Case study

Protecting Valuable Media Assets from the Threat of Piracy

Background

The way that we access and consume video content has changed dramatically in recent years. The evolution in the Pay TV landscape now means that consumers have a wealth of choice from content which is broadcast and consumed on set top boxes to OTT content which can be delivered to any device.

Protecting TV services from the threat of piracy, against this evolving backdrop, is creating new challenges for Pay TV operators. Set top box piracy is a serious, and growing threat with a host of premium content offered to users through illegal services at much less than the cost of a cable or satellite subscription. This can hit the operator's business hard; as the loss of valuable media assets through activities such as card sharing by pirate de-crypters can have a significant and far reaching impact on revenue. Operators, need to protect their investment, delivering uncompromising security to satisfy content owners, or risk the loss of rights to premium content. Guaranteeing the protection of valuable media assets is critical both to the Pay TV business model and to operator's revenues.

The challenge

One organization which is at the forefront of the fight back against these threats is Irdeto, a world leader in Media Protection, Multi-screen and Revenue Assurance solutions for pay TV operators. Irdeto delivers robust real-time defences against piracy for pay-media companies and content owners.

With some 350 customers including Liberty Global, Foxtel, Cablevision and Comcast, Irdeto provides solutions based on the most advanced hardware and software technologies which enable consumers to securely access premium content from any device. The cornerstone of Irdeto's security offering is the Security Key Server Technology, which protects critical cryptographic operations and guards against intrusion attempts. For Pay-Tv content protection the Irdeto Key Management System (KMS) is 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, the Irdeto Key Server ensures that operators' digital media is secured with the best encryption technology.

The server has to fulfill the following requirements:

- Investment Protection: The Irdeto Key Server solution has to be fully backward compatible with all deployed Irdeto smart cards and software releases.
- Future-proof cryptography: enable the decryption of subscriber database records established during the smart card personalisation phase.
- Offer high resistance against attacks with proven cryptographic strength and indefinitely updateable Algorithms.
- Guarantee operator separation, reducing the risk of threats spreading from one operator to another.

The solution:

To provide the platform for these media protection solutions, Irdeto turned to Utimaco, a leading provider of a hardware security module (HSM) which enables cryptographic keys that are truly unique and cannot be accessed by a third party. It is built on an open platform enabling developers to program their own algorithms into the HSM.
The combination of hardware resilience and a flexible, open platform, backed up by the ongoing service and consultancy support of a global company, has made them the partner of choice for Irdeto since 2008.

One platform, one technology:

Senior Product Director Frank Poppelsdorf of Irdeto comments: "What most impressed us about Utimaco – and which proved to be decisive in the selection process - is that we can have our own tailor - made solution. The flexibility of Utimaco's open appliance platform meant that our developers could program and design our own Software Architecture, in the way that we need it to work. It means we can provide higher resistance against attacks and respond swiftly to the discovery of new threats. There are no restrictions."

He continues: "Utimaco delivers the maximum flexibility for us on both levels: the open software platform and the open HSM platform. These two factors have enabled us to design the best in class, future proof, Key Management platform." The result is a FIPS 4 certified, hardware security module which provides operators with the highest levels of security for content protection, to protect critical cryptographic operations combined with simplified operational management. It is fully tamper proof, with sensors to detect mechanical, chemical, temperature and power attacks and the ability to destroy sensitive information upon intrusion attempts.

Through Utimaco's OEM program, the Key Management Server is shipped with the Irdeto brand and Utimaco has worked to ensure that logistics are adapted to suit Irdeto's requirements so that shipping of hardware is a seamless process. Frank Poppelsdorf of Irdeto concludes: "With Utimaco we have a partnership that fulfils our requirements both from a technological and operational standpoint. The solution is robust and but we also benefit from the logistical and consultancy support of an organization which is a true leader in its field."

More resources:

https://hsm.utimaco.com/

http://irdeto.com/