

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

Marlin – Profile and Capability Signaling

Version 1.0
Final

Source	Marlin Engineering Workgroup
Date	July 18, 2008

32 **Notice**

33 THIS DOCUMENT IS PROVIDED "AS IS" WITH NO REPRESENTATION OR
34 WARRANTY, EXPRESS OR IMPLIED, CONCERNING THE COMPLETENESS,
35 ACCURACY, OR APPLICABILITY OF ANY INFORMATION CONTAINED IN
36 THIS DOCUMENT. THE MARLIN DEVELOPER COMMUNITY ("MDC") ON
37 BEHALF OF ITSELF AND ITS PARTICIPANTS (COLLECTIVELY, THE
38 "PARTIES") DISCLAIM ALL LIABILITY OF ANY KIND WHATSOEVER,
39 EXPRESS OR IMPLIED, ARISING OR RESULTING FROM THE RELIANCE OR
40 USE BY ANY PARTY OF THIS DOCUMENT OR ANY INFORMATION
41 CONTAINED HEREIN. THE PARTIES COLLECTIVELY AND INDIVIDUALLY
42 MAKE NO REPRESENTATIONS CONCERNING THE APPLICABILITY OF ANY
43 PATENT, COPYRIGHT (OTHER THAN THE COPYRIGHT TO THE
44 DOCUMENT DESCRIBED BELOW) OR OTHER PROPRIETARY RIGHT OF
45 THIS DOCUMENT OR ITS USE, AND THE RECEIPT OR ANY USE OF THIS
46 DOCUMENT OR ITS CONTENTS DOES NOT IN ANY WAY CREATE BY
47 IMPLICATION, ESTOPPEL OR OTHERWISE, ANY LICENSE OR RIGHT TO
48 OR UNDER ANY PATENT, COPYRIGHT, TRADEMARK OR TRADE SECRET
49 RIGHTS WHICH ARE OR MAY BE ASSOCIATED WITH THE IDEAS,
50 TECHNIQUES, CONCEPTS OR EXPRESSIONS CONTAINED HEREIN.

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

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

54 Copyright © 2003 - 2009 by MDC, 415-112 North Mary Avenue #383 Sunnyvale, CA
55 94085, USA. All rights reserved. Third-party brands and names are the property of
56 their respective owners.

57 **Intellectual Property**

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

60 **Contact Information**

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

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

64
65

Contents

66	1	Introduction.....	4
67	1.1	Document Organization.....	4
68	1.2	Conformance Conventions.....	4
69	1.3	Namespaces and Identifiers.....	4
70	1.3.1	Namespaces and Notation.....	4
71	1.4	References.....	5
72	1.4.1	Normative References.....	5
73	2	Marlin Profile and Capability Signaling.....	6
74	2.1	Attribute Names and Value-space (Informative).....	6
75	2.2	Scope and Qualification of Attributes.....	6
76	2.2.1	profile Attribute Name.....	6
77	2.3	profile Qualified Attributes.....	6
78	2.3.1	topology Attribute Name.....	7
79	2.3.2	protocols Attribute Name.....	7
80	2.3.3	features Attribute Name.....	7
81	3	Signaling with SAML Attributes.....	8
82	3.1	SAML Assertion Profile.....	8
83	3.1.1	Assertion Composition.....	8
84	3.1.2	AttributeStatement Composition.....	8
85	3.1.3	Subject Identification.....	8
86	3.1.4	Attribute Naming.....	8
87	3.1.5	Attribute Values.....	9
88	3.1.6	Assertion Signature.....	9
89	4	NEMO Basic Secure Message Binding.....	10
90	5	SAML Profile and Capability Example (Informative).....	11
91	5.1	Signaling Mandatory and Optional Features.....	11

92 1 Introduction

93 This document describes a mechanism by which a Marlin client implementation can
94 signal to a Marlin service the set of mandatory functions and optional features supported
95 by the Marlin client implementation.

96 1.1 Document Organization

97 This document is organized as follows:

- 98 • Introduction and conventions
- 99 • Attribute definitions
- 100 • Signaling profile and binding

101 1.2 Conformance Conventions

102 The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”,
103 “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this
104 specification are to be interpreted as described in IETF RFC 2119 [RFC2119].
105

106 These capitalized key words are used to unambiguously specify requirements and
107 behavior that affect the interoperability and security of implementations. When these key
108 words are not capitalized they are meant in their natural-language sense.
109

110 All elements of this specification are considered Normative unless specifically marked
111 Informative. All Normative Elements are Mandatory to implement, except where such an
112 element is specifically marked OPTIONAL. Finally, where Normative elements are
113 described as OPTIONAL, they MAY be omitted from an implementation, but when
114 implemented, they MUST be implemented as described.

115 1.3 Namespaces and Identifiers

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

122 1.3.1 Namespaces and Notation

123 The table below summarizes the normative schemas defined by this specification, and
124 their XML namespace [XMLns] URIs. These URIs MUST be used by implementations of
125 this specification.
126

Prefix	XML Namespace
pacs:	urn:marlin:pacs

Table 1: Normative Namespaces

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

128

Prefix	XML Namespace	Description
xsd:	http://www.w3.org/2001/XMLSchema	[Schema]

Prefix	XML Namespace	Description
xsi:	http://www.w3.org/2001/XMLSchema-instance	[Schema]
saml	urn:oasis:names:tc:SAML:1.0:assertion	[SAML1.1]
S11:	http://schemas.xmlsoap.org/soap/envelope	[SOAP11]

Table 2: Supporting Namespaces

129

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

134 1.4 References

135 1.4.1 Normative References

136

[MIAR]	Marlin Identifier and Attribute Registry (TBD)
[MBB]	Marlin Engineering Work Group, Marlin Broadband Delivery System Specification, version 1.2 and latest errata
[MCS]	Marlin Engineering Work Group, Marlin – Core System Specification, version 1.3 and latest errata
[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
[SAML1.1]	Eve Maler, Prateek Mishra and Rob Philpott, eds., <i>Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1</i> , http://www.oasis-open.org/committees/download.php/3405/oasis-sstc-saml-bindings-1.1.pdf
[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/ XML Schema Part 2: Datatypes W3C Recommendation. P. Biron, A. Malhotra. May 2001. http://www.w3.org/TR/2001/REC-xmlschema-2-20010502/
[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-SECSAML]	Phillip Hallam-Baker <i>et al.</i> , eds., <i>Web Services Security: SAML Token Profile</i> , OASIS Standard, December 2004, http://docs.oasis-open.org/wss/oasis-wss-saml-token-profile-1.0.pdf

137 2 Marlin Profile and Capability Signaling

138 This specification defines a general framework to provide Marlin client implementations
139 with a mechanism to communicate support for optional functionality. The general notion
140 is to be able to signal to a relying party the set of well-known Marlin profiles (mandatory
141 functions) and optional features that the Marlin client implementation supports.

142
143 This framework is designed to support a case where a Marlin client implementation
144 supports more than one Marlin profile. A Marlin client that implements more than one
145 profile implies the Marlin client implements optional features in one profile that may be
146 mandatory in the other. In this case, it is RECOMMENDED that Marlin client
147 implementations signal the optional features for the less feature-rich profiles.

148
149 The framework is designed to be extensible. To this end, signaled identifiers are
150 registered in [MIAR] §2.7 along with a normative reference to the implemented
151 functionality indicated by the signal.

152 2.1 Attribute Names and Value-space (Informative)

153 A normative list of identifiers and attributes is maintained in [MIAR]. Table 3 exemplifies
154 the attribute name identifiers and the values that can be signaled by this framework.

155

Attribute Name	Attribute Value-space
profile	Profile defined URI
topology	urn:marlin:bb:1-2:topology:any
protocols	urn:marlin:bb:1-2:dcs urn:marlin:bb:1-2:dus urn:marlin:mcs:1-3:licensefer
features	urn:marlin:dmz:1-0

Table 3. Example of attribute value

156 2.2 Scope and Qualification of Attributes

157 The utility of the signaling mechanism is twofold. First, it enables a Marlin client
158 implementation to unambiguously indicate the basic set of functionality it implements.
159 This is accomplished by signaling a profile attribute as defined in §2.2.1. Secondly, this
160 mechanism enables a Marlin client to indicate the optional features, qualified by the
161 profile, that the Marlin client also implements. These profile qualified attributes are
162 defined in §2.3.

163 2.2.1 profile Attribute Name

164 When signaling, the client is REQUIRED to supply the profile attribute. That is, all
165 Implementations of Marlin profiles MUST signal this attribute using a profile specific URI.

166 2.3 profile Qualified Attributes

167 Attributes are scoped by the Marlin profile attribute defined in §2.2.1. One or more
168 attributes defined in this section MAY be signalled along with the MANDATORY profile
169 attribute. Signaling attributes in this manner indicates to the relying party the optional

170 features implemented by the Marlin client. A Marlin client MUST NOT signal attributes
171 deemed mandatory by the designated Marlin profile.

172 **2.3.1 topology Attribute Name**

173 Services represent the supported business models by implementing an Octopus
174 Node/Link topology. Marlin delivery system specifications define services (e.g.,
175 Registration Service) that, through DRM Client interactions, issue Octopus Nodes and
176 Links that formulate this topology. DRM Clients implementing a particular delivery
177 system specification are required to support the prescribed topology. However, Octopus
178 Nodes and Links are generic technologies, when implemented accordingly, enable
179 services and clients to formulate and support other node/link topologies beyond the
180 mandatory ones defined by the delivery system specification. This attribute is used to
181 signal this DRM Client capability.

182
183 The topology attribute signals that the DRM Client implementation is capable of
184 supporting optional node/link topologies that can be formulated with the Octopus Node
185 types the delivery system specification supports. A DRM Client that asserts this
186 capability indicates that the implementation conforms to all the mandatory protocol and
187 processing requirements to support the optional topologies. That is, the DRM Client will:

- 188 • Conform to the requirements of Octopus Node and Link acquisition protocols,
189 including Agent processing, as well as other Octopus Node and Link related
190 protocols defined by the delivery system. For example, the license acquisition
191 protocols (i.e., binding a license to an Octopus Node) or the deregistration
192 protocol (i.e., termination of the link relationship between two Octopus Nodes).
- 193 • Enforce link constraints (i.e., securely execute control programs).
- 194 • Process and derive Scuba keys distributed within the Octopus Link Objects.

195
196 The value-space of the topology identifier MUST be a URI and it is RECOMMENDED
197 that it include delivery system specification version information (e.g.,
198 urn:marlin:broadband:1-2:topology:any). This allows for future enhancements to the
199 node/link topology prescribed by the delivery system specification.

200 **2.3.2 protocols Attribute Name**

201 This attribute signals a Marlin client implementation supports the designated
202 communication protocol.

203 **2.3.3 features Attribute Name**

204 This attribute signals the optional features supported by a Marlin client implementation.

205 **3 Signaling with SAML Attributes**

206 Various Marlin specifications utilize SAML Assertions to convey trusted attributes about
207 a system entity (typically a Nemo node). However the lifecycle and security properties of
208 these assertions greatly differ from the requirements of the attributes signaled with this
209 framework. Specifically the lifecycle of, and the type of information signaled with this
210 framework are generally bound to the lifecycle of a client implementation, not its security
211 posture. Therefore, this SAML Assertion Profile is defined here to support the different
212 lifecycle requirements.

213
214 The following SAML Assertion Profile defines the mechanism by which a Marlin client
215 implementation **MUST** convey the attributes defined in §2. That is, a qualified profile and
216 any optional features the implementation supports beyond what is mandated by the
217 qualified profile.

218 **3.1 SAML Assertion Profile**

219 **3.1.1 Assertion Composition**

220 The <saml:Assertion> **MUST** contain a <saml:AttributeStatement> element for each
221 supported Marlin Profile.

222 **3.1.2 AttributeStatement Composition**

223 The <saml:AttributeStatement> **MUST** contain a single <saml:Subject> element and one
224 or more <saml:Attribute> elements.

225
226 An <saml:AttributeStatement> **MUST** have one or more <saml:Attribute> elements. In
227 the set of <saml:Attribute> elements one **MUST** signal the profile attribute. This profile
228 attribute qualifies the remaining <saml:Attribute> elements within the
229 <saml:AttributeStatement>.

230
231 If a Marlin client supports more than one profile then it **MUST** communicate this fact in a
232 separate <saml:AttributeStatement> elements.

233 **3.1.3 Subject Identification**

234 The <saml:Subject> element **MUST** contain a single <saml:NameIdentifier> element to
235 identify the entity for which attributes apply. The Format XML attribute of the
236 <saml:NameIdentifier> element **SHOULD** be;

237
238 **http://nemo.intertrust.com/2004/saml/name-format/uri**

239
240 The value of the <saml:NameIdentifier> element **MUST** be a URI. This URI **SHOULD** be
241 managed under the “urn:marlin:organization” namespace. The <saml:NameIdentifier>
242 **SHOULD** reflect the same identity as the subject of the client’s NEMO Client Keys.

243 **3.1.4 Attribute Naming**

244 For this assertion profile, the AttributeNamespace XML attribute in all <saml:Attribute>
245 elements **MUST** be;

246 **urn:marlin:pacs**

247

248 The AttributeName XML attribute in the <saml:Attribute> elements MUST be one of the
249 attribute names defined in §2.

250 **3.1.5 Attribute Values**

251 The schema type of the contents of the <saml:AttributeValue> element MUST be
252 indicated with the xsi:type attribute. All attribute values MUST be represented as
253 xsd:string. Multiple values for an attribute MUST be represented with multiple
254 <saml:AttributeValue> elements. An example follows:

255

```
256 <Attribute AttributeNamespace="urn:marlin:pacs"  
257     AttributeName="protocols">  
258     <AttributeValue xsi:type="xsd:string">urn:marlin:bb:1-2:dcs  
259     </AttributeValue>  
260     <AttributeValue xsi:type="xsd:string">urn:marlin:bb:1-2:dus  
261     </AttributeValue>  
262 </Attribute>
```

263

264 The value space of the <saml:AttributeValue> element SHOULD be one or more of the
265 attribute values defined [MIAR].

266 **3.1.6 Assertion Signature**

267 The <saml:Assertion> MAY be independently signed. When signed, the guidance given
268 in [MCS] §12.2 and [SAML1.1] §5 SHALL be followed.

269

270 If signed, the signer of the assertion MAY be either the authority that signs the
271 DRM Client Role Attribute Assertion [MCS] or the DRM Client with its NEMO Client
272 Signing Key.

273 **4 NEMO Basic Secure Message Binding**

274 These attribute assertions SHOULD be conveyed in the Request Message of each
275 NEMO Basic Secure Message exchange.

276
277 The assertion SHALL be placed as a direct child element of a <wsse:Security> element,
278 and SHALL be referenced from a <wsse:KeyIdentifier> element in a
279 <wsse:SecurityTokenReference> element, as specified in [WS-SECSAML] §3.3.

280
281 The <wsse:SecurityTokenReference> element that references these SAML attribute
282 assertions SHALL contain a nemosec:Usage attribute with the following value:

283

urn:marlin:pacs:1.0:profile-capability-attributes:assertion

284

285 5 SAML Profile and Capability Example (Informative)

286 5.1 Signaling Mandatory and Optional Features

```
287 <Assertion xmlns="urn:oasis:names:tc:SAML:1.0:assertion"
288     xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
289     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
290     AssertionID="AQAjCGN1" IssueInstant="2007-06-19T18:36:47.942Z"
291     Issuer=" urn:marlin:organization:phony:model"
292     MajorVersion="1" MinorVersion="1">
293   <AttributeStatement>
294     <Subject>
295       <NameIdentifier
296         Format=" http://nemo.intertrust.com/2004/saml/name-format/uri">
297         urn:marlin:organization:phony:model:pd-x1:firmware:v1.0
298       </NameIdentifier>
299     </Subject>
300     <!-- The MANDATORY profile attribute -->
301     <Attribute AttributeNamespace="urn:marlin:pacs"
302       AttributeName="profile">
303       <AttributeValue xsi:type="xsd:string">
304         urn:marlin:profile:jimmyjet:1-0
305       </AttributeValue>
306     </Attribute>
307     <!-- Signal additional protocols implemented by the client -->
308     <Attribute AttributeNamespace="urn:marlin:pacs"
309       AttributeName="protocols">
310       <AttributeValue xsi:type="xsd:string">urn:marlin:bb:1-2:dcs
311     </AttributeValue>
312       <AttributeValue xsi:type="xsd:string">urn:marlin:bb:1-2:dus
313     </AttributeValue>
314     </Attribute>
315     <!-- Signal implementation can understand any nodes types -->
316     <Attribute AttributeNamespace="urn:marlin:pacs"
317       AttributeName="topology">
318       <AttributeValue xsi:type="xsd:string">
319         urn:marlin:broadband:1-2:any
320       </AttributeValue>
321     </Attribute>
322   </AttributeStatement>
323 </Assertion>
324
325
```