Marlin – Broadband Network Service Profile Specification

Version 1.2.1
Final

Source	Marlin Developer Community
Date	April 5, 2011

Notice

Use of this document is subject to the agreement executed between you and the Parties, if any.

Any copyright notices shall not be removed, varied, or denigrated in any manner.

Intellectual Property

A commercial implementation of this specification requires a license from the Marlin Trust Management Organization.

Contact Information

Feedback on this specification should be addressed to: editor@marlin-community.com

Contact information for the Marlin Trust Management Organization can be found at: http://www.marlin-trust.com/

Contents

1 Introduction

This document describes the Marlin – Broadband Network Service Profile Specification. This specification is comprised of an implementation compendium, operational policies and informative guidance to enable effective deployments of broadband services.

The compendium simplifies adopter’s implementation requirements of the Marlin Broadband Delivery System Specification [MBB] by minimizing the mandatory to implement functionalities in both [MBB] and the Marlin Core System Specification [MCS] so as to ensure consistent interpretation and interoperable implementations of [MBB].

The operational policies further qualify the implementation requirements above and beyond those detailed in the compendium.

The implementation guidance recommends common approaches to deploying Marlin DRM in a network service. This guidance includes descriptions of the most common business models in use.

This specification allows two implementation levels, Full Implementation and Compact Implementation. Compact Implementation provides a subset of Full Implementation, which includes the mandatory functionalities require for streaming. Unless stated, the descriptions in this specification apply to both implementation levels.

1.1 Document Organization

This document is organized as follows:

- (This) introduction, including abbreviations, definitions and references.
- Broadband Network Service Overview
- Broadband Implementation Compendium
- Operational Policies
- Recommended usage of DRM Objects

1.2 Conformance Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this specification are to be interpreted as described in IETF RFC 2119 [RFC2119].

1.3 Namespaces and Identifiers

This specification defines schemas conforming to XML Schemas [Schema] and normative text to describe the syntax and semantics of XML-encoded objects and protocol messages. In cases of disagreement between the schema documents and the schema listings in this specification the schema documents take precedence. Note that in some cases the normative text of this specification imposes constraints beyond those indicated by the schema documents.

1.3.1 Namespaces and Notation

The table below summarizes the external schemas used in this specification:

Prefix	XML Namespace	Description
wsa:	http://www.w3.org/2005/08/addressing	[WS-Addr]
wsse:	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd	[WS-SEC]
S11:	http://schemas.xmlsoap.org/soap/envelope	[SOAP11]

Table 1: Supporting Namespaces

As a convention throughout this document we use the namespace prefixes described above to qualify XML elements and attributes which are specified elsewhere. That is the typographical convention is: <MarlinElement>, <ns:ForeignElement>, XMLAttribute, Datatype, OtherKeyword.

1.4 Abbreviations

NEMO	Networked Environment for Media Orchestration

1.5 References

Normative References

[8pus]	Octopus DRM Technology Platform Specifications, Version 1.0
[OCTXSD]	Octopus schema definition: Octopus.xsd
[BBTS]	Marlin Engineering Work Group, Marlin Broadband Transport Stream Specification, Version1.1
[MBB]	Marlin Engineering Work Group, Marlin Broadband Delivery System Specification, Version1.2, latest Marlin Errata: Marlin Broadband Delivery System v1.2
[MCS]	Marlin Engineering Work Group, Marlin – Core System Specification, Version1.3, latest Marlin Errata: Marlin Core System v1.3
[MFF]	Marlin Engineering Work Group, Marlin – File Formats Specification, Version1.1
[MIAR]	Marlin Engineering Work Group, Marlin - Identifier and Attribute Registry, Version1.0
[MOC]	Marlin Engineering Work Group, Marlin – Output Control v1.0
[MPAC]	Marlin Engineering Work Group, Marlin – Profile and Capability Signaling, Version1.0
[MURIT10]	URI Templates for Marlin, Version 1.0
[OMARLIN]	Marlin Engineering Work Group, OMArlin Specification, Version 1.0
[RFC2119]	S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, IETF RFC 2119, March 1997. http://www.ietf.org/rfc/rfc2119.txt.

Informative Reference

[Schema]	XML Schema Part 1: Structures. W3C Recommendation. D. Beech, M. Maloney, N. Mendelsohn, H. Thompson. May 2001. http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/

[SOAP11]	"Simple Object Access Protocol (SOAP) 1.1," Box, Don, Ehnebuske, David , Kakivaya, Gopal, Layman, Andrew, Mendelsohn, Noah, Nielsen, Henrik Frystyk, Winer, Dave, eds. World Wide Web Consortium W3C Note (08 May 2000). http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
[WS-Addr]	Web Services Addressing 1.0 - Core, W3C Candidate Recommendation, 17 August 2005, http://www.w3.org/TR/2005/CR-ws-addr-core-20050817 Web Services Addressing 1.0 - SOAP Binding, W3C Candidate Recommendation, 17 August 2005, http://www.w3.org/TR/2005/CR-ws-addr-soap-20050817
[WS-SEC]	Web Services Security (WS-Security), Version 1.0, OASIS, April 5, 2002. http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf

2 Broadband Network Service Overview (Informative)

The Broadband Network Service Profile focuses on following functionalities which are typically deployed by broadband network type of service.

Rendering of progressive download content
Rendering of unicast streamed content
Rendering of multicast streamed content

Full Implementation also focuses on the following functionality.

Rendering and export of downloaded content

There are some entities for the Broadband Network Service Profile which are:

DRM client,
DRM server,
Content server,
Store web site, illustrated in Figure 1.

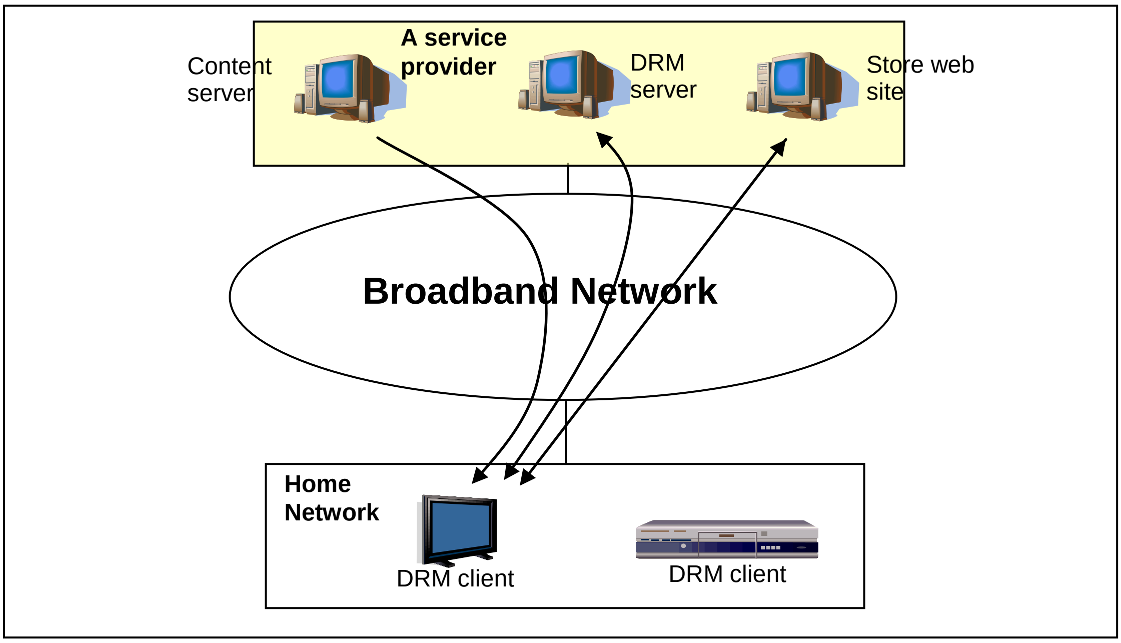

Figure 1: Broadband Network Service Overview

The scopes of Broadband Network Service Profile Specification are DRM protocols between DRM server and DRM client to acquire DRM data such as DRM license from DRM server. The protocols between DRM client and store web site for payment transaction and acquisition of Action Token, and the protocols between DRM Client and content server are not scope of this specification.

For the rendering of downloaded content, the following steps are typically implemented between a compliant device and service:

(1) Purchase content from store web site by user interaction. (payment transaction)
(2) Acquire the corresponding encrypted content from content server by requesting the content by using any protocol such as HTTP. (content request and acquisition based on the request)
(3) Acquire Action Token and Configuration Token defined in [MBB] from store web site which enables the DRM client to make a request for the DRM license to a License Service [MBB]. Given the request, the License Service generates the

DRM license based on the purchase condition for the content, and sends the DRM license to the DRM client. (license request and acquisition based on the request)

(4) Once the client has acquired the encrypted content and DRM license in step (2) and step (3) respectively, DRM client renders the encrypted content with the DRM license.

Please note that the order of step (2) and step (3) can be reversed as far as these steps are completed prior to step (4).

For the rendering of progressive download content, unicast streamed content, and multicast streamed content, the same steps as above shall be followed except that the step (3) shall happen prior to the step (2). Then, the encrypted content is acquired based on the request from the client (in progressive download and unicast case) or on the selection by the client (in multicast case) thorough some protocols.

3 Broadband Implementation Compendium

The intention of this compendium is to aid adopters in bringing products and services to market. Unless stated otherwise in this section, the normative descriptions defined in [MCS] and [MBB] apply. Broadband Network Service Profile refers to [MFF], [OMARLIN], and [BBTS] for content protection formats.
It is RECOMMENDED for device implementations to support one or more of content protection formats from [MFF], [OMARLIN] and [BBTS].

3.1 Marlin Core System Roles and Services per [MCS] §4

Client implementations assert the Device and DRMClient roles. Implementations of Device and DRMClient roles MAY expose services in accordance with [MCS] §4.1 and §4.2.

3.2 Marlin Core System Protocols per [MCS] §5

The Discovery protocol defined in [MCS] §5.4 MAY be implemented.
The Inspection protocol defined in [MCS] §5.5 MAY be implemented.
The Subscription and Notification protocol defined in [MCS] §5.6 MAY be implemented.
The Service-specific Protocols defined in [MCS] §5.7 MAY be implemented

3.3 Marlin Protocol Bindings per [MCS] §6

The communication protocol bindings utilized by [MBB] are limited to the normative descriptions defined in [MCS] §6.3.

3.4 Marlin BB System Protocols per [MBB] §5

Services implement the protocols defined in [MBB] §5.2 in accordance to business models they support.

Clients are REQUIRED to implement the License acquisition protocol defined in [MBB] §5.2.1. Clients that support more than the mandatory Octopus Node types in the request parameter SHOULD follow the signaling mechanism prescribed in §6.2.

In case of Full Implementation, Clients are REQUIRED to implement the following protocols required for Registration Service defined in [MBB] §5.2.2. For Compact Implementation, the following protocols MAY be implemented and the support for Broadband Domain and Subscription is OPTIONAL.

- Clients SHALL support the Node acquisition protocol for both User and Subscription Nodes.
- Clients SHALL support the Link acquisition protocol to acquire Octopus Links to User and Subscription Nodes.
- Clients SHALL support the Deregistration protocol to terminate User Link relationship. Clients that support more than the mandatory Octopus Node types in the request parameter SHOULD follow the signaling mechanism prescribed in §6.2.

Clients MAY implement the Data Certification protocol defined in [MBB] §5.2.3.

Clients MAY implement the Data Update protocol defined in [MBB] §5.2.4.

Clients MAY implement the Metering Data protocol defined in [MBB] §5.2.5.

3.5 Octopus Objects

For clarification of handling Scuba keys, refer to §3.2.1 of [MCS].

4 Operational Policies

This section describes the operational policies regarding output control.

A default set of output control for BasicCCI and DTCP that can be overridden by the mechanism defined in [MOC] §4,[1]

4.1 Default set for BasicCCI

The following table defines the default set of BasicCCI.

Name	Type	Default Value	Description
EPN	Integer	1	EPN-unasserted
CCI	Integer	00	Copy Control Not Asserted
ImageConstraintToken	Integer	1	High Definition Analog Output in High Definition Analog Form
DigitalOnlyToken	Integer	0	Output of decrypted content is allowed for Analog/Digital Outputs
APS	Integer	00	APS off

4.2 Default set for DTCP

The following table defines the default set of DTCP.

Name	Type	Default Value	Description
RetensionMoveMode	Integer	1	Non_Retension_mode
RetensionState	Integer	N/A	
EPN	Integer	1	EPN-unasserted
DTCP_CCI	Integer	00	Copy-free
ImageConstraintToken	Integer	1	High Definition Analog Output in High Definition Analog Form
APS	Integer	00	Copy-free

4.3 License Issuing with Output Control

This section describes an operation policy for usage of output control mechanism defined in [MOC].
In this specification, the following policy is recommended:

- When a default value for a certain parameter is used, output control obligation/permission SHOULD NOT be used for the parameter.

---

[1] The default set in this section may be changed and defined in MTMO.

5 Usage of DRM Objects

This section describes the Node Link Topologies supported by this specification and provides the licenses and links which the Client are required to support.

5.1 Node Link Topologies

Figure 2 provides an overview of the Node Link topologies and associated options for license binding and targeting that are supported by the Broadband Network Service Profile Specification.

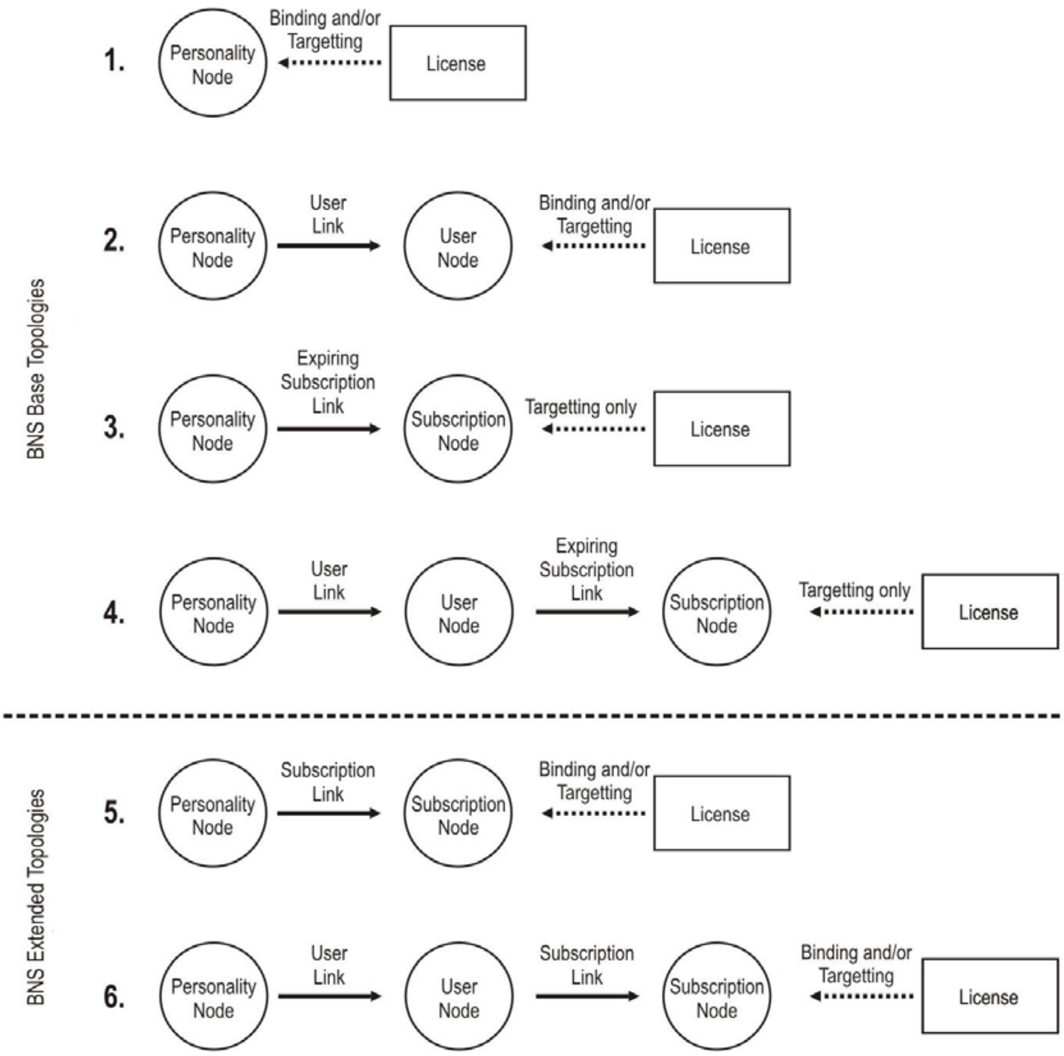

Figure 2: Supported Node Link Topologies

In case of the Compact Implementation, all Clients SHALL enable topology 1, to have a Personality Node and the acquisition and evaluation of Licenses that are bound and/or targeted to the Personality Node. Other topologies are OPTIONAL.
In case of Full Implementation, these topologies are provided in two sets: the mandatory BNS Base Topologies and the optional BNS Extended Topologies.

5.1.1 BNS Base Topologies of Full Implementation

All Clients are mandated to have a Personality Node and to support all necessary functionality and protocols for the acquisition and deregistration of User Nodes and User Links and the acquisition and evaluation of Licenses that are bound and/or targeted to the Personality Node or to User Nodes. This enables topologies 1 and 2.

The mandatory functionality with respect to Subscription Nodes, topologies 3 and 4, however is more limited. Since no means to acquire a license bound to a subscription node is mandatory, the base topologies only effectively support subscription nodes to be used to target licenses to – the licenses acquired through mandatory protocols need to be bound to either a User Node or Personality Node as per topology 1 or 2. Also, the protocol to deregister a Subscription Link is not mandatory. Consequently, only links with a fixed expiry date can effectively be used.

5.1.2 BNS Extended Topologies of Full Implementation

The restrictions with respect to the Subscription Node that apply for the BNS Base Topologies do not apply for the BNS Extended Topologies.

Consequently, Clients that signal support for the BNS Extended Topologies are mandated to support also all necessary functionality and protocols for the acquisition and deregistration of Subscription Nodes and Subscription Links and the acquisition and evaluation of Licenses that are bound and/or targeted to Subscription Nodes.

5.2 Marlin License

This section describes a set of the recommended Marlin Licenses in this profile. The set includes Marlin Licenses for the license models Electronic Sell-Through and Rental. In case of Full Implementation, Subscription license model is also included.

5.2.1 Electronic Sell-Through License

This license type is destined to be used by a particular device or, in case of Full Implementation, within a user domain on any devices on that domain. Hence, the license is targeted and bound to an Octopus Personality Node or User Node. Note that there are no time constraints on the validity of the license.

The B.2.1 is an example of License Bundle which includes Control Program enforcing the EST License Model.

5.2.2 Rental License

This rental license is similar to the Electronic Sell-Through type that is targeted and bound to an Octopus Personality Node or, in case of Full Implementation, to a User Node, but, there are time constraints on the validity of the license. There are following 2 types of Rental License:

- Rental period in absolute validity period
  One or more of the following conditions are specified:
    - Not before
    - Not after
- Rental period in relative validity period (Full Implementation only)

The relative period is specified by minutes from the first usage of the license. The relative period is set along with an absolute validity period so that this relative period from the first usage is allowed within a certain fixed period specified by the absolute validity period. Note that this license is typically targeted and bound to an Octopus Personality Node.

The B.2.2 is an example of License Bundle which includes Control Program enforcing the Rental License in absolute validity period.

5.2.3 Subscription License (Full Implementation only)

The subscription license is bound to a Personality Node, User Node, or Subscription Node, and targeted at least to the Subscription Node.

The B.2.3 is an example of License Bundle which includes Control Program enforcing the Subscription License Model.
Generally it is recommended to apply the time constraint to the Subscription Link instead of Subscription License because the Link object is easier to update. This way all subscription contents can be updated by single Link update.

5.3 Marlin Link (Full Implementation only)

This section describes a set of the recommended Marlin Link for Full Implementation in this profile. The set includes Marlin Links for the link models User Link and Subscription Link.

5.3.1 User Link

The User Link is the link from an Octopus Personality Node to a User Node. This User Link may include constraints such as a validity period or membership check of the corresponding domain.

The B.2.4 is an example of User Link.

5.3.2 Subscription Link

The Subscription Link is a link from a Personality Node or User Node to a Subscription Node. Note that this link is associated a time validity.

The B.2.5 is an example of Subscription Link.

6 BNS Profile

A DRM Client implementing optional functionality described in this specification SHOULD indicate this by using the signalling mechanism defined in [MPAC] and the profile URI defined in §6.1 with the defined attribute identifiers in [MIAR].

6.1 Profile Signalling of Full Implementation

A DRM Client implementing mandatory functionality of Full Implementation described in this specification SHOULD indicate this by means of the signalling mechanism defined in [MPAC]. The requisite URI value used to signal this profile is defined in the following table. This profile is assumed in the absence of signalling.

Attribute Name	Attribute Value-space
profile	urn:marlin:profiles:bns:1-0

6.2 BNS Extended Topology of Full Implementation

This specification defines the following URI to signal the supported topology of Full Implementation.

Attribute Name	Attribute Value-space
topology	urn:marlin:bb:1-2:topology:bnsx:1-0

When this attribute is signaled, a DRM Client which implements this specification MUST support the following functions:

- License acquisition protocol to bind Marlin License to Subscription Node
- Deregistration from a domain represented by Subscription Node where a corresponding Subscription Link SHALL have the following properties:
    - LinkFrom: Personality Node or User Node
    - LinkTo: Subscription Node

6.3 Profile Signalling of Compact Implementation

A DRM Client not implementing mandatory functionality of Full Implementation, but implementing mandatory functionality of Compact Implementation described in this specification SHALL indicate this by means of the signalling mechanism defined in [MPAC]. The requisite URI value used to signal this profile is defined in the following table.

Attribute Name	Attribute Value-space
profile	urn:marlin:profiles:bns:1-0:compact

7 Octopus Object Attributes

The following attributes MAY be used in any Octopus Object as defined in [8pus] §2. A client MAY understand these attributes and MUST ignore attributes it does not understand; unless specified elsewhere (e.g., in a profile), understanding these attributes is OPTIONAL for a client.

7.1 Object Expiration Date

The purpose of this attribute is to convey to a client a hint that an object is no longer useful after a certain expiration date and that, therefore, the client MAY decide to remove such object from persistent storage or cache.

Attribute Name	Attribute Type	Attribute Value
urn:marlin:core:node:attribute:expiration-date	integer	The object's expiration date expressed as the number of minutes since Jan 1, 1970 00:00:00 UTC

7.2 User Friendly Name

The purpose of this attribute is to convey a human-readable name for an Octopus Node (such as a person's name for a User Node, for example).

Attribute Name	Attribute Type	Attribute Value
urn:marlin:core:node:attribute:friendly-name	string	The human-readable friendly name for the node, encoded as a UTF-8 string.

7.3 Marlin Broadband Specific Attributes

The following attributes only apply to implementations of [MBB].

7.3.1 Octopus Link Renewal Date

This attribute, when present, indicates the date after which a client MAY try to automatically renew the Octopus Link object using the Marlin Broadband Registration Service as specified in [MBB].

Attribute Name	Attribute Type	Attribute Value
urn:marlin:broadband:link:attribute:renewal-date	Integer	The renewal date expressed as the number of minutes since Jan 1, 1970 00:00:00 UTC

A client that understands this attribute SHOULD try to obtain an Action Token for a Registration Service as soon as possible after the date indicated in the value of this attribute. The Action Token location MUST be specified in the Silent Renewal URL attribute in the same Octopus Link object as specified in §7.3.2.

7.3.2 Octopus Link Renewal URL

This attribute, when present, indicates the URI template (as specified in [MURIT10]) that can be transformed into an HTTP URL referencing an Action Token document containing the information needed by a client to engage in a Registration Service interaction as specified in [MBB]

Attribute Name	**Attribute Type**	**Attribute Value**
urn:marlin:broadband:link:attribute:renewal-url	string	A URI Template that can be transformed into an HTTP URL

A client that understands this attribute and wants to make use of it MUST convert the URI template into a URL as specified in [MURIT10] and perform an HTTP GET request for that URL to acquire a document. The document obtained by the HTTP GET request MUST have a mime type signaled in the Content-Type HTTP response header. If the document obtained as a response to this request contains an Action Token, the mime type MUST be application/vnd.marlin.drm.actiontoken+xml as specified in [MBB]. If the response to the request is an error, or is a document with a different mime type, the client's behavior is unspecified (for example, if the server cannot respond with an Action Token document, it MAY respond with an HTML document which the client MAY display in its user interface).

When the response to the HTTP request is an Action Token document, the client MUST process it as soon as possible.

8 Levels

This section defines Levels representing a way towards assuring portability and interoperability of licenses. A Level represents a set of resources that are made available by a Marlin BB implementation. Thus, a license respecting the resources offered by such a Level should be portable and interoperable among all those implementations that support this Level.

8.1 Level definition

8.1.1 Resources

The following table lists the resources required in level definition:

Resource Name	Definition
Available Data Memory Size	Size in bytes of the Data Memory [8pus] §4 available for a code module per Plankton VM instance. This includes the data memory used to load the image of the Data Segment, as well as the data memory used by the Data Stack. This does not include any pseudo registers or reserved or unspecified address space before the first Data Segment.
Code Memory Size	Size of Code Memory [8pus] §4 in bytes per code module, i.e., per Plankton VM instance.
Call Stack Depth	The number of nested subroutine calls (OP_JSR and OP_JSRR) [8pus] §4 that must be supported by the VM.
Number of Plankton Virtual Machine Instances	Number of Plankton Virtual Machine instances that can simultaneously be created by the execution of a single routine listed in the Export Table of a Control. This includes spawned Virtual Machines and Virtual Machines necessary for Link processing.
Number of Octopus Nodes per License (Full Implementation only)	Number of Octopus Nodes necessary for the evaluation of a single License. This resource is required for Full Implementation only.
Number of Octopus Links per License (Full Implementation only)	Number of Octopus Links necessary for the evaluation of a single License. This resource is required for Full Implementation only.
XML size of a Single Signed Octopus Object	Overall size in bytes of all the XML elements representing one signed Octopus object [OCTXSD]. This includes Links, Nodes, Licenses, and NEMO messages.
Length of a PKI Certificate Chain	The number of X.509 certificates in the certification path from a leaf certificate that is to be validated to the root certificate of a trusted root certification authority including

	the leaf and the root certificate.
Usage of SeaShell DB Space per License (Full Implementation only)	This value is defined implicitly via the Number of write operations per License, and via the Size of data per write operation. This resource is required for Full Implementation only.
Number of write operations per License	Number of System.Host.SetObject [8pus] §4 in all standard actions as defined in [8pus] §3.7.
Size of data per write operation	Size of Database Object including the associated meta data as defined in [8pus] §7.2 per write operation.
Size of a Marlin BB Action Token	Overall size in bytes of the XML representation of an Action Token [MBB].
Size of a Marlin BB Business Token	Overall size in bytes of a Business Token [MBB].
Size of a Marlin BB Configuration Token	Overall size in bytes of the XML representation of a Configuration Token [MBB].

8.1.2 Basic Level

The Basic Level is the baseline for all levels in Marlin BB. Thus, any other level that may be defined in the future SHALL be superset of the Basic Level.

The following table lists the amount of the required resources for Basic Level. The values in the list provide the lower bound for resources offered by Level-compliant Marlin Broadband (BB) Client implementation. Furthermore, the values also provide the upper bound for resources requested by Level-compliant license.

Resource Name	Value
Available Data Memory Size	8 KB
Code Memory Size	16 KB
Call Stack Depth	8
Number of Plankton Virtual Machine Instances	4
Number of Octopus Nodes per License (Full Implementation only)	3 (See §5.1)
Number of Octopus Links per License (Full Implementation only)	2 (See §5.1)
XML size of a Single Signed Octopus Object (Link, Node, License, and NEMO msg)	96KB
Length of a PKI Certificate Chain	4
Usage of SeaShell DB Space per License (Full Implementation only)	
Number of write operations per License	9
Size of data per write operation	768B
Size of a Marlin BB Action Token	4KB
Size of a Marlin BB Business Token	256B
Size of a Marlin BB Configuration Token	75KB

8.1.3 Advanced Level

The Advanced Level is reserved for the future extension.

8.2 Signalling of Levels

The Basic Level is the baseline for all Marlin BB implementations. Hence, all Marlin BB clients SHALL comply with the Basic Level. A server SHALL NOT signal levels in licenses requiring resources exceeding the signaled capability of the client. Note that the server MAY determine the Level of the client via explicit signaling as defined in this document or by some other implicit mechanism. If the server is unable to determine the Level of the Client, it MUST assume only Basic Level resources in the client.

8.2.1 Level Attribute Values

The following table lists the Attribute Values used for signalling a certain Level.

Level	Attribute Value-space	Citation
Basic Level	urn:marlin:broadband:client:capabilities:level:basic	§8.1.2
Advanced Level	urn:marlin:broadband:client:capabilities:level:advanced	§8.1.3

8.2.2 Client Capability Signalling

A DRM Client supporting levels other than the Basic Level SHOULD indicate this by means of the signaling mechanism defined in [MPAC] via the following attribute.

Attribute Name	Attribute Value-space
Level	Attribute Value-space given in the table in §8.2.1, except unknown

8.2.3 License Signalling

If a license is known to be conformant with a certain level, the Level (e.g., basic) of the license SHOULD be signaled via the following attribute in an Octopus Control [8pus] §3. It is highly recommended that services signal the level to ensure clients can consistently process the license.

If a license explicitly signals a certain Level, it SHALL conform to this Level.

Attribute Name	Attribute Type	Attribute Value
urn:marlin:bnsp:level	String	Attribute Value-space given in the table in § 8.2.1

Appendix A Guidelines for Identifier definitions (Informative)

This section describes a number of informative guideline that can be helpful for a service provider when launching a service and for a better harmonisation among service providers.

A.1 ID Structure in SeaShell

A.1.1 Root Container

The Root Container has the following properties:

Properties	Value
Name	Marlin
Path	/Octopus/SeaShell/Databases/Marlin
Owner	urn:marlin:drmservices:seashell

The Root Container is required to be hard-coded in Marlin DRM Client as specified in §12.5.1 of [MCS].

A.1.2 Adopter Container

In this document, the Adopter Container is assumed as the direct child container of the Root Container. The Adopter Container has the following properties and values:

Properties	Value
Name	@company@
Path	/Octopus/SeaShell/Databases/Marlin/@company@
Owner	urn:marlin:organization:@company@:drmsvc:seashell

The uniqueness of @company@ is managed by MTMO, and each of Adopters is required to register the @company@ to MTMO.

The Adopter Container is generated in SeaShell database by executing the MTMO SeaShell Delegate Control provided from MTMO. For the request of MTMO SeaShell Delegate Control, the Adopter SHALL specify the @company@ as a parameter. When an Adopter manages all of its service end entities credentials by itself rather than to have some aggregated entities (e.g. Adopters' key center), the MTMO SeaShell Delegate Control is acquired and managed by the Adopter.

A.1.3 Service Container

In this document, the Service Container is assumed as the direct child container of the Adopter Container. For Marlin Broadband Delivery System, there are two Service Containers. One is the Service Container for License Service (i.e. License Service Container). The other is the Service Container for Registration Service (i.e. Registration Service Container).

The License Service Container has the following properties:

Properties	Value
Name	@ls@
Path	/Octopus/SeaShell/Databases/Marlin/@company@/@ls@
Owner	urn:marlin:organization:@company@:licensesign:@ID@

The Registration Service Container has the following properties:

Properties	Value

Name	@rs@
Path	/Octopus/SeaShell/Databases/Marlin/@company@/@rs@
Owner	urn:marlin:organization:@company@:registsign:@ID@

The uniqueness of @ls@ and @rs@ under the @company@, and the uniqueness of @ID@ in each of License and Registration Service SHALL be ensured by the Adopter.

When an Adopter manages all of its service end entities credentials by itself rather than to have some aggregated entities (e.g. Adopters' key center), Adopter's SeaShell Delegate Control which generates Service Containers SHALL be prepared by the Adopter.

The Owner Values for respective Service Containers SHALL also be set to the subjects of corresponding License and Registration Service certificates which sign Control/Controller objects to allow accesses for each of Service Containers in SeaShell. It also means that even if the Adopter renews for the License and Registration Service certificates above, the renewed certificates SHALL also have the same Owner Values as the subjects of the certificates.

A.2 Parameter List

This section describes parameter list for subsets of [MBB].

- The @company@ is identifier for company. This value is unique for the Adopter in Marlin.
- The @pdc@ is used as an identifier for PDC (Provisioning Data Center). This value is unique for the PDC in Marlin.
- The @ID@ is used as an identifier for each of service subject specified in its credentials.
- The @RID@ is used as an identifier to ensure uniqueness of urns for Octopus Objects and NEMO Message Certificates.
- The @policyID@ is used as an identifier to ensure uniqueness of domain policy for the @company@.

A.2.1 License Service

A.2.1.1 Credentials for License Service

@ID@ is same among License Service

Parameter	Convention
Subject of license signing cert	urn:marlin:organization:@company@:licensesign:@ID@
Subject of NEMO signing/enc cert	urn:marlin:organization:@pdc@:@company@:licensenemo:@ID@
NotOnOrAfterDate	DDMMYYYY or None

A.2.1.2 Octopus Objects provided from License Service

The assumption is that "urn:marlin:organization:@company@:licensesign:@ID@" is common for all of parameters for Octopus Objects issued by the License Service and the subsequent value from "urn:marlin:organization:@company@:licensesign:@ID@" is determined by the License Service to ensure uniqueness of urns for each of Octopus Objects in the License Service.
The urn for reference to content is provided from a content packager to License Service. In the format of urn:

- The @service@ is used as an identifier of service in @company@. This value is unique for the service in @company@.
- The @content-type@ is used as an identifier of content type (e.g. Video, Audio, etc.) The @content-type@ includes @id@ part to identify the content in the content type.
  - ✧ content-v-@id@ : Video Track
  - ✧ content-a-@id@ : Audio Track
  - ✧ content-s-@id@ : Subtitle Track
- The @PID@ is provided from the content packager to ensure uniqueness of the content file.

Parameter	Convention
Control/@uid	urn:marlin:organization:@company@:licensesign:@ID@:control-@RID@
Controller/@uid	urn:marlin:organization:@company@:licensesign:@ID@:controller-@RID@
ContentKey/@uid	urn:marlin:organization:@company@:licensesign:@ID@:content-key-@RID@
ContentKey/SecretKey/@uid	urn:marlin:organization:@company@:licensesign:@ID@:secret-key-@RID@
Protector/@uid	urn:marlin:organization:@company@:licensesign:@ID@:protector-@RID@
Protector/ProtectedTargets/ContentReference/Uid	urn:marlin:organization:@company@:@content-type@:@PID@

A.2.2 Registration Service

A.2.2.1 Credentials for Registration Service

@ID@ is specified for Registration Service

Parameter	Convention
Subject of reg. signing cert	urn:marlin:organization:@company@:registsign:@ID@
Subject of NEMO signing/enc cert	urn:marlin:organization:@pdc@:@company@:registnemo:@ID@
NotOnOrAfterDate	DDMMYYYY or None

A.2.2.2 Octopus Objects provided from Registration Service

The assumption is “urn:marlin:organization:@company@:registsign:@ID@” is common for all of parameters for Octopus Objects issued by the Registration Service and the subsequent value from “urn:marlin:organization:@company@:registsign:@ID@” is determined by the Registration Service to ensure uniqueness of urns for each of Octopus Objects in the Registration Service.

- User Node

Parameter	Convention
Node/@uid	urn:marlin:organization:@company@:registsign:@ID@:8pususer:@RID@
Node/ExtensionList/Extension/@uid	urn:marlin:organization:@company@:registsign:@ID@:8pususer:@RID@:scuba:public
Node/ExtensionList/Extension/ScubaKeys/PublicKey/@uid	urn:marlin:organization:@company@:registsign:@ID@:8pususer:@RID@:scuba:public:sharing
Node/ExtensionList/Extension/ScubaKeys/PublicKey/@pair	urn:marlin:organization:@company@:registsign:@ID@:8pususer:@RID@:scuba:pair:sharing

- User Link

Parameter	Convention
Link/@uid	urn:marlin:organization:@company@:registsign:@ID@:@RID@
Link/AttributeList/Attribute (name="urn:marlin:link:attribute:domain-id")	urn:marlin:organization:@company@:registsign:@ID@:8pususer:@RID@
Link/AttributeList/Attribute (name="urn:marlin:link:attribute:domain-policy")	urn:marlin:broadband:domain-policy:organization:@compnay@:@policyID@
Link/ExtensionList/Extension/@uid	urn:marlin:organization:@company@:registsign:@ID@:@RID@:scuba:private
Link/ExtensionList/Extension/ScubaKeys/SecretKey/@uid	urn:marlin:organization:@company@:registsign:@ID@:8pususer:@RID@:scuba:secret:sharing
Link/ExtensionList/Extension/ScubaKeys/PrivateKey/@uid	urn:marlin:organization:@company@:registsign:@ID@:8pususer:@RID@:scuba:private:sharing
Link/ExtensionList/Extension/ScubaKeys/PrivateKey/@pair	urn:marlin:organization:@company@:registsign:@ID@:8pususer:@RID@:scuba:pair:sharing
Link/Control/@uid	urn:marlin:organization:@company@:registsign:@ID@:control:@RID@

- Agent

Parameter	Convention
AgentCarrier/@contextId	urn:marlin:organization:@company@:registsign:@ID@:@RID@
AgentCarrier/Bundle/Control/@uid	urn:marlin:organization:@company@:registsign:@ID@:control-@RID@

- Delegate1 (This is provided for Root Container from MTMO)

Since the Delegate1 is provided from MTMO, the uid is also issued by MTMO.

Parameter	Convention
Control/@uid	urn:marlin:drmservices:seashell:control:@RID@

- Delegate2 (This is generated by Service Provider)

Parameter	Convention
Control/@uid	urn:marlin:organization:@company@:drmservices:seashell:control:@RID@

A.2.3 Marlin BB DRM Client

- Octopus Personality Node Public Part

Parameter	Convention
uid	urn:marlin:organization:@pdc@:@company@:8pusperso:@RID@
device-class	Dedicated Device, Personal Computer, or Portable Device

- NEMO Message Signing/Encipherment Certificate

Subject value is same between NEMO Message Signing Certificate and NEMO Message Encipherment Certificate for a client.

Parameter	Convention

Subject	urn:marlin:organization:@pdc@:@company@:clientnemo:@RID@

- NEMO Role Assertion

Subject value is same between NEMO Role Assertion and NEMO Message Signing/Encipherment Certificate for a client.

Parameter	Convention
Subject	urn:marlin:organization:@pdc@:@company@:clientnemo:@RID@
NotOnOrAfterDate	DDMMYYYY or None
Marlin Core Spec. Major Version	Major security version of Marlin Core System Specification
Marlin Core Spec. Minor Version	Minor security version of Marlin Core System Specification
Marlin BB Spec. Major Version	Major security version of Marlin Broadband Delivery System Specification
Marlin BB Spec. Minor Version	Minor security version of Marlin Broadband Delivery System Specification
trusted-time	Yes or None
license-suspension	Yes or None
meter-play-duration	Yes or None
manufacturer	urn:marlin:organization:@company@
model	model name which is unique under manufacturer (string)
version	version number of the model (X.X.X)

Appendix B Sample Data (Informative)

This section presents a number of sample data exchanged between Marlin entities. This data should help to better understanding the Marlin specifications.

B.1 NEMO Messages

Here is an example of exchange of NEMO messages between a Marlin Client and a Marlin Service. The message exchange corresponds to the Link Acquisition protocol in Marlin BB, thus, involving three messages: a request, a response, and a confirmation.

Note that for more readability the contents of XML elements with large raw data are represented shortened. Moreover, the Assertions are represented shortened as their content is not relevant for the presentations of NEMO messages.

B.1.1 Request Message

```
<senv:Envelope>

<senv:Header>

<wsa:Action>urn:marlin:broadband:1-1:registration-service:linkAcquisition</wsa:Action>

<wsa:MessageID wsu:Id="sigid0009">
urn:marlin:organization:testpdc:device-maker-x:clientnemo:aa08a1:870f18b787295a41
</wsa:MessageID>

<wsse:Security>

<nemosec:ProtocolDeclaration URI="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0" wsu:Id="sigid0002"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-protocol">
<nemosec:Step Type="request"/>
<nemosec:Reference URI="#NemoIntegrity"
nemosec:TargetUsage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#request-signature"/>
<nemosec:Reference URI="#NemoConfidentiality"
nemosec:TargetUsage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#request-encryptedMessageKey"/>
</nemosec:ProtocolDeclaration>

<nemosec:Profile URI="urn:marlin:core:1.0:nemo:protocol:profile:1" wsu:Id="sigid0003"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/profile"/>

<wsse:Nonce EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary" wsu:Id="sigid0006"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#request-nonce">ZS9sr…RcjqQ==</wsse:Nonce>

<wsu:Timestamp wsu:Id="sigid0005"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#request-timestamp">
<wsu:Created>2008-04-03T13:35:53Z</wsu:Created>
</wsu:Timestamp>

<nemosec:ToNode wsu:Id="sigid0004"
```

```
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#request-toNode">urn:marlin:organization:testpdc:service-provider-
v:registnemo:100</nemosec:ToNode>

<xenc:EncryptedKey Id="NemoConfidentiality">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
</xenc:EncryptionMethod>
<ds:KeyInfo>
<wsse:SecurityTokenReference>
<wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3SubjectKeyIdentifier">segmkG9…2MJg=</wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
<xenc:CipherData>
<xenc:CipherValue>ks1oP7McK…IBBQxtj9c=</xenc:CipherValue>
</xenc:CipherData>
<xenc:ReferenceList>
<xenc:DataReference URI="#EncryptedMessageKey"/>
<xenc:DataReference URI="#EncryptedBody"/>
<xenc:DataReference URI="#EncryptedSignature"/>
</xenc:ReferenceList>
</xenc:EncryptedKey>

<xenc:EncryptedData Id="EncryptedMessageKey"
Type="http://www.w3.org/2001/04/xmlenc#Element">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
<xenc:CipherData>
<xenc:CipherValue>9NxboI…N3gssut4m0=</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>

<wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1"
wsu:Id="sigid0007" nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#response-encryptionKey">MIIJhz…7Yi3HrAqvg==
</wsse:BinarySecurityToken>

<wsse:BinarySecurityToken EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-
200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1"
wsu:Id="sigid0008" nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#request-signingKey">MIIJhTC…Awsb524=
</wsse:BinarySecurityToken>

<Assertion AssertionID="AQAjA0sB" IssueInstant="2007-06-19T16:17:39.745Z"
Issuer="urn:marlin:organization:testpdc:device-maker-x:drmperso" MajorVersion="1"
MinorVersion="1">
        …
</Assertion>

<wsse:SecurityTokenReference
nemosec:Usage="http://nemo.intertrust.com/2004/attribute/role">
<wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID">AQAjA0sB</wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
```

```
<xenc:EncryptedData Id="EncryptedSignature"
Type="http://www.w3.org/2001/04/xmlenc#Element">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
<xenc:CipherData>
<xenc:CipherValue>Zw7U3…dVRgZ</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>

</wsse:Security>

</senv:Header>

<senv:Body wsu:Id="soapBody">

<xenc:EncryptedData Id="EncryptedBody"
Type="http://www.w3.org/2001/04/xmlenc#Content">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
<xenc:CipherData>
<xenc:CipherValue>A8F42x…2dFFjV</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>

</senv:Body>

</senv:Envelope>
```

B.1.2 Response Message

```
<SOAP-ENV:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"
SOAP-ENV:encodingStyle="http://schema.xmlsoap.org/soap/encoding/">

<SOAP-ENV:Header>

<wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" RelationshipType="http://nemo.intertrust.com/2004/addressing/originatesFrom"
wsu:Id="response-relatesToOriginatesFrom" SOAP-
ENV:mustUnderstand="1">urn:marlin:organization:testpdc:device-maker-
x:clientnemo:aa08a1:870f18b787295a41</wsa:RelatesTo>

<wsa:MessageID xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" wsu:Id="response-messageID"
SOAP-ENV:mustUnderstand="1">urn:marlin:organization:testpdc:device-maker-
x:clientnemo:aa08a1:0C764B019FB436FD</wsa:MessageID>

<wsa:Action xmlns:wsa="http://www.w3.org/2005/08/addressing">urn:marlin:broadband:1-
1:registration-service:linkAcquisition</wsa:Action>

<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" SOAP-ENV:mustUnderstand="1">

<nemosec:ProtocolDeclaration
xmlns:nemosec="http://nemo.intertrust.com/2005/10/security" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
URI="http://nemo.intertrust.com/2005/10/security/secure-protocol/basic/1.0"
wsu:Id="response-protocolDeclaration"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-protocol">
```

```
<nemosec:Step Type="response" />
<nemosec:Reference URI="#confidentiality"
nemosec:TargetUsage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#response-encryptedMessageKey" />
<nemosec:Reference URI="#drmIntegrity"
nemosec:TargetUsage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#response-signature" />
</nemosec:ProtocolDeclaration>

<nemosec:Profile xmlns:nemosec="http://nemo.intertrust.com/2005/10/security"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" URI="urn:marlin:core:1.0:nemo:protocol:profile:1" wsu:Id="response-profile"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/profile" />

<wsse:Nonce xmlns:nemosec="http://nemo.intertrust.com/2005/10/security"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binary" wsu:Id="response-nonce"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#response-nonce">wbi81tbefyo…5NjY4NjIx</wsse:Nonce>

<wsse:Nonce xmlns:nemosec="http://nemo.intertrust.com/2005/10/security"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binary" wsu:Id="response-returnedNonce"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#response-returnedNonce">ZS9srU…GRcjqQ==</wsse:Nonce>

<wsu:Timestamp xmlns:nemosec="http://nemo.intertrust.com/2005/10/security"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" wsu:Id="response-timestamp"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#response-timestamp">
<wsu:Created>2008-04-03T13:34:28.621Z</wsu:Created>
</wsu:Timestamp>

<nemosec:ToNode xmlns:nemosec="http://nemo.intertrust.com/2005/10/security"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" wsu:Id="response-toNode"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#response-toNode">urn:marlin:organization:testpdc:device-maker-
x:clientnemo:aa08a1</nemosec:ToNode>

<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="drmEncryptedMessageKey" Type="http://www.w3.org/2001/04/xmlenc#Element">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
<xenc:CipherData>
<xenc:CipherValue>Jpn5+C5…642Uw==</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>

<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="drmEncryptedSignature" Type="http://www.w3.org/2001/04/xmlenc#Element">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
<xenc:CipherData>
<xenc:CipherValue>gCZ2nq…HBjd9s</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>
```

```
<xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="confidentiality">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"
/>
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<wsse:SecurityTokenReference>
<wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3SubjectKeyIdentifier">CkeE5WkKw…mjHtzh0=</wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
<xenc:CipherData>
<xenc:CipherValue>L8uhR…x9Ss0=</xenc:CipherValue>
</xenc:CipherData>
<xenc:ReferenceList>
<xenc:DataReference URI="#drmEncryptedMessageKey" />
<xenc:DataReference URI="#drmEncryptedSignature" />
<xenc:DataReference URI="#drmEncryptedBody" />
</xenc:ReferenceList>
</xenc:EncryptedKey>

</wsse:Security>

</SOAP-ENV:Header>

<SOAP-ENV:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="soapBody">

<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="drmEncryptedBody" Type="http://www.w3.org/2001/04/xmlenc#Element">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
<xenc:CipherData>
<xenc:CipherValue>3yj2+ztr…0h7TTo=</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>
```

B.1.3 Confirmation Message

```
<senv:Envelope xmlns:senv="http://schemas.xmlsoap.org/soap/envelope/">
<senv:Header>

<wsa:Action xmlns:wsa="http://www.w3.org/2005/08/addressing">urn:marlin:broadband:1-
1:registration-service:confirmDRMObjects</wsa:Action>

<wsa:RelatesTo xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" RelationshipType="http://nemo.intertrust.com/2004/addressing/originatesFrom"
wsu:Id="sigid0008">urn:marlin:organization:testpdc:device-maker-
x:clientnemo:aa08a1:870f18b787295a41</wsa:RelatesTo>

<wsa:MessageID xmlns:wsa="http://www.w3.org/2005/08/addressing"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" wsu:Id="sigid0009">urn:marlin:organization:testpdc:device-maker-
x:clientnemo:aa08a1:2a8eafa92a1e1feb</wsa:MessageID>
```

```
<wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd">

<nemosec:ProtocolDeclaration
xmlns:nemosec="http://nemo.intertrust.com/2005/10/security" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
URI="http://nemo.intertrust.com/2005/10/security/secure-protocol/basic/1.0"
wsu:Id="sigid0002" nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol">
<nemosec:Step Type="confirmation" />
<nemosec:Reference URI="#NemoIntegrity"
nemosec:TargetUsage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#confirmation-signature" />
<nemosec:Reference URI="#NemoConfidentiality"
nemosec:TargetUsage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#confirmation-encryptedMessageKey" />
</nemosec:ProtocolDeclaration>

<nemosec:Profile xmlns:nemosec="http://nemo.intertrust.com/2005/10/security"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" URI="urn:marlin:core:1.0:nemo:protocol:profile:1" wsu:Id="sigid0003"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/profile" />

<wsse:Nonce xmlns:nemosec="http://nemo.intertrust.com/2005/10/security"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binary" wsu:Id="sigid0006"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#confirmation-returnedNonce">wbi81tb…NjY4NjIx</wsse:Nonce>

<wsu:Timestamp xmlns:nemosec="http://nemo.intertrust.com/2005/10/security"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" wsu:Id="sigid0005"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#confirmation-timestamp">
<wsu:Created>2008-04-03T13:35:53Z</wsu:Created>
</wsu:Timestamp>

<nemosec:ToNode xmlns:nemosec="http://nemo.intertrust.com/2005/10/security"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" wsu:Id="sigid0004"
nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#confirmation-toNode">urn:marlin:organization:testpdc:service-provider-
v:registnemo:100</nemosec:ToNode>

<xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="NemoConfidentiality">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
<ds:DigestMethod xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
</xenc:EncryptionMethod>
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<wsse:SecurityTokenReference>
<wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
1.0#X509v3SubjectKeyIdentifier">segmkG9…2MJg=</wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
</ds:KeyInfo>
```

```
<xenc:CipherData>
<xenc:CipherValue>aMUK…KMddc=</xenc:CipherValue>
</xenc:CipherData>
<xenc:ReferenceList>
<xenc:DataReference URI="#EncryptedMessageKey" />
<xenc:DataReference URI="#EncryptedBody" />
<xenc:DataReference URI="#EncryptedSignature" />
</xenc:ReferenceList>
</xenc:EncryptedKey>

<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="EncryptedMessageKey" Type="http://www.w3.org/2001/04/xmlenc#Element">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
<xenc:CipherData>
<xenc:CipherValue>jqjaE…TmtAA=</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>

<wsse:BinarySecurityToken xmlns:nemosec="http://nemo.intertrust.com/2005/10/security"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-
message-security-1.0#Base64Binary" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509PKIPathv1"
wsu:Id="sigid0007" nemosec:Usage="http://nemo.intertrust.com/2005/10/security/secure-
protocol/basic/1.0#confirmation-
signingKey">MIIJhTC…sb524=</wsse:BinarySecurityToken>

<Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion" AssertionID="AQAjA0sB"
IssueInstant="2007-06-19T16:17:39.745Z" Issuer="urn:marlin:organization:testpdc:device-
maker-x:drmperso" MajorVersion="1" MinorVersion="1">
…
</Assertion>

<wsse:SecurityTokenReference
xmlns:nemosec="http://nemo.intertrust.com/2005/10/security"
nemosec:Usage="http://nemo.intertrust.com/2004/attribute/role">
<wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/oasis-wss-saml-token-
profile-1.0#SAMLAssertionID">AQAjA0sB</wsse:KeyIdentifier>
</wsse:SecurityTokenReference>
<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="EncryptedSignature" Type="http://www.w3.org/2001/04/xmlenc#Element">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
<xenc:CipherData>
<xenc:CipherValue>CQ29Mk…L86Go</xenc:CipherValue>
</xenc:CipherData>
</xenc:EncryptedData>

</wsse:Security>

</senv:Header>

<senv:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="soapBody">

<xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
Id="EncryptedBody" Type="http://www.w3.org/2001/04/xmlenc#Content">
<xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc" />
<xenc:CipherData>
<xenc:CipherValue>GMSon…b5TdR</xenc:CipherValue>
```

```
</xenc:CipherData>
</xenc:EncryptedData>

</senv:Body>

</senv:Envelope>
```

B.2 Sample Supported DRM Objects

Here is an example of supported DRM objects

Note that for more readability the contents of XML elements with large raw data are represented shortened.

B.2.1 EST License

The following is the sample EST License introduced in §5.2.1.

```
<Bundle xmlns="http://www.octopus-drm.com/profiles/base/1.0"
        xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
        xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <ContentKey
           uid="urn:marlin:organization:foobar:license-service:content-key-111485935">
           <SecretKey
              uid="urn:marlin:organization:foobar:license-service:secret-key-111485935">
              <KeyData encoding="xmlenc" format="RAW">
                 <xenc:EncryptedData>
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
                    <dsig:KeyInfo>
                       <dsig:KeyName>urn:marlin:organization:testpdc:device-maker-
x:8pusperso:aa08a2:scuba:secret:sharing</dsig:KeyName>
                    </dsig:KeyInfo>
                    <xenc:CipherData>
                       <xenc:CipherValue>qoMhF.....zKHXWC</xenc:CipherValue>
                    </xenc:CipherData>
                 </xenc:EncryptedData>
              </KeyData>
           </SecretKey>
        </ContentKey>
        <Protector
           uid="urn:marlin:organization:foobar:license-service:protector-970395650">
           <ContentKeyReference>
              <Uid>urn:marlin:organization:foobar:license-service:content-key-111485935</Uid>
           </ContentKeyReference>
           <ProtectedTargets>
              <ContentReference>
                 <Uid>urn:marlin:organization:foobar:8puslic:0000…0004d2</Uid>
              </ContentReference>
           </ProtectedTargets>
        </Protector>
        <Control Id="control"
           uid="urn:marlin:organization:foobar:license-service:control-2006478942">
           <ControlProgram protocol="http://www.octopus-drm.com/specs/scp-1_0">
              <CodeModule type="http://www.octopus-drm.com/specs/pkcm-
1_0">AAANenBrQ00AAACQcGtFWAAAAAQbQ29udHJvbC5BY3Rpb25zLlBsYXkuQ2hlY2sAAAAEqR5Db
250cm9sLkFjdGlvbnMuUGxheS5EZXNjcmliZQAAAAclGkNvbnRyb2wuQWN0aW9ucy5QbGF5LkluaXQAA
AAEnR1Db250cm9sLkFjdGlvbnMuUGxheS5QZXJmb3JtAAAABKkAAAficGtDUwAAAQAAAAQaAQAAAbc
FGwEAAAAEGgEAAAGzBRoEAQAAAAQaAQAAALMFBAEAAAAEGgEAAAG3BRoBAAAAAyADAQAAA
DIYBAEAAAAEGgEAAAG7BRsEAwH/////CwEAAAAOGQsPAQAAABMZAQAAAAAVAgIBAAAAAABUEAgQ
CFQH////6FQEAAAAEGgEAAAAABRsBAAAABBoBAAAABAUbAwEAAAAECwEAAABAGAEAAAAEBwEA
AAAEGgEAAAAEBQMaBAMaAQAAAAQFBBsaAQAAAAQaAQAAAAAFAxoEAxoBAAAABAUEGxsB////sx
YDAQAAAAALAQAAAEAZAQAAAAEHAQAAAAQaAQAAAAQFAxoEAxoBAAAAAQUEGxwBAAAABBoB
```

```
AAAAAAUDGgQDGgEAAAABBQQbHQH///+zFgIVBB4BAAAABAUaAQAAAAQFGwEAAAAMBRsVBAEA
AAAAAQAAAAgaAQAAAWEFExUeAQAAAAgFGgEAAAAIGgEAAAE1BRMEAwEAAAAQFwIDAQAAABg
FAQAAAAAEGxUBAAAABBoFAxoEAQAAAAQFHgEAAAAIBRoBAAAAGAUBAAAACBoBAAAAfwUTFQQ
BAAAAAQEAAAAIGgEAAAHOBRMVHgEAAAAIBRoBAAAACBoBAAABNQUTBAMBAAAAEBcCAwEAAA
AYBQEAAAAABBsVBAMBAAAAGAUBAAAAAQQbBAMaBAEAAAAEBR4BAAAACAUaAQAAABgFAQAA
AAQFAQAAAAgaAQAAAH8FExUDAQAAAAALAQAAAJ0ZAwEAAAAECwEAAABIGAEAAAAEBwEAAAA
EGgEAAAAABRsDGh4BAAAACAUaGgsPAQAAAHMZBAEAAAAEBQQBAAAABAUBAAAABBoBAAAAA
AUaAf///58WFQEAAAABBwEAAAAEGgEAAAAABRsDHB4BAAAACAUaHAsPAQAAACsZBAEAAAABBQ
QBAAAAAQUBAAAABBoBAAAAAAUaAf///1cWFQICAgEAAAAAFQICAf////8VAx4BAAAACAUaHAQcCw8
BAAAAJRkDHAEAAAAVGQQBAAAAAQUEAQAAAAEFAf///9AWFQICAQAAAAAVAgIB/////xUeAQAAAAg
FGgEAAAAEGgEAAAAABRsBAAAACBoBAAAAAAUTAwEAAACIGAIBAAAABBoBAAAAAAUaAQAAAAQ
aAQAAALMFBAMBAAAAAQsBAAAAMBkDAQAAAAILAQAAADEZAgEAAAAEGgEAAAG7BRoBAAAACB
oBAAACNgUTAwEAAAAlGBUCGgQaCwMPAQAAABcZFQIBAAAACBoBAAAC8QUTAwEAAAABGBUCA
QAAAAAB/////xUEAgEAAAAABBUBAAAABBoBAAABtwUbAf////8EAQAAAAQaAQAAAbcFGgEAAAAIGgE
AAAAABRMDAQAAAAEYFQEAAAAABAEAAAAEGgEAAARqBRoEAQAAAAQaAQAABG4FGgQVAQAA
AAgaAQAAAzIFEwMBAAAAARgVAQAAAAQaAQAABGoFGgQBAAAABBoBAAAEbgUaBBUBAAAAZQQ
BAAAAZQQBAAAABBoBAAAB7QUEAQAAAAgaAQAABUsFExUBAAAAABUB/////xUBAAAABBoDAQAAB
G4FAQAAAEAEGwMBAAAEagUEAQAAAb8FBBsBAAAABBoDAQAABIkFBAEAAAACBAEAAARyBQEA
AAAAAQAAAAgaAQAABEQFEwEAAAAxGAEAAAAEGgMBAAAEyQUaBAMBAAAEzQUaBAEAAAJSBQ
EAAAAIGgEAAAFNBRMBAAAAABUBAAAABBoBAAACUgUBAAAACBoBAAABugUTBBUBAAAABBoBA
AAE0QUaBQEAAAAIGgEAAAB/BRMBAAAABBoBAAAE0QUaBQEAAAAEGgEAAATRBRsBAAAABBoBA
AAE1QUDGgEAAAABBQQbFQMBAAAABBoBAAAE0QUaBQEAAAAEBBsDAQAAAAQaAQAABNEFAxo
BAAAABAUBAAAABBoBAAAE2QUbAwMaAQAAAAgFBBsaBR4BAAAACAUaBBsDAQAAAAQaAQAABN
EFAwMaAQAAAAQFBBsaBR4BAAAACAUaBB4BAAAAEAUaBAEAAAAIGgEAAAB/BRMEAQAAAAQaA
QAABNEFGgUDAQAAAAQaAQAABNEFGwUBAAAABwQbAgEAAAAEGgEAAATRBQMDGgEAAAAEBQ
QbAwMaAQAAAAQaAQAABN0FGwMaAQAAAAQFBBsDGgEAAAAEGgEAAAThBRsDGgEAAAAEBQQb
AQAAAAABAAAABBoBAAAE1QUbFQMBAAAABBoBAAAE0QUaAQAAAAQaAQAABNkFGgEAAAAEBQc
EAQAAAAQaAQAABNkFGgUbAwEAAAAEGgEAAATRBRoBAAAABBoBAAAE3QUaAQAAAAQFBwQBA
AAABBoBAAAE3QUaBRsBAAAABBoBAAAE1QUaBAEAAAAEGgEAAAThBRoFGxUBAAAABBoBAAACU
gUDAQAAAEAEAQAAAAAEAQAAAAgaAQAAATUFEwEAAAABBAEAAAAYBRsBAAAAHAEAAAAEGgE
AAATRBRsBAAAABBoBAAACUgUDAQAAAAQaAQAABOUFBAEAAAASBAEAAAAIGgEAAAWYBRMDA
QAAAAgaAQAABHYFEwMBAAAACBoBAAAGowUTAgEAAAAEGgEAAAJSBQEAAAAAFQEAAAAEGgE
AAAJSBQH/////FQAABQBwa0RTAAAAAAAAAAAAAAAApwAAAAEAAAAEAAAAmwAAAAxPYmxpZ2F0a
W9ucwAAAAAHAAAAgwAAAAEAAAAFAAAAdwAAAAEAAAAOT3V0cHV0Q29udHJvbAAAAAAHAAAAW
QAAAAIAAAACAAAACUJhc2ljQ0NJAAAAAAcAAAA8AAAAAgAAAAQAAAAUAAAABENDSQAAAAAAAA
AABAAAAAMAAAAEAAAAFAAAAARBUFMAAAAAAAAAAAAQAAAABAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAI8AAAAEAAAAhwAAABJ
EZXZpY2VDb25zdHJhaW50cwAAAAAHAAAAaQAAAAEAAAAEAAAAXQAAABFEZXZpY2VJZFJlcXVpcm
VkAAAAAAIAAABAdXJuOm1hcmxpbjpvcmdhbml6YXRpb246dGVzdHBkYzpkZXZpY2UtbWFrZXIteDo4cH
VzcGVyc286YWEwOGEyAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABPY3RvcHVzL1BlcnNvbmFsaXR5L0lkAHVybjptYXJsa
W46b3JnYW5pemF0aW9uOnRlc3RwZGM6ZGV2aWNlLW1ha2VyLXg6OHB1c3BlcnNvOmFhMDhhMgAA
AAAIAAAAAQAAAAAAAAAAAAAAAAAAAAAAAARGV2aWNlQ29uc3RyYWludHMA</CodeModule>
        </ControlProgram>
      </Control>
      <Controller Id="controller"
        uid="urn:marlin:organization:foobar:license-service:controller-1579340869">
        <ControlReference>
          <Uid>urn:marlin:organization:foobar:license-service:control-2006478942</Uid>
          <Digest>
            <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <dsig:DigestValue>3SdJV….. xP+1Y=</dsig:DigestValue>
          </Digest>
        </ControlReference>
        <ControlledTargets>
          <ContentKeyReference>
            <Uid>urn:marlin:organization:foobar:license-service:content-key-111485935</Uid>
            <Digest>
              <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
              <dsig:DigestValue>l6Ezo…..YF8ZE=</dsig:DigestValue>
            </Digest>
          </ContentKeyReference>
        </ControlledTargets>
      </Controller>
      <dsig:Signature Id="PKSig" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
        <dsig:SignedInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
          <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <dsig:Reference URI="#controller">
            <dsig:Transforms>
              <dsig:Transform Algorithm="http://www.octopus-drm.com/octopus/specs/cbs-1_0"/>
            </dsig:Transforms>
            <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <dsig:DigestValue>MLQGs8P1zSbYzSsZsyTJEGdOjaw=</dsig:DigestValue>
          </dsig:Reference>
        </dsig:SignedInfo>
        <dsig:SignatureValue>puBQk.....TB2rIpOw==</dsig:SignatureValue>
        <dsig:KeyInfo>
          <dsig:X509Data>
            <dsig:X509Certificate>MIIEF...../osnwE8=</dsig:X509Certificate>
            <dsig:X509Certificate>MIID2.....VgiT9ai</dsig:X509Certificate>
          </dsig:X509Data>
        </dsig:KeyInfo>
      </dsig:Signature>
      <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
        <dsig:SignedInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
          <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
          <dsig:Reference URI="#controller">
            <dsig:Transforms>
              <dsig:Transform Algorithm="http://www.octopus-drm.com/octopus/specs/cbs-1_0"/>
            </dsig:Transforms>
            <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <dsig:DigestValue>MLQGs…..GdOjaw=</dsig:DigestValue>
          </dsig:Reference>
          <dsig:Reference URI="#PKSig">
            <dsig:Transforms>
              <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            </dsig:Transforms>
            <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <dsig:DigestValue>l7Wav..... yvwxfY=</dsig:DigestValue>
          </dsig:Reference>
        </dsig:SignedInfo>
     <dsig:SignatureValue>zh++3..... wudBAG4=</dsig:SignatureValue>
        <dsig:KeyInfo>
          <dsig:KeyName>urn:marlin:organization:foobar:license-service:secret-key-
111485935</dsig:KeyName>
        </dsig:KeyInfo>
      </dsig:Signature>
    </Bundle>
```

B.2.2 Rental License

The following is the sample Rental License in absolute validity period introduced in §5.2.2.

```
<Bundle xmlns="http://www.octopus-drm.com/profiles/base/1.0"
    xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <ContentKey
        uid="urn:marlin:organization:foobarv:license-service:content-key-425107268">
        <SecretKey
            uid="urn:marlin:organization:foobarv:license-service:secret-key-425107268">
            <KeyData encoding="xmlenc" format="RAW">
                <xenc:EncryptedData>
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-
cbc"/>
                    <dsig:KeyInfo>
                        <dsig:KeyName>urn:marlin:organization:testpdc:device-maker-
x:8pusperso:aa08a2:scuba:secret:sharing</dsig:KeyName>
                    </dsig:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>IsaZK.....TNJIvdrvl</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
            </KeyData>
        </SecretKey>
    </ContentKey>
    <Protector uid="urn:marlin:organization:foobarv:license-service:protector-346716407">
        <ContentKeyReference>
            <Uid>urn:marlin:organization:foobarv:license-service:content-key-425107268</Uid>
        </ContentKeyReference>
        <ProtectedTargets>
            <ContentReference>
                <Uid>urn:marlin:organization:foobarv:8puslic:000000000004d2</Uid>
            </ContentReference>
        </ProtectedTargets>
    </Protector>
    <Control Id="control"
        uid="urn:marlin:organization:foobarv:license-service:control-257327869">
        <ControlProgram protocol="http://www.octopus-drm.com/specs/scp-1_0">
            <CodeModule type="http://www.octopus-drm.com/specs/pkcm-1_0">
AAAQD3BrQ00AAACQcGtFWAAAAAQbQ29udHJvbC5BY3Rpb25zLlBsYXkuQ2hlY2sAAAAF1R5Db250
cm9sLkFjdGlvbnMuUGxheS5EZXNjcmliZQAAAAiZGkNvbnRyb2wuQWN0aW9ucy5QbGF5LkluaXQA
AAAFth1Db250cm9sLkFjdGlvbnMuUGxheS5QZXJmb3JtAAAABdUAAAmhcGtDUwAAAQAAAAQaAQAA
AbcFGwEAAAAEGgEAAAGzBRoEAQAAAAQaAQAAALMFBAEAAAAEGgEAAAG3BRoBAAAAAyADAQA
AADIYBAEAAAAEGgEAAAG7BRsEAwH/////CwEAAAAOGQsPAQAAABMZAQAAAAAVAgIBAAAAAABUEA
gQCFQH////6FQEAAAAEGgEAAAAABRsBAAAABBoBAAAABAUbAwEAAAAECwEAAABAGAEAAAAEBw
EAAAAEGgEAAAAEBQMaBAMaAQAAAAQFBBsaAQAAAAQaAQAAAAAFAxoEAxoBAAAABAUEGxsB////
sxYDAQAAAAALAQAAAEAZAQAAAAEHAQAAAAQaAQAAAAQFAxoEAxoBAAAAAQUEGxwBAAAABBo
BAAAAAAUDGgQDGgEAAAABBQQbHQH///+zFgIVBB4BAAAABAUaAQAAAAQFGwEAAAAMBRsVBAE
AAAAAAQAAAAgaAQAAAWEFExUeAQAAAAgFGgEAAAAIGgEAAAE1BRMEAwEAAAAQFwIDAQAAAB
gFAQAAAAAEGxUBAAAABBoFAxoEAQAAAAQFHgEAAAAIBRoBAAAAGAUBAAAACBoBAAAAfwUTFQ
QBAAAAAQEAAAAIGgEAAAHOBRMVHgEAAAAIBRoBAAAACBoBAAABNQUTBAMBAAAAEBcCAwEAA
AAYBQEAAAAABBsVBAMBAAAAGAUBAAAAAQQbBAMaBAEAAAAEBR4BAAAACAUaAQAAABgFAQA
AAAQFAQAAAAgaAQAAAH8FExUBAAAABBoBAAAFKAUaDwMBAAAAIRkCAQAAAAQaAQAABQ0FAQ
AAAAIgAwEAAAAEGgEAAAUoBRsVAQAAAAQaAQAABSgFGiAEAgMBAAAADhgLAQAAABsXAgEAAA
AAFQQCAgEAAAAABAEAAAAIAf////8VAQAAAAAEAQAAAAgB/////xUBAAAABBoBAAAFKAUaIAQCAwEA
AAAOGAsBAAAAGxgCAQAAAAAVBAICAQAAAAAEAQAAAAgB/////xUBAAAAAAAQBAAAACAH/////FQEA
AAAiBAEAAAAiBAEAAAAEGgEAAAHvBQQBAAAACBoBAAAGvwUTFQEAAAAhBAEAAAAhBAEAAAAE
GgEAAAJBBQQBAAAACBoBAAAGvwUTFQMBAAAAAAsBAAAAnRkDAQAAAAQLAQAAAEgYAQAAAA
QHAQAAAAQaAQAAAAAFGwMaHgEAAAAIBRoaCw8BAAAAcxkEAQAAAAQFBAEAAAAEBQEAAAAEG
gEAAAAABRoB////nxYVAQAAAAEHAQAAAAQaAQAAAAAFGwMcHgEAAAAIBRocCw8BAAAAKxkEAQA
AAAEFBAEAAAABBQEAAAAEGgEAAAAABRoB////VxYVAgICAQAAAAAVAgIB/////xUDHgEAAAAIBRocB
BwLDwEAAAAlGQMcAQAAABUZBAEAAAABBQQBAAAAAQUB////0BYVAgIBAAAAAABUCAgH/////FR4BA
AAACAUaAQAAAAQaAQAAAAAFGwEAAAAIGgEAAAAABRMDAQAAAIgYAgEAAAAEGgEAAAAABRoB
AAAABBoBAAAAswUEAwEAAAABCwEAAAAwGQMBAAAAAgsBAAAAMRkCAQAAAAQaAQAAAbsFGg
EAAAAIGgEAAANPBRMDAQAAACUYFQIaBBoLAw8BAAAAFxkVAgEAAAAIGgEAAAQKBRMDAQAAAA
EYFQIBAAAAAAH/////FQQCAQAAAAAEFQEAAAAEGgEAAAG3BRsB/////wQBAAAABBoBAAABtwUaAQA
AAAgaAQAAAAAFEwMBAAAAARgVAQAAAAAEAQAAAAQaAQAABSwFGgQBAAAABBoBAAAFMAUaB
BUBAAAACBoBAAAESwUTAwEAAAABGBUBAAAABBoBAAAFLAUaBAEAAAAEGgEAAAUwBRoEFQE
AAABlBAEAAABlBAEAAAAEGgEAAAKQBQQBAAAACBoBAAAGvwUTFQEAAAAIGgEAAAI2BRMBAAA
ABhgBAAAAAABUB/////xUBAAAABBoBAAABvwUBATFMzAEAAAAIGgEAAAJtBRMBAAAAqxgBAAAABBo
BAAACEQUBATF0LAEAAAAIGgEAAAK3BRMBAAAAhxgBAAAABBoDAQAABTAFAQAAAEAEGwMBAA
AFLAUEAQAAAmIFBBsBAAAABBoDAQAABUsFBAEAAAACBAEAAAU0BQEAAAAAAQAAAAgaAQAAB
```

```
V0FEwEAAAAxGAEAAAAEGgMBAAAFiwUaBAMBAAAFjwUaBAEAAAL1BQEAAAAIGgEAAAFNBRMBA
AAAABUBAAAABBoBAAAC9QUBAAAACBoBAAABugUTBBUBAAAABBoBAAAFkwUaBQEAAAAIGgEAA
AB/BRMBAAAABBoBAAAFkwUaBQEAAAAEGgEAAAWTBRsBAAAABBoBAAAFlwUDGgEAAAABBQQbF
QMBAAAABBoBAAAFkwUaBQEAAAAEBBsDAQAAAAQaAQAABZMFAxoBAAAABAUBAAAABBoBAAAF
mwUbAwMaAQAAAAgFBBsaBR4BAAAACAUaBBsDAQAAAAQaAQAABZMFAwMaAQAAAAQFBBsaBR4
BAAAACAUaBB4BAAAAEAUaBAEAAAAIGgEAAAB/BRMEAQAAAAQaAQAABZMFGgUDAQAAAAQaAQ
AABZMFGwUBAAAABwQbAgEAAAAEGgEAAAWTBQMDGgEAAAAEBQQbAwMaAQAAAAQaAQAABZ8
FGwMaAQAAAAQFBBsDGgEAAAAEGgEAAAWjBRsDGgEAAAAEBQQbAQAAAAABAAAABBoBAAAFlw
UbFQMBAAAABBoBAAAFkwUaAQAAAAQaAQAABZsFGgEAAAAEBQcEAQAAAAQaAQAABZsFGgUbA
wEAAAAEGgEAAAWTBRoBAAAABBoBAAAFnwUaAQAAAAQFBwQBAAAABBoBAAAFnwUaBRsBAAAA
BBoBAAAFlwUaBAEAAAAEGgEAAAWjBRoFGxUBAAAABBoBAAAC9QUDAQAAAEgEAQAAAAAEAQA
AAAgaAQAAATUFEwEAAAACBAEAAAAYBRsBAAAAHAEAAAAEGgEAAAWTBRsBAAAABBoBAAAC9Q
UDAQAAAAQaAQAABacFBAEAAAASBAEAAAAIGgEAAAcMBRMDAQAAAAgaAQAABY8FEwMBAAAAC
BoBAAAIFwUTAwEAAAAEGgEAAAW5BQQBAAAAFAQBAAAACBoBAAAHDAUTAwEAAAAIGgEAAAMB
BRMDAQAAAAgaAQAAAygFEwMBAAAACBoBAAAIFwUTAgEAAAAEGgEAAAL1BQEAAAAAFQEAAAA
EGgEAAAL1BQH/////FQAABdZwa0RTAAAAAAAAAAAAAAAApwAAAAEAAAAEAAAAmwAAAAxPYmxpZ
2F0aW9ucwAAAAAHAAAAgwAAAAEAAAAFAAAAdwAAAAEAAAAOT3V0cHV0Q29udHJvbAAAAAAHAA
AAWQAAAAIAAAACAAAACUJhc2ljQ0NJAAAAAAcAAAA8AAAAAgAAAAQAAAAUAAAABENDSQAAAAA
AAAAABAAAAAMAAAAEAAAAFAAAAARBUFMAAAAAAAAAAAAAQAAAABAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAE4AAAAEAAAARgAA
ABRUZW1wb3JhbENvbnN0cmFpbnRzAAAAAAcAAAAmAAAAAQAAAAQAAAAaAAAACk5vdEJlZm9yZQ
AAAAADAAAABAExTMwAAABNAAAABAAAAEUAAAAUVGVtcG9yYWxDb25zdHJhaW50cwAAAAAHAA
AAJQAAAAEAAAAEAAAAGQAAAAlOb3RBZnRlcgAAAAADAAAABAExdCwAAACPAAAABAAAAIcAAAA
SRGV2aWNlQ29uc3RyYWludHMAAAAABwAAAGkAAAABAAAABAAAAF0AAAARRGV2aWNlSWRSZXF
1aXJlZAAAAAACAAAAQHVybjptYXJsaW46b3JnYW5pemF0aW9uOnRlc3RwZGM6ZGV2aWNlLW1ha2Vy
LXg6OHB1c3BlcnNvOmFhMDhhMgAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAFN5c3RlbS5Ib3N0LkdldFRydXN0ZWRUaW1lAAAAAAAAAAAAA
AAAAAAAE9jdG9wdXMvUGVyc29uYWxpdHkvSWQAdXJuOm1hcmxpbjpvcmdhbml6YXRpb246dGVzdHB
kYzpkZXZpY2UtbWFrZXIteDo4cHVzcGVyc286YWEwOGEyAAAAAgAAAABAAAAAAAAAAAAAAAAAAAA
AAAAAAABEZXZpY2VDb25zdHJhaW50cwBUZW1wb3JhbENvbnN0cmFpbnRzAA== </CodeModule>
        </ControlProgram>
    </Control>
    <Controller Id="controller"
        uid="urn:marlin:organization:foobarv:license-service:controller-878926980">
        <ControlReference>
            <Uid>urn:marlin:organization:foobarv:license-service:control-257327869</Uid>
            <Digest>
                <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <dsig:DigestValue>ChKPFeHpLKfxELAnkiS4NzH1BMo=</dsig:DigestValue>
            </Digest>
        </ControlReference>
        <ControlledTargets>
            <ContentKeyReference>
                <Uid>urn:marlin:organization:foobarv:license-service:content-key-425107268</Uid>
                <Digest>
                    <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <dsig:DigestValue>5q3NHXTUruXIuRrzWdZq8fL+a0Y=</dsig:DigestValue>
                </Digest>
            </ContentKeyReference>
        </ControlledTargets>
    </Controller>
    <dsig:Signature Id="PKSig" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
        <dsig:SignedInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
```

```
            <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <dsig:Reference URI="#controller">
                <dsig:Transforms>
                    <dsig:Transform Algorithm="http://www.octopus-drm.com/octopus/specs/cbs-1_0"/>
                </dsig:Transforms>
                <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <dsig:DigestValue>lS8URwbli6tyGIEnWVgslbwzDV0=</dsig:DigestValue>
            </dsig:Reference>
        </dsig:SignedInfo>
        <dsig:SignatureValue>GC9f...cR6WmQ==</dsig:SignatureValue>
        <dsig:KeyInfo>
            <dsig:X509Data>
                <dsig:X509Certificate>MIIEFTC....snwE8=</dsig:X509Certificate>
                <dsig:X509Certificate>MIID2jCC....giT9ai</dsig:X509Certificate>
            </dsig:X509Data>
        </dsig:KeyInfo>
    </dsig:Signature>
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
        <dsig:SignedInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
            <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
            <dsig:Reference URI="#controller">
                <dsig:Transforms>
                    <dsig:Transform Algorithm="http://www.octopus-drm.com/octopus/specs/cbs-1_0"/>
                </dsig:Transforms>
                <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <dsig:DigestValue>lS8UR.....zDV0=</dsig:DigestValue>
            </dsig:Reference>
            <dsig:Reference URI="#PKSig">
                <dsig:Transforms>
                    <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                </dsig:Transforms>
                <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <dsig:DigestValue>Rt87w.....kubg=</dsig:DigestValue>
            </dsig:Reference>
        </dsig:SignedInfo>
        <dsig:SignatureValue>Mlfcn.....Kds=</dsig:SignatureValue>
        <dsig:KeyInfo>
            <dsig:KeyName>urn:marlin:organization:foobarv:license-service:secret-key-
425107268</dsig:KeyName>
        </dsig:KeyInfo>
    </dsig:Signature>
</Bundle>
```

B.2.3 Suscription License

The following is the sample Subscription License introduced in §5.2.3.

```
<Bundle xmlns="http://www.octopus-drm.com/profiles/base/1.0"
    xmlns:dsig="http://www.w3.org/2000/09/xmldsig#"
    xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <ContentKey
        uid="urn:marlin:organization:foobarv:license-service:content-key-1908710845">
        <SecretKey
            uid="urn:marlin:organization:foobarv:license-service:secret-key-1908710845">
            <KeyData encoding="xmlenc" format="RAW">
                <xenc:EncryptedData>
                    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-
cbc"/>
                    <dsig:KeyInfo>
    <dsig:KeyName>urn:marlin:organization:foobarv:8pususer:0:scuba:secret:sharing</dsig:KeyName>
                    </dsig:KeyInfo>
                    <xenc:CipherData>
                        <xenc:CipherValue>sskQ2.....AzLDxB</xenc:CipherValue>
                    </xenc:CipherData>
                </xenc:EncryptedData>
            </KeyData>
        </SecretKey>
    </ContentKey>
    <Protector
        uid="urn:marlin:organization:foobarv:license-service:protector-767599052">
        <ContentKeyReference>
            <Uid>urn:marlin:organization:foobarv:license-service:content-key-1908710845</Uid>
        </ContentKeyReference>
        <ProtectedTargets>
            <ContentReference>
                <Uid>urn:marlin:organization:foobarv:8puslic:00000000004d2</Uid>
            </ContentReference>
        </ProtectedTargets>
    </Protector>
    <Control Id="control"
        uid="urn:marlin:organization:foobarv:license-service:control-997979030">
        <ControlProgram protocol="http://www.octopus-drm.com/specs/scp-1_0">
            <CodeModule type="http://www.octopus-drm.com/specs/pkcm-1_0">
AAAhEnBrQ00AAACQcGtFWAAAAAQbQ29udHJvbC5BY3Rpb25zLlBsYXkuQ2hlY2sAAAAOkh5Db250
cm9sLkFjdGlvbnMuUGxheS5EZXNjcmliZQAAABLIGkNvbnRyb2wuQWN0aW9ucy5QbGF5LkluaXQA
AAAOTR1Db250cm9sLkFjdGlvbnMuUGxheS5QZXJmb3JtAAAAEC0AABRTcGtDUwAAAQAAAAQaAQAA
AdMFGwEAAAAEGgEAAAHPBRoEAQAAAAQaAQAAAM8FBAEAAAAEGgEAAAHTBRoBAAAAAyADAQ
AAADIYBAEAAAAEGgEAAAHXBRsEAwH/////CwEAAAAOGQsPAQAAABMZAQAAAAAVAgIBAAAAAABUE
AgQCFQH////6FQEAAAAEGgEAAAAABRsBAAAABBoBAAAABAUbAwEAAAAECwEAAABAGAEAAAAEB
wEAAAAEGgEAAAAEBQMaBAMaAQAAAAQFBBsaAQAAAAQaAQAAAAAFAxoEAxoBAAAABAUEGxsB/
///sxYDAQAAAAALAQAAAEAZAQAAAAEHAQAAAAQaAQAAAAQFAxoEAxoBAAAAAQUEGxwBAAAABB
oBAAAAAAUDGgQDGgEAAAABBQQbHQH///+zFgIVBB4BAAAABAUaAQAAAAQFGwEAAAAMBRsVBA
EAAAAAAQAAAAgaAQAAAWEFExUeAQAAAAgFGgEAAAAIGgEAAAE1BRMEAwEAAAAQFwIDAQAAA
BgFAQAAAAAEGxUBAAAABBoFAxoEAQAAAAQFHgEAAAAIBRoBAAAAGAUBAAAACBoBAAAAfwUTF
QQBAAAAAQEAAAAIGgEAAAHOBRMVHgEAAAAIBRoBAAAACBoBAAABNQUTBAMBAAAAEBcCAwE
AAAAYBQEAAAAABBsVBAMBAAAAGAUBAAAAAQQbBAMaBAEAAAAEBR4BAAAACAUaAQAAABgFA
QAAAAQFAQAAAAgaAQAAAH8FExUBAAAABBoBAAAJLAUaDwMBAAAAIRkCAQAAAAQaAQAACREF
AQAAAAIgAwEAAAAEGgEAAAksBRsVAQAAAAQaAQAACSwFGiAEAgMBAAAADhgLAQAAABsXAgEA
AAAAFQQCAgEAAAAABAEAAAAIAf////8VAQAAAAAEAQAAAAgB/////xUBAAAABBoBAAAJLAUaIAQCAw
EAAAAOGAsBAAAAGxgCAQAAAAAVBAICAQAAAAAEAQAAAAgB/////xUBAAAAAAAQBAAAACAH/////FQ
EAAAAiBAEAAAAiBAEAAAAEGgEAAAILBQQBAAAACBoBAAAQ7gUTFQEAAAAhBAEAAAAhBAEAAAA
EGgEAAAJdBQQBAAAACBoBAAAQ7gUTFQMBAAAAAAsBAAAAnRkDAQAAAAQLAQAAAEgYAQAAAA
QHAQAAAAQaAQAAAAAFGwMaHgEAAAAIBRoaCw8BAAAAcxkEAQAAAAQFBAEAAAAEBQEAAAAEG
gEAAAAABRoB////nxYVAQAAAAEHAQAAAAQaAQAAAAAFGwMcHgEAAAAIBRocCw8BAAAAKxkEAQA
AAAEFBAEAAAAABBQEAAAAEGgEAAAAABRoB////VxYVAgICAQAAAAAVAgIB/////xUDHgEAAAAIBRocB
BwLDwEAAAAlGQMcAQAAABUZBAEAAAAABBQQBAAAAAQUB////0BYVAgIBAAAAAABUCAgH/////FR4BA
AAACAUaAQAAAAQaAQAAAAAFGwEAAAAIGgEAAAAABRMDAQAAAIgYAgEAAAAEGgEAAAAABRoB
AAAABBoBAAAAzwUEAwEAAAABCwEAAAAwGQMBAAAAAgsBAAAAMRkCAQAAAAQaAQAAAdcFGg
EAAAAIGgEAAANPBRMDAQAAACUYFQIaBBoLAw8BAAAAFxkVAgEAAAAIGgEAAAQKBRMDAQAAAA
EYFQIBAAAAAAH/////FQQCAQAAAAAEFQEAAAAEGgEAAAHTBRsB/////wQBAAAABBoBAAAB0wUaAQ
AAAAgaAQAAAAAFEwMBAAAAARgVAQAAAAAEAQAAAAQaAQAACTAFGgQBAAAABBoBAAAJNAUa
BBUBAAAACBoBAAAESwUTAwEAAAABGBUBAAAABBoBAAAJMAUaBAEAAAAEGgEAAAk0BRoEFQQ
eAQAAAAQFGgEAAAAKCAMBAAAADhkBAAAACBoBAAAFjwUTAwIEAQAAAAoJAQAAADAFHgEAAAA
EBRodAQAAAAEFFQMBAAAAFRgBAAAACBoBAAAFjwUTAQAAAAAEHRUKBAMaAQAAAC0EHQEAA
AABBQQB////0xYBAAAAAAAQDHAEAAAAUGQEAAAABBQQBAAAAAQUEAf///+QWAhUEAwEAAAAIGgE
AAAYFBRMBAAAAAQUEHgEAAAAIBRoDAQAAAAgaAQAABgUFEwUBAAAACBoBAAAAfwUTAhUBAA
AAAAQBAAAABBoBAAAJigUEAQAAAAgaAQAAAAAFEwMBAAABMxgCAQAAAAEBAAAABBoBAAAJnA
UBAAAABBoBAAAAzwUaAwEAAAAEGgEAAAmyBRsBAAAACBoBAAAAAAAUTAwEAAADyGAIBAAAABB
oBAAAAzwUaAQAAAAEHAwEAAADXGAMBAAAABBoBAAAJogUDAQAAAEAEHQEAAAABBQQBAAAA
CBoBAAAF0QUTHgEAAAAMBRoeAQAAAAwFGgEAAAAEGgEAAAmiBQEAAAAEGgEAAAmyBRoBAAA
ACBoBAAAESwUTAQAAAAcZAgH///+HFgEAAAAEGgMBAAAJlQUEAQAACaIFAQAAAAgaAQAABikFEx
4BAAAABAUaAQAAAAIBAAAABBoBAAAJogUBAAAABBoBAAAJsgUaAQAAAAgaAQAABEsFEwEAAAA
HGQIB////JhYCAgICAQAAAAAVBAIEAgQCAQAAAAAEFQEAAAAABAEAAAAAAAQAAAAgaAQAAAAAFE
wMBAAABCxgCAQAAAAEBAAAABBoBAAAJnAUBAAAABBoBAAAAzwUaAwEAAAAEGgEAAAm8BRsB
AAAACBoBAAAAAAAUTAwEAAADKGAIBAAAABBoBAAAAzwUaAQAAAAEHAwEAAAC0GAMBAAAABBo
BAAAJtgUDAQAAAEAEHQEAAAABBQQBAAAACBoBAAAF0QUTAQAAAAABAAAABBoBAAAJtgUBAAA
ABBoBAAAJvAUaAQAAAAgaAQAAAAAFEwMBAAAAUhgCAQAAAAQaAQAAAM8FGh4BAAAADAUaAQ
AAAAIeAQAAABAFGgEAAAAEGgEAAADPBRoBAAAACBoBAAAGZQUTAQAAAAgZAgIB////TRYEAgQC
BAIVBAIEAgQCFQICAgH/////FQEAAAAEGgEAAAnABRoDAf////8LAQAAAAMZBAIVAgEAAAAEGgMBAAA
```

```
J+gUEAwEAAAnWBQQBAAAJxAUBAAAACBoBAAAHzAUTAwEAAAARGAQCAwEAAAAEGgEAAAnAB
RsVAgEAAAAABAEAAABAAf////8VAQAAAAgaAQAACcYFEwMBAAAAERkEAgQCAQAAACIYAgEAAAA
AFQIBAAAACBoBAAAJxgUTAQAAAAcYAgEAAAAAFQEAAAAABAEAAABAAf////8VAQAAAAEEAQAAAA
QaAQAACcAFGgEAAAAIGgEAAAAABRMDAQAAABEYAgEAAAAEGgEAAADPBRoECxUEAhUBAAAAN
gQBAAAANgQBAAAABBoBAAACrAUEAQAAAAgaAQAAEO4FExUBAAAANgQBAAAANgQBAAAABBoB
AAAC4gUEAQAAAAgaAQAAEO4FExUBAAAABBoBAAAKOAUaDwMBAAAAIRkCAQAAAAQaAQAACho
FAQAAAAIgAwEAAAAEGgEAAAo4BRsVAQAAAAQaAQAACjgFGiAEAgMBAAAAAxgEAhUCAQAAAAAE
AQAAAAQB/////xUBAAAAaQQBAAAAaQQBAAAABBoBAAADRwUEAQAAAAgaAQAAEO4FExUBAAAAY
wQBAAAAYwQBAAAABBoBAAAD3wUEAQAAAAgaAQAAEO4FExUBAAAABBoBAAABzwUaBAEAAAAE
GgEAAADPBQQBAAAAAAAEAAAADIAQCAwEAAAAiFwMB////+gsPAQAAAAgZAgIBAAAAAABUEAQAAAA
QB/////xUCAQAAAAAEAQAAAAQB/////xUBAAAAMAQBAAAAMAQBAAAABBoBAAAEcQUEAQAAAAgaA
QAAEO4FExUeAQAAAAwFGh4BAAAACAUaHgEAAAAIBRoBAAAACBoBAAAAAAAUTAwEAAAAPGAQC
BAIEAgQCBAIEAgQCFQIBAAAABCADAQAAACQYAgEAAAAEBAEAAAABBB4BAAAADAUaBAEAAAAA
AQAAAAQgBAIVBAIEAhUBAAAABCADAQAAAC0YBAMBAAAAJhkEAgEAAAAEBAEAAAABBB4BAAAA
DAUaBAEAAAAAAQAAAAQgBAIVBAIEAhUBAAAAAAAEAAAAIGgEAAAv8BRMDAQAAAAMYBAIVBAEA
AAAEAf////8VAQAAAAQaAQAAAc8FGgQBAAAABBoBAAAAzwUEAQAAAAABAAAAAyAEAgMB////+gsBA
AAAVhkDAQAAAD8YAQAAAAELAQAAABMZAgIBAAAAAAAQBAAAACAH/////FQMBAAAABBoBAAAAzwU
aBBsaBQEAAAAIGgEAAAK3BRMVBAIEAgQBAAAACAH/////FQICAgIBAAAAAABUEAxoBAAAAcxcDAQAA
AAQaAQAACSwFGiAEAgMBAAAARRgEGwEAAAAEGgEAAAAABRsBAAAABAQBAAAAAQQBAAAABB
oBAAAAAAUaBAEAAAAAAQAAAAgaAQAAC4oFEwMBAAAADRgEAhUEAgQCBAIEAgQCBAEAAAAIAf//
//8VAgICAgIBAAAAABUBAAAAJgQBAAAAJgQBAAAABBoBAAAE0QUEAQAAAAgaAQAAEO4FExUBAA
AAAQEAAAAEGgEAAAr9BQEAAAAAAQAAAAgaAQAAAAAFEwEAAAB8GAEAAAAEGgEAAADPBRoDA
QAAAAQaAQAABUUFGwEAAAACBQEAAAAEGgEAAAVmBRsDAQAAACIEAQAAACIEAQAAAAQaAQA
ABScFBAEAAAAIGgEAABDuBRMBAAAAIQQBAAAAIQQBAAAABBoBAAAFSQUEAQAAAAgaAQAAEO4
FExUCFQEAAAAIGgEAAAI2BRMBAAAALBgBAAAACBoBAAAKTwUTAQAAABkYAQAAAAgaAQAAAjYF
EwEAAAAGGAEAAAAAFQH/////FQEAAAAEGgEAAAHbBQEBELPfAQAAAAgaAQAAAm0FEwEAAAFcGA
EAAAAEGgEAAAItBQEBQN3fAQAAAAgaAQAAArcFEwEAAAE4GAEAAAAEGgEAAAJ+BQEAAAAIGgEA
AAkEBRMBAAABGRgBAAAABBoBAAACfgUBAAAAAwEAAAAEGgMBAAAJYQUEAQAAAAEEAQAACTg
FAQAAAAgaAQAACXUFEwEAAADbGAEAAAAEGgMBAAADGAUEAQAACjwFAQAAAAgaAQAACoYFE
wEAAAC0GAEAAAAEGgMBAAADsAUEAQAACngFAQAAAAgaAQAACoYFEwEAAACNGAEAAAAEGgM
BAAAEQgUEAQAACq4FAQAAAAgaAQAACwAFEwEAAABmGAEAAAAEGgMBAAAEoQUEAQAAAAIEA
wEAAAtTBQQBAAAK/QUBAAAACBoBAAAMYwUTAQAAADEYAQAAAAQaAwEAAAvBBRoEAwEAAAvF
BRoEAQAABWoFAQAAAAgaAQAAAU0FEwEAAAAAFQEAAAAEGgEAAAVqBQEAAAAIGgEAAAG6BRM
EFQEAAAAIGgEAAA6SBRMDAQAAAAEZFQQDAQAAAAQFGgEAAAABCw8BAAAAAhkEFQICAQAAAA
QaAwEAAAShBQQDAQAAC70FBAMBAAALVwUEAwEAAAtTBQQBAAAK/QUBAAAACBoBAAAM+AUTA
QAAADEYAQAAAAQaAwEAAAvJBRoEAwEAAAvNBRoEAQAABWoFAQAAAAgaAQAAAU0FEwEAAAAA
FQEAAAAEGgEAAAVqBQEAAAAIGgEAAAG6BRMEFQEAAAAABBUBAAAABBoBAAAL0QUaBQEAAAA
IGgEAAAB/BRMBAAAABBoBAAAL0QUaBQEAAAAEGgEAAAvRBRsBAAAABBoBAAAL1QUDGgEAAAA
BBQQbFQMBAAAABBoBAAAL0QUaBQEAAAAEBBsDAQAAAAQaAQAAC9EFAxoBAAAABAUBAAAABB
oBAAAL2QUbAwMaAQAAAAgFBBsaBR4BAAAACAUaBBsDAQAAAAQaAQAAC9EFAwMaAQAAAAQFB
BsaBR4BAAAACAUaBB4BAAAAEAUaBAEAAAAIGgEAAAB/BRMEAQAAAAQaAQAAC9EFGgUDAQAAA
AQaAQAAC9EFGwUBAAAABwQbAgEAAAAEGgEAAAvRBQMDGgEAAAAEBQQbAwMaAQAAAAQaAQ
AAC90FGwMaAQAAAAQFBBsDGgEAAAAEGgEAAAvhBRsDGgEAAAAEBQQbAQAAAAABAAAABBoBA
AAL1QUbFQMBAAAABBoBAAAL0QUaAQAAAAQaAQAAC9kFGgEAAAAEBQcEAQAAAAQaAQAAC9kF
GgUbAwEAAAAEGgEAAAvRBRoBAAAABBoBAAAL3QUaAQAAAAQFBwQBAAAABBoBAAAL3QUaBRs
BAAAABBoBAAAL1QUaBAEAAAAEGgEAAAvhBRoFGxUBAAAABBoBAAAFagUDAQAAAEwEAQAAAAA
EAQAAAAgaAQAAATUFEwEAAAADBAEAAAAYBRsBAAAAHAEAAAAEGgEAAAvRBRsBAAAABBoBAA
AFagUDAQAAAAQaAQAAC+UFBAEAAAASBAEAAAAIGgEAABE7BRMDAQAAAAgaAQAACgEFEwMBA
AAACBoBAAAKKAUTAwEAAAAIGgEAABJGBRMDAQAAAAQaAQAAC/cFBAEAAAATBAEAAAAIGgEAA
BE7BRMDAQAAAAgaAQAACrIFEwMBAAAACBoBAAAK2QUTAwEAAAAIGgEAAAtjBRMDAQAAAAgaA
QAAEkYFEwMBAAAABBoBAAAMCgUEAQAAABQEAQAAAAgaAQAAETsFEwMBAAAACBoBAAADAQU
TAwEAAAAIGgEAAAMoBRMDAQAAAAgaAQAADX8FEwMBAAAACBoBAAANpgUTAwEAAAAIGgEAABJ
GBRMCAQAAAAQaAQAABWoFAQAAAAAVAQAAAAQaAQAABWoFAf////8VAAAMJ3BrRFMAAAAAAAA
AAAAAAADDAAAAAQAAAAQAAAC3AAAADE9ibGlnYXRpb25zAAAAAAAcAAACfAAAAAQAAAAUAAACT
AAAAAQAAADR1cm46bWFybGluOmJyb2FkYmFuZDpvYmxpZ2F0aW9uOm1ldGVyLXBsYXktZHVyYXRp
b24AAAAABwAAAE8AAAACAAAAAgAAADF1cm46bWFybGluOm9yZ2FuaXphdGlvbjpzZXJ2aWNlLXByb
3ZpZGVyLXY6bWV0ZXIAAAAAAgAAAApNMDAwMDAwMDEAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAQAAAAAAAAAAAAAAAAAE4AAAAEAAAAARgAAABRUZW
1wb3JhbENvbnN0cmFpbnRzAAAAAAcAAAAmAAAAAQAAAAQAAAAaAAAACk5vdEJlZm9yZQAAAAAD
AAAABAEQs98AAABNAAAABAAAAEUAAAAUVGVtcG9yYWxDb25zdHJhaW50cwAAAAAHAAAAJQAAA
AEAAAAEAAAAGQAAAAlOb3RBZnRlcgAAAAADAAAABAFA3d8AAACWAAAABAAAAI4AAAASRGV2aW
NlQ29uc3RyYWludHMAAAAABwAAAHAAAAACAAAABAAAAC4AAAAedXJuOm1hcmxpbjpjb3JlOnZlcnN
```

```
pb24tbWFqb3IAAAAAAAAAAAAQAAAABAAAABAAAAC4AAAAedXJuOm1hcmxpbjpjb3JlOnZlcnNpb24tbW
lub3IAAAAAAAAAAAAQAAAADAAAAlAAAAAQAAACMAAAAE0dlbmVyaWNDb25zdHJhaW50cwAAAAAH
AAAAbQAAAAEAAAAEAAAAYQAAABlOb2RlUmVhY2hhYmlsaXR5UmVxdWlyZWQAAAAAAgAAADx1cm
46bWFybGluOm9yZ2FuaXphdGlvbjpzZXJ2aWNlLXByb3ZpZGVyLXY6OHB1c3N1YjowMTAwMDAwNAAA
AACOAAAABAAAAIYAAAATR2VuZXJpY0NvbnN0cmFpbnRzAAAAAAcAAABnAAAAAQAAAAQAAABbA
AAAGU5vZGVSZWFjaGFiaWxpdHlSZXF1aXJlZAAAAAACAAAANnVybjptYXJsaW46b3JnYW5pemF0aW
9uOnNlcnZpY2UtcHJvdmlkZXItdjo4cHVzdXNlcjowAAAAAFsAAAAEAAAAUwAAABNHZW5lcmljQ29uc3Ry
YWludHMAAAAABwAAADQAAAABAAAABAAAACgAAAASTGljZW5zZVJldm9jYXRpb24AAAAAAgAAAAp
SMDAwMDAwMDEAAAAAUgAAAAQAAABKAAAAFFRlbXBvcmFsQ29uc3RyYWludHMAAAAABwAAACo
AAAABAAAABAAAAB4AAAAOTm90TG9uZ2VyVGhhbgAAAAAAAAAAAABAAAAHgAAABvAAAABAAAAGc
AAAAUVGVtcG9yYWxDb25zdHJhaW50cwAAAAAHAAAARwAAAAIAAAAEAAAAGgAAAApOb3RCZWZv
cmUAAAAAAwAAAAQAAAAAAAAAABAAAABkAAAAJTm90QWZ0ZXIAAAAAAwAAAAQAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAABTeXN0ZW0uSG9zdC5HZXRUcnVzdGVkVGltZQAAAAA
AAAAAAAAAABBdHRyaWJ1dGVzL3VybjptYXJsaW46Y29yZTp2ZXJzaW9uLW1ham9yAEF0dHJpYnV0
ZXMvdXJuOm1hcmxpbjpjb3JlOnZlcnNpb24tbWlub3IAQXR0cmlidXRlcwAvQE5hbWUAQFNpemUAICAgIC
AgICAgICAgICAgAAAAAAAgICAgIAAAAAAA/////01hcmxpbi9Bc3NlcnRpb25zAHVybjptYXJsaW46bmVtbzo
yMDA0OmF0dHJpYnV0ZTpyb2xlAHVybjptYXJsaW46Y29yZTpyb2xlOmRybS1jbGllbnQAT2N0b3B1cy5Ma
W5rcy5Jc05vZGVSZWFjaGFibGUAAAAAAHVybjptYXJsaW46b3JnYW5pemF0aW9uOnNlcnZpY2UtcHJvd
mlkZXItdjo4cHVzc3ViOjAxMDAwMDA0AHVybjptYXJsaW46b3JnYW5pemF0aW9uOnNlcnZpY2UtcHJvdml
kZXItdjo4cHVzdXNlcjowAE1hcmxpbi9MaWNlbnNlU3VzcGVuc2lvbi91cm46bWFybGluOm9yZ2FuaXphdGl
vbjpzb255OmNvbm5lY3QvSWRMaXN0L1IwMDAwMDAwMQBPY3RvcHVzL1NlYVNoZWxsL0RhdGFiYXN
lcy9NYXJsaW4vc2VydmljZS1wcm92aWRlci12L0xpY2Vuc2VTZXJ2ZXIvcGxheSBmb3IgMiBtaW51dGVzA
AAAAABPY3RvcHVzL1NlYVNoZWxsL0RhdGFiYXNlcy9NYXJsaW4vc2VydmljZS1wcm92aWRlci12L0xp
Y2Vuc2VTZXJ2ZXIvcGxheSBmb3IgMiBtaW51dGVzL0BFeHBpcmF0aW9uRGF0ZQABQN3fAAAACAAA
AAEAAAAIAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAARGV2aWNlQ29uc3RyYWludHMAR2VuZXJpY
0NvbnN0cmFpbnRzAFRlbXBvcmFsQ29uc3RyYWludHMA </CodeModule>
            </ControlProgram>
      </Control>
      <Controller Id="controller"
            uid="urn:marlin:organization:foobarv:license-service:controller-1670859984">
            <ControlReference>
                  <Uid>urn:marlin:organization:foobarv:license-service:control-997979030</Uid>
                  <Digest>
                        <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <dsig:DigestValue>qotWg.....0xFI=</dsig:DigestValue>
                  </Digest>
            </ControlReference>
            <ControlledTargets>
                  <ContentKeyReference>
                        <Uid>urn:marlin:organization:foobarv:license-service:content-key-1908710845</Uid>
                        <Digest>
                              <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                              <dsig:DigestValue>epdwj.....VeQ=</dsig:DigestValue>
                        </Digest>
                  </ContentKeyReference>
            </ControlledTargets>
      </Controller>
      <dsig:Signature Id="PKSig" xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
            <dsig:SignedInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
```

```
                <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                <dsig:Reference URI="#controller">
                    <dsig:Transforms>
                        <dsig:Transform Algorithm="http://www.octopus-drm.com/octopus/specs/cbs-1_0"/>
                    </dsig:Transforms>
                    <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <dsig:DigestValue>dVpa9.....zyP0=</dsig:DigestValue>
                </dsig:Reference>
            </dsig:SignedInfo>
            <dsig:SignatureValue>lqXSq.....XBaQ==</dsig:SignatureValue>
            <dsig:KeyInfo>
                <dsig:X509Data>
                    <dsig:X509Certificate>MIIEF.....nwE8=</dsig:X509Certificate>
                    <dsig:X509Certificate>MIID2.....iT9ai</dsig:X509Certificate>
                </dsig:X509Data>
            </dsig:KeyInfo>
        </dsig:Signature>
        <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
            <dsig:SignedInfo xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
                <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
                <dsig:Reference URI="#controller">
                    <dsig:Transforms>
                        <dsig:Transform Algorithm="http://www.octopus-drm.com/octopus/specs/cbs-1_0"/>
                    </dsig:Transforms>
                    <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <dsig:DigestValue>dVpa9f.....zyP0=</dsig:DigestValue>
                </dsig:Reference>
                <dsig:Reference URI="#PKSig">
                    <dsig:Transforms>
                        <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    </dsig:Transforms>
                    <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <dsig:DigestValue>moji4.....6Qn4=</dsig:DigestValue>
                </dsig:Reference>
            </dsig:SignedInfo>
            <dsig:SignatureValue>RK1RO.....USyP1A=</dsig:SignatureValue>
            <dsig:KeyInfo>
                <dsig:KeyName>urn:marlin:organization:foobarv:license-service:secret-key-
1908710845</dsig:KeyName>
            </dsig:KeyInfo>
        </dsig:Signature>
</Bundle>
```

B.2.4 User Link

The following is the sample User Link introduced in §5.3.1.

```
<oct:Bundle Id="publicBundle" xmlns:oct="http://www.octopus-drm.com/profiles/base/1.0">
    <oct:Link Id="link"
        uid="urn:marlin:organization:foobar:registration-service:Paa08a2U0T1193FA83267">
        <oct:AttributeList>
            <oct:Attribute name="urn:marlin:link:attribute:domain-id"
                >urn:marlin:organization:foobar:8pususer:0</oct:Attribute>
            <oct:Attribute name="urn:marlin:link:attribute:domain-policy"
                >urn:marlin:broadband:domain-policy:organization:foobar:policy:1</oct:Attribute>
        </oct:AttributeList>
        <oct:ExtensionList>
            <oct:Extension critical="false"
                uid="urn:marlin:organization:foobar:registration-
service:Paa08a2U0T1193FA83267:scuba:private">
                <oct:ScubaKeys>
                    <oct:SecretKey uid="urn:marlin:organization:foobar:8pususer:0:scuba:secret:sharing">
                        <oct:KeyData encoding="xmlenc" format="RAW">
                            <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
```

```
                                xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                <xenc:EncryptionMethod
                                    Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
                                <ds:KeyInfo>
                                    <ds:KeyName>urn:marlin:organization:testpdc:device-maker-
x:8pusperso:aa08a2:scuba:pair:sharing</ds:KeyName>
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>FTs…x8=</xenc:CipherValue>
                                </xenc:CipherData>
                            </xenc:EncryptedData>
                        </oct:KeyData>
                    </oct:SecretKey>
                    <oct:PrivateKey
pair="urn:marlin:organization:foobar:8pususer:0:scuba:KeySharing:key-pair"
uid="urn:marlin:organization:foobar:8pususer:0:scuba:private:sharing">
                        <oct:KeyData encoding="xmlenc" format="PKCS#8">
                            <xenc:EncryptedData xmlns:xenc="http://www.w3.org/2001/04/xmlenc#"
                                xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                <xenc:EncryptionMethod
                                    Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
                                <ds:KeyInfo>
                                    <xenc:EncryptedKey>
                                        <xenc:EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
                                        <ds:KeyInfo>
<ds:KeyName>urn:marlin:organization:testpdc:device-maker-
x:8pusperso:aa08a2:scuba:pair:sharing</ds:KeyName>
                                        </ds:KeyInfo>
                                        <xenc:CipherData>
                                            <xenc:CipherValue>SDPCK…..ClFZvZw=
</xenc:CipherValue>
                                        </xenc:CipherData>
                                    </xenc:EncryptedKey>
                                </ds:KeyInfo>
                                <xenc:CipherData>
                                    <xenc:CipherValue>eWMK…8vRM/c= </xenc:CipherValue>
                                </xenc:CipherData>
                            </xenc:EncryptedData>
                        </oct:KeyData>
                    </oct:PrivateKey>
                </oct:ScubaKeys>
            </oct:Extension>
        </oct:ExtensionList>
        <oct:LinkFrom>
            <oct:Uid>urn:marlin:organization:testpdc:device-maker-x:8pusperso:aa08a2</oct:Uid>
        </oct:LinkFrom>
        <oct:LinkTo>
            <oct:Uid>urn:marlin:organization:foobar:8pususer:0</oct:Uid>
        </oct:LinkTo>
        <oct:Control
            uid="urn:marlin:organization:foobar:registration-service:control:Paa83267">
            <oct:ControlProgram protocol="http://www.octopus-drm.com/specs/scp-1_0">
                <oct:CodeModule type="http://www.octopus-drm.com/specs/pkcm-
1_0">AAAMvHBrQ00AAAB3cGtFWAAAAAMdQ29udHJvbC5MaW5rLkNvbnN0cmFpbnQuSW5pdAAAAASdHkN
vbnRyb2wuTGluay5Db25zdHJhaW50LkNoZWNrAAAABKkhQ29udHJvbC5MaW5rLkNvbnN0cmFpbnQuRGVzY
3JpYmUAAAAHFgAAB9Nwa0NTAAABAAAABBoBAAAAAAUbAQAAAAQaAQAAAAQFGwMBAAAABAsBAAAA
QBgBAAAABAcBAAAABBoBAAAABAUDGgQDGgEAAAAEBQQbGgEAAAAEGgEAAAAABQMaBAMaAQAAAA
QFBBsbAf///7MWAwEAAAAACwEAAABAGQEAAAABBwEAAAAEGgEAAAAEBQMaBAMaAQAAAAEFBBscAQ
AAAAQaAQAAAAAFAxoEAxoBAAAAAQUEGx0B////sxYCFQQeAQAAAAQFGgEAAAAEBRsBAAAADAUbFQQ
BAAAAAAEAAAAIGgEAAADiBRMVHgEAAAAIBRoBAAAACBoBAAAAtgUTBAMBAAAAEBcCAwEAAAAYBQE
AAAAABBsVAQAAAAQaBQMaBAEAAAAEBR4BAAAACAUaAQAAABgFAQAAAAgaAQAAAAAFExUEAQAAA
AEBAAAACBoBAAABTwUTFR4BAAAACAUaAQAAAAgaAQAAALYFEwQDAQAAABAXAgMBAAAAGAUBAAA
AAAQbFQQDAQAAABgFAQAAAAEEGwQDGgQBAAAABAUeAQAAAAgFGgEAAAAYBQEAAAAEBQEAAAAI
GgEAAAAABRMVAwEAAAAACwEAAACdGQMBAAAABAsBAAAASBgBAAAABAcBAAAABBoBAAAAAAUbAxo
eAQAAAAgFGhoLDwEAAABzGQQBAAAABAUEAQAAAAQFAQAAAAQaAQAAAAAFGgH///+fFhUBAAAAAQcB
```

```
AAAABBoBAAAAAAUbAxweAQAAAAgFGhwLDwEAAAArGQQBAAAAAQUEAQAAAAEFAQAAAAQaAQAAAA
AFGgH///9XFhUCAgIBAAAAABUCAgH/////FQMeAQAAAAgFGhwEHAsPAQAAACUZAxwBAAAAFRkEAQAAAA
EFBAEAAAABBQH////QFhUCAgEAAAAAFQICAf////8VAQAAAAQaAQAABCoFGwEAAAAEGgEAAAQmBRoEA
QAAAAQaAQAAAyYFBAEAAAAEGgEAAAQqBRoBAAAAAyADAQAAADIYBAEAAAAEGgEAAAQuBRsEAwH///
//CwEAAAAOGQsPAQAAABMZAQAAAAAVAgIBAAAAABUEAgQCFQH////6FR4BAAAACAUaAQAAAAQaAQA
AAAAFGwEAAAAIGgEAAAKzBRMDAQAAAIgYAgEAAAAEGgEAAAAABRoBAAAABBoBAAADJgUEAwEAAAA
BCwEAAAAwGQMBAAAAAgsBAAAAMRkCAQAAAAQaAQAABC4FGgEAAAAIGgEAAAG3BRMDAQAAACUY
FQIaBBoLAw8BAAAAFxkVAgEAAAAIGgEAAAJyBRMDAQAAAAEYFQIBAAAAAAH/////FQQCAQAAAAAEFQE
AAAAEGgEAAAQqBRsB/////wQBAAAABBoBAAAEKgUaAQAAAAgaAQAAArMFEwMBAAAAARgVAQAAAAAE
AQAAAAQaAQAAApgFGgQBAAAABBoBAAACnAUaBBUBAAAACBoBAAADMgUTAwEAAAABGBUBAAAABB
oBAAACmAUaBAEAAAAEGgEAAAKcBRoEFQEAAABJBAEAAABJBAEAAAAEGgEAAAA3BQQBAAAACBoBA
AAFPAUTFQEAAAAAFQH/////FQEAAAAEGgMBAAAACAUEAQAAApgFGwEAAAAEGgMBAAADIgUEAQAAAA
EEAQAAAqAFAQAAAAABAAAACBoBAAAERAUTAQAAADEYAQAAAAQaAwEAAAQyBRoEAwEAAAQ2BRoE
AQAAAIAFAQAAAAgaAQAAAM4FEwEAAAAAFQEAAAAEGgEAAACABQEAAAAIGgEAAAE7BRMEFQEAAAA
EGgEAAAQ6BRoFAQAAAAgaAQAAAAAFEwEAAAAEGgEAAAQ6BRoFAQAAAAQaAQAABDoFGwEAAAAEG
gEAAAQ+BQMaAQAAAAEFBBsVAwEAAAAEGgEAAAQ6BRoFAQAAAAQEGwMBAAAABBoBAAAEOgUDGgE
AAAAEBQEAAAAEGgEAAARCBRsDAxoBAAAACAUEGxoFHgEAAAAIBRoEGwMBAAAABBoBAAAEOgUDAx
oBAAAABAUEGxoFHgEAAAAIBRoEHgEAAAAQBRoEAQAAAAgaAQAAAAAFEwQBAAAABBoBAAAEOgUaB
QMBAAAABBoBAAAEOgUbBQEAAAAHBBsCAQAAAAQaAQAABDoFAwMaAQAAAAQFBBsDAxoBAAAABBo
BAAAERgUbAxoBAAAABAUEGwMaAQAAAAQaAQAABEoFGwMaAQAAAAQFBBsBAAAAAAEAAAAEGgEAA
AQ+BRsVAwEAAAAEGgEAAAQ6BRoBAAAABBoBAAAEQgUaAQAAAAQFBwQBAAAABBoBAAAEQgUaBRsD
AQAAAAQaAQAABDoFGgEAAAAEGgEAAARGBRoBAAAABAUHBAEAAAAEGgEAAARGBRoFGwEAAAAEG
gEAAAQ+BRoEAQAAAAQaAQAABEoFGgUbFQEAAAAEGgEAAACABQMBAAAABAQBAAAAAAAQBAAAACBo
BAAAAtgUTAQAAAAEEAQAAABgFGwEAAAAcAQAAAAQaAQAABDoFGwEAAAAEGgEAAACABQMBAAAAB
BoBAAAETgUEAQAAABMEAQAAAAgaAQAABYkFEwMBAAAACBoBAAAEdgUTAwEAAAAIGgEAAAaUBRMC
AQAAAAQaAQAAAIAFAQAAAAAVAQAAAAQaAQAAAIAFAf////8VAAAEanBrRFMAAAAAAAAAAAAAAAAB0AAA
ABAAAAGwAAAATR2VuZXJpY0NvbnN0cmFpbnRzAAAAAAcAAABNAAAAAQAAAAQAAABBAAAADExpbmtF
bmFibGVkAAAAAAIAAAApODM3QkI2QzVBMUM2RTdCMDdBRjNBNzQzOEQwRTU1QUFBN0YyMjAxOQAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAT2N0b3B1cy9TZWFTaGV
sbC9EYXRhYmFzZXMvTWFybGluL3NlcnZpY2UtcHJvdmlkZXItdi9SZWdpc3RyYXRpb25TZXJ2ZXIvVXNlclJlZ2l
zdHJhdGlvbi84MzdCQjZDNUExQzZFN0IwN0FGM0E3NDM4RDBFNTVBQUE3RjIyMDE5AAAAAAEAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAEdlbmVyaWNDb25zdHJhaW50cwA=</oct:CodeModule>
                </oct:ControlProgram>
            </oct:Control>
        </oct:Link>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
            <ds:SignedInfo>
                <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                <ds:Reference URI="#link">
                    <ds:Transforms>
                        <ds:Transform Algorithm="http://www.octopus-drm.com/octopus/specs/cbs-1_0"/>
                    </ds:Transforms>
                    <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <ds:DigestValue>AO07fup1IkfNnKuqLqzvhFpyZLM=</ds:DigestValue>
                </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>dlZxAixioLAtK3iqJ…..tReB4xkg==</ds:SignatureValue>
            <ds:KeyInfo>
<ds:X509Data><ds:X509Certificate>MIIEJD…../YduP0ss=</ds:X509Certificate>
                    <ds:X509Certificate>MIID2j…..VgiT9ai</ds:X509Certificate>
                </ds:X509Data>
            </ds:KeyInfo>
        </ds:Signature>
</oct:Bundle>
```

B.2.5 Subscription Link

The following is the sample Subscription Link introduced in §5.3.2.

```
<oct:Bundle Id="publicBundle" xmlns:oct="http://www.octopus-drm.com/profiles/base/1.0">
        <oct:Link Id="link"
                uid="urn:marlin:organization:service-provider-v:registration-service:U0S01000004T1194E9B5060">
                <oct:LinkFrom>
                        <oct:Uid>urn:marlin:organization:service-provider-v:8pususer:0</oct:Uid>
                </oct:LinkFrom>
                <oct:LinkTo>
                        <oct:Uid>urn:marlin:organization:service-provider-v:8pussub:01000004</oct:Uid>
                </oct:LinkTo>
                <oct:Control
                        uid="urn:marlin:organization:service-provider-v:registration-
service:control:U0S01000004T1194E9B5060">
                        <oct:ControlProgram protocol="http://www.octopus-drm.com/specs/scp-1_0">
                                <oct:CodeModule type="http://www.octopus-drm.com/specs/pkcm-1_0">
AAAJwnBrQ00AAAB3cGtFWAAAAAMdQ29udHJvbC5MaW5rLkNvbnN0cmFpbnQuSW5pdAAAAALQHkNvbnRy
b2wuTGluay5Db25zdHJhaW50LkNoZWNrAAAAAu8hQ29udHJvbC5MaW5rLkNvbnN0cmFpbnQuRGVzY3JpYm
UAAAAFXQAABihwa0NTAAABAAAABBoBAAAAAAUbAQAAAAQaAQAAAAQFGwMBAAAABAsBAAAAQBgBA
AAABAcBAAAABBoBAAAABAUDGgQDGgEAAAAEBQQbGgEAAAAEGgEAAAAABQMaBAMaAQAAAAQFBBs
bAf///7MWAwEAAAAACwEAAABAGQEAAAABBwEAAAAEGgEAAAAEBQMaBAMaAQAAAAEFBBscAQAAAA
QaAQAAAAAFAxoEAxoBAAAAAQUEGx0B////sxYCFQQeAQAAAAQFGgEAAAAEBRsBAAAADAUbFQQBAAA
AAAEAAAAIGgEAAADiBRMVHgEAAAAIBRoBAAAACBoBAAAAtgUTBAMBAAAAEBcCAwEAAAAYBQEAAAA
ABBsVAQAAAAQaBQMaBAEAAAAEBR4BAAAACAUaAQAAABgFAQAAAAgaAQAAAAAFExUEAQAAAAEBA
AAACBoBAAABTwUTFR4BAAAACAUaAQAAAAgaAQAAALYFEwQDAQAAABAXAgMBAAAAGAUBAAAAAAQ
bFQQDAQAAABgFAQAAAAEEGwQDGgQBAAAABAUeAQAAAAgFGgEAAAAYBQEAAAAEBQEAAAAIGgEAA
AAABRMVAQAAAAQaAQAAAt4FGg8DAQAAACEZAgEAAAAEGgEAAALDBQEAAAACIAMBAAAABBoBAAAC
3gUbFQEAAAAEGgEAAALeBRogBAIDAQAAAA4YCwEAAAAbFwIBAAAAABUEAgIBAAAAAAQBAAAACAH/////
FQEAAAAABAEAAAAIAf////8VAQAAAAQaAQAAAt4FGiAEAgMBAAAADhgLAQAAABsYAgEAAAAAFQQCAgE
AAAAABAEAAAAIAf////8VAQAAAAAEAQAAAAgB/////xUBAAAAIgQBAAAAIgQBAAAABBoBAAAAOAUEAQAAA
AgaAQAAA4MFExUBAAAAIQQBAAAAIQQBAAAABBoBAAAAigUEAQAAAAgaAQAAA4MFExUBAAAACBoBA
AABtwUTAQAAAAYYAQAAAAAVAf////8VAQAAAAQaAQAAAAgFAQExTMwBAAAACBoBAAAB7gUTAQAAAFU
YAQAAAAQaAQAAAFoFAQExdCwBAAAACBoBAAACOAUTAQAAADEYAQAAAAQaAwEAAALiBRoEAwEAAA
LmBRoEAQAAAKsFAQAAAAgaAQAAAM4FEwEAAAAAFQEAAAAEGgEAAACrBQEAAAAIGgEAAAE7BRMEF
QEAAAAEGgEAAALqBRoFAQAAAAgaAQAAAAAFEwEAAAAEGgEAAALqBRoFAQAAAAQaAQAAAuoFGwEA
AAAEGgEAAALuBQMaAQAAAAEFBBsVAwEAAAAEGgEAAALqBRoFAQAAAAQEGwMBAAAABBoBAAAC6g
UDGgEAAAAEBQEAAAAEGgEAAALyBRsDAxoBAAAACAUEGxoFHgEAAAAIBRoEGwMBAAAABBoBAAAC6g
UDAxoBAAAABAUEGxoFHgEAAAAIBRoEHgEAAAAQBRoEAQAAAAgaAQAAAAAFEwQBAAAABBoBAAAC6g
UaBQMBAAAABBoBAAAC6gUbBQEAAAAHBBsCAQAAAAQaAQAAAuoFAwMaAQAAAAQFBBsDAxoBAAAAB
BoBAAAC9gUbAxoBAAAABAUEGwMaAQAAAAQaAQAAAvoFGwMaAQAAAAQFBBsBAAAAAAEAAAAEGgEA
AALuBRsVAwEAAAAEGgEAAALqBRoBAAAABBoBAAAC8gUaAQAAAAQFBwQBAAAABBoBAAAC8gUaBRsD
AQAAAAQaAQAAAuoFGgEAAAAEGgEAAAL2BRoBAAAABAUHBAEAAAAEGgEAAAL2BRoFGwEAAAAEGgE
AAALuBRoEAQAAAAQaAQAAAvoFGgUbFQEAAAAEGgEAAACrBQMBAAAACAQBAAAAAAQBAAAACBoBAA
AAtgUTAQAAAAEEAQAAABgFGwEAAAAcAQAAAAQaAQAAAuoFGwEAAAAEGgEAAACrBQMBAAAABBoBA
AAC/gUEAQAAABQEAQAAAAgaAQAAA9AFEwMBAAAACBoBAAACggUTAwEAAAAIGgEAAAKpBRMDAQAA
AAgaAQAABNsFEwIBAAAABBoBAAAAqwUBAAAAABUBAAAABBoBAAAAqwUB/////xUAAAMbcGtEUwAAAAA
AAAAAAAAAAE4AAAAEAAAARgAAABRUZW1wb3JhbENvbnN0cmFpbnRzAAAAAAcAAAAmAAAAAQAAAAQ
AAAAaAAAACk5vdEJlZm9yZQAAAAADAAAABAExTMwAAABNAAAABAAAAEUAAAAUVGVtcG9yYWxDb25zd
HJhaW50cwAAAAAHAAAAJQAAAAEAAAAEAAAAGQAAAAlOb3RBZnRlcgAAAAADAAAABAExdCwAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAFN5c3RlbS5Ib3N0LkdldFRydXN0ZWRUaW1lAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAVGVtcG9yYWxDb25zdHJhaW50cwA=
                </oct:CodeModule>
            </oct:ControlProgram>
        </oct:Control>
    </oct:Link>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:SignedInfo>
            <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
            <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <ds:Reference URI="#link">
                <ds:Transforms>
                    <ds:Transform Algorithm="http://www.octopus-drm.com/octopus/specs/cbs-1_0"/>
                </ds:Transforms>
                <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <ds:DigestValue>Xh2z83mHg/vGYna6FXF/lRocF2s=</ds:DigestValue>
            </ds:Reference>
        </ds:SignedInfo>
        <ds:SignatureValue>Wqb/s37…SrNiQ==</ds:SignatureValue>
        <ds:KeyInfo>
            <ds:X509Data>
                <ds:X509Certificate>MIIEJDC…P0ss=</ds:X509Certificate>
                <ds:X509Certificate>MIID2…giT9ai</ds:X509Certificate>
            </ds:X509Data>
        </ds:KeyInfo>
    </ds:Signature>
</oct:Bundle>
```