Cabinet Office

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

## Identity Assurance Programme, 7 August 2015


**Document identifier:**

IDAP/HubService/Profiles/SAML/Attributes

**Editors:**

Mike Pegman, Department for Work and Pensions
Adam Cooper, Government Digital Service
Stephen Dunn, Government Digital Service

**Previous Contributors:**

Paul Toal, Oracle UK Ltd
Brandon Murdoch, Microsoft UK Ltd
Additional review and contributions were made by CESG.



**Abstract:**

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

# Table of Contents

# 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.
```

# 2 SAML Attributes

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

## 2.1 Required Information

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

## 2.2 SAML Attribute Naming

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

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

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

### 2.2.1 Attribute Name Comparison

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

## 2.3 Profile-Specific XML Attributes

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

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

## 2.4 SAML Attribute Values

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

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

```
<xs:schema
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
        xmlns="http://www.cabinetoffice.gov.uk/resource-
library/ida/attributes"
        elementFormDefault="qualified"
        attributeFormDefault="qualified"
        blockDefault="substitution"
        targetNamespace="http://www.cabinetoffice.gov.uk/resource-
library/ida/attributes">
```

```
    <xs:annotation>
        <xs:documentation>
        </xs:documentation>
    </xs:annotation>

    <xs:attribute name="From" type="FormattedDateType"/>
    <xs:attribute name="To" type="FormattedDateType"/>
    <xs:attribute name="Language" type="xs:language" default="en-GB"/>
    <xs:attribute name="Order" type="xs:integer"/>
    <xs:attribute name="Verified" type="xs:boolean" default="false"/>

    <xs:complexType name="AddressType">
        <xs:annotation>
            <xs:documentation>A FormattedAddressType
            </xs:documentation>
        </xs:annotation>
        <xs:complexContent>
            <xs:extension base="FormattedAddressType">
                <xs:attribute ref="Language"/>
                <xs:attribute ref="From"/>
                <xs:attribute ref="To"/>
                <xs:attribute ref="Verified"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>

    <xs:complexType name="FormattedAddressType" mixed="true">
        <xs:sequence>
            <xs:element name="Line" type="AddressLineType" minOccurs="1"
                        maxOccurs="5"/>
            <xs:element name="PostCode" type="PostCodeType"
minOccurs="0"/>
            <xs:element name="InternationalPostCode"
type="InternationalPostCodeType"
                        minOccurs="0"/>
            <xs:element name="UPRN" type="UPRNType" minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>

    <xs:simpleType name="AddressLineType">
        <xs:annotation>
            <xs:documentation>A FormattedStringType restricted in length
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="FormattedStringType">
            <xs:minLength value="1"/>
            <xs:maxLength value="100"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="DateTimeType">
        <xs:annotation>
            <xs:documentation>A date and time constructed in accordance
with the
                W3C Date and Time Formats Specification at
                http://www.w3.org/TR/NOTE-datetime.
            </xs:documentation>
        </xs:annotation>
```

```
        <xs:restriction base="xs:string">
            <xs:pattern value="(\d\d\d\d)(-(\d\d)(-
(\d\d)(T(\d\d):(\d\d)(:(\d\d)(\.\d+)?)?Z)?)?)?"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="FormattedDateType">
        <xs:annotation>
            <xs:documentation>A date constructed in accordance with the
                W3C Date and Time Formats Specification at
                http://www.w3.org/TR/NOTE-datetime.
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:pattern value="(\d\d\d\d)(-(\d\d)(-(\d\d))?)?"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="DateType">
        <xs:annotation>
            <xs:documentation>A FormattedDateType e.g. DoB
            </xs:documentation>
        </xs:annotation>
        <xs:simpleContent>
            <xs:extension base="FormattedDateType">
                <xs:attribute ref="From"/>
                <xs:attribute ref="To"/>
                <xs:attribute ref="Verified"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>

    <xs:simpleType name="EmailAddressType">
        <xs:annotation>
            <xs:documentation>Base email address type
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:minLength value="3"/>
            <xs:maxLength value="254"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="FormattedStringType">
        <xs:annotation>
            <xs:documentation>Base type for string use
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:minLength value="0"/>
            <xs:maxLength value="512"/>
         </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="SimpleGenderType">
        <xs:restriction base="xs:string">
            <xs:enumeration value="Male"/>
            <xs:enumeration value="Female"/>
```

```
            <xs:enumeration value="Not Specified"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="GenderType">
        <xs:annotation>
            <xs:documentation>A SimpleGenderType
            </xs:documentation>
        </xs:annotation>
        <xs:simpleContent>
            <xs:extension base="SimpleGenderType">
                <xs:attribute ref="From"/>
                <xs:attribute ref="To"/>
                <xs:attribute ref="Verified"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>

    <xs:simpleType name="PostCodeType">
        <xs:annotation>
            <xs:documentation>Type derived from xs:string with a pattern
                restriction to UK Post Codes
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:pattern
                    value="[A-Z]{1,2}[0-9R][0-9A-Z]? [0-9][A-Z-
[CIKMOV]]{2}"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="InternationalPostCodeType">
        <xs:annotation>
            <xs:documentation>Type derived from xs:string representing an
                international postal code
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="20"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="UPRNType">
        <xs:annotation>
            <xs:documentation>Type derived from xs:string representing a
UPRN
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:minLength value="1"/>
            <xs:maxLength value="12"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="IPAddressType">
        <xs:annotation>
            <xs:documentation>Simple IP Address type
```

```
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:minLength value="7"/>
            <xs:maxLength value="128"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="GPG45StatusType">
        <xs:annotation>
            <xs:documentation>GPG45 Status code, see latest version of
GPG45 and the operations manual for required values
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:minLength value="4"/>
            <xs:maxLength value="8"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:simpleType name="IDPFraudEventIDType">
        <xs:annotation>
            <xs:documentation>Unique fraud event ID
            </xs:documentation>
        </xs:annotation>
        <xs:restriction base="xs:string">
            <xs:minLength value="12"/>
            <xs:maxLength value="100"/>
        </xs:restriction>
    </xs:simpleType>

    <xs:complexType name="PersonNameType">
        <xs:annotation>
            <xs:documentation>A FormattedStringType restricted in length
            </xs:documentation>
        </xs:annotation>
        <xs:simpleContent>
            <xs:extension base="FormattedStringType100">
                <xs:attribute ref="Language"/>
                <xs:attribute ref="From"/>
                <xs:attribute ref="To"/>
                <xs:attribute ref="Order"/>
                <xs:attribute ref="Verified"/>
            </xs:extension>
        </xs:simpleContent>
    </xs:complexType>

    <xs:simpleType name="FormattedStringType100">
        <xs:restriction base="FormattedStringType">
            <xs:minLength value="1"/>
            <xs:maxLength value="100"/>
        </xs:restriction>
    </xs:simpleType>

</xs:schema>
```

## 2.5 Matching Dataset Attribute Definitions

### 2.5.1 Firstname

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

**Name:** MDS_firstname

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

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

Fig, 2.5.1.1 Firstname provided without attribute history

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

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

Fig. 2.5.1.2 Firstname and history of Firstname

### 2.5.2 Surname

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

**Name:** MDS_surname

One or more `<AttributeValue>` elements each containing a `PersonNameType` as specified in the profile-specific schema in section 2.4.
Attribute values describing history of Surname should be identified by the inclusion of the profile specific From and To attributes.

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

### 2.5.3 Middle Name(s)

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

**Name:** MDS_middlename

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

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

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

### 2.5.4 Date of Birth

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

**Name:** MDS_dateofbirth

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

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

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

### 2.5.5 Gender

This value represents the SAML assertion subject's gender.

**Name:** MDS_gender

A single `<AttributeValue>` element containing a `GenderType` as specified in the profile-specific schema in section 2.4[1].

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

### 2.5.6 Current Address

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

**Name:** MDS_currentaddress

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

```
<saml:Attribute FriendlyName="Current Address" Name="MDS_currentaddress"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
            <saml:AttributeValue ida:From="1969-01-11" ida:Language="en-
GB" xsi:type="ida:AddressType">
                <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

```
                <ida:Line>Wurpel Lane</ida:Line>
                <ida:Line>Reading</ida:Line>
                <ida:PostCode>RG99 1YY</ida:PostCode>
            </saml:AttributeValue>
   </saml:Attribute>
```

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

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

### 2.5.7 Previous Address

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

**Name:** MDS_previousaddress

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

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

## 2.6 Authentication Event Assertion Attribute Definitions

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

### 2.6.1 IPAddress

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

**Name:** TXN_IPaddress

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

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

## 2.7 Fraud Event Contextual Information Assertion Attribute Definitions

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

### 2.7.1 GPG45Status

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

**Name:** FECI_GPG45Status

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

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

### 2.7.2 IDPFraudEventID

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

**Name:** FECI_IDPFraudEventID

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

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