



# SAML V2.0 Subject Identifier Attributes Profile Version 1.0

~~Working Committee Specification Draft 02~~  
~~Public Review Draft 025~~

~~109 April~~ July 2018

## Specification URIs

### ~~This~~ Previous 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](mailto:hardjono@mit.edu)), M.I.T.

## Editor:

Scott Cantor ([cantor.2@osu.edu](mailto: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](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 <a href="#">[SAML2Core]</a> .
samlp:	urn:oasis:names:tc:SAML:2.0:protocol	This is the SAML V2.0 protocol namespace <a href="#">[SAML2Core]</a> .
md:	urn:oasis:names:tc:SAML:2.0:metadata	This is the SAML V2.0 metadata namespace <a href="#">[SAML2Meta]</a> .
mdattr:	urn:oasis:names:tc:SAML:metadata:attributes	This is the SAML V2.0 metadata extension for entity attributes namespace <a href="#">[MetaAttr]</a> .
xsd:	<a href="http://www.w3.org/2001/XMLSchema">http://www.w3.org/2001/XMLSchema</a>	This namespace is defined in the W3C XML Schema specification <a href="#">[XMLSCHEMA-2]</a> .

## 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>.
- [ShibMetaExt]** **Shibboleth Project**, “Shibboleth Metadata Extensions V1.0”, July 2018. <https://wiki.shibboleth.net/confluence/x/QACt>.

---

## 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 synchronization<sup>1</sup> 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 ASCII characters, ~~at each of which is~~ either an alphanumeric  
125 ASCII character or the, an equals sign (ASCII 61), or a hyphen (ASCII 45). The first character MUST be  
126 alphanumeric.

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

133 The ABNF [RFC2234] grammar is therefore:

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

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

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

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

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

### 142 3.3.2 Semantics and Practices

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

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

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

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

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

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

161 Note that, policy permitting, a given value could be provided by any asserting party, and the requirement  
162 still holds: identical values correspond to the same subject. While it will be common in many deployments

163 to limit values with a given scope to a single asserting party, this is ultimately left to the discretion of the  
164 relying party and the use case.

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

### 167 3.3.3 Example

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

```
169 <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:subject-id"  
170     NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
171     <saml:AttributeValue>idm123456789@example.com</saml:AttributeValue>  
172 </saml:Attribute>
```

## 173 3.4 Pairwise Subject Identifier

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

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

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

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

### 180 3.4.1 Syntax and Handling

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

### 183 3.4.2 Semantics and Practices

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

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

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

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

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

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

204 Assuming a particular scope, a given subject MUST be identified with a different, though consistent,  
205 unique ID for each relying party to which a value is provided; however, the relationship between relying

206 parties and SAML entities is not defined by this profile and is interpreted from the perspective of the  
207 asserting party. For example, in the context of the SAML Web Browser SSO profile [[SAMLProf](#)] it would  
208 be typical for an Identity Provider to base its notion of a relying party boundary on a single Service  
209 Provider's entity identifier, but that is not specifically required by this profile. The boundary MAY be larger  
210 or even smaller, at the Identity Provider's discretion or as addressed by additional profiles.

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

### 216 3.4.3 Strategies

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

### 225 3.4.4 Differences from "persistent" NameIDs

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

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

### 237 3.4.5 Example

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

```
239 <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:pairwise-id"  
240   NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">  
241   <saml:AttributeValue>  
242   HA2TKNZZGE2TOZDCGMZWKOLDHQBQWIMBSGM4TGZBYGUYGINRQHAYTINBZGYZDOZBZMZRGKNZTME3TMN  
243   BXGYTYIOBYGMYWKNLFMYDAYY=@osu.edu  
244   </saml:AttributeValue>  
245 </saml:Attribute>
```

## 246 3.5 Considerations for SAML Profiles

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

### 251 3.5.1 Requirements Signaling

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

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

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

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

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

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

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

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

### 277 3.5.2 NameID Considerations

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

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

285 This specification does not define any syntax by which the SAML Attributes defined within would be used  
286 directly within the NameID construct. Such use is discouraged, but is not within the scope of precluded by  
287 this specification. In practice, the most appropriate mechanism to express any string-valued SAML  
288 Attribute in a <saml:NameID> element is to express the Attribute's Name as a Format and omit any  
289 qualifiers, and such an approach is safe to use with the Attributes defined in this specification.

### 290 | **3.5.3 Security Considerations**

291 | All identifiers have inherent and generally well-understood concerns; most applications traditionally  
292 | associate users directly with resources, privileges, and/or data by uniquely identifying those users and  
293 | remembering them during subsequent interactions. Federated protocols don't alter these concerns, but  
294 | can complicate them because of the particular issues introduced by mutiple asserting parties that may (but  
295 | usually do not) share a common identifier namespace.

296 | Applications not originally designed to support federation often treat each asserting party as a kind of silo  
297 | of identity, and the identifiers used are inherently segregated by these silos such that global uniqueness  
298 | (or lack thereof) is irrelevant. In such cases, the asserting party's own identifier acts as an implicit "scope"  
299 | for all of the identifiers it asserts. In some cases, a lack of this implicit enforcement of scope has led to  
300 | security vulnerabilities involving impersonation of users across asserting parties, demonstrating that, no  
301 | matter what kind of identifier is used, some form of scoping of user identifiers is an absolute necessity in  
302 | federated systems. This requirement is more obvious when applications are truly federated and combine  
303 | identifiers from multiple asserting parties within a data set.

304 | The identifier attributes defined in this specification contain an explicit scope as part of their syntax,  
305 | providing globally uniqueness, but, more subtly, creating indirection between the scopes and the asserting  
306 | party or parties that provide them. That is, the scope is explicit, but the relationship between that scope  
307 | and an asserting party is indirect, at least when looking solely at the identifier. This indirection adds power,  
308 | in that use cases involving identity linking between asserting parties become simpler to support, and it  
309 | adds simplicity from the point of view of safe handling of identifier values since the scope is harder to  
310 | "lose" or ignore. But this also adds complexity because a policy decision is required to authorize an  
311 | asserting party to supply identifiers in a given scope.

312 | As an example, consider an identifier such as "abcdef123@osu.edu"; SAML doesn't define anything in its  
313 | core machinery that associates "osu.edu" with the Identity Provider representing The Ohio State  
314 | University. Domain ownership proofs are of course a common and sensible practice to use to establish  
315 | this association, but nothing in SAML specifies that, so it's an additional step.

316 | This specification does not define a single such policy layer, principally because the most common  
317 | community of practice from which it has emerged already has one based on a proprietary SAML metadata  
318 | extension [ShibMetaExt] that associates authorized scope values with asserting parties. By using SAML  
319 | metadata, the problem of self-assertion is addressed; if an asserting party were able to self-authorize its  
320 | ability to supply an identifier in a different asserting party's scope, impersonation becomes easy.  
321 | Communities that rely on curated, third-party sources of metadata have a vehicle for automating policy  
322 | around scopes, and for off-loading domain/scope verification. Thus, use of metadata in this fashion and  
323 | use of scoped identifiers become mutually reinforcing.

---

## 324 4 Conformance

### 325 4.1 Conformance Clause 1: Asserting Party Implementations

326 | An asserting party implementation conforms to this specification if it can be configured to produce ~~the-~~  
327 | ~~two~~ identifier Attributes conforming to the normative requirements in Sections 3.3 and 3.4.

### 328 4.2 Conformance Clause 2: Relying Party Implementations

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

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

---

334 **Appendix A Acknowledgments**

335 The following individuals have participated in the creation of this specification and are gratefully acknowl-  
336 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



---

337 **Appendix B Revision History**

<b>Revision</b>	<b>Date</b>	<b>Editor</b>	<b>Changes Made</b>
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

338