PlayReady® SL3000 Playbook

Microsoft Corporation

20 February 2016

Table of Contents

1. Introduction

1.1.Scope

This document is intended to serve as a step-by-step guide for PlayReady Licensees seeking SL3000 Compliance for PlayReady Intermediate or Final Products. The document outlines the end-to-end process for Intermediate and Final Products and details the requirements for SL3000 Conformant Intermediate Products.

1.2.Document Organization

This document contains two main sections.

The **SL3000 Design Process** section outlines the end-to-end process to be followed by a PlayReady Licensee seeking SL3000 Compliance for an Intermediate Product or a PlayReady Final Product.

The **SL3000 Requirements** section details the requirements for SL3000 Conformant Intermediate Products. It is important, and required, that IPLs verify these requirements and document this verification for FPLs in a form of "checklist", because of the nature of the requirements: they're deep in the hardware and the TEE, and FPLs might not always be in the capacity of verifying these requirements themselves. The provided test report or checklist is a tool to use by IPLs so FPLs know what tests were already run and passed, and can confidently do the supplemental tests that verify the entire conformity of the Final Product.

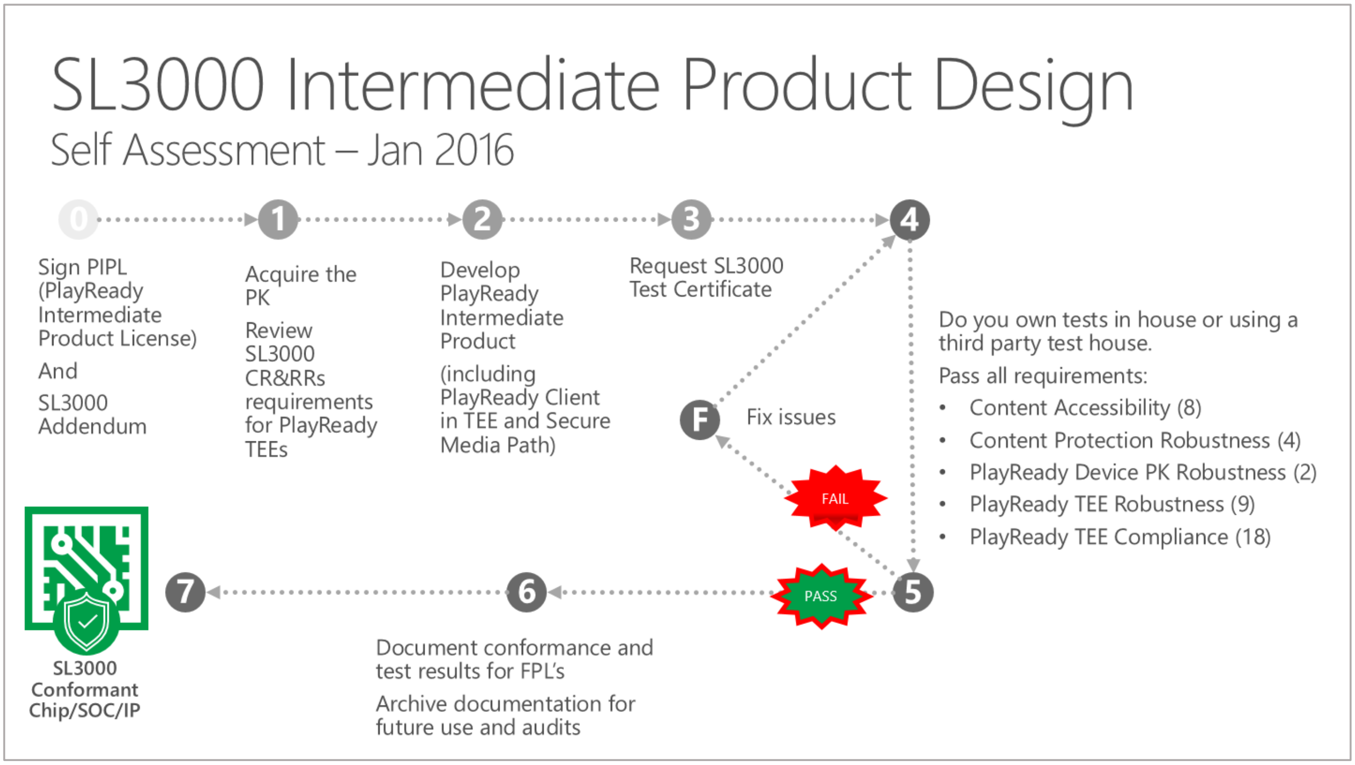
There is no such section detailing the requirements for Final Products, because FPLs make the final self-assessment of the Final Product that they distribute to end-users, and are not required to communicate their tests to anyone.

2. SL3000 Design Process Overview

A PlayReady Security Level is a publicly available and widely understood definition of robustness for PlayReady Products. While products may exceed the robustness requirements for a specific PlayReady Security Level, it establishes the minimum bar that must be met by a product in order to consume content requiring the defined level of protection. The PlayReady Compliance and Robustness Rules updated in April 2015 introduce the PlayReady Security Level 3000 (SL3000), and requirements for PlayReady TEE implementations to meet the hardware security requirements for PlayReady Enhanced Content Protection. PlayReady SL3000 is designed to be sufficient to meet the security standards for a wide range of content producers, including premium Hollywood content.

PlayReady SL3000 Self-Assessment is intended to assist PlayReady Licensees in obtaining distribution rights for UHD (4K), other types of Enhanced Content (e.g. HDR, 3D, etc.), and new Enhanced Content Delivery Models (e.g., early window).

The security of a PlayReady Product depends critically on the robustness of the PlayReady implementation. A security review, including hardware and firmware, is required for Intermediate Products to qualify for SL3000. The security review is based on the SL3000 Requirements, outlined in Section 4 of this document. This security review must be documented, and the documentation communicated to companies building a Final Products based on this Intermediate Product. This security review can be conducted by a third-party test house, or by the implementer themselves (the IPL).



SL3000 Intermediate Product Design

Self Assessment – Jan 2016

Sign PIPL (PlayReady Intermediate Product License)

And

SL3000 Addendum

Acquire the PK

Review SL3000 CR&RRs requirements for PlayReady TEEs

Develop PlayReady Intermediate Product

(including PlayReady Client in TEE and Secure Media Path)

Request SL3000 Test Certificate

Do you own tests in house or using a third party test house.

Pass all requirements:

- Content Accessibility (8)
- Content Protection Robustness (4)
- PlayReady Device PK Robustness (2)
- PlayReady TEE Robustness (9)
- PlayReady TEE Compliance (18)

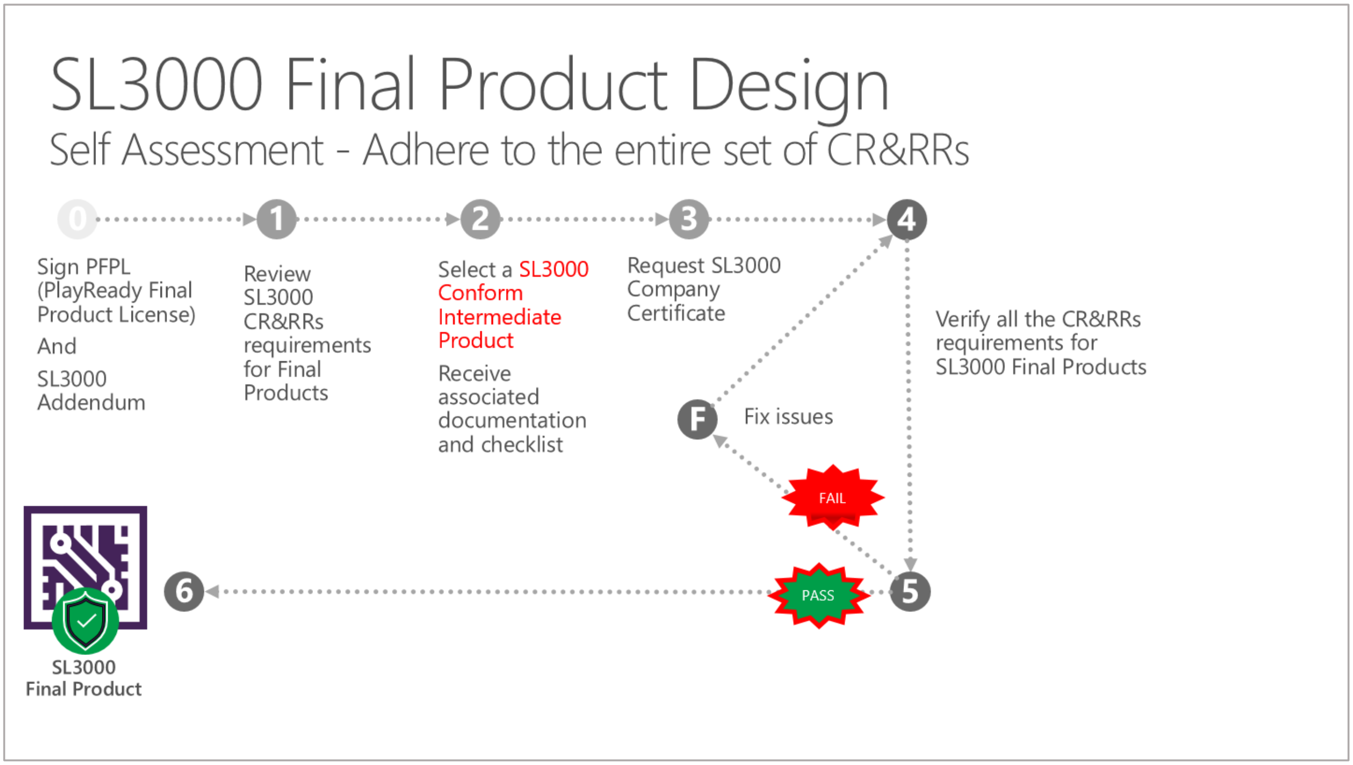
Fix issues

Document conformance and test results for FPL's

Archive documentation for future use and audits

SL3000 Conformant Chip/SOC/IP

PlayReady Final Products are not required to be reviewed by a third-party test house to qualify for SL3000 Compliance. However, Final Products that wish to ship with an SL3000 Certificate may only do so when they meet the requirements for SL3000 Compliant Final Products. This requires the Final Product to utilize an SL3000 Conformant Intermediate Product and conform to the SL3000 Compliance and Robustness rules.



SL3000 Final Product Design

Self Assessment - Adhere to the entire set of CR&RRs

Sign PFPL (PlayReady Final Product License)

And

SL3000 Addendum

Review SL3000 CR&RRs requirements for Final Products

Select a SL3000 Conform Intermediate Product

Receive associated documentation and checklist

Request SL3000 Company Certificate

Verify all the CR&RRs requirements for SL3000 Final Products

Fix issues

SL3000 Final Product

3. Terminology, Acronyms, Abbreviations

4K

This is generally defined as content with a resolution of 3840x2160. See also Ultra-High Definition (UHD).

Application Secrets

PlayReady stub library provided to Company and secrets, such as symmetric keys and private keys that reside in the application binary and/or in the process space of the application.

A/V Content

PlayReady A/V Content.

Certificate

A Certificate is a unique PlayReady object used to verify trust.

Certificate Security Level (CSL)

The security value specified in the leafmost certificate in the certificate chain associated with a PlayReady Final Product. A PlayReady Final Product may consume only Content that has an associated License Security Level no greater than the PlayReady Final Product's Certificate Security Level.

Company Certificate

A Certificate unique to Company issued by Microsoft for the purpose of issuing other Device/Model Certificates.

Compliance Rules

Compliance Rules specify the required behaviors of PlayReady implementations and the software accessing the implementations. Compliance Rules describe how content may be accessed and passed using specific policy rules.

Content

PlayReady Content.

Content Key

A symmetric key used to encrypt and decrypt Content.

Content Protection Functions

Functions related to protection of Content, including but not limited to authentication, encryption, decryption, Device Certificate signing, output protection, Metering, Secure Clock, Content revocation, key management, rights enforcement or storing/updating information in the PlayReady Data Stores as such term is described and required in the Microsoft Implementation, to the extent such functions are implemented in a PlayReady Final Product.

Device Secrets

Device Private Key, the private portion of the Fallback Keys, the private portion of the Device Model Keys, the Device Secret Key, the Certificate Signing Private Key, Certificate Signing Symmetric Key, Key File Protection Key and the private portion of the Domain Keys.

Enhanced Content Protection (ECP)

Content protection measures over and beyond those generally considered sufficient to obtain HD content in the past.

Final Product

A hardware product that (i) is in a final form of manufacturing with a fully functional user interface and (ii) is intended for distribution to and/or use by end users.

Final Product Licensee (FPL)	An entity licensed under a PlayReady Agreement to develop and/or distribute PlayReady Final Products.
Full Ultra-High Definition Content (Full UHD)	UHD content with Full 4K resolution - 4096 x 2160 pixels.
Integrated Circuit (IC)	A set of electronic circuits on one small plate ("chip") of semiconductor material, normally silicon.
Intermediate Product	A software or hardware product that is designed to be incorporated into or combined with a Final Product.
Intermediate Product Licensee (IPL)	An entity licensed under a PlayReady Agreement to develop and/or distribute PlayReady Intermediate Products.
License Integrity Key	A symmetric key used to verify that a License has not been tampered with.
Microsoft Implementation	The implementation of PlayReady Functionality provided to Company as source code, binaries, technical documentation, tools, and/or sample files under Company's PlayReady Agreement.
Personally Identifiable Information	Any information that can be used to identify, contact, or locate end users of PlayReady.
PlayReady Components	Components of a SL2000 or SL3000 qualified product which are subject to the PlayReady Compliance and Robustness Rules.
PlayReady Data Stores	The databases required for PlayReady features. This includes, but is not limited to, license store, Secure Store, metering store, metering certificate store, domain certificate store, and license synchronization store, as required by the Microsoft Implementation.
PlayReady Final Product	A Final Product that includes PlayReady as more specifically described in a PlayReady Agreement.
PlayReady Interface for Trusted Execution Environment (PRiTEE)	The PlayReady Interface for Trusted Execution Environments created using the PlayReady Porting Kit as described in PlayReady Documentation.
PlayReady Intermediate Product	An Intermediate Product that includes PlayReady, as more specifically described in a PlayReady Agreement.
PlayReady License	A data structure that contains, but is not limited to, (i) an encrypted Content Key or an encrypted key used to decrypt a Content Key associated with specific PlayReady Content, and (ii) PlayReady Policy associated with specific PlayReady Content
PlayReady Device Porting Kit 3.0 (PK 3.0)	The latest version of the PlayReady Device Porting Kit provided under a PlayReady Agreement.
PlayReady Product	A PlayReady Final Product implementing any feature(s) or functionality(s) of the Device Porting Kit or a PlayReady Intermediate Product implementing a PlayReady Trusted Execution Environment

PlayReady SL3000 Certificate	A Certificate provided by Microsoft for the purpose of enabling PlayReady Final Products to access PlayReady SL3000 Functionality.
PlayReady SL3000 Compliant Product	PlayReady Final Product which uses an SL3000 Conformant Intermediate Product and conforms to the SL3000 Compliance and Robustness Rules.
PlayReady Trusted Execution Environment	A Trusted Execution Environment found on any computing device reporting a Certificate Security Level of 3000.
Professional Software Tools	Professional tools, such as the software equivalent of in-circuit emulators, disassemblers, loaders, or patchers, implemented in software, such as would be used primarily by persons of professional skill and training, but not including either (i) professional tools or equipment that are made available on the basis of a non-disclosure agreement or (ii) Circumvention Tools.
Protocol Secrets	All numerical, algorithmic and implementation secrets related to protocol execution.
Robustness Rules	Robustness Rules specify different PlayReady assets and the levels of robustness required to protect each asset type.
Root Public Key	A public key controlled by Microsoft that is trusted by PlayReady Final Products.
Secure Code	Any code which is authorized to execute inside the TEE.
SL2000	PlayReady Security Level 2000
SL3000	PlayReady Security Level 3000
Specifically Set	To set a Trust Value, for example the Serial Number, in such a manner as to violate the condition of uniqueness as prescribed by the applicable compliance rules and/or robustness rules for that Trust Value.
Standard Definition Content (SD)	Video with a resolution of 640x480. See High Definition and Ultra-High Definition.
System on a Chip (SoC)	An integrated circuit (IC) that integrates all components of a computer or other electronic system into a single chip. It may contain digital, analog, mixed-signal, and often radio-frequency functions—all on a single chip substrate.
Trust Values	A value that PlayReady Final Products must resist attempts to modify or set, as specified in the Robustness Rules. Trust Values include Device Secrets, Serial Number, Secure Clock State, Revocation Data, Validation State, Timer State, Protocol Secrets, Last Known Good Date and Time, Secure Code, Working Set, and Output Protection State.

Trusted Execution Environment (TEE)

A hardware-enforced secure processing environment on a device that: (i) provides a Hardware Root of Trust, (ii) provides a Secure Boot process, (iii) runs only authenticated code which has been approved for use within the secure processing environment, (iv) provides for Secure Execution of PlayReady functionality, and (v) provides a Secure Media Pipeline and has a Certificate Security Level of 3000.

Ultra-High Definition Content (UHD)

Ultra-High Definition content. This is generally defined as content with a resolution of 3840x2160 – i.e. 4K content. However, this may also be used to include content with any of these following advanced features: Early-window content, Enhanced Chroma, Increased frame rate. See Full High Definition, Ultra-High Definition and Full 4K Content.

4. SL3000 Requirements for Intermediate Products

The security of a PlayReady Product depends critically on the robustness of the PlayReady implementation. As such, Microsoft has defined requirements in the PlayReady Compliance and Robustness rulesthatall PlayReady Intermediate Products MUST meet or exceed before they can be distributed to Final Product Licensees. The checklist below is a tool for IPLs to document the security review they've run on their product before they distribute it. This security review documentation must be communicated to companies building a Final Product based on this Intermediate Product.

The requirements are broken into 5 categories:

1) **CA: Content Accessibility**

2) **CPR: Content Protection Robustness**

3) **PKR: PlayReady Device Porting Kit Robustness**

4) **TEER: PlayReady Trusted Execution Environment (TEE) Robustness**

5) **TEEC: PlayReady Trusted Execution Environment (TEE) Compliance**

SL3000 Requirements for Intermediate Products Test Report – Check List

Intermediate Product Information	
Test Completion Date	
Test Company (if different than Vendor)	
Intermediate Product Vendor Name	
Chipset Model Name and Full Reference Tested	
Intermediate Product Firmware Version Tested	
Other identifying information (if applicable):	

Require-ment	**Under-lying Rule**	**Title**	**Requirement**	**Testing Procedure(s) Overview & Resource Usage**
CA-1.1	RR 2.2.1	Product Design - TEE	PlayReady Product is clearly designed such that is uses a PlayReady Trusted Execution Environment (TEE).	
CA-1.2	RR 2.2.1	Product Design - TEE	PlayReady Product only uses Content Protection Functions implemented by a PlayReady TEE.	
CA-2.1	RR 2.2.2.1	Decrypted Content	Decrypted A/V Content must not be readable or be placed outside the PlayReady Trusted Execution Environment. Decrypted A/V Content must not be available to code running outside the PlayReady TEE	
CA-2.2	RR 2.2.2.2	Application Secrets	Application Secrets must not be available in contiguous cleartext memory except when in use to decrypt Content and/or keying material. Application Secrets must not be available to code running outside the PlayReady Trusted Execution Environment.	

CA-3	RR 2.2.3	Video Transmission	PlayReady Products must be clearly designed such that when the video portion of Compressed or Uncompressed decrypted A/V Content is transmitted, such data is secure from unauthorized interception using Widely Available Tools, Specialized Tools, or Professional Software Tools and can only with difficulty be intercepted using Professional Hardware Tools. The level of difficulty applicable to Professional Hardware Tools is such that a typical consumer should not be able to use Professional Hardware Tools, with or without instructions, to intercept such data without risk of serious damage to the product or personal injury.	
CPR-1.1	RR 3.1.2	Device Secrets, Protocol Secrets, and Application Secrets	Implemented Content Protection Functions and characteristics set forth in Section 1.2.1 (Discover, reveal, and/or use without authority the Device Secrets, Protocol Secrets, and/or Application Secrets) of the PlayReady Robustness Rules: - Cannot be defeated or circumvented using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the PlayReady Trusted Execution Environment.	
CPR-1.2	RR 3.1.2	Device Secrets, Protocol Secrets, and Application Secrets	Implemented Content Protection Functions and characteristics set forth in Section 1.2.1 (Discover, reveal, and/or use without authority the Device Secrets, Protocol Secrets, and/or Application Secrets) of the PlayReady Robustness Rules: - Can only with difficulty be defeated or circumvented using Professional Hardware Tools.	
CPR-2.1	RR 3.2	Content Keys, License Integrity Keys, and Intermediate Keys	Implemented Content Protection Functions and characteristics set forth in Section 1.2.2 (Discover, reveal, and/or use without authority the Content Keys, License Integrity Keys, and/or Intermediate Keys) of the PlayReady Robustness Rules: - Cannot be defeated or circumvented using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the PlayReady Trusted Execution Environment.	

CPR-2.2	RR 3.2	Content Keys, License Integrity Keys, and Intermediate Keys	Implemented Content Protection Functions and characteristics set forth in Section 1.2.2 (Discover, reveal, and/or use without authority the Content Keys, License Integrity Keys, and/or Intermediate Keys) of the PlayReady Robustness Rules: - Can only with difficulty be defeated or circumvented using Professional Hardware Tools.	
CPR-3.1	RR 3.3.2	Root Public Keys	Implemented Content Protection Functions and characteristics set forth in Section 1.3.1 (Replace without authority the Root Public Keys) of the PlayReady Robustness Rules: - Cannot be defeated or circumvented using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the PlayReady Trusted Execution Environment.	
CPR-3.2	RR 3.3.2	Root Public Keys	Implemented Content Protection Functions and characteristics set forth in Section 1.3.1 (Replace without authority the Root Public Keys) of the PlayReady Robustness Rules: - Can only with difficulty be defeated or circumvented using Professional Hardware Tools.	
CPR-4.1	RR 3.4.1	Confidential Information	Implemented Content Protection Functions and characteristics set forth in Section 1.4 (Keep Confidential) of the PlayReady Robustness Rules, wherever applicable: - Cannot be defeated or circumvented using Widely Available Tools.	
CPR-4.2	RR 3.4.1	Confidential Information	Implemented Content Protection Functions and characteristics set forth in Section 1.4 (Keep Confidential) of the PlayReady Robustness Rules, wherever applicable: - Can only with difficulty be defeated or circumvented using Specialized Tools, Professional Software Tools, or Professional Hardware Tools.	

PKR-1.1	RR 5.2.2.1	Anti-Rollback Clock - Last Known Good Time	Implemented Trust Values and characteristics set forth in Section 5.1.2.8 (Last Known Good Date and Time, for PlayReady Final Products implementing an Anti-Rollback Clock) of the PlayReady Robustness Rules: - Cannot be modified without authority using Widely Available Tools or Specialized Tools.	
PKR-1.2	RR 5.2.2.1	Anti-Rollback Clock - Last Known Good Time	Implemented Trust Values and characteristics set forth in Section 5.1.2.8 (Last Known Good Date and Time, for PlayReady Final Products implementing an Anti-Rollback Clock) of the PlayReady Robustness Rules: - Can only with difficulty be modified without authority using Professional Software Tools or Professional Hardware Tools.	
PKR-2.1	RR 5.2.4	Validation State and Timer State	Implemented Trust Values and characteristics set forth in Section 5.1.2.5 (Validation State) and Section 5.1.2.6 (Timer State) of the PlayReady Robustness Rules: - Cannot be modified without authority using Widely Available Tools.	
PKR-2.2	RR 5.2.4	Validation State and Timer State	Implemented Trust Values and characteristics set forth in Section 5.1.2.5 (Validation State) and Section 5.1.2.6 (Timer State) of the PlayReady Robustness Rules: - Can only with difficulty be modified without authority using Specialized Tools, Professional Software Tools, or Professional Hardware Tools.	
TEER-1.1	RR 7.2.1	Secure Clock - Secure Clock State	Implemented Content Protection Functions and characteristics set forth in Section 7.1.2.3 (Secure Clock State, for PlayReady Final Products implementing a Secure Clock) of the PlayReady Robustness Rules: - Cannot be modified without authority using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.	

TEER-1.2	RR 7.2.1	Secure Clock - Secure Clock State	Implemented Content Protection Functions and characteristics set forth in Section 7.1.2.3 (Secure Clock State, for PlayReady Final Products implementing a Secure Clock) of the PlayReady Robustness Rules: - Can only with difficulty be modified without authority using Professional Hardware Tools. The level of difficulty applicable to Professional Hardware Tools is such that a typical consumer should not be able to use Professional Hardware Tools, with or without instructions, to modify without authority the Content Protection Functions and the characteristics set forth in Section 7.1.2.3 (Secure Clock State, for PlayReady Trusted Execution Environment Implementations implementing a Secure Clock) without risk of serious damage to the product or personal injury.	
TEER-2.1	RR 7.2.2	Device Secrets, Revocation Data, Timer State, Protocol Secrets, Working Set, and Output Protection State	Implemented Trust Values and characteristics set forth in Section 7.1.2.1 (Device Secrets), Section 7.1.2.4 (Revocation Data), Section 7.1.2.5 (Timer State, for PlayReady Products implementing a Secure Clock), Section 7.1.2.6 (Protocol Secrets), Section 7.1.2.8 (Working Set), and Section 7.1.2.9 (Output Protection State) of the PlayReady Robustness Rules: - Cannot be modified without authority using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.	

TEER-2.2	RR 7.2.2	Device Secrets, Revocation Data, Timer State, Protocol Secrets, Working Set, and Output Protection State	Implemented Trust Values and characteristics set forth in Section 7.1.2.1 (Device Secrets), Section 7.1.2.4 (Revocation Data), Section 7.1.2.5 (Timer State, for PlayReady Products implementing a Secure Clock), Section 7.1.2.6 (Protocol Secrets), Section 7.1.2.8 (Working Set), and Section 7.1.2.9 (Output Protection State) of the PlayReady Robustness Rules: - Can only with difficulty be modified without authority using Professional Hardware Tools. The level of difficulty applicable to Professional Hardware Tools is such that a typical consumer should not be able to use Professional Hardware Tools, with or without instructions, to modify without authority the Trust Values and characteristics set forth in Section 7.1.2.1 (Device Secrets), Section 7.1.2.4 (Revocation Data), Section 7.1.2.5 (Timer State, for PlayReady Products implementing a Secure Clock), Section 7.1.2.6 (Protocol Secrets), Section 7.1.2.8 (Working Set), and Section 7.1.2.9 (Output Protection State) without risk of serious damage to the product or personal injury.	
TEER-3.1	RR 7.2.3	Serial Numbers	Implemented Trust Values and characteristics set forth in Section 7.1.2.2 (Serial Number) of the PlayReady Robustness Rules: - Cannot be Specifically Set using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.	
TEER-3.2	RR 7.2.3	Serial Numbers	Implemented Trust Values and characteristics set forth in Section 7.1.2.2 (Serial Number) of the PlayReady Robustness Rules: - Can only with difficulty be Specifically Set using Professional Hardware Tools. The level of difficulty applicable to Professional Hardware Tools is such that a typical consumer should not be able to use Professional Hardware Tools, with or without instructions, to Specifically Set the Trust Values and characteristics set forth in Section 7.1.2.2 (Serial Number) without risk of serious damage to the product or personal injury.	

TEER-4.1	RR 7.2.4	Secure Code	Implemented Trust Values and characteristics set forth in Section 7.1.2.7 (Secure Code) of the PlayReady Robustness Rules: - Cannot be modified without authority using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.	
TEER-4.2	RR 7.2.4	Secure Code	Implemented Trust Values and characteristics set forth in Section 7.1.2.7 (Secure Code) of the PlayReady Robustness Rules: - Cannot be modified without authority due to a transition of power state, whether authorized or unauthorized.	
TEER-4.3	RR 7.2.4	Secure Code	Implemented Trust Values and characteristics set forth in Section 7.1.2.7 (Secure Code) of the PlayReady Robustness Rules: - Cannot be modified without authority due to a lack of any Required Process, including but not limited to Secure Boot Processes.	
TEER-4.4	RR 7.2.4	Secure Code	Implemented Trust Values and characteristics set forth in Section 7.1.2.7 (Secure Code) of the PlayReady Robustness Rules: - Can only with difficulty be modified without authority using Professional Hardware Tools. The level of difficulty applicable to Professional Hardware Tools is such that a typical consumer should not be able to use Professional Hardware Tools, with or without instructions, to modified without authority the Trust Values and characteristics set forth in Section 7.1.2.7 (Secure Code) without risk of serious damage to the product or personal injury.	

TEER-5.1	RR 7.3.1	Secure Boot Process	Implemented required processes set forth in Section 7.1.3.1 (Secure Boot Processes) of the PlayReady Robustness Rules, including without exception their utilized data, secrets, and process flow: - Cannot be modified without authority using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.	
TEER-5.2	RR 7.3.1	Secure Boot Process	Implemented required processes set forth in Section 7.1.3.1 (Secure Boot Processes) of the PlayReady Robustness Rules, including without exception their utilized data, secrets, and process flow: - Can only with difficulty be modified without authority using Professional Hardware Tools. The level of difficulty applicable to Professional Hardware Tools is such that a typical consumer should not be able to use Professional Hardware Tools, with or without instructions, to modify without authority the Trust Values and characteristics set forth in Section 7.1.3.1 (Secure Boot Process) without risk of serious damage to the product or personal injury	
TEER-6.1	RR 7.3.2	Secure Update Process	Implemented required processes set forth in Section 7.1.3.2 (Secure Update Processes) of the PlayReady Robustness Rules: - Cannot be modified without authority using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.	
TEER-6.2	RR 7.3.2	Secure Update Process	Implemented required processes set forth in Section 7.1.3.2 (Secure Update Processes) of the PlayReady Robustness Rules: - Cannot be rolled back to any previous state when doing so would reduce the level of robustness of the process or any related Trust Values.	

TEER-6.3	RR 7.3.2	Secure Update Process	Implemented required processes set forth in Section 7.1.3.2 (Secure Update Processes) of the PlayReady Robustness Rules: - Can only with difficulty be modified without authority using Professional Hardware Tools. The level of difficulty applicable to Professional Hardware Tools is such that a typical consumer should not be able to use Professional Hardware Tools, with or without instructions, to modify without authority the Trust Values and characteristics set forth in Section 7.1.3.2 (Secure Update Process) without risk of serious damage to the product or personal injury	
TEER-7.1	RR 7.4.1	Remote Provisioning	Implemented optional processes set forth in Section 7.1.4.1 (Remote Provisioning) of the Robustness Rules: - Cannot be modified without authority using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.	
TEER-7.2	RR 7.4.1	Remote Provisioning	Implemented optional processes set forth in Section 7.1.4.1 (Remote Provisioning) of the Robustness Rules: - Can only with difficulty be modified without authority using Professional Hardware Tools. The level of difficulty applicable to Professional Hardware Tools is such that a typical consumer should not be able to use Professional Hardware Tools, with or without instructions, to modify without authority the Trust Values and characteristics set forth in Section 7.1.4.1 (Remote Provisioning) without risk of serious damage to the product or personal injury.	
TEER-7.3	RR 7.4.1	Remote Provisioning	Implemented optional processes set forth in Section 7.1.4.1 (Remote Provisioning) of the Robustness Rules: - Cannot utilize Device Secrets to prove authenticity unless such Secrets are unique to the device and meet the requirements in Section 7.2.2.	

TEEC-1.1	CR 19.2.1	Hardware identification	PlayReady Trusted Execution Environment (TEE) supplies unique Hardware Identifier.	
TEEC-1.2	CR 19.2.2	Hardware identification	PlayReady TEE's Hardware Identifier is persistent across device reboots.	
TEEC-1.3	CR 19.2.2	Hardware identification	PlayReady TEE's Hardware Identifier is persistent across device firmware updates.	
TEEC-2.1	CR 19.3.1	Interface Definition	All functions of the PlayReady Interface for Trusted Execution Environments (PRiTEE) have been implemented within the PlayReady TEE.	
TEEC-2.2	CR 19.3.1	Interface Definition	A secure replacement implementation has been provided for any function which is documented as requiring replacement in the Microsoft Implementation.	
TEEC-2.3	CR 19.3.3	Interface Definition	PlayReady TEE has not changed the structure or content of method parameters defined by the PRiTEE.	
TEEC-3.1	CR 19.3.2	Key Material	PlayReady Product’s TEE provides a symmetric key unique to each client.	
TEEC-3.2	CR 19.3.2	Key Material.	PlayReady Product’s symmetric key is only accessible to code running inside the PlayReady TEE.	
TEEC-4	CR 19.4.1	Required Protection Policies	PlayReady TEE has implemented Output controls, as defined in Section 3.6 (Output Controls) of the PlayReady Compliance Rules.	
TEEC-5.1	CR 19.5.1	Output Protection Requirements	PlayReady TEE supports all Output Control requirements found in Section 3.6 (Output Controls) of the PlayReady Compliance Rules.	
TEEC-5.2	CR 19.5.1	Output Protection Requirements	All output protection requirements are enforced within the PlayReady TEE regardless of the minimum License Security Level of any License being interpreted.	

TEEC-6.1	CR 19.6.2	Secure Clock	Secure Clock implemented within PlayReady TEE does not provide a valid time upon being reset.	
TEEC-6.2	CR 19.6.2	Secure Clock	Secure Clock can only be set from within the PlayReady TEE.	
TEEC-6.3	CR 19.6.2	Secure Clock	Secure Clock can be set on a regular basis.	
TEEC-6.4	CR 19.6.3	Secure Clock	PlayReady TEE reporting that is supports a Secure Clock, uses such Secure Clock to enforce license expiration.	
TEEC-7	CR 19.8.1	Key History	Upon updating or changing a key, PlayReady TEE is able to recover all previous keys to decrypt stored content.	