GLOBALPLATFORM®

THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY

Improving Premium Content Protection with the Trusted Execution Environment

White Paper

September 2015

secretariat@globalplatform.org | www.globalplatform.org | © 2015 GlobalPlatform Inc.

Table of Contents

About GlobalPlatform

GlobalPlatform defines and develops specifications to facilitate the secure deployment and management of multiple embedded applications on secure chip technology. Its standardized infrastructure empowers service providers to develop services once and deploy across different markets, devices and channels. GlobalPlatform's security and privacy parameters enable dynamic combinations of secure and non-secure services from multiple providers on the same device, providing a foundation for market convergence and innovative new cross-sector partnerships.

GlobalPlatform is *the* international industry standard for trusted end-to-end secure deployment and management solutions. The technology's widespread global adoption across finance, mobile/telecom, government, healthcare, retail and transit sectors delivers cost and time-to-market efficiencies to all. GlobalPlatform supports the long-term interoperability and scalability of application deployment and management through its secure chip technology open compliance program.

As a non-profit, member-driven association, GlobalPlatform has cross-market representation from all continents. 130+ members contribute to technical committees and market-led task forces. For more information on GlobalPlatform membership visit www.globalplatform.org.

Publication Acknowledgements

GlobalPlatform wishes to thank all members of the Premium Content Task Force, which helped to shape the vision for GlobalPlatform's Premium Content White Paper. Special thanks go out to the following GlobalPlatform members and their respective organizations:

GlobalPlatform Members:

Mike Borza – Elliptic Technologies
Jim Helman – MovieLabs
Pascal van Gimst - Riscure
Sanjeev Verma – Samsung Mobile
Hervé Sibert – ST Microelectronics
Michael Lu – Trustonic

GlobalPlatform Team Members:

Kevin Gillick – Executive Director of GlobalPlatform
Gil Bernabeu – Technical Director of GlobalPlatform
Alliances Management – GlobalPlatform Operations Secretariat

Intended Audience

This document is intended for executives in media organizations, especially content owners, rights holders, and Premium Content providers. It is further intended for manufacturers of media consumption devices, such as televisions, set-top boxes, tablets, mobile devices, and more. The intended reader should have an interest in understanding how GlobalPlatform Specifications can be leveraged to assist with protection of media on devices, as well as how the technology can be leveraged to enhance content consumption.

This white paper requires a general familiarity with GlobalPlatform technologies, most specifically the Trusted Execution Environment (TEE). To learn more read the TEE White Paper or visit the GlobalPlatform website.

Executive Summary

Streaming and downloading movies, music, TV shows, and other copyrighted material to a variety of devices is a rising trend in the Premium Content industry. With the ongoing proliferation of content formats, Conditional Access (CA) systems, and Digital Rights Management (DRM) schemes for Premium Content, the cost and complexity of ensuring content security is on the rise.

GlobalPlatform has defined an infrastructure that safeguards the security, integrity, and privacy of services deployed on a platform, even when alongside services from other providers. GlobalPlatform's Trusted Execution Environment (TEE) enables Premium Content to run in an isolated environment, giving service providers peace of mind that they, and only they, can control their services. The services are not at risk from – nor a risk to – other services sharing the platform. GlobalPlatform's TEE provides a standard, secure environment for mobile applications deployed around the globe.

The TEE, as a secure area of the main processor, offers an execution space that provides a higher level of security than a Rich OS. By ensuring that sensitive data is stored, processed, and protected in an isolated, trusted environment, while still proving performance necessary to run most applications, the TEE offers an exceptional balance of security and performance.

GlobalPlatform's TEE specifications define the TEE and standardize the TEE APIs. Standardization brings many benefits to the industry, most importantly, it allows service providers to develop a Trusted Application (TA) once, yet deploy it across all device types, regardless of other applications that are present on the TEE. This means that the service provider does not need to know what kind of platform the end user will be viewing their content on, which addresses compatibility and scalability issues often encountered in multi-channel, multi-device, and multi-app deployments. The specifications are designed to satisfy the market requirements of a broad ecosystem of stakeholders, including manufacturers of televisions, set-top boxes, tablets, mobile devices, and more. GlobalPlatform's TEE certification program provides the final key piece of the TEE solution

Many industries have already started using the TEE for their applications. For Premium Content, the TEE brings several benefits:

- The TEE is already present on mobile devices worldwide, there are no additional hardware requirements for the service provider or user.
- The TEE provides a higher level of security than the Rich OS, and better performance than a SE.
- The TEE and TEE APIs are standardized, so the behavior of the TEE is consistent and platform agnostic.

This white paper describes the current state of affairs in Premium Content and its security, and identifies opportunities for Premium Content providers to leverage the TEE for accelerated time to market, reduced content risk, and lower deployment costs based on a trusted standard for platform security.

SECTION 1: Challenges with Premium Content Distribution in the Media Market

The rapid evolution of Premium Content distribution within the media market has raised new security concerns. Understanding these changes and associated concerns is a necessary prerequisite to leveraging the TEE to resolve them.

1.1 Major Changes in Premium Content Distribution

Over the last several decades, technological advances have dramatically expanded the channels for delivering Premium Content to consumers. From the very beginnings of motion pictures, technology has shaped and changed how they reach viewers. Initially, movies could only be seen on the big screen. Then they could be enjoyed on the small screen at home, first in ad-supported television and then through pay TV services, made possible by cable and satellite technologies. More recent decades have seen the advent of physical media like VHS, DVD, and Blu-ray, which enabled new sales and rental business models. Today, the transition to digital distribution is already at an advanced stage, with Internet streaming and download delivering Premium Content to a wide range of home and personal devices.

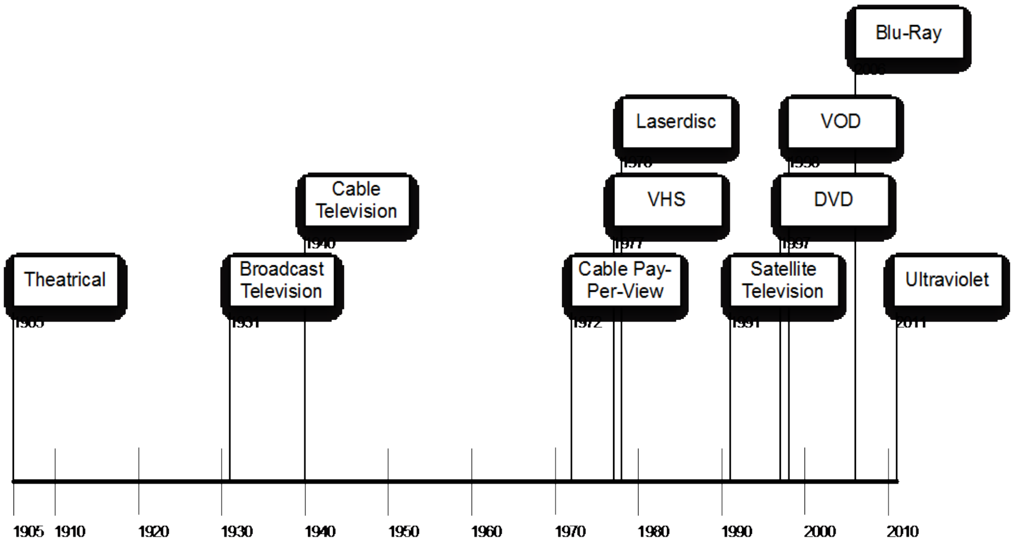

Figure 1: Timeline of Major Premium Content Distribution Formats

As part of this move to Internet distribution, the traditional Multichannel Video Programming Distributors (MVPDs) – the cable and satellite providers – have had to move quickly to provide mobile and web-based applications for viewing. Internet video technologies have also given rise to the new class of Internet Protocol Television (IPTV) MVPDs.

In addition, entirely new classes of distributors have arisen. They are frequently referred to as Over-The-Top (OTT) providers or Online Video Providers (OVPs). The face of this new industry is characterized by major brands such as Amazon Instant Video, Apple iTunes, Google Play, Hulu, Microsoft Xbox, Netflix, and Sony PlayStation.

With the introduction of movies on ad-supported TV, this new distribution channel changed the movie distribution model, and led to the creation of different release windows. In the standard release model, movies are first released through movie theaters (theatrical window), followed by physical media and rental, via Blu-ray and DVD (video window), then Transactional Video On Demand (TVOD). These are followed by Pay TV, then Subscription Video On Demand (SVOD), including OTT subscription services. Some movies eventually come to ad-supported distribution, either online or via cable, satellite, or broadcast channels. Very early digital windows before Blu-ray, sometimes called Super Premium Video On Demand (SPVOD), are also emerging. Episodic content distribution has a simpler windowing structure, but uses many of the same distribution technologies.

Another dimension is the quality of the content, which has also increased dramatically as video has evolved from low-resolution analog transmission to digital formats ranging from Standard Definition (SD) to High Definition (HD) and Ultra High Definition (UHD/4K) video, which can also include more vivid color and dynamic range. Generally the value of Premium Content is higher when it is in an earlier release window and when it is higher quality.

This explosion of technologies, devices, operators, and business models has created new opportunities for consumers to enjoy content on more devices, in more places, and with greater convenience and flexibility than ever before. But it also poses significant challenges to content distribution.

1.2 Distribution Challenges

When theaters and over the air television were the main distribution channels, copying and redistributing video content was technically difficult, as it required expensive and specialized equipment. Recordable media made this somewhat easier. But with digital files and the Internet, it has never been easier to create high quality copies and to redistribute them with or without a license from the content creator. The same technologies that have enabled a revolution of quality and convenience in video delivery have also dramatically expanded the problem of unlicensed distribution.

Piracy is a complex problem, with many legal and social facets and no single solution. But technology has been key in limiting the damage it causes. Although the layman's perception of content protection technology is that it is intended to stop all piracy, in reality content protection is a cost-recovery and risk-mitigation program intended to reduce the financial damage caused by piracy. A major goal is to make the official products and services more attractive and competitive than their pirate counterparts. Content protection is one tool that helps by reducing the quality, reliability, and availability of pirated products. It is also important in maintaining a visible distinction to the consumer between legitimate and illegitimate services.

Piracy has traditionally been split into two groups: 1) Consumers who distribute content casually between acquaintances, and 2) Organizations that create counterfeit goods or services for profit, such as authentic looking DVDs or Pay TV descramblers. This latter group has been the main problem for the content industry. But with the advent of online file sharing services and video streaming sites, a single posting of a video, at virtually no cost, can seed its unlicensed distribution on a massive scale. These technological advancements have dramatically altered the scale and impact of video piracy over the last decade.

The historical evolution of the premium video ecosystem has created four major technological silos for content protection: theatrical, pay television, physical media, and online distribution. Broadcast television, when distributed through a MVPD, has its own content protection schemes in the form of proprietary Conditional Access Systems (CAS). Physical distribution through VHS, DVD, and Blu-ray has been protected by a number of proprietary and standard content protection schemes that have varied by format, such as Macrovision Analog Content Protection (ACP) for VHS, DVD Content Scramble System (CSS), and Blu-ray Advanced Access Content System (AACS). Online distribution is marked by a distinct lack of content protection standards, with content owners and distributors negotiating the rights to use Digital Rights Management (DRM) content protection schemes on a case-by-case basis. Over the last several years, many standards organizations have attempted to reconcile the heterogeneity of online DRM, most notably Ultraviolet, which selected six DRM schemes as part of their standard: Microsoft PlayReady, Adobe Primetime, Google Widevine, Marlin, OMA CMLA-OMA v2, and DivX Plus. Other initiatives, such as the Secure Content Storage Association (SCSA), hold promise to help further reduce the problem.

With the major changes in Premium Content distribution – new distribution channels, content protection formats, and the proliferation of heterogeneous consumer electronics devices – the use of content protection has become increasingly complex and difficult to manage. When Pay TV operators started employing content protection to prevent theft of service, there was a clear chain of responsibility and interest. Both the content provider and the service provider had a financial interest in preventing unlicensed distribution. The content provider could require the service operator to protect the content, and the service operator usually owned and specified the design of the receiver and its Conditional Access System. In the case of digital cinema on physical media, such as DVD and Blu-ray, devices were 'purpose built' to play the format. And so industry consortia could develop and specify specific content protection systems. In all these cases, there was a clear chain of privity from the content owner through the operator or consortium to the manufacturer and its implementation of the content protection system.

Over-The-Top (OTT) delivery has radically changed and complicated content protection. Unlike audio and video, where there are industry-wide standards that drive hardware and software implementations, there are no industry-wide standards for content protection. Each individual service operator can choose one or more content protection schemes, which then need to be implemented across a broad range of devices. This involves significant effort and business overhead, since often the design and specification of the device, its operating system, and the content protection system(s) it supports are not under the control of the video service operator. The device (e.g. tablet, phone, TV, laptop, or set-top box) may be designed by one company; the operating system by another; and the content protection system by a third. Unlike traditional Pay TV, none of these companies necessarily build to the specific requirements of the video service operator, of which there may be many for any device. Without an agreed upon standard from an industry consortium that includes content owners and some compliance or certification process (like Blu-ray or UltraViolet), each service operator must have its content protection approved by each content owner, potentially for each new class of devices and content. This creates a combinatorial explosion in the number of individual content protection implementations that must be developed, maintained, and approved. The resulting overhead unnecessarily slows the deployment of new video services and distribution channels.

With all of the above content protection schemes, it is not only important to prevent content from being made available outside of its intended use, but it is also important to be able to monitor, report, and resolve the unlicensed distribution of content. In this regard, technologies such as forensic watermarking are important as an end-to-end content protection ecosystem because they can allow security compromises to be identified and addressed.

Additionally, all forms of content protection are subject to the “analog hole” – the ability to record content as it is rendered to a screen using a camcorder or other device. The threat has been seen mostly in theatrical distribution, where it led to the inclusion of forensic watermarking in the specification for digital cinema equipment. This allows the determination of the date and location of the recording. Also, the use of camcorders to create copies can indicate a system’s success at protecting the pristine digital version, while lowering the quality of pirated copies, thereby decreasing their value compared with the legitimate product.

The fragmentation of content protection technologies across different distribution channels, business models, formats, and devices, along with the requirement for on-going enforcement, creates a number of serious problems for content owners. Every content protection scheme must be evaluated for its level of protection and its applicability to various business rules:

- One or more approved content protection schemes must be approved for use with each distributor.
- Root-of-trust infrastructure and rights must be managed on an ongoing basis.
- Security must constantly be re-evaluated to ensure that content remains safe.
- Policing must be provided on an ongoing basis.

Addressing each of these points in a fragmented ecosystem is not just a costly affair, but creates risks and liabilities due to technical differences and lack of resources.

The end result is that the fragmentation of the content protection ecosystem, which is only becoming more severe with the major changes underway in Premium Content distribution, creates an undue burden on all members of the distribution chain. Of equal importance, it does not achieve the level of security that is both desirable and technically possible. The impact is noticeable for Consumer Electronic Equipment Manufacturers (CE OEMs) and software developers; both end up needing to develop and maintain support for multiple content protection schemes to receive content from multiple distribution channels – each of which has different requirements and implementations.

1.3 The Importance of TEE and Certification

The GlobalPlatform Trusted Execution Environment (TEE) provides a critical solution for content owners, distributors, and device manufacturers. Although it does not fully address all issues surrounding evaluation, negotiation, enforcement, and implementation, it reduces them significantly – especially as it is backed by a common certification program.

Evaluation of which content protection schemes are sufficient becomes much easier with a common platform for content protection. The GlobalPlatform certification program, with pre-defined threat vectors and a well-known Protection Profile, establishes a baseline of security and reliability for all content protection schemes and significantly reduces the per-scheme evaluation that must be done. In addition, the maintenance of security becomes much simpler as threat vectors and Protection Profiles can be updated when new attacks are uncovered.

Simplified evaluation and maintenance leads to simplified contract negotiations, where studios and distributors can quickly agree on new and existing content protection schemes and compare their security against a common baseline established by a TEE. By either noting or requiring that a content protection scheme relies on TEE certification, a level of trust and an understanding of risk can quickly be established without protracted conversations and technical evaluations.

Certification can also play an important role in enforcement, where a portion of the certification program can be dedicated to ensuring a correct implementation of forensic watermarking schemes. Enforcement lowers the overhead of ensuring that these technologies are implemented on a device-by-device and format-by-format basis.

Finally, the implementation overhead for CE OEMs and software developers is significantly reduced. With a common platform for multiple content protection schemes, more software and hardware is common to multiple implementations, lowering time to market and engineering costs.

Overall, the GlobalPlatform TEE and an associated certification can bring a degree of unification and efficiency to the fragmented and diverging Premium Content ecosystem.

SECTION 2: Understanding GlobalPlatform's Trusted Execution Environment

As the market has evolved—from smart cards at GlobalPlatform's inception to mobile and other devices today—GlobalPlatform has evolved its specifications to adapt to market needs. Understanding the TEE and how it is applicable in the area of Premium Content requires understanding, briefly, the evolution of GlobalPlatform's specifications:

GlobalPlatform specifications address three main areas: Messaging, Secure Element (SE), and Trusted Execution Environment (TEE).

- Messaging specifications define the roles and responsibilities of systems in a secure chip infrastructure, and develop a standard for information exchange.[1]
- The Secure Element is a tamper-resistant platform capable of securing applications and their confidential and cryptographic data.[2]
- The TEE is an isolated execution environment that runs alongside a Rich OS and hosts trusted services offered to that rich environment. The TEE offers an execution space that provides a higher level of security than a Rich OS, and delivers performance that is sufficient for most applications.

In 2010, GlobalPlatform pioneered the concept of the Trusted Execution Environment (TEE). The effort was initiated in response to changes in the mobile market: As consumers began using mobile devices to conduct financial and payment transactions, there was a need for enhanced security. Subsequently, as consumers increased their consumption of video, music, and other media on multiple devices, it became apparent that outdated ways of protecting content were insufficient in a world with multiple devices, an open distribution environment, and privacy concerns. The TEE has since become the mobile industry's best way of meeting various stakeholder needs while ensuring content security.

These security needs are complicated by the fact that new devices employ an open environment, including an operating system that allows users to add or delete applications. The user obviously enjoys the flexibility of such a model, but such user control impacts the security and stability of the device, thereby making it vulnerable to malware or other attacks. To protect their Premium Content from theft, content owners and rights holders have traditionally made use of content protection, Digital Rights Management (DRM), or Conditional Access (CA). Such schemes often favor hardware-strengthened content protection, and today they must operate within an environment that has an increasing number of actors.

In addition, the proliferation of ways that content is distributed (including 3G, 4G, Wi-Fi, WiMAX, Bluetooth, and Near Field Communication (NFC)) increases the pressure to ensure that all communication methods securely handle the content being distributed and consumed.

Consider the following (often competing) priorities of actors involved in media distribution and consumption in today's market:

- Content Owners/Rights Holders – While they wish to ensure that consumers can get access to content as easily as possible, guaranteeing content security is paramount to ensuring long-term business success.
- Consumers – Ease of use and flexibility are the primary drivers for consumers, who wish to retain control over their devices, consume media when and where they want it, and make use of new services as they become available.

[1] See http://www.globalplatform.org/mediaguideMobileMessage.asp.
[2] See http://www.globalplatform.org/mediaguideSE.asp.

- Device Manufacturers – Device trustworthiness is critical, but devices must meet the needs of operators, service providers, consumers, and more. Delays in certifying or launching products would negatively impact their business.
- Platform Providers and Silicon Vendors – While they compete on various features (security and reliability included), they are concerned about interoperability as it enables their products to be leveraged across different end products and industries.
- Operating System (OS) and Application Developers – Often the objective is to deploy applications or an OS to as many devices and environments as possible. There is a need to balance security with the consumer's desire for flexibility.
- Mobile Network Operators (MNOs) – The use of a UICC (usually owned and managed by the MNO) is appropriate for deploying certain services, but some applications exceed the resource capabilities of the UICC. These applications need a higher level of security than the Rich OS offers in order to protect the assets of the MNO and their partners, as well as their customers' information.

To meet the security and market needs of these diverse industry participants, GlobalPlatform introduced the TEE, which it defined as "an isolated execution environment that runs alongside the Rich OS and provides security services to that rich environment."[3] By isolating access to the TEE's hardware and software security resources—and keeping these separate from the Rich OS and its applications—the TEE enables safe execution of authorized security software, which GlobalPlatform terms Trusted Applications (TAs). These Trusted Applications are kept independent from one another and are prevented from accessing each other's security resources, which is accomplished using the TEE Internal APIs and the TEE Client API.

The TEE offers an exceptional balance by allowing for greater security than a Rich OS environment while offering greater functionality than the Secure Element (SE). Therefore, the TEE is the ideal solution for meeting the security requirements of Premium Content providers. Figure 2, which can also be found in GlobalPlatform's TEE White Paper, illustrates the TEE architecture.

[3] "The Trusted Execution Environment: Delivering Enhanced Security at a Lower Cost to the Mobile Market." Published by GlobalPlatform's Device Committee and Trusted Execution Environment Task Force. Read the full TEE White Paper.

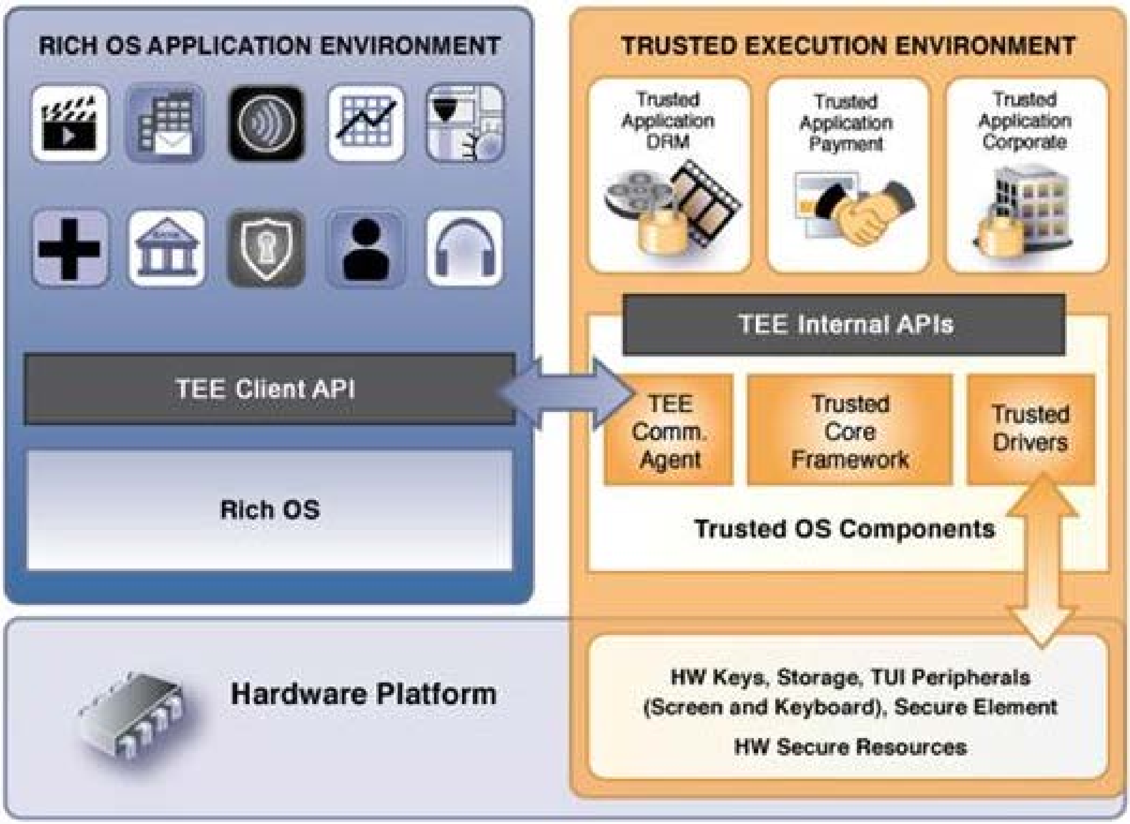
RICH OS APPLICATION ENVIRONMENT
TRUSTED EXECUTION ENVIRONMENT
Trusted Application DRM
Trusted Application Payment
Trusted Application Corporate
TEE Internal APIs
TEE Client API
TEE Comm. Agent
Trusted Core Framework
Trusted Drivers
Rich OS
Trusted OS Components
Hardware Platform
HW Keys, Storage, TUI Peripherals (Screen and Keyboard), Secure Element
HW Secure Resources

Figure 2: Architecture of the TEE

While the technologies available via the TEE offer an obvious path to content protection for content owners and rights holders, there are two additional requirements to ensure that the solution is complete. First, the TEE should be standardized, as opposed to proprietary, to avoid fragmentation. A standardized TEE solution enables unified implementation, simplified deployment and assurances of interoperability. The second requirement—a certification program—is critical to ensure that the TEE is indeed *trusted*.

Some within the media industry have purported to provide solutions within the framework of a “Trusted Execution Environment.” Without a certification program in place to ensure that devices are interoperable and that applications are indeed trusted, such a TEE could be an inadequate solution. To protect Premium Content within the media industry, what is needed is a true implementation of GlobalPlatform’s TEE—standardized and with accompanying certification—to create what some have redundantly referred to as a “*Trusted* TEE.”

SECTION 3: Certification: The Path to Assurance for TEEs

Certification is a critical requirement to ensure that the TEE is interoperable across devices and applications and delivers the promised security for Premium Content.

While standardizing TEE-related programming interfaces (see section 4) will ensure the interoperability of implementations across devices and applications, it is critical to underscore that the key value proposition of the TEE is to bring security to “open” devices. As discussed above, a TEE must truly be *trusted* across open devices for its impact to be felt across the industry.

A robust certification process is necessary to qualify the TEE against a range of threats and attacks; the sophistication of this process must match the value of the assets and media content being protected by the TEE.

3.1 The Threat Model

With the proliferation of mobile devices, there has been an increase in hacking attempts targeting flagship smartphones. The hackers hope to “break once, exploit many,” meaning that identifying a vulnerability in a particular device enables them to exploit thousands or hundreds of thousands of devices.

There are several types of attackers, each with different motivations for seeking to break devices. Some hope to find vulnerabilities that end-users can exploit to gain privileges and capabilities. Jailbreaking and rooting are examples of such attacks. Other attack types include attacks based on intercepting communication (SMS, MMS, GSM, Wi-Fi, and Bluetooth), installing malicious software (virus, Trojan, spyware), and password cracking.

When it comes to finding a vulnerability, skilled attackers may go as far as dumping the ROM of a chipset, using advanced fuzzing tools to find abnormal TEE implementation behavior, or spying on external buses to monitor or intentionally inject data into the exchanges between the chipset and external memory. As underlined above, the interest is most intense if the vulnerability can then be exploited simply on many devices, without all the skills, time, and equipment necessary to uncover it.

The TEE security model was developed in such a way that it is directly applicable to the dominant threats within the mobile space. The purpose of the TEE is to isolate sensitive services from the main system in a device (which can be corrupted); these sensitive services are subsequently handled within the TEE’s secure environment.

Certifying the TEE is necessary to ensure that it conforms to specifications and is robust and effective against such attacks.

3.2 TEE Security Features for Content Protection

A compliant TEE will provide a set of capabilities for the platform that may be evaluated objectively against the TEE Protection Profile to ensure that the TEE adequately protects the platform’s security assets. Applications that are clients of the TEE (of which Content Protection applications are an example) use those capabilities to achieve their own security objectives.

Content Protection methodologies define their security objectives in a slightly different way: typically, they define a set of assets that need to be protected and specify a set of robustness and compliance criteria that implementations must achieve to satisfy those criteria. So it is logical to ask: Does a compliant TEE provide sufficient capabilities to meet the compliance and robustness criteria of Content Protection schemes?

To answer this question, consider an inventory of the capabilities provided in a compliant TEE. This list is adapted from the GlobalPlatform TEE Protection Profile, with some simplifications and omissions to make it more relevant for this discussion. Next, it is necessary to identify a set of capabilities required in a modern Content Protection scheme. This list is based on a compendium of robustness and compliance criteria from many current Content Protection schemes (e.g. HDCP and PlayReady), and the MovieLabs Specification for Enhanced Content Protection (ECP)[4]. The MovieLabs requirements have been chosen, in particular, because they signal the direction that many major content producers and owners wish to see Content Protection methodologies move in the near future.

Consider the following high-level illustration of how TEE capabilities meet the MovieLabs Content Protection requirements:

- Encryption – While the requirements specify support for an AES-128 stream cypher and a true random number generator, the TEE exceeds those requirements by providing additional cypher support along with a suite of cryptographic services.
- Attack Resistant – The requirement for resisting software attacks (e.g. device rooting, debuggers) and moderate physical attacks (e.g. fuzzing, clock and I/O glitching, bus analyzers) is met through the TEE's capabilities of secure application delivery, integrity checking, secure (or disabled) debugging, secure application management, and isolation between Trusted Applications (TAs).
- Secure Storage – There is a direct mapping between the Content Protection requirements for secure storage and the TEE's ability to provide secure storage.
- Secure Time – Many of the Content Protection requirements for secure time are met through the TEE's secure clock capabilities. (See note below about optional support for rollback.)
- Code Confidential – The TEE exceeds the requirement for confidential code by having its own requirements for an end-to-end development environment that is consistent with the sensitivity of security applications.
- Secure Environment – The basic Content Protection requirements of runtime integrity checking and protected memory are just a subset of the capabilities of the TEE to provide a secure and trusted execution environment.

For a detailed analysis of how TEE capabilities compare to Content Protection requirements, refer to Appendix A: TEE Features. The table in that appendix indicates the requirements that are fully supported by the TEE. These include most of the generic (non-MovieLabs) requirements (identified in the appendix by the prefix "RG"). Secure time requirements are widely specified, suggesting that although this is an optional feature in GlobalPlatform TEE specifications, suitable TEE implementations must implement this optional feature. TEEs that do not implement anti-rollback support will impose that obligation on the Content Protection TAs that do require it.

Some requirements for Content Protection systems are not implemented directly in the TEE: secure rendering, link protection (e.g. HDCP), watermarking, and Cinavia support. These are supported through a combination of TEE functionality, TA support, and third-party hardware support (e.g. HDMI implementations for HDCP).

[4] Motion Picture Laboratories, Inc. ("MovieLabs") is a non-profit 501(c)(6) research and development joint venture started by the six major motion picture studios. To learn more visit, http://www.movielabs.com/ngvideo/

The requirement for third-party certification is specified by MovieLabs, as it is in some other Content Protection systems. While a compliant TEE implementation that has itself undergone TEE certification can simplify and speed the certification of the Content Protection system relying on it, it is neither sufficient nor does it assure that the Content Protection implementation will attain its certification. Many content owners and stakeholders have clarified that TEE certification would have to be complemented by additional certification activities to reach certification of the Content Protection system, before authorizing distribution of their high value content to a particular implementation.

3.3 Certification Process

GlobalPlatform's initial activity in the area of TEE certification has involved the development and publication of a TEE Protection Profile. This follows the Common Criteria methodology and defines the following:

- The perimeter of what should be evaluated
- The product life cycle
- The assets (and their properties) that must be protected
- The security functionality it provides
- The threat model

The next step is to deduce a list of functional security requirements. The actual evaluation is carried out by an independent laboratory that is responsible for the following:

- Analyzing the product based on the Protection Profile
- Designing attacks against the product
- Reviewing the attacks to make sure that they are not more sophisticated than the security bar that has been chosen

The Protection Profile is ready to be used, so candidates can follow the standard certification process as stipulated by Common Criteria and work with national bodies that fully recognize the TEE Protection Profile. Additionally, GlobalPlatform is creating its own certification process, which complements the Common Criteria option in order to extend the geographic coverage for TEE certification. Starting in late 2015 or early 2016, candidates to certification will thus be able to choose an evaluation facility qualified by GlobalPlatform.

With a wealth of options being offered to stakeholders that wish to be certified, GlobalPlatform will also issue a unifying TEE certification stamp to TEEs certified using either option, thus bringing consistency across the different certification paths. Leveraging a single scheme for certification, with several certification paths underneath, will ensure that certified devices have met the same standards, which in turn will increase interoperability and security.

SECTION 4: The Case for Standardizing the TEE

Previous sections have focused on defining the TEE and discussing its applicability within the media industry. However, proprietary TEEs, even supported by a robust certification process that addresses the concerns outlined in section 3, fall short of delivering what the market requires; only some of the benefits of a TEE would be achieved with proprietary solutions. Standardization is key to avoid fragmentation of APIs, which would lead to the proliferation of non-compatible, proprietary solutions. Were this to occur, the market would be plagued by higher costs, the need for specialized skills for each development project, and longer time-to-market.

In order for the TEE to be a complete solution it needs to be standardized, as well as certified.

4.1 Before the TEE: Plug-Ins—and Problems that Follow

Within today's market there are already several software-based solutions that are either pre-integrated with the platform or downloaded as a browser plug-in. For example, PlayReady DRM is tightly integrated with Silverlight and downloaded as the browser plug-in. A number of these solutions use code obfuscation and validation, as well as other code-based anti-tampering mechanisms. The DRM module, downloaded either as a browser plug-in or by using another secure delivery mechanism, is installed in the secure area of the platform. However, while there are benefits of this approach (mostly related to convenience), the media industry requires a more robust solution for high-value Premium Content Protection.

The market has hardware-based mechanisms available to protect Premium Content, but these use OEM and DRM vendor-specific proprietary solutions. The compliance and robustness requirements of such implementations are typically enforced by the trust management authority managed by the corresponding DRM vendors. A majority of such implementations use tamper-resistant hardware to protect DRM secrets. While this approach works, it causes market fragmentation due to the proprietary nature of solutions. It also complicates matters for OEMs since they need to customize solutions for different markets and platforms. They also need to have their products certified by the Trust Management Organizations that have been approved or managed by various DRM vendors. The absence of a single certification body muddles the process for service providers.

Only GlobalPlatform's TEE model combines the flexibility of software-based solutions, the robustness of hardware-based solutions, and the convenience of a single certification body.

4.2 Benefits of Standardizing via GlobalPlatform's TEE

TEE standardization based on GlobalPlatform specifications will enable simpler and unified implementations that allow different stakeholders to interact in ways that would be impossible if the market were to be dominated by proprietary solutions. Furthermore, standardization provides a clear path to certification, which, as discussed in section 3, is critical to ensure that a TEE is in fact *trusted*.

In order to protect Premium Content, it is essential that TEE security certification meets the media industry's baseline requirements for compliance and robustness. It should be noted that a particular content distribution ecosystem or DRM vendor might require additional certification on top of the baseline security certification provided by the GlobalPlatform TEE certification.

There are two possible ways to leverage the TEE to support Premium Content Protection:

1. Implementing one or more DRM solutions within the TEE at the time of manufacture.
2. Using GlobalPlatform's remote management mechanism to download the DRM solution supported by a particular service provider or ecosystem within the secure, trusted platform provided by the TEE.

The first solution can be implemented in a controlled fashion at the time of manufacture. However, it may be a costly solution for OEMs since it requires them either to support multiple DRM solutions, or to limit the market of a device by supporting only the specific Content Protection needs of a particular market or service provider. Furthermore, it limits the ability of service providers to broaden their customer base after device release.

The second solution, using GlobalPlatform's remote management mechanism, provides more flexibility since a single secure, trusted platform can be leveraged across different service providers and ecosystems. OEMs benefit because they only need to certify their devices once—through GlobalPlatform—as having met the baseline security requirements. The cost of additional service provider certifications (if any) should be minimal, and OEMs further benefit by not having to implement multiple DRMs or proprietary solutions for various markets and platforms.

This remote management solution does require service providers to ensure that their DRM agent has been successfully installed in the TEE. Specifically, the additional requirements include the following:

1. Service providers need to formulate rules regarding the download code that specifies where the DRM can run in the device.
2. Service providers must be able to remotely attest to the integrity of the installed media application—including the media player and DRM agent. Furthermore, they should be able to remotely monitor and attest to the dynamic run-time behavior of the media application.

With these two additional requirements, service providers will benefit from the implementation of a remote management-oriented TEE model since they can provide service to a wider subscriber base. The downloadable model further provides for improved risk management, where piracy can be prevented by updating the DRM module in the event of a security breach or detection of a security vulnerability. Figure 3 below illustrates a DRM implementation using a GlobalPlatform TEE model with remote management.

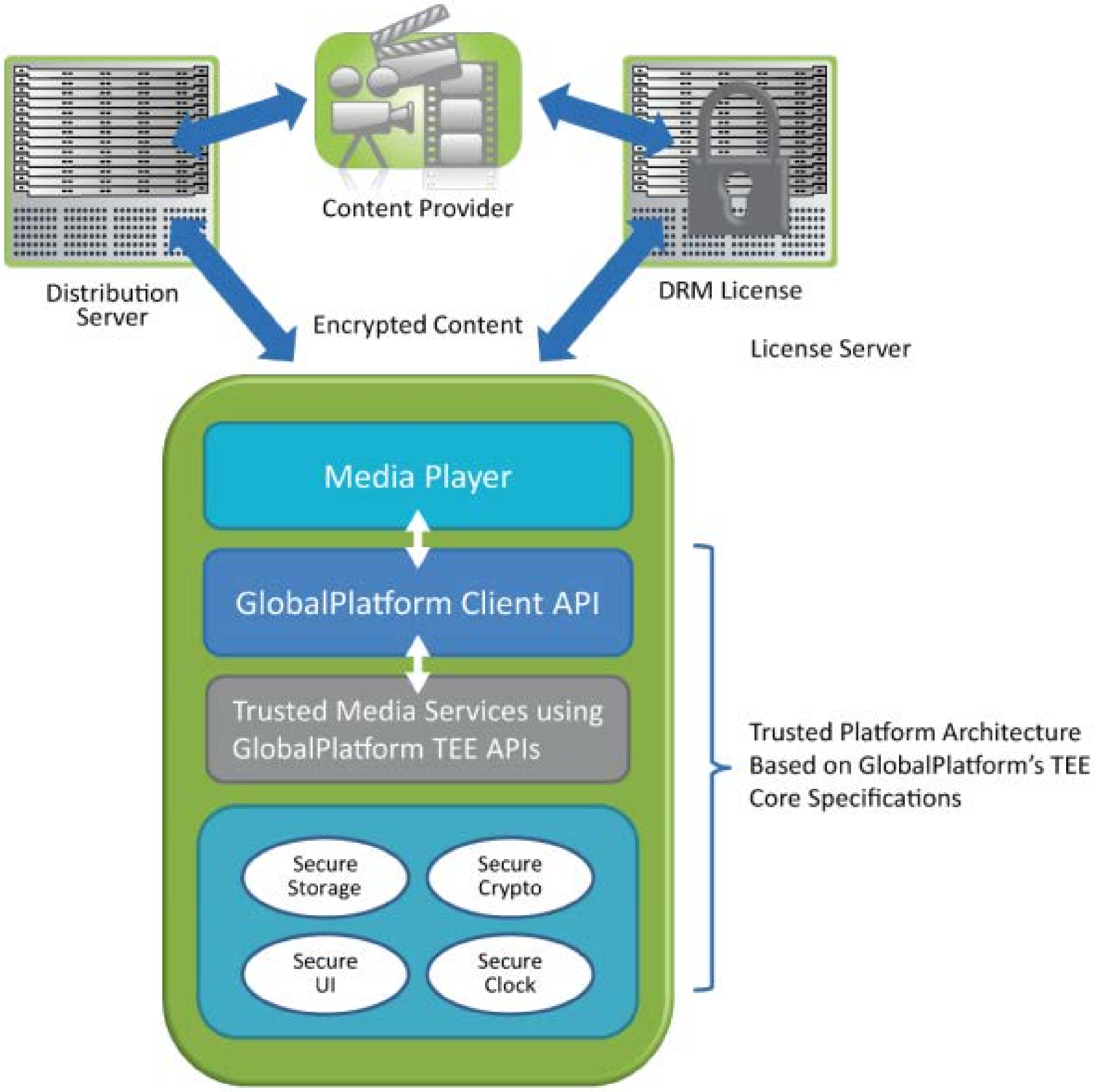
Content Provider
Distribution Server
DRM License
Encrypted Content
License Server
Media Player
GlobalPlatform Client API
Trusted Media Services using GlobalPlatform TEE APIs
Secure Storage
Secure Crypto
Secure UI
Secure Clock
Trusted Platform Architecture Based on GlobalPlatform's TEE Core Specifications

Figure 3: A DRM Implementation Using GlobalPlatform's TEE

4.3 How the TEE Supports Different Devices & Different Markets

Not only does use of a standardized TEE simplify deployment and improve interoperability across various platforms, it also enables the baseline security requirements of multiple devices and markets to be met via a single TEE certification authority. Even with incremental certification requirements (e.g. market- or vendor-specific), standardization improves time to market for OEMs and reduces development and support needs for service providers.

Furthermore, use of standardized APIs enables service providers to reach a wider audience or subscriber base. In this model, users would have the freedom to purchase a GlobalPlatform-certified device and subsequently download and install the DRM Module (along with the multimedia application) on the GlobalPlatform-certified TEE in the device.

4.4 TEE Positioning in Trusted Media Playback Platform & Parallel Standards Efforts

There are other industry efforts underway to improve Premium Content Protection, and it is valuable to understand how GlobalPlatform's TEE complements these initiatives.

Figure 4 illustrates a typical trusted end-to-end video rendering path. A media player downloads or streams encrypted media content hosted by a content distribution server. The content is then decrypted and decoded by a content decryption module in the device. The content is then re-encrypted using a link protection system such as HDCP for display on a monitor device.

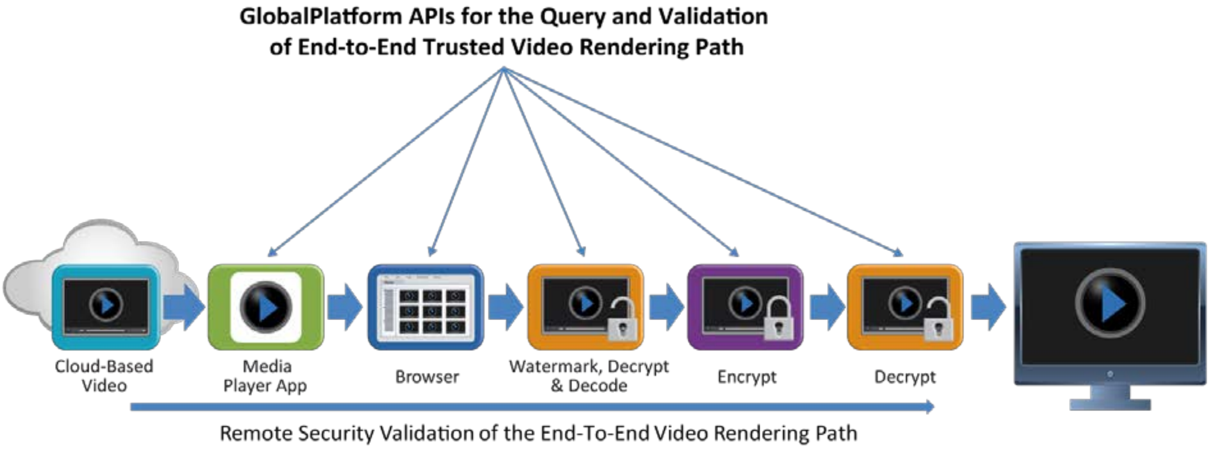
GlobalPlatform APIs for the Query and Validation
of End-to-End Trusted Video Rendering Path
Cloud-Based Video
Media Player App
Browser
Watermark, Decrypt & Decode
Encrypt
Decrypt
Remote Security Validation of the End-To-End Video Rendering Path

Figure 4: A Typical Trusted End-To-End Video Rendering Path

Introducing a GlobalPlatform TEE as part of the Trusted Media Playback platform provides an isolated secure execution environment that can be leveraged whenever valuable assets need to be accessed in the end-to-end video rendering path. The TEE plays the following roles in providing an end-to-end trusted video path:

1. It enables robust DRM implementation to protect assets such as the following:
    a. DRM Application Secrets and Keys
    b. License Storage and Management
    c. Usage Policy
    d. Account Information
2. It interfaces with other components/modules, whether secure or unsecure.
    a. It aids with media playback, scheduling, and rendering.
    b. It makes possible the secure download of DRM modules, as well as integration with the media player.
3. It integrates with a large number of application layers, such as HTML5.
4. It provides static and dynamic attestation information for the remote validation of the video rendering path.

While the TEE brings several benefits to the media industry, it is crucial that GlobalPlatform APIs for supporting premium media applications interface with media APIs being developed by W3C to enable playback of the protected content.[5] The W3C HTML Working Group is currently developing HTML Media Extensions for the support of Interoperable Commercial Web Media Services. There are two main developments within W3C regarding the delivery of commercial video to consumers over the web:

- Encrypted Media Extensions (EME): These HTML Media Extensions extend the HTML Media Element to enable playback of the protected content.
- Media Source Extensions (MSE): These HTML Media Extensions extend the HTML Media Element to facilitate use cases like adaptive streaming and time-shifted live streams.

For a standardized TEE implementation to deliver the maximum possible value to the media industry, it must be accompanied by standardized interfaces to Web Media Services, which will facilitate the download and installation of Content Protection solutions and Web Media applications in the TEE-enabled platform.

[5] W3C is a worldwide community working together to develop Web standards, and its work extends to media APIs. To learn more, visit http://www.w3.org/.

Conclusion: A Call To Action

Premium Content providers and vendors of DRM and CA solutions share common goals of accelerating time to market while reducing security risks and increasing return on investment. Meeting these goals has become increasingly challenging over the last decade as the number of content formats and distribution channels has not only expanded, but seems to be accelerating in its fragmentation. The costs of piracy are high, and with 4K content being put into distribution the stakes have never been higher. Recent specifications from MovieLabs identify the requirements for securing content, not only as it is stored in a device but also as it is rendered to the screen.

The Trusted Execution Environment meets the needs of Premium Content providers, and is already trusted by financial institutions, mobile network operators, and other organizations that view security as essential to their livelihood. Now is the time to expand the role of the TEE to ensure that Premium Content can be securely distributed and rendered based on well-understood specifications and a related certification process. With the participation of both Premium Content providers and technology vendors, Premium Content can finally be both secure and widely available in the formats and distribution channels of a Premium Content owner’s choosing.

All feedback is welcome, and all comments or questions may be submitted to secretariat@globalplatform.org.

Appendix A: TEE Features

This appendix provides a detailed analysis of the mapping of TEE features to Content Protection requirements. It contains three tables: TEE capabilities, Content Protection requirements, and a mapping between TEE capabilities and Content Protection requirements.

A.1 TEE Capabilities

TEE Capability	**Description**
C.CA_TA_IDENTIFICATION	TEE server applications provide means to strongly bind a TEE service instance to its client application instance (so that the server cannot be hijacked).
C.CRYPTOGRAPHY	The TEE provides cryptographic services for clients that include enforcement of key usage policies.
C.DEBUG	The TEE either permanently disables debugging in the TEE or requires strong authentication of the request to enable debugging.
C.DEVICE_ID	The TEE provides unique device identity suitable for use in cryptographic identification and authentication protocols.
C.INITIALIZATION	The TEE provides robust integrity protection starting from each system boot operation.
C.INSTANCE_TIME	The TEE provides monotonically increasing time at each instantiation.
C.INTEGRATION_CONFIGURATION	If the TEE implements the GlobalPlatform specifications.
C.MANAGEMENT	The TEE will only install, load, or delete TAs that are authentic and only within the limits of its management policy.
C.OPERATION	The TEE ensures correct operation of its security functions.
C.PROTECTION_AFTER_DELIVERY	The TEE must be installed and configured according to its manufacturer's policy and procedures.
C.RNG	The TEE provides a cryptographic quality random number generator.
C.ROLLBACK	Any TEE limitations on rollback protection are specified for TA developers to take into account.
C.ROLLBACK_PROTECTION (optional)	The TEE prevents replay of persistent data to previous versions if persistent time is provided.

TEE Capability	Description
C.RUNTIME_CONFIDENTIALITY	The TEE protects the confidentiality of sensitive runtime data.
C.RUNTIME_INTEGRITY	The TEE provides runtime integrity assurance of its operation and sensitive data used by it.
C.SECRETS	Personalization data that exists outside the TEE (e.g. in manufacturing) must be handled securely.
C.TA_DEVELOPMENT	TA development must be done in a manner consistent with the security sensitive nature of end use.
C.TA_ISOLATION	The TEE isolates TAs from each other.
C.TA_PERSISTENT_TIME (optional)	The TEE may provide persistent monotonic time across TEE resets.
C.TEE_DATA_PROTECTION	The TEE provides secure storage of persistent data to assure authenticity, consistency, and confidentiality.
C.TEE_FIRMWARE_UPGRADE	The TEE provides a trusted firmware upgrade methodology.
C.TEE_ISOLATION	The TEE protects itself from unauthorized access from outside and from TAs resident within it.
C.TRUSTED_STORAGE	The TEE provides means for Trusted Storage.
C.UNIQUE_DEVICE_ID	The Device Unique Identifier is a statistically unique value.

A.2 Content Protection Requirements

The Content Protection requirements are summarized in the following table. Requirements labelled with an RG prefix are generically (but not universally) common across the robustness and compliance criteria of many widely used Content Protection schemes. The other requirements come from the MovieLabs ECP document and are not widely satisfied in today's consumer-oriented Content Protection systems.

Requirement	**Description**
R.CERTIFIED	The device must be submitted for certification to an unspecified 3rd party authority.
R.CINAVIA	The device must support Cinavia playback controls on all content.
R.HARDWARE_ROT	The device must provide a securely provisioned RoT including a private DUK that is: usable for cryptography, but never visible to software (even in the TEE); usable for device identification and authentication purposes; and usable to create bound and enveloped storage.
R.LINK_PROTECTION	The device must provide HDCP 2.2 protection on output links for DRM content, and DRM content can only be output through protected links.
R.SECURE_ENVIRONMENT	The device must provide a secure processing environment (effectively a TEE) that includes: protected memory for secure processing; and runtime integrity checking of the TEE code.
R.SECURE_RENDER_PIPELINE	The media rendering pipeline must be secure from content decryption through display output.
R.WATERMARK	The device must be able to support forensic watermarking.
RG.ATTACK_RESISTANT	The device must resist software based attacks using commonly available tools and methods (e.g. device rooting, debuggers) and moderate physical attacks (e.g. fuzzing, clock and I/O glitching, bus analyzers).
RG.CODE_CONFIDENTIAL	The device must provide protection for secret algorithms and resist attempts to trace execution or modify the code.
RG.ENCRYPTION	The device must supply at least an AES stream cipher mode at 128 bits or higher and a True Random Number Generator; and must incorporate side channel analysis resistance.

Requirement	Description
RG.RENEWABLE	The device must support an upgrade path for software or firmware to allow compromised schemes to be healed.
RG.SECURE_STORAGE	The device must provide secure storage to ensure the confidentiality of secret data used in the protocol.
RG.SECURE_TIME	The device must provide secure monotonic time in any runtime instance.

A.3 TEE and Content Protection Requirements Mapping

And finally, a look at how the requirements map onto the capabilities:

Legend: √ - Requirement fully supported by TEE P – Partial support O – Optional support	RG.ENCRYPTION	RG.ATTACK_RESISTANT	RG.SECURE_STORAGE	RG.CODE_CONFIDENTIAL	RG.SECURE_TIME	R.SECURE_RENDER_PIPELINE	R.SECURE_ENVIRONMENT	R.HARDWARE_ROT	R.LINK_PROTECTION	R.WATERMARK	R.CINAVIA	RG.RENEWABLE	R.CERTIFIED
C.CA_TA_IDENTIFICATION		√					√						√
C.CRYPTOGRAPHY	√		√				√						√
C.DEVICE_ID							√	P					√
C.INITIALIZATION		√	√	O			√						√
C.INSTANCE_TIME					O		√						√
C.OPERATION							√						√
C.RNG	P						√						√
C.RUNTIME_CONFIDENTIALITY				√			√						√
C.RUNTIME_INTEGRITY		√					√						√
C.TA_ISOLATION		√					√						√
C.TEE_DATA_PROTECTION			√				√						√
C.TEE_FIRMWARE_UPGRADE		√					√					√	√
C.TEE_ISOLATION		√		√			√						√
C.TRUSTED_STORAGE			√				√						√
C.ROLLBACK_PROTECTION		O					√						√
C.TA_PERSISTENT_TIME					O		√						√

Legend: √ - Requirement fully supported by TEE P – Partial support O – Optional support	RG.ENCRYPTION	RG.ATTACK_RESISTANT	RG.SECURE_STORAGE	RG.CODE_CONFIDENTIAL	RG.SECURE_TIME	R.SECURE_RENDER_PIPELINE	R.SECURE_ENVIRONMENT	R.HARDWARE_ROT	R.LINK_PROTECTION	R.WATERMARK	R.CINAVIA	RG.RENEWABLE	R.CERTIFIED
C.DEBUG		√		√			√						√
C.INTEGRATION_ CONFIGURATION			√	√			√						√
C.MANAGEMENT		√					√					√	√
C.PROTECTION_AFTER_ DELIVERY		√	√				√						√
C.ROLLBACK		O					√						√
C.SECRETS		√	√				√						√
C.TA_DEVELOPMENT		√	√	√	O	√	√		√	√	√	√	√
C.TEE_FIRMWARE_UPGRADE							√					√	√
C.UNIQUE_DEVICE_ID							√	P		√			√

Appendix B: Definitions & Abbreviations

B.1 Definitions

Term	Definition
Content Protection	A cost-recovery and risk-mitigation program intended to reduce the financial damage caused by piracy.
Premium Content	Digital material that is downloaded for a fee, such as articles, images, audio books, music, movies, and TV shows.
Protection Profile	A document used as part of the certification process according to ISO/IEC 15408 and the Common Criteria (CC).
Rich Execution Environment	An environment that is provided and governed by a Rich OS, potentially in conjunction with other supporting operating systems; it is outside of the TEE, therefore, both the environment and the applications running on it are considered untrusted.
Rich OS	A High-Level Operating System (HLOS) environment with a rich capability set; allows consumers to download and run applications. Examples include Android™, Linux®, Symbian OS™, and Microsoft® Windows Phone 7®.
Secure Element	A tamper-resistant combination of hardware, software, and protocols capable of embedding smart card-grade applications. Typical implementations include UICC, embedded SE, and removable memory cards.
TEE Client API	A low-level communication interface designed to enable a client application running in a Rich OS to access and exchange data with a Trusted Application running inside a TEE.
TEE Internal APIs	APIs that offers client applications a set of Rich OS-friendly APIs that allow access to some TEE services, such as cryptography or secure storage.
Trusted Application	An application on a mobile or other electronic device that runs within a Trusted Execution Environment and provides security related functionality to other applications.
Trusted Execution Environment	An isolated execution environment that runs alongside the Rich OS. The TEE provides security services to that rich environment and isolates access to its hardware and software security resources from the Rich OS and its applications
Trusted TEE	A term increasingly used in the media industry to refer to a TEE that is interoperable and certified, this term is in fact a redundancy caused by market confusion over what a true TEE implementation requires and how certain market participants are misrepresenting themselves.

Term	Definition
W3C	An international community working together to develop Web standards. Its work extends to media APIs.

B.2 Abbreviations

Abbreviation	Meaning
AACS	Advanced Access Content System
ACP	Analog Content Protection
API	Application Programming Interface
CA	Conditional Access
CAS	Conditional Access Systems
CE OEMs	Consumer Electronic Equipment Manufacturers
CMLA	Content Management License Administrator
CSS	Content Scramble System
DRM	Digital Rights Management
DUK	Derived Unique Key
DVD	Digital Versatile Disc
EME	Encrypted Media Extensions
eSE	Embedded Secure Element
GSM	Global System for Mobile communication
HD	High Definition
HDCP	High-Bandwidth Digital Content Protection
HDMI	High-Definition Multimedia Interface
IPTV	Internet Protocol Television
MMS	Multimedia Messaging Service
MNO	Mobile Network Operator
MSE	Media Source Extensions
MVPD	Multichannel Video Programming Distributor
NFC	Near Field Communication

Abbreviation	Meaning
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OS	Operating System
OTT	Over-The-Top
OVP	Online Video Provider
RoT	Root of Trust
SCSA	Secure Content Storage Association
SD	Standard Definition
SE	Secure Element
SMS	Short Message Service
SPVOD	Super Premium Video on Demand
SVOD	Subscription Video On Demand
TA	Trusted Application
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TV	Television
TVOD	Transactional Video On Demand
UDP	User Datagram Protocol
UHD or 4K	Ultra High Definition
UICC	Universal Integrated Circuit Card
VHS	Video Home System
VOD	Video On Demand