

# IRDETO KEY MANAGEMENT SYSTEM

## THE SECURE AND RENEWABLE SOLUTION FOR PAY-TV CONTENT PROTECTION

The Irdeto Key Management System (KMS) is a versatile, modular and scalable component of the Irdeto conditional access system (CAS), deployed at the head-end in conjunction with Irdeto Key Server. Used in combination with an Irdeto-approved client device and security client such as a set-top box (STB) and an Irdeto security client such as a smart card or a software-based client, Irdeto KMS ensures that operators' digital media is secured with the best encryption technology.

### DEPLOYMENT OPTIONS<sup>1</sup>

#### Basic

- Scalability<sup>2</sup>:** 500,000 smart cards or software-based clients
- Redundancy:** None
- Configuration:** One IBM System x3550 server, with
  - Microsoft Windows Server 2003 R2 Standard Edition
  - Microsoft SQL Server 2008 Standard Edition

#### Enterprise

- Scalability<sup>2</sup>:** 20 million smart cards or software-based clients
- Redundancy:** None
- Configuration:** One IBM System x3550 server for application, with
  - Microsoft Windows Server 2003 R2 Standard Edition
 One IBM System x3550 server for database, with
  - Microsoft Windows 2003 Server R2 Standard Edition
  - Microsoft SQL Server 2008 Standard Edition

#### Full System Redundancy

- Scalability<sup>2</sup>:** 20 million smart cards or software-based clients
- Redundancy:** Full redundancy (FSR)
- Configuration:** Two IBM servers or server blades, similarly configured as the IBM System X3550 for application, with
  - Microsoft Windows Server 2003 R2 Standard Edition
 Two IBM servers or server blades, similarly configured as the IBM System X3550 for database, with
  - Microsoft Windows 2003 Server R2 Enterprise Edition
  - Microsoft SQL Server 2008 Standard Edition
 One IBM System Storage DS3200 (recommended)

<sup>1</sup> One or more Irdeto Key Servers are required in each deployment option.  
<sup>2</sup> This assumes one active sector per smart card.

### Functionalities and Specifications

- Support for STB Secure Loader
- DVB Service Information (DVB SI) generation for applications such as electronic program guide (EPG)
- Easy-to-use APIs to subscriber management systems



### KEY FEATURES

#### Best-In-Class, Renewable Security

- Built-in recoverability and renewability: Irdeto KMS 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:

- Irdeto KMS, in conjunction with Irdeto Premium card, 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 KMS 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 Business Models

Irdeto KMS has a large number of optional modules to support advanced functionality to raise ARPU, such as personal video recorder (PVR) and video on demand (VOD) and pre-paid pay TV.

#### Compliance with Industry Standards

Irdeto leverages industry standard technology for scalability and redundancy, and complies with DVB standards such as DVB Simulcrypt (version 1 and 2) to protect operators' investments.

#### Easy-To-Use System for Efficient Deployment

With the intuitive and user-friendly interface, Irdeto KMS is easy to configure, maintain and monitor. Irdeto KMS supports all deployed smart cards and set-top boxes, simplifying migration and maximizing the return on investment for Irdeto customers.

