



2 **Identity Assurance Hub Service Profile –**
3 **SAML Attributes v1.2a**

4 **Identity Assurance Programme, 7 August 2015**

5 **Document identifier:**

6 IDAP/HubService/Profiles/SAML/Attributes

7 **Editors:**

8 Mike Pegman, Department for Work and Pensions

9 Adam Cooper, Government Digital Service

10 Stephen Dunn, Government Digital Service

11

12 **Previous Contributors:**

13 Paul Toal, Oracle UK Ltd

14 Brandon Murdoch, Microsoft UK Ltd

15 Additional review and contributions were made by CESG.

16 **Abstract:**

17 This specification defines a profile for the use of SAML assertions and request-response
18 messages to be used between participants in the Identity Assurance federation architecture.

19

20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42

Table of Contents

1	Introduction	3
1.1	Notation	3
2	SAML Attributes	4
2.1	Required Information	4
2.2	SAML Attribute Naming.....	4
2.2.1	Attribute Name Comparison	4
2.3	Profile-Specific XML Attributes.....	4
2.4	SAML Attribute Values	4
2.5	Matching Dataset Attribute Definitions	9
2.5.1	Firstname.....	9
2.5.2	Surname	9
2.5.3	Middle Name(s).....	9
2.5.4	Date of Birth	10
2.5.5	Gender.....	10
2.5.6	Current Address	10
2.5.7	Previous Address	11
2.6	Authentication Event Assertion Attribute Definitions.....	11
2.6.1	IPAddress.....	11
2.7	Fraud Event Contextual Information Assertion Attribute Definitions.....	12
2.7.1	GPG45Status.....	12
2.7.2	IDPFraudEventID	12

43
44
45
46
47
48
49
50
51
52
53
54
55
56

1 Introduction

The Identity Assurance Hub Service SAML v2.0 Profile describes how service providers offering online government services can use any number of Hub Services for the brokering of a citizen authentication and enrichment of citizen attributes.

This document describes the SAML Attributes to be used in conjunction with the Hub Service SAML 2.0 Profile.

1.1 Notation

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

```
Schema listings appear like this.
```

```
Example code listings appear like this.
```

57 2 SAML Attributes

58 This section details the Matching Dataset attributes and mandatory attributes supported by this profile for
59 the expressing of data related to the SAML assertion subject.

60 2.1 Required Information

61 **Identification:** `http://www.cabinetoffice.gov.uk/resource-library/ida/attributes` (this corresponds to the
62 target namespace specified in the schema in section 2.4)

63 2.2 SAML Attribute Naming

64 The `NameFormat` XML attribute in `<Attribute>` elements MUST be
65 `urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified` unless otherwise specified in
66 the schema.

67 The XML attribute `Name` value MUST be one of the descriptors defined in section 2.4.

68 The optional XML attribute `FriendlyName` value, if present, MUST be one of the friendly descriptors
69 associated with the `Name` descriptor. Examples are included later in this document for clarity.

70 2.2.1 Attribute Name Comparison

71 `<Attribute>` elements refer to the same SAML attribute if and only if the `Name` XML attribute values are
72 equal.

73 2.3 Profile-Specific XML Attributes

74 This following profile-specific XML attributes MAY be specified for an `<AttributeValue>` element as
75 specified in the schema in section 2.4:

- 76 • `From`, a date constructed in accordance with the W3C Date and Time Formats Specification at
77 `http://www.w3.org/TR/NOTE-datetime`.
- 78 • `To`, a date constructed in accordance with the W3C Date and Time Formats Specification at
79 `http://www.w3.org/TR/NOTE-datetime`
- 80 • `Language`, represents natural language identifiers as defined by [RFC 3066] with a default of
81 "en-GB".
- 82 • `Order`, represents the order in which an `<AttributeValue>` element MUST be processed
83 when multiple attribute values exist for and `<Attribute>`. Starting at 1 with increments of 1.
- 84 • `Verified`, denotes an `<AttributeValue>` as being verified or not in accordance with GPG45.

85 2.4 SAML Attribute Values

86 The schema type of the contents of the `<AttributeValue>` element MUST be drawn from one of the
87 types specified below. The `xsi:type` attribute MUST be present and be given the appropriate value.

88
89 The following schema defines the XML attributes and complex types supported by this profile:
90

```
91  
92 <xs:schema  
93     xmlns:xs="http://www.w3.org/2001/XMLSchema"  
94     xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"  
95     xmlns="http://www.cabinetoffice.gov.uk/resource-  
96 library/ida/attributes"  
97     elementFormDefault="qualified"  
98     attributeFormDefault="qualified"  
99     blockDefault="substitution"  
100     targetNamespace="http://www.cabinetoffice.gov.uk/resource-  
101 library/ida/attributes">
```

```

102 <xs:annotation>
103     <xs:documentation>
104     </xs:documentation>
105 </xs:annotation>
106
107 <xs:attribute name="From" type="FormattedDateType"/>
108 <xs:attribute name="To" type="FormattedDateType"/>
109 <xs:attribute name="Language" type="xs:language" default="en-GB"/>
110 <xs:attribute name="Order" type="xs:integer"/>
111 <xs:attribute name="Verified" type="xs:boolean" default="false"/>
112
113 <xs:complexType name="AddressType">
114     <xs:annotation>
115         <xs:documentation>A FormattedAddressType
116         </xs:documentation>
117     </xs:annotation>
118     <xs:complexContent>
119         <xs:extension base="FormattedAddressType">
120             <xs:attribute ref="Language"/>
121             <xs:attribute ref="From"/>
122             <xs:attribute ref="To"/>
123             <xs:attribute ref="Verified"/>
124         </xs:extension>
125     </xs:complexContent>
126 </xs:complexType>
127
128 <xs:complexType name="FormattedAddressType" mixed="true">
129     <xs:sequence>
130         <xs:element name="Line" type="AddressLineType" minOccurs="1"
131             maxOccurs="5"/>
132         <xs:element name="PostCode" type="PostCodeType"
133 minOccurs="0"/>
134         <xs:element name="InternationalPostCode"
135 type="InternationalPostCodeType"
136             minOccurs="0"/>
137         <xs:element name="UPRN" type="UPRNType" minOccurs="0"/>
138     </xs:sequence>
139 </xs:complexType>
140
141 <xs:simpleType name="AddressLineType">
142     <xs:annotation>
143         <xs:documentation>A FormattedStringType restricted in length
144         </xs:documentation>
145     </xs:annotation>
146     <xs:restriction base="FormattedStringType">
147         <xs:minLength value="1"/>
148         <xs:maxLength value="100"/>
149     </xs:restriction>
150 </xs:simpleType>
151
152 <xs:simpleType name="DateTimeType">
153     <xs:annotation>
154         <xs:documentation>A date and time constructed in accordance
155 with the
156             W3C Date and Time Formats Specification at
157             http://www.w3.org/TR/NOTE-datetime.
158         </xs:documentation>
159     </xs:annotation>

```

```

160     <xs:restriction base="xs:string">
161         <xs:pattern value="(\\d\\d\\d\\d) (- (\\d\\d) (-
162 (\\d\\d) (T(\\d\\d):(\\d\\d) (: (\\d\\d) (\\.\\d+)?)?Z)?)?)?"/>
163     </xs:restriction>
164 </xs:simpleType>
165
166 <xs:simpleType name="FormattedDateType">
167     <xs:annotation>
168         <xs:documentation>A date constructed in accordance with the
169             W3C Date and Time Formats Specification at
170             http://www.w3.org/TR/NOTE-datetime.
171         </xs:documentation>
172     </xs:annotation>
173     <xs:restriction base="xs:string">
174         <xs:pattern value="(\\d\\d\\d\\d) (- (\\d\\d) (- (\\d\\d)?)?)?"/>
175     </xs:restriction>
176 </xs:simpleType>
177
178 <xs:complexType name="DateType">
179     <xs:annotation>
180         <xs:documentation>A FormattedDateType e.g. DoB
181     </xs:documentation>
182 </xs:annotation>
183 <xs:simpleContent>
184     <xs:extension base="FormattedDateType">
185         <xs:attribute ref="From"/>
186         <xs:attribute ref="To"/>
187         <xs:attribute ref="Verified"/>
188     </xs:extension>
189 </xs:simpleContent>
190 </xs:complexType>
191
192 <xs:simpleType name="EmailAddressType">
193     <xs:annotation>
194         <xs:documentation>Base email address type
195     </xs:documentation>
196 </xs:annotation>
197     <xs:restriction base="xs:string">
198         <xs:minLength value="3"/>
199         <xs:maxLength value="254"/>
200     </xs:restriction>
201 </xs:simpleType>
202
203 <xs:simpleType name="FormattedStringType">
204     <xs:annotation>
205         <xs:documentation>Base type for string use
206     </xs:documentation>
207 </xs:annotation>
208     <xs:restriction base="xs:string">
209         <xs:minLength value="0"/>
210         <xs:maxLength value="512"/>
211     </xs:restriction>
212 </xs:simpleType>
213
214 <xs:simpleType name="SimpleGenderType">
215     <xs:restriction base="xs:string">
216         <xs:enumeration value="Male"/>
217         <xs:enumeration value="Female"/>

```

```

218         <xs:enumeration value="Not Specified"/>
219     </xs:restriction>
220 </xs:simpleType>
221
222 <xs:complexType name="GenderType">
223     <xs:annotation>
224         <xs:documentation>A SimpleGenderType
225     </xs:documentation>
226 </xs:annotation>
227     <xs:simpleContent>
228         <xs:extension base="SimpleGenderType">
229             <xs:attribute ref="From"/>
230             <xs:attribute ref="To"/>
231             <xs:attribute ref="Verified"/>
232         </xs:extension>
233     </xs:simpleContent>
234 </xs:complexType>
235
236 <xs:simpleType name="PostCodeType">
237     <xs:annotation>
238         <xs:documentation>Type derived from xs:string with a pattern
239             restriction to UK Post Codes
240     </xs:documentation>
241 </xs:annotation>
242     <xs:restriction base="xs:string">
243         <xs:pattern
244             value="[A-Z]{1,2}[0-9R][0-9A-Z]? [0-9][A-Z-
245 [CIKMOV]]{2}"/>
246     </xs:restriction>
247 </xs:simpleType>
248
249 <xs:simpleType name="InternationalPostCodeType">
250     <xs:annotation>
251         <xs:documentation>Type derived from xs:string representing an
252             international postal code
253     </xs:documentation>
254 </xs:annotation>
255     <xs:restriction base="xs:string">
256         <xs:minLength value="1"/>
257         <xs:maxLength value="20"/>
258     </xs:restriction>
259 </xs:simpleType>
260
261 <xs:simpleType name="UPRNType">
262     <xs:annotation>
263         <xs:documentation>Type derived from xs:string representing a
264 UPRN
265     </xs:documentation>
266 </xs:annotation>
267     <xs:restriction base="xs:string">
268         <xs:minLength value="1"/>
269         <xs:maxLength value="12"/>
270     </xs:restriction>
271 </xs:simpleType>
272
273 <xs:simpleType name="IPAddressType">
274     <xs:annotation>
275         <xs:documentation>Simple IP Address type

```

```

276         </xs:documentation>
277     </xs:annotation>
278     <xs:restriction base="xs:string">
279         <xs:minLength value="7"/>
280         <xs:maxLength value="128"/>
281     </xs:restriction>
282 </xs:simpleType>
283
284 <xs:simpleType name="GPG45StatusType">
285     <xs:annotation>
286         <xs:documentation>GPG45 Status code, see latest version of
287 GPG45 and the operations manual for required values
288     </xs:documentation>
289     </xs:annotation>
290     <xs:restriction base="xs:string">
291         <xs:minLength value="4"/>
292         <xs:maxLength value="8"/>
293     </xs:restriction>
294 </xs:simpleType>
295
296 <xs:simpleType name="IDPFraudEventIDType">
297     <xs:annotation>
298         <xs:documentation>Unique fraud event ID
299     </xs:documentation>
300     </xs:annotation>
301     <xs:restriction base="xs:string">
302         <xs:minLength value="12"/>
303         <xs:maxLength value="100"/>
304     </xs:restriction>
305 </xs:simpleType>
306
307 <xs:complexType name="PersonNameType">
308     <xs:annotation>
309         <xs:documentation>A FormattedStringType restricted in length
310     </xs:documentation>
311     </xs:annotation>
312     <xs:simpleContent>
313         <xs:extension base="FormattedStringType100">
314             <xs:attribute ref="Language"/>
315             <xs:attribute ref="From"/>
316             <xs:attribute ref="To"/>
317             <xs:attribute ref="Order"/>
318             <xs:attribute ref="Verified"/>
319         </xs:extension>
320     </xs:simpleContent>
321 </xs:complexType>
322
323 <xs:simpleType name="FormattedStringType100">
324     <xs:restriction base="FormattedStringType">
325         <xs:minLength value="1"/>
326         <xs:maxLength value="100"/>
327     </xs:restriction>
328 </xs:simpleType>
329
330 </xs:schema>
331

```


332 2.5 Matching Dataset Attribute Definitions

333 2.5.1 Firstname

334 This value represents the SAML assertion subject's first name and any historic values for the subject's
335 first name as known to the asserting entity.

336 **Name:** MDS_firstname

337 One or more <AttributeValue> elements each containing a PersonNameType as specified in the
338 profile-specific schema in section 2.4.

```
339  
340 <saml:Attribute FriendlyName="Firstname" Name="MDS_firstname"  
341 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">  
342     <saml:AttributeValue ida:Language="en-GB"  
343 xsi:type="ida:PersonNameType">John</saml:AttributeValue>  
344 </saml:Attribute>
```

345 Fig. 2.5.1.1 Firstname provided without attribute history

346
347 Attribute values describing history of Firstname should be identified by the inclusion of the profile specific
348 From and To attributes as can be seen in the following example.

```
349  
350 <saml:Attribute FriendlyName="Firstname" Name="MDS_firstname"  
351 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">  
352     <saml:AttributeValue ida:Language="en-GB"  
353 xsi:type="ida:PersonNameType">John</saml:AttributeValue>  
354     <saml:AttributeValue ida:Language="en-GB"  
355     ida:From="1969-01-11" ida:To="2000-01-11"  
356     xsi:type="ida:PersonNameType">Johnathan</saml:AttributeValue>  
357 </saml:Attribute>
```

358 Fig. 2.5.1.2 Firstname and history of Firstname

359 2.5.2 Surname

360 This value represents the SAML assertion subject's surname and any historic values for the subject's
361 surname as known to the asserting entity.

362 **Name:** MDS_surname

363 One or more <AttributeValue> elements each containing a PersonNameType as specified in the
364 profile-specific schema in section 2.4.

365 Attribute values describing history of Surname should be identified by the inclusion of the profile specific
366 From and To attributes.

```
367  
368 <saml:Attribute FriendlyName="Surname" Name="MDS_surname"  
369 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">  
370     <saml:AttributeValue ida:Language="en-GB"  
371 xsi:type="ida:PersonNameType">Doe</saml:AttributeValue>  
372 </saml:Attribute>
```

373

374 2.5.3 Middle Name(s)

375 This value represents the SAML assertion subject's middle name(s) and any historic values for the
376 subject's middle name(s) as known to the asserting entity.

377 **Name:** MDS_middlename

378 One or more <AttributeValue> elements each containing a PersonNameType as specified in the
379 profile-specific schema in section 2.4. Where there are multiple middle names for the individual these
380 should be separated by a space as shown in the example below.

```
381
382 <saml:Attribute FriendlyName="Middlename(s)" Name="MDS_middlename"
383 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
384     <saml:AttributeValue ida:Language="en-GB"
385     xsi:type="ida:PersonNameType">Mark David</saml:AttributeValue>
386 </saml:Attribute>
```

387
388 Attribute values describing history of Middle Name(s) should be identified by the inclusion of the profile
389 specific From and To attributes.

390 2.5.4 Date of Birth

391 This value represents the SAML assertion subject's date of birth and any historic values for the subject's
392 date of birth as known to the asserting entity.

393 **Name:** MDS_dateofbirth

394 One or more <AttributeValue> elements each containing a DateType as specified in the profile-
395 specific schema in section 2.4.

```
396
397 <saml:Attribute FriendlyName="Date of Birth" Name="MDS_dateofbirth"
398 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
399     <saml:AttributeValue xsi:type="ida:DateType">1994-11-
400     05</saml:AttributeValue>
401 </saml:Attribute>
```

402
403 Attribute values describing history of date of birth should be identified by the inclusion of the profile
404 specific From and To attributes.

405 2.5.5 Gender

406 This value represents the SAML assertion subject's gender.

407 **Name:** MDS_gender

408 A single <AttributeValue> element containing a GenderType as specified in the profile-specific
409 schema in section 2.4¹.

```
410
411 <saml:Attribute FriendlyName="Gender" Name="MDS_gender"
412 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
413     <saml:AttributeValue xsi:type="ida:GenderType">
414         Male
415     </saml:AttributeValue>
416 </saml:Attribute>
```

417

418 2.5.6 Current Address

419 This value represents the SAML assertion subject's current address.

420 **Name:** MDS_currentaddress

421 One or more <AttributeValue> elements each containing an AddressType as specified in the
422 profile-specific schema in section 2.4.

```
423
424 <saml:Attribute FriendlyName="Current Address" Name="MDS_currentaddress"
425 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
426     <saml:AttributeValue ida:From="1969-01-11" ida:Language="en-
427     GB" xsi:type="ida:AddressType">
428         <ida:Line>1 Cherry Cottage</ida:Line>
```

¹ In version 1.2 of the profile history of gender MUST NOT be sent by an asserting entity

```
429         <ida:Line>Wurpel Lane</ida:Line>
430         <ida:Line>Reading</ida:Line>
431         <ida:PostCode>RG99 1YY</ida:PostCode>
432     </saml:AttributeValue>
433 </saml:Attribute>
```

434
435 Optionally the UPRN (Unique Property Reference Number) may also be included in the subject's address
436 details to uniquely identify the address and therefore aid matching where a local data set also includes
437 UPRN. UPRNs are integers that can be up to 12 digits in length; they can therefore be less than 12 digits
438 long and do not require leading zeros.

439
440 If a non-UK address is represented the `<InternationalPostCode>` element MUST be used instead of
441 the UK-centric `<PostCode>` element.
442

443 2.5.7 Previous Address

444 This value represents the SAML assertion subject's previous address or addresses as known to the
445 asserting entity.

446 **Name:** MDS_previousaddress

447 One or more `<AttributeValue>` elements each containing an `AddressType` as specified in the
448 profile-specific schema in section 2.4.
449

```
450 <saml:Attribute FriendlyName="Previous Address" Name="MDS_previousaddress"
451 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
452     <saml:AttributeValue ida:From="1969-01-11" ida:To="2000-01-11"
453     ida:Language="en-GB" xsi:type="ida:AddressType">
454         <ida:Line>1 Cherry Cottage</ida:Line>
455         <ida:Line>Wurpel Lane</ida:Line>
456         <ida:Line>Reading</ida:Line>
457         <ida:PostCode>RG99 1YY</ida:PostCode>
458     </saml:AttributeValue>
459 </saml:Attribute>
```

461 2.6 Authentication Event Assertion Attribute Definitions

462 The Authentication Event Assertion, as described in the SAML Profile, provides the IDA service with
463 additional contextual information regarding the authentication event to be used for transactional
464 monitoring purposes. In the case of version 1.2 of the SAML Profile this contextual information is to be
465 initially limited to IP Address (of the user-agent used for authentication) and the level of assurance
466 achieved (as returned within the `<AuthnContext>`). Additional attribute definitions will be added during
467 the lifetime of this profile following elaboration with Identity Providers and Service Providers.

468 2.6.1 IPAddress

469 This value represents the IP Address as used by the user-agent when authenticating the principal.

470 **Name:** TXN_IPAddress

471 The single `<AttributeValue>` element contains a `IPAddressType` as specified in the profile-specific
472 schema in section 2.4.
473

```
474 <saml:Attribute FriendlyName="IPAddress" Name="TXN_IPAddress"
475 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
476     <saml:AttributeValue
477     xsi:type="ida:IPAddressType">10.168.8.2</saml:AttributeValue>
478 </saml:Attribute>
```

480 2.7 Fraud Event Contextual Information Assertion Attribute Definitions

481 The Fraud Event Contextual Information Assertion, as described in the SAML Profile, provides the IDA
482 service with additional contextual information regarding a fraud event.

483 2.7.1 GPG45Status

484 This value represents the resulting status of the GPG45 IPV process where fraudulent activity has been
485 identified by the identity provider.

486 **Name:** FECI_GPG45Status

487 The single <AttributeValue> element contains a GPG45StatusType as specified in the profile-
488 specific schema in section 2.4. **Note that the latest values for the GPG45 status attribute value**
489 **should be sourced from the IPV Operations Manual the example below is indicative only.** IDPs
490 should return the “SAML Response – Fraud Warning Code” in this status field as specified in the IPV
491 Operations Manual.

```
492  
493 <saml:Attribute FriendlyName="GPG45Status" Name="FECI_GPG45Status"  
494 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">  
495     <saml:AttributeValue  
496 xsi:type="ida:GPG45StatusType">FI01</saml:AttributeValue>  
497 </saml:Attribute>  
498
```

499 2.7.2 IDPFraudEventID

500 This value represents the unique IDP specific fraud event reference code.

501 **Name:** FECI_IDPFraudEventID

502 The single <AttributeValue> element contains a IDPFraudEventIDType as specified in the profile-
503 specific schema in section 2.4.

```
504  
505 <saml:Attribute FriendlyName="IDPFraudEventID" Name="FECI_IDPFraudEventID"  
506 NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">  
507     <saml:AttributeValue  
508 xsi:type="ida:IDPFraudEventType">XYZ001975435</saml:AttributeValue>  
509 </saml:Attribute>  
510
```