RSCRYPTO

RSCRYPTO Comments to TRAI Solution Architecture for Technical Interoperable Set Top Box

20th Sep 2017

Levent Le
COO& Co Founder
Levent.Le@rs-crypto.com

Mr. Sunil Kumar Singhal
Advisor (B&CS)
Telecom Authority of India
sksinghal@trai.gov.in
gs.kesarwani@trai.gov.in

Dear Mr. Singhal,

RSCRYPTO, is a CAS company now actively promoting new generation CAS, which supports "Securely Replaceable" feature.

We are pleased that TRAI has been paying attention to interoperability of STB. And here comes the proposed solution architecture via C Dot.

After looking into the paper, we'd comment as below

➢ **Current Framework is based on Smartcard only**

On Page 6 of C Dot framework, it writes "C-DOT framework is based on operator specific detachable smart card approach."

✧ Cardless/software CA Solution shall be considered in the Framework
Cardless CAS solution appeared 6 years ago. Most of the CAS vendors own their own cardless solution. Already Cardless CAS had been proved to be a success with massive deployment, especially suitable for emerging market for cost down.

Already Cardless solution has become an important part of CAS technology. As the wave of more and more DVB networks migrating to Bi-way, Cardless solution shall play a more important role.

Also keep in mind that STB main Chip SOC level security (advanced security) dedicated to certain CAS vendor is a must, so as to prevent control word sharing between Smartcard and STB in this scenario.

If considering from a bigger picture, IPTV CAS STB, OTT DRM STB might need to be involved in this framework.

✧ Smartcard Capacity
"The exponential increase in the smart card processing power, security features & memory capacity (in Smart Card) and decreasing price gives an impetus to the concept of performing Conditional Access (CA) functions totally in Smart Card and also profiling the STB through the Smart Cards as per the service provider specific requirements towards interoperability."

Above statement is very brief without detailed indication what exact workload to be done in Smartcard. It is necessary to engage with Smartcard manufacturers and CAS vendors for further evaluations.

Among most of the technical challenges involved towards STB interoperability, listed in the paper, many of which can be bypassed via specify minimum requirement in future after certain sunrise timing such as MPEG2/4, SD/HD etc, while many of which can be avoided via standardization/downloading such as EPG/UI. However the CAS interoperability/ migration/ replacement never happened in the past. It would be good if the trust authority could play a role to issue root certificate, based on which all CAS vendor will integrate their library into STB.

RSCRYPTO, together with our partner Sypher Media International (SMI)- an independent third party Black Box Key provisioning service provider, are promoting new generation CAS. It enables operators to change the CAS on seeded STB via OTA/IP, without any compromise of the advanced security.

PS：Attached presentation “Replaceable CAS White Paper”

睿 胜 科 技
RScrypto Technology Co. Ltd

RSCRYPTO Replaceable CAS

Technical White Paper

contents

1 Who and Why Need Replace

2 How to Replace

2.1 The Concept of Replaceable CAS

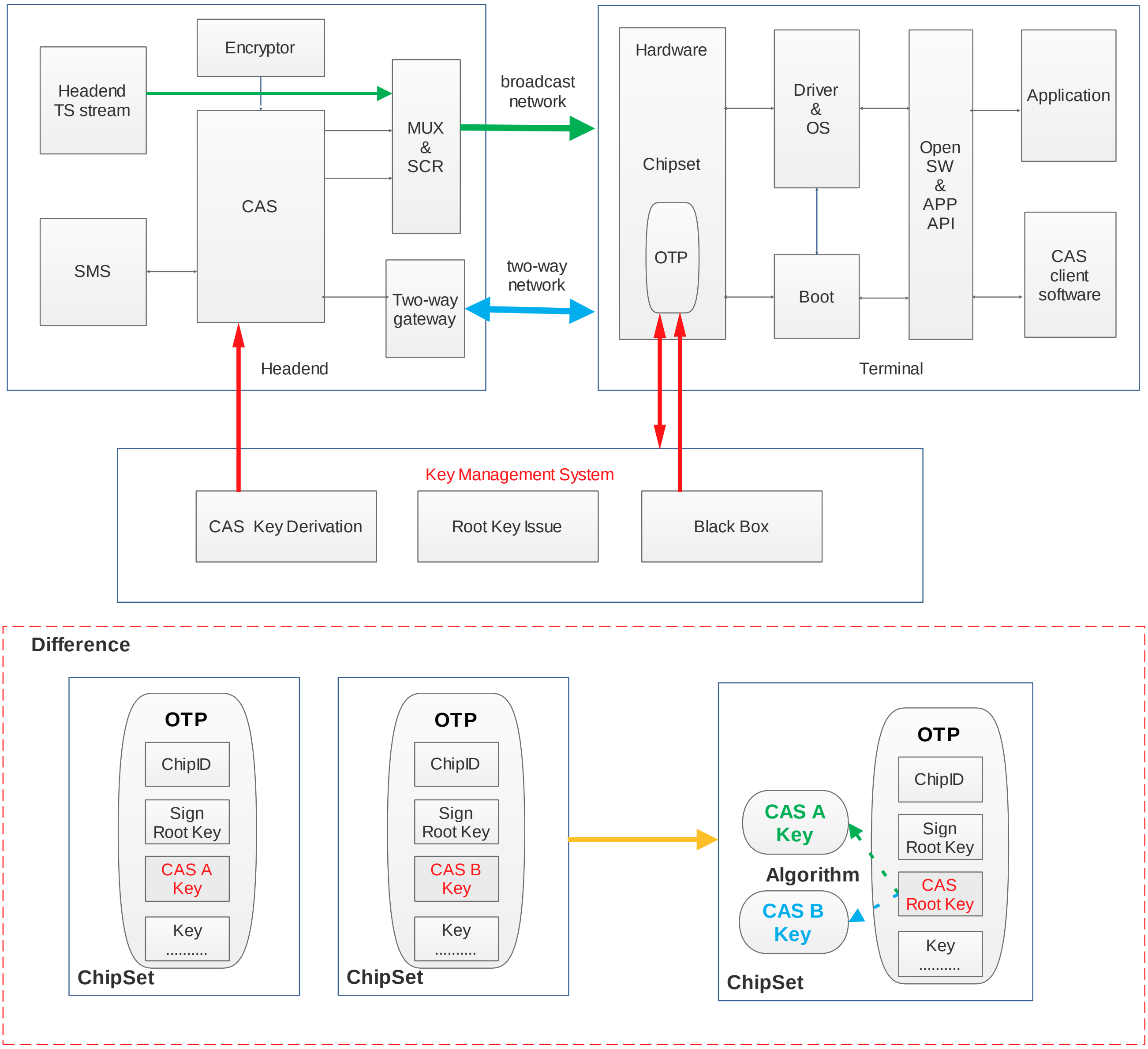
In order to ensure the safety of CAS, the protection means needed mainly include the following: signing the program and data for verification; safety be used of all kinds of secret keys used by the terminal; Setting CW to descrambler by ciphertext. To ensure the safety of the CAS system, all the kind of keys are controlled in CAS vendors own hands, in the meanwhile using a variety of confidential ways to burn them to the OTP area in the chipset. The program's signature and verification process and algorithm are mostly secured by chip manufacturers. Setting CW to descrambler by ciphertext is realized through the chip side support the algorithm.

This causes the CAS secret key to be controlled only by one CAS vendor. Therefore, we put forward a design that separation of the secret key and the CAS system, use a method derive the CAS secret key —every CAS system would derive itself CAS vendor secret key through the root key in the OTP region, instead of publish the secret key to any CAS vendor. The core part separated out is called the key management system. This system will be controlled by the broadcast operator. The operator can provide the derived secret keys to each CAS vendor, thus laying the foundation for CAS system's replaceability.

When operator want replace the terminal from one CAS vendor to another, key management system can derive the corresponding CAS vendor key, then deliver it to the new CAS system. In this way, the CAS client software can use the secret key. Operator sign the application through the standard signature process, and upgrade the user terminal, so the newly replaced CAS system can run on the terminal, to achieve the effect of CAS system replacement.

2.2 Technology Architecture Diagram

The technical principle of replaceability is that unified management the key through the key management platform, control key derivation, publish. Each CAS system could use the derived CAS key from the same root key, Any CAS system can run on the same one terminal through the open terminal software platform and application program interface. So, any CAS system can upgrade and run at any time on the same one terminal.



2.3 Constituent Parts

According to the technical principle, the system consists of three parts: headend CAS system, terminal set-top boxes, and the key management system.

And there are four main objects, respectively is chipset manufacturer, CAS vendor, terminal manufacturer and the broadcast operator.

CAS vendor have control of their own business secret-keys, which are derived and issued by the key management system;

Chipset manufacturer is responsible for burn the secret key in, taking use of security tools provided by the key management system such as the black box to embed the root key in the OTP;

Terminal manufacturer is in charge of providing open software platform and application interface to enable the CAS system to call a variety of interfaces for encryption and decryption;

The key management system issues and manages all secret keys, burned to the OTP area, and issue and derive required CAS keys for different CAS vendor; sign on all the programs running in the terminal.

Regarding the architecture of the system, the key management system has become the secure core for the whole solution, also the core of management and control. Therefore, operators can build server with secure environment by themselves, according to the actual situation to carry out operation and maintenance of the key management system.

Open software platform: the public software module upon terminal hardware and drivers, which has the following functions:

1. Support bootloader, upgraded and replacing of the CAS client software;
2. Provide the required standard application interface for the CAS client software;

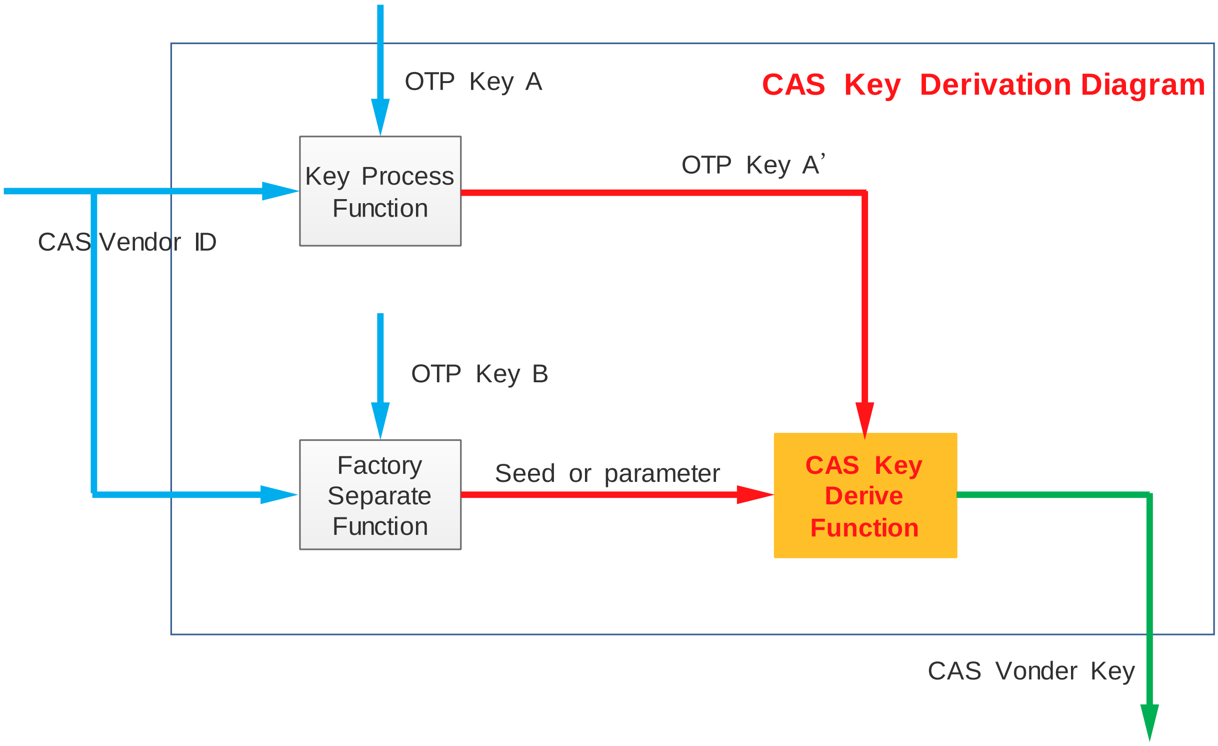
3. Ensure the CAS client software integrity, reliability and security in the process of upgrading, start-up and running;

3 What Operators Control

3.1 Core Modules

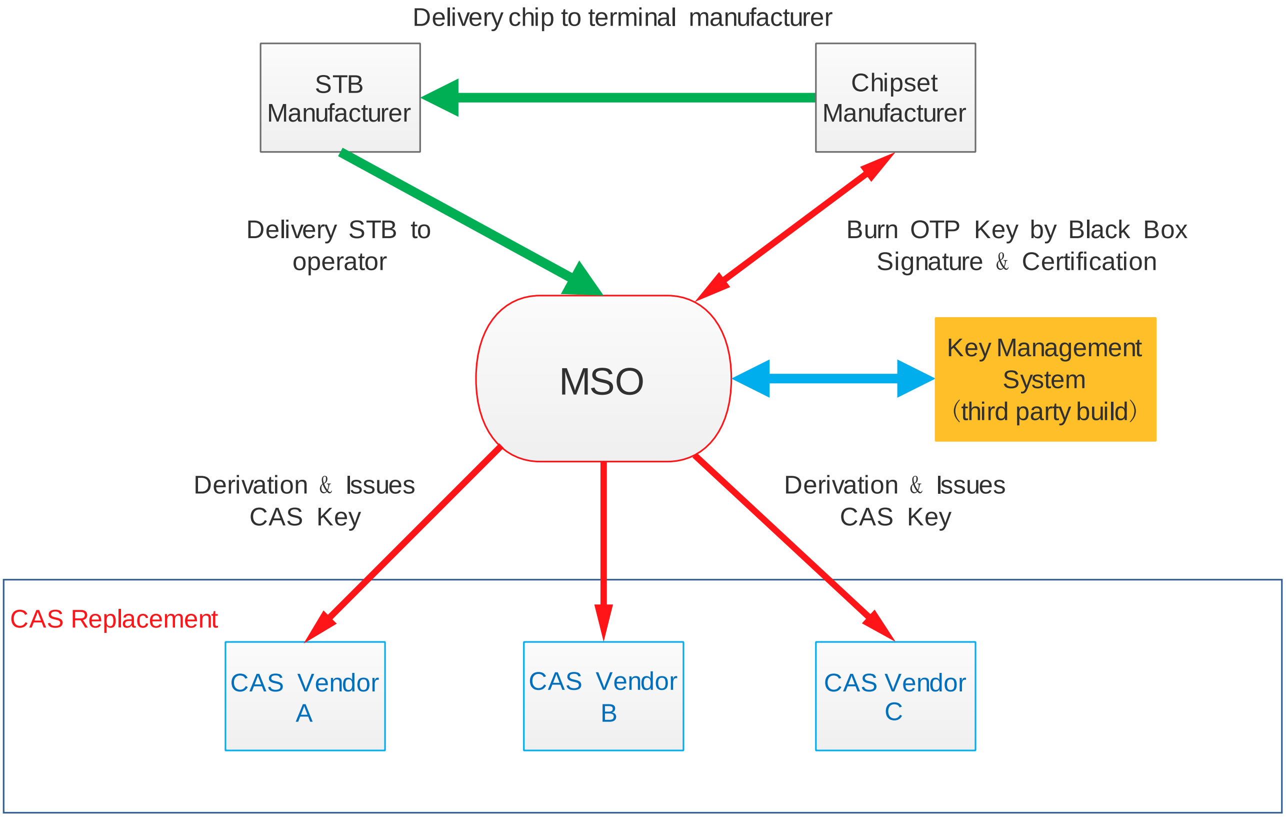
The key management system: the central control unit of the whole solution, taking control of the root key publish, CAS key derivation and management.

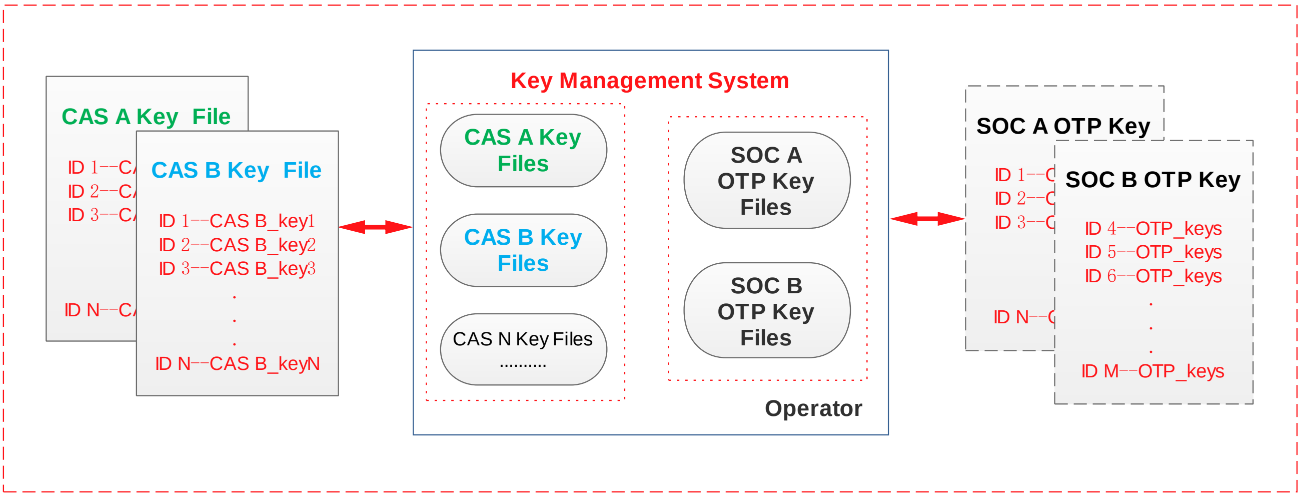
1. The secret key issuing system is in charge of the entire system root keys management, issuing and maintenance, which better is managed and controlled by the broadcast operator;
2. CAS key derivation system, responsible for CAS keys derivation for different CAS vendor and to safely transmit them to the CAS vendor;
3. Black Box, responsible for integrate with chipset manufacturers to safely write various secret keys into the OTP.



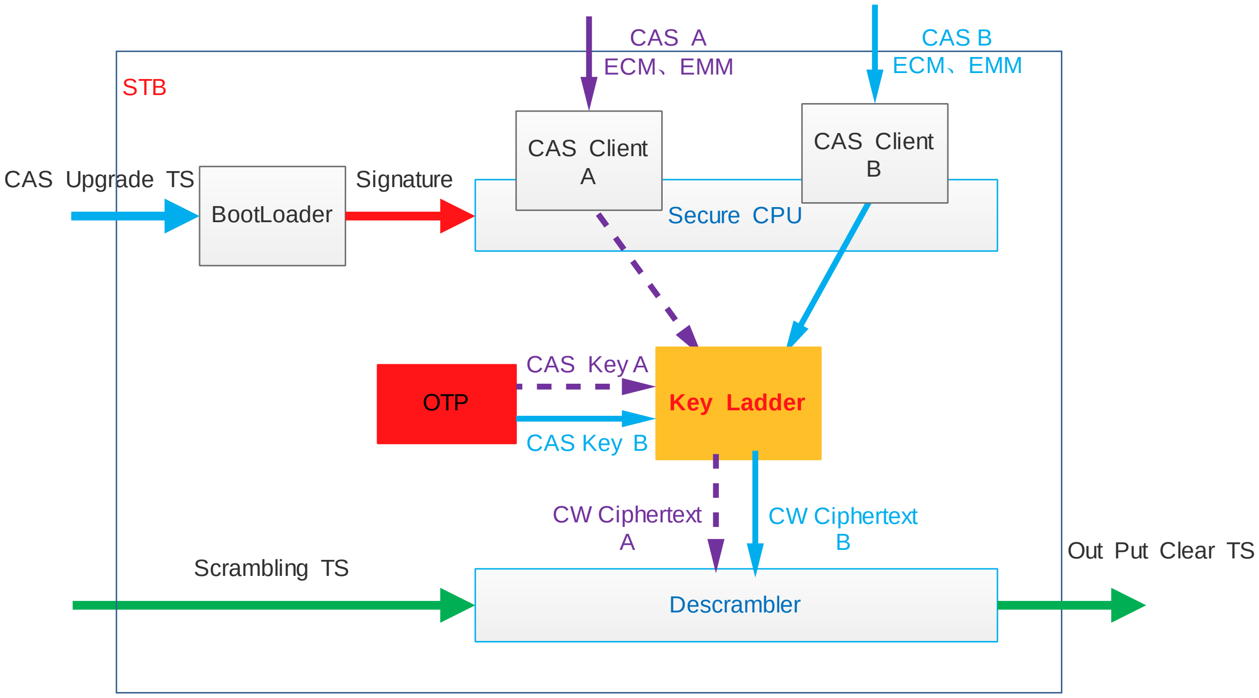
3.2 Secret–key Distribution

The key management platform can be set up and managed by the third party or by the operator. The operator is responsible for the secret keys issuing and distribution. Different CAS vendor accesses their own CAS secret key, so as to start over different CAS and decrypt channels on the same terminal.


Delivery chip to terminal manufacturer
STB Manufacturer
Chipset Manufacturer
Delivery STB to operator
Burn OTP Key by Black Box Signature ＆ Certification
MSO
Key Management System (third party build)
Derivation ＆ Issues CAS Key
Derivation ＆ Issues CAS Key
CAS Replacement
CAS Vendor A
CAS Vendor B
CAS Vendor C



3.3 CAS Upgrade



4 Operation and Implementation

4.1 CAS Replace

According to the technical principle above, the operators can obtain flexibility when need to replace the CAS vendor client to the user terminal.

It mainly has the following two situations:

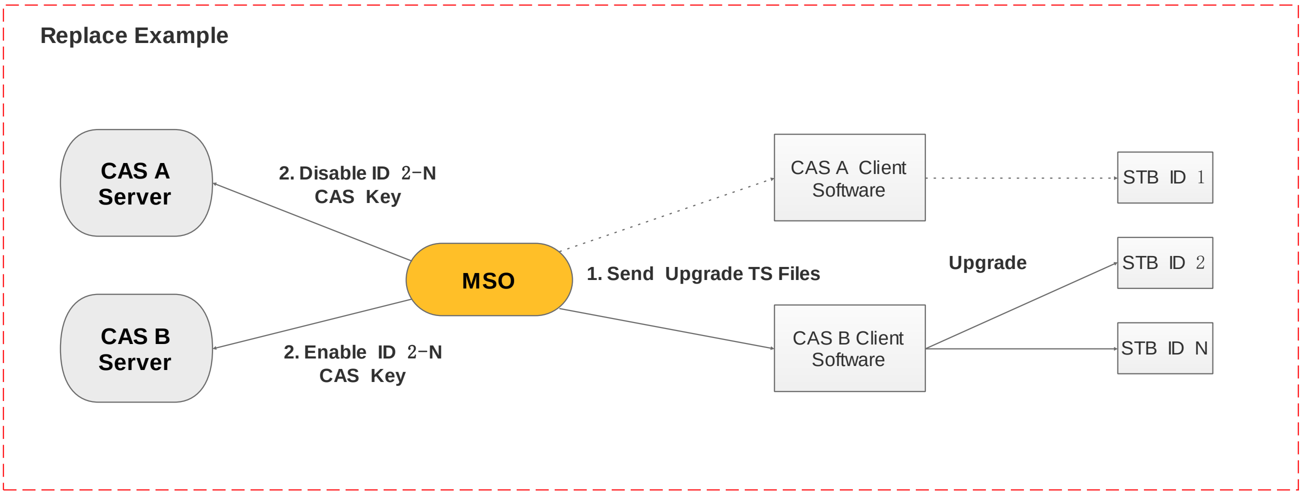
1. To simulcrypt with a new CAS system.

The CAS secret keys will be issued to the new CAS vendor, and the operator signs on the CAS client software, then the headend send upgrading stream of the CAS client software to ensure the normal start-up of the terminal.

Synchronize subscribers entitlements to new CAS system by SMS,then the terminal can decrypt programs when receive the entitlements.

2. Replace the CAS system of waiting state.

At this time, we just synchronize subscribers' entitlements to the ready CAS system by SMS, and upgrade CAS client to user terminal.

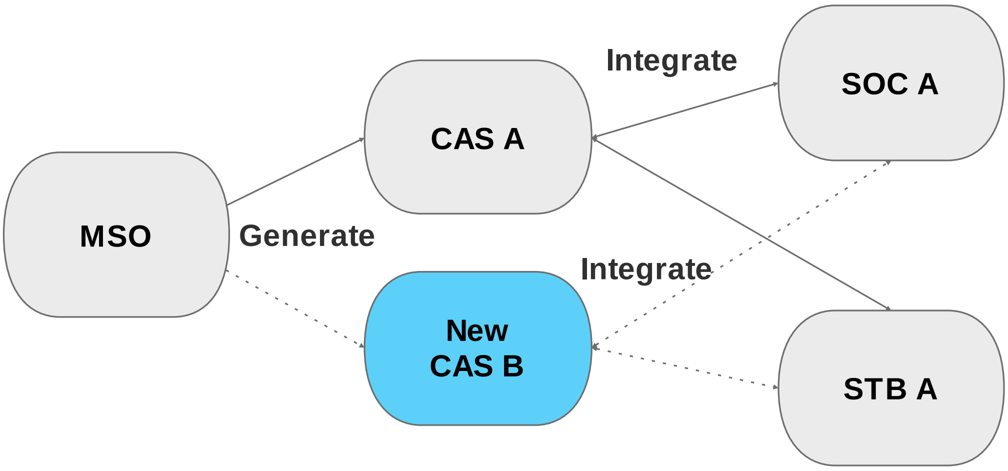


4.2 Operation Process

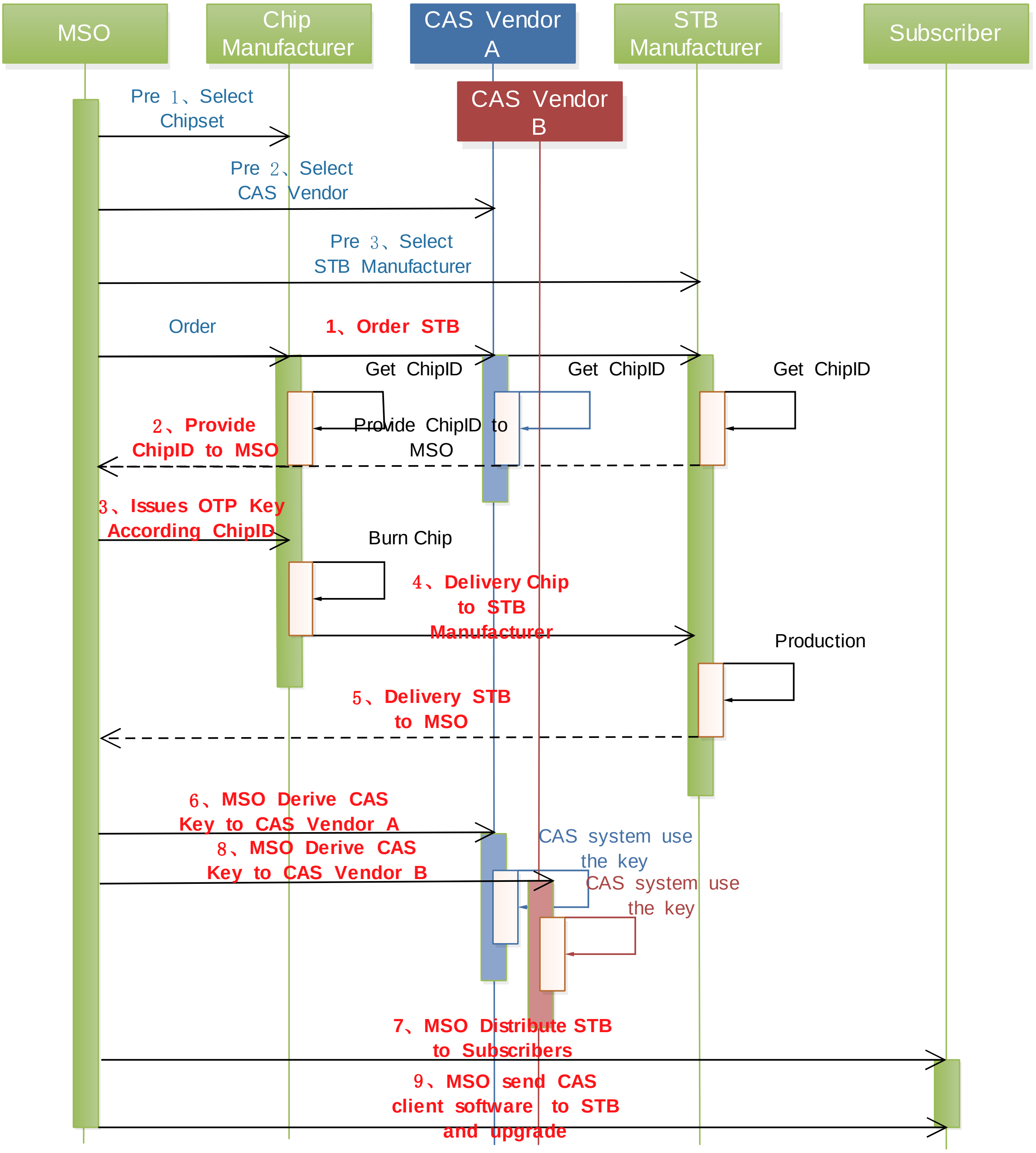
1. The operator orders terminals from the manufacturer (chip manufacturer or CAS manufacturer or terminal manufacturer);
2. The manufacturer obtains the chip ID according to the order, and provide it to the operator;
3. The key management system issues the secret key basing on the chip ID, and provide relevant data to the chip manufacturer to burn the secret key in OTP;
4. Chip manufacturer burns the secret key finished, then delivering the chips to the terminal manufacturers;
5. Terminal manufacturer production completion and delivering terminals to the operator;
6. The operator issues the CAS secret key send to the CAS vendor in a safe way;
7. The operator distributes the terminals to subscribers;
8. The operator issues another CAS secret key to the new CAS vendor when planning to replace another CAS system;

9. The new CAS system simulcrypt on headend and running, the operator send another CAS terminal client software to broadcast network and upgrade user terminal through upgrading platform, thus to realize CAS system replacement.

10. Repeat step 6 - step 9 for CAS system replacement.



4.3 Flow Diagram


MSO
Chip Manufacturer
CAS Vendor A
STB Manufacturer
Subscriber
CAS Vendor B
Pre 1、Select Chipset
Pre 2、Select CAS Vendor
Pre 3、Select STB Manufacturer
Order
1、Order STB
Get ChipID
Get ChipID
Get ChipID
2、Provide ChipID to MSO
Provide ChipID to MSO
3、Issues OTP Key According ChipID
Burn Chip
4、Delivery Chip to STB Manufacturer
Production
5、Delivery STB to MSO
6、MSO Derive CAS Key to CAS Vendor A
CAS system use the key
8、MSO Derive CAS Key to CAS Vendor B
CAS system use the key
7、MSO Distribute STB to Subscribers
9、MSO send CAS client software to STB and upgrade