

Introduction

Convenient uses **betacrypt2**, its self developed Conditional Access System which allows the encryption of digital pay TV content and the content to be delivered securely to the authorized subscriber.

The offered system is pre-installed to support services such as pay per channel (PPC), pay per view (PPV) and (near) video on demand ((N)VOD). The system integrates seamlessly into various video-server- and scheduler setups. Due to open and standardized interfaces, the system can be completed by off-the-shelf third party components to support local video on demand services, electronic programming guides, TV-Mailing Clients, as long as an appropriate set-top box is selected.

betacrypt2 systems can be scaled easily and cost-efficiently, since additional subscriber capacity can be reached by simply exchanging the hardware through one which provides for more computing power and hard drive capacity. The number of PPC/(I)PPV/(N)VOD channels can be scaled by adding or removing multiplexers and scramblers. Due to the open interfaces of **betacrypt2**, IP based multiplexers can be integrated into the system allowing for additional routes of broadcast. No additional licenses have to be purchased for augmentation of up to millions of subscribers.

Convenient practices an open policy for set-top box vendors. Virtually all set-top box vendors can enable their set-top boxes for **betacrypt2**, by embedding Convenient's royalty free software solution for set-top boxes. There is no royalty charged for the set-top box vendor.

System Overview

The **betacrypt2** Conditional Access System consists of a central headend device and of individual smart cards, which are distributed to the subscriber.

The operator and content provider controls the **betacrypt2** environment by connecting a customer care and billing system to the SMS interface of the headend device of **betacrypt2**. Since the **betacrypt2** SMS interface is ASCII and TCP/IP based, the integration into existing Customer Care and Billing solutions can easily be performed.

The headend of **betacrypt2** connects to the Avante HD Digital Headend to control the encryption of the content and to insert **betacrypt2** control data into the data stream which is transmitted to the subscriber's set-tops.

The **betacrypt2** enabled subscriber receives the encrypted content and control data via a **betacrypt2** compliant set-top box. The individual smart card of the end subscriber uses the control data to make the encrypted content available to the entitled subscriber.

betacrypt2

Convenient's **betacrypt2** Conditional Access System is used in combination with the DVB Common Scrambling Algorithm for scrambling broadcast audio, video and data. For descrambling, a control word is transmitted via ECM to a user device, e.g. a set-top box.

The control word is generated in the scrambler, encrypted in the Conditional Access System (CAS) and transmitted via the DVB-compliant hardware.

betacrypt2 is accessible by the operator via graphical user interfaces. All encryption within the CAS is done by **betacrypt2** encryptors. The encryptors are armed by using a set of smart cards. No non-encrypted key data ever leaves the encryptors. Several **betacrypt2** encryptors can be connected to the CAS to increase availability and computing power.

To enhance the security, **betacrypt2** was developed from scratch to ensure that no source code is shared with the predecessor CA system. This has been possible by utilizing the in-depth experience of our highly specialized development team. Nevertheless a detailed and continuous surveillance of potential piracy attacks is necessary to provide appropriate adaptive security strategies.

betacrypt2 offers a set of security mechanisms, such as 128 bit key length and shadow keys on air (key diversification). Control sequences are only accepted once by the smart card (reply attack prevention) and the uniqueness of the smart cards cryptographic content protects the system against global attacks (zero learning curve).

Active security is achieved by additional envelope encryption where the keys are changed every few seconds. **betacrypt2** uses volatile keys that are never used twice. As an additional active security mechanism the smart card memory organization is continuously varied.

betacrypt2 is designed to react on attacks using adaptive security mechanisms. In case of piracy it is possible to renew the cryptographic content of the smart card if a key is compromised, by using protected backup keys or replaces compromised algorithms by new, never previously used ones which are already implemented in the smart card. The Security Sector Manager of **betacrypt2** offers even more complex mechanisms to prolong the lifetime of **betacrypt2**.

Interfaces of CAS

DVB Simulcrypt interface

The EMMs and ECMs, encrypted by the encryptors, are transmitted from the CAS to a DVB Scrambler and Multiplexer using the DVB Simulcrypt standard protocols (as defined in the ETSI Standard TS 103 197).

betacrypt2 is already adapted to DVB multiplexer and scrambler equipment of Adtec, Tandberg, Scientific Atlanta, Sencore and others.

SMS interface

betacrypt2 has an open, ASCII-based interface for Subscriber Management Systems via an IP based VPN.

So far, the CAS software has been interfaced with both proprietary and industry standard SMS software, such as Convergys and GLDS. Convenient makes the **betacrypt2** SMS interface available to all its customers, thus an integration into existing Customer Care and Billing solutions can be easily performed.

Consumer Equipment

To watch encrypted programs, the consumer needs a set-top box with **betacrypt2** decoding facilities.

Currently, Toner offers several options for digital set-top boxes. These are the DCM4-SD, DCM4-HD, DCM4-HDR (a DVR model) and in early 2011 the DCM4-HD3000 which is a higher end HD set-top. These set-tops are MPEG2, as well as MPEG4, and have all the required licensing such as MPEG-LA, Dolby, ATSC, DVB, and are also FCC, UL RoHS and CE approved as needed. These set-tops operate with the Convenient CAS system based on the DVB standard. These set-tops do not have separable conditional access and therefore do not meet any Open Cable requirements. Use of these set-tops and the CAS systems is entirely the decision of the cable system operator. Toner Cable Equipment Inc. makes no claims as to the suitability of the system or the compliance with any federal, state, or local requirements for current, past or future standards and or mandates.

Convenient will license all suitable set-top box manufacturers for integration of **betacrypt2**, those who are recommended by the platform operator.

betacrypt2 allows the operation of set-top boxes in a one-way or two-way network environment. The one-way communication is based on EMM and ECM messages in standardized DVB data components which are addressed to the smart cards. The two-way network communication depends on the return channel functionality of the set-top box, e.g. IP, PSTN and DAVIC. The return channel is separately encrypted with independent return keys to enhance security.

Features

Technical Features of **betacrypt2**

betacrypt2 is designed to support all functions for a large Pay TV operator. Some sample features are listed below:

Pay Per Channel (PPC):

The customer subscribes to a package (e.g. sport- or feature film channel) pays, e.g. a monthly fee, to watch all events of in this specific package.

Pay Per View (PPV):

The customer pays only for individual televised events.

Pre-Entitlement:

The smart card could be pre-configured during the production cycle with different entitlements allowing for special marketing promotions, e.g. viewing a specific package free of charge for 30 days.

Middleware independent CA based parental control:

Safe parental control that fulfils the very strict legal requirements, and works independent of the set-top box middleware.

Depending on the respective set-top box and middleware used, the following additional sample features of **betacrypt2** are available as AV option.

Impulse Pay Per View (IPPV):

betacrypt2 enables the interactive ordering of separate events or services either with or without return channel.

Virtual Private Video Recorder (V-PVR):

Pausing NVoD consumption without requiring a hard disk. This is a time stamp based technique. Subsequent pressing of the 'Play' button triggers a selection of the NVoD feed, which lies nearest to the last time stamp.

On-Screen-Messages:

Displaying enquiries and messages directly on the customer's TV screen. The Display Messages function enables the content provider to establish contact with the customer quickly and cost effectively over the air.

Storage of subscriber related data on the smart card:

Memory cell for bank account details , delivery addresses, telephone numbers and much more (subject to the local legal framework).

Private Video Recorder (PVR):

If the STB provides a hard disk **betacrypt2** can be used to securely store content on a hard drive and reuse this content.

HD Content:

betacrypt 2 is compliant to HD ready headend and end consumer equipment.

Redundancy

For **betacrypt2** different redundancy implementations are possible. Entry level systems are available with a minimum of redundancy such as mirrored hard drives. The highest availability is achieved if a 1:1 hot standby redundancy is being implemented.

System and location requirements

Dimensions: min. 4 Rack Units (19" rack)

Hardware: **betacrypt2** Encryptor

Sun Fire/Opteron (1x CPU, 1GB RAM, 2x36GB HD)

Standard PC with MS Windows 2000 min. 1,3 GHZ, 256MB RAM, 4GB HD, CDROM, Floppy, Ethernet-card 100 Mbits (not included)

Software: Oracle Database (5 named user)

Sun Solaris Operating System

Operating, Maintenance & Support

Training offered by Convenient

A five day installation and training of 8 hours per day to operate the complete system is included. This is offered on site at time of commissioning.

In addition a special training for operators and call centre agents is also available.

Database management

Administration of the databases is done by Oracle standard tools and Perl / SQL scripts. Tools and standard scripts are included.

Operating manuals

A full set of English user manuals is provided with the installation, plus detailed training documentation.

Maintenance categories

Silver

Help desk is provided working day between 9 am and 6 PM local time Monday through Friday. Response time is 24 hours, weekends and public holidays excluded. Current updates are included.

Gold (Optional)

Help desk is provided working day between 9 a.m. and 6 p.m. local time Monday through Friday. Response time is 24 hours, weekends and public holidays excluded. Current updates, hardware support and remote maintenance are included.

License restrictions:

Delivery and usage of **betacrypt2** is subject to the conclusion of individual License Agreement(s) (which supersede(s) any other Convenient standard conditions) or to the unreserved acceptance of the „Standard Business Terms and Licensing Conditions of Convenient for the Delivery of Hard- and Software“, as well as other Standard Business Terms and Conditions third parties (e.g. ORACLE).

Business and product names cited within this Proposal are the property of its respective rights holders and protected by international Property and Trademark Laws.

On the basis of Convenient's extensive experience in Conditional Access Systems and headend software solutions, you will gain a partner with detailed knowledge of sophisticated broadcasting solutions.