB TS which is being watched
10. The DVB Service which is being watched
11. The status of PIN code lock
12. The watching level of the terminal
13. The watching level of the TS
14. The start time of working hours
15. The end time of working hours
16. Fingerprint is being displayed or not
17. Card status
18. The present time of CAS
19. Terminal CHIPID
20. The end time of authorization
21. Authorization time

3.10.2 Addressing Conditions Customized by Operator

Operators can define the addressing conditions by themselves if the conditions pre-defined by CAS vendor can't meet their requirements. These conditions can be used after they are written to the terminal through certain interface. Customized conditions can be written in business hall through professional device or broadcasted to terminals via transmission network. 800 bits are reserved in terminal for operators to define the conditions.

3.11 Free Period

Each program type of CAS (V5.3) can be set with a certain start time as the free period.

Operator can decide whether to release preview or not and how long the it is. During free period, all subscribers can watch the programs without any charge.

3.12 Free Preview

During the digital TV promotion period, operators can use free preview to let the subscribers watch programs without any charge. Such measures can stimulate the subscribers to buy programs so that the products can be sold more than normal. Operators can set the property of the programs in the CAS headend, like how many times the subscribers can watch by free preview and how long they can watch without charge each time. Subscribers can watch some certain time of free preview each day if they don't buy this program.

3.13 Set Operator Information

Operators' information can be written into terminals from the CAS headend.

3.14 Terminal Localization Control

Terminal CA module is unique. Only CA module appointed by the local operator can work in the region. Terminals from other operators can't work there.

3.15 Suspend / Resume Terminal

Terminal can be suspended by headend. After that, the terminal can't work even it has been authorized. The terminal can work again after the resume operation.

3.16 Fingerprint Tracing

Operators can use fingerprint tracing to show 'fingerprint information' on TV. This function can help operators trace the origin of the piracy. The time, position, font, color

of the ‘fingerprint information’ can be modified if needed. Fingerprint can be shown by single terminal, all terminals or the terminals which are corresponding to the advanced addressing condition.

3.17 Emergency Program Broadcasting

Operators can force the eligible or all subscribers to watch the same program in case of emergency. Emergency message will also be shown on TV. The condition can be card number in a certain region or scope. Terminals will switch to the appointed channel for emergency broadcasting when the CAS command is received. At this moment, subscribers can’t change to any other program because none of the buttons of remote control can work. Terminal will return to normal after the emergency broadcasting.

3.18 Product Management

CAS (V5.3) provides a Windows GUI to help the operators manage the definition and configuration of all kinds of product.

1. Import product information files: according to the format defined in advance, analyze the XML files provided by the SMS, obtaining program information and product information.
2. Product information query: service as the index to show event information. Event as the index to show product information.
3. Product information query: product as the index to show the corresponding event information.
4. AC generation and analysis: generate the unique AC for each product; analyze the information of an existing AC.

3.19 Simulcrypt

CAS (V5.3) is completely in conformity with DVB simulcrypt standard, and has been

successfully done simulcrypt with many domestic CAS provider (such as TFCAS, CTI CAS, DTVIA CAS, etc.) and many overseas CAS provider (such as Irdeto CAS, based on Irdeto scrambling platform).

3.20 Auto cycle and Update of Keys

Key cycling and update mechanism of CAS (V5.3) is an essential guarantee of system security. The system defines two groups of security keys, each group contain several security keys. For each data package, the headend sending system and terminal receiving system use a specific security key to encrypt and decrypt by protocol dynamically. Meanwhile, the operator can command CAS system to update a specific group of security key, even if the operator has not updated the security key, the CAS system can update the security key automatically in a specific time period.

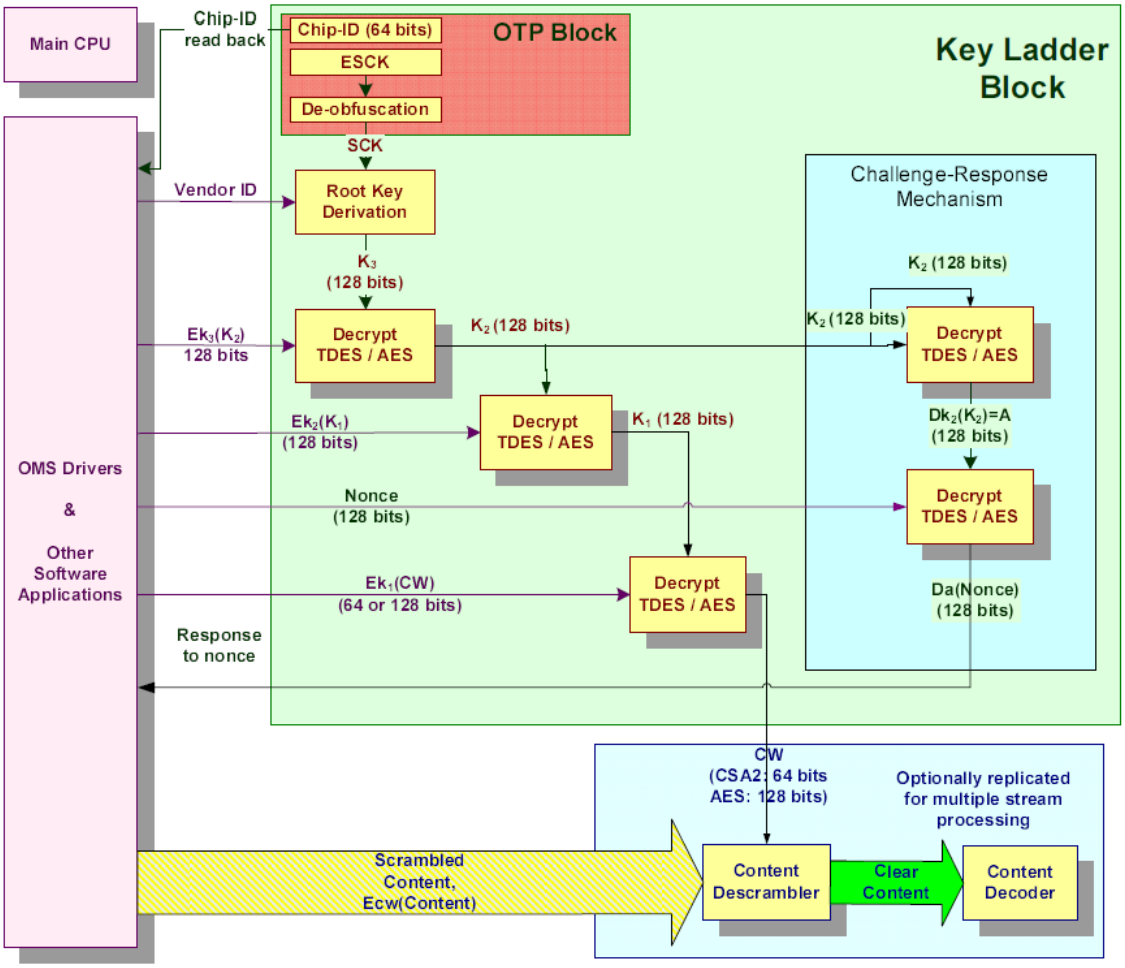
3.21 Updating Encryption Algorithm

CAS (V5.3) supports updating of encryption algorithm, which is another essential guarantee of system security. The updating of encryption algorithm can be conducted by specific device in business hall, and also through transmit network broadcast to terminals.

3.22 Terminal Software Online Updating

CAS (V5.3) supports remote online updating of terminals. When the headend sends updating stream, terminal users can choose update online through terminal menu at home. If updating is failed, there will not be any damage to terminal, user just need to re-update online again. Also, CAS (V5.3) can realize software downloading with different terminal vendors, to update new functions and services.

4 CAS (V5.3) Security



As shown in the figure above, adopts the hierarchy structure of 3-level secret key. Data in OTP Block is written by third party. Input VendorID, SCK to generate K3 of different CAS vendors via Root Key Derivation. When changing CAS, terminal download new CAS software, input new VerdorID and generate new K3. New CAS headend uses new K3, which can guarantee security and smooth replacement.

For security, downloadable CAS requires bi-directional network, every start needs handshake authentication, ensuring the validity of the terminal. After authentication, headend issues authorization to terminals via bi-directional network, and the

terminals are enable to watch the programs. All the authorizations are stored in the headend, so refreshing secret key and algorithm can be both in high efficiency. In this way, the security of downloaded CAS can be well guaranteed. However, in one-way network, authorizations are stored in terminal, which will cause low efficiency of refreshing secret key and algorithm, and will cause security problem. For this issue, Sumavision adopts group addressing mechanism to accelerate refreshing secret key, ensuring the security of terminal.