



# SAML V2.0 Information Card Token Profile Version 1.0

## Committee Specification 01

21 July 2010

### Specification URIs:

#### This Version:

<http://docs.oasis-open.org/imi/identity/cs/imi-saml2.0-profile-cs-01.html>  
<http://docs.oasis-open.org/imi/identity/cs/imi-saml2.0-profile-cs-01.doc> (Authoritative)  
<http://docs.oasis-open.org/imi/identity/cs/imi-saml2.0-profile-cs-01.pdf>

#### Previous Version:

<http://docs.oasis-open.org/imi/identity/cd/imi-saml2.0-profile-cd-03.html>  
<http://docs.oasis-open.org/imi/identity/cd/imi-saml2.0-profile-cd-03.doc> (Authoritative)  
<http://docs.oasis-open.org/imi/identity/cd/imi-saml2.0-profile-cd-03.pdf>

#### Latest Version:

<http://docs.oasis-open.org/imi/identity/imi-saml2.0-profile.html>  
<http://docs.oasis-open.org/imi/identity/imi-saml2.0-profile.doc> (Authoritative)  
<http://docs.oasis-open.org/imi/identity/imi-saml2.0-profile.pdf>

### Technical Committee:

OASIS Identity Metasystem Interoperability (IMI) TC

### Chair(s):

Marc Goodner, Microsoft Corporation  
Anthony Nadalin, Microsoft Corporation

### Editor(s):

Scott Cantor, Internet2  
Michael B. Jones, Microsoft Corporation

### Related work:

This specification replaces or supersedes:

- None

This specification is related to:

- OASIS Standard, "Identity Metasystem Interoperability Version 1.0", July 2009.  
<http://docs.oasis-open.org/imi/identity/v1.0/identity.pdf>
- OASIS Standard, "Security Assertion Markup Language (SAML) V2.0", March 2005.  
<http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- OASIS Committee Draft, "SAML V1.1 Information Card Token Profile Version 1.0", July 2010. <http://docs.oasis-open.org/imi/identity/cd/imi-saml1.1-profile-cd-02.pdf>

### Declared XML Namespace(s):

<http://docs.oasis-open.org/imi/ns/token/saml2/200908>

### Abstract:

This profile describes a set of rules for Identity Providers and Relying Parties to follow when using SAML V2.0 assertions as managed Information Card security tokens, so that interoperability and security is achieved commensurate with other SAML authentication profiles.

**Status:**

This document was last revised or approved by the Identity Metasystem Interoperability TC on the above date. The level of approval is also listed above. Check the “Latest Version” or “Latest Approved Version” location noted above for possible later revisions of this document.

Technical Committee members should send comments on this specification to the Technical Committee’s email list. Others should send comments to the Technical Committee by using the “Send a Comment” button on the Technical Committee’s web page at <http://www.oasis-open.org/committees/imi/>.

For information on whether any patents have been disclosed that may be essential to implementing this specification, and any offers of patent licensing terms, please refer to the Intellectual Property Rights section of the Technical Committee web page (<http://www.oasis-open.org/committees/imi/ipr.php>).

The non-normative errata page for this specification is located at <http://www.oasis-open.org/committees/imi/>.

---

## Notices

Copyright © OASIS® 2010. All Rights Reserved.

All capitalized terms in the following text have the meanings assigned to them in the OASIS Intellectual Property Rights Policy (the "OASIS IPR Policy"). The full Policy may be found at the OASIS website.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to OASIS, except as needed for the purpose of developing any document or deliverable produced by an OASIS Technical Committee (in which case the rules applicable to copyrights, as set forth in the OASIS IPR Policy, must be followed) or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by OASIS or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and OASIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY OWNERSHIP RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

OASIS requests that any OASIS Party or any other party that believes it has patent claims that would necessarily be infringed by implementations of this OASIS Committee Specification or OASIS Standard, to notify OASIS TC Administrator and provide an indication of its willingness to grant patent licenses to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification.

OASIS invites any party to contact the OASIS TC Administrator if it is aware of a claim of ownership of any patent claims that would necessarily be infringed by implementations of this specification by a patent holder that is not willing to provide a license to such patent claims in a manner consistent with the IPR Mode of the OASIS Technical Committee that produced this specification. OASIS may include such claims on its website, but disclaims any obligation to do so.

OASIS takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; neither does it represent that it has made any effort to identify any such rights. Information on OASIS' procedures with respect to rights in any document or deliverable produced by an OASIS Technical Committee can be found on the OASIS website. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this OASIS Committee Specification or OASIS Standard, can be obtained from the OASIS TC Administrator. OASIS makes no representation that any information or list of intellectual property rights will at any time be complete, or that any claims in such list are, in fact, Essential Claims.

The name "OASIS" is a trademark of OASIS, the owner and developer of this specification, and should be used only to refer to the organization and its official outputs. OASIS welcomes reference to, and implementation and use of, specifications, while reserving the right to enforce its marks against misleading uses. Please see <http://www.oasis-open.org/who/trademark.php> for above guidance.

---

# Table of Contents

|       |  |    |
|-------|--|----|
| 1     | Introduction .....                             | 5  |
| 1.1   | Notational Conventions .....                   | 5  |
| 1.2   | Namespaces.....                                | 6  |
| 1.3   | Normative References.....                      | 6  |
| 1.4   | Non-Normative References .....                 | 7  |
| 2     | SAML V2.0 Information Card Token Profile ..... | 8  |
| 2.1   | Required Information .....                     | 8  |
| 2.2   | Profile Overview .....                         | 8  |
| 2.3   | Identity Provider Requirements .....           | 8  |
| 2.3.1 | Token Types.....                               | 8  |
| 2.3.2 | Identifying Token Issuers .....                | 8  |
| 2.3.3 | General Assertion Requirements .....           | 9  |
| 2.3.4 | Proof Keys and Subject Confirmation .....      | 9  |
| 2.3.5 | Conditions .....                               | 10 |
| 2.3.6 | Encryption .....                               | 10 |
| 2.4   | Relying Party Requirements.....                | 10 |
| 2.4.1 | Token Types.....                               | 10 |
| 2.4.2 | Identifying Token Issuers .....                | 10 |
| 2.4.3 | Identifying Relying Parties.....               | 10 |
| 2.4.4 | Identifying Claim Types .....                  | 11 |
| 2.4.5 | Assertion Validity.....                        | 11 |
| 2.5   | Use of SAML Metadata .....                     | 11 |
| 2.6   | Security Considerations.....                   | 12 |
| 2.6.1 | Unconstrained Bearer Assertions.....           | 12 |
| 2.6.2 | Encryption .....                               | 12 |
| 2.7   | Examples.....                                  | 12 |
| 2.7.1 | Two Required Claims .....                      | 12 |
| 2.7.2 | One Required Claim, as Federated NameID.....   | 13 |
| 3     | Conformance.....                               | 15 |
| A.    | Acknowledgements .....                         | 16 |
| B.    | Revision History .....                         | 17 |

---

# 1 Introduction

OASIS has standardized a set of profiles for acquiring and delivering security tokens, collectively referred to as "Information Card" technology. These profiles are agnostic with respect to the format and semantics of a security token, but interoperability between Issuing and Relying Parties cannot be achieved without additional rules governing the creation and use of the tokens exchanged. This document describes a set of rules for the use of SAML V2.0 assertions, as defined in [SAML2Core], as security tokens within the Information Card architecture.

## 1.1 Notational Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119].

This specification uses the following syntax to define outlines for assertions:

- The syntax appears as an XML instance, but values in italics indicate data types instead of literal values.
- Characters are appended to elements and attributes to indicate cardinality:
  - "?" (0 or 1)
  - "\*" (0 or more)
  - "+" (1 or more)
- The character "|" is used to indicate a choice between alternatives.
- The characters "(" and ")" are used to indicate that contained items are to be treated as a group with respect to cardinality or choice.
- The characters "[" and "]" are used to call out references and property names.
- Ellipses (i.e., "...") indicate points of extensibility. Additional children and/or attributes MAY be added at the indicated extension points but MUST NOT contradict the semantics of the parent and/or owner, respectively. By default, if a receiver does not recognize an extension, the receiver SHOULD ignore the extension; exceptions to this processing rule, if any, are clearly indicated below.
- XML namespace prefixes (see Section 1.2) are used to indicate the namespace of the element being defined.

Elements and Attributes defined by this specification are referred to in the text of this document using XPath 1.0 expressions. Extensibility points are referred to using an extended version of this syntax:

- An element extensibility point is referred to using {any} in place of the element name. This indicates that any element name can be used, from any namespace other than the namespace of this specification.
- An attribute extensibility point is referred to using @{any} in place of the attribute name. This indicates that any attribute name can be used, from any namespace other than the namespace of this specification.

Extensibility points in the exemplar may not be described in the corresponding text.

This specification uses the following typographical conventions in text: <SAML*Element*>, <ns:ForeignElement>, Attribute, **Datatype**, OtherCode.

41 **1.2 Namespaces**

42 Conventional XML namespace prefixes are used throughout the listings in this specification to stand for  
 43 their respective namespaces as follows, whether or not a namespace declaration is present in the  
 44 example:

| <b>Prefix</b> | <b>XML Namespace</b>   | <b>Comments</b>  |
|---------------|--|--|
| saml :        | urn:oasis:names:tc:SAML:2.0:assertion  | This is the SAML V2.0 assertion namespace defined in the SAML V2.0 core specification [SAML2Core].   |
| md :          | urn:oasis:names:tc:SAML:2.0:metadata   | This is the SAML V2.0 metadata namespace defined in the SAML V2.0 metadata specification [SAML2Meta].  |
| ic :          | http://schemas.xmlsoap.org/ws/2005/05/identity   | This is the Information Card namespace defined in the Identity Metasystem Interoperability standard [IMI].   |
| wsa :         | http://www.w3.org/2005/08/addressing   | This is the WS-Addressing namespace defined in the WS-Addressing specification [WS-Addressing].  |
| wsp :         | http://schemas.xmlsoap.org/ws/2004/09/policy   | This is the WS-Policy namespace defined in the March 2006 WS-Policy specification [WS-Policy].   |
| sp :          | <i>May refer to either<br/> <a href="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy">http://schemas.xmlsoap.org/ws/2005/07/securitypolicy</a><br/>           or <a href="http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702">http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702</a> since both may be used</i>   | This is either the WS-SecurityPolicy namespace defined by the WS-SecurityPolicy 1.1 specification [WS-SecPol11] or the OASIS WS-SecurityPolicy 1.2 specification [WS-SecPol12].                      |
| wst :         | <i>May refer to any of<br/> <a href="http://schemas.xmlsoap.org/ws/2005/02/trust">http://schemas.xmlsoap.org/ws/2005/02/trust</a>,<br/> <a href="http://docs.oasis-open.org/ws-sx/ws-trust/200512">http://docs.oasis-open.org/ws-sx/ws-trust/200512</a>, or<br/> <a href="http://docs.oasis-open.org/ws-sx/ws-trust/200802">http://docs.oasis-open.org/ws-sx/ws-trust/200802</a>,<br/>           since all may be used</i> | This is one the WS-Trust namespaces defined in the February 2005 WS-Trust specification [WS-Trust12], the OASIS WS-Trust 1.3 standard [WS-Trust13], or the OASIS WS-Trust 1.4 standard [WS-Trust14]. |
| ds :          | http://www.w3.org/2000/09/xmldsig#   | This is the XML Signature namespace [XMLSig].  |

45 **1.3 Normative References**

46 **[IMI]** OASIS Standard, “Identity Metasystem Interoperability V1.0”, July 2009.  
 47 <http://docs.oasis-open.org/imi/identity/v1.0/os/identity-1.0-spec-os.pdf>

48 **[RFC2119]** S. Bradner. “Key words for use in RFCs to Indicate Requirement Levels”. IETF  
 49 RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.

50 **[SAML2Core]** OASIS Standard, “Assertions and Protocols for the OASIS Security Assertion  
 51 Markup Language (SAML) V2.0”, March 2005. [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)  
 52 [open.org/security/saml/v2.0/saml-core-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf)

53 **[SAML2Meta]** OASIS Standard, “Metadata for the OASIS Security Assertion Markup Language  
 54 (SAML) V2.0”, March 2005. [http://docs.oasis-open.org/security/saml/v2.0/saml-](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)  
 55 [metadata-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf)

56       **[SAML2Prof]**       OASIS Standard, “Profiles for the OASIS Security Assertion Markup Language  
57       (SAML) V2.0”, March 2005. [http://docs.oasis-open.org/security/saml/v2.0/saml-  
58       profiles-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)

59       **[WS-Addressing]**   M. Gudgin et al. “WS-Addressing 1.0 Core”. World Wide Web Consortium  
60       Recommendation, May 2006. [http://www.w3.org/TR/2006/REC-ws-addr-core-  
61       20060509/](http://www.w3.org/TR/2006/REC-ws-addr-core-20060509/)

62       **[WS-Policy]**       “Web Services Policy Framework, Version 1.2”, March 2006.  
63       <http://specs.xmlsoap.org/ws/2004/09/policy/ws-policy.pdf>

64       **[WS-SecPol11]**     “Web Services Security Policy Language”, July 2005.  
65       <http://specs.xmlsoap.org/ws/2005/07/securitypolicy/ws-securitypolicy.pdf>

66       **[WS-SecPol12]**     OASIS Standard, “WS-SecurityPolicy 1.2”, July 2007. [http://docs.oasis-  
67       open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.pdf](http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.pdf)

68       **[WS-Trust12]**     “Web Services Trust Language (WS-Trust)”, February 2005.  
69       <http://specs.xmlsoap.org/ws/2005/02/trust/WS-Trust.pdf>

70       **[WS-Trust13]**     OASIS Standard, “WS-Trust 1.3”, March 2007. [http://docs.oasis-open.org/ws-  
71       sx/ws-trust/200512/ws-trust-1.3-os.pdf](http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf)

72       **[WS-Trust14]**     OASIS Standard, “WS-Trust 1.4”, February 2009. [http://docs.oasis-open.org/ws-  
73       sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.pdf](http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.pdf)

74       **[XMLSig]**         D. Eastlake et al. “XML-Signature Syntax and Processing, Second Edition”.  
75       World Wide Web Consortium Recommendation, June 2008.  
76       <http://www.w3.org/TR/xmldsig-core/>

## 77       **1.4 Non-Normative References**

78       **[SAML2Sec]**       OASIS Standard, “Security Considerations for the OASIS Security Assertion  
79       Markup Language (SAML) V2.0”, March 2005. [http://docs.oasis-  
80       open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf)

81       **[SAML1.1IMI]**     OASIS Committee Draft, “SAML V1.1 Information Card Token Profile Version  
82       1.0”, July 2010. [http://docs.oasis-open.org/imi/identity/cd/imi-saml1.1-profile-cd-  
83       02.pdf](http://docs.oasis-open.org/imi/identity/cd/imi-saml1.1-profile-cd-02.pdf)

---

## 84 2 SAML V2.0 Information Card Token Profile

### 85 2.1 Required Information

86 **Identification:** <http://docs.oasis-open.org/imi/ns/token/saml2/200908>

87 **Contact information:** [imi-comment@lists.oasis-open.org](mailto:imi-comment@lists.oasis-open.org)

88 **Description:** Given below

89 **Updates:** None

### 90 2.2 Profile Overview

91 Identity Providers and Relying Parties employing the Identity Metasystem Interoperability [IMI] profile to  
92 request and exchange security tokens are able to use arbitrary token formats, provided there is  
93 agreement on the token's syntax and semantics, and a way to connect the token's content to the  
94 supported protocol features.

95 This profile provides a set of requirements and guidelines for the use of SAML V2.0 assertions as security  
96 tokens that, where possible, emulates existing SAML V2.0 authentication profiles [SAML2Prof] so as to  
97 limit the amount of new work that must be done by existing software to support the use of Information  
98 Cards. It also provides for the use of SAML assertions in this new context that is safe and consistent with  
99 best practices in similar contexts.

100 This profile does not seek to alter the required behavior of existing Identity Selector software, or conflict  
101 with the profile defined by [IMI].

### 102 2.3 Identity Provider Requirements

103 While the SAML V2.0 specification [SAML2Core] defines an Identity Provider solely in terms of the SAML  
104 Authentication Request protocol, the term is generally applicable to an entity that issues authentication  
105 assertions by means of other, similar protocols. In this case, the Identity Provider functions as an Identity  
106 Provider/Security Token Service (IP/STS) in the Information Card vocabulary, and issues assertions in  
107 response to <wst:RequestSecurityToken> messages [WS-Trust12] or [WS-Trust13] or [WS-  
108 Trust14].

109 As defined by [IMI], the request contains information that provides input into the assertion creation  
110 process. The following sections outline requirements for interpreting this input and the resulting assertion  
111 content.

#### 112 2.3.1 Token Types

113 Identity Providers MUST support both of the following token type strings in conjunction with this profile:

- 114 • <http://docs.oasis-open.org/imi/ns/token/saml2/200908>
- 115 • `urn:oasis:names:tc:SAML:2.0:assertion`

116 These strings appear in various content produced and consumed by an Identity Provider, such as (but not  
117 limited to) the <wst:TokenType> element.

118 Information Cards issued by the Identity Provider MUST indicate support for both token types above.

#### 119 2.3.2 Identifying Token Issuers

120 Information Cards produced by Identity Providers MUST contain the Identity Provider's unique name as  
121 the value of the <ic:Issuer> element. This name corresponds to the SAML concept of an "entityID"  
122 and may correspond to an actual entityID in the SAML sense of the term, or a logically equivalent name  
123 for the Identity Provider.



### 124 **2.3.3 General Assertion Requirements**

125 Assertions issued in accordance with this profile MUST contain a single `<saml:AuthnStatement>` that  
126 reflects the authentication of the token requester to the Identity Provider. Note that it does NOT reflect the  
127 authentication taking place by means of the assertion to the Relying Party. It MAY contain a single  
128 `<saml:AttributeStatement>` that carries one or more `<saml:Attribute>` elements reflecting the  
129 claims requested by the Relying Party, in the manner specified by [IMI].

130 When satisfying these requested claims, the resulting `<saml:Attribute>` element's `NameFormat` XML  
131 attribute MUST be:

132 `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`

133 The element's `Name` XML attribute MUST correspond to the requested claim type's URI value (e.g., in  
134 `<ic:ClaimType>` elements).

135 A `<saml:NameID>` element MAY be included in the assertion's `<saml:Subject>` element. If the  
136 requested claim types include a claim type with a URI corresponding to a SAML name identifier format  
137 known to the Identity Provider, it may satisfy that claim request by including a `<saml:NameID>` element  
138 of the proper format in the assertion's subject. If more than one claim type corresponding to a name  
139 identifier format is requested, the Identity Provider MAY fault the request or choose any requested format,  
140 at its discretion. If two such claim types are "required" by the Relying Party, a fault MUST be generated.

141 The assertion's `<saml:Subject>` element MUST contain at least one  
142 `<saml:SubjectConfirmation>` element, the details of which are defined in Section 2.3.4 below.

143 Finally, the assertion MUST be signed.

### 144 **2.3.4 Proof Keys and Subject Confirmation**

145 [IMI] defines three classes of "proof keys" that bind the issued token to key material controlled by the  
146 client: symmetric, asymmetric, and no key. The notion of a proof key maps directly to a  
147 `<saml:SubjectConfirmation>` element in the issued assertion.

148 If a token request does not include a `<wst:KeyType>` element, the Identity Provider SHOULD assume  
149 that a symmetric proof key is required, in accordance with [WS-Trust13] or [WS-Trust14].

150 Both symmetric and asymmetric proof key types generally correspond to the "holder-of-key" confirmation  
151 method defined in Section 3.1 of [SAML2Prof]. For the proof key types and algorithms specified by [IMI],  
152 the resulting assertion MUST contain a `<saml:SubjectConfirmation>` element with a `Method` of:

153 `urn:oasis:names:tc:SAML:2.0:cm:holder-of-key`

154 The accompanying `<ds:KeyInfo>` element MUST identify the proof key. In the case of an RSA  
155 asymmetric proof key, the key SHOULD be represented as a `<ds:RSAKeyValue>` element within a  
156 `<ds:KeyValue>` element.

157 Proof key algorithms defined outside of [IMI] MAY specify alternate `<saml:SubjectConfirmation>`  
158 content, if necessary.

159 The "no key" proof key type corresponds to the "bearer" confirmation method defined in Section 3.3 of  
160 [SAML2Prof]. The resulting assertion MUST contain a `<saml:SubjectConfirmation>` element with a  
161 `Method` of:

162 `urn:oasis:names:tc:SAML:2.0:cm:bearer`

163 In the case of bearer assertions, the `<saml:SubjectConfirmation>` element MUST include a  
164 `<saml:SubjectConfirmationData>` element containing a `NotOnOrAfter` XML attribute to limit their  
165 use, typically to a very short window of time, although the exact duration may be use case dependent.  
166 The attribute MAY be included for "holder-of-key" assertions, at the discretion of the Identity Provider.

167 The `<saml:SubjectConfirmationData>` element, if present, MUST NOT contain a `NotBefore` or  
168 `Recipient` XML attribute. The `Address` XML attribute MAY be included to indicate the expected  
169 network address of the client to the Relying Party.

170 Finally, note that other `<saml:SubjectConfirmation>` elements MAY be included at the discretion of  
171 the Identity Provider.

### 172 **2.3.5 Conditions**

173 Assertions MAY contain a `<saml:Conditions>` element with `NotBefore` and `NotOnOrAfter`  
174 attributes. This validity period can be independent of the window during which the client can present the  
175 assertion to a Relying Party as a security token (see Section 2.3.4), but of course must be a superset of  
176 that window.

177 If the request contains a `<wsp:AppliesTo>` element, then a `<saml:AudienceRestriction>`  
178 containing a `<saml:Audience>` element MUST be included with the value of that element.

179 Other conditions MAY be included at the discretion of the Identity Provider.

### 180 **2.3.6 Encryption**

181 If a suitable key belonging to the Relying Party is known, the Identity Provider SHOULD encrypt the  
182 resulting assertion in accordance with Section 6 of [SAML2Core], and return the result to the requester in  
183 the form of a `<saml:EncryptedAssertion>` element.

184 If a public key belonging to the Relying Party is communicated to the Identity Provider in the  
185 `<wst:RequestSecurityToken>` request message in the `<wsp:AppliesTo>` element, this key  
186 SHOULD be used in preference to any other key known to the Identity Provider through other means  
187 (e.g., SAML V2.0 metadata).

## 188 **2.4 Relying Party Requirements**

189 A Relying Party uses the mechanisms defined by [IMI] to request security tokens in the form of SAML 2.0  
190 assertions issued by particular or arbitrary Identity Providers. The following sections outline requirements  
191 for describing a Relying Party's needs based on this profile.

### 192 **2.4.1 Token Types**

193 Relying Parties SHOULD use the following token type string when requesting a token in conjunction with  
194 this profile:

195 `http://docs.oasis-open.org/imi/ns/token/saml2/200908`

196 This string appears in various content produced by a Relying Party, such as (but not limited to) the  
197 `<wst:TokenType>` element.

198 For backward compatibility, Relying Parties MAY use the following token type string:

199 `urn:oasis:names:tc:SAML:2.0:assertion`

200 When using the legacy token type, Relying Parties should be aware that the resulting assertions may or  
201 may not conform to this profile. If such a guarantee is required, the newer token type SHOULD be used  
202 instead.

### 203 **2.4.2 Identifying Token Issuers**

204 When identifying a requirement for a specific token issuer, the Relying Party SHOULD use the Identity  
205 Provider's unique name (i.e., its "entityID"), either as the value of the `<sp:Issuer>/<wsa:Address>`  
206 element in its security policy or as the value of the `issuer` OBJECT tag parameter.

### 207 **2.4.3 Identifying Relying Parties**

208 If the Relying Party provides security policy metadata (see Section 3.1 of [IMI]), it MAY include a  
209 `<wsp:AppliesTo>` element inside a `<sp:RequestSecurityTokenTemplate>` element that refers to  
210 its own unique name (i.e., its "entityID") in the `<wsa:Address>` element.

211 If it does include a `<wsp:AppliesTo>` element, it SHOULD NOT identify itself using the location of its  
212 endpoint, as this complicates the Identity Provider's ability to identify the Relying Party. A logical name  
213 SHOULD be used instead.

## 214 2.4.4 Identifying Claim Types

215 SAML attributes required or desired by the Relying Party are identified by using the SAML attribute's  
216 Name XML attribute in various places, such as the `<ic:ClaimType>` element's `Uri` XML attribute. Such  
217 SAML attributes MUST have a `NameFormat` XML attribute of:

218 `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`

219 A claim type URI corresponding to a SAML name identifier format MAY be used to request a particular  
220 type of `<saml:NameID>` element in the resulting assertion. A Relying Party MUST NOT request more  
221 than one "required" claim type corresponding to a name identifier format.

## 222 2.4.5 Assertion Validity

223 Relying Parties SHOULD evaluate assertions using the rules defined by [SAML2Core] (and [SAML2Prof]  
224 in the case of the defined subject confirmation methods). Invalid assertions SHOULD NOT be used to  
225 authenticate clients that present them.

226 In assessing validity, a Relying Party MUST verify the signature over the assertion, evaluate any  
227 conditions present, and successfully evaluate at least one `<saml:SubjectConfirmation>` element in  
228 the assertion based on the presentation of the assertion. This may include verifying that the  
229 `NotOnOrAfter` attribute in the `<saml:SubjectConfirmationData>` (if present) has not passed,  
230 subject to allowable clock skew between it and the Identity Provider.

231 If the `<saml:SubjectConfirmationData>` includes an `Address` attribute, the Relying Party MAY  
232 check the client address against it.

233 In the case of the "holder-of-key" method, the Relying Party MUST establish proof of possession by the  
234 client of the key identified by the accompanying `<ds:KeyInfo>` element, such as through the use of a  
235 message signature or authentication over a secure transport. The exact means are out of scope of this  
236 profile.

237 In the case of the "bearer" method, the Relying Party MUST ensure that assertions are not replayed, by  
238 maintaining the set of used ID values for the length of time for which the assertion would be considered  
239 valid based on the `NotOnOrAfter` attribute in the `<saml:SubjectConfirmationData>` element.

## 240 2.5 Use of SAML Metadata

241 While not required, sites exchanging SAML assertions based on this profile MAY rely on SAML V2.0  
242 metadata [SAML2Meta] as a way of deriving information about endpoints and keys, to supplement  
243 mechanisms that exist within [IMI]. Where similarities or overlaps exist, precedence MUST be given to  
244 metadata information exchanged using the mechanisms defined by [IMI].

245 When referring to token issuers or Relying Parties by "logical" names, in the manner described by [IMI],  
246 the names used SHOULD correspond to the "entityID" values used in SAML metadata.

247 The value `http://docs.oasis-open.org/imi/ns/token/saml2/200908` MUST be used in the  
248 `protocolSupportEnumeration` attribute to identify support for this profile within a  
249 `<md:IDPSSODescriptor>` or `<md:SPSSODescriptor>` role.

250 If `<md:SingleSignOnService>` or `<md:AssertionConsumerService>` endpoints supporting this  
251 profile are included, the same value MUST be used as the value of the `Binding` attribute. In addition, a  
252 `<wsa:EndpointReference>` element MAY be included within an endpoint element to describe the  
253 endpoint and its security policy in accordance with [IMI].

## 254 2.6 Security Considerations

### 255 2.6.1 Unconstrained Bearer Assertions

256 The Information Card model's support for hiding the identity of the Relying Party from the Identity  
257 Provider, combined with constraints on the implementation of the model for use with web browsers, leads  
258 to requests for "unconstrained" bearer assertions with no audience or subject confirmation conditions on  
259 use. While all uses of bearer assertions are subject to certain threats and attacks (see [SAML2Sec]), the  
260 lack of conditions on such assertions introduces additional serious threats to consider.

261 Ordinarily, the threat of a stolen assertion is mitigated by the fact that it can only be used to authenticate  
262 to a particular Relying Party. Without conditions on use, an attacker that successfully steals such an  
263 assertion has many more targets of opportunity. Essentially, the ability to mount an attack against a user's  
264 interactions with any single Relying Party become effective against all parties that are willing to accept  
265 such an assertion. Consider that some low value services may choose to forgo the use of TLS/SSL,  
266 leaving the assertions issued for their use much more vulnerable to theft. A successful attacker can then  
267 impersonate the intended user even with Relying Parties that choose to deploy such protection, rendering  
268 their investment moot.

269 Perhaps more seriously, Relying Parties that choose to accept such assertions are in turn empowered  
270 with the opportunity to impersonate the user for the duration of the subject confirmation window with any  
271 other like-minded Relying Parties. This threat looms larger when one considers that a compromised  
272 Relying Party could expose all its users to this risk if an attacker can tap the flow of incoming assertions.  
273 With traditional constraints in place, this threat is mitigated by the fact that a compromise, while potentially  
274 exposing user data, does not extend beyond the scope of access to the affected Relying Party.

275 Note that one of the only mitigating mechanisms to these threats are to enforce restrictions on use of  
276 assertions based on an IP address placed into the assertion by the Identity Provider. While moderately  
277 effective, this practice often proves impractical for services offered to large user populations, many of  
278 whom are likely to encounter proxies and network configurations that result in inability to satisfy the  
279 restriction.

280 As a result, this profile recommends against the use of unconstrained bearer assertions as a general  
281 matter, and urges implementations to provide deployers with the ability to control this behavior. The  
282 privacy advantages of such a model need to be carefully weighed against the risks to users and Relying  
283 Parties.

### 284 2.6.2 Encryption

285 Identity Providers should generally make every attempt to encrypt the assertions they produce if a key for  
286 the Relying Party can be established. If encryption is not used, then the Identity Provider should be aware  
287 of the potential for exposure of the assertion's contents, both to the requester and potentially to network  
288 observers if TLS/SSL is not used (particularly between the requester and the eventual Relying Party).

289 Caution, however, should be exercised in relying solely on the TLS/SSL certificate found at a Relying  
290 Party's endpoint to identify the key. In particular, the key has to be authenticated in order to ensure that it  
291 actually belongs to the eventual endpoint used by the client. Furthermore, there can be no guarantee that  
292 the software responsible for decrypting the security token will have access to the corresponding private  
293 key.

## 294 2.7 Examples

### 295 2.7.1 Two Required Claims

296 In this example, a Relying Party asks for two required claims, an email address and a displayable name.  
297 These are standard, well-known LDAP/X.500 attributes with a standard representation in SAML.

298 Given the following OBJECT syntax:

```
299 <OBJECT type="application/x-informationCard" name="xmlToken">  
300   <PARAM Name="tokenType"  
301     Value="http://docs.oasis-open.org/imi/ns/token/saml2/200908">
```

```

302 <PARAM Name="issuer" Value="https://idp.example.org/entity">
303 <PARAM Name="requiredClaims"
304   Value="urn:oid:0.9.2342.19200300.100.1.3 urn:oid:2.16.840.1.113730.3.1.241">
305 </OBJECT>

```

306 the following assertion could be issued:

```

307 <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
308   ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
309   IssueInstant="2009-04-17T00:46:02Z" Version="2.0">
310 <Issuer>https://idp.example.org/entity</Issuer>
311 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
312   ...
313 </ds:Signature>
314 <Subject>
315   <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
316     <SubjectConfirmationData Address="192.168.1.1"
317       NotOnOrAfter="2009-04-17T00:51:02Z" />
318   </SubjectConfirmation>
319 </Subject>
320 <Conditions
321   NotBefore="2009-04-17T00:46:02Z" NotOnOrAfter="2009-04-17T01:51:02Z">
322   <AudienceRestriction>
323     <Audience>https://puppies.com/entity</Audience>
324   </AudienceRestriction>
325 </Conditions>
326 <AuthnStatement AuthnInstant="2009-04-17T00:46:00Z">
327   <AuthnContext>
328     <AuthnContextClassRef>
329       urn:oasis:names:tc:SAML:2.0:ac:classes:Password
330     </AuthnContextClassRef>
331   </AuthnContext>
332 </AuthnStatement>
333 <AttributeStatement>
334   <Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
335     Name="urn:oid:0.9.2342.19200300.100.1.3" FriendlyName="mail">
336     <AttributeValue>jdoe@example.org</AttributeValue>
337   </Attribute>
338   <Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
339     Name="urn:oid:2.16.840.1.113730.3.1.241" FriendlyName="displayName">
340     <AttributeValue>John Doe</AttributeValue>
341   </Attribute>
342 </AttributeStatement>
343 </Assertion>

```

## 344 2.7.2 One Required Claim, as Federated NameID

345 In this example, a Relying Party asks for a single claim using a name that is recognized by the Identity  
346 Provider as a SAML name identifier format. Any claim name could be interpreted in this fashion since the  
347 taxonomy of such formats is extensible, but it is expected that deployments making use of SAML name  
348 identifiers would already agree on appropriate use of them.

349 Given the following OBJECT syntax:

```

350 <OBJECT type="application/x-informationCard" name="xmlToken">
351 <PARAM Name="tokenType"
352   Value="http://docs.oasis-open.org/imi/ns/token/saml2/200908">
353 <PARAM Name="issuer" Value="https://idp.example.org/entity">
354 <PARAM Name="requiredClaims"
355   Value="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent">
356 </OBJECT>

```

357 the following assertion could be issued:

```

358 <Assertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
359   ID="_a75adf55-01d7-40cc-929f-dbd8372ebdfc"
360   IssueInstant="2009-04-17T00:46:02Z" Version="2.0">

```

```

361 <Issuer>https://idp.example.org/entity</Issuer>
362 <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
363   ...
364 </ds:Signature>
365 <Subject>
366   <NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-format:persistent"
367     NameQualifier="https://idp.example.org/entity"
368     SPNameQualifier="https://puppies.com/entity">
369     rfhyfeefod893434923gqwdmtgr9090f
370   </NameID>
371   <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
372     <SubjectConfirmationData Address="192.168.1.1"
373       NotOnOrAfter="2009-04-17T00:51:02Z" />
374   </SubjectConfirmation>
375 </Subject>
376 <Conditions>
377   NotBefore="2009-04-17T00:46:02Z" NotOnOrAfter="2009-04-17T01:51:02Z">
378   <AudienceRestriction>
379     <Audience>https://puppies.com/entity</Audience>
380   </AudienceRestriction>
381 </Conditions>
382 <AuthnStatement AuthnInstant="2009-04-17T00:46:00Z">
383   <AuthnContext>
384     <AuthnContextClassRef>
385       urn:oasis:names:tc:SAML:2.0:ac:classes:Password
386     </AuthnContextClassRef>
387   </AuthnContext>
388 </AuthnStatement>
389 </Assertion>

```

---

### 390 **3 Conformance**

391 An Identity Provider implementation conforms to this profile if it can produce assertions consistent with the  
392 normative text in Section 2.3.

393 A Relying Party implementation conforms to this profile if it can accept assertions consistent with the  
394 normative text of Section 2.4.

395 Use of SAML V2.0 metadata [[SAML2Meta](#)] per Section 2.5 is OPTIONAL.

---

396 **A. Acknowledgements**

397 The editors would like to acknowledge the contributions of the OASIS Identity Metasystem Interoperability  
398 Technical Committee, whose voting members at the time of publication were:

399 **Participants:**

400 John Bradley, Individual  
401 Scott Cantor, Internet2  
402 Marc Goodner, Microsoft (Chair)  
403 Michael B. Jones, Microsoft (Editor)  
404 Dale Olds, Novell  
405 Anthony Nadalin, Microsoft (Chair)  
406 Drummond Reed, Cordance

407 The editors would also like to acknowledge the following contributors:

- 408
  - Jim Fox, University of Washington



## B. Revision History

| Revision | Date             | Editor           | Changes Made   |
|----------|------------------|------------------|--|
| cd-03    | 7 July 2010      | Michael B. Jones | Committee draft for promotion to committee specification.  |
| ed-07    | 10 June 2010     | Michael B. Jones | Incorporate feedback from public review. Changes made are non-normative. They address issue IMI-36: "Examples in sections 2.7.1 and 2.7.2 are incorrect" and keep the references between the SAML 1.1 and SAML 2.0 profiles in sync. |
| cd-02    | 31 March 2010    | Michael B. Jones | Committee draft for public review.   |
| ed-06    | 2 February 2010  | Michael B. Jones | Typographic corrections.   |
| ed-05    | 1 February 2010  | Michael B. Jones | Consistency pass relative to other IMI TC documents. Made internal references hyperlinks.  |
| ed-04    | 16 December 2009 | Scott Cantor     | Resolutions to issues IMI-26 and IMI-27.   |
| cd-01    | 6 December 2009  | Scott Cantor     | Committee Draft 01, CD edits.  |
| ed-03    | 16 November 2009 | Scott Cantor     | Legacy token type language added.  |
| ed-02    | 27 October 2009  | Scott Cantor     | Revised based on IMI TC feedback and to correct for spec formatting issues.  |
| ed-01    | 19 August 2009   | Scott Cantor     | Revised from Draft 02 of the SSTC-submitted version of this profile.   |