
SAML V2.0 Subject Identifier Attributes Profile Version 1.0

Working Draft 03

15 September 2017

Technical Committee:

OASIS Security Services (SAML) TC

Chair:

Thomas Hardjono (hardjono@mit.edu), M.I.T.

Editor:

Scott Cantor (cantor.2@osu.edu), Internet2

Additional artifacts:

None

Related work:

This specification is related to:

- eduPerson Object Class Specification (201602)

Declared XML namespaces:

None

Abstract:

This specification standardizes two new SAML Attributes to identify security subjects, as a replacement for long-standing inconsistent practice with the `<saml:NameID>` and `<saml:Attribute>` constructs, and to address recognized deficiencies with the SAML persistent NameID format.

Status:

This [Working Draft](#) (WD) has been produced by one or more TC Members; it has not yet been voted on by the TC or [approved](#) as a Committee Draft (Committee Specification Draft or a Committee Note Draft). The OASIS document [Approval Process](#) begins officially with a TC vote to approve a WD as a Committee Draft. A TC may approve a Working Draft, revise it, and re-approve it any number of times as a Committee Draft.

This Working Draft is being developed under the [RF on RAND Terms](#) Mode of the [OASIS IPR Policy](#), the mode chosen when the Technical Committee was established. All members of the TC should be familiar with this document, which may create obligations regarding the disclosure and availability of a member's patent, copyright, trademark and license rights that read on an approved OASIS specification. 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 TC's web page (<https://www.oasis-open.org/committees/security/ipr.php>).

Any machine-readable content ([Computer Language Definitions](#)) declared Normative for this Work Product must also be provided in separate plain text files. In the event of a discrepancy between such plain text file and display content in the Work Product's prose narrative document(s), the content in the separate plain text file prevails.

URI patterns:

Initial publication URI:

<http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/csd01/saml-subject-id-attr-v1.0-csd01.odt>

Permanent "Latest version" URI:

<http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.odt>

Copyright © OASIS Open 2017. 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.

Table of Contents

1	Introduction.....	4
1.1	IPR Policy.....	4
1.2	Terminology and Notation.....	4
1.3	Normative References.....	4
1.4	Non-Normative References.....	5
2	Motivation.....	6
2.1	Problem Statement.....	6
2.2	Relationship to Existing Work.....	7
3	SAML V2.0 Subject Identifier Attributes Profile Version 1.0.....	8
3.1	Required Information.....	8
3.2	Overview.....	8
3.3	Standard Subject Identifier.....	8
3.3.1	Syntax and Handling.....	8
3.3.2	Semantics and Practices.....	9
3.4	Pairwise Subject Identifier.....	9
3.4.1	Syntax and Handling.....	9
3.4.2	Semantics and Practices.....	10
3.4.3	Strategies.....	10
3.4.4	Differences from "persistent" NameIDs.....	10
3.5	Considerations for SAML Profiles.....	11
3.5.1	Requirements Signaling.....	11
3.5.2	NameID Considerations.....	11
4	Conformance.....	12
4.1	Conformance Clause 1: Asserting Party Implementations.....	12
4.2	Conformance Clause 2: Relying Party Implementations.....	12
Appendix A	Acknowledgments.....	13
Appendix B	Revision History.....	14

1 Introduction

1.1 IPR Policy

This Working Draft is being developed under the [RF on RAND Terms](#) Mode of the [OASIS IPR Policy](#), the mode chosen when the Technical Committee was established.

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 TC's web page (<https://www.oasis-open.org/committees/security/ipr.php>).

1.2 Terminology and Notation

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

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

Prefix	XML Namespace	Comments
saml:	urn:oasis:names:tc:SAML:2.0:assertion	This is the SAML V2.0 assertion namespace [SAML2Core] .
samlp:	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace [SAML2Core] .
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace [SAML2Meta] .
mdattr:	urn:oasis:names:tc:SAML:metadata:attributes	This is the SAML V2.0 metadata extension for entity attributes namespace [MetaAttr] .
xsd:	http://www.w3.org/2001/XMLSchema	This namespace is defined in the W3C XML Schema specification [XMLSCHEMA-2] .

1.3 Normative References

- [RFC2119]** Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels”, BCP 14, RFC 2119, March 1997. <http://www.ietf.org/rfc/rfc2119.txt>.
- [SAML2Core]** *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*. Edited by Scott Cantor, John Kemp, Rob Philpott, Eve Maler. 15 March 2005. OASIS Standard. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>
- [MetaAttr]** *SAML V2.0 Metadata Extension for Entity Attributes Version 1.0*. Edited by Scott Cantor. 4 August 2009. OASIS Committee Specification. <http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr-cs-01.pdf>. Latest version: <http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr.pdf>.
- [SAML2Errata]** *SAML V2.0 Errata*. Edited by Scott Cantor. 1 May 2012. OASIS Approved Errata. <http://docs.oasis-open.org/security/saml/v2.0/errata05/os/saml-v2.0-errata05-os.pdf>. Latest version: <http://docs.oasis-open.org/security/saml/v2.0/sstc-saml-approved-errata-2.0.pdf>
- [SAML2Meta]** *Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0*. Edited by Scott Cantor, Jahan Moreh, Rob Philpot, Eve Maler. 15 March 2005. OASIS Standard. <http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf>

35 **[XMLSCHEMA-2]** *XML Schema Part 2: Datatypes Second Edition*. Paul V. Biron, A. Malhotra,
36 Editors. W3C Recommendation. October 28, 2004.
37 <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/>. Latest version:
38 <http://www.w3.org/TR/xmlschema-2/>.

39 **1.4 Non-Normative References**

40 **[eduPerson]** Internet2, “eduPerson Object Class Specification (201602)”, February 2016.
41 [http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-](http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html)
42 [201602.html](http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html).
43 **[RFC4648]** Josefson, S., “The Base16, Base32, and Base64 Data Encodings”, RFC 4648,
44 October 2006. <http://www.ietf.org/rfc/rfc4648.txt>.
45 **[SAML2Prof]** *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0*. Edited
46 by John Hughes, Scott Cantor, Jeff Hodges, Frederick Hirsch, Prateek Mishra,
47 Rob Philpot, Eve Maler. 15 March 2005. OASIS Standard. [http://docs.oasis-](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)
48 [open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf](http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf)

49 2 Motivation

50 2.1 Problem Statement

51 Identification of subjects in security protocols and applications has a fraught history of inconsistent syntax,
52 bugs, terrible but deeply cemented practices such as misuse of email addresses, vertical market-specific
53 approaches, and failure to precisely communicate intended semantics and constraints. These problems
54 lead to overly complex burdens on both asserting and relying parties to supply and consume a variety of
55 different identifiers in different formats, many of which work poorly with off the shelf applications. Much of
56 this is self-inflicted fragmentation due to the constant tension between fixing problems with new solutions
57 and avoiding them to gain scale.

58 SAML itself has its origins in a design philosophy that tried to avoid breaking new ground in this area, and
59 instead attempted to design for generality, which is valuable, but did not ease adoption due to a lack of
60 guidance. SAML also complicates itself by providing an optional, singly-appearing construct for
61 identification (the `<saml:NameID>` element) *and* a more general multiply-appearing
62 `<saml:Attribute>` construct that inherently overlap.

63 This, together with inconsistent technical precision by implementers and deployers, creates complexity.
64 Deployment experience has shown that use of the NameID feature is confusing in many implementations.
65 It also, through its presence in the SAML Single Logout protocol, potentially appears in web access logs,
66 leading to the added complexity of encryption when privacy is a consideration.

67 There is a general consensus by most federated identity practitioners around a few common
68 requirements:

- 69 • Identifiers should be as stable as possible and should never have a risk of reassignment to
70 different subjects due to the lack of tight synchronization¹ inherent between loosely-coupled
71 systems.
- 72 • Opaque (i.e., superficially random) identifiers are inherently more stable than name-based
73 identifiers or email addresses in many organizations.
- 74 • Identifiers should be compact and simple to handle and manipulate.
- 75 • The ability to clearly express the scope of an identifier's uniqueness and enforce policy around the
76 issuers permitted to supply an identifier is crucial to federated systems and the lack of such policy
77 has led to widely-publicized breaches.

78 Another requirement perhaps more common to education and research is the ability for different asserting
79 parties to issue the same identifier. This is facilitated by ensuring the scope of an identifier is part of its
80 value and not implicit in a protocol-specific value specific to an asserting party.

81 SAML does not define an identifier that meets all of these requirements well. It does standardize a kind of
82 NameID termed "persistent" that meets some of them in the particular case of so-called "pairwise"
83 identification, where an identifier varies by relying party. It has seen minimal adoption outside of a few
84 contexts, and fails at the "compact" and "simple to handle" criteria above, on top of the disadvantages
85 inherent with all NameID usage.

86 Pairwise identification helps meet certain privacy and regulatory requirements, but does not address many
87 common use cases that demand cross-system correlation without the friction of complex linking protocols
88 and the involvement of the data subject.

89 In addition, it has come to light that many, if not most, applications have a predisposition to handle
90 identifiers case-insensitively, partly due to a long-standing, though factually untrue, assumption that e-mail
91 address mailbox names are case-insensitive data. SAML's "persistent" NameID definition explicitly
92 requires case-sensitive handling, making them impossible to use safely with such applications without
93 resorting to additional layers of profiling. Note that any other specification promulgating such identifiers is
94 potentially unsafe in combination with such applications and should be used with caution.

1 It's worth noting that SAML actually defines a protocol for managing changes to NameID values, but it has seen very little adoption, further demonstrating the lack of value of NameID usage.

95 For all these reasons, this profile attacks these problems using a clean-slate approach that abandons
96 existing practice instead of attempting to layer more profiling and out of band agreements on top of
97 existing solutions, an approach that has seemingly reached its breaking point.

98 **2.2 Relationship to Existing Work**

99 Clean slate notwithstanding, this profile is based on a thorough review of practice within the higher
100 education sector, which has seen extensive adoption of SAML and partially-successful efforts to
101 standardize subject identification and avoid the “email address” trap that most of the technical world fell
102 into many years ago.

103 Among the significant work in this space, the [eduPerson] schema includes a number of identifier
104 attributes, some widely adopted and some less so. This profile is particularly influenced by:

- 105 • Experience with the SAML “persistent” NameID construct and the eduPersonTargetedID attribute.
- 106 • The eduPersonPrincipalName and eduPersonUniqueid attributes, the former successful but
107 deeply flawed, the latter less successful but more consciously defined.
- 108 • Success with DNS domain-based scoping of values and managing policy around their use in
109 SAML.
- 110 • Challenges in the adoption of profiles required to accommodate the limitations of widely deployed
111 identifiers.

112 Portions of this specification are borrowed liberally from the [eduPerson] specification in a deliberate
113 desire to remain consistent with the formulation of the eduPersonUniqueid attribute.

114 3 SAML V2.0 Subject Identifier Attributes Profile 115 Version 1.0

116 3.1 Required Information

117 **Identification:** urn:oasis:names:tc:SAML:profile:subject-id

118 **Contact information:** security-services-comment@lists.oasis-open.org

119 **Description:** Given below.

120 **Updates:** None.

121 3.2 Overview

122 This profile defines a pair of SAML Attributes providing for unique identification of security subjects
123 (generally but not exclusively people). One is designed for general use as a correlatable identifier, and the
124 other is a pairwise identifier suitable for more specialized use.

125 Both Attributes are limited to a single value when expressed in SAML assertions and other constructs.
126 They may be mapped to and form other technical forms (e.g., LDAP) but this profile does not include such
127 mappings.

128 In the terminology used in this profile:

- 129 • "asserting party" refers to a SAML entity, uniquely identified by an entityID, that issues assertions
130 containing one or both of these Attributes
- 131 • "relying party" refers to one or more SAML entities, each uniquely identified by an entityID, that
132 receive assertions containing one or both of these Attributes

133 In addition, this profile defines a signaling mechanism for a Service Provider to express its subject
134 identification requirements via SAML metadata [[SAML2Meta](#)], by means of the
135 <mdattr:EntityAttributes> extension [[MetaAttr](#)]. This allows Identity Providers to unambiguously
136 understand the requirements of the service and facilitates deployment profiles that wish to mandate
137 support for one or both of these Attributes, while maintaining appropriate privacy expectations.

138 3.3 Standard Subject Identifier

139 For standard identification of subjects, the following SAML Attribute is defined:

140 **Name:** urn:oasis:names:tc:SAML:attribute:subject-id

141 **NameFormat:** urn:oasis:names:tc:SAML:2.0:attrname-format:uri

142 This is a long-lived, non-re-assignable, omni-directional identifier suitable as a globally-unique external key
143 by applications.

144 3.3.1 Syntax and Handling

145 This Attribute, when appearing as a SAML <saml:Attribute> element, MUST contain exactly one
146 <saml:AttributeValue> element, whose xsi:type SHOULD be absent or if present MUST BE
147 bound to the XML Schema xsd:string data type [[XMLSCHEMA-2](#)].

148 Any leading or trailing whitespace present in the <saml:AttributeValue> element's content is not
149 significant and MUST be stripped by the relying party prior to evaluation or comparison.

150 The value consists of two substrings (termed a "unique ID" and a "scope" in the remainder of this
151 definition) separated by an @ symbol (ASCII 64) as an inline delimiter.

152 The unique ID consists of from 1 to 127 characters, all either alphanumeric or the equals sign (ASCII 61)
153 or hyphen (ASCII 45). The first character MUST be alphanumeric.

154 The scope consists of 1 to 127 alphanumeric, hyphen (ASCII 45), or period (ASCII 46) characters. The
155 first character MUST be alphanumeric. The scope deliberately resembles, and typically may be, a DNS
156 domain name, but is drawn from a more limited character set due to case folding considerations, and no
157 attempt is made to limit the allowable grammar to legal domain names (e.g., it allows consecutive
158 periods).

159 The ABNF grammar is therefore:

```
160     <value> = <uniqueID> "@" <scope>  
161     <uniqueID> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "=" / "-")  
162     <scope> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "-" / ".")
```

163 Value comparison MUST be performed case-insensitively (that is, values that differ only by case are the
164 same, and refer to the same subject). It is RECOMMENDED that alphabetic characters be in lower-case
165 when expressing and storing values.

166 3.3.2 Semantics and Practices

167 A value (the unique ID and scope together) MUST be bound to only one subject, but the same unique ID
168 given a different scope may refer to the same or (far more likely) a different subject.

169 The relationship between an asserting party and a scope is an arbitrary one and does not reflect any
170 assumed relationship between a scope in the form of a domain name and a domain found in a given
171 SAML entityID.

172 A value MUST NOT be assigned to more than a single subject over its lifetime of use under any
173 circumstances. The unique ID should therefore be constructed in a fashion that reduces the probability of
174 non-technical or political considerations leading to a violation of this requirement, and any such violation
175 should be treated as a potential security risk to the relying parties to which the value may have been
176 given.

177 Relying parties should not treat this identifier as an email address for the subject as it is unlikely (though
178 not precluded) for it to be valid for that purpose. Most organizations will find that existing email address
179 values will not serve well as values for this Attribute.

180 The unique ID should not change as a result of a change to any other data associated with the subject
181 (e.g., name, email address, age, organizational role).

182 A given value MUST identify the same subject regardless of the context of use and for which relying
183 parties to which the Attribute is given. It is therefore to be assumed by relying parties that receive a given
184 value that the same subject has been identified.

185 Note that, policy permitting, a given value could be provided by any asserting party, and the requirement
186 still holds: identical values correspond to the same subject. While it will be common in many deployments
187 to limit values with a given scope to a single asserting party, this is ultimately left to the discretion of the
188 relying party and the use case.

189 Inevitably, a single subject may be identified simultaneously by multiple values, but this should be
190 minimized to the extent possible.

191 3.4 Pairwise Subject Identifier

192 For pairwise identification of subjects, the following SAML Attribute is defined:

193 **Name:** urn:oasis:names:tc:SAML:attribute:pairwise-id

194 **NameFormat:** urn:oasis:names:tc:SAML:2.0:attrname-format:uri

195 This is a long-lived, non-re-assignable, uni-directional identifier suitable as a unique external key specific
196 to particular applications. Its value for a given subject depends on the relying party to whom it is given,
197 preventing unrelated systems from using it as a basis for correlation.

198 3.4.1 Syntax and Handling

199 The requirements for this Attribute are identical to those described in Section 3.3.1. That is, values of this
200 Attribute are indistinguishable, lacking context, from the other.

201 **3.4.2 Semantics and Practices**

202 Given a particular relying party, a value (the unique ID and scope together) MUST be bound to only one
203 subject, but the same unique ID given a different scope may refer to the same or (far more likely) a
204 different subject. The same value provided to different relying parties MAY refer to different subjects, and
205 indeed that is the primary distinguishing characteristic of this identifier Attribute.

206 The relationship between an asserting party and a scope is an arbitrary one and does not reflect any
207 assumed relationship between a scope in the form of a domain name and a domain found in a given
208 SAML entityID.

209 A value MUST NOT be assigned to more than a single subject over its lifetime of use under any
210 circumstances. The unique ID should therefore be constructed in a fashion that reduces the probability of
211 non-technical or political considerations leading to a violation of this requirement, and any such violation
212 should be treated as a potential security risk to the relying parties to which the value may have been
213 given.

214 The value MUST NOT be reversible by a relying party into a non-pairwise identifier for the subject through
215 ordinary effort.

216 Relying parties should not treat this identifier as an email address for the subject as it is unlikely (though
217 not precluded) for it to be valid for that purpose. Most organizations will find that existing email address
218 values will not serve well as values for this Attribute.

219 The unique ID should not change as a result of a change to any other data associated with the subject
220 (e.g., name, email address, age, organizational role).

221 Assuming a particular scope, a given subject MUST be identified with a different, though consistent,
222 unique ID for each relying party to which a value is provided; however, the relationship between relying
223 parties and SAML entities is not defined by this profile and is interpreted from the perspective of the
224 asserting party. While it would be typical for an Identity Provider to base its notion of a relying party
225 boundary on a single Service Provider's entityID, that is not specifically required by this profile. The
226 boundary MAY be larger or even smaller, at the Identity Provider's discretion or as addressed by
227 additional profiles.

228 While it will be common in many deployments to limit values with a given scope to a single asserting party,
229 this is ultimately left to the discretion of the relying party and the use case. It is unspecified by this profile
230 whether a given value provided by two or more asserting parties correspond to the same subject. This
231 would depend on out of band arrangements made between the parties. But, in such cases, the "standard"
232 subject identifier defined in Section 3.3 is likely to be a much better choice.

233 **3.4.3 Strategies**

234 Supporting pairwise identifiers typically involves either the generation and storage of random values, or
235 the computation of reproducible values that can be produced on demand but need not be stored. This
236 profile does not require any specific approach, but implementers should be aware that some techniques
237 for computing values may result in an unacceptable risk of case conflicts. For example, a salted hash over
238 a seed identifier together with a relying party identifier produces a "safe" generated value, but becomes
239 unsafe when encoded in Base64 [RFC4648] (and the allowable character set is defined in part to preclude
240 this choice). However, encoding hashes in Base32 [RFC4648] is a safe choice, and the equals sign is
241 included in the allowable character set to accommodate this.

242 **3.4.4 Differences from "persistent" NameIDs**

243 This Attribute is a direct replacement for the `urn:oasis:names:tc:SAML:2.0:nameid-`
244 `format:persistent` NameID Format defined in SAML [SAML2Core]. There are obvious syntactic
245 differences, in a deliberate attempt at simplification. The XML syntax and data "triple" are replaced with a
246 simpler id/scope pair encoded into a string, and the awkward use of a URI to qualify the value is replaced
247 with a simpler, shorter, and more flexible approach that more easily emulates the email address syntax
248 required by many applications, and decouples identifier scoping from SAML entity naming.

249 One functional gap is the interoperable mechanism of SAML "affiliations" to group entities for the purpose
250 of targeting pairwise identifiers to multiple Service Providers, which was baked into the SAML protocol. It
251 has been left out of this profile due to the general lack of adoption by implementers or deployers in the

252 intervening years since the publication of the standard. Were there demand, it could be incorporated into a
253 future revision of this work.

254 3.5 Considerations for SAML Profiles

255 The Attributes defined in this profile are designed to be used in conjunction with any SAML profiles that
256 support the use of SAML Attributes, though its predominant expected use is with the various SAML
257 authentication profiles [SAML2Prof] such as the Browser SSO and Enhanced Client and Proxy profiles.

258 3.5.1 Requirements Signaling

259 In the event that SAML metadata [SAML2Meta] is used, a relying party MUST express its identifier
260 requirements by including an <mdattr:EntityAttribute> extension [MetaAttr] in its metadata
261 containing the following Attribute:

262 **Name:** urn:oasis:names:tc:SAML:profile:subject-id

263 **NameFormat:** urn:oasis:names:tc:SAML:2.0:attrname-format:uri

264 This Attribute, MUST contain exactly one <saml:AttributeValue> element, whose xsi:type
265 SHOULD be absent or if present MUST BE bound to the XML Schema xsd:string data type
266 [XMLSCHEMA-2].

267 The value MUST be one of the following, signaling the corresponding requirement:

- 268 • subject-id
 - 269 ◦ The relying party requires the standard identifier Attribute defined in Section 3.3.
- 270 • pairwise-id
 - 271 ◦ The relying party requires the pair-wise identifier Attribute defined in Section 3.4.
- 272 • none
 - 273 ◦ The relying party does not require any subject identifier and is designed to operate without a
274 specific user identity (e.g., with authorization based on non-identifying data).
- 275 • any
 - 276 ◦ The relying party will accept any of the identifier Attributes defined in this profile but requires
277 at least one.

278 This profile does not define specific normative behavior on the part of asserting parties in response to this
279 metadata, but it is expected that other profiles will do so in the future.

280 3.5.2 NameID Considerations

281 While the Attributes defined in this profile have as a goal the explicit replacement of the <saml:NameID>
282 element as a means of subject identification, it is certainly possible to compose them with existing NameID
283 usage provided the same subject is being identified. This can also serve as a migration strategy for
284 existing applications.

285 In addition, some profiles such as the Single Logout Profile [SAML2Prof] require the use of a
286 <saml:NameID> element, which implies the earlier use of a NameID. In such cases, it is
287 RECOMMENDED that the urn:oasis:names:tc:SAML:2.0:nameid-format:transient NameID
288 Format be used.

289 4 Conformance

290 4.1 Conformance Clause 1: Asserting Party Implementations

291 An asserting party implementation conforms to this specification if it can be configured to produce the two
292 identifier Attributes conforming to the normative requirements in Sections 3.3 and 3.4.

293 4.2 Conformance Clause 2: Relying Party Implementations

294 A relying party implementation conforms to this specification if it can be configured to consume neither,
295 either, and both of the two identifier Attributes conforming to the normative requirements in Sections 3.3
296 and 3.4.

297 If the relying party implementation provides a mechanism for generation and/or publication of SAML
298 metadata [[SAML2Meta](#)], then it MUST support the inclusion of the extension defined in Section 3.5.1.

299 **Appendix A Acknowledgments**

300 The following individuals have participated in the creation of this specification and are gratefully acknowl-
301 edged:

Contributors to the InCommon Deployment Profile Working Group

302 **Appendix B Revision History**

Revision	Date	Editor	Changes Made
WD 01	30 Aug 2017	Scott Cantor	Initial draft
WD 02	13 Sep 2017	Scott Cantor	Added considerations for other profiles
WD 03	15 Sep 2017	Scott Cantor	Added hyphen as legal character in unique ID

303