Solution Overview

Media Protection

Irdeto Conditional Access

A FULLY RENEWABLE AND SCALABLE SOLUTION FOR PROTECTING CONTENT AND BUSINESS MODELS ON BROADCAST AND IP NETWORKS

Irdeto's conditional access system provides the most stringent content security for pay-TV operations. It also enables pay-TV operators and broadcasters to offer more services, payment options and device support which equates to choice, flexibility and convenience for their customers. Whether via cable, satellite, terrestrial, IP, mobile or hybrid networks, Irdeto's flexible solutions enable broadcasters to easily deploy new TV services and support new devices without interrupting existing subscriber services or compromising their digital assets.

KEY BENEFITS

- **Stay ahead of evolving security threats with Renewable Security**
  Irdeto's successful, holistic security strategy has produced not only the industry's best technology, but also provides an on-going roadmap of security enhancements. To protect customers' investments, the Irdeto conditional access system (CAS) was designed to deliver renewable security [FlexiFlash], enabling operators to update not only software-based security clients, but also card-based ones quickly and easily without costly card swaps.

- **A Variety of Pay-TV Options**
  Irdeto CAS offers a large number of modules, combined with the appropriate client options, to support advanced functionalities. It enables operators to provide more flexibility to subscribers and raise ARPU.

- **Flexible Deployment Models**
  In addition to choosing either a smartcard or software-based security client, the Irdeto CAS can be configured to meet the needs of a specific market. It can be tailored for small to medium-sized operations, as well as large-scale networks for millions of subscribers in a fully redundant setup and is available as a managed service. Irdeto's solutions are also fully standards-based and compatible with a wide range of set-top boxes, client devices, compression equipment and subscriber management systems. This open approach allows operators to select the components of their choice or rely on Irdeto for a pre-integrated, end-to-end solution.

- **Operational Simplification for Broadcast and OTT with the Integrated Management System**
  The head-end management system for Irdeto CAS has been designed so that operators who want to deploy a multiscreen offer on mobile devices can centrally configure and manage both the DRM security and their CA solution through a single, unified system. This allows operators develop new mobile service offerings while simplifying operations with central control of access rules and policies for both broadcast including IPTV and OTT.

Irdeto's CAS enables pay-TV operators and broadcasters offer more services, payment options and device support which equates to choice, flexibility and convenience for their customers.

EFFECTIVE AND VIGILANT ANTI-PIRACY EFFORTS

Digital content piracy is a worldwide issue, where well-funded criminal organizations are constantly looking to exploit security systems. The art is therefore not only in the prevention of such efforts, but in how one can effectively respond to them when they occur. In addition to best-in-class security technology as the foundation of the Irdeto CAS, Irdeto continuously provides advanced countermeasures as plug-ins to the system to help operators quickly respond to new threats and ensure rapid recoverability.

To effectively utilize the tools, Irdeto offers a suite of services to help operators manage security over the lifecycle of the content, from ensuring site security and auditing operator platforms and devices from the start, watching and defending on an on-going basis, to keeping security up-to-date to stay ahead of ever-evolving security threats.

Irdeto also works diligently to fight piracy on a worldwide basis by securing stricter antipiracy legislation and collaborating with customers, partners and law enforcement entities to investigate and prosecute pirate activities.

RENEWABLE SECURITY

The cornerstone of Irdeto's security strategy is renewability, enabling operators to update the head-end and deployed clients quickly and easily through the FlexiFlash mechanism, whether for software-based or smart card clients without requiring costly card swaps.

Highlights of the security benefits include:

Built-in recoverability and renewability:
Irdeto CAS renews security by updating smart cards or software-based clients over the air via Irdeto's FlexiFlash technology. This built-in mechanism allows Irdeto to introduce new features and piracy countermeasures as plug-ins to the system, which results in shorter development, test and release times. This design enables operators to quickly respond to new threats and ensure rapid recoverability.

Future-proof cryptography:
In conjunction with Irdeto Premium card or Cloaked CA client, the Irdeto Key Management System (KMS), a head-end component of the Irdeto Integrated Management System, uses the latest advances in cryptography to create Irdeto-specific algorithms and an operator-unique cryptographic layer, resulting in:

- No single point of security failure
- Higher resistance against attacks with proven cryptographic strength and indefinitely updateable algorithms
- Operator separation, reducing the risk of threats spreading from one operator to the next

Countermeasures against control word sharing (CWS):
Irdeto CAS provides effective defense against CWS, including:

- A heuristic algorithm to detect smart cards used for analog re-broadcasting on cable networks
- An improved communications interface layer with intellectual property rights (IPR) support to enable prosecution when an Irdeto Premium card is used in emulation set-top boxes

A VARIETY OF PAY-TV OPTIONS

Irdeto CAS offers a large number of optional modules to support advanced functionalities. This enables operators to provide more flexibility to subscribers and increase ARPU. Supported services include:

Subscription:	Up to 65,000 packages Ordered pay per view (PPV): multiple ordering methods
Impulse PPV:	With or without feedback, pre- or post-paid
Pre-paid pay TV:	Scratch card, cash payment
Preview:	Allowing consumers a configurable, limited time window to experience a service for free in order to convert them into paying customers
Personal (or digital) video recorder (PVR):	Stored content encryption, on/off control for subscription PVR, digital rights management (DRM) rules for copied content
Auto-expiry card:	Variable packages and validity periods
Video on demand (VOD):	Subscription or PPV

FLEXIBLE DEPLOYMENT MODELS

The Irdeto CAS can be deployed in multiple different configurations and across a variety of client devices to address unique business, security and operational requirements. It can also be provided as a managed service. Irdeto's solutions are also compliant with industry standards, enabling interoperability and ease of integration with third-party products to provide maximum choice to operators.

CI Plus CAM for integrated digital television (iDTV): a variety of pay-TV services, such as home network support and PVR, directly to the iDTV set without the need for an STB

Home networking: Controlled sharing and distribution of subscriber content across multiple screens (both secondary TVs and across consumer devices) within a household. Also include options for download and go on specific devices.

Multi-room: Content viewing in multiple rooms within a household from a single subscription

Proximity control: A cost-effective multi-view implementation, to share content on the PVR via the home network while preventing STBs – and the content - from moving outside the home

Enable OTT and Broadcast content on STB; The cardless Cloaked CA client can support both IP and DVB transmissions on a same client device, giving operators additional flexibility in their business models

FEATURE HIGHLIGHTS

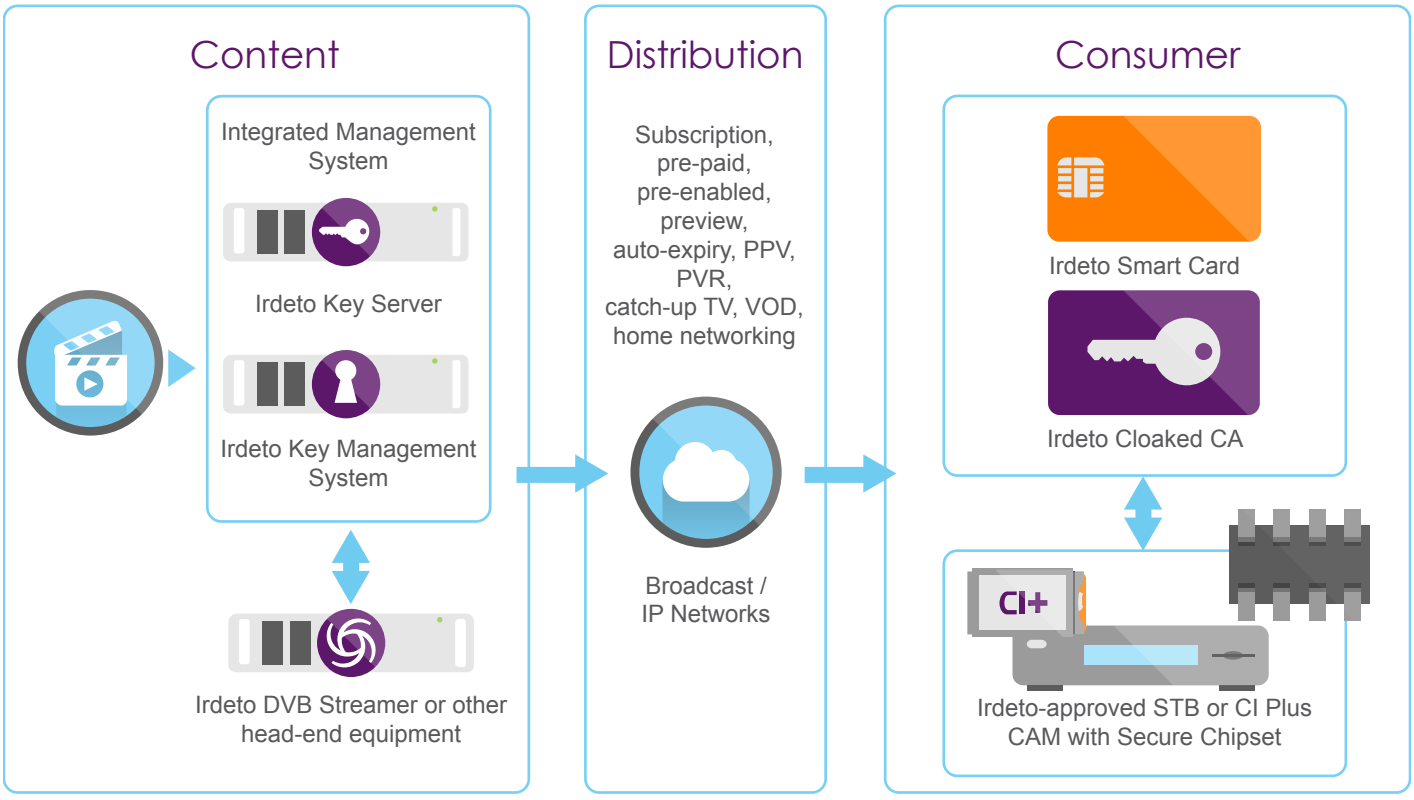
Flexible Security Client Update
Irdeto's Conditional Access is based on the industry's most recent microchip technology and allows smart card and software clients to be securely updated over the air after they have been deployed. This feature, called FlexiFlash, is unique to Irdeto and allows for major security and functionality updates to the subscriber devices. For example, operators can use FlexiFlash to renew 100% of the conditional access (CA) software on both the Premium card and the Cloaked CA client.

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 a piracy attack. By using FlexiFlash, operators maximize their return on investment by extending the effectiveness of their CA solution for as long as possible, and renew security clients without disrupting subscribers' viewing experience.

Secure Chipset
The Irdeto Secure Chipset solution is the ideal response to the challenges of securing a set-top box or conditional access module 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 STB or CAM
- The unique personalization of this chip during 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 STB chip which is paired to that card or client. This 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.



A Choice of Hardware and Software CA Client Solutions
Irdeto offers its customers the CA solution that best suits their content protection and business model requirements using both hardware and software security clients. Both solutions, when used with Irdeto's Secure Chipset technology, provide the same level of uncompromising protection against the latest forms of piracy and are fully upgradable while in the field. A unified head-end system enables the operator to easily manage both clients, making a mixed-based deployment simple and cost effective.

Each security client uses a "secure container" to ensure it is highly robust against hacking, reverse engineering and tampering. Irdeto smart cards use the latest silicon technology available from leading manufacturers, while the Irdeto Cloaked CA is protected by Irdeto's innovative security technology for source code obfuscation, data transformations and white box cryptography. This results in "cloaked" code that is meaningless to anyone who should attempt to reverse-engineer it.

ARCHITECTURE AND COMPONENTS

The Irdeto CAS consists of the following components:
Single, unified management system at the head-end for both operator-owned and unmanaged consumer devices through the Irdeto **Integrated Management System (IMS)**

- Irdeto Key Management System
- Irdeto Key Server
- (Optional) Irdeto Control (IMS module required for unmanaged devices)
- (Optional) Irdeto DVB Streamer, Irdeto Pre-Encryption Server
- (Optional) Third-party integrated solutions, e.g. VOD services

Secure client options at the subscriber side
On Irdeto-approved set-top boxes, CI or CI+ conditional access modules (CAMs), with Irdeto type-approved advanced security chipsets

- Irdeto smart card
- Irdeto Cloaked CA

Additional options for mobile devices
Irdeto offers a range of options for securing content on unmanaged mobile devices. As for operator set-tops and gateways, these can be centrally managed via a single head end interface, simplifying subscriber management and billing.
These include:

- Irdeto Secure Key Exchange for studio grade protection on iOS and Android devices that scales particularly well for multiple live streams
- Irdeto Third Party DRM for integration of any industry-recognized DRM (some of which can be hardened by Irdeto technology), to provide maximum reach across the widest range of devices

CAS-RELATED SERVICES

Irdeto has a unique team of consulting professionals to support a global customer base. A full range of professional services is available to meet customers' needs; examples include:

System integration services: Project management, vendor management, installation planning, commissioning of equipment and customer trial management to deliver projects with quality, on time and within budget

Integration and customization services: Requirements analysis for the design and development of the project, integration support to manufacturers, and technical integration consultancy to help Irdeto customers develop unique strategies and innovative ideas for their business

Head-end implementation services: Pre-Installation and system preparation of the Irdeto head-end equipment to help operators install and integrate equipment with minimal interruption to their services, perform acceptance tests and provide on-site operational and intensive product trainings to ensure the maintainability of the system

Testing and field trial support: Develop test designs and scripts, manage regression and extensive systems testing, report test progress using innovative software tools to deliver results to all levels of audiences within or outside the organization

Security Lifecycle Services audit, update and implementation services: Conduct an audit of the CAS location, configuration and management processes based on CA Site Security Certification requirements, help operators mitigate the risk of piracy and fraud resulting from incorrect and unsafe operation of the CAS, reduce vulnerability to social engineering attacks.

CAS Optimization Service: Provide an assessment of customer's content protection system and its environment in order to give appropriate recommendations for configuration, tuning, system implementation, security improvement and to support implementation of such recommendations.