Digital Scotland
Digital Identity Scotland

Digital Identity Scotland

Service Description for Relying Parties

Version 0.6 Work in Progress
Date 26th June 2019

Document Status
This is a work-in-progress document and is subject to change. It is indicative of the scope of the potential future service to be provided by Digital Identity Scotland to Scottish public sector services.

This initial version of the document was written to help with scoping of the OIX Alpha PoC, as indicated throughout.

Digital Scotland
Digital Identity Scotland

Contents

1. Introduction

1.1. Service Scope

This document describes the potential service offered by the Digital Identity Scotland to Scottish public services, providing a common approach to digital identity.

The Digital Identity Service will allow users to obtain and use a digital identity account that facilitates access to Scottish public services. It is anticipated that there will be a range of digital identity account providers, allowing the user to choose one that is most suitable for their needs.

The Digital Identity Service will provide public services with a single consistent way to integrate with these digital identity services.

The Digital Identity Service will provide the following key services:

- Digital identity accounts for users
- Identification, authentication and attribute services within the context of those digital identity accounts
- Portal to support face-to-face checks to be performed by Scottish Public Sector services (To be confirmed)

The Digital Identity Service will **not** provide:

- E.g. Access to background sources such as Credit Bureaux

1.2. Organisational roles

[CONTEXT DIAGRAM TO BE ADDED IN FUTURE VERSION]

The following primary organisations are involved in the Digital Identity Service

- Identity Providers – who provide digital identity accounts to users, perform identification and authentication of those users and may provide additional attributes.
- Relying Parties – Scottish public service that use the Digital Identity Service to access digital identity services. Relying parties may also provide attributes arising from the services they offer.
- Digital Identity Scotland Service – the service providing a common approach to digital identity and the subject of this document.

1.3. Service List

Services are organised as follows:

Area	Service List
Discovery Services to find out the status of user digital identity account	(None defined yet)
Identification Services to establish a re-usable identifier for the user	Identification: Identify User – no claimed identity Identification: Identify User – claimed identity Identification: Face-to-face identity checks Identification: Perform Face-to-face Check Identification: Obtain Face-to-face Check Result Identification: Feedback to IDPs Identification: Feedback Identity Assurance Information
Authentication Services to authenticate the user in the current session or transaction, through the provision and management of authentication credentials.	Authentication: Authenticate Known User Authentication: Get Authenticated Identifier Authentication: Step Up Authentication
Attributes Services to obtain attributes for the user	Attribute: Attribute Discovery Attribute: Locate Attribute Attribute: Attribute Request Attribute: Get Attributes Attribute: Query Attributes Attribute: Get Authenticated Identifier and Attributes Attribute: Get Authenticated Identifier and Query Attributes Attribute: Attribute Management Attribute: Subscribe to Attribute Updates Attribute: Publish Attribute Update Attribute: Receive Attribute Update

Note however that some services provide aggregated capabilities, e.g. “Attribute: Get Authenticated Identifier and Attributes” will return attributes having first authenticated and potentially identified the customer.

1.4. Levels of Assurance

Assurance levels are used to enable Relying Parties to specify the strength of digital identities used to access their service and are a means of ensuring equivalence across the system.

Levels of assurance are defined for each aspect of the service as follows[1]:

[1] This level of granularity will provide maximum flexibility going forwards, including the decoupling of identity (i.e. unique, identifiable user) from any specific attributes.|

- Level of identification – the strength of processes employed to ensure that a user linked to an identifier being presented is real, unique and identifiable.
- Level of authentication – the strength of authentication credential employed at the point a user is attempting to access a service
- Level of attribute assurance - the confidence that can be put in an attribute associated with an identifier based on the originator of the attribute and processes they employ.

Whilst these levels are defined independently of each other, they will normally be used in combination. Digital Identity Scotland intends to align with UK assurance standards as far as possible.[2]

[2] Further analysis / guidance will be required here.

2. Using the Service

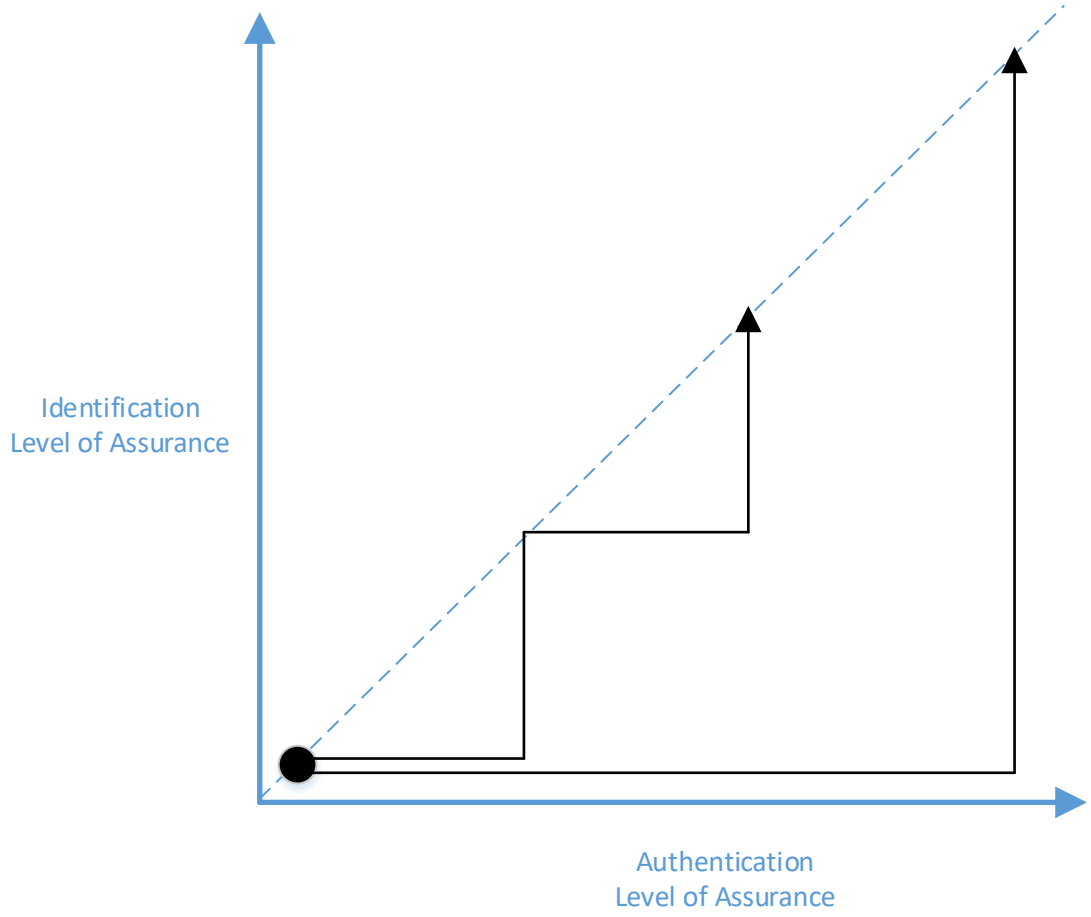
2.1. Relying Party Access

TBC – this will outline the operational processes for gaining access to DIS.

2.2. Customer Lifecycle

TBC – this will describe the typical customer lifecycle

2.2.1. Typical Digital Identity Lifecycle



Notes:

- Addressing identity only. Additional content required to describe attribute lifecycle and linkage of attributes to identities.
- Assumption is that person will have an "identity account". The diagram shows how the status of such an account may be improved over time.
- Assurance can also go down (e.g. when evidence used to establish identity is revoked or fraud is detected).
- The Level of Assurance for Identification (available in a transaction) can only ever be as good as the Level of Assurance for Authentication.
- In practice then various identity account lifecycles can be envisaged including:

- Identification and authentication are progressed in parallel (i.e. following the diagonal line)
- Authentication is progress ahead of identification, e.g. a customer might have an account that is protected by a strong authentication credential but not (yet) undergone an identity verification process to establish who the customer is.

2.3. Service Usage

The way that Relying Parties will use the service will depend on the status of the customer within the relying party, the user experience that the relying party wishes to deliver and other factors. The following table provides some examples

Scenario	DIS Service Calls
New customer to both IDP and RP (IDP performs identification up front) In this scenario, when the customer attempts to access the service of the RP, the RP will call DIS to provide the customer with an identity account and verify the customer's identity. This is the basic scenario and would be applicable where: • Identification needs to be done up front • The customer will be able to complete the account setup and identification process at the same time as completing the service sign-up.	Single call to "*Attribute: Get Authenticated Identifier and Attributes*"
New customer to both IDP and RP (RP performs identification up front) TBC	TBC
New customer to both IDP and RP (RP performs identification later) In this scenario, when the customer attempts to access the service of the RP, the RP initially just gets an identifier from DIS. This allows the customer to complete their service access over multiple sessions. The RP themselves undertakes identification steps and passes the evidence back to the IDP out-of-band (but with the customer's consent.	Initial call to either "*Authentication: Get Authenticated Identifier*" or "*Attribute: Get Authenticated Identifier and Attributes*" Subsequent calls to either "*Authentication: Authenticate Know User*" or "*Authentication: Get Authenticated Identifier*" The RP passes evidence back using "*Identification: Feedback Identity Assurance Information*"
New customer to both IDP and RP (Identification performed face-to-face) TBC	TBC
Customer known to RP but not IDP (Vouching) TBC	TBC
Customer known to IDP but not RP TBC	TBC
Apply for RP service but delay identification to decision point TBC	TBC

3. Discovery Services

To be completed. Aim is to provide services

Potentially should include:

- Does user have Digital Identity account already?
- Is user able to perform step-up authentication?
- Is user able to get digital identity account?
- Is RP vouching needed?

4. Identification Services

4.1. Standalone Identification

4.1.1. Identify User – no claimed identity ***(Not in scope for Alpha)***

Description	Standalone request for identity information of user, where there is no requirement for ongoing interaction with the user. Consequently this service will not create an identifier to be used in subsequent transactions.[3] The service should be called when the core attributes of the user (name, address, date of birth, gender) are not known. It returns that core set of attributes. A flag is used to indicate whether new identification should be undertaken (in the event the user does not yet have an identity account) or whether to only return data from existing identity accounts.
Inputs	Required level of identification Perform new identification flag
Outputs	Level of identification achieved For each core attribute (name, address, date of birth, gender): • Attribute value • Level of attribute assurance achieved.

4.1.2. Identify User – claimed identity ***(Not in scope for Alpha)***

Description	Standalone request for identity information of user, where there is no requirement for ongoing interaction with the user. Consequently this service will not create an identifier to be used in subsequent transactions.[4] This method should be called when the core set of attributes (name, address, date of birth, gender) to be verified are known. This could be because the user has provided them to the relying party as part of the service request being made or because the user is already known to the relying party. Returns confirmation of the core set of attributes (name, address, date of birth, gender). A flag is used to indicate whether new identification should be undertaken (in the event the user does not yet have an identity account) or whether to only return data from existing identity accounts.
Inputs	Required level of identification Core attribute values to be confirmed (name, address, date of birth, gender) Perform new identification flag
Outputs	Level of identification achieved For each core attribute (name, address, date of birth, gender): • Attribute value confirmation • Level of attribute assurance achieved.

[3] Where an identifier is required for subsequent interactions, the methods in section 5 and 6 should be used.
[4] Where an identifier is required for subsequent interactions, the methods in section 5 and 6 should be used.

4.2. Face-to-face identity checks

4.2.1. Perform Face-to-face Check (In scope for Alpha)

Description	Portal service provided for where Relying Parties can perform face-to-face checks.
Inputs	N/A
Outputs	N/A

4.2.2. Obtain Face-to-face Check Result (Not in scope for Alpha)

Description	Allow RP to get results of face-to-face check including uplift to LoA
Inputs	TBC
Outputs	TBC

4.3. Feedback to IDPs

4.3.1. Feedback Identity Assurance Information (Not in scope for Alpha)

Description	Service to allow RP to feed identity assurance information back to IDPs, that can be used by IDPs to increase the level of identification for the customer. **Note: This service requires additional analysis. It is linked to ongoing standards work being conducted as part of OIX Alpha Stream 2. The service will need to ensure appropriate consents have been obtained.**
Inputs	Identifier for user Evidence to be fed back to IDP (to be expanded)
Outputs	Confirmation of receipt

5. Authentication Services

5.1. Known User

5.1.1. Authenticate Known User ***(Not in scope for Alpha)***

Description	General method for authenticating customer where: • RP is able to specify customer to be authenticated, by providing an identifier. This will be because the authentication is being performed in a context where the customer is already identified. • RP provides transaction or service specific reference to ensure that the authentication is done in the context of the service in question
Inputs	Identifier Transaction or session reference Level of authentication required
Outputs	Result of authentication. Will be one of: • Authentication at requested level successful • Authentication at lower level (specified) successful • Authentication failed Binding to transaction or session reference

5.2. Unknown User

5.2.1. Get Authenticated Identifier ***(Not in scope for Alpha)***

Description	Authenticate the user within the current session / transaction and return an identifier that can be used to refer to the customer going forwards.
Inputs	Transaction or session reference Level of identification (for identifier) required Level of authentication required
Outputs	Identifier Level of identification for identifier achieved Result of authentication. Will be one of: • Authentication at requested level successful • Authentication at lower level (specified) successful • Authentication failed Binding to transaction or session reference

5.2.2. Step Up Authentication ***(Not in scope for Alpha)***

Description	Within session request additional authentication to raise authentication level
Inputs	TBC
Outputs	TBC

6. Attribute Services

6.1. Attribute Discovery

6.1.1. Locate Attribute (Not in scope for Alpha)

Description	Find places (could be multiple) where attribute for user is held
Inputs	TBC
Outputs	TBC

6.2. Attribute Request

6.2.1. Get Attributes (Not in scope for Alpha)

Description	Get requested attribute for specific user (identifier) Must be called after *Get Authenticated Identifier*.
Inputs	TBC
Outputs	TBC

6.2.2. Query Attributes (Not in scope for Alpha)

Description	Query attribute for specific user (identifier) Returns Y or N depending on whether Attribute with specified value exists for user (identifier). Must be called after *Get Authenticated Identifier*.
Inputs	TBC
Outputs	TBC

6.2.3. Get Authenticated Identifier and Attributes (May be in scope for Alpha)

Usage	Combined method for authenticating customer, obtaining attributes and establishing an identifier in a single call: • RP is not able to specify customer to be authenticated, by providing an identifier. This could be because the user is a new customer or because RP is unable to determine the identifier from the context. • RP provides transaction or service specific reference to ensure that the authentication is done in the context of the service in question This service should be called when the attributes are not known.
Inputs	Transaction or session reference Level of identification required (for identifier) Attributes required including level of attribute assurance (optional)
Outputs	Identifier Result of authentication: • Authentication at requested level successful • Authentication at lower level (specified) successful

	• Authentication failed Binding to transaction or session reference For each attribute requested: • Attribute value • Level of attribute assurance achieved.

6.2.4. *Get Authenticated Identifier and Query Attributes* ***(May be in scope for Alpha)***

Usage	Combined method for authenticating customer, obtaining confirmation of attributes and establishing an identifier in a single call: • RP is not able to specify customer to be authenticated, by providing an identifier. This could be because the user is a new customer or because RP is unable to determine the identifier from the context. • RP provides transaction or service specific reference to ensure that the authentication is done in the context of the service in question This method should be called when the attributes to be verified are known. This could be because the user has provided them to the relying party as part of the service request being made or because the user is already known to the relying party.
Inputs	Transaction or session reference Level of identification required (for identifier) Attribute values to be confirmed including level of attribute assurance (optional)
Outputs	Identifier Result of authentication: • Authentication at requested level successful • Authentication at lower level (specified) successful • Authentication failed Binding to transaction or session reference For each attribute requested: • Attribute value confirmation • Level of attribute assurance achieved.

6.3. Attribute Management

6.3.1. *Subscribe to Attribute Updates* ***(Not in scope for Alpha)***

Description	Request to receive updates on changes to attributes (for specific user)
Inputs	TBC
Outputs	TBC

6.3.2. *Publish Attribute Update* ***(Not in scope for Alpha)***

Description	Publish an update to an attribute to subscribers
Inputs	TBC
Outputs	TBC

6.3.3. *Receive Attribute Update* ***(Not in scope for Alpha)***

Description	Receive update to attribute that has been subscribed to.
Inputs	TBC
Outputs	TBC

7. Protocols

To be expanded:

- OIDC is default protocol for Identification and Authentication Services. This is because OIDC is expected to be supported by commercial products (used by RPs) reducing development time and interoperability issues.
- SAML to also be supported **(Not in scope for Alpha)**
- Proprietary API may be developed if required **(Not in scope for Alpha)**
- Additional APIs defined for services that OIDC does not naturally support **(Not in scope for Alpha)**

7.1. OpenID Connect Usage

7.1.1. Standard Configuration

Parameter	**Type**
Client Registration	Manual
Authentication Flow	Authorization Code Flow
ID Token	Will utilise for returning core identity attributes (“claims” in OIDC terminology)
UserInfo Endpoint	Will be used for returning additional meta data (on core identity attributes) and additional attributes that DIS may define.

7.1.2. Sample Flow

The basic authentication will follow the standard OIDC Authorization Code Flow as follows:

- Authentication Request
- Authentication Response
- Token Request
- Token Response
- /UserInfo Endpoint Request (optional)
- /UserInfo Endpoint Response (optional)

Messages will be populated as follows:

Authentication Request

Parameter	**Type**	**Comment**
scope	REQUIRED	“openid” Note, OIDC has predefined claim sets that can be requested via scopes (e.g. “profile”) these may not match onto specific RP requirements.
response_type	REQUIRED	“code”
client_id	REQUIRED	Identifier for RP (i.e. “client” in OIDC terminology)
redirect_uri	REQUIRED	Redirection URI from RP
state	RECOMMENDED	Used for maintaining state. Suggest to use as per OIDC guidance.

response_mode	OPTIONAL	Tbc
nonce	OPTIONAL	Tbc
display	OPTIONAL	Tbc
prompt	OPTIONAL	Tbc
max_age	OPTIONAL	Tbc
ui_locales	OPTIONAL	Tbc
id_token_hint	OPTIONAL	Tbc
login_hint	OPTIONAL	Tbc
acr_values	OPTIONAL	Should be used to specific LoA required
claims	OPTIONAL	Used for requesting tailored sets of claims – so likely to be more suitable for DIS. **IMPORTANT NOTE: this may not be supported by all OIDC Providers so need to investigate.**

Authentication Response

Parameter	Type	Comment
code	REQUIRED	Code generated by DIS that will be used in token request below
state	REQUIRED	"code"

Token Request

Parameter	Type	Comment
grant_type	REQUIRED	"authorization_code"
code	REQUIRED	Code received from DIS above
redirect_uri	REQUIRED	Redirection URI from RP
client_id	REQUIRED	Identifier for RP (i.e. "client" in OIDC terminology)

Token Response

Parameter	Type	Comment
access_token	REQUIRED	Access token from DIS for retrieving additional claims from /userinfo endpoint
token_type	REQUIRED	"Bearer"
refresh_token	OPTIONAL	TBD
expires_in	RECOMMENDED	When token expires
id_token	REQUIRED	Token containing standard identity claims

/UserInfo Endpoint Request

Parameter	Type	Comment
Authorization	REQUIRED	Bearer token from Token Response

/UserInfo Endpoint Response

Parameter	Type	Comment
JSON Object	REQUIRED	Object includes requested claims

8. Identifiers

To be covered

- Definition of identifiers
- Identifier mapping supported by DIS
- Identifier management and maintenance in DIS

Responsibilities on RPs

- Ability to handle multiple identifiers per user and related account management within the RP. DIS will not be able to prevent all scenarios where a user may present multiple identifiers, e.g. Existing user starts using new LoA0 identifier – DIS may not be able to tell this is the same user if the user has not explicitly linked identifiers together.

9. Usage

The aim is to provide straightforward services that allow relying parties to discover whether a user has the relevant [Digital Identity] before asking them to present it. This should enable the user experience to be simplified, with users only being asked to do things they can actually complete.

The APIs allow authentication to be done without identification where the Relying Party either doesn't need it or has other means to determine who the user is. When this occurs the service provides the facility for the RP to feedback information it has about the user to ensure that the user's digital identity grows in usefulness.

9.1. Scenarios

To be done. Describe some user journeys, show how the service supports the journeys and the role an RP will play.

9.1.1. First use of digital identity

TBC

9.1.2. Using existing digital identity with new RP

TBC

9.1.3. End user has multiple IDPs

TBC

9.1.4. End user migrates to new IDP

TBC – ideally this will be invisible to the RP (managed by DIS) so does not need to be described in this RP service description.

9.1.5. Others

TBC