CxCrypt System 5.1 ver.F (Aug.2008)

Conditional Access Introduction

Digital pay-TV services, whether delivered by satellite or terrestrial broadcasting, use encryption to protect a service from unauthorized viewing. The process of encryption involves the use of a mathematical procedure, or algorithm, which operates on the digital data to be protected, in conjunction with a secret piece of information called a 'control word'. The operation produces encrypted data, which will be meaningless to anyone who receives it, except those who possesses the secret decryption control word to recover the correct data. In the case of pay-TV, customers who subscribe to a channel or service are sent a smart card. The smart card is inserted into a slot in the digital receiver, and is able to recover the control word, which is sent to the customer over the air. The smart card may also hold a record of customer entitlements (CA profile), which can also be updated over the air.

Although this process sounds simple, it is made complicated by a number of practical considerations:

- The control word is usually changed frequently (often at regular intervals of several seconds), to make decryption difficult for any unauthorized "pirate" viewers, forcing them to find each new decryption key, as the key is changed.

- Each new control word has to be distributed to authorize viewers over the air (or broadcast channel), in advance of the change.

- Because the only medium allowing communication with the viewer's smart card, once the card has been issued, is the broadcast channel itself, an encryption hierarchy is often used to give a layered defense.

The decryption process or algorithm may be secret (as in GSM mobile telephony) or open (as in the DES, AES), and in either case, is standard, or unchanging. The critical components of security, which must remain secret, are the decryption key(s), which may be changed frequently.

Scrambling

The encryption of the content is done by means of a scrambler, which should be a hardware device such as the TsFormer Embedded Scrambler on the multiplexer.

Entitlement Control Message

The control word is sent to the IRD in an Entitlement Control Message (ECM). Every 10 seconds a different control word is used for scrambling. The current as well as the next control word is sent to the IRD per one ECM

Entitlement Management Message

The ECM message above also contains the 'CA profile' of a service. If a subscriber complies with

this CA profile then the video and audio will be descrambled. In other words, the CA profile was previously written to the smart card. The CA profile is written to the smart card by sending an Entitlement Management Message (EMM) to the smart card over the air.

Smart Card

The smart card component of the system is unique to each viewer. A smart card will usually contain a small micro controller (microcomputer), which is powered when the card is inserted into a digital receiver. Each smart card carries a unique identifier, and may be individually addressed. The card is used to hold the product entitlements (those pay services subscribed to by the user), which can be altered using EMM's (Entitlement Management Messages) sent over the air, and passed to the smart card from the Conditional Access Module (CAM) of IRD.

The card will also contain what can be considered a root decryption key, which is fixed, and written to the card at the time of issue, and will be used as sparingly as possible. The root decryption key is used to decrypt the next key in the key hierarchy, sent via the EMM's. This next key is used to decrypt Entitlement Control Messages (ECM's). ECM's are sent at regular, frequent time intervals, each one carrying the current and next service key required to decrypt the subscribed product video and audio data packets. These final control words are changed at regular intervals (typically every 10s), making it impractical for a pirate decoder to break the encryption in real time.

The other keys in the key hierarchy are changed at less frequent intervals, sometimes only when they are suspected of being compromised. Possession of a key higher in the hierarchy will allow all keys beneath it in the hierarchy to be decrypted, and therefore the data in the transport stream to be decrypted.

All keys from the root decryption key to the key necessary to decrypt the control word will be stored in the smart card memory. The smart card will recover the control words as they are sent out in ECM's, but these control words will be used by the Conditional Access Module (CAM).

Since a user may remove a smart card, leave it out of the receiver for a while, and then reinsert it, there is a need for regular play out of the EMM's containing the keys of the hierarchy, so that updates can be received upon reinsertion of a valid card.

The MPEG2 data is then decoded to analogue format.

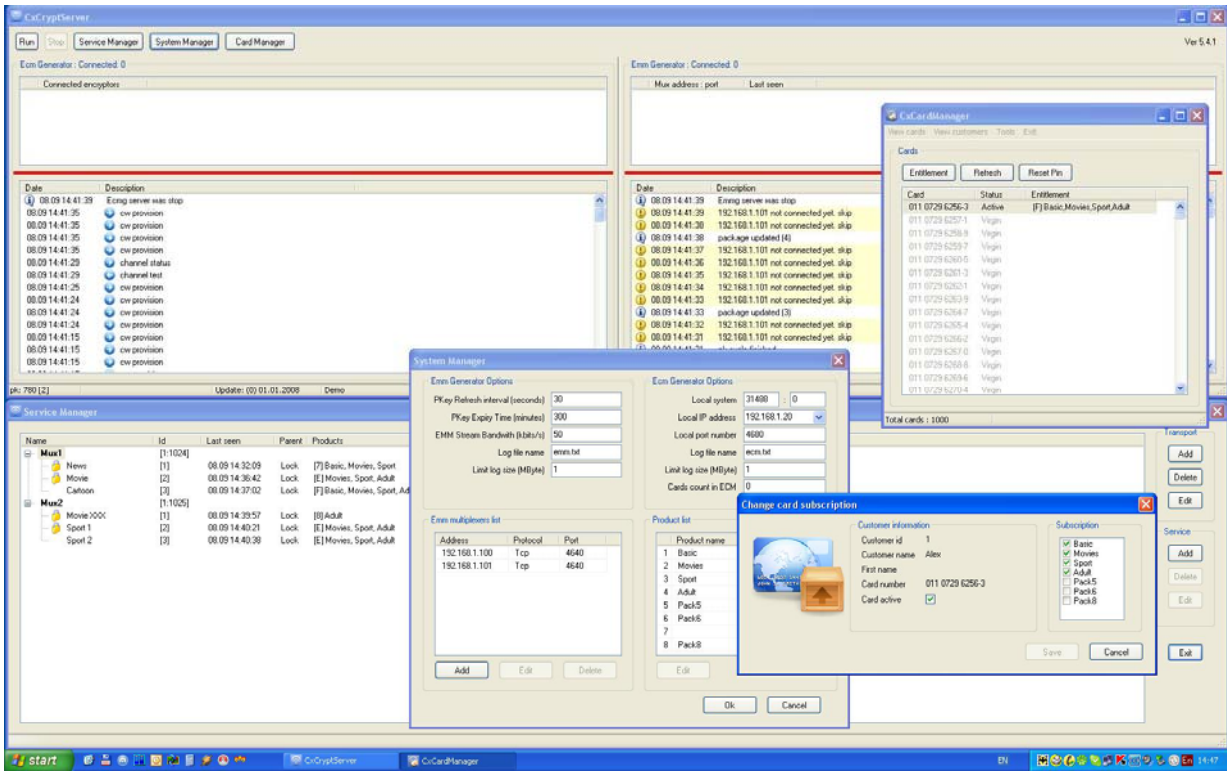
CxCrypt System Introduction

CxCrypt System CA is the compact conditional access system. Condensed from our experience, CxCrypt System CA is user-friendly and cost effective, yet gives small to medium-sized operators the benefit of all our broadcasting security experience. The most compact digital system yet, CxCrypt System CA can be used to encrypt audio and video signals. The system can be installed from a CD-ROM onto a standard PC running on a Windows XP platform, thus minimizing the required investment in hardware and system configuration.

CxCrypt System Modules

- CxCryptServer

- CxCardManager
- TsFormer Embedded Scrambler
- CxCrypt Smartcards



Operating Requirements Hardware

The following is the specification for a PC to run CxCrypt System CA:

Operating system:

- Windows XP SP2

Hardware specification:

- Pentium PC
- 512 MB RAM
- 800 MHz processor
- 30 GB hard disk
- Ethernet network card (UTP)
- CD ROM drive 48x

Infrastructure

CxCrypt System CA requires a simple LAN to connect it to the rest of the DVB network equipment and other applications.

Interfaces

- For the CA messages, CxCrypt System interfaces with the TsFormer multiplexer.

- On the other side it interfaces with CxCrypt embedded IRD set-top-box.

- It is possible to add an external subscriber management system, the SMS interface integrates
CxCrypt System and the SMS system where the operator chooses to use an external Subscriber Management System. It consists of ASCII-based (textual) commands and tables to manage a smart card's entitlements.

Components of CxCrypt Access CA Control System

Provisioning

Define who gets access to what	Subscriber management system (SMS) **CxCardManager**
Determine the length of time the subscriber has access to a piece of content	Subscriber management system (SMS) **CxCardManager** with possibility of import subscriber data from 3rd party application

Key Management

Generate keys for encryption of content	**CxCrypt Server**
Add/Remove entitlements (keys) from subscriber	**CxCrypt Server**
Cycle the keys for increased level of security	**CxCrypt Server**

Encryption

Encrypt the content being transmitted	**TsFormer embedded encryptor**

Decryption

Decrypt the content being transmitted	**CxCrypt smartcard** **CxCrypt embedded IRD**

Comprehensive system overall description

1. Easy control system
2. Virtually unlimited cards number in system (depend on computer)

3. Up to 8 products/packages support (ability of upgrade to 16 and more)
4. Any combination of products can be assigned to card
5. Unlimited number of service/product combination

Security and anti-piracy modes

1. Special design ISO 7816-3 compatible secure smart card
2. 3-level key security design
3. Entitlement ready to be sent over ECM in case blocked EMM
4. Possibility to find piracy card in case blocked EMM
5. Every 2 month key updates remove all pirates any case

Clients operations

1. Client Database
2. History of card/client operations
3. Remember of previous client entitlement state when card was blocked
4. ASCII interface to simplify SMS operations