



Irdeto CI Plus Solution

- A VARIETY OF PAY TV SERVICES ON IDTV, WITHOUT STB INVESTMENTS
- BEST-IN-CLASS SECURITY FOR HIGH-VALUE CONTENT
- EASE OF MANAGEMENT WITH PROVEN CONDITIONAL ACCESS SOLUTION
- FAST TIME TO MARKET WITH PRE-INTEGRATED CI PLUS CAMS

THE SECURE AND INTEGRATED SOLUTION FOR PAY TV SERVICES ON IDTV

The Irdeto Common Interface (CI) Plus solution is designed to address the fast-growing integrated digital television (IDTV or iDTV) market. An IDTV set, with a built-in digital tuner, does not require a set-top box (STB) for converting signals for reception on a TV. However, it is commonly equipped with a CI slot to allow the use of a conditional access module (CAM) for pay TV services. The Irdeto CI Plus solution, compliant with the CI Plus specification released by the CI Plus LLP, provides operators with an elegant and secure way to deliver revenue-generating services to an IDTV home. It delivers the stringent security demanded by content owners and operators, and enables operators to offer a variety of advanced services based on the device capabilities:

HOME NETWORK SUPPORT

Support of a PC-based server or a personal video recorder (PVR)

DIGITAL VIDEO RECORDER (DVR)

Support for time-shift TV and local storage of content based on SD memory size

IDTV, IPTV AND OVER-THE-TOP (OTT) READY DEVICE

DVB/IP-convergent CAM, connected via Ethernet for a home network environment and OTT video delivery (contact Irdeto for more information about Irdeto's content management solution can help with OTT content management and delivery).

RICH USER INTERFACE EXPERIENCE WITH MHEG5

Ease of customization enabling a variety of services, such as electronic program guide (EPG), targeted advertising, gaming and weather forecast

In keeping with Irdeto's dedication to innovation, Irdeto, along with its partners, is the first conditional access provider to deliver a CI Plus solution to the market. Irdeto's CI Plus solution enables

KEY FEATURES

The solution delivers the following based on the CI Plus specification:

PHASE 1

- Usage rules information (URI) transfer
- Trigger content control key (CCK) refresh
- Control the life time of CCK
- Switch revocation signalling data (RSD) detection on or off

PHASE 2

- Registered service mode (RSM)
- Personal video recorder (PVR)
- System renewability message (SRM) delivery
- RSD delivery

operators to capture new subscribers in the IDTV market, where consumers seeking pay TV services may purchase CAMs from retail channels or directly from the operators depending on the operators' business models

CI PLUS

CI Plus is a technical specification that ensures a secure link for transport stream packets between a CAM and a TV. It includes extensions to the DVB-CI specification that add protocol messages and features on both devices in order to protect content from being copied.

A CHOICE OF HARDWARE AND SOFTWARE CA CLIENTS

Irdeto offers its customers the CA solution that best suits their content protection and business model requirements using both hardware and software security clients. Irdeto's trusted smart cards are used to protect the highest value content with the most complex business models, while the software-only Irdeto Cloaked CA can be used as an alternative to smart cards, without the associated costs involved in the storage, handling and distribution of cards. Both solutions, when used with Irdeto's Secure Chipset technology, provide optimal protection against the latest forms of piracy and are fully upgradable while in the field.

Each security client uses a "secure container" to ensure it is highly robust to hacking, reverse engineering and tampering. Irdeto smart cards use the latest silicon technology available from leading manufacturers, while the Cloaked CA is protected by Irdeto innovative software security tools.

COMPONENTS

- Irdeto conditional access (CA) system with Irdeto CI Plus license
- Irdeto-approved* CI Plus CAM with Irdeto-approved secure chipset
- A choice of CA clients: Irdeto smart card, Irdeto Cloaked CA

**CAMs passing the Irdeto device verification test (DVT) obtain the Irdeto-approved status. CAM manufacturers must obtain the CI Plus certification directly from the CI Plus Trust Authority.*

CI PLUS CAM PARTNERS

- Neotion, SMIT

Contact Irdeto for a complete list.

SECURE CHIPSET

Although the Irdeto smart card and software-based client can be used with standard security devices, the Irdeto Secure Chipset solution is the ideal response to the challenges of securing a CI Plus CAM against two forms of piracy: control word redistribution and device software tampering.

Irdeto's Secure Chipset solution is based on:

- The presence of an advanced security descrambler chip in the CAM
- The unique personalization of this chip during its production
- A pairing relationship between the security client and the chip integrated into the device

These attributes enable the smart card or software-based client to be securely bound to a device, thus giving operators full control. In this solution, control word messages are uniquely encrypted as they pass between the Irdeto smart card or client and Irdeto type approved advanced security chipset in the device. They can only be decrypted by the authorized chip which is paired to that card or client. The unique pairing between the device and the card or client also ensures that targeted downloads can only be received by the intended device, and enhanced protection of the flash memory prevents attacks on services processed by the device.

FLEXIBLE SECURITY CLIENT UPDATE

Irdeto smart cards are based on the industry's latest silicon technology and allow smart card software to be securely updated over the air after cards have been deployed. This feature, called FlexiFlash, is unique to Irdeto and allows for major security and functionality changes to the smart card software. For example, operators can use FlexiFlash to renew 100% of the CA software on the Irdeto Premium Card. In Irdeto's customer networks, FlexiFlash has proven to speed up the deployment of functionality upgrades and enable proactive security updates or rapid response to piracy. By using FlexiFlash, operators maximize their return on investment by extending the card life for as long as possible, and renew security clients without disrupting subscribers' viewing experience.

The Irdeto Cloaked CA is also fully renewable in the field and can be updated over the air using operators' existing device management tools, enabling operators to easily add new functionalities and security to grow their business.

IRDETO CLOAKED CA

The latest version of the Cloaked CA is used to protect both the code and the data through obfuscation and data transformations. The application of these tools makes it extremely difficult to reverse engineer the Cloaked CA binary.

Code obfuscation takes normal software code and uses various mathematical calculations to convert code into "spaghetti-code" that is meaningless to anyone who should attempt to reverse engineer it. This is done in such a way that the code continues to function normally, but is virtually impossible to decompile and analyze. Irdeto has also created new types of data transformations and a 3DES white box. These new data transformations and the 3DES white box play a key role in preventing cloning and essentially help to anchor Cloaked CA to a specific user device.