

## Irdeto Cloaked CA Solution

- A CONDITIONAL ACCESS (CA) SOLUTION THAT INCORPORATES IRDETO'S TECHNOLOGY FOR BEST-IN-CLASS CARDLESS CONTENT SECURITY ON IRDETO'S INNOVATIVE TECHNOLOGY, SATELLITE, IP AND TERRESTRIAL NETWORKS

The Irdeto Cloaked CA Solution uses an innovative software security client as an alternative to smart cards for protecting digital TV content. The solution is designed for pay TV operators and broadcasters who want to offer digital services to their customers using a highly cost-effective, upgradable and future-proof conditional access solution. To assure content owners that their assets are protected against theft or viewing in unauthorized territories, operators must deploy a conditional access solution with uncompromising security, and yet they need that solution to incur the lowest possible long-term costs in combination with the desired devices, such as set-top box (STB), CI Plus conditional access module (CAM) or digital terminal adaptor (DTA). Cloaked CA enables operators to do both.

Hardened and protected by a variety of technologies and fully renewable in the field, Cloaked CA is audited and certified by industry-recognized experts such as T-Systems and Farncombe Technology Ltd. and trusted by major Hollywood studios. It provides a comparable level of security as smart card-based solutions, but without the associated costs involved in the storage, handling and distribution of cards. The solution employs Irdeto's patented technology for device code and data protection. The solution supports the "hardware root of trust" concept by locking each client uniquely to Irdeto keys embedded in the secure chipset of the device upon manufacture, thereby protecting against cloning, software tampering and control word redistribution.

This solution is future-proof, as the Cloaked CA Agent can be updated over the air using operators' existing device management tools. It enables operators to easily add new functionalities and security to grow their businesses.



### KEY BENEFITS

#### SECURE YET COST-EFFECTIVE SOLUTION

Based on Irdeto's proven smart card-based solution, Cloaked CA provides security for best-in-class content protection. Several technologies unique to Irdeto ensure the security of Cloaked CA: Secure ROM boot code in the device provides increased protection against device software tampering.

- Each device contains unique keys and is cryptographically locked to the Cloaked CA Agent to prevent cloning.
- White-box cryptography and code obfuscation further protect device code from tampering and reverse engineering.

#### DECREASED LOGISTICAL COMPLEXITY AND COSTS

Devices are pre-loaded with the Cloaked CA Agent at the factory, thus they need simply to be activated and are ready for use with pay TV or other encrypted services.

Cloaked CA is ideal for use in mass retail markets where devices are sold and distributed to consumers without operators' smart cards. The device can be prepared for use with multiple operators, each of which uses its own Irdeto CAS.

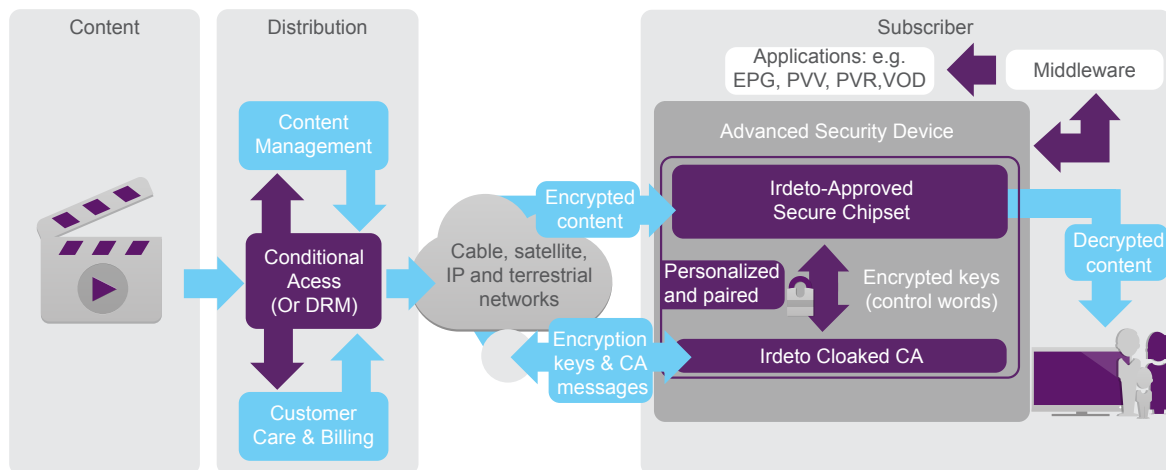
Security updates, new features and functionalities are easily downloaded over the air to the device, eliminating the need for costly card swaps. This can also be done far more quickly than developing and distributing a new smart card.

#### A VARIETY OF BUSINESS MODELS TO GROW INTO

Cloaked CA can be deployed with different profiles on the same network, supporting a variety of business models including subscription, pre-paid TV, pay per view (PPV), network or local personal video recorder (PVR), pull or push video on demand (Pull / Push VOD) and time-shift TV.

## SOLUTION CONFIGURATION

In this solution, the Irdeto CAS is deployed at the operator's head-end, and content is delivered securely from the operator to the subscriber via the cable or other transport network. In the subscriber's home, the client device is secured by Cloaked CA, which enables the subscriber to view the appropriate subscription package.



## SECURITY BASED ON IRDETO'S TECHNOLOGY

The latest version of Irdeto's technology 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 Agent 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 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.

## RISK REDUCTION THROUGH CLIENT BASE DIVERSIFICATION

### INTER-OPERATOR DIVERSIFICATION

Each operator using Cloaked CA receives a unique version of the client. This means that devices produced for a specific operator can only be used for this operator's services, and cannot be used by any other operator without this operator's permission. In addition, a security concern in an operator's network will not affect any other operator's system.

### INTRA-OPERATOR DIVERSIFICATION

Multiple Cloaked CA Agent versions can be randomly distributed and deployed per operator, thus limiting the operator's exposure to any successful attack. If one device with Cloaked CA is compromised, that compromise will only work on other devices using that same variant, further limiting the impact of piracy.

## CLOAKED CA WITH SECURE CHIPSET

The Irdeto Secure Chipset Solution is the ideal response to the challenges of securing a STB or conditional access module (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
- 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 Cloaked CA Agent 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 Cloaked CA Agent and Irdeto type approved advanced security chipset in the device. They can only be decrypted by the authorized chip which is paired to that Cloaked CA Agent. The unique pairing between the device and the Cloaked CA Agent 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.

For more information, please refer to the Irdeto Secure Chipset datasheet or contact Irdeto.

## IRDETO CLOAKED CA, A GREENER WAY TO PROTECT PAY TV



One great example of Irdeto's green initiative is Irdeto Cloaked CA, an innovative card-less software security solution that delivers the same level of uncompromising security as a smart card, for protecting digital TV content. As a cardless solution, Cloaked CA eliminates the energy and waste associated with smart card production, distribution and disposal. All this leads to a significant amount of savings on energy usage and waste, which clearly has a positive impact on the environment and operators' bottom line. Being "green" does not mean any compromises on the "cool factor", either, as security updates, new features and functionalities for Cloaked CA can be easily downloaded over the air to the device on both one-way and two-way networks.