Cabinet Office

Identity Assurance Hub Service Profile – Authentication Contexts v1.2a

Identity Assurance Programme, 7 August 2015

Document identifier:
IDAP/HubService/Profiles/SAML/AuthnContexts

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

Contributors:
Additional review and contributions were made by CESG.

Abstract:

This specification defines the SAML authentication contexts to be used in conjunction with the Identity Assurance Hub Service Profile v1.2.

© Crown Copyright

Table of Contents

1 Introduction 3

1.1 Notation 3

2 Authentication Contexts 4

2.1 Specifying Level of Assurance in <AuthnRequest> 4

2.2 Returning Level of Assurance in <Response> 4

2.3 Authentication Context values for Level of Assurance 5

2.3.1 Level 1 Authentication Context 5

2.3.2 Level 2 Authentication Context 5

2.3.3 Level 3 Authentication Context 6

2.3.4 Level 4 Authentication Context 6

2.3.5 Level X Authentication Context (Fraud Event) 7

© Crown Copyright

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 authentication contexts 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.
```


© Crown Copyright

2 Authentication Contexts

This document describes the authentication contexts specified for use with the IDA hub service profile.

When requesting authentication for an individual or responding to that request the level of assurance requested (or attained) must be specified. The IDA hub service profile conforms to the definitions of level of assurance as described in *GPG 45 – Identity Proofing and Verification of an Individual*.

This document describes how level of assurance is specified and recorded in interactions between the hub services, identity providers and service providers. An additional authentication context is included for the purpose of reporting fraud as detected by an identity provider, Level X.

2.1 Specifying Level of Assurance in <AuthnRequest>

Service providers and the hub service will construct a `<RequestedAuthnContext>` within the `<AuthnRequest>` that describes the level of assurance required to enable the principal to transact with the service.

An example `<RequestedAuthnContext>` can be seen below (in this case a request for a LoA of 1 as a minimum, LoA2 preferred).

```
<saml2p:RequestedAuthnContext
        Comparison="minimum"
        xsi:type="saml2p:ActionType">
        <saml2:AuthnContextClassRef
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
            urn:uk:gov:cabinet-office:tc:saml:authn-context:level2
        </saml2:AuthnContextClassRef>
        <saml2:AuthnContextClassRef
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
            urn:uk:gov:cabinet-office:tc:saml:authn-context:level1
        </saml2:AuthnContextClassRef>
</saml2p:RequestedAuthnContext>
```

2.2 Returning Level of Assurance in <Response>

The `<Assertion>` returned in the `<Response>` to the hub service MUST include an `<AuthnStatement>` which includes the level of assurance to which the principal has been authenticated.

An example `<AuthnStatement>` can be seen below (in this case level of assurance is LoA2).

```
<saml2:AuthnStatement
    SessionIndex="post-office"
    xsi:type="saml2:AuthnStatementType">

    <saml:AuthnContext>
        <saml:AuthnContextClassRef>
            urn:uk:gov:cabinet-office:tc:saml:authn-context:level2
        </saml:AuthnContextClassRef>
    </saml:AuthnContext>
</saml2:AuthnStatement>
```


© Crown Copyright

2.3 Authentication Context values for Level of Assurance

The schemas defined in section 2.3.1 onwards denote authentication contexts matching the levels of assurance described in *GPG 45 – Identity Proofing and Verification of an Individual*. These authentication contexts are to be used by service providers and the hub service when requesting authentication at a specific level of assurance, and by identity providers when responding to an authentication request.

2.3.1 Level 1 Authentication Context

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:uk:gov:cabinet-office:tc:saml:authn-context:level1"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:uk:gov:cabinet-office:tc:saml:authn-context:level1"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

    <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
        <xs:documentation>
        Class identifier: urn:uk:gov:cabinet-office:tc:saml:authn-context:level1
        Document identifier: saml-schema-authn-context-ip-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
        V1.2 (Sept, 2014):
          New authentication context class schema for SAML V2.0 - denotes
authentication at LoA1
        </xs:documentation>
        </xs:annotation>
    </xs:redefine>
</xs:schema>
```

2.3.2 Level 2 Authentication Context

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:uk:gov:cabinet-office:tc:saml:authn-context:level2"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:uk:gov:cabinet-office:tc:saml:authn-context:level2"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

    <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
        <xs:documentation>
        Class identifier: urn:uk:gov:cabinet-office:tc:saml:authn-context:level2
        Document identifier: saml-schema-authn-context-ip-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
        V1.2 (Sept, 2014):
          New authentication context class schema for SAML V2.0 - denotes
authentication at LoA2
        </xs:documentation>
        </xs:annotation>
    </xs:redefine>
</xs:schema>
```


© Crown Copyright

2.3.3 Level 3 Authentication Context

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:uk:gov:cabinet-office:tc:saml:authn-context:level3"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:uk:gov:cabinet-office:tc:saml:authn-context:level3"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

    <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
        <xs:documentation>
        Class identifier: urn:uk:gov:cabinet-office:tc:saml:authn-context:level3
        Document identifier: saml-schema-authn-context-ip-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
        V1.2 (Sept, 2014):
          New authentication context class schema for SAML V2.0 - denotes
authentication at LoA3
        </xs:documentation>
        </xs:annotation>
    </xs:redefine>
</xs:schema>
```

2.3.4 Level 4 Authentication Context

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:uk:gov:cabinet-office:tc:saml:authn-context:level4"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:uk:gov:cabinet-office:tc:saml:authn-context:level4"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

    <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
        <xs:documentation>
        Class identifier: urn:uk:gov:cabinet-office:tc:saml:authn-context:level4
        Document identifier: saml-schema-authn-context-ip-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
        V1.2 (Sept, 2014):
          New authentication context class schema for SAML V2.0 - denotes
authentication at LoA4
        </xs:documentation>
        </xs:annotation>
    </xs:redefine>
</xs:schema>
```


© Crown Copyright

2.3.5 Level X Authentication Context (Fraud Event)

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
  targetNamespace="urn:uk:gov:cabinet-office:tc:saml:authn-context:levelX"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns="urn:uk:gov:cabinet-office:tc:saml:authn-context:levelX"
  finalDefault="extension"
  blockDefault="substitution"
  version="2.0">

    <xs:redefine schemaLocation="saml-schema-authn-context-types-2.0.xsd">

    <xs:annotation>
        <xs:documentation>
        Class identifier: urn:uk:gov:cabinet-office:tc:saml:authn-context:levelX
        Document identifier: saml-schema-authn-context-ip-2.0
        Location: http://docs.oasis-open.org/security/saml/v2.0/
        Revision history:
        V1.2 (Sept, 2014):
          New authentication context class schema for SAML V2.0 - denotes fraud
event at unspecified level of assurance
        </xs:documentation>
        </xs:annotation>
    </xs:redefine>
</xs:schema>
```


© Crown Copyright