



SAML V2.0 Subject Identifier Attributes Profile Version 1.0

Committee Specification Draft 02 /
Public Review Draft 02

10 April 2018

Specification URIs

This version:

<http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/csprd02/saml-subject-id-attr-v1.0-csprd02.odt> (Authoritative)
<http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/csprd02/saml-subject-id-attr-v1.0-csprd02.html>
<http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/csprd02/saml-subject-id-attr-v1.0-csprd02.pdf>

Previous version:

<http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/csprd01/saml-subject-id-attr-v1.0-csprd01.odt> (Authoritative)
<http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/csprd01/saml-subject-id-attr-v1.0-csprd01.html>
<http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/csprd01/saml-subject-id-attr-v1.0-csprd01.pdf>

Latest version:

<http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.odt> (Authoritative)
<http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html>
<http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.pdf>

Technical Committee:

OASIS Security Services (SAML) TC

Chair:

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

Editor:

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

Related work:

This specification is related to:

- eduPerson Object Class Specification (201602)
<http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html>.

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 V2.0 `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent` Name Identifier format.

Status:

This document was last revised or approved by the OASIS Security Services (SAML) TC on the above date. The level of approval is also listed above. Check the "Latest version" location noted above for possible later revisions of this document. Any other numbered Versions and other technical work produced by the Technical Committee (TC) are listed at https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#technical.

TC members should send comments on this specification to the TC's email list. Others should send comments to the TC's public comment list, after subscribing to it by following the instructions at the "Send A Comment" button on the Technical Committee's web page at <https://www.oasis-open.org/committees/security/>.

This specification is provided 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 Work Product, 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>).

Note that any machine-readable content ([Computer Language Definitions](#)) declared Normative for this Work Product is provided in separate plain text files. In the event of a discrepancy between any 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.

Citation format:

When referencing this Work Product the following citation format should be used:

[SAML-SubjectID-v1.0]

SAML V2.0 Subject Identifier Attributes Profile Version 1.0. Edited by Scott Cantor. 10 April 2018. OASIS Committee Specification Draft 02 / Public Review Draft 02. <http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/csprd02/saml-subject-id-attr-v1.0-csprd02.html>. Latest version: <http://docs.oasis-open.org/security/saml-subject-id-attr/v1.0/saml-subject-id-attr-v1.0.html>.

Notices

Copyright © OASIS Open 2018. 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 <https://www.oasis-open.org/policies-guidelines/trademark> for above guidance.

Table of Contents

1	Introduction.....	5
1.1	IPR Policy.....	5
1.2	Terminology and Notation.....	5
1.3	Normative References.....	5
1.4	Non-Normative References.....	6
2	Motivation.....	7
2.1	Problem Statement.....	7
2.2	Relationship to Existing Work.....	8
3	SAML V2.0 Subject Identifier Attributes Profile Version 1.0.....	9
3.1	Required Information.....	9
3.2	Overview.....	9
3.3	General Purpose Subject Identifier.....	9
3.3.1	Syntax and Handling.....	9
3.3.2	Semantics and Practices.....	10
3.3.3	Example.....	11
3.4	Pairwise Subject Identifier.....	11
3.4.1	Syntax and Handling.....	11
3.4.2	Semantics and Practices.....	11
3.4.3	Strategies.....	12
3.4.4	Differences from "persistent" NameIDs.....	12
3.4.5	Example.....	12
3.5	Considerations for SAML Profiles.....	12
3.5.1	Requirements Signaling.....	12
3.5.2	NameID Considerations.....	13
4	Conformance.....	14
4.1	Conformance Clause 1: Asserting Party Implementations.....	14
4.2	Conformance Clause 2: Relying Party Implementations.....	14
Appendix A	Acknowledgments.....	15
Appendix B	Revision History.....	16

1 Introduction

1.1 IPR Policy

This specification is provided 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>.
- [RFC2234]** Crocker, D, Overell, P., “Augmented BNF for Syntax Specifications: ABNF”, RFC 2234, November 1997. <http://www.ietf.org/rfc/rfc2234.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>
- [SAML2Prof]** *Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0.* Edited by John Hughes, Scott Cantor, Jeff Hodges, Frederick Hirsch, Prateek Mishra, Rob Philpot, Eve Maler. 15 March 2005. OASIS Standard. <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>
- [XMLSCHEMA-2]** *XML Schema Part 2: Datatypes Second Edition.* Paul V. Biron, A. Malhotra, Editors. W3C Recommendation. October 28, 2004. <http://www.w3.org/TR/2004/REC-xmlschema-2-20041028/>. Latest version: <http://www.w3.org/TR/xmlschema-2/>.

17 1.4 Non-Normative References

- [eduPerson]** Internet2, “eduPerson Object Class Specification (201602)”, February 2016. <http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html>.
- [RFC4648]** Josefson, S., “The Base16, Base32, and Base64 Data Encodings”, RFC 4648, October 2006. <http://www.ietf.org/rfc/rfc4648.txt>.

18 2 Motivation

19 2.1 Problem Statement

20 Identification of subjects in security protocols and applications has a fraught history of inconsistent syntax,
21 bugs, terrible but deeply cemented practices such as misuse of email addresses, vertical market-specific
22 approaches, and failure to precisely communicate intended semantics and constraints. These problems
23 lead to overly complex burdens on both asserting and relying parties to issue and consume a variety of
24 different identifiers in different formats, many of which work poorly with off the shelf applications. Much of
25 this is self-inflicted fragmentation due to the constant tension between fixing problems with new solutions
26 and avoiding new solutions to ensure wider adoption.

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

32 This, together with inconsistent technical precision by implementers and deployers, creates complexity.
33 Deployment experience has shown that use of the NameID feature is confusing in many implementations.
34 It also, through its presence in the SAML Single Logout protocol, potentially appears (indirectly but
35 recoverably) in web access logs, leading to the added complexity of encryption when privacy is a
36 consideration.

37 There is a general consensus by most federated identity practitioners around a few common
38 requirements:

- 39 • Identifiers should be as stable as possible and should have little or no risk of reassignment to
40 different subjects due to the lack of tight synchronization¹ inherent between loosely-coupled
41 systems.
- 42 • Opaque (i.e., superficially random) identifiers are inherently more stable than name-based
43 identifiers or email addresses in many organizations.
- 44 • Identifiers should be compact and simple to handle and manipulate.
- 45 • The ability to clearly express the scope of an identifier's uniqueness and enforce policy stipulating
46 the asserting parties permitted to issue an identifier is crucial to federated systems and the lack of
47 such policy has led to widely-publicized breaches.

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

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

56 Pairwise identification may help meet certain privacy and regulatory requirements (though this is far from
57 clear to date), but does not address many common use cases that demand cross-system correlation
58 without the friction of complex linking protocols and the involvement of the data subject.

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.

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

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

68 **2.2 Relationship to Existing Work**

69 A clean slate notwithstanding, this profile is based on a thorough review of practice within the higher
70 education sector, which has seen extensive adoption of SAML and partially-successful efforts to
71 standardize subject identification and avoid the "email address" trap that most of the technical world fell
72 into many years ago.

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

- 75 • Experience with the SAML "persistent" NameID construct and the related eduPersonTargetedID
76 attribute.
- 77 • The eduPersonPrincipalName and eduPersonUniqueid attributes, the former successful but
78 deeply flawed, the latter less successful but more carefully defined.
- 79 • Success with DNS domain-based scoping of values and managing policy around their use in
80 SAML.
- 81 • Challenges in the adoption of profiles required to accommodate the limitations of widely deployed
82 identifiers.

83 Portions of this specification are borrowed liberally from the [\[eduPerson\]](#) specification in a deliberate
84 desire to remain consistent with the formulation of the eduPersonUniqueid attribute.

85 3 SAML V2.0 Subject Identifier Attributes Profile 86 Version 1.0

87 3.1 Required Information

88 **Identification:** urn:oasis:names:tc:SAML:profiles:subject-id

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

90 **Description:** Given below.

91 **Updates:** None.

92 3.2 Overview

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

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

99 In the terminology used in this profile:

- 100 • "asserting party" refers to a uniquely-named SAML entity that issues assertions containing one or
101 both of these Attributes
- 102 • "relying party" refers to one or more uniquely-named SAML entities that receive assertions
103 containing one or both of these Attributes

104 In addition, this profile defines a signaling mechanism for a relying party to express its subject
105 identification requirements via SAML metadata [[SAML2Meta](#)], by means of the
106 <mdattr:EntityAttributes> extension [[MetaAttr](#)]. This allows asserting parties to unambiguously
107 understand the requirements of a peer and facilitates deployment profiles that wish to mandate support for
108 one or both of these Attributes, while maintaining appropriate privacy expectations.

109 3.3 General Purpose Subject Identifier

110 For general purpose identification of subjects, the following SAML Attribute is defined:

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

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

113 This is a long-lived, non-reassignable, omni-directional identifier suitable for use as a globally-unique
114 external key. Its value for a given subject is independent of the relying party to whom it is given.

115 3.3.1 Syntax and Handling

116 The <saml:Attribute> element MUST contain exactly one <saml:AttributeValue> element,
117 whose xsi:type SHOULD be absent or if present MUST BE bound to the XML Schema xsd:string
118 data type [[XMLSCHEMA-2](#)].

119 Any leading or trailing whitespace, as defined by XML (ASCII 32, ASCII 9, ASCII 10, ASCII 13), present in
120 the <saml:AttributeValue> element's content is not significant and MUST be stripped by the relying
121 party prior to evaluation or comparison.

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

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

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

130 The ABNF [RFC2234] grammar is therefore:

131 <value> = <uniqueID> "@" <scope>

132 <uniqueID> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "=" / "-")

133 <scope> = (ALPHA / DIGIT) 0*126(ALPHA / DIGIT / "-" / ".")

134 Value comparison MUST be performed case-insensitively (that is, values that differ only by case are the
135 same, and MUST refer to the same subject).

136 In the grammar above, only the ALPHA production contains characters that can be expressed in both
137 upper and lower case. It is RECOMMENDED that alphabetic characters be in lower-case when
138 expressing and storing values to facilitate ease of comparison.

139 3.3.2 Semantics and Practices

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

142 The relationship between an asserting party and a scope is an arbitrary one and does not reflect any
143 assumed relationship between a scope in the form of a domain name and a domain found in a given
144 SAML entity identifier.

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

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

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

154 A given value MUST identify the same subject regardless of the context of use or the relying parties to
155 which the Attribute is given. It is therefore to be assumed by relying parties that receive a given value that
156 the same subject has been identified.

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

161 A single subject MAY be identified simultaneously by a single asserting party by multiple values, but this
162 should be minimized to the extent possible.

163 3.3.3 Example

164 The following is an example of the SAML Attribute defined in this section:

```
165 <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:subject-id"  
166     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
167   <saml:AttributeValue>idm123456789@example.com</saml:AttributeValue>  
168 </saml:Attribute>
```

169 3.4 Pairwise Subject Identifier

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

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

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

173 This is a long-lived, non-reassignable, uni-directional identifier suitable for use as a unique external key
174 specific to a particular relying party. Its value for a given subject depends upon the relying party to whom it
175 is given, thus preventing unrelated systems from using it as a basis for correlation.

176 3.4.1 Syntax and Handling

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

179 3.4.2 Semantics and Practices

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

184 The relationship between an asserting party and a scope is an arbitrary one and does not reflect any
185 assumed relationship between a scope in the form of a domain name and a domain found in a given
186 SAML entity identifier.

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

191 The value MUST NOT be mappable by a relying party into a non-pairwise identifier for the subject through
192 ordinary effort. This precludes the degenerate case of providing a non-pairwise value to all relying parties
193 for a given subject.

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

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

199 Assuming a particular scope, a given subject MUST be identified with a different, though consistent,
200 unique ID for each relying party to which a value is provided; however, the relationship between relying
201 parties and SAML entities is not defined by this profile and is interpreted from the perspective of the
202 asserting party. For example, in the context of the SAML Web Browser SSO profile [[SAMLProf](#)] it would
203 be typical for an Identity Provider to base its notion of a relying party boundary on a single Service
204 Provider's entity identifier, but that is not specifically required by this profile. The boundary MAY be larger
205 or even smaller, at the Identity Provider's discretion or as addressed by additional profiles.

206 While it will be common in many deployments to limit values with a given scope to a single asserting party,
207 this is ultimately left to the discretion of the relying party and the use case. It is unspecified by this profile

208 whether a given value provided by two or more asserting parties correspond to the same subject. This
209 would depend on out of band arrangements made between the parties. But, in such cases, the "standard"
210 subject identifier defined in Section 3.3 is likely to be a much better choice.

211 3.4.3 Strategies

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

220 3.4.4 Differences from "persistent" NameIDs

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

227 One functional gap is the interoperable mechanism of SAML "affiliations" to group entities for the purpose
228 of targeting pairwise identifiers to multiple Service Providers, which was baked into the SAML protocol. It
229 has been left out of this profile due to the general lack of adoption by implementers or deployers in the
230 intervening years since the publication of the standard. Were there demand, it could be incorporated into a
231 future revision of this work.

232 3.4.5 Example

233 The following is an example of the SAML Attribute defined in this section:

```
234 <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:pairwise-id"  
235     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
236   <saml:AttributeValue>  
237   HA2TKNZZGE2TOZDCGMZWKOLDHBQWIMBSGM4TGZBYGUYGINRQHAYTINBZGYZDOZBZMZRGKNZTME3TMN  
238   BXGYTTIOBYGMYWKNLFMYDAYY=@osu.edu  
239   </saml:AttributeValue>  
240 </saml:Attribute>
```

241 3.5 Considerations for SAML Profiles

242 The Attributes defined in this profile are designed to be used in conjunction with any SAML profiles that
243 support the use of SAML Attributes, though its predominant expected use is with the various SAML single
244 sign-on profiles [SAML2Prof] such as the Web Browser SSO Profile and Enhanced Client or Proxy (ECP)
245 Profile.

246 3.5.1 Requirements Signaling

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

250 **Name:** `urn:oasis:names:tc:SAML:profiles:subject-id:req`

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

252 This Attribute, MUST contain exactly one `<saml:AttributeValue>` element, whose `xsi:type`
253 SHOULD be absent or if present MUST BE bound to the XML Schema `xsd:string` data type
254 [[XMLSCHEMA-2](#)].

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

- 256 • `subject-id`
 - 257 ◦ The relying party requires the standard identifier Attribute defined in Section 3.3.
- 258 • `pairwise-id`
 - 259 ◦ The relying party requires the pair-wise identifier Attribute defined in Section 3.4.
- 260 • `none`
 - 261 ◦ The relying party does not require any subject identifier and is designed to operate without a
 - 262 specific user identity (e.g., with authorization based on non-identifying data).
- 263 • `any`
 - 264 ◦ The relying party will accept any of the identifier Attributes defined in this profile but requires at
 - 265 least one.

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

268 This profile does not provide (nor preclude) any guidance around the use of the
269 `<md:RequestedAttribute>` element for signaling requirements, but notably it is impossible without
270 additional specification work to reflect the semantics of the `any` value defined above using that
271 mechanism.

272 **3.5.2 NameID Considerations**

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

277 Some profiles such as the Single Logout Profile [[SAML2Prof](#)] require the use of a `<saml:NameID>`
278 element, which implies the earlier use of a NameID. In such cases, it is RECOMMENDED that the
279 `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` NameID Format be used.

280 This specification does not define any syntax by which the SAML Attributes defined within would be used
281 directly within the NameID construct. Such use is discouraged, but is not within the scope of this
282 specification.

283 4 Conformance

284 4.1 Conformance Clause 1: Asserting Party Implementations

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

287 4.2 Conformance Clause 2: Relying Party Implementations

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

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

293 **Appendix A Acknowledgments**

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

Scott Cantor, Internet2
Thomas Hardjono, MIT
Mohammad Jafari, Veterans Health Administration
Hal Lockhart, Oracle Corporation
Madalina Sultan, Connectis

Contributors to the InCommon Deployment Profile Working Group

296 **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
WD 04	1 Feb 2018	Scott Cantor	Many nits, missing references, clarifying changes in response to public review

297