intertrust®

Provisioning secure identities in media and entertainment devices

White Paper

Secure Systems

Contents

Executive summary 2

Why are device identities essential for pay-TV and streaming services? 3

Different types of device identities required for media players 4

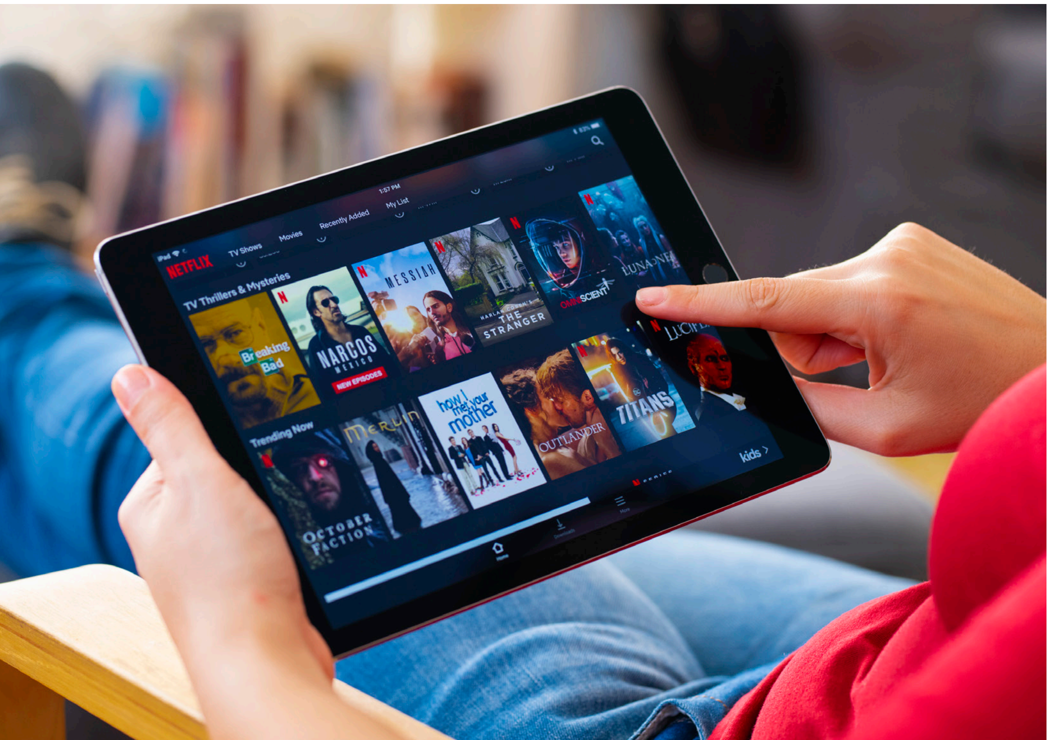
The media player device provisioning supply chain 7

Seacert offering for media and entertainment services 9

Executive summary

The Media and Entertainment (M&E) industry relies heavily on secure identities and cryptographic keys embedded in media player devices to provide services securely. They allow devices to authenticate with pay-TV and streaming services, and to authorize media playback while protecting premium content delivered to subscribers.

During the lifecycle of a media player device, several types of device identities and key hierarchies must be programmed and managed. This white paper describes methods for provisioning the variety of such essential secrets at different steps of the manufacturing supply chain. It shows how the M&E industry can leverage a managed key provisioning service from a trusted certificate authority to efficiently and economically generate, provision, and manage the device identities and keys throughout the device lifecycle.



Why are device identities essential for pay-TV and streaming services?

With the growing demand for subscriptions in the M&E industry, pay-TV operators and multichannel video programming distributors (MVPD) find themselves in a vastly altered environment that encompasses an immense array of devices and media players used by their subscribers. In order to fulfill security requirements imposed by content rights holders, it is crucial to establish a trusted pay-TV ecosystem that includes the media player devices, and which can protect content delivery for each programming type and service.

The growing number of pay-TV offerings and streaming services is also increasing the threat of piracy from illegitimate or compromised devices and media players. The recently released Video Piracy: Ecosystem, Risks, and Impact report estimates that the value of pirated video services accessed by pay-TV and non-pay-TV consumers will exceed $67 billion worldwide by 2023.[1] To address content owners' piracy concerns, the media industry depends upon hardware-backed security on media player devices. Historically, this involved smartcard-based security devices embedded in the cable and satellite set-top boxes (STB) used in broadcasting services. However, the new norm takes advantage of content delivery over the internet and leverages hybrid STBs or smart TVs that fully connect to the pay-TV service. The new hybrid media player devices rely on card-less security solutions or digital rights management (DRM) technologies, which utilize hardware device identities at the system on a chip (SoC) level for the highest degree of protection of premium content.

The types of devices vary from connected smart TVs, or cable, satellite or IPTV STBs, to other types of internet-connected streaming devices such as phones, tablets, and game consoles. All of these devices need to be part of a trusted ecosystem of an authorized service supported by the pay-TV operator. Any unauthorized or compromised device must be detected and removed from the pay-TV trusted ecosystem.

When it comes to protecting content delivery to the authorized devices, several levels of protection keys must be employed to ensure that only trusted devices can access the premium content. Creating and maintaining such a trusted ecosystem of connected media players requires mutual authentication between the end device and the pay-TV service operator. By leveraging device identities and mutual authentication standards, the media players and devices can prove to the pay-TV operator that they are an authorized member of the trusted ecosystem.
In the next section, we look at the different types of media player device identities and root keys that are essential for protecting premium content.

[1] **Source:**
Video Piracy: Ecosystem, Risks, and Impact
by Parks Associates (Q4 2019)

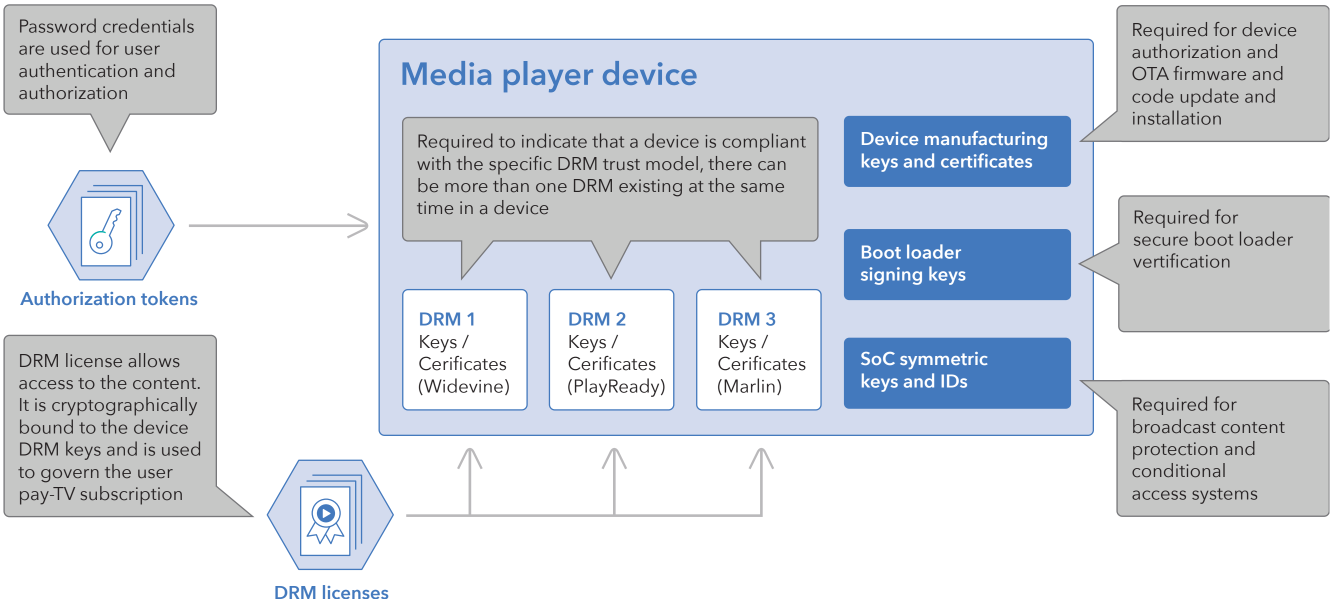
Different types of device identities required for media players

In general, each media player device owns a set of cryptographic keys and a digital certificate that enables it to authenticate securely with the pay-TV service provider. The combination of such keys and digital certificate, also called a secure identity, enables the media player device to perform many different types of cryptographic operations as required.

These operations permit authorization of the device to media content, as well as access to the decryption keys required to play back pay-TV channels or streaming services. In order to maintain the integrity of the device, software and firmware updates are secured using specific identities and keys throughout the device lifecycle.

Figure 1 shows the different types of cryptographic keys and certificates required by a typical media player device, along with the use case for each type of item. In order for the device to be compliant with the pay-TV service requirements, it needs to pass the service certification. This certification validates the existence of SoC symmetric keys, device manufacturing keys, certificates, secure bootloader, and digital rights management (DRM) keys and certificates.

Figure 1:
Different types of keys and certificates required for a media player device


Password credentials are used for user authentication and authorization
Authorization tokens
DRM license allows access to the content. It is cryptographically bound to the device DRM keys and is used to govern the user pay-TV subscription
DRM licenses
Media player device
Required to indicate that a device is compliant with the specific DRM trust model, there can be more than one DRM existing at the same time in a device
DRM 1 Keys / Cerificates (Widevine)
DRM 2 Keys / Cerificates (PlayReady)
DRM 3 Keys / Certificates (Marlin)
Device manufacturing keys and certificates
Boot loader signing keys
SoC symmetric keys and IDs
Required for device authorization and OTA firmware and code update and installation
Required for secure boot loader vertification
Required for broadcast content protection and conditional access systems

Symmetric key package

Symmetric keys and IDs generally get assigned to the SoC of a media player device and programmed in the one-time programmable (OTP) fuses, which are hardware protected and not readable or modifiable by device software. Sometimes such root keys are used to generate the encryption keys that protect the broadcast content in Conditional Access Systems (CAS). They are used as the root keys in the ETSI key ladder, which generates the channel keys or content decryption keys on the media player device. For example, the "SoC Black-Box Key Package" shown in Figure 2 includes SoC root key materials and is generated and delivered to SoC manufacturers for programming and provisioning at the SoC level.

Device manufacturing keys and certificates

Media player devices, like all connected devices, rely on public key infrastructure (PKI) for authentication and authorization into a trusted ecosystem. Not only do the device identities and cryptographic keys need to be issued by a single source and tied to a unified domain, but also the private part of key pairs must be protected in the hardware of media player devices. These keys, typically programmed during the device manufacturing process, are used for authorization and authentication of the device, as well as over the air (OTA) firmware and code updates. Examples of such PKI keys include device root certificates, firmware and code signing public and private keys, and certificate revocation lists. A third-party certificate authority, on behalf of the pay-TV service provider, typically generates and manages these keys.

Boot loader and code signing keys

When an STB or TV device boots up, the bootloader code loads the OS and other software components required to connect to the pay-TV service. The integrity of the bootloader code is crucial to prevent hackers from jailbreaking the device and its software. For this reason, the device manufacturer or service operator always signs the bootloader code. The process of validating the bootloader signature and other software components in the media player device is called secure boot or secure code verification. The public key used as the boot and code signing key must be programmed securely during the manufacturing process. It is used for signature verification of the software during the boot up process. Figure 3 shows the different components of PKI credentials and bootloader verification keys programmed in a media player device during the device manufacturing process.

Figure 2:
Examples of SoC BlackBox Key Package

SoC Blackbox Key Package
SoC Symmetric Key ID
SoC Symmetric Keys (AES128)

Figure 3:
Examples of device manufacturing keys and certificates

Media Player PKI Credentials
Device Root Public Key Certificate
Device Root Private Key
Boot Signing Vertification Public Key Certificate
CA Root Public Key Certifcate

DRM keys and certificates

When a media player connects to a streaming service such as Netflix, Amazon, or Disney+, the content is protected by digital rights management (DRM) technology. A device with a valid subscription authenticates to the streaming service provider, then receives authorization to play the content based on a DRM license delivered to the media player. Authenticating the media player device securely and delivering a DRM license requires DRM-specific device identities and DRM-related root keys. Examples of such keys and identities include Google Widevine DRM credentials, Microsoft PlayReady DRM Sub CA (Certificate Authority) credentials, and Marlin DRM Personalization Packets; these credentials are included in the DRM key package.

For example, for Widevine DRM, the media player device requires a Widevine DRM root of trust that is provisioned onto the device by the original equipment manufacturer (OEM). This root of trust is used to authenticate with the Widevine server before a Widevine DRM certificate can be installed. It is also used to authenticate with the service provider to receive a DRM license during playback.

Figure 4:
Examples of DRM keys and certificates

DRM Key Package
Widevine DRM Root Key
PlayReady DRM Sub Keys
Marlin DRM Personalization Packets

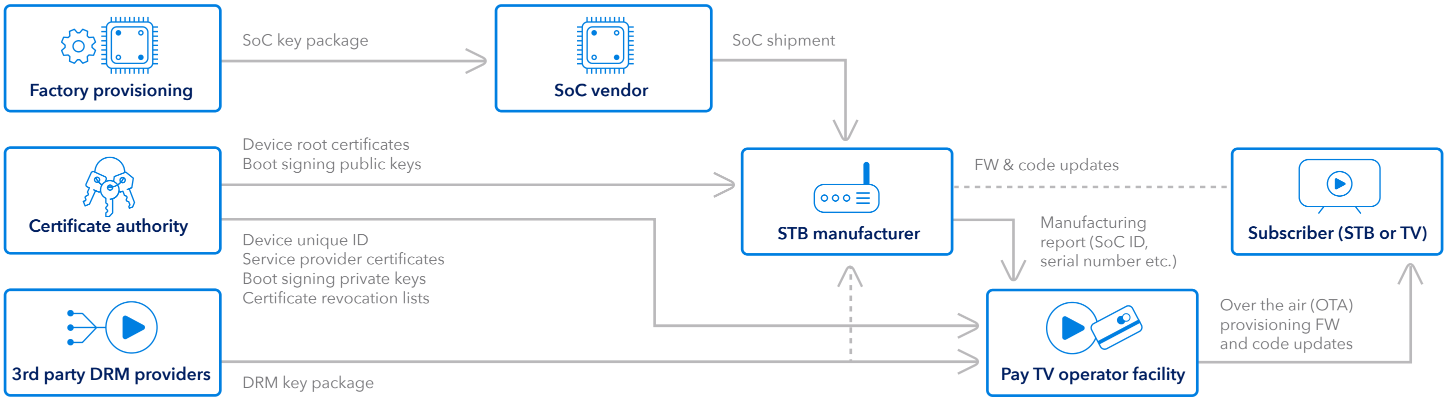
The media player device provisioning supply chain

A typical media player device like an STB is manufactured by an OEM and includes an SoC designed specifically for media delivery. The different components of the device identity are programmed at different stages of device lifecycle. Some keys and identities are programmed during SoC production and configuration, some during device manufacturing by the OEM vendor, and some might be in the field with the STB already connected to the pay-TV service.

Figure 5 shows the different parties involved in a typical supply chain for the M&E industry and methods of delivering different types of device identities and keys to different vendors. The process starts by programming SoCs during production and configuration with certain symmetric keys and identities, which become part of the SoC key package. Typically the pay-TV operator contracts with a key provisioning service to provide these. Once the SoC is programmed and shipped to the STB manufacturer, the CA provides additional device root keys and certificates for provisioning during STB manufacturing.

Note that the CA entity managing the certificate hierarchy and generating device PKI certificates could be the same vendor managing key provisioning for the SoC vendors, or it could be an independent certificate authority. Once manufactured, the STBs are shipped to the pay-TV service provider's facility for configuration, readying the device for field deployment. A manufacturing report that contains device specific metadata such as SoC ID, device serial number, version number, etc. is usually provided along with the device.

Figure 5:
Media player device provisioning supply chain



In parallel, third-party DRM keys such as Widevine, PlayReady, and Marlin are either provided directly to the STB manufacturer, or to the pay-TV operator's facility. Such credentials, delivered as part of the DRM key package, are used to configure the device for additional streaming services such as Netflix, Amazon Prime, etc. In the case where the DRM key package is delivered to the pay-TV operator's facility, installation of these keys is performed via the OTA channel into the STBs at the consumer home, using the pay-TV operator's cloud service.

A similar approach is used to upgrade the firmware and for code updates, as well as revoking device certificates based on the Certificate Revocation List (CRL) from the CA. During the lifetime of the device, the service provider will continue to use the OTA channel to manage the device identity lifecycle by updating the device certificates or device firmware when required.

Seacert offering for media and entertainment services

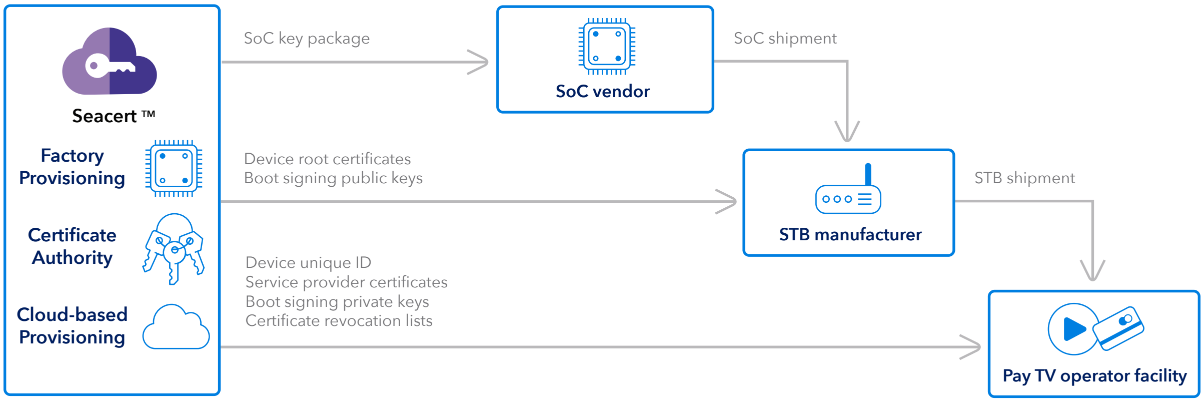
For any trusted ecosystem, regardless of the industry, it is critical that device identities and cryptographic keys are issued by a trust authority experienced in generating and managing identities, root keys, and key hierarchies. Moreover, the same vendor needs to sign all public keys that are part of the trusted ecosystem.

Provisioning device identities requires an understanding of the supply chain, manufacturing environment, cryptography, and cryptographic hardware. In addition, large scale deployments present their own set of challenges, making vendor experience in provisioning devices at such scale crucial.

Seacert provides a complete, full-service managed PKI that specializes in delivering device identities at scale for trusted ecosystems, with extensive experience in M&E.

Seacert has already provisioned over 2 billion devices across the globe, from STBs to smart TVs. It is built to scale easily, with a proven track record of provisioning up to 10 million devices per day. Seacert supports SoC factory provisioning, OEM factory provisioning for STB and smart TV devices, as well as cloud-based field provisioning, to meet all the requirements of the M&E device provisioning supply chain. Figure 6 shows how Seacert is used for provisioning secure identities for media player devices.

Figure 6:
Seacert device provisioning for Media and Entertainment supply chain



Seacert benefits for media and entertainment

Seacert has been used for over 15 years in the key provisioning of media player devices. Unlike traditional PKI, which is built for enterprise applications, Seacert was designed and engineered specifically to manage and provision identities for STBs and smart TVs. It has generated billions of device identities for different types of media player devices.

Seacert is highly scalable and flexible to meet evolving M&E application needs. Through its scalable cloud provisioning service, it supports provisioning from 100 to 10M device identities per day. In 2018 alone, Seacert provisioned identities to more than 724 million devices. Using the Seacert Managed PKI Service eliminates the need to run an in-house operation, with your own PKI experts who know how to set up and protect the appropriate facilities, staff, technology, and processes.

Secure and trustworthy service

Seacert is both WebTrust compliant and ISO 9001:2015 certified. The WebTrust annual audit covers all aspects of a Certificate Authority from the people to the process, to the infrastructure, and business continuity plans. In addition, ISO 9001:2015 certification ensures that Seacert delivers the best-of-breed services at the highest possible quality.

Since its inception in 2008, Seacert has earned an impeccable reputation, fulfilling orders 100% on-time and error-free. Seacert's professional services team brings a vast understanding of the complexity of device entities to design and implement customized schemes tailored to your specific business needs.

To learn more, contact a Seacert PKI expert or visit:
intertrust.com/products/seacert

About Intertrust

Intertrust provides trusted computing products for leading corporations–from mobile, CE and IoT manufacturers, to service providers, and enterprise software companies. These products include the world's leading digital rights management (DRM), software tamper resistance, and technologies to enable secure data exchanges for various verticals including energy, entertainment, retail, automotive, and fintech.

Intertrust is headquartered in Silicon Valley with regional offices globally. The company has a legacy of invention, with fundamental contributions in computer security and digital trust. Intertrust holds hundreds of patents that are key to internet security, trust, privacy management, mobile code, networked operating environments, web services, and cloud computing.

intertrust®

Building trust for the connected world

Learn more at: intertrust.com
Contact us at: +1 408 616 1600

Intertrust Technologies Corporation
920 Stewart Drive, Sunnyvale, CA 94085