

# CONDITIONAL ACCESS

TODAY'S CONSUMERS HAVE SO MANY OPTIONS WHEN IT COMES TO DIGITAL CONTENT FOR ENTERTAINMENT. AND THOSE CHOICES MULTIPLY DAILY AS BOTH PROFESSIONALS AND AMATEURS MAKE NEW CONTENT AVAILABLE. MEANWHILE, MORE AND MORE DEVICES FOR VIEWING CONTENT ARE CONTINUOUSLY INTRODUCED.

These are some of the major drivers behind the constant push-pull facing content owners and distributors in their quest to deliver quality, in-demand content via broadband and broadcast networks that is targeted to specific audience interests. Along with meeting customer demands on a variety of devices, content owners and distributors need to protect their own interests. They cannot afford to compromise quality or security when it comes to maximizing the value of their digital assets.

However, pulling all the pieces together to meet these objectives is far from simple. This is where Irdeto can help by offering a comprehensive portfolio of technology solutions for protecting content while supporting business objectives. From content creation to middleware integration to distribution, Irdeto technology goes beyond protecting digital assets and provides platforms that create more engaging customer experiences, improve customer service and easily extend existing offerings through up-sell opportunities.

## Irdeto's Conditional Access System (CAS)

provides the most stringent content security for TV broadcasters. Irdeto's CAS also enables TV broadcasters to offer more services, payment options and device support which equates to choice, flexibility and convenience for customers.

Whether it's via cable, satellite, terrestrial, IP, mobile or hybrid networks, Irdeto's flexible solutions enable TV broadcasters to freely experiment with new services and support new devices without risking compromises to their digital assets.

# BENEFITS

---

## BEST-IN-CLASS AND RENEWABLE SECURITY

Irdeto's successful, holistic security strategy produces not only the industry's best technology, but an ongoing roadmap of security enhancements. To protect customers' investments, the Irdeto CAS was designed to deliver renewable security, enabling operators to update deployed clients quickly and easily without 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. A built-in mechanism allows Irdeto to introduce unforeseen features and 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, Irdeto Key Management System (KMS), a head-end component of the Irdeto CAS, uses the latest advances in cryptography to create Irdeto-specific algorithms and an operator-unique cryptographic layer. It results 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

## EFFECTIVE AND VIGILANT ANTI-PIRACY EFFORTS

Digital content piracy is a worldwide issue, and its protection is trusted to a select number of recognized experts in this area, who are constantly battling well-funded, well-organized and criminal organizations who are tirelessly 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 and advanced countermeasures, Irdeto remains diligent in anti-piracy efforts, working to secure stricter anti-piracy legislation and collaborating with customers, partners and law enforcement entities to investigate and prosecute pirate activities.

## A VARIETY OF PAY-TV DISTRIBUTION MODELS

Irdeto CAS offers a large number of optional modules, combined with the appropriate client options, to support advanced functionality. It enables operators to provide more flexibility to subscribers and raise 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
- **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), push VOD:** subscription or PPV
- **High definition (HD)**
- **Multi-view:** content viewing in multiple rooms within a household from a single subscription
- **Proximity control:** a cost-effective multi-view implementation, possibly re-using legacy STBs, sharing content on the PVR via the home network and preventing STBs from moving out of the home
- **CI Plus CAM for integrated digital television (iDTV):** a variety of pay-TV services, such as home network support and PVR, to the iDTV set without the need for an STB
- **PC content delivery:** delivery of digital content over a delivery medium such as broadcasting or the Internet to a personal computer

## FLEXIBLE DEPLOYMENT MODELS

The Irdeto CAS can be flexibly deployed to meet the specific needs of an operator. It can be configured to support small to medium-sized networks, as well as large-scale networks for millions of subscribers in a fully-redundant setup.

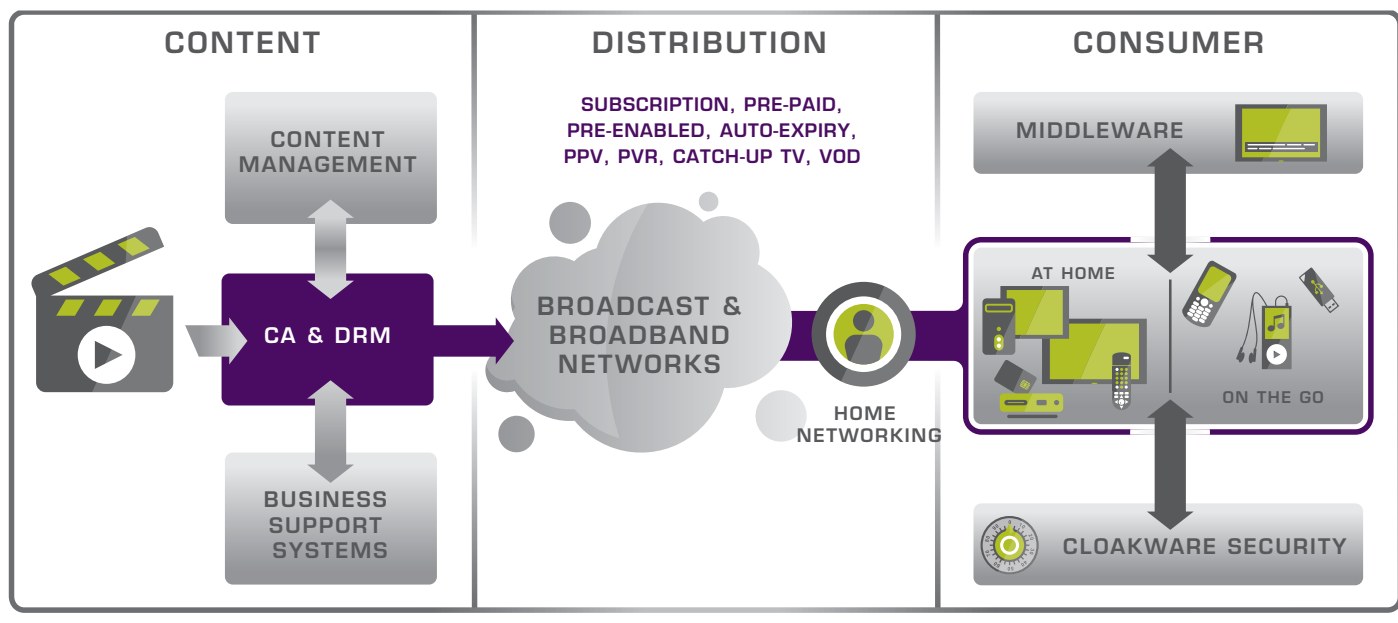
Irdeto's solutions are also fully standards-based and compatible with a wide range of set-top boxes, client devices, compression equipment, and subscriber management systems, including Irdeto's own Customer Care and Billing solution. It allows operators to select the components of their choice or rely on Irdeto for a pre-integrated, end-to-end solution.

## EASY-TO-USE SYSTEM FOR EFFICIENT DEPLOYMENT

With the intuitive and user-friendly GUIs, the Irdeto CAS is easy to configure, maintain and monitor, saving operators time and expense in running their operations. Irdeto also leverages industry standard technology for scalability and redundancy and complies with DVB standards such as DVB Simulcrypt, making it simple to build from the operators' current infrastructure and preserving their investments.

# THE SOLUTION

The Irdeto CAS can be deployed in different configurations and on a variety of client options to address unique business, security and operational requirements of the operator. 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.



## COMPONENTS

THE IRDETO CAS CONSISTS OF THE FOLLOWING COMPONENTS:

### CONTROL SYSTEM AT THE HEAD-END

- Irdeto Key Management System (successor of Irdeto PIsys)
- Irdeto Key Server (successor of Irdeto Encryptor)
- (Optional) Irdeto DVB Streamer, Irdeto Pre-Encryption Server
- (Optional) Third-party integrated solutions, e.g. VOD services

### SECURE CLIENT CHOICES 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

### On mobile devices

- Irdeto smart card chip as a surface-mounted device (SMD)
- Irdeto Java applet on subscriber identity module (SIM) card
- Irdeto Java applet on microSD

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
- Integration and customization services
- Head-end implementation services
- Middleware support services
- Testing and field trial support
- Security audit, update and implementation services

For operators looking for pre-integrated, turnkey solutions, the Irdeto SmartStart family bundles the following components to enable fast and cost-effective deployments:

- Irdeto conditional access system
- Irdeto Java-based middleware platform
- Irdeto business support systems
- Irdeto content management solution
- Professional services and worldwide support

# FEATURE HIGHLIGHTS

---

## FLEXIBLE SECURITY CLIENT UPDATE

Irdeto smart cards are based on the industry's most recent microchip 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 conditional access (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 STB management tools, enabling operators to easily add new functionalities and security to grow their business.

## SECURE CHIPSET

Although the Irdeto smart card and software-based client can be used with standard security STBs, 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 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 STB 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.

## 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. 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 to protect lower-value content or content only requiring basic subscriber control (e.g. license fee enforcement) or geographic restriction. 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 Irdeto Cloaked CA is protected by Irdeto subsidiary Cloakware's innovative software security tools. Cloakware's tools are used to protect both the client code and the data processed by it through obfuscation, data transformations and white box technology. This results in "cloaked" code that is meaningless to anyone who should attempt to reverse-engineer it.