

Robustness Rules for PlayReady Products

Microsoft Corporation

14th July 2021

Contents

[1 CONSTRUCTION 1](#_Toc489365916)

[2 ACCESSIBILITY OF CONTENT 1](#_Toc489365917)

[3 REQUIRED LEVELS OF ROBUSTNESS 3](#_Toc489365918)

[4 NEW CIRCUMSTANCES 5](#_Toc489365919)

[5 ROBUSTNESS RULES FOR PLAYREADY FINAL PRODUCTS IMPLEMENTING THE PLAYREADY DEVICE PORTING KIT 5](#_Toc489365920)

[6 ROBUSTNESS RULES FOR PLAYREADY FINAL PRODUCTS USING THE PLAYREADY PC SDK 12](#_Toc489365921)

[7 ROBUSTNESS RULES FOR PLAYREADY TRUSTED EXECUTION ENVIRONMENTS 13](#_Toc489365922)

**ROBUSTNESS RULES FOR MICROSOFT PLAYREADY APPLICATIONS AND DEVICES**

Capitalized terms have the meanings set forth in the document entitled “Defined Terms - Microsoft PlayReady Compliance Rules and Robustness Rules,” which is incorporated herein by this reference. Other initially capitalized terms not defined in these Robustness Rules have the meanings ascribed to them in the PlayReady Agreement or the Microsoft Implementation.

These Robustness Rules apply to PlayReady Products.

# **CONSTRUCTION**

## **Generally**. PlayReady Products as shipped must meet the applicable Compliance Rules and these Robustness Rules, and must be designed and manufactured to resist or prohibit, as more specifically described herein, attempts to modify such PlayReady Products so as to defeat the functions of the Microsoft Implementation.

## **Keep** **Secrets**. PlayReady Products must be designed and manufactured such that they resist attempts to each and all of the following:

### Discover, reveal, and/or use without authority the Device Secrets, Protocol Secrets, and/or Application Secrets.

### Discover, reveal, and/or use without authority the Content Keys, License Integrity Keys, and/or Intermediate Keys.

## **Protect** **Trust** **Values**. PlayReady Products must be designed and manufactured such that they resist attempts to modify or Specifically Set any of the following Trust Values:

### Replace without authority the Root Public Keys.

## **Keep** **Confidential**. PlayReady Products must be designed and manufactured such that they resist unauthorized attempts to discover Personally Identifiable Information.

# **ACCESSIBILITY** **OF** **CONTENT**

## With a License Security Level of 2000

### Company must design and develop PlayReady Products such that decrypted Content is not available to Outputs or APIs except as expressly specified (and in the form specified) in these Robustness Rules and/or applicable Compliance Rules.

#### A/V Content must not travel or otherwise be placed outside the application process except as allowed by the Compliance Rules.

#### Application Secrets must not be available in contiguous cleartext memory except when in use to decrypt Content and/or keying material.

### PlayReady Products must be clearly designed such that when the video portion of Uncompressed decrypted A/V Content with Source ID value of 258 (DTCP sourced content) with an Effective Resolution greater than 520,000 pixels per frame is transmitted over a User Accessible Bus, such data is reasonably secure from unauthorized interception, except with difficulty, using either Widely Available Tools or Specialized Tools. The level of difficulty applicable to Widely Available Tools is such that a typical consumer should not be able to use Widely Available Tools, with or without instructions, to intercept such data without risk of serious damage to the product or personal injury.

### PlayReady Products must be clearly designed such that when the video portion of Compressed decrypted A/V Content is transmitted over a User Accessible Bus, such data is reasonably secure from unauthorized interception, except with difficulty, using either Widely Available Tools or Specialized Tools. The level of difficulty applicable to Widely Available Tools is such that a typical consumer should not be able to use Widely Available Tools, with or without instructions, to intercept such data without risk of serious damage to the product or personal injury. This Section 2.1.3 does not prohibit Company from designing and manufacturing PlayReady Portable Devices which incorporate means, such as test points, used by Company or professionals to analyze or repair products, provided, however, that such means (i) are reasonably secure from unauthorized access, except with difficulty, using either Widely Available Tools or Specialized Tools, and (ii) are not a pretext for allowing consumers access to internal connectors or other portions of PlayReady Products which are required to be secured, including but not limited to internal connectors carrying Compressed decrypted A/V Content.

## With a License Security Level of 3000 or higher

### PlayReady Products must be clearly designed such that they use a PlayReady Trusted Execution Environment. The PlayReady Product must only use Content Protection Functions implemented by a PlayReady Trusted Execution Environment.

### Company must design and develop PlayReady Products such that decrypted Content is not available to Outputs or APIs except as expressly specified (and in the form specified) in these Robustness Rules and/or applicable Compliance Rules.

#### 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 Trusted Execution Environment.

#### 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.

### 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.

# **REQUIRED** **LEVELS** **OF** **ROBUSTNESS**

## The Content Protection Functions and the characteristics set forth in Section 1.2.1 (Discover, reveal, and/or use without authority the Device Secrets, Protocol Secrets, and/or Application Secrets) must be implemented so that it is reasonably certain that they:

### For PlayReady Products reporting a Certificate Security Level of 2000

#### Cannot be defeated or circumvented using Widely Available Tools or Specialized Tools.

#### Can only with difficulty be defeated or circumvented using Professional Software Tools or Professional Hardware Tools.

### For PlayReady Products reporting a Certificate Security Level of 3000

#### Cannot be defeated or circumvented using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the PlayReady Trusted Execution Environment.

#### Can only with difficulty be defeated or circumvented using Professional Hardware Tools.

## The Content Protection Functions and the 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) must be implemented so that it is reasonably certain that they:

### For PlayReady Products reporting a Certificate Security Level of 2000

#### Cannot be defeated or circumvented using Widely Available Tools or Specialized Tools.

#### Can only with difficulty be defeated or circumvented using Professional Software Tools or Professional Hardware Tools.

### For PlayReady Products reporting a Certificate Security Level of 3000

#### Cannot be defeated or circumvented using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the PlayReady Trusted Execution Environment.

#### Can only with difficulty be defeated or circumvented using Professional Hardware Tools.

## The Content Protection Functions and the characteristics set forth in Section 1.3.1 (Replace without authority the Root Public Keys) must be implemented so that it is reasonably certain that they:

### For PlayReady Products reporting a Certificate Security Level of 2000

#### Cannot be defeated or circumvented using Widely Available Tools or Specialized Tools.

#### Can only with difficulty be defeated or circumvented using Professional Software Tools or Professional Hardware Tools.

### For PlayReady Products reporting a Certificate Security Level of 3000

#### Cannot be defeated or circumvented using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the PlayReady Trusted Execution Environment.

#### Can only with difficulty be defeated or circumvented using Professional Hardware Tools.

## The Content Protection Functions and the characteristics set forth in Section 1.4 (Keep Confidential), wherever applicable, must be implemented so that it is reasonably certain that they:

### For PlayReady Products reporting a Certificate Security Level of 2000 or higher

#### Cannot be defeated or circumvented using Widely Available Tools or Specialized Tools.

#### Can only with difficulty be defeated or circumvented using Professional Software Tools or Professional Hardware Tools.

# **NEW** **CIRCUMSTANCES**

## If a PlayReady Product complies with these Robustness Rules when designed and when shipped, but at any time thereafter new circumstances arise which, had they been existing at the time of design or shipment, would have caused such PlayReady Product to fail to comply with these Robustness Rules (“New Circumstances”), then upon becoming aware of such New Circumstances, Company must promptly redesign the affected PlayReady Product or make available upgrades to its affected PlayReady Product to make such PlayReady Product compliant with these Robustness Rules under the New Circumstances, and, as soon as reasonably practicable, consistent with ordinary product cycles and taking into account the level of threat to Content under the New Circumstances, must incorporate such redesign or replacement into its affected PlayReady Product, or if such redesign or upgrade is not possible or practical, must cease manufacturing and/or distributing such affected PlayReady Product.

# **ROBUSTNESS** **RULES** **FOR** **PLAYREADY** **FINAL** **PRODUCTS** **IMPLEMENTING** **THE** **PLAYREADY** **DEVICE** **PORTING** **KIT**

## **Construction**. In addition to complying with Section 1 (Construction), Section 2 (Accessibility of Content), Section 3 (Required Levels of Robustness) and, if applicable, Section 4 (New Circumstances) and Section 7 (Robustness Rules for PlayReady Trusted Execution Environments) of these Robustness Rules, PlayReady Final Products implementing any feature(s) or functionality(s) of the PlayReady Device Porting Kit must comply with all of the requirements of this Section 5 (Robustness Rules for PlayReady Final Products Implementing the PlayReady Device Porting Kit), including the following:

### **Defeating** **Functions** **and** **Features**. PlayReady Final Products subject to this Section 5 (Robustness Rules for PlayReady Final Products Implementing the PlayReady Device Porting Kit) must not include switches, jumpers or traces that may be cut, or control functions means (such as end user remote control functions or keyboard, command or keystroke bypass), debuggers or Debugging Aids or software equivalents of any of the foregoing by which content protection technologies or other mandatory provisions of the Microsoft Implementation, Robustness Rules, or Compliance Rules may be defeated or by which decrypted Content may be exposed to unauthorized copying, usage or distribution.

### **Protect** **Trust** **Values**. PlayReady Final Products subject to this Section 5 (Robustness Rules for PlayReady Final Products Implementing the PlayReady Device Porting Kit) must be designed and manufactured such that they resist attempts to modify or Specifically Set any Trust Values:

#### Device Secrets

#### Serial Number

#### Secure Clock State, for PlayReady Final Products implementing a Secure Clock

#### Revocation Data

#### Validation State

#### Timer State

#### Protocol Secrets

#### Secure Code

#### Working Set

#### Output Protection State

### **Protect Required Processes.** PlayReady Final Products subject to this Section 5 (Robustness Rules for PlayReady Final Products Implementing the PlayReady Device Porting Kit) must be designed and manufactured such that they provide all Required Processes. PlayReady Final Products must also prohibit attempts to modify or replace without authority any of the following Protected Required Processes:

#### Secure Update Processes

**Protect Optional Processes.** PlayReady Final Products subject to thisSection 5 (Robustness Rules for PlayReady Final Products Implementing the PlayReady Device Porting Kit) may be designed and manufactured such that they provide Optional Processes.

#### Remote Provisioning

#### Secure Boot Processes

## Required Levels of Robustness for Trust Values

### The Content Protection Functions and the characteristics set forth in Section 5.1.2.3 (Secure Clock State, for PlayReady Final Products implementing a Secure Clock) must be implemented so that it is reasonably certain that they:

#### With a License Security Level of 2000

##### Cannot be modified without authority using Widely Available Tools or Specialized Tools.

##### Can only with difficulty be modified without authority using Professional Software Tools or Professional Hardware Tools.

#### With a License Security Level of 3000 or higher

##### Meet the Required Level of Robustness for PlayReady Trusted Execution Environments found in Section 7.2 (Required Levels of Robustness for Trust Values).

### The Trust Values and characteristics set forth in Section 5.1.2.1 (Device Secrets), Section 5.1.2.4 (Revocation Data), and Section 5.1.2.7 (Protocol Secrets) must be implemented so that it is reasonably certain that they:

#### With a License Security Level of 2000

##### Cannot be modified without authority using Widely Available Tools or Specialized Tools.

##### Can only with difficulty be modified without authority using Professional Software Tools or Professional Hardware Tools.

#### With a License Security Level of 3000 or higher

##### Meet the Required Level of Robustness for PlayReady Trusted Execution Environments found in Section 7.2 (Required Levels of Robustness for Trust Values).

### The Trust Values and characteristics set forth in Section 5.1.2.5 (Validation State) and Section 5.1.2.6 (Timer State) must be implemented so that it is reasonably certain that they:

#### With a License Security Level of 2000 or higher

##### Cannot be modified without authority using Widely Available Tools.

##### Can only with difficulty be modified without authority using Specialized Tools, Professional Software Tools, or Professional Hardware Tools.

### The Trust Values and characteristics set forth in Section 5.1.2.2 (Serial Number) must be implemented so that it is reasonably certain that they:

#### With a License Security Level of 2000

##### Cannot be Specifically Set using Widely Available Tools or Specialized Tools.

##### Can only with difficulty be Specifically Set using Professional Software Tools or Professional Hardware Tools.

#### With a License Security Level of 3000 or higher

##### Meet the Required Level of Robustness for PlayReady Trusted Execution Environments found in Section 7.2 (Required Levels of Robustness for Trust Values).

### The Trust Values and characteristics set forth in Section 5.1.2.9 (Secure Code), Section 5.1.2.10 (Working Set), and Section 5.1.2.11 (Output Protection State) must be implemented so that it is reasonably certain that they:

#### With a License Security Level of 3000 or higher

##### Meet the Required Level of Robustness for PlayReady Trusted Execution Environments found in Section 7.3 (Required Levels of Robustness for Required Processes).

## Required Levels of Robustness for Required Processes

### The processes set forth in Section 5.1.3.2 (Secure Update Processes) must be implemented so that it is reasonably certain that they:

#### Meet the Required Level of Robustness for PlayReady Trusted Execution Environments found in Section 7.3 (Required Levels of Robustness for Required Processes).

## Required Levels of Robustness for Optional Processes

### The processes set forth in Section 5.1.4.1 (Remote Provisioning) must be implemented so that it is reasonably certain that they:

#### For PlayReady Products which will only support a Certificate Security Level of 2000

##### Cannot be defeated or circumvented using Widely Available Tools or Specialized Tools.

##### Can only with difficulty be defeated or circumvented using Professional Software Tools or Professional Hardware Tools.

##### Cannot utilize Device Secrets to prove authenticity unless such Secrets are unique to the device and meet the requirements in Section 5.2.2.

##### Protect Trust Values used during the processes to the level(s) defined in Section 5.2 (Required Levels of Trust for Trust Values).

#### For all other PlayReady Products

##### Meet the Required Level of Robustness for PlayReady Trusted Execution Environments found in Section 7.4 (Required Levels of Robustness for Optional Processes).

### The processes set forth in Section 5.1.4.2 (Secure Boot Processes) must be implemented so that it is reasonably certain that the processes, including without exception their utilized data, secrets, and process flow:

#### Meet the Required Level of Robustness for PlayReady Trusted Execution Environments found in Section 7.3 (Required Levels of Robustness for Required Processes).

## **Methods** **of** **Making** **Functions** **Robust**. PlayReady Final Products subject to this Section 5 (Robustness Rules for PlayReady Final Products Implementing the PlayReady Device Porting Kit) must use at least the following techniques to be designed to effectively frustrate efforts to circumvent or defeat all applicable Content Protection Functions and protections specified in the applicable Compliance Rules and Robustness Rules:

### **Robustness** **Requirements** **Applicable** **to** **Software** **Implementations**. PlayReady Final Products that implement one or more of the Content Protection Functions, in whole or in part, in software must also comply with this Section 5.5.1 (Robustness Requirements Applicable to Software Implementations).

#### PlayReady Final Products must comply with Section 1.2 (Keep Secrets), Section 5.1.2 (Protect Trust Values) and Section 1.4 (Keep Confidential) of these Robustness Rules by reasonable and effective methods, which may include, but are not limited to: encryption, embodiment in a secure physical implementation, using techniques of obfuscation and/or cryptographic whiteboxing technologies to disguise and hamper attempts to discover the approaches used or secrets concealed within the software, and/or self-checking of integrity in such a manner as to result in a failure to execute Content Protection Functions in the event of unauthorized modification.

#### PlayReady Final Products must be implemented such that the failure of a Content Protection Function would cause the PlayReady Final Product to cease further processing and explicitly fail safely.

### **Robustness** **Requirements** **Applicable** **to** **Hardware** **Implementations**. PlayReady Final Products that implement one or more Content Protection Functions, in whole or in part, in hardware must also comply with this Section 5.5.2 (Robustness Requirements Applicable to Hardware Implementations). The fact that a software implementation operates on a hardware computing platform does not, in and of itself, cause such hardware computer platform to be subject to the requirements set forth in this Section 5.5.2 (Robustness Requirements Applicable to Hardware Implementations) and Section 5.5.3 (Robustness Requirements Applicable to Hybrid Implementations). If, however, the software implementation relies on hardware or any hardware component to satisfy any of these Robustness Rules, then such hardware or hardware component must satisfy all of the Robustness Rules set forth in this Section 5.5.2 (Robustness Requirements Applicable to Hardware Implementations).

#### For PlayReady Products reporting a Certificate Security Level of 2000

##### PlayReady Final Products must comply with Section 1.2 (Keep Secrets), Section 5.1.2 (Protect Trust Values), Section 1.3 (Protect Trust Values), and Section 1.4 (Keep Confidential) of these Robustness Rules, by reasonable and effective means, including but not limited to: embedding secrets in silicon circuitry or firmware that cannot reasonably be read or replaced, or the techniques described in Section 5.5.1 (Robustness Requirements Applicable to Software Implementations).

#### For PlayReady Products reporting a Certificate Security Level of 3000

##### PlayReady Final Products must comply with Section 1.2 (Keep Secrets), Section 5.1.2 (Protect Trust Values), Section 5.1.3 (Protect Required Processes), Section 5.1.4 (Protect Optional Processes), Section 1.3 (Protect Trust Values), and Section 1.4 (Keep Confidential) of these Robustness Rules, by reasonable and effective means, including but not limited to: embedding secrets in silicon circuitry or other hardware-protected means that cannot reasonably be read or replaced.

### **Robustness** **Requirements** **Applicable** **to** **Hybrid** **Implementations**. The interfaces between hardware and software portions of PlayReady Final Products must be designed so that the hardware portions comply with Section 5.5.2 (Robustness Requirements Applicable to Hardware Implementations) and the software portions comply with Section 5.5.1 (Robustness Requirements Applicable to Software Implementations).

#  **ROBUSTNESS** **RULES** **FOR** **PLAYREADY** **FINAL** **PRODUCTS** **USING** **THE** **PLAYREADY** **PC** **SDK**

## Construction

### **Generally**. In addition to complying with Section 1 (Construction), Section 2 (Accessibility of Content), Section 3 (Required Levels of Robustness) and, if applicable, Section 4 (New Circumstances) of these Robustness Rules, PlayReady Final Products using the PlayReady PC Software Development Kit must comply with all of the requirements of this Section 6 (Robustness Rules for PlayReady Final Products using the PlayReady PC SDK), including the following:

### **Defeating** **Functions** **and** **Features**. PlayReady Final Products subject to this Section 6 must not include control functions means, software switches, backdoors, bypasses, end-user selectable options, debuggers or Debugging Aids, or mechanisms for self-tampering or delayed loading by which the Content Protection Functions may be defeated. Such PlayReady Final Products must not use, incorporate, call or enable any software that modifies the behavior of the PlayReady Final Product in a manner that causes it to violate the Compliance Rules.

## **Methods** **of** **Making** **Functions** **Robust**. PlayReady Final Products subject to this Section 6 (Robustness Rules for PlayReady Final Products using the PlayReady PC SDK) must use at least the following techniques to be designed to effectively frustrate efforts to circumvent or defeat all applicable Content Protection Functions and protections specified in the Compliance and Robustness Rules:

### The PlayReady Final Product must achieve compliance by reasonable and effective methods, including varying the memory location of the Export Boundary, and may include use of techniques of obfuscation and/or cryptographic whiteboxing technologies to disguise and hamper attempts to discover the approaches used and/or secrets concealed within the software, and/or self-checking of integrity in such a manner as to result in a failure to execute Content Protection Functions in the event of unauthorized modification.

### The PlayReady Final Product must be implemented such that the failure of a Content Protection Function would cause the implementation to cease further processing and explicitly to fail safely.

ROBUSTNESS RULES FOR PLAYREADY TRUSTED EXECUTION ENVIRONMENTS

## **Construction**. In addition to complying with Section 1 (Construction), Section 2 (Accessibility of Content), Section 3 (Required Levels of Robustness) and, if applicable, Section 4 (New Circumstances) of these Robustness Rules, PlayReady Products providing a PlayReady Trusted Execution Environment must comply with all of the requirements of this Section 7 (Robustness Rules for PlayReady Trusted Execution Environments), including the following:

### **Defeating** **Functions** **and** **Features**. PlayReady Products subject to this Section 7 (Robustness Rules for PlayReady Trusted Execution Environments) must not include switches, jumpers or traces that may be cut, or control functions means (such as end user remote control functions or keyboard, command or keystroke bypass), debuggers or Debugging Aids or software equivalents of any of the foregoing by which content protection technologies or other mandatory provisions of the Microsoft Implementation, Robustness Rules, or Compliance Rules may be defeated or by which decrypted Content may be exposed to unauthorized copying, usage or distribution.

### **Protect** **Trust** **Values**. PlayReady Products subject to this Section 7 (Robustness Rules for PlayReady Trusted Execution Environments) must be designed and manufactured such that they prohibit attempts to modify or Specifically Set any Trust Values including:

#### Device Secrets

#### Serial Number

#### Secure Clock State, for PlayReady Products implementing a Secure Clock

#### Revocation Data

#### Timer State, for PlayReady Products implementing a Secure Clock

#### Protocol Secrets

#### Secure Code

#### Working Set

#### Output Protection State

### **Protect Required Processes.** PlayReady Products subject to this Section 7 (Robustness Rules for PlayReady Trusted Execution Environments) must be designed and manufactured such that they provide all Required Processes. PlayReady Products must also prohibit attempts to modify or replace without authority any of the following Protected Required Processes:

#### Secure Boot Processes

#### Secure Update Processes

**Protect Optional Processes.** PlayReady Products subject to this Section 7 (Robustness Rules for PlayReady Trusted Execution Environments) may be designed and manufactured such that they provide Optional Processes.

#### Remote Provisioning

Required Levels of Robustness for Trust Values

### The Content Protection Functions and the characteristics set forth in Section 7.1.2.3 (Secure Clock State, for PlayReady Products implementing a Secure Clock) must be implemented so that it is reasonably certain that they:

#### Cannot be modified without authority using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.

#### 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.

### 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) must be implemented so that it is reasonably certain that they:

#### Cannot be modified without authority using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.

#### 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.

### The Trust Values and characteristics set forth in Section 7.1.2.2 (Serial Number) must be implemented so that it is reasonably certain that they:

#### Cannot be Specifically Set using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.

#### 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.

### The Trust Values and characteristics set forth in Section 7.1.2.7 (Secure Code) must be implemented so that it is reasonably certain that they:

#### Cannot be modified without authority using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.

#### Cannot be modified without authority due to a transition of power state, whether authorized or unauthorized.

#### Cannot be modified without authority due to a lack of any Required Process, including but not limited to Secure Boot Processes.

#### 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.

## Required Levels of Robustness for Required Processes

### The processes set forth in Section 7.1.3.1 (Secure Boot Process) must be implemented so that it is reasonably certain that the processes, 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.

#### 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.

### The processes set forth in Section 7.1.3.2 (Secure Update Process) must be implemented so that it is reasonably certain that they:

#### Cannot be modified without authority using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.

#### 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.

#### 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.

## Required Levels of Robustness for Optional Processes

### The processes set forth in Section 7.1.4.1 (Remote Provisioning) must be implemented so that it is reasonably certain that they:

#### Cannot be modified without authority using Widely Available Tools, Specialized Tools, Professional Software Tools, or any software running outside the Trusted Execution Environment.

#### 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.

#### Cannot utilize Device Secrets to prove authenticity unless such Secrets are unique to the device and meet the requirements in Section 7.2.2.

#### Protect Trust Values used during the processes to the level(s) defined in Section 7.2 (Required Levels of Trust for Trust Values).

## **Methods** **of** **Making** **Functions** **Robust**. PlayReady Products subject to this Section 7 (Robustness Rules for PlayReady Trusted Execution Environments) must use at least the following techniques to be designed to effectively frustrate efforts to circumvent or defeat all applicable Content Protection Functions and protections specified in the applicable Compliance Rules and Robustness Rules:

### **Robustness** **Requirements** **Applicable** **to** **Hardware** **Implementations**. PlayReady Trusted Execution Environments must satisfy all of the Robustness Rules set forth in this Section 7.5.1 (Robustness Rules Applicable to Hardware Implementations).

#### PlayReady Products must comply with Section 1.2 (Keep Secrets), Section 7.1.2 (Protect Trust Values), Section 7.1.2 (Protect Required Processes), Section 7.1.4 (Protect Optional Processes), Section 1.3 (Protect Trust Values), and Section 1.4 (Keep Confidential) of these Robustness Rules, by reasonable and effective means, including but not limited to: embedding secrets in silicon circuitry or other hardware-protected means that cannot reasonably be read or replaced.