International Government Assurance Profile (iGov)

1. Types of eID Scheme

The eID schemes used for access to government systems varies considerably between nations and can be crudely categorised by the origin of eID issuance (e.g. public or private sector), and the model of eID federation (direct or broker / hub model).

Overlaid are the legal requirements for eID largely derived from more general law such as Data Protection / Privacy regulations and acts under national and / or international law. There are some specific eID laws although the most widespread currently is the eIDAS Regulation applying to all 28 EU Member States.

These variances should be reflected in the flexibility of the iGov profile in order to support the widest possible range of government eID solutions.

1. Federation models to be considered for iGOV Profile
2. Direct RP / IDP relationship

In this model the RP and IDP(s) are known to each other directly and the user is able to select IDP (where multiple choices are available) directly when interacting with the RP service. This is often the case where there are a small number of national eID IDPs and those providers are relatively static.

This model assumes that the Relying Party and the Identity Provider have a direct relationship and do not require a broker or federation hub to route authentication requests.

### Use Cases

|  |  |
| --- | --- |
| **Use Case** | **Description** |
| The user selects an IDP for sign-in at the RP | The user selects an identity provider as presented by the RP (the method of presentation is implementation specific). The RP must generate an authentication request to sent to the IDP and send this request in accordance with the messaging requirements of the relevant profile. |
| RP selects an IDP for sign-in (without user intervention) | This is a special case of “user selects an IDP for sign-in” where the RP has prior knowledge of the requirements for authentication e.g. only a specific identity provider meets the requirements for authentication such as level of assurance. |
| The user authenticates at the IDP | The user provides relevant credentials to the IDP to facilitate sign-in (i.e. those issued following a successful registration process with the IDP).  The IDP must provide a status code describing the nature of any failure to the RP when the authentication is not successful at the IDP. This may be the result of a user cancel action, failure to authenticate, or other error state as described by the scheme rules for the federation. |
| The IDP asserts the identity of the user to the RP | The IDP must either assert an ID Token to the RP or an error status as described in the profile. |
| The RP identifies the user by consuming information in the identity assertion | The RP must be able to consume an ID Token from an IDP and to check the integrity of that token as prescribed in the profile.  The RP must also retrieve claims for the individual referred to by the ID Token (i.e. from the UserInfo Endpoint). The RP is then responsible for matching the claims in the response to the known ‘accounts’ held within its systems. In the case of a positive match this should result in the identification of a local identifier (relevant to the RP) for the user. |

1. Broker (or hub) model

There are a variety of examples nationally where an identity broker or federation hub has been deployed such as the UK, Sweden and Denmark as well the US (Connect.Gov). It is clear that this model will persist and that other nations are considering the implementation of similar models.

In this case a Broker or federation Hub is used to route requests for authentication from Relying Parties to the required Identity Provider. The method used to choose an identity provider is implementation specific and can be user and/or Relying Party driven.

### Use Cases

|  |  |
| --- | --- |
| **Use Case** | **Description** |
| The RP requests authentication from the Broker | The RP sends an authentication request to the Broker including any specific authentication requirements. |
| The user selects an IDP for sign-in at the Broker | The user selects an identity provider as presented by the Broker (the method of presentation is implementation specific). |
| The Broker requests authentication from the (chosen) IDP | The Broker must generate an authentication request to send to the IDP and send this request in accordance with the messaging requirements of the relevant profile. This request must mirror any specific requirement of the RP as indicated in the RP authentication request. |
| The user authenticates at the IDP | The user provides relevant credentials to the IDP to facilitate sign-in (i.e. those issued following a successful registration process with the IDP).  The IDP must provide a status code describing the nature of any failure to the RP when the authentication is not successful at the IDP. This may be the result of a user cancel action, failure to authenticate, or other error state as described by the scheme rules for the federation. |
| The IDP asserts the identity of the user to the Broker | The IDP must either assert an ID Token to the Broker or an error status as described in the profile. |
| The Broker relays the assertion of identity to the RP | The Broker should relay the IDP assertion (ID Token) to the RP in response to the originating RP authentication request. |
| The RP identifies the user by consuming information in the identity assertion | The RP must be able to consume an ID Token from an IDP and to check the integrity of that token as prescribed in the profile.  The RP may also retrieve claims for the individual referred to by the ID Token and / or perform matching (see optional use cases below). |

1. Optional (general) Use Cases

|  |  |
| --- | --- |
| **Use Case** | **Description** |
| The RP performs matching to identify a local identifier or account for the user | The RP may also retrieve claims for the individual referred to by the ID Token (i.e. from the UserInfo Endpoint). The RP is then responsible for matching the claims in the response to the known ‘accounts’ held within its systems. In the case of a positive match this should result in the identification of a local identifier (relevant to the RP) for the user (see Claims Requirements below). |
| RP requests additional attributes during authentication request | Support for domain specific attributes (claims) is of great importance to EU member states. An outline of how this could be implemented should be included in the profile. |
| RP specifies a level of assurance when requesting authentication | The RP specifies requirements for authentication in particular the required level of assurance acceptable for sign-in to the service. |
| The IDP asserts transaction monitoring and / or additional authentication context information alongside identity assertion | Transaction monitoring and authentication context information may be of great importance to protect the RP (service) from attack or alert the RP to potential fraud. |

1. Claims Requirements (UserInfo)

In the interests of data minimisation balanced with the requirement to successfully identity the individual signing in to a service claims have been split into mandatory and optional user info (identity) claims. It is expected that these claims would be made available via a UserInfo endpoint.

1. Mandatory UserInfo / Identity Claims

|  |  |
| --- | --- |
| **Claim** | **Description** |
| unique\_identifier | This uniquely identifies the identity asserted in the country of origin but does not necessarily reveal any discernible correspondence with the subject's actual identifier (for example, username, fiscal number etc) |
| given\_name | The current given name / forename of the individual |
| family\_name | The current family name (surname) of the individual |
| middle\_name | Any middle name(s) associated with the individual |
| birthdate | Date of Birth includes a date using the following format: YYYY + “-“ + MM + “-“ + DD (as defined for xsd:date) |

1. Optional UserInfo / Identity Claims

|  |  |
| --- | --- |
| **Claim** | **Description** |
| address | Free format address data base64 encoded |
| postal\_code | Postal code of the individual’s current address where available |
| email | Current and active email address of the subject |
| email\_verified | Verified email address (see email above) |
| gender | Gender of the individual where the identity provider has gained consent. Values for Gender attributes MUST be one of the following:   Male   Female   Not Specified |
| birth\_place | Place of birth as recorded on official documentation such as passport or birth certificate. |

1. The need to support identity matching

Matching of the identity assertion based on claims to a local identifier or ‘account’ related to the individual identity at a level of assurance is a requirement where the government in question is not able to provide a single identifier for all citizens based on an authoritive register of citizens.

The requirement for matching is also of importance where a cross-border or cross-jurisdiction authentication is required and therefore the availability of a single identifier (e.g. social security number) cannot be guaranteed for the individual wishing to authenticate.

In general, matching an asserted set of claims for an identity to relying party held records for know individuals requires a minimum set of data elements to be provided. Research in the UK and across the EU under the eIDAS Regulation has identified the minimum set of citizen attributes required to affect a successful match. Due to regional and national law this set of attribute may vary although the key elements are: name, date of birth, current address (including postal code), gender (were consent given).

1. Levels of Assurance

Identity Providers must include an Authentication Context describing the level of assurance achieved for the asserted identity. These values will be described as URIs in the same format as the SAML Authentication Context Class Reference construct.

It is recommended that both FICAM and eIDAS levels of assurance are supported in the authentication context by default.

Current NIST Levels of Assurance:

|  |
| --- |
| **NIST LoA** |
| <http://idmanagement.gov/ns/assurance/loa/1> |
| <http://idmanagement.gov/ns/assurance/loa/2> |
| <http://idmanagement.gov/ns/assurance/loa/3> |

Current eIDAS Levels of Assurance:

|  |
| --- |
| **eIDAS LoA** |
| <http://eidas.europa.eu/LoA/low> |
| <http://eidas.europa.eu/LoA/substantial> |
| <http://eidas.europa.eu/LoA/high> |

There is no requirement for authentication methods to be described in the Authentication Context as standards for levels of assurance should be outcome based. This also removes the requirement for RPs and IDPs to have a shared understanding of the authentication method values.

1. Technical Requirements

Technical considerations for the messaging flow to protect the consuming services and individual users from attack.

|  |  |
| --- | --- |
| **Requirement** | **Description** |
| Message Integrity | Method of proving the integrity of a message often accomplished through the addition of a digital signature to the response message or a specific element of the payload such as claims. |
| Message Confidentiality | Method of preventing the interception and reading of messages in transit either at the user agent (e.g. browser) or in transit between trusted ‘nodes’ in the federation such as RP, SP and Broker (Hub). |
| Replay Protection | Prevent the replay of authentication requests and responses. For example, SSL encryption when sending messages between entities specifically to prevent the interception and replay of claims. Consider the use of a digital signature mechanism to sign messages as well as setting a validity period for the message. |