Enabler Test Specification for DRM-V2_0

Candidate Version 2.0 – 07 Feb 2006

Open Mobile Alliance

OMA-ETS-DRM-Conformance_Test_Client-V2_0-20060207-C

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at http://www.openmobilealliance.org/ipr.html. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR’S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

Contents

Figures

Tables

1. Scope

This document describes in detail DRM Client conformance test cases for the OMA DRM v 2.0 specification.

2. References

2.1 References

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. URL:http://www.ietf.org/rfc/rfc2119.txt

[OCSP] Myers, M., Ankney, R., Malpani, A., Galperin, S. and C. Adams, "Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol - OCSP", RFC 2560, June 1999. http://www.ietf.org/rfc/rfc2560.txt

[OCSP-MP] OMA Online Certificate Status Protocol (profile of [OCSP]) V 1.0, http://www.openmobilealliance.org/

[DRM-v2.0] "DRM Rights Management". Open Mobile Alliance™. OMA-DRM-DRM-V2_0 (Sept 2005 release). URL:http://www.openmobilealliance.com/.

[DRMCF-v2.0] "DRM Content Format". Open Mobile Alliance™. OMA-DRM-DCF-V2_0 (Sept 2005 release).doc. URL:http://www.openmobilealliance.com/.

[DRMREL-v2.0] "DRM Rights Expression Language". Open Mobile Alliance™. OMA-DRM-REL-V2_0 (Sept 2005 release).doc. URL:http://www.openmobilealliance.com/.

[ETP] Enabler Test Plan for DRM 2.0

OMA-ETP-DRM-V2_0 (July 2005 release)

URL:http://www.openmobilealliance.com/

2.2 Informative References

[ETS] Enabler Test Specification for DRM 2.0

OMA-ETS-DRM-V2_0-Interoperability

URL:http://www.openmobilealliance.com/.

[Conf-RI] Enabler Test Specification for DRM 2.0

OMA-ETS-DRM-V2_0-Conformance-Right-Issuer

URL:http://www.openmobilealliance.com/

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

See [DRM-v2.0], [DRMCF-v2.0] and [DRMREL-v2.0].

3.3 Abbreviations

See [DRM-v2.0], [DRMCF-v2.0] and [DRMREL-v2.0].

CRL	Certificate Revocation List
DCF	DRM Content Format
DRM	Digital Rights Management
REL	Rights Expression Language
TA	Trust Anchor

4. Introduction

This document describes in detail conformance test cases for the OMA DRM V2.0 Enabler specification as specified in [DRM-v2.0], [DRMCF-v2.0] and [DRMREL-v2.0]. These conformance test cases are aimed to verify the adherence to normative requirements described in the technical specifications. Only testcases for the DRM client are listed in this document.

The OMA DRM V2.0 specification contains many mandatory (MUST, SHALL) or optional (SHOULD, MAY) requirements. The optional requirements will not be covered by the conformance tests listed in this document.

The Testcases related to IOP will be covered in [ETS]. The conformance tests for the Righs Issuer will be covered in [Conf-RI].

5. General setup for DRM Agent Conformance tests

This section gives a specification of the setup and system parameters that apply to all DRM Agent conformance tests.

5.1 Public Key Infrastructure for DRM Agent conformance tests

In order to successfully conduct conformance tests, Test server and DRM Agent (DUT) have to agree upon some system parameters, generally refered to as Public Key Infrastructure (PKI). Normally this PKI is defined by the Trust Anchor. For these conformance tests, the PKI's will be used that have been specified in [ETP].

5.2 Discard History

In order to prevent any influence of previous communication each conformance test shall start with a virgin DRM Agent and Rights Issuer. I.e. all cached information like RI context, OCSP response, installed RO's and content shall be deleted before starting the test.

5.3 Freshness

In some test cases, the current DRM time will be compared with another time value, e.g. expiration time. In a practical system, a certain margin will be allowed. This is in order to allow for some deviation of DRM time in the device from the actual time. For these conformance tests this margin shall be set to 0 seconds.

5.4 Cryptographical algorithms

The cryptographical algorithms that will be used during all the conformance tests are the default algorithms as defined in [DRM-v2.0].

5.5 Version

Whenever applicable the value of the <version> element, denoting the version of the OMA-DRM specification will be 2.0.

Whenever applicable the value of the <version> element, denoting the version of the OMA-REL specification will be 2.0.

Whenever applicable the value of the <version> element, denoting the version of the OMA-DCF specification will be 0.

5.6 Key Identifier

Whenever applicable, the value of the key identifier will be the SHA-1 value of the public key.

5.7 Conformance tests for Unconnected Devices

Appart from DeviceRO processing, an Unconnected Device connected via OBEX to a Connected Device SHALL comply to all mandatory requirements of the DRM-2.0 enabler specification. Thus, all conformance test, defined in this document, appart from the tests related to DeviceRO processing shall also be applied to Unconnected Devices.

5.8 Test Tool and Testcode

All testcases described in this document can be performed using a test tool.

For none of the testcases any specific testcode is required.

6. DRM Conformance Test Cases

6.1 ROAP related conformance tests

6.1.1 ROAP trigger with expired RI context

Testcase ID	DRM-2.0-con-1
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 5.4.2.4.1 If the RI Context has expired, the Device MUST NOT execute any other protocol than the 4-pass Registration protocol with this RI. This test also covers: [DRM-v2.0] 5.2.1 The **<riID>** element identifies the RI as specified in Section 5.4.2.2.1. For triggers besides the **<registrationRequest>**, the DRM Agent MUST use this value to verify that it has a valid RI Context with the Rights Issuer. If the DRM Agent does not have a valid RI Context with the identified Rights Issuer then the DRM Agent MUST initiate the Registration Protocol before initiating the protocol indicated in the **<roapTrigger>** element.
SCR Reference	DRM-CLI-CMN-037
Preconditions	PKI : Model A State: - DRM Agent and RI Server have established an RI Context that has expired.
Test Procedure	- The DRM Agent receives a trigger for RO acquisition, Join Domain or Leave Domain protocol.
Pass-Criteria	- The DRM Agent sends a DeviceHello message to the RI
Test Case Deployment [1]	

	Registration Trigger	**b**	Join Domain Trigger
A	RO Acquisition Trigger	**c**	Leave Domain Trigger

[1] **Test Case Deployment**

Many test case description can and shall be deployed to several processing steps in the protocol. By example, in the tescase described shall be executed for:

- RO Acquisition Trigger (testcase DRM-2.0-con-1.a)
- JoinDomain Trigger (testcase DRM-2.0-con-1.b)
- LeaveDomain Trigger (testcase DRM-2.0-con-1.c)

6.1.2 Deleted

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-2</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">Deleted</td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3"></td></tr>
<tr><td></td><td colspan="3">-</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.3 Missing Signature in Leave Domain trigger

Testcase ID	DRM-2.0-con-3		
Test Object	DRM Agent		
Test Case Description	See section header.		
Specification Reference	[DRM-v2.0] 5.2.1 In case a **<leaveDomain>** element is present, the RI MUST include a **<signature>** element and, with one exception (see below), Devices MUST verify this signature. If the Device cannot verify the signature, the Device SHOULD inform the user and MUST discard the ROAP Trigger. The only exception to the verification requirement is when the Device is not a member of the identified Domain, and the trigger has been authenticated with a MAC based on the Domain Key. In this case the device may have to obtain user consent before initiating ROAP, section 5.1.8 defines when explicit user consent is required.		
SCR Reference			
Preconditions	PKI : Model A State: - DRM Agent and RI Server have established an RI Context and the DRM Agent is a member of the Domain.		
Test Procedure	- The DRM Agent receives a Leave Domain trigger without a <signature> element.		
Pass-Criteria	- The DRM Agent will not send the Leave Domain request.		
Test Case Deployment			
	Registration Trigger		Join Domain Trigger
	RO Acquisition Trigger	**a**	Leave Domain Trigger

6.1.4 Invalid Signature in Leave Domain trigger

Testcase ID	DRM-2.0-con-4
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 5.2.1 In case a **<leaveDomain>** element is present, the RI MUST include a **<signature>** element and, with one exception (see below), Devices MUST verify this signature. If the Device cannot verify the signature, the Device SHOULD inform the user and MUST discard the ROAP Trigger. The only exception to the verification requirement is when the Device is not a member of the identified Domain, and the trigger has been authenticated with a MAC based on the Domain Key. In this case the device may have to obtain user consent before initiating ROAP, section 5.1.8 defines when explicit user consent is required.
SCR Reference	
Preconditions	PKI : Model A State: - DRM Agent and RI Server have established an RI Context and the DRM Agent is a member of the Domain.
Test Procedure	- The DRM Agent receives a Leave Domain trigger with invalid signature.
Pass-Criteria	- The DRM Agent will not send the Leave Domain request.

Test Case Deployment			
	Registration Trigger		Join Domain Trigger
	RO Acquisition Trigger	**a**	Leave Domain Trigger

6.1.5 Missing Status attribute in ROAP Response

Testcase ID	DRM-2.0-con-5
Test Object	DRM Agent
Test Case Description	ROAP Response has no status attribute
Specification Reference	[DRM-v2.0] 5.3.6 Upon transmission or receipt of a message for which Status is not "Success", the default behaviour, unless explicitly stated otherwise below, is that both the RI and the Device SHALL immediately close the connection and terminate the protocol. RI systems and Devices are required to delete any session-identifiers, nonces, keys, and/or secrets associated with a failed run of the ROAP protocol.
SCR Reference	
Preconditions	PKI : Model A State: -
Test Procedure	- Necessary steps to prepare the following step. - The DRM Agent receives a ROAP Response without a status attribute
Pass-Criteria	- The DRM agent aborts the protocol
Test Case Deployment	

a	RI Hello processing	**d**	Join Domain Response processing
b	Reg. Response processing	**e**	Leave Domain Response processing
c	RO Responsep processing		

6.1.6 Status ≠ Success in ROAP Response

Testcase ID	DRM-2.0-con-6
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 5.3.6 Upon transmission or receipt of a message for which Status is not "Success", the default behaviour, unless explicitly stated otherwise below, is that both the RI and the Device SHALL immediately close the connection and terminate the protocol. RI systems and Devices are required to delete any session-identifiers, nonces, keys, and/or secrets associated with a failed run of the ROAP protocol.
SCR Reference	
Preconditions	PKI : Model A State: -
Test Procedure	- Necessary steps to prepare the following step. - The DRM Agent receives a ROAP Response with status abort.
Pass-Criteria	- DRM Agent aborts the ROAP protocol

Test Case Deployment			
a	RI Hello processing	**d**	Join Domain Response processing
b	Reg. Response processing	**e**	Leave Domain Response processing
c	RO Responsep processing		

6.1.7 Missing Signature in ROAP Response

Testcase ID	DRM-2.0-con-7
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 5.4.2.4.1 A Device MUST NOT accept the Registration protocol as successful unless the signature verifies,… [DRM-v2.0] 5.4.3.2 A Device MUST NOT accept the RO acquisition as successful unless the signature verifies,…. [DRM-v2.0] 5.4.4.2.1 A Device MUST NOT accept the Join Domain protocol as successful unless the signature verifies,…
SCR Reference	
Preconditions	PKI : Model A State: -
Test Procedure	- Necessary steps to prepare the following step. - The DRM Agent receives a ROAP Response that does not contain a <signature> element.
Pass-Criteria	- The DRM Agent detects the absence of the signature and aborts the protocol.
Test Case Deployment	

	RI Hello processing	**C**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Responsep processing		

6.1.8 Invalid Signature in ROAP Response

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-8</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">[DRM-v2.0] 5.4.2.4.1
A Device MUST NOT accept the Registration protocol as successful unless the signature verifies,…
[DRM-v2.0] 5.4.3.2
A Device MUST NOT accept the RO acquisition as successful unless the signature verifies,….
[DRM-v2.0] 5.4.4.2.1
A Device MUST NOT accept the Join Domain protocol as successful unless the signature verifies,…</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3">DRM-CLI-CMN-019</td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
-</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- Necessary steps to prepare the following step.
- The DRM Agent receives a ROAP Response that contains an invalid signature.</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent detects the invalid signature and aborts the protocol.</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td></td><td>RI Hello processing</td><td><b>c</b></td><td>Join Domain Response processing</td></tr>
<tr><td><b>a</b></td><td>Reg. Response processing</td><td></td><td>Leave Domain Response processing</td></tr>
<tr><td><b>b</b></td><td>RO Response processing</td><td></td><td></td></tr>
</table>

6.1.9 ROAP Response reception while expired RI context

Testcase ID	DRM-2.0-con-9
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 5.4.3.2 A Device MUST NOT accept the RO acquisition as successful unless the signature verifies,…. Section 5.4.2.4.1: However, if the Device does store RI certificate verification data in this way, it MUST store the expiry time of the RI's certificate (as indicated by the notAfter field within the certificate) in the RI Context and MUST compare the Device's current DRM Time with the stored RI certificate expiry time whenever verifying the signature on signed messages from the RI. If the Device's current DRM Time is after the stored RI certificate expiry time, then the Device MUST abandon processing the RI message and MUST initiate the registration protocol.
SCR Reference	DRM-CLI-CMN-028
Preconditions	PKI : Model A The Device supports storage of certificate validation data in the RI context. State: - DRM agent has no valid RI context
Test Procedure	- The DRM agent initiates a 4- pass registration protocol to create a RI context with RI certificate validation data. - Wait until the RI context is expired. - DRM agent receives a 1-pass RO Response with an RI ID that matches the RI ID of the RI context that has just expired.
Pass-Criteria	- The DRM Agent initiates the 4-pass registration protocol.

Test Case Deployment			
	RI Hello processing		Join Domain Response processing
	Reg. Response processing		Leave Domain Response processing
a	1-pass RO Response processing		

6.1.10 Missing signature in certificate chain of ROAP response

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="2">DRM-2.0-con-10</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="2">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="2">Missing signature in certificate chain of ROAP response</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="2">[DRM-v2.0] 5.4.2.4.1
A Device MUST NOT accept the Registration protocol as successful unless the signature verifies, the RI certificate chain has been successfully verified,…
[DRM-v2.0] 5.4.3.2
A Device MUST NOT accept the RO acquisition as successful unless the signature verifies, the RI certificate chain has been successfully verified,….
[DRM-v2.0] 5.4.4.2.1
A Device MUST NOT accept the Join Domain protocol as successful unless the signature verifies, the RI certificate chain has been successfully verified,…</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="2">PKI : Model A</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="2">- Necessary steps to prepare the following step.
- DRM Agent receives a ROAP response with a certificate chain with two certificates (one for the device and one for an intermediate CA). The Certificate for the intermediate CA has no signature.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="2">- The DRM Agent aborts the ROAP protocol</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td></td><td>RI Hello processing</td><td><b>c</b></td><td>Join Domain Response processing</td></tr>
<tr><td><b>a</b></td><td>Reg. Response processing</td><td></td><td>Leave Domain Response processing</td></tr>
<tr><td><b>b</b></td><td>RO Response processing</td><td></td><td></td></tr>
</table>

6.1.11 Invalid signature in certificate chain of ROAP response

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-11</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="3">[DRM-v2.0] 5.4.2.4.1
A Device MUST NOT accept the Registration protocol as successful unless the signature verifies, the RI certificate chain has been successfully verified,…
[DRM-v2.0] 5.4.3.2
A Device MUST NOT accept the RO acquisition as successful unless the signature verifies, the RI certificate chain has been successfully verified,….
[DRM-v2.0] 5.4.4.2.1
A Device MUST NOT accept the Join Domain protocol as successful unless the signature verifies, the RI certificate chain has been successfully verified,…</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="3">PKI : Model A</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="3">- Necessary steps to prepare the following step.
- DRM Agent receives a ROAP response with a certificate chain with two certificates (one for the device and one for an intermediate CA). The Certificate for the intermediate CA has an invalid signature.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent aborts the ROAP protocol</td></tr>
<tr><td colspan="5"><b>Test Case Deployment</b></td></tr>
<tr><td></td><td colspan="2">RI Hello processing</td><td><b>c</b></td><td>Join Domain Response processing</td></tr>
<tr><td><b>a</b></td><td colspan="2">Reg. Response processing</td><td></td><td>Leave Domain Response processing</td></tr>
<tr><td><b>b</b></td><td colspan="2">RO Responsep processing</td><td></td><td></td></tr>
</table>

6.1.12 Certificate chain of ROAP response – UTC time - NotBefore

Testcase ID	DRM-2.0-con-12
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 5.4.2.4.1 A Device MUST NOT accept the Registration protocol as successful unless the signature verifies, the RI certificate chain has been successfully verified, and the OCSP response indicates that the RI certificate status is `good`. [DRM-v2.0] 5.4.3.2 A Device MUST NOT accept the RO acquisition as successful unless the signature verifies, the RI certificate chain has been successfully verified, and the OCSP response indicates that the RI certificate status is `good`. [DRM-v2.0] 5.4.4.2.1 A Device MUST NOT accept the Join Domain protocol as successful unless the signature verifies, the RI certificate chain has been successfully verified, and the OCSP response indicates that the RI certificate status is `good`.
SCR Reference	
Preconditions	PKI : Model A
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with a certificate chain with two certificates (one for the device and one for an intermediate CA). The Certificate for the intermediate CA has a Validity 'NotBefore' condition that is not met. Time is expressed in UTC.
Pass-Criteria	- The DRM Agent aborts the ROAP protocol

Test Case Deployment			
	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Responsep processing		

6.1.13 Certificate chain of ROAP response – Gen. time - NotAfter

Testcase ID	DRM-2.0-con-13		
Test Object	DRM Agent		
Test Case Description	Certificate chain of ROAP Response. Condition for Validity/NotAfter not met. Time is expressed in Generalised time (see RFC3280).		
Specification Reference	[DRM-v2.0] 5.4.2.4.1 A Device MUST NOT accept the Registration protocol as successful unless the signature verifies, the RI certificate chain has been successfully verified, and the OCSP response indicates that the RI certificate status is `good`. [DRM-v2.0] 5.4.3.2 A Device MUST NOT accept the RO acquisition as successful unless the signature verifies, the RI certificate chain has been successfully verified, and the OCSP response indicates that the RI certificate status is `good`. [DRM-v2.0] 5.4.4.2.1 A Device MUST NOT accept the Join Domain protocol as successful unless the signature verifies, the RI certificate chain has been successfully verified, and the OCSP response indicates that the RI certificate status is `good`.		
SCR Reference			
Preconditions	PKI : Model A		
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with a certificate chain with two certificates (one for the device and one for an intermediate CA). The Certificate for the intermediate CA has a Validity 'NotAfter' condition that is not met. Time is expressed in Generalised time.		
Pass-Criteria	- The DRM Agent aborts the ROAP protocol		
Test Case Deployment			
	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Responsep processing		

6.1.14 RI Trust Anchor not in DRM Agent's Trusted Authorities

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-14</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="3">See section header</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="3">[DRM-v2.0] 5.4.2.2.1:
<i>Trusted Device Authorities</i> is a list of Device trust anchors recognized by the RI. This parameter is optional. The parameter is not sent if the RI already has the Device's certificate or otherwise is able to verify a signature made by the Device. If the parameter is present but empty, it indicates that the Device is free to choose any Device certificate to authenticate itself. Otherwise the Device MUST choose a certificate chaining back to one of the recognized trust anchors.</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- The device has only one Certificate Chain.</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="3">- Necessary steps to prepare the following step.
- DRM Agent receives an RIHello message that holds a Trusted Device Authorities List. This List contains only one CertID. This ID does not correspond to the CertID of the Trust Anchor of the Certificate chain of the DRM agent.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent aborts the ROAP protocol</td></tr>
<tr><td colspan="5"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td colspan="2">RI Hello processing</td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

6.1.15 Certificate chain of Registration Response not corresponding to RI Authority list

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-15</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="3">See section header</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="3">[DRM-v2.0] 5.4.2.4.1:
<i>Certificate chain:</i> This parameter MUST be present unless the preceding ROAP-RegistrationRequest message contained the <i>Peer Key Identifier</i> extension, the extension was not ignored by the RI, and its value identified the RI's current key. When present, the value of a <i>Certificate Chain</i> parameter shall be a certificate chain including the RI's certificate. The chain MUST NOT include the root certificate. The RI certificate must come first in the list. Each following certificate must directly certify the one preceding it. If the Device indicated trust anchor preferences in its ROAP-RegistrationRequest message, the RI SHOULD select a certificate and chain which chains back to one of the trust anchors in the Device's list. This mimics the features of [RFC3546].</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM Agent does not have validation data for the certificate chain.</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="3">- Necessary steps to prepare the following step.
- DRM Agent receives a Registration Response message that holds a Certificate chain of the RI that does not chain back to one of the Trust Anchors in the Trusted RI Authorities List of the corresponding Registration request.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent aborts the ROAP protocol</td></tr>
<tr><td colspan="5"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td colspan="2">Registration Response processing</td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

6.1.16 OCSP Handling / Missing OCSP response in ROAP response

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-16</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">[DRM-v2.0] 6.2:
A Device which did not send the <i>No OCSP Response</i> extension in its ROAP-Request message MUST check that an OCSP response is present in the received ROAP-Response message. If no OCSP response is present then the Device MUST abort the protocol.</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
-</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- Necessary steps to prepare the following step.
- DRM agent sends ROAP request without No OCSP Response extention.
- DRM Agent receives a ROAP response without an <ocspResponse> element.</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- DRM Agent aborts the ROAP protocol.</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td></td><td>RI Hello processing</td><td><b>c</b></td><td>Join Domain Response processing</td></tr>
<tr><td><b>a</b></td><td>Reg. Response processing</td><td></td><td>Leave Domain Response processing</td></tr>
<tr><td><b>b</b></td><td>RO Response processing</td><td></td><td></td></tr>
</table>

6.1.17 OCSP Handling / Missing signature in OCSP response

Testcase ID	DRM-2.0-con-17
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[OCSP-MP] 5.4.1 A Device MUST check the signature on a fresh response.
SCR Reference	
Preconditions	PKI : Model A State: - DRM Agent does not have cached OCSP responses
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with the OCSP response for the RI. The signature of this OCSP response is missing.
Pass-Criteria	- DRM Agent aborts the protocol
Test Case Deployment	

	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Responsep processing		

6.1.18 OCSP Handling / Invalid signature in OCSP response

Testcase ID	DRM-2.0-con-18		
Test Object	DRM Agent		
Test Case Description	Invalid signature in OCSP response		
Specification Reference	[OCSP-MP] 5.4.1 A Device MUST check the signature on a fresh response.		
SCR Reference			
Preconditions	PKI : Model A State: - DRM Agent does not have cached OCSP responses		
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with the OCSP response for the RI. The signature of this OCSP response is invalid.		
Pass-Criteria	- DRM Agent aborts the protocol		
Test Case Deployment			
	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Response processing		

6.1.19 OCSP Handling / OCSP response with status ≠ Successful

Testcase ID	DRM-2.0-con-19
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 6.2 A Device MUST verify signed RI responses and ROs. The signature verification MUST include a check of the validity of all the certificates in the RI certificate chain, and of the revocation status of all revocable certificates in the RI certificate chain,… The determination of which certificates in an RI certificate chain are revocable is deemed to be part of the trust model of the root of trust of that chain. In case the root of trust does not specify such a policy, devices SHALL assume a default model. In the default model only the RI certificate is revocable and requires an OCSP response to prove its status.
SCR Reference	
Preconditions	PKI : Model A State: - DRM Agent does not have cached OCSP responses
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with the OCSP response for the RI. The status of the OCSP response = 'internalError'
Pass-Criteria	- DRM Agent aborts the protocol

Test Case Deployment			
	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Responsep processing		

6.1.20 OCSP Handling / Validity period of OCSP response; thisUpdate

Testcase ID	DRM-2.0-con-20
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[OCSP-MP] 5.4.1 To ensure freshness of OCSP Clients MUST NOT accept a response that is out dated.
SCR Reference	
Preconditions	PKI : Model A State: - DRM Agent does not have cached OCSP responses
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with the OCSP response for the RI. The 'this Update' time of this OCSP response is too old.
Pass-Criteria	- The DRM Agent aborts the ROAP protocol
Test Case Deployment	

	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Response processing		

6.1.21 OCSP Handling / Validity period of OCSP response; nextUpdate

Testcase ID	DRM-2.0-con-21
Test Object	DRM Agent
Test Case Description	Not Fresh OCSP response; nextUpdate
Specification Reference	[OCSP-MP] 5.4.1 To ensure freshness of OCSP Clients MUST NOT accept a response that is out dated.
SCR Reference	
Preconditions	PKI : Model A State: - DRM Agent does not have cached OCSP responses
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with the OCSP response for the RI. The ‘nextUpdate’ time of this OCSP response is earlier than current DRM Time.
Pass-Criteria	- The DRM Agent aborts the ROAP protocol

Test Case Deployment			
	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Response processing		

6.1.22 OCSP Handling / Invalid CertID in OCSP response

Testcase ID	DRM-2.0-con-22
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[OCSP] 3.2 Prior to accepting a signed response as valid, the OCSP client shall confirm that the certificate identified in the received response corresponds to that which was identified in the corresponding request.
SCR Reference	
Preconditions	PKI : Model A State: -
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with the OCSP response for the RI. CertID in this OCSP response does not correspond to the CertID of the RI.
Pass-Criteria	- The DRM Agent aborts the ROAP protocol
Test Case Deployment	

	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Response processing		

6.1.23 OCSP Handling / Revocation Status OCSP response = ‘revoked’

Testcase ID	DRM-2.0-con-23
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 6.2 The Device MUST verify that the OCSP-provided status of all revocable certificates in the RI certificate chain is good. The determination of which certificates in an RI certificate chain are revocable is deemed to be part of the trust model of the root of trust of that chain. In case the root of trust does not specify such a policy, devices SHALL assume a default model. In the default model only the RI certificate is revocable and requires an OCSP response to prove its status.
SCR Reference	
Preconditions	PKI : Model A State: - DRM Agent does not have cached OCSP responses
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with the OCSP response for the RI. The cert. status of this response is ‘revoked’.
Pass-Criteria	- The DRM Agent aborts the ROAP protocol
Test Case Deployment	

	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Response processing		

6.1.24 OCSP Handling / Revocation Status OCSP response = ‘Unknown’

Testcase ID	DRM-2.0-con-24
Test Object	DRM Agent
Test Case Description	Cert. Status of OCSP response = ‘Unknown’
Specification Reference	[DRM-v2.0] 6.2 The Device MUST verify that the OCSP-provided status of all revocable certificates in the RI certificate chain is good. The determination of which certificates in an RI certificate chain are revocable is deemed to be part of the trust model of the root of trust of that chain. In case the root of trust does not specify such a policy, devices SHALL assume a default model. In the default model only the RI certificate is revocable and requires an OCSP response to prove its status.
SCR Reference	
Preconditions	PKI : Model A State: - DRM Agent does not have cached OCSP responses
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with the OCSP response for the RI. The cert. status of this response is ‘Unknown’.
Pass-Criteria	- The DRM Agent aborts the ROAP protocol

Test Case Deployment			
	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Response processing		

6.1.25 OCSP Handling / Missing signature in certificate of OCSP responder

Testcase ID	DRM-2.0-con-25
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 6.2 A Device MUST verify signed RI responses and ROs. The signature verification MUST include a check of the validity of all the certificates in the RI certificate chain, and of the revocation status of all revocable certificates in the RI certificate chain,… The determination of which certificates in an RI certificate chain are revocable is deemed to be part of the trust model of the root of trust of that chain. In case the root of trust does not specify such a policy, devices SHALL assume a default model. In the default model only the RI certificate is revocable and requires an OCSP response to prove its status.
SCR Reference	
Preconditions	PKI : Model A State: - DRM Agent does not have validation data for the certificate chain of the OCSP responder.
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with an OCSP response; The Certificate of the OCSP responder does not hold a signature.
Pass-Criteria	- The DRM Agent aborts the ROAP protocol
Test Case Deployment	

	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Response processing		

6.1.26 OCSP Handling / Invalid signature in certificate of OCSP Responder

Testcase ID	DRM-2.0-con-26
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 6.2 A Device MUST verify signed RI responses and ROs. The signature verification MUST include a check of the validity of all the certificates in the RI certificate chain, and of the revocation status of all revocable certificates in the RI certificate chain,… The determination of which certificates in an RI certificate chain are revocable is deemed to be part of the trust model of the root of trust of that chain. In case the root of trust does not specify such a policy, devices SHALL assume a default model. In the default model only the RI certificate is revocable and requires an OCSP response to prove its status.
SCR Reference	
Preconditions	PKI : Model A State: - DRM Agent does not have validation data for the certificate chain of the OCSP responder.
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with an OCSP response; The Certificate of the OCSP responder holds an invalid signature.
Pass-Criteria	- The DRM Agent aborts the ROAP protocol

Test Case Deployment			
	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Response processing		

6.1.27 OCSP Handling / Validity period OCSP Responder Certificate - NotBefore

Testcase ID	DRM-2.0-con-27		
Test Object	DRM Agent		
Test Case Description	See section header.		
Specification Reference	[DRM-v2.0] 6.2 A Device MUST verify signed RI responses and ROs. The signature verification MUST include a check of the validity of all the certificates in the RI certificate chain, and of the revocation status of all revocable certificates in the RI certificate chain,… The determination of which certificates in an RI certificate chain are revocable is deemed to be part of the trust model of the root of trust of that chain. In case the root of trust does not specify such a policy, devices SHALL assume a default model. In the default model only the RI certificate is revocable and requires an OCSP response to prove its status.		
SCR Reference			
Preconditions	PKI : Model A State: - DRM Agent does not have validation data for the certificate chain of the OCSP responder.		
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with an OCSP response. The Certificate for the OCSP responder has a Validity ‘NotBefore’ condition that is not met. Time is expressed in UTC.		
Pass-Criteria	- The DRM Agent aborts the ROAP protocol		
Test Case Deployment			
	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Response processing		

6.1.28 OCSP Handling / Validity period OCSP Responder Certificate - NotAfter

Testcase ID	DRM-2.0-con-28
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 6.2 A Device MUST verify signed RI responses and ROs. The signature verification MUST include a check of the validity of all the certificates in the RI certificate chain, and of the revocation status of all revocable certificates in the RI certificate chain,… The determination of which certificates in an RI certificate chain are revocable is deemed to be part of the trust model of the root of trust of that chain. In case the root of trust does not specify such a policy, devices SHALL assume a default model. In the default model only the RI certificate is revocable and requires an OCSP response to prove its status.
SCR Reference	PKI : Model A State: - DRM Agent does not have validation data for the certificate chain of the OCSP responder.
Preconditions	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with an OCSP response. The Certificate for the OCSP responder has a Validity 'NotAfter' condition that is not met. Time is expressed in Generalised time.
Test Procedure	- The DRM Agent aborts the ROAP protocol
Pass-Criteria	DRM Agent

Test Case Deployment			
	RI Hello processing	**c**	Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
b	RO Response processing		

6.1.29 Missing Session ID in registration response

Testcase ID	DRM-2.0-con-29
Test Object	DRM agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 5.4.2.3.1 *Session ID* SHALL be identical to the *Session ID* parameter of the preceding ROAP-RIHello message, otherwise the RI SHALL terminate the Registration protocol. [DRM-v2.0] 5.4.2.4.1 *Session ID* SHALL be identical to the *Session ID* of the preceding ROAP-RegistrationRequest (and ROAP-RIHello) message. If the Session ID of the ROAP-RegistrationResponse does not equal the Session ID of the corresponding ROAP-RIHello, the Device MUST terminate the protocol. The Session ID can be present only if the Rights Issuer could detect the session identifier in the registration request.
SCR Reference	-
Preconditions	PKI : Model A State: -
Test Procedure	- Agent initiates 4-pass registration with the RI - The DRM agent receives a Registration Response message without sessionId attribute.
Pass-Criteria	- Device sends DeviceHello; RI responds with RIHello containing a SessionID; Device sends a RegistrationRequest WITH the same SessionID. - DRM agent aborts the registration protocol

Test Case Deployment			
a	Reg. Response processing		

6.1.30 Invalid Session ID in registration response

Testcase ID	DRM-2.0-con-30
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 5.4.2.4.1 *Session ID* SHALL be identical to the *Session ID* of the preceding ROAP-RegistrationRequest (and ROAP-RIHello) message. If the Session ID of the ROAP-RegistrationResponse does not equal the Session ID of the corresponding ROAP-RIHello, the Device MUST terminate the protocol. The Session ID can be present only if the Rights Issuer could detect the session identifier in the registration request.
SCR Reference	
Preconditions	PKI : Model A State: -
Test Procedure	- *Necessary steps to prepare the following step.* - The DRM agent receives a Registration Response with invalid session id.
Pass-Criteria	- The DRM agent aborts the registration protocol.
Test Case Deployment	

a	Reg. Response processing		

6.1.31 Missing Device ID in ROAP response; 2 pass RO acquisition and Join Domain.

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-31</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">[DRM-v2.0] 5.4.3.2.1
<i>Device ID</i> identifies the requesting Device, in the same manner as in the ROAP-DeviceHello message as specified in section 5.4.2.1.1. The value returned here MUST equal the Device ID sent by the Device in the ROAP-RORequest message that triggered this response in the 2-pass ROAP. In the 1-pass ROAP, the RI selects the Device ID of the recipient Device. If the Device ID is incorrect, the ROAP-ROResponse processing will fail and the Device MUST discard the received ROResponse PDU.
[DRM-v2.0] 5.4.4.2.1
<i>Device ID</i> identifies the requesting Device. The value returned here MUST equal the Device ID sent by the Device in the ROAP-JoinDomainRequest message that triggered this response.</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
-</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- <i>Necessary steps to prepare the following step.</i>
- The DRM agent receives a ROAP Response without a <deviceID> element.</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- The DRM agent aborts the ROAP protocol.</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>RO Response processing</td><td><b>b</b></td><td>Join Domain Response processing</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.32 Invalid Device ID in ROAP response; 2 pass RO acquisition and Join Domain.

Testcase ID	DRM-2.0-con-32
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 5.4.3.2.1 *Device ID* identifies the requesting Device, in the same manner as in the ROAP-DeviceHello message as specified in section 5.4.2.1.1. The value returned here MUST equal the Device ID sent by the Device in the ROAP-RORequest message that triggered this response in the 2-pass ROAP. In the 1-pass ROAP, the RI selects the Device ID of the recipient Device. If the Device ID is incorrect, the ROAP-ROResponse processing will fail and the Device MUST discard the received ROResponse PDU. [DRM-v2.0] 5.4.4.2.1 *Device ID* identifies the requesting Device. The value returned here MUST equal the Device ID sent by the Device in the ROAP-JoinDomainRequest message that triggered this response.
SCR Reference	-
Preconditions	PKI : Model A State: -
Test Procedure	- *Necessary steps to prepare the following step.* - The DRM agent receives a ROAP Response with Device ID not equal to DeviceID in corresponding request.
Pass-Criteria	- The DRM agent aborts the registration protocol.

Test Case Deployment			
a	RO Response processing	**b**	Join Domain Response processing

6.1.33 Missing Device ID in 1 pass RO response.

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-33</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="3"></td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="3">[DRM-v2.0] 5.4.3.2.1
<i>Device ID</i> identifies the requesting Device, in the same manner as in the ROAP-DeviceHello message as specified in section 5.4.2.1.1. The value returned here MUST equal the Device ID sent by the Device in the ROAP-RORequest message that triggered this response in the 2-pass ROAP. In the 1-pass ROAP, the RI selects the Device ID of the recipient Device. If the Device ID is incorrect, the ROAP-ROResponse processing will fail and the Device MUST discard the received ROResponse PDU.</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
-</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="3">- <i>Necessary steps to prepare the following step.</i>
- The DRM agent receives a 1-pass ROResponse without a <deviceID> element.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="3">- The DRM agent aborts the RO Response processing.</td></tr>
<tr><td colspan="5"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td colspan="2">RO Response processing</td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

6.1.34 Invalid Device ID in 1 pass RO response.

Testcase ID	DRM-2.0-con-34
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 5.4.3.2.1 *Device ID* identifies the requesting Device, in the same manner as in the ROAP-DeviceHello message as specified in section 5.4.2.1.1. The value returned here MUST equal the Device ID sent by the Device in the ROAP-RORequest message that triggered this response in the 2-pass ROAP. In the 1-pass ROAP, the RI selects the Device ID of the recipient Device. If the Device ID is incorrect, the ROAP-ROResponse processing will fail and the Device MUST discard the received ROResponse PDU.
SCR Reference	
Preconditions	PKI : Model A State: -
Test Procedure	- *Necessary steps to prepare the following step.* - The DRM agent receives a ROAP Response with Device ID that does not match any of the DeviceID's of the DRM Agent.
Pass-Criteria	- The DRM agent aborts the RO response processing.

Test Case Deployment			
a	RO Response processing		

6.1.35 Missing Device Nonce in ROAP response

Testcase ID	DRM-2.0-con-35
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 5.4.3.2.1 *Device Nonce*: This parameter, if present (2-pass), MUST have the same value as the corresponding parameter value in the preceding ROAP-RORequest. Section 5.4.4.2.1 *Device Nonce*: This parameter MUST have the same value as the corresponding parameter value in the preceding ROAP-JoinDomainRequest. Section 5.4.4.4.1 *Device Nonce* is the nonce sent by the Device. This parameter MUST have the same value as the corresponding parameter value in the preceding ROAP-LeaveDomainRequest.
SCR Reference	
Preconditions	PKI : Model A State: -
Test Procedure	- *Necessary steps to prepare the following step.* - The DRM agent receives a ROAP Response without a Device Nonce (<nonce> element).
Pass-Criteria	- The DRM agent aborts the ROAP protocol.

Test Case Deployment			
a	RO Response processing	**a**	Join Domain Response processing
		b	Leave Domain Response

6.1.36 Invalid Device Nonce in ROAP response

Testcase ID	DRM-2.0-con-36		
Test Object	DRM Agent		
Test Case Description	See section header.		
Specification Reference	Section 5.4.3.2.1 *Device Nonce*: This parameter, if present (2-pass), MUST have the same value as the corresponding parameter value in the preceding ROAP-RORequest. Section 5.4.4.2.1 *Device Nonce*: This parameter MUST have the same value as the corresponding parameter value in the preceding ROAP-JoinDomainRequest. Section 5.4.4.4.1 *Device Nonce* is the nonce sent by the Device. This parameter MUST have the same value as the corresponding parameter value in the preceding ROAP-LeaveDomainRequest.		
SCR Reference			
Preconditions	PKI : Model A State: -		
Test Procedure	- *Necessary steps to prepare the following step.* - The DRM agent receives a ROAP Response with invalid Device Nonce.		
Pass-Criteria	- The DRM agent aborts the ROAP protocol.		
Test Case Deployment			
a	RO Response processing	**b**	Join Domain Response processing
		c	Leave Domain Response

6.1.37 Missing RI ID in ROAP response

Testcase ID	DRM-2.0-con-37		
Test Object	DRM Agent		
Test Case Description	See section header.		
Specification Reference	[DRM-v2.0] 5.4.3.2.1 *RI ID* identifies the RI. In the 2-pass protocol, the value MUST equal the RI ID sent by the Device in the preceding ROAP-RORequest message. [DRM-v2.0] 5.4.4.2.1 *RI ID* identifies the RI. The value returned here MUST equal the RI ID sent by the Device in the preceding ROAP-JoinDomainRequest message.		
SCR Reference			
Preconditions	PKI : Model A State: -		
Test Procedure	- *Necessary steps to prepare the following step.* - The DRM agent receives a ROAP Response without an <riID> element.		
Pass-Criteria	- The DRM agent aborts the ROAP protocol.		
Test Case Deployment			
a	RO Response processing	**b**	Join Domain Response processing

6.1.38 Invalid RI ID in ROAP response

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="2">DRM-2.0-con-38</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="2">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="2">See section header.</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="2">[DRM-v2.0] 5.4.3.2.1
<i>RI ID</i> identifies the RI. In the 2-pass protocol, the value MUST equal the RI ID sent by the Device in the preceding ROAP-RORequest message.
[DRM-v2.0] 5.4.4.2.1
<i>RI ID</i> identifies the RI. The value returned here MUST equal the RI ID sent by the Device in the preceding ROAP-JoinDomainRequest message.</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="2">PKI : Model A
State:
-</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="2">- <i>Necessary steps to prepare the following step.</i>
- The DRM agent receives a ROAP Response with invalid RI ID.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="2">- The DRM agent aborts the ROAP protocol.</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>RO Response processing</td><td><b>b</b></td><td>Join Domain Response processing</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.39 DRM Time Synchronise Triggered by Reg. Response

Testcase ID	DRM-2.0-con-39
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 6.3 A Device, which receives a ROAP-RegistrationResponse message containing a nonce-based OCSP response where the nonce in the OCSP response matches the nonce sent in the Device's ROAP-RegistrationRequest, MUST adjust its time to match the time in the producedAt component of the OCSP response, assuming the Registration protocol exchange otherwise was successful. Barring network latency and response times, the procedure described here will synchronize the Device's DRM Time with the OCSP responder's.
SCR Reference	
Preconditions	PKI : Model A State: - DRM Agent supports DRM Time
Test Procedure	- Necessary steps to prepare the following step. - DRM Agent receives a ROAP response with a nonce based OCSP response.
Pass-Criteria	- The DRM Agent updates the DRM Time.
Test Case Deployment	

	RI Hello processing		Join Domain Response processing
a	Reg. Response processing		Leave Domain Response processing
	RO Responsep processing		

6.1.40 Install Device RO from RO Response; Invalid Signature

Testcase ID	DRM-2.0-con-40
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 9.3.1.3: When a Device receives a Device RO through a successful execution of the RO Acquisition protocol, it MUST proceed as follows: Verifications: If the Device RO was signed (i.e. the **<signature>** element is present in the **roap:ROPayload**), the Device MUST verify the signature using the RI's Public Key. The Device MUST verify the MAC on the Device RO using the **<mac>** element of the **roap:ProtectedRO**. The Device MUST verify that the **<riID>** element of the **roap:ROPayload** identifies the same RI as signed the **roap:ROResponse** message. The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail. Likewise, Device ROs received in unsuccessful executions of the RO Acquisition protocol MUST NOT be installed.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent successfully processes a RO acquisition response with a RO payload that holds signature but the signature is invalid.
Pass-Criteria	- The DRM Agent does not install the RO

Test Case Deployment			
a	RO Response Processing		

6.1.41 Install Device RO from RO Response; Missing MAC element

Testcase ID	DRM-2.0-con-41
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 9.3.1.3: When a Device receives a Device RO through a successful execution of the RO Acquisition protocol, it MUST proceed as follows: Verifications: If the Device RO was signed (i.e. the **<signature>** element is present in the **roap:ROPayload**), the Device MUST verify the signature using the RI’s Public Key. The Device MUST verify the MAC on the Device RO using the **<mac>** element of the **roap:ProtectedRO**. The Device MUST verify that the **<riID>** element of the **roap:ROPayload** identifies the same RI as signed the **roap:ROResponse** message. The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail. Likewise, Device ROs received in unsuccessful executions of the RO Acquisition protocol MUST NOT be installed.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent successfully processes a RO acquisition response with a Device RO. The <mac> element in the Protected RO is missing.
Pass-Criteria	- The DRM Agent does not install the Device RO

Test Case Deployment			
a	RO Response Processing		

6.1.42 Install Device RO from RO Response; Invalid MAC element

Testcase ID	DRM-2.0-con-42
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 9.3.1.3: When a Device receives a Device RO through a successful execution of the RO Acquisition protocol, it MUST proceed as follows: Verifications: If the Device RO was signed (i.e. the **<signature>** element is present in the **roap:ROPayload**), the Device MUST verify the signature using the RI's Public Key. The Device MUST verify the MAC on the Device RO using the **<mac>** element of the **roap:ProtectedRO**. The Device MUST verify that the **<riID>** element of the **roap:ROPayload** identifies the same RI as signed the **roap:ROResponse** message. The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail. Likewise, Device ROs received in unsuccessful executions of the RO Acquisition protocol MUST NOT be installed.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent successfully processes a RO acquisition response with a Device RO. The MAC in the Protected RO is invalid.
Pass-Criteria	- The DRM Agent does not install the Device RO
Test Case Deployment	

a	RO Response Processing		

6.1.43 Install Device RO from RO Response; Missing RI ID

<table>
<tr><td colspan="2">**Testcase ID**</td><td colspan="3">DRM-2.0-con-43</td></tr>
<tr><td colspan="2">**Test Object**</td><td colspan="3">DRM Agent</td></tr>
<tr><td colspan="2">**Test Case Description**</td><td colspan="3">See section header.</td></tr>
<tr><td colspan="2">**Specification Reference**</td><td colspan="3">Section 9.3.1.3:
When a Device receives a Device RO through a successful execution of the RO Acquisition protocol, it MUST proceed as follows:
Verifications:
If the Device RO was signed (i.e. the **<signature>** element is present in the **roap:ROPayload**), the Device MUST verify the signature using the RI's Public Key.
The Device MUST verify the MAC on the Device RO using the **<mac>** element of the **roap:ProtectedRO**.
The Device MUST verify that the **<riID>** element of the **roap:ROPayload** identifies the same RI as signed the **roap:ROResponse** message.
The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail. Likewise, Device ROs received in unsuccessful executions of the RO Acquisition protocol MUST NOT be installed.</td></tr>
<tr><td colspan="2">**SCR Reference**</td><td colspan="3"></td></tr>
<tr><td colspan="2">**Preconditions**</td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context</td></tr>
<tr><td colspan="2">**Test Procedure**</td><td colspan="3">- DRM agent successfully processes an RO acquisition response that holds a Device RO without an <riID> element in the RO Payload.</td></tr>
<tr><td colspan="2">**Pass-Criteria**</td><td colspan="3">- The DRM Agent does not install the Device RO</td></tr>
<tr><td colspan="5">**Test Case Deployment**</td></tr>
<tr><td>**a**</td><td colspan="2">RO Response Processing</td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

6.1.44 Install Device RO from RO Response; Invalid RI ID

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="2">DRM-2.0-con-44</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="2">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="2">See section header.</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="2">Section 9.3.1.3:
When a Device receives a Device RO through a successful execution of the RO Acquisition protocol, it MUST proceed as follows:
Verifications:
If the Device RO was signed (i.e. the <b><signature></b> element is present in the <b>roap:ROPayload</b>), the Device MUST verify the signature using the RI's Public Key.
The Device MUST verify the MAC on the Device RO using the <b><mac></b> element of the <b>roap:ProtectedRO</b>.
The Device MUST verify that the <b><riID></b> element of the <b>roap:ROPayload</b> identifies the same RI as signed the <b>roap:ROResponse</b> message.
The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail. Likewise, Device ROs received in unsuccessful executions of the RO Acquisition protocol MUST NOT be installed.</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="2">PKI : Model A
State:
- DRM agent has a valid RI context</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="2">- DRM agent successfully processes a RO acquisition response that holds a Device RO with RI ID in RO Payload that does not match with the RI ID that signed the RO Response.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="2">- The DRM Agent does not install the Device RO</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>RO Response Processing</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.45 Install Device RO from DCF; Missing Signature

Testcase ID	DRM-2.0-con-45
Test Object	DRM Agent
Test Case Description	See section Header.
Specification Reference	Section 9.3.1.3: The Device MAY support receiving a Device RO in other ways than through a successful execution of the RO Acquisition protocol. In this case, the device MUST proceed as follows: Verifications: The device MUST verify that the signature (i.e. the **<signature>** element in the **roap:ROPayload**) is present The Device MUST verify the signature using the RI's Public Key. The Device MUST verify the MAC on the Device RO using the **<mac>** element of the **roap:ProtectedRO**. The Device MUST verify that the **<riID>** element of the **roap:ROPayload** matches the RI Identifier in any valid RI context The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent receives a Device RO in a DCF without a <signature> element in the RO Payload.
Pass-Criteria	- The DRM Agent does not install the Device RO
Test Case Deployment	

a	DCF processing		

6.1.46 Install Device RO from DCF; Invalid Signature

Testcase ID	DRM-2.0-con-46
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 9.3.1.3: The Device MAY support receiving a Device RO in other ways than through a successful execution of the RO Acquisition protocol. In this case, the device MUST proceed as follows: Verifications: The device MUST verify that the signature (i.e. the **<signature>** element in the **roap:ROPayload**) is present The Device MUST verify the signature using the RI's Public Key. The Device MUST verify the MAC on the Device RO using the **<mac>** element of the **roap:ProtectedRO**. The Device MUST verify that the **<riID>** element of the **roap:ROPayload** matches the RI Identifier in any valid RI context The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent receives a Device RO in DCF with invalid signature in RO Payload.
Pass-Criteria	- The DRM Agent does not install the Device RO
Test Case Deployment	

a	DCF processing		

6.1.47 Install Device RO from DCF; Missing MAC element

Testcase ID	DRM-2.0-con-47
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 9.3.1.3: The Device MAY support receiving a Device RO in other ways than through a successful execution of the RO Acquisition protocol. In this case, the device MUST proceed as follows: Verifications: The device MUST verify that the signature (i.e. the **<signature>** element in the **roap:ROPayload**) is present The Device MUST verify the signature using the RI's Public Key. The Device MUST verify the MAC on the Device RO using the **<mac>** element of the **roap:ProtectedRO**. The Device MUST verify that the **<riID>** element of the **roap:ROPayload** matches the RI Identifier in any valid RI context The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent receives a DCF with a Device RO without a <mac> element.
Pass-Criteria	- The DRM Agent does not install the Device RO

Test Case Deployment			
a	DCF processing		

6.1.48 Install Device RO from DCF; Invalid MAC element

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="2">DRM-2.0-con-48</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="2">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="2">See section header.</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="2">Section 9.3.1.3:
The Device MAY support receiving a Device RO in other ways than through a successful execution of the RO Acquisition protocol. In this case, the device MUST proceed as follows:
Verifications:
The device MUST verify that the signature (i.e. the <b><signature></b> element in the <b>roap:ROPayload</b>) is present
The Device MUST verify the signature using the RI’s Public Key.
The Device MUST verify the MAC on the Device RO using the <b><mac></b> element of the <b>roap:ProtectedRO</b>.
The Device MUST verify that the <b><riID></b> element of the <b>roap:ROPayload</b> matches the RI Identifier in any valid RI context
The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail.</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="2">PKI : Model A
State:
- DRM agent has a valid RI context</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="2">- DRM agent receives a DCF with a Device RO with invalid MAC element</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="2">- The DRM Agent does not install the Device RO</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>DCF processing</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.49 Install Device RO from DCF; Missing RI ID

Testcase ID	DRM-2.0-con-49
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 9.3.1.3: The Device MAY support receiving a Device RO in other ways than through a successful execution of the RO Acquisition protocol. In this case, the device MUST proceed as follows: Verifications: The device MUST verify that the signature (i.e. the **<signature>** element in the **roap:ROPayload**) is present The Device MUST verify the signature using the RI's Public Key. The Device MUST verify the MAC on the Device RO using the **<mac>** element of the **roap:ProtectedRO**. The Device MUST verify that the **<riID>** element of the **roap:ROPayload** matches the RI Identifier in any valid RI context The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent receives a DCF wth a Device RO without an <riID> element in the RO Payload.
Pass-Criteria	- The DRM Agent does not install the Device RO
Test Case Deployment	

a	DCF processing		

6.1.50 Install Device RO from DCF; Invalid RI ID

Testcase ID	DRM-2.0-con-50
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 9.3.1.3: The Device MAY support receiving a Device RO in other ways than through a successful execution of the RO Acquisition protocol. In this case, the device MUST proceed as follows: Verifications: The device MUST verify that the signature (i.e. the **<signature>** element in the **roap:ROPayload**) is present The Device MUST verify the signature using the RI's Public Key. The Device MUST verify the MAC on the Device RO using the **<mac>** element of the **roap:ProtectedRO**. The Device MUST verify that the **<riID>** element of the **roap:ROPayload** matches the RI Identifier in any valid RI context The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent receives a DCF with a Device RO with RI ID in RO Payload that does not match the RI ID of any valid RI context.
Pass-Criteria	- The DRM Agent does not install the Device RO
Test Case Deployment	

a	DCF processing		

6.1.51 Install Device RO from DCF; RI Context Expired

Testcase ID	DRM-2.0-con-51
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 9.3.1.3: The Device MAY support receiving a Device RO in other ways than through a successful execution of the RO Acquisition protocol. In this case, the device MUST proceed as follows: Verifications: The device MUST verify that the signature (i.e. the **<signature>** element in the **roap:ROPayload**) is present The Device MUST verify the signature using the RI's Public Key. The Device MUST verify the MAC on the Device RO using the **<mac>** element of the **roap:ProtectedRO**. The Device MUST verify that the **<riID>** element of the **roap:ROPayload** matches the RI Identifier in any valid RI context The Device MUST inform the user and MUST NOT install the Device RO if any of the above verifications fail. Section 5.4.2.4.1: However, if the Device does store RI certificate verification data in this way, it MUST store the expiry time of the RI's certificate (as indicated by the notAfter field within the certificate) in the RI Context and MUST compare the Device's current DRM Time with the stored RI certificate expiry time whenever verifying the signature on signed messages from the RI. If the Device's current DRM Time is after the stored RI certificate expiry time, then the Device MUST abandon processing the RI message and MUST initiate the registration protocol.
SCR Reference	
Preconditions	PKI : Model A The Device supports storage of certificate validation data in the RI context. State: - DRM agent no valid RI context
Test Procedure	- The DRM agent initiates a 4- pass registration protocol to create a RI context. - Wait until the RI context is expired. - DRM agent receives a DCF with a Device RO that holds a Signature and with RI ID in RO Payload that matches the RI ID RI context that has just expired.
Pass-Criteria	- The DRM Agent does not install the Device RO
Test Case Deployment	

a	DCF processing		

6.1.52 Consume rights in Device RO; Invalid Hash value

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-52</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="3">Section 9.1:
For integrity protection of the DCF, a cryptographic hash value of the DCF MAY BE generated and inserted into the Rights Object. This hash value MUST BE generated according to the DCF hash calculation procedure specified in section |12.4. If the Rights Object contains a DCF hash value, DRM Agents in client Devices MUST verify that this hash value is identical to the hash value calculated by the DRM Agent over the DCF. If the hash values are not identical, the DRM Agent MUST prohibit the DCF from being decrypted and used.</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="3">- DRM agent receives a DCF.
- DRM agent receives a Device RO in a RO Response. The Hash value in Rights object is not equal to the Hash value of the corresponding DCF.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent installs the Device RO
- The DRM Agent does not allow rendering of the DCF.</td></tr>
<tr><td colspan="5"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td colspan="2">DCF rendering</td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

6.1.53 Install Domain Context; Missing MAC

Testcase ID	DRM-2.0-con-53
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 5.4.4.2.2: The **<mac>** element provides key-confirmation through a MAC on the canonical version according to Section 5.3.3 of the **<domainKey>** element (excluding the **<mac>** element itself) using the MAC key K_{MAC} wrapped in the **<encKey>** element. The MAC algorithm to use is defined by the RI Context. Devices MUST NOT install domain keys where the MAC is invalid.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent receives Join Domain Response that holds a Protected DomainKey without a <mac> element.
Pass-Criteria	- The DRM Agent does not install the Domainkey (domain context).

Test Case Deployment			
a	Join Domain Response Processing		

6.1.54 Install Domain Context; Invalid MAC

Testcase ID	DRM-2.0-con-54		
Test Object	DRM Agent		
Test Case Description	Install Domain Context; Invalid MAC		
Specification Reference	Section 5.4.4.2.2: The **<mac>** element provides key-confirmation through a MAC on the canonical version according to Section 5.3.3 of the **<domainKey>** element (excluding the **<mac>** element itself) using the MAC key K_{MAC} wrapped in the **<encKey>** element. The MAC algorithm to use is defined by the RI Context. Devices MUST NOT install domain keys where the MAC is invalid.		
SCR Reference			
Preconditions	PKI : Model A State: - DRM agent has a valid RI context		
Test Procedure	- DRM agent receives Join Domain Response that holds a Protected DomainKey with invalid <mac> element.		
Pass-Criteria	- The DRM Agent does not install the Domainkey (domain context).		
Test Case Deployment			
a	Join Domain Response Processing		

6.1.55 Install Domain Context; Missing RI ID in DomainKey

Testcase ID	DRM-2.0-con-55
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 5.4.4.2.2: The **<riID>** element is necessary for key confirmation purposes. A Device MUST verify that it has the same value as the **<riID>** element of the ROAP-JoinDomainResponse message itself.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent receives Join Domain Response that holds a Protected DomainKey without an <riID> element.
Pass-Criteria	- The DRM Agent does not install the Domainkey (domain context).

Test Case Deployment			
a	Join Domain Response Processing		

6.1.56 Install Domain Context; Invalid RI ID in DomainKey

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-56</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="3">Section 5.4.4.2.2:
The <b>&lt;riID&gt;</b> element is necessary for key confirmation purposes. A Device MUST verify that it has the same value as the <b>&lt;riID&gt;</b> element of the ROAP-JoinDomainResponse message itself.</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="3">- DRM agent receives Join Domain Response that holds a Protected DomainKey with a mismatched RI ID (i.e. the <riID> element contains a different value to the JoinDomainResponse message).</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent does not install the Domainkey (domain context).</td></tr>
<tr><td colspan="5"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td colspan="2">Join Domain Response Processing</td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

6.1.57 Delete Domain Context

Testcase ID	DRM-2.0-con-57		
Test Object	DRM Agent		
Test Case Description	See section header.		
Specification Reference	Section 5.4.4.3.1: The Device MUST ensure that the Domain Context of the corresponding Domain is deleted **before** sending the ROAP-LeaveDomainRequest to the RI.		
SCR Reference			
Preconditions	PKI : Model A State: - DRM agent has a valid Domain context and valid RI Context		
Test Procedure	- DRM agent sends Leave Domain Request - (DRM agent does not receive a Leave Domain Response) - DRM agent receives Domain RO for domain that has been deleted		
Pass-Criteria	- The DRM Agent does not install the Domain RO		
Test Case Deployment			
a	Leave Domain Request Processing		

6.1.58 Install Domain RO; No valid RI context with corresponding RI ID

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-58</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">Section 8.7.2.1:
When a Device receives a Domain RO, it MUST determine if it has a valid RI Context with the RI that issued the RO, by comparing the value of the <b>roap:ROPayload</b>‘s <b><riID></b> element with the RI Identifiers in all valid RI Contexts stored in the Device. If the value of the <b><riID></b> element does not match that of an RI Identifier in a valid RI Context, the device SHALL NOT install the Domain RO.</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has no valid RI context</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- The DRM Agent receives a DCF with a Domain RO. The RI ID of the Domain RO does not correspond to any of the valid RI contexts stored in the device.</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent does not install the Domain RO</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Domain RO processing</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.59 Install Domain RO; Missing Signature

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-59</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">Section 8.7.2.1:
The Device MUST verify the signature of the Domain RO using the RI's Public Key. If the verification fails the Device SHALL NOT install the Domain RO.</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- DRM agent successfully processes a RO acquisition response that holds a Domain RO without a <signature> element in the RO Payload</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent does not install the Domain RO</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Domain RO processing</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.60 Install Domain RO; Invalid Signature

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-60</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">Section 8.7.2.1:
The Device MUST verify the signature of the Domain RO using the RI's Public Key. If the verification fails the Device SHALL NOT install the Domain RO.</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- DRM agent successfully processes a RO acquisition response that holds a Domain RO with invalid signature in RO Payload</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent does not install the Domain RO</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Domain RO processing</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.61 Install Domain RO; Missing Domain ID

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-61</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">Section 5.3.9:
The <ds:KeyInfo> child element of the <encKey> element SHALL identify the wrapping key. In the case of a Rights Object intended for a Device, ... In the case of a Rights Object intended for a Domain, it will be of the type <roap:domainID> element, identifying the correct Domain key.
Section 8.7.2.1:
2. The Domain baseID of the <b><domainID></b> field matches the Domain baseID of a stored Domain identifier in a valid Domain Context already established with the RI, but the Domain Generation of the RO is greater than the Generation of the stored domain ID. The device MAY attempt to upgrade the Domain by sending a ROAP-JoinDomainRequest to the riURL in the Domain Context. The Device may have to obtain user consent to contact the RI, section 5.1.8 defines when explicit user consent is required
If the Domain upgrade is successful, the Device MAY install the Domain RO. Otherwise the Device SHALL NOT install the Domain RO.</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- DRM agent successfully processes a RO acquisition response that holds a Domain RO without a <roap:domain ID> element in the <ds:KeyInfo> element of the <encKey> element in the RO Payload</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent does not install the Domain RO</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Domain RO processing</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.62 Install Domain RO; Invalid Domain Generation

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-62</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">Section 5.4.4.1.2
The following schema fragment defines the <b>roap:DomainIdentifier</b> type. The last three characters (digits) represent the Domain Generation (see section 8.8 for further information). The other, preceding characters represent the Domain baseID.</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context
- DRM agent has a valid Domain Context</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- DRM agent successfully processes a RO acquisition response that holds a Domain RO with invalid Domain Generation (e.g. containing alpha characters).</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent does not install the Domain RO.</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Domain RO processing</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.63 Install Domain RO; Device not in the domain.

Testcase ID	DRM-2.0-con-63
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 8.7.2.1: 3. The Domain baseID of the **<domainID>** field does not match a Domain baseID in any valid Domain Context already established with the RI. The Device MAY attempt to join the Domain by sending an HTTP GET request to the URL specified in the ***riURL*** attribute of the **roap:ROPayload**.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent successfully processes a RO acquisition response that holds a Domain RO with invalid Domain baseID.
Pass-Criteria	- The DRM Agent does not install the Domain RO OR - The DRM Agent sends a HTTP GET Request to the roap:ROPayload and handles the response.

Test Case Deployment			
a	Domain RO processing		

6.1.64 Install Domain RO; Missing MAC.

Testcase ID	DRM-2.0-con-64
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 8.7.2.1: Before installing a Domain RO, the Device MUST successfully verify the MAC (using the **<mac>** element of the **roap:ProtectedRO**). If this verification fails, the Device SHALL NOT install the Domain RO.
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context
Test Procedure	- DRM agent successfully processes a RO acquisition response that holds a Protected Domain RO without a <mac> element.
Pass-Criteria	- The DRM Agent does not install the Domain RO
Test Case Deployment	

a	Domain RO processing		

6.1.65 Install Domain RO; Invalid MAC.

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-65</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">Section 8.7.2.1:
Before installing a Domain RO, the Device MUST successfully verify the MAC (using the <b><mac></b> element of the <b>roap:ProtectedRO</b>). If this verification fails, the Device SHALL not install the Domain RO.</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- DRM agent successfully processes a RO acquisition response that holds a Protected Domain RO with invalid MAC.</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent does not install the Domain RO</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Domain RO processing</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.66 Install Domain RO; RI Context Expired

Testcase ID	DRM-2.0-con-66
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 8.7.2.1: The Device MUST verify the signature of the Domain RO using the RI's Public Key. If the verification fails the Device SHALL NOT install the Domain RO. Section 5.4.2.4.1: However, if the Device does store RI certificate verification data in this way, it MUST store the expiry time of the RI's certificate (as indicated by the notAfter field within the certificate) in the RI Context and MUST compare the Device's current DRM Time with the stored RI certificate expiry time whenever verifying the signature on signed messages from the RI. If the Device's current DRM Time is after the stored RI certificate expiry time, then the Device MUST abandon processing the RI message and MUST initiate the registration protocol.
SCR Reference	
Preconditions	PKI : Model A The Device supports storage of certificate validation data in the RI context. State: - DRM agent no valid RI context
Test Procedure	- The DRM agent initiates a 4- pass registration protocol to create a RI context. - Wait until the RI context is expired. - DRM agent receives a DCF with a Domain RO with RI ID in RO Payload that matches the RI ID RI context that has just expired.
Pass-Criteria	- The DRM Agent discards the Domain RO
Test Case Deployment	

a	Domain RO processing		

6.1.67 Replay protection – Stateful RO with RITS; Future RITS

Testcase ID	DRM-2.0-con-67
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	Section 9.4.2.1: When receiving a stateful RO with a **<timestamp>** element (RITS), the Device MUST perform the following procedure: a) If the RITS is more than 24 hours in the future when compared to the Device's DRM Time then the Device MUST reject the RO. The user MUST be informed of the event and of the present Device DRM Time, and SHOULD be asked if the Device's DRM Time is correct. If the DRM Time is not correct the Device SHOULD initiate Device DRM Time synchronization by re-registering with the RI using the Registration protocol. b) ….
SCR Reference	
Preconditions	PKI : Model A State: - DRM agent has a valid RI context - GUID of RO is not in the <GUID, RITS> replay cache or <GUID> replay cache.
Test Procedure	- DRM agent successfully processes a RO Response messages that holds a stateful RO with RITS > DRMTime + 24 hours.
Pass-Criteria	- The DRM Agent does not install the RO

Test Case Deployment			
a	Device RO processing		
b	Domain RO processing		

6.1.68 Replay protection – Stateful RO with RITS; In Replay cache

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-68</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">Section 9.4.2.1:
When receiving a stateful RO with a <b>&lt;timestamp&gt;</b> element (RITS), the Device MUST perform the following procedure:
a) ..
b) Failing a), if the GUID for the RO is already in the <GUID, RITS> replay cache then the Device MUST reject the RO.
c) Failing b), if the <GUID, RITS> replay cache is not full, the Device MUST accept the RO and insert the ROs GUID and RITS values as an entry in the replay cache. Note: The GUID value is the <b><i>id</i></b> attribute of the <b>roap:ROPayload</b> value.
d) ..</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context
- GUID of RO is not in the <GUID, RITS> replay cache or <GUID> replay cache.</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- DRM agent successfully processes a RO acquisition response that holds a stateful RO with RITS of which GUID is not in the <GUID, RITS> replay cache.
- DRM agent receives the same RO again</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent installs the first RO
- The DRM agent rejects the second RO</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Device RO processing</td><td></td><td></td></tr>
<tr><td><b>b</b></td><td>Domain RO processing</td><td></td><td></td></tr>
</table>

6.1.69 Replay protection – Stateful RO with RITS; Early RITS

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-69</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">Section 9.4.2.1:
When receiving a stateful RO with a <b><timestamp></b> element (RITS), the Device MUST perform the following procedure:
a) ..
b) ..
c) ..
d) If the replay cache is full, and the RITS is before the earliest RI Time Stamp in the replay cache the Device MUST reject the RO.
e) ..</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context
- The <GUID, RITS> replay cache is full.</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- DRM agent successfully processes a RO acquisition response that holds a stateful RO with RITS that is before the earliest RI Time Stamp in the replay cache.</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent does not install the RO</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Device RO processing</td><td></td><td></td></tr>
<tr><td><b>b</b></td><td>Domain RO processing</td><td></td><td></td></tr>
</table>

6.1.70 Replay protection – Stateful RO without RITS; In Replay cache

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-70</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">Section 9.4.2.2:
When receiving a stateful RO without a <b><timestamp></b> element, the Device MUST perform the following procedure:
a) If the RO's GUID is in the GUID-only replay cache then the Device MUST reject the RO.
b) Failing a), if the GUID-only replay cache is not full, the Device MUST accept the RO and insert the RO's GUID value as an entry in the cache.
c) Otherwise – if the GUID-only replay cache is full, the Device MUST accept the RO and insert the RO's GUID value as an entry in the GUID-only replay cache by deleting an existing entry in the cache. The Device MAY use FIFO in the GUID-only replay cache or MAY select a random entry for deletion.</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context
- GUID of RO is not in the <GUID> replay cache or <GUID> replay cache.</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- DRM agent successfully processes a RO acquisition response that holds a stateful RO without RITS of which GUID is not in the <GUID> replay cache.
- DRM agent receives the same RO again</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent installs the first RO
- The DRM agent rejects the second RO</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Device RO processing</td><td></td><td></td></tr>
<tr><td><b>b</b></td><td>Domain RO processing</td><td></td><td></td></tr>
</table>

6.1.71 Parent Rights object; Invalid Rights issuer

<table>
<tr><td><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-71</td></tr>
<tr><td><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td><b>Specification Reference</b></td><td colspan="3">Section 9.5:
Client Devices MUST verify that the Child Rights Object and its related Parent Rights Object were issued by the same Rights Issuer before the associated content is made available to the user.</td></tr>
<tr><td><b>SCR Reference</b></td><td colspan="3"></td></tr>
<tr><td><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- DRM agent has a valid RI context for RI-1 and
- DRM Agent has a valid RI context for RI-2.</td></tr>
<tr><td><b>Test Procedure</b></td><td colspan="3">- DRM Agent successfully processes a RO acquisition response from RI-1 that holds a valid parent RO with RO-IDx..
- The DRM Agent installs the Parent RO.
- DRM Agent successfully processes a second RO acquisition response from RI-2 that holds a valid child RO that refers to the Parent RO with RO-IDx.
-</td></tr>
<tr><td><b>Pass-Criteria</b></td><td colspan="3">- DRM Agent does not allow inheritance from the parent RO by the Child RO.</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Content Consumption</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.1.72 Nonce generation on Device without system shutdown

Testcase ID	DRM-2.0-con-72
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRM-v2.0] 5.3.10 For each ROAP message that requires a nonce element to be sent, a fresh nonce SHALL be generated randomly each time. Nonce values MUST be at least 14 octets long. Devices MUST at least support nonce values 14 octets long.
SCR Reference	
Preconditions	PKI : Model A State: -
Test Procedure	- Necessary steps to prepare the following step. - The DRM agent sends a ROAP request with Device Nonce. This is repeated 5 times.
Pass-Criteria	- The nonces generated by the device are all different. - The generated nonces are at least 14 octets in length.

Test Case Deployment			
a	Registration Request	**c**	JoinDomain Request
b	RO Request	**d**	LeaveDomain

6.1.73 Nonce generation on Device with system shutdown

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="2">DRM-2.0-con-73</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="2">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="2">Nonce Generation with system shutdown</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="2">[DRM-v2.0] 5.3.10
For each ROAP message that requires a nonce element to be sent, a fresh nonce SHALL be generated randomly each time.
Nonce values MUST be at least 14 octets long. Devices MUST at least support nonce values 14 octets long.</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="2"></td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="2">PKI : Model A
State:
-</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="2">- The DRM agent is shut down and powered up.
- <i>Necessary steps to prepare the following step.</i>
- The DRM agent sends a ROAP request with Device Nonce.
- The last two steps are repeated 5 times.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="2">- The nonces generated by the device are all different.
- The generated nonces are at least 14 octets in length</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Registration Request</td><td><b>c</b></td><td>JoinDomain Request</td></tr>
<tr><td><b>b</b></td><td>RO Request</td><td><b>d</b></td><td>LeaveDomain</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.2 REL/DCF related Testcases

6.2.1 Wrong permissions for an image object

Testcase ID	DRM-2.0-con-74
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRMREL] Chapter 5.4.
SCR Reference	DRMREL-GEN-008, DRMREL-GEN-009, DRMREL-GEN-010, DRMREL-GEN-012
Preconditions	PKI : Model A State: - The DRM Agent has a valid RI Context with the RI. - There is a DCF containing an encrypted image stored on the terminal. - There is a Rights Object with <play> and <execute> permissions stored on the terminal.
Test Procedure	- User tries to display the image DCF.
Pass-Criteria	- The DRM Agent does not allow the user to diplay the image.

Test Case Deployment			
a	Content consumption		

6.2.2 Wrong permissions for a sound object

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-75</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="3">[DRMREL] Chapter 5.4.</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="3">DRMREL-GEN-008, DRMREL-GEN-009, DRMREL-GEN-011, DRMREL-GEN-012, DRMREL-GEN-013</td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- The DRM Agent has a valid RI Context with the RI.
- There is a DCF containing an encrypted sound file stored on the terminal.
- There is a Rights Object with <display>, <print> and <execute> permissions stored on the terminal.</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="3">- User tries to play the sound DCF.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent does not allow the user to play the sound.</td></tr>
<tr><td colspan="5"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td colspan="2">Content consumption</td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

6.2.3 Wrong permissions for an application object

Testcase ID	DRM-2.0-con-76
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRMREL-v2.0] Section 5.4
SCR Reference	DRMREL-GEN-008, DRM-REL-GEN-C-009, DRM-REL-GEN-C-010, DRM-REL-GEN-C-011, DRM-REL-GEN-C-013
Preconditions	PKI : Model A State: • The DRM Agent has a valid RI Context with the RI. • There is a DCF containing an encrypted application stored on the terminal. • There is a Rights Object with <display>, <print> and <play> permissions stored on the terminal.
Test Procedure	- User tries to execute the application.
Pass-Criteria	- The DRM Agent does not allow the user to execute the application.

Test Case Deployment			
a	Content consumption		

6.2.4 Unknown permissions

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-77</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="3">[DRMREL] Chapter 5.4.</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="3">DRMREL-GEN-008, DRMREL-GEN-009, DRMREL-GEN-010, DRMREL-GEN-011, DRMREL-GEN-012, DRMREL-GEN-013</td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- There is a DCF containing an encrypted image stored on the terminal.
- There is a Rights Object containing a <display>, <print> and an unknown permission (eg, <delete>) stored on the terminal.</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="3">- User tries to display the image DCF.
- User tries to print the image DCF (if supported by device).</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent allows the user to display the image.
- The DRM Agent allows the user to print the image (if supported by device).
- The unknown permission is ignored by the DRM Agent.</td></tr>
<tr><td colspan="5"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td colspan="2">Content consumption</td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

6.2.5 Export permissions ("move") for rights with stateless permissions

Testcase ID	DRM-2.0-con-78
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRMREL-v2.0] Section 5.4.6, [DRM-v2.0] Section 9.6
SCR Reference	DRM-REL-GEN-C-008, DRM-REL-GEN-C-009, DRM-REL-GEN-C-010, DRM-REL-GEN-C-011, DRM-REL-GEN-C-012, DRM-REL-GEN-C-013, DRM-REL-GEN-C-014, DRM-REL-GEN-C-015, DRM-REL-GEN-C-016, DRM-CLI-CMN-044, DRM-CLI-CMN-048
Preconditions	PKI : Model A State: - There is a DCF and RO stored on the terminal. - The Rights Object contains <export> permissions with "move" (without quotes) value in the "mode" attribute. The RO defines a stateless valid constraint (e.g. <datetime>) for the consumption of the content.
Test Procedure	- User tries to use the DCF in the DRM Agent. - User tries to export the DCF from the device. - User tries to use the content in the DRM Agent where the content was exported.
Pass-Criteria	- The DRM Agent allows the user to use the DCF according to the RO. - The DRM Agent allows the user to export the DCF and RO from the device. - The DRM Agent is not able to use the content anymore.

Test Case Deployment

a	Content consumption		

6.2.6 Export permissions ("copy") for DCFs with stateless rights object

Testcase ID	DRM-2.0-con-79
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRMREL-v2.0] Section 5.4.6, [DRM-v2.0] Section 9.6
SCR Reference	DRM-REL-GEN-C-008, DRM-REL-GEN-C-009, DRM-REL-GEN-C-010, DRM-REL-GEN-C-011, DRM-REL-GEN-C-012, DRM-REL-GEN-C-013, DRM-REL-GEN-C-014, DRM-REL-GEN-C-015, DRM-REL-GEN-C-016, DRM-CLI-CMN-044, DRM-CLI-CMN-048
Preconditions	PKI : Model A State: - There is a DCF and RO stored on the terminal. - The Rights Object contains <export> permissions with "copy" (without quotes) value in the "mode" attribute. The RO defines a stateless constraint (e.g. <datetime>) for the use of the content.
Test Procedure	- User tries to use the DCF in the DRM Agent. - User tries to export the DCF and from the device. - User tries to use the exported content in the DRM Agent from where the content was exported.
Pass-Criteria	- The DRM Agent allows the user to use the DCF according to the RO. - The DRM Agent allows the user to export the DCF and RO from the device. - The user can still use the content, according to the RO, in the DRM Agent.
Test Case Deployment	

a	Content consumption		

6.2.7 Export permissions ("move") for DCFs with stateful rights object

Testcase ID	DRM-2.0-con-80
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRMREL-v2.0] Section 5.4.6, [DRM-v2.0] Section 9.6
SCR Reference	DRM-REL-GEN-C-008, DRM-REL-GEN-C-009, DRM-REL-GEN-C-010, DRM-REL-GEN-C-011, DRM-REL-GEN-C-012, DRM-REL-GEN-C-013, DRM-REL-GEN-C-014, DRM-REL-GEN-C-015, DRM-REL-GEN-C-017, DRM-CLI-CMN-030, DRM-CLI-CMN-044, DRM-CLI-CMN-048
Preconditions	PKI : Model A State: - There is a DCF and RO stored on the terminal. - The Rights Object contains <export> permissions with "move" (without quotes) value in the "mode" attribute. The RO defines a stateful constraint (e.g. <count>) for the use of the content.
Test Procedure	- User tries to use the DCF in the DRM Agent. - User tries to export the DCF from the device. The user should export the object before the state restrictions has been completely consumed. - User tries to use the exported content in the DRM Agent from where the content was exported.
Pass-Criteria	- The DRM Agent allows the user to use the DCF according to the RO. The state information is changed according to the usage (e.g. counter is decreased). - The DRM Agent allows the user to export the DCF and RO from the device. Also the state information is exported. - The DRM Agent is not able to use the content anymore.

Test Case Deployment			
a	Content consumption		

6.2.8 Export permissions ("copy") for DCFs with stateful rights object

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="2">DRM-2.0-con-81</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="2">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="2">See section header.</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="2">[DRMREL-v2.0] Section 5.4.6, [DRM-v2.0] Section 9.6</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="2">DRM-REL-GEN-C-008, DRM-REL-GEN-C-009, DRM-REL-GEN-C-010, DRM-REL-GEN-C-011, DRM-REL-GEN-C-012, DRM-REL-GEN-C-013, DRM-REL-GEN-C-014, DRM-REL-GEN-C-015, DRM-REL-GEN-C-017, DRM-CLI-CMN-030, DRM-CLI-CMN-044, DRM-CLI-CMN-048</td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="2">PKI : Model A
State:
- There is a DCF and RO stored on the terminal.
- The Rights Object contains <export> permissions with "copy" (without quotes) value in the "mode" attribute. The RO defines a stateful constraint (e.g. <count>) for the use of the content.</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="2">1. User tries to use the DCF in the DRM Agent.
2. User tries to export the DCF and RO from the device.
3. User tries to use the exported content in the DRM Agent from where the content was exported.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="2">1. The DRM Agent allows the user to use the DCF according to the RO. The state information is changed according to the usage (e.g. counter is decreased).
2. The DRM Agent allows the user to export the DCF and RO from the device. The state information is <b>not</b> exported; and the target system receives the consumption rights as per the original RO (without export).
3. The user can continue to use the content on the original device, according to the updated state information from step 1</td></tr>
<tr><td colspan="4"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td>Content consumption</td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.2.9 Export permissions not present for DCF

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="3">DRM-2.0-con-82</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="3">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="3">See section header.</td></tr>
<tr><td colspan="2"><b>Specification Reference</b></td><td colspan="3">[DRMREL-v2.0] Section 5.4.6, [DRM-v2.0] Section 9.6</td></tr>
<tr><td colspan="2"><b>SCR Reference</b></td><td colspan="3">DRM-REL-GEN-C-008, DRM-REL-GEN-C-009, DRM-REL-GEN-C-010, DRM-REL-GEN-C-011, DRM-REL-GEN-C-012, DRM-REL-GEN-C-013, DRM-REL-GEN-C-014, DRM-CLI-CMN-044, DRM-CLI-CMN-048</td></tr>
<tr><td colspan="2"><b>Preconditions</b></td><td colspan="3">PKI : Model A
State:
- There is a DCF and RO stored on the terminal.
- The Rights Object does not contain <export> permissions.</td></tr>
<tr><td colspan="2"><b>Test Procedure</b></td><td colspan="3">- User tries to use the DCF in the DRM Agent.
- User tries to export the DCF from the device.</td></tr>
<tr><td colspan="2"><b>Pass-Criteria</b></td><td colspan="3">- The DRM Agent allows the user to use the DCF according to the RO.
- The DRM Agent does not allow the user to export the content.</td></tr>
<tr><td colspan="5"><b>Test Case Deployment</b></td></tr>
<tr><td><b>a</b></td><td colspan="2">Content consumption</td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
</table>

6.2.10 Instant Preview

Testcase ID	DRM-2.0-con-83
Test Object	DRM Agent.
Test Case Description	See section header.
Specification Reference	[DRMDCF] 5.2.2.2
SCR Reference	DRM-DCF-CLI-7, DRM-CLI-CMN-026, DRM-CLI-CD-063
Preconditions	PKI : Model A State: • There exists a multipart DCF with one encrypted content container box and one unencrypted content container box. • The encrypted content container contains a Preview Header. • The Preview Header's preview-method is set to "instant". • The Preview Header's parameter contains a preview-element-uri, which points to the unencrypted content box. • The DCF resides on the terminal.
Test Procedure	- User accesses the DCF.
Pass-Criteria	- DRM Agent recognizes Preview Header. - DRM Agent allows user to access embedded Preview Header.

Test Case Deployment			
a	Content consumption		

6.2.11 Deleted

<table>
<tr><td colspan="2"><b>Testcase ID</b></td><td colspan="2">DRM-2.0-con-84</td></tr>
<tr><td colspan="2"><b>Test Object</b></td><td colspan="2">DRM Agent</td></tr>
<tr><td colspan="2"><b>Test Case Description</b></td><td colspan="2">Deleted</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="2"></td><td colspan="2"></td></tr>
<tr><td colspan="4"></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

6.2.12 Erroneous Count constraint

Testcase ID	DRM-2.0-con-85
Test Object	DRM Agent
Test Case Description	To test erroneous <count> constraint for a DCF.
Specification Reference	[DRMREL-v2.0] Section 5.5.
SCR Reference	DRM-REL-GEN-C-015, DRM-REL-GEN-C-016, DRM-REL-GEN-C-017, DRM-CLI-CMN-030
Preconditions	PKI : Model A State: - There is a DCF stored on the terminal. - The RI has issued an RO containing only a permission with an associated count constraint set to negative or zero.
Test Procedure	- User requests a RO for the DCF residing on the terminal. - User tries to use the DCF.
Pass-Criteria	- The DRM Agent does not allow the user to use the DCF.

Test Case Deployment			
a	Content consumption		

6.2.13 Erroneous Timed-Count constraint

Testcase ID	DRM-2.0-con-86
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRMREL-v2.0] Section 5.5.3
SCR Reference	DRM-REL-GEN-C-015, DRM-REL-GEN-C-016, DRM-REL-GEN-C-018
Preconditions	PKI : Model A State: - There is a DCF stored on the terminal. - The RI has issued an RO containing only a permission with an associated timed-count constraint set to 2 and a timer attribute set to zero.
Test Procedure	- User requests a RO for the DCF residing on the terminal. - User tries to use the DCF.
Pass-Criteria	- The DRM Agent does not allow the user to use the DCF.

Test Case Deployment			
a	Content consumption		

6.2.14 Erroneous Datetime constraint

Testcase ID	DRM-2.0-con-87
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRMREL-v2.0] Section 5.5.4
SCR Reference	DRM-REL-GEN-C-015, DRM-REL-GEN-C-016, DRM-REL-GEN-C-019, DRM-REL-GEN-C-020, DRM-REL-GEN-C-021, DRM-CLI-CMN-030
Preconditions	PKI : Model A State: - There are three DCFs stored on the terminal. - The RI has issued three ROs for these DCFs: In the RO for the first DCF the value of the <end> element is smaller than the value of the <start> element. In the RO for the second DCF the format of the <start> element is faulty. In the RO for the third DCF the format of the <end> element is faulty.
Test Procedure	- User requests ROs for the DCFs residing on the terminal. - User tries to use the first DCF. - User tries to use the second DCF. - User tries to use the third DCF.
Pass-Criteria	- The DRM Agent does not allow the user to use the first DCF. - The DRM Agent does not allow the user to use the second DCF. - The DRM Agent does not allow the user to use the third DCF.

Test Case Deployment			
a	Content consumption		

6.2.15 Erroneous Interval constraint

Testcase ID	DRM-2.0-con-88		
Test Object	DRM Agent		
Test Case Description	See section header.		
Specification Reference	[DRMREL-v2.0] Section 5.5.5		
SCR Reference	DRM-REL-GEN-C-015, DRM-REL-GEN-C016, DRM-REL-GEN-C-022, DRM-CLI-CMN-030		
Preconditions	PKI : Model A State: - There are two DCFs stored on the terminal. - The RI has issued two ROs: In the RO for the first DCF the value of the <interval> constraint is zero. In the RO for the second DCF the format of the <interval> constraint is faulty.		
Test Procedure	- User requests ROs for the DCFs residing on the terminal. - User tries to use the first DCF. - User tries to use the second DCF.		
Pass-Criteria	- The DRM Agent does not allow the user to use the first DCF. - The DRM Agent does not allow the user to use the second DCF.		
Test Case Deployment			
a	Content consumption		

6.2.16 Erroneous Accumulated constraint

Testcase ID	DRM-2.0-con-89
Test Object	DRM Agent
Test Case Description	To test erroneous <accumulated> constraint for a DCF.
Specification Reference	[DRMREL-v2.0] Section 5.5.5
SCR Reference	DRM-REL-GEN-C-015, DRM-REL-GEN-C016, DRM-REL-GEN-C-023
Preconditions	PKI : Model A State: - There are two DCFs stored on the terminal. - The RI has issued two ROs each containing only a permission with an associated accumulated constraint: - In the RO for the first DCF the accumulated period is faulty (e.g. includes specification of months.) - In the RO for the second DCF the accumulated period is zero.
Test Procedure	- User requests ROs for the DCFs residing on the terminal. - User tries to use the first DCF. - User tries to use the second DCF.
Pass-Criteria	- The DRM Agent does not allow the user to use the first DCF. - The DRM Agent does not allow the user to use the second DCF.
Test Case Deployment	

a	Content consumption		

6.2.17 Error in inheritance model: Reference to non-existing Parent rights object

Testcase ID	DRM-2.0-con-90
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRMCF-v2.0] Section 5.6 and 5.6.1, [DRM-v2.0] Section 9.5
SCR Reference	DRM-REL-GEN-C-026, DRM-CLI-CMN-047
Preconditions	PKI : Model A State: - There is a DCF stored on the terminal. - The RI has issued two ROs: The first RO is a Parent RO and contains a <datetime> constraint for the use of the content. The Parent RO does not reference any DCF. The second RO is a Child RO where the <uid> element of the <context> elemet in the <inherit> element **does not** match the <uid> element of the <context> element of the <asset> element of the parent RO. The child RO refers the DCF and contains a <count> constraint for the use of the content. - The same Rights Issuer has issued bothrights objects.
Test Procedure	- User requests rights for the DCF residing on the terminal and receives both of the rights objects. - The DRM Agent tries to use the content during the time the <datetime> constraint allows to do it.
Pass-Criteria	- The DRM Agent is **not** allowed to use the delivered content during the time the <datetime> constraint allows to do it.

Test Case Deployment			
a	Content consumption		

6.2.18 Error in inheritance model: Parent rights object inherits from another rights object

Testcase ID	DRM-2.0-con-91
Test Object	DRM Agent
Test Case Description	See section header.
Specification Reference	[DRMCF-v2.0] Section 5.6 and 5.6.1, [DRM-v2.0] Section 9.5
SCR Reference	DRM-REL-GEN-C-026, DRM-CLI-CMN-047
Preconditions	PKI : Model A State: - There is a DCFs stored on the terminal. - There are two ROs stored on the terminal: The first RO is a Parent RO and contains a <datetime> constraint for the use of the content. This rights object also contains a <inherit> element indicating that it inherits from another rights object. The Parent RO does not reference any DCF. The second rights object is the Child rights object where the <uid> element of the <context> elemet in the <inherit> element matches the <uid> element of the <context> element of the <asset> element of the parent RO. The child RO refers the DCF and contains a <count> constraint for the use of the content. - The same Rights Issuer has issued both rights objects.
Test Procedure	- The DRM Agent tries to use the content.
Pass-Criteria	- The DRM Agent is not allowed to use the delivered content because the parent rights object inherits from another rights object.
Test Case Deployment	

a	Content consumption		

7. DRM Interoperability Test Cases

See [ETS] for Interoperability Testcases.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-ETS-DRM-V2_0-Conformance-Client-20050727-A	26 July 2005	Initial approved version
OMA-ETS-DRM-V2_0-Conformance-Client-20051114-A	14 Nov 2005	This version reflects the upgrade as described in OMA-IOP-BROWSING-2005-0106-CR_upgrade_DRM2.0_Client_Conformance_Test_Spec and in OMA-IOP-BROWSING-2005-0112R01-CR Trusted Device Authorities checking Approved Ref# OMA-TP-2005-0342-DRM-2.0-New-Conformance-Client-ETS

A.2 Draft/Candidate Version History

Reference	Date	Description
OMA-ETS-DRM-V2_0-Conformance-Client-20060207-C	7 Feb 2006	This version reflects the upgrade as described in OMA-IOP-BRO-2006-0018R02-DRM-Client-Conformance-ETS-updates