

1 Entity Selection Profile entity attribute

2 Draft for community consultation

3 12 March 2025

4 Motivation

5 Federation operators have rules for entity registration to ensure a good user experience within
6 that federation. These rules are typically published in a Metadata Registration Practice
7 Statement. When we look at a wider ecosystem where multiple federation operators register
8 SPs and IdPs, we need prioritization and selection rules. The rule that many people know about
9 is the metadata combination rule in eduGAIN metadata aggregation, which enforces unique
10 entityIDs.

11 However, unique entityIDs are not sufficient to provide a good user experience in an
12 ecosystem. Accurate and complete metadata (such as DisplayName and logos) will help
13 people select the appropriate IdP when logging in, although this still requires an individual to
14 make the correct choice at login time. What if there was also a mechanism in metadata for an
15 SP to describe which IdPs it would prefer to interoperate with? This Entity Selection Profile
16 aims to provide that.

17 Building on earlier work from SeamlessAccess, we are developing a profile that can allow SPs
18 to identify a set of IdPs, either by entityID or generically by registrationAuthority or entity
19 attribute. They coined the term “trustinfo” although we’re realising it’s actually an entity
20 selection profile.

21 The first step is to define an entity attribute as a container for transporting selection rules and
22 profiles. This step focusses on the current SAML environment.

23 There is supporting material in the REFEDS wiki on the Working Group page [WG]

24 XML namespaces and prefixes

25 Conventional namespace prefixes are used

Namespace prefix	Namespace	Reference
md:	urn:oasis:names:tc:SAML:2.0:metadata	SAML2Meta
mdattr:	urn:oasis:names:tc:SAML:metadata:attributes	MetaAttr

26

27 Definitions

28 The Entity Selection Profile is an entity attribute which contains filtering rules. These filtering
29 rules allow SP owners and others to define selection rules for which IdPs to display in a
30 discovery service.

31 The entity attribute has Name="https://refeds.org/entity-selection-profile"
32 and NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"

33 Syntax

34 The entity attribute is found in md:EntityDescriptor/md:Extensions/
35 mdattr:EntityAttributes. We recognise that the Entity Attributes specification allows
36 md:EntitiesDescriptor/md:Extensions/md:EntityAttributes elements, but
37 we rule them out for operational and conceptual reasons.

38 There is only one instance of an Entity Selection Profile entity attribute in an entity. Behaviour
39 when more than one is present is not defined by this profile.

40 Composition with other sources of filtering is not defined by this profile

41 The value of the entity attribute is a JSON data structure that has been Base64 encoded
42 [Base64]

43 Any whitespace before, after or internal to the value must be ignored

44 Semantics

45 The expected consumer of the entity attribute is a discovery service. Federation operators and
46 entity operators are not expected to decode the value.

47 Semantics of the decoded value are defined by the metadata consumer.

48 We recommend that null values, incorrectly encoded values or other errors are treated as if
49 there was no filtering. We do not recommend that the whole entity metadata is considered
50 invalid.

51 If the decoded value does not conform to the requirements of the consumer, we recommend
52 that the consumer assumes there is no filtering. We do not recommend that the entity
53 metadata is considered invalid.

54 Registration criteria

55 Any entity that has a SP role can register this entity attribute

56 Examples

57 This example contains JSON which defines profiles for filtering in
58 SeamlessAccess

```
59 <mdattr:EntityAttributes>
60   <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
61   format:uri"
62     Name="https://refeds.org/entity-selection-profile">
63     <saml:AttributeValue>
64 eyJwcm9maWxlcYI6eyJzd2FtaWQtb25seSI6eyJzdHJpY3QiOnRydWUsImVudGl0aWV
65 zIjpbeyJzZWx1Y3QiOiJodHRwOi8vd3d3LnN3YW1pZC5zZS8iLCJtYXRjaCI6InJlZ2
66 lzdHJhdGlvbKFI6dGhvcml0eSIsImluY2x1ZGUiOnRydWV9XX0sImVkdWdhaW4iOnsiZ
67 W50aXRpZXMlOi8t7ImluY2x1ZGUiOmZhbnN1LCJtYXRjaCI6InJlZ2lzdHJhdGlvbKFI
68 dGhvcml0eSIsInNlbGVjdCI6Imh0dHBzOi8vb3BlbmF0aGVucy5uZXQifV0sInN0cm1
69 jdCI6IHJydWV9fX0=
70     </saml:AttributeValue>
71   </saml:Attribute>
72 </mdattr:EntityAttributes>
```

```
73 The filtering rule is {"profiles":{"swamid-
74 only":{"strict":true,"entities":[{"select":"http://www.swamid.se/",
75 "match":"registrationAuthority","include":true}]},"edugain":{"entit
76 ies":[{"include":false,"match":"registrationAuthority","select":"ht
77 tps://openathens.net"}],"strict": true}}}
```

78 This non-functional example has an entity attribute with no value

79 The metadata consumer should ignore the attribute and perform no filtering.

```
80 <mdattr:EntityAttributes>
81   <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
82   format:uri"
83     Name="https://refeds.org/entity-selection-profile">
84     <saml:AttributeValue />
85   </saml:Attribute>
86 </mdattr:EntityAttributes>
```

87 This non-functional example contains a space

88 The metadata consumer should ignore the attribute and perform no filtering.

```
89 <mdattr:EntityAttributes>
90   <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
91   format:uri"
92     Name="https://refeds.org/entity-selection-profile">
93     <saml:AttributeValue> </saml:AttributeValue>
94   </saml:Attribute>
95 </mdattr:EntityAttributes>
```

96 This non-functional example contains an incorrectly encoded value

97 The metadata consumer should ignore the attribute and perform no filtering.

```
98 <mdattr:EntityAttributes>
99   <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
100   format:uri"
101     Name="https://refeds.org/entity-selection-profile">
102     <saml:AttributeValue>*</saml:AttributeValue>
103   </saml:Attribute>
104 </mdattr:EntityAttributes>
```

105 Security considerations

106 to be determined

107 References

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

111 MetaAttr - SAML V2.0 Metadata Extension for Entity Attributes Version 1.0. Edited by Scott
112 Cantor. 4 August 2009. OASIS Committee Specification. [http://docs.oasis-](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr-cs-01.pdf)
113 [open.org/security/saml/Post2.0/sstc-metadata-attr-cs-01.pdf](http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-attr-cs-01.pdf).

114 Base64 - The Base16, Base32, and Base64 Data Encodings. RFC 4648.
115 <https://datatracker.ietf.org/doc/html/rfc4648>

116 WG - REFEDS wiki page for the working group.
117 [https://wiki.refeds.org/display/GROUPS/SeamlessAccess+Trustinfo+Metadata+Working+Grou](https://wiki.refeds.org/display/GROUPS/SeamlessAccess+Trustinfo+Metadata+Working+Group)
118 [p](https://wiki.refeds.org/display/GROUPS/SeamlessAccess+Trustinfo+Metadata+Working+Group)