Scottish Government

Digital Identity Scotland

SAPS

Technical Brief for Industry

6 October 2020

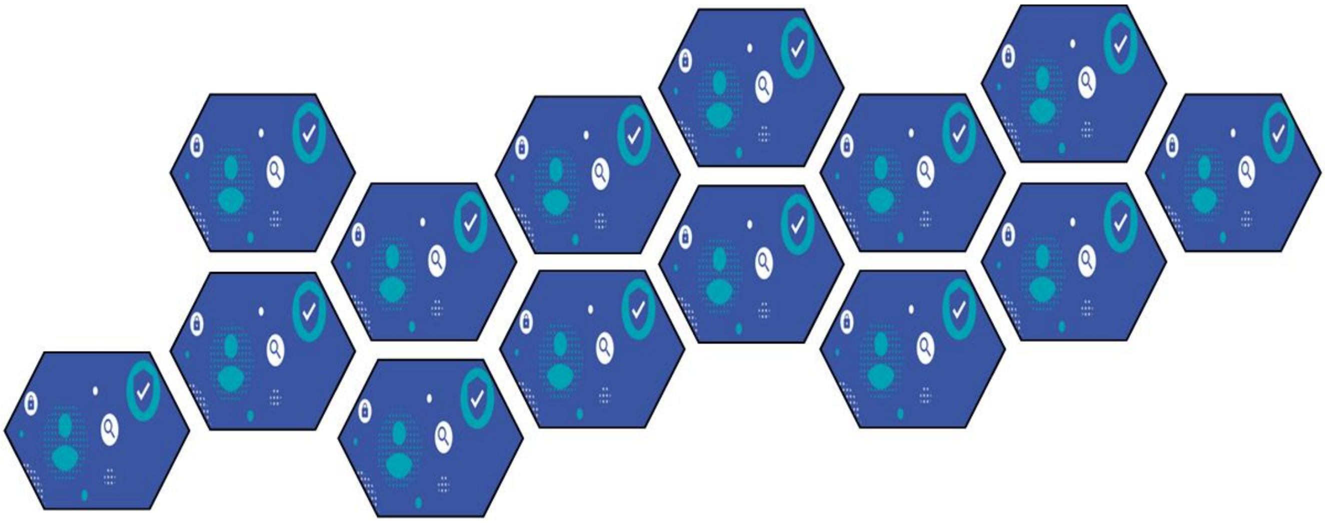


Table of Contents

A. Document History

Author/Reviewed By	Date	Version
Author Claire Lumsdaine	1/10/2020	v1.0
Reviewers Mike Crockart Liza McLean	5/10/2020	V1.0

B. Authorisation

No	Name	Title	Date
1	**Mike Crockart**	**Service Manager, Digital Identity Scotland**	**06/10/2020**

C. Related Documents

Number	Title	Version/Date
1	DIS SAPS Market Engagement Indicative Requirements	**October 2020 v1.0**
2	DIS SAPS Market Engagement Presentation Slides	**October 2020 v1.0**
3	DIS SAPS Market Engagement Presentation Script	**October 2020 v1.0**
4	DIS SAPS Market Engagement Questions	**October 2020 v1.0**
5	DIS SAPS Strategy	**June 2020 v1.0**

1. Introduction

This note is for the market / industry recipients participating in a non-binding PIN *(Ref: AUG392892)* in Q4 2020. It is a brief for industry, overviewing the technical needs of the Digital Identity Scotland, Scottish Attribute Provider Service (SAPS) programme, providing sufficient information that a respondent could respond to the engagement **in an informed and fully contextualised way**. The programme expects responses to its needs and challenges, and wishes to avoid general marketing or pitches based on generalised / hypothesised needs.

This document takes the position of making public significant levels of detail of our considerations to date, and transparently seeking industry comment, proposition and counter-proposal.

We welcome input from the market which will help inform our thinking and are open to suggestions on how to achieve our goals, and alternatives where a coherent case can be made. Any such input received will be considered and may be referred to in future communications from the DIS team.

For a technical audience, this Technical Briefing document, presents a technical overview of the architecture and capabilities needed. The associated document Market Engagement Questions (Ref. 04) contains questions to which respondents may provide responses.

Respondents are also recommended to consult SAPS Indicative Requirements (Ref. 01) which presents some of the high-level indicative requirements for the components in the SAPS architecture included in this market engagement.

Other documents which respondents may consider include the DIS SAPS Strategy (Ref. 05).

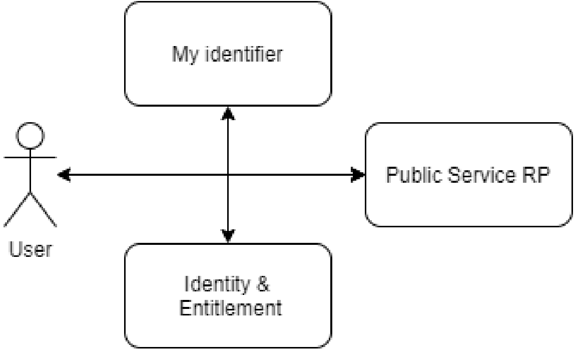
2. Overview of Concepts

This section presents the overall approach being taken by SAPS in addressing the Scottish Government's need to enable digital interaction with the public.

Summary This section presents SAPS as a closed ecosystem, to provide public services, enabling value from one public service, in the form of 'things proved about me', to be reused in another service, in partnership with the service user who is the owner and controller of all their 'verified attributes'. The user experiences lower friction and effort since they are given a single credential, without needing to prove any personal identity attributes, and a secure place only they can access to store and to control their attributes. Only the user can control their otherwise encrypted store; only when in session with a service will their consent be actioned. If they consent to reusing attributes, form filling becomes effortless and errorless and they do not have to provide evidence to reprove their data. RPs receive metadata and proofs of integrity on which to base their business decisions and receive only the minimum data needed and specifically authorised by the owner. Owners can appoint delegates with limited powers of access (and no powers of authorisation policy). Professionals and professional services can provide attestations into the user's store.

2.1 Core SAPS Components

In SAPS, a user has a suitable *secure identifier* associated only with that user, protected to a standard 'level of assurance of the credential', managed by a *Credential Provider (CP),* which enables sign in to each service. The act of 'signing in' discloses no more information to the *Relying Party (RP)* than a unique identifier.



The user has ownership and sole control of their *verified attributes* – identity, entitlement and other attributes. In a verified attribute the data item and related metadata are permanently associated by the originating service and are integrity protected. The user's verified attributes are managed by an *Attribute Store (AtS).*

RPs *may ask* for disclosure of the user's verified attributes, on the basis of which they offer service if the associated metadata matches the service's risk profile. In the course of delivering the service, RPs may ask the user for other data, and may verify other data. RPs *must offer* to return the attributes they verify to the user, so that the user and other RPs can gain benefit in the future. In all cases, the user gives informed consent for disclosure and informed revocable consent for the maintenance of verified attributes by the service.

2.2 Public Service Scope

Our objective is to enable lower friction user journeys for our users of public services. We seek to reduce error, risk, effort and cost in those public services by reusing value created in one service in subsequent services which the user visits. The exclusive focus is on the user and on public services; we do not seek to create an ecosystem open to the private sector, nor, in the main, to utilise private sector data sources. SAPS is a public service to support public services.

As the aspiration is for SAPS to offer authentication and verified attribute services across a wide range of public services, it is vital that the integration cost and skills are manageable for those services. This constrains SAPS technology choices and informs integration capabilities.

2.3 Incremental Trust, Strong Credential

Unlike previous approaches in which the user experienced significant and often insurmountable friction at the start of their journey in a proofing process, SAPS will provide a mechanism for growing trust over time. The user will obtain a zero proofed, but strong authentication credential from the outset. A strong credential is one which complies with GPG44 at least Medium (level 2) as operated by a certified supplier.

The integrity of the binding of the authentication credential to the person (irrespective of the identity of the person) provides a basis for increasing trust over time. Trust in the behaviour of the credential is an element of this trust, but mainly trust is incremented over time by the association of data with that credential and the proof of this data by services using it over time.

2.4 Credential Providers

The SAPS Credential Provider operates user facing services, supporting user registration, providing authenticators (e.g. passwords, e.g. mobile apps supporting push, e.g. grid cards in post, e.g. OTP over landline), offering users a choice of these, and securely operating these authenticators as authentication methods to achieve multi-factor authentication. It enables recovery and repair. It appropriately monitors the credential life cycle. It maintains and uses the minimum personal data necessary to operate their service.

The CP enables user authentication in compliance with an authentication protocol (OIDC) and releases a minimum of personal information in accordance with SAPS standards. SAPS seeks to provide 'near anonymous' authentication in which only a unique identifier is issued, along with authentication context to support security analysis protecting user and ecosystem from attack.

A CP will preferably be GPG44 certified by an appropriate certification body.

2.5 Value is added in Public Services and offered to Users as Verified Attributes

All public services process data to achieve an outcome for the user or the state. Almost always this involves some form of validation or verification of the data provided by the user. For relevant data items SAPS 'attribute origin' RPs will represent this value as metadata elements associated with the data item, and bind the data and the metadata together as a Verified Attribute.

2.6 Service-users keep value in their own Attribute Store

SAPS origin RPs will, via SAPS infrastructure, *offer* the owner user the ability to store the Verified Attribute in their Attribute Store (AtS). The owner is the custodian of the value added by public services. The benefits of the service to the user and to the state are dependent upon uptake and cooperation, thus on transparency and trust.

An AtS instance, at no cost to the user, is owned and controlled by the user, the data subject of the Verified Attributes. Their AtS stores only their Verified Attributes, and only the data subject controls access to it by means of a Consent Management feature. Only the owner can view the contents or manage their consents. Only the owner (or their delegate) can decrypt the contents of their AtS (not the government, nor the supplier of the AtS service).

2.7 The user is in control – Consent Management

The user may accept the *offer* of having a SAPS Attribute Store, this is optional. (Of course, SAPS and public services will encourage this ownership as it is mutually beneficial.)

Consent for attribute receipt and disclosure is managed (policy) and enforced (authorisation) at the AtS. The AtS has an integral feature – a user-facing Consent Management capability, at which the user can view and maintain consents.

Usually such a consent management process will occur when the user is authenticated to both an RP *and* their AtS, as part of a user journey to access services provided by an RPThus, normally these components will have a concurrent user session, initiated following authentication by the federated CP. In addition, the user can authenticate to their AtS and revoke consents at any time, irrespective of RP involvement.

The user may *accept* an offer of a verified attribute from a public service origin RP, by giving *consent* for that attribute to be written to their AtS. Additionally, and optionally, the user may consent to having the attribute maintained over time.

Similarly, when the user is seeking a public service at an RP, this 'consuming RP' *requests* verified attributes from the user. The user may give *consent* for their AtS to disclose a verified attribute, to that service, for that occasion only, while the user is in session with the RP and their AtS.

Given that, at all times the user is in control of disclosure, and of update, and of selection of attributes for disclosure, two key characteristics of the service are clear:

- Consuming RPs cannot rely on an attribute as being 'guaranteed' up to date. So, RPs must have their own assessment of metadata and associated risk management (just as they do in current processes, where almost all data items have no metadata at all).
- The SAPS service is to encourage low friction, effort, error, cost and risk data integration via the user; it is not a counter fraud service, it is not a mechanism to broadcast data.
  Only a partnership of trust between the user user and the public services will achieve the intended mutually beneficial outcomes.

2.8 The user is the point of integration

The user, as controller of their AtS, is the *only* point of integration of personal attributes in SAPS. (SAPS is not a system to system, nor organisation to organisation 'data sharing' scheme). Verified attributes are persisted in the AtS; in the AtS the attributes are *outside* the scope of any public service RP.

Only the user can enable attribute update by, or disclosure to, a public service. The user must be present *in session with any SAPS public service* for their consent to be given to the Consent Manager for disclosure or to be acted upon for the AtS to write an update.

When a consuming RP asks for disclosure of verified attributes, if consent is given and the user has selected appropriate attributes, the Verified Attributes (as an indivisible whole, including all their metadata) are disclosed to the RP. Usually this RP will automatically populate relevant forms or other UI structures with the data from the Verified Attributes. In this way the user sees that they are the point of integration (all data comes from them, from their AtS), and the user experience is that of 'filling the form automatically with data already proved about me'.

2.9 Minimal Disclosure – Derived Attributes

SAPS RPs (and in general DPA18 compliant services) must ask for the minimum personal information they need to meet their outcome.

Attribute Stores will include standardised mechanisms for deriving attributes, e.g. age derived from date of birth and current date, e.g. over 18 today, e.g. number of children from children's details, e.g. is resident of local authority from residential postcode.

In addition, SAPS specialised services *(stateless services)* are provided to derive attributes by arbitrarily complex rules from the existing content of a user's AtS. The user consents to this assessment (a disclosure to the specialised service) and their AtS receives a new verified attribute which represents the results of the derivation. This enables complex derivations based on business rules, outside the remit of the AtS provider.

A particularly important example of such a service is IoDS, section '4.9'.

2.10 RPs and the AtS all use Standard metadata

Origin RPs, consuming RPs and the AtSs all need to process metadata.

Origin RPs author metadata based on the process outcomes which to some level and in some way 'proved' the associated data item.

Consuming RPs formulate requests for Verified Attributes by creating 'templates' of metadata. An example of such a template is: address (name of attribute class), residential (semantic modifier), less than 6 months (timeliness of last proof), postal-loop (minimum assurance level).

At the AtS, if templates match against the user's available attributes, these attributes might fulfil the RP's need. (Of course, even when they match, the Verified Attributes are not disclosed without explicit consent of the owner.)

Consuming RPs know that the Verified Attribute is reliable as it has integrity controls imposed at the origin. Consuming RPs interpret standard metadata in line with their own error and risk management needs.

Thus, there is a need for a cross eco-system standard for metadata. SAPS is creating such a standard and intends to increment this standard over significant time as new RPs are onboarded, and the spectrum of use cases grows, and the range of assurance processes is expanded. This is another advantage of SAPS closed public service focus: it can iteratively develop standards as needed, and accordingly need neither wait for, nor be bound by, external standardisation or other processes.

Of course, SAPS will monitor potential metadata standards as (and if) they emerge. SAPS can also provide translation for down-stream uses (such as asserting an identity to an external scheme), so this lack of universal or open standards is not seen as an impediment to making progress in Scotland.

2.11 Delegation

Some SAPS users may wish to appoint another SAPS user for the purposes of administering their affairs at a particular SAPS RP. (Note both parties are assumed to be users of SAPS CP and AtS services; other forms of proxy or attorney relationship may be considered separately.)

Such delegation necessitates:

- Appointment of delegate by the owner-user (represented by a Verified Attribute in their AtS containing the unique identifier of their delegate).
- The owner setting consent policy at their AtS so that the delegate can access (disclose and update) specific attributes when the delegate is in session at the specific service.
- Arrangements at SAPS RPs so that they offer a 'delegation aware' service in which the delegate authenticates and proves a claim to represent the owner in the owner's account at the RP (i.e. the service obtains the delegates identifier and tests against the claimed owner-user's AtS).
- Capabilities in infrastructure and in the authorisation process at the AtS to disclose / update according to the owner's policy whilst their delegate is in session with SAPS service.

2.12 Attestation

A SAPS user may ask (out of band) a professional or other professional service provider to issue an attestation about them (e.g. 'a proof that I have diabetes'). Such a proof would typically be needed to prove an entitlement when subsequently processed by a SAPS RP.

The request relies on pre-existing relationships with the professional, identity proofs and professional record systems; all of these are outside the scope of SAPS. In the out of band conversation the data subject asks the professional and provides a single-use credential, issued previously to the SAPS user for this purpose, to the professional. The professional creates the attestation in a suitable system (probably an enhancement of an existing professional system), associates the user's credential, and the system sends the attestation to a SAPS adapter service. The adapter constitutes a SAPS standard Verified Attribute using the attestation from the external service and, using the user's credential, obtains the user's identifier so that the Verified Attribute containing the proof is queued for the next time the user authenticates to a SAPS service.

When the user authenticates in SAPS (perhaps to the RP offering the service for which the proof is required), they consent to receiving the Verified Attribute and can subsequently disclose it to the RP.

Such a capability has many uses beyond medical certification. Given suitable enhancements to system and process in government or commerce it might be used to obtain proofs of land ownership, or driving licence, or provide financial status. It could also provide one mechanism to loosely integrate Identity Attribute Providers without the involvement of a SAPS RP (see also section '4.8').

3. SAPS Capabilities – technical overview

This section visits SAPS capabilities and discusses its technical characteristics, with the objective of shaping the needs at a higher level than requirements (which are Ref 0.1). It outlines SAPS thinking and demonstrates how the components interact to deliver service. Summaries of use cases motivate component collaboration and associated flow diagrams are given to aid understanding.

3.1 Use Cases

The **core SAPS** service offering may be summarised by the following user stories / use cases.

1. Given I want to use a digital public service to which I need to return, I want a secure way to **sign me in** to a public service so that I can keep my account safe across sessions.
2. Given I want to remember and use the fewest number of mechanisms to log in, I want every public service to use the same **sign me in** service so that I can gain access to all public sector services.
3. Given I want to have as few possible steps in my journey, I want **sign me in** to operate across the parts of my journey (the Attribute process, the Consent process, as well as the service itself) so that I don't have to repeat signing in to the components to achieve an outcome in a session with a public service.
4. Given I understand that each public service has to 'verify or prove' 'things about me', called 'verified attributes', I want to be able to **reuse my evidence** from one service whenever I give consent in another public service.
5. Given all my personal data and evidence belongs to me, I want to **lock my evidence** so that I am in complete control of it and I am assured of its security, so that I can be comfortable and reuse my evidence for my benefit, and for the benefit of other public services.

In addition, the following use cases enable **standard identity attributes** to be consumed or to be produced.

6. Given that I need to prove my identity to a standard for a service[1], I want to reuse my locked evidence to obtain a proof of identity.
7. Given that I need to prove my identity to a standard for a SAPS service, I want to obtain a proof provided by an external identity service[2].

This section does not discuss the use cases associated with **delegation** or **attestation**.

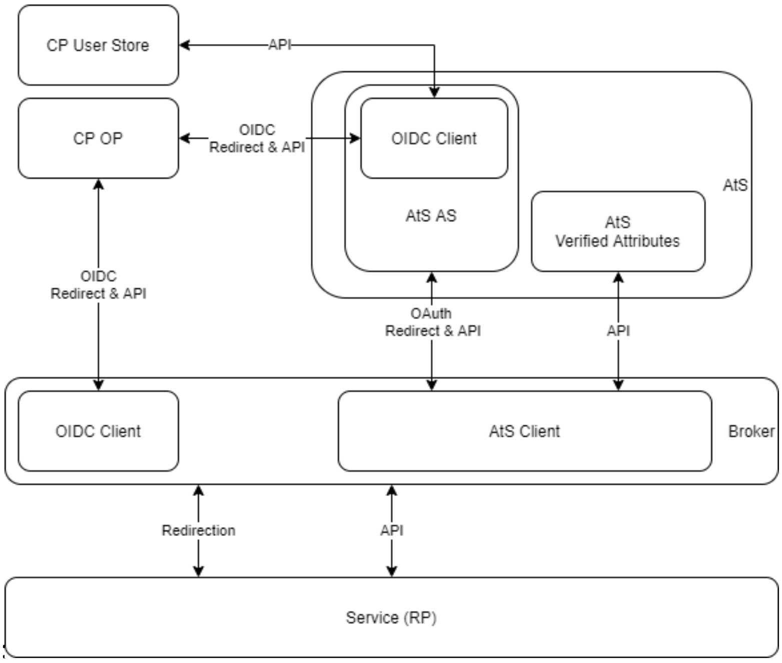
3.2 Core SAPS Components

This diagram shows components (CP, AtS, Broker and RP) which can deliver SAPS core capabilities, and indicates *one possible implementation* using OIDC and OAuth protocols.

(We note this is only one possible protocol set. See also section '4.6' which raises the desirable option of UMA for comment in this RFI. See also sections '4.10, 5.2' which request response from the SSI community.)

[1] A SAPS service, **or** a non-SAPS, external public service such as a UK gov service.

[2] Such as a (future) 'Verify 2' IDP, or in this document, an external Identity Attribute Provider (IAP)



Notes on diagram:

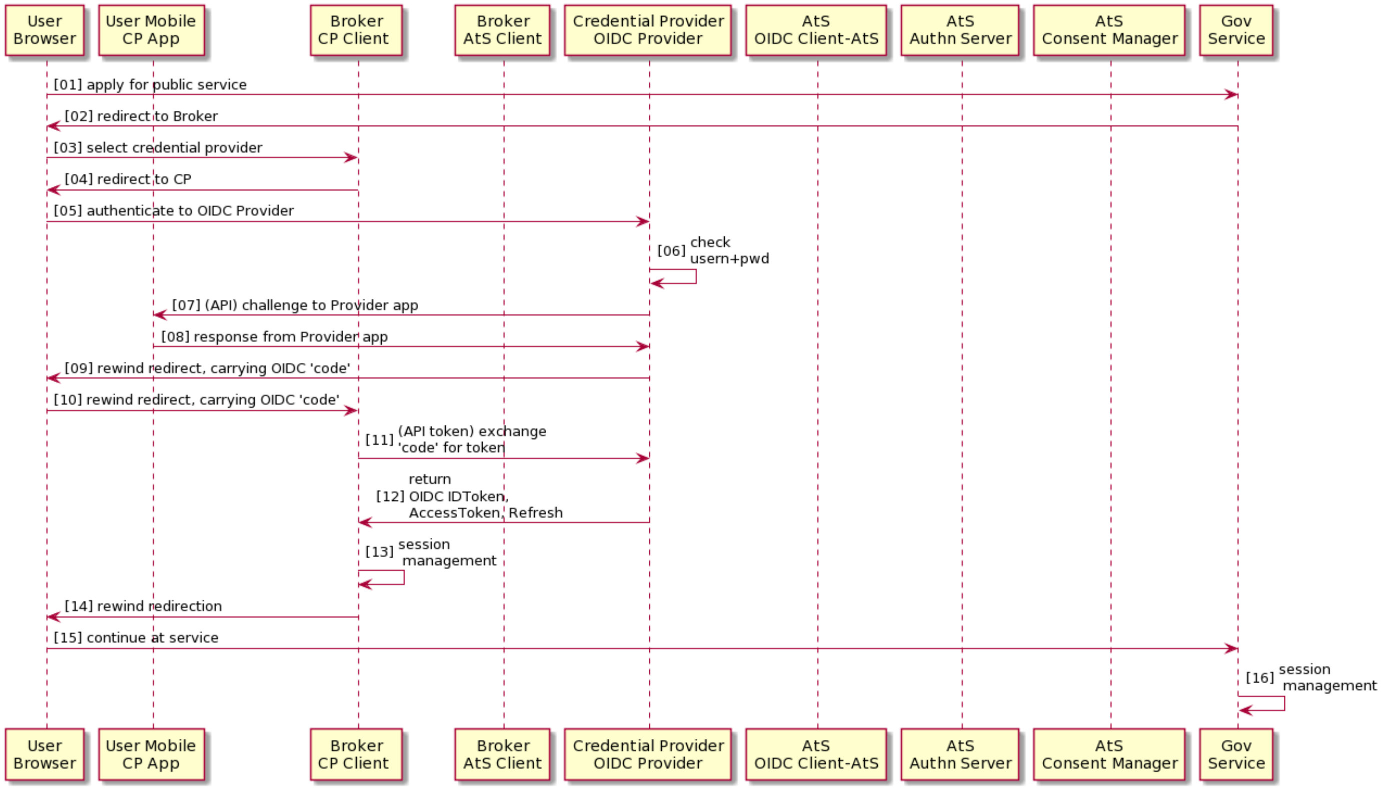
- An Open ID Connect Provider in the CP has clients in the broker and the AtS.
- The Broker OIDC CP Client supports authentication to the Service/RP (Section '3.3' below.)
- The AtS OIDC CP client supports authentication to the AtS. (Section '3.4' below.)
- The CP exposes an API to its user profile, authorised by its OIDC Provider authorisation server, for writing arbitrary custom claims. (Section '3.4' below.)
- The AtS exposes an API to the AtS verified attribute store, authorised by its OAuth authorisation server, so that the broker can read / write attributes.
  The Broker AtS Client utilises the AtS API. (Sections '3.6, 3.5' below.)
- The RP Service to Broker protocol is of secondary concern in this paper and details of RP-Broker integration are omitted.

3.3 Authentication

Use cases 1&2

The CP provides a service to register a user and manage credential lifecycles to GPG44 Level Medium, collecting minimal personal information to do so; it provides the means to authenticate to public sector SAPS compliant RPs and to the AtS.

An implementation using OIDC supports both web clients, with an out of band second factor, and mobile app authenticators. For example, the following diagram shows a user authenticating to a service using a CP with a mobile app authenticator.



This is a standard OIDC redirection flow, using a back channel authentication app as a second factor. Ultimately the CP OIDC provider returns an ID Token to the Broker CP OIDC Client, which starts a session at the broker.

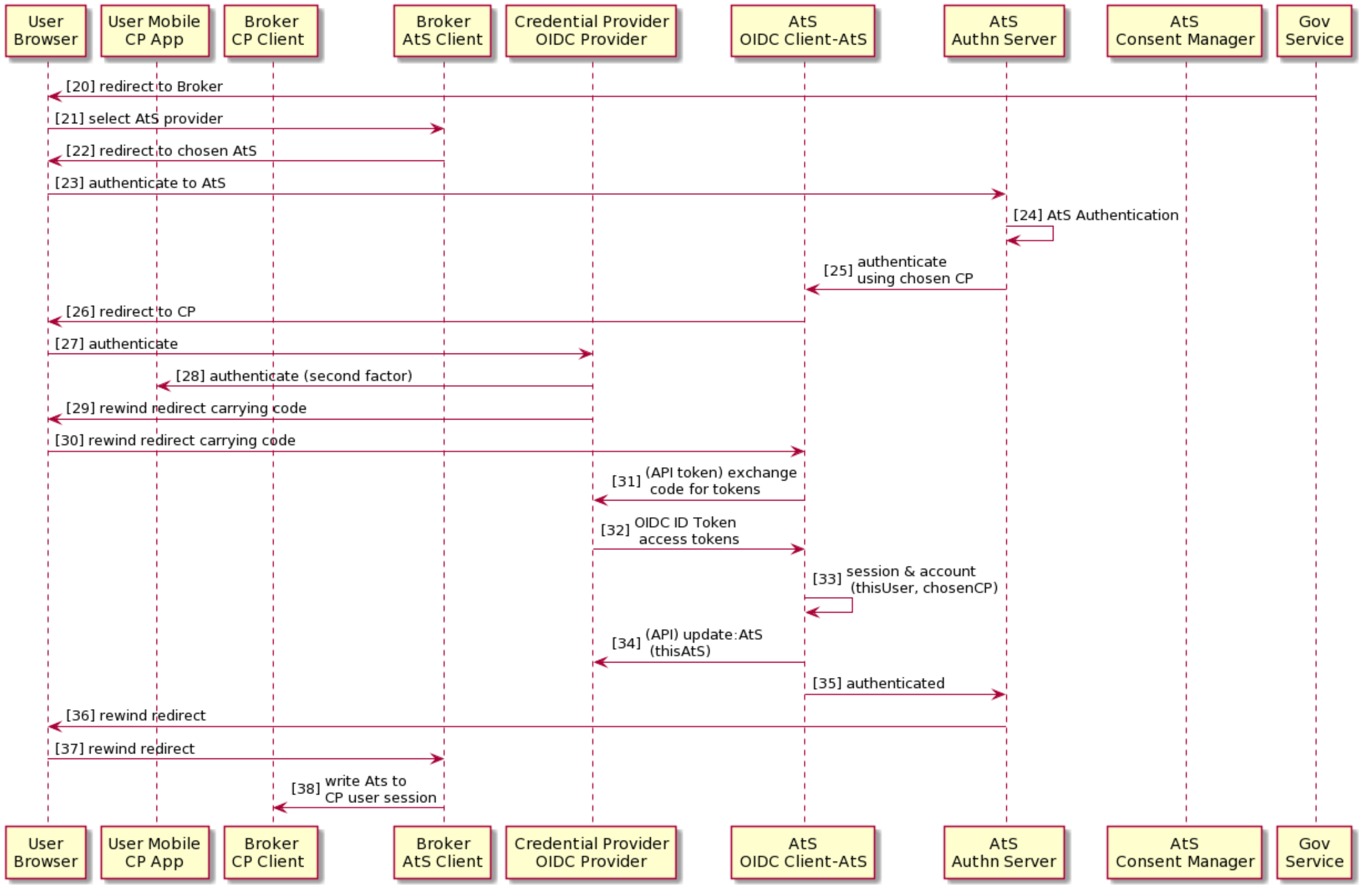
We note that there will be *three* sessions in progress after this flow: CP, Broker and RP. In later flows we see a *fourth* session at the AtS.

3.4 Provisioning and Binding an Attribute Store

Use case 3

Provisioning an AtS instance for a user might be via API call to the AtS provider or it might be via web redirection of the user to the AtS provider. Either way, initially the user will need to interact with the AtS instance directly to establish confidentiality and recovery mechanisms so that the AtS account can be protected and recovered if the user loses their CP account. The AtS must accept the CP as a federated authentication provider, so that the user subsequently experiences minimal friction through a single sign on across RP and AtS. The AtS and the CP accounts are associated – this 'binding' is persisted – specifically in the CP user profile (as encrypted claims) as well as in the AtS.

When an RP has attributes to offer to the user, or otherwise when an AtS is being provisioned to the user, the browser is redirected to the broker (step 20 below). The following sequence diagram illustrates the 'binding' of a CP account to an AtS instance – i.e. establishing a federated authentication of the AtS by a CP. The result is that both the CP and the AtS 'know' about each other, and the user can authenticate to the AtS with minimal friction in future interactions.



Here the AtS is provisioned either previously or on the fly (just before step 23). Either way, the user may need to authenticate using credentials specific to the AtS instance at step 24. If this is the first visit to the AtS, the user will probably also establish recovery codes and protocols with the AtS at this point.

Step 34 writes the AtS instance handle to the user profile at the CP. Step 33 keeps the CP account handle at the AtS.

The authentication steps themselves (26-32) will only be visible to the user if the CP (which will usually be in session if the user was authenticated prior to this flow, for instance with the RP) chooses to force additional authentication; perhaps in the case above, the CP may limit itself to a push message ‘Bind to your AtS y/n?’ at step 28.

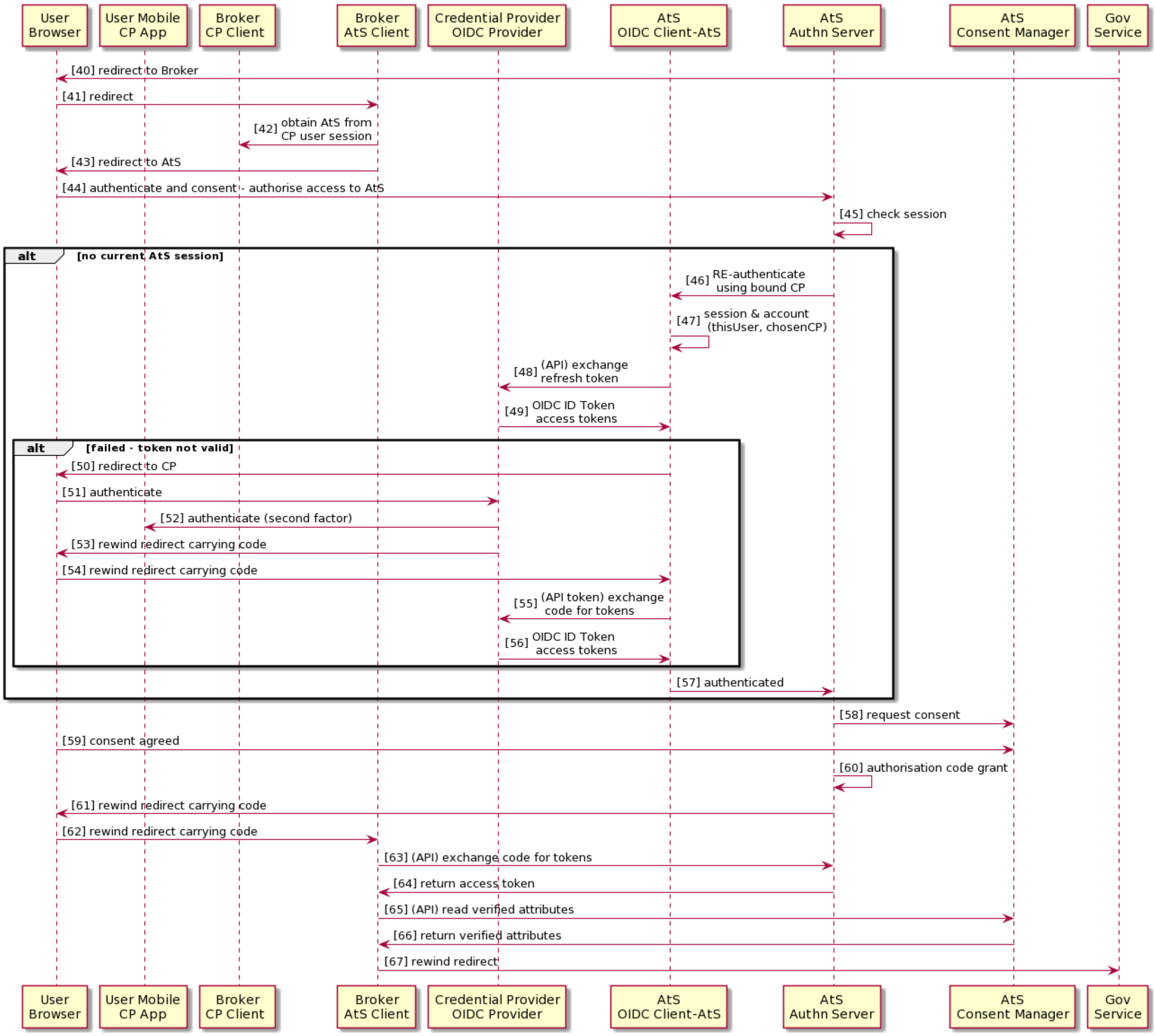
3.5 Disclosing Attributes

Use case 4

When a consuming RP wishes to obtain verified attributes, metadata describing the service’s *requests* are processed by the AtS, potentially matching attributes are located and presented to the user, and the user consents (or not) via their AtS Consent Manager to their disclosure to the service.

Consent means: Only ‘the specific service I am signed into NOW’ can see only those ‘specific attributes’ to which ‘I consent, NOW’.

The following sequence diagram illustrates a front channel (standard browser) flow in which the AtS uses the ‘bound CP’ – to federate OIDC authentication in steps 45 to 57. If the user consents to matching attributes being disclosed, steps 58, 59, an OAuth authorisation token is issued for reading the AtS verified attributes, steps 60 to 67.


User Browser
User Mobile CP App
Broker CP Client
Broker AtS Client
Credential Provider OIDC Provider
AtS OIDC Client-AtS
AtS Authn Server
AtS Consent Manager
Gov Service
[40] redirect to Broker
[41] redirect
[42] obtain AtS from CP user session
[43] redirect to AtS
[44] authenticate and consent - authorise access to AtS
[45] check session
alt [no current AtS session]
[46] RE-authenticate using bound CP
[47] session & account (thisUser, chosenCP)
[48] (API) exchange refresh token
[49] OIDC ID Token access tokens
alt [failed - token not valid]
[50] redirect to CP
[51] authenticate
[52] authenticate (second factor)
[53] rewind redirect carrying code
[54] rewind redirect carrying code
[55] (API token) exchange code for tokens
[56] OIDC ID Token access tokens
[57] authenticated
[58] request consent
[59] consent agreed
[60] authorisation code grant
[61] rewind redirect carrying code
[62] rewind redirect carrying code
[63] (API) exchange code for tokens
[64] return access token
[65] (API) read verified attributes
[66] return verified attributes
[67] rewind redirect

Of course, if the AtS is already in session (45) or a session can be renewed by API (47-49), or if the CP has a current session (51) the user will see no additional authentication activity, and the first apparent interaction with be consent for disclosing attributes (58).

3.6 Writing Attributes

Use case 5

When an originating RP offers verified attributes, the user needs to consent (or not) to them being stored in the AtS. Users do this at their AtS' Consent Manager UI which might be offered by web redirection or via an AtS Consent Manager mobile app.

Consent means: 'Specific attributes' will be written to by 'the specific service I am signed into NOW', to which 'I consent NOW' for '*a single-update'* and (optionally) '*maintenance* over <time period>'.

Separately the user may also authenticate to their AtS and modify such consents, for instance by revoking them.

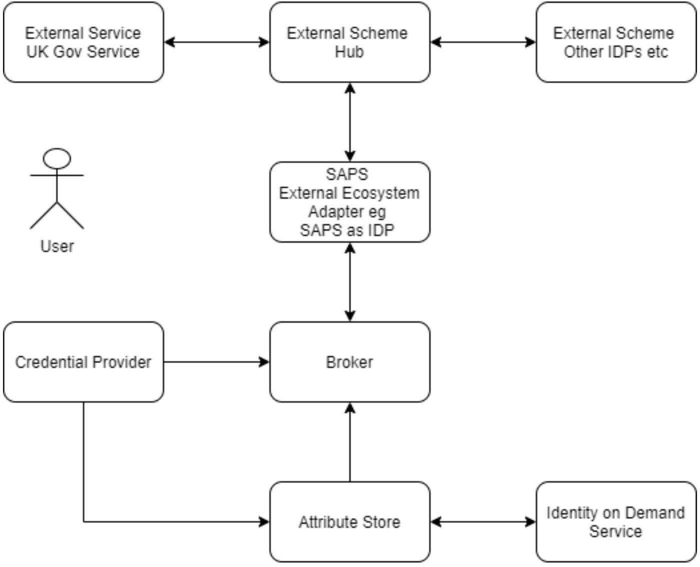
The flow in the previous section (Disclosing) is almost the same as that required for initially writing attributes: only the grant (60) would match the consent and the AtS API would be 'write' at step 65.

Whilst the flows here have presented full front channel web redirect for reading or writing we are investigating back channel variants to an AtS Consent Manager native mobile app which may have benefits for the user journey. Please see section '4.6.

3.7 Identity on Demand Service (IoDS)

Use case 6

A user can consent to an assessment of their Identity Level of Confidence (LoC GPG45) from a specialised SAPS service in the form of a verified attribute. This is managed by the stateless service 'Identity on Demand' (IoDS) in the lower part of this diagram which *derives* the LoC attribute from relevant attributes already in the AtS (see also more detail in section '4.9'). Such a verified attribute can be consumed by a SAPS service in the same way as it consumes any other attribute.

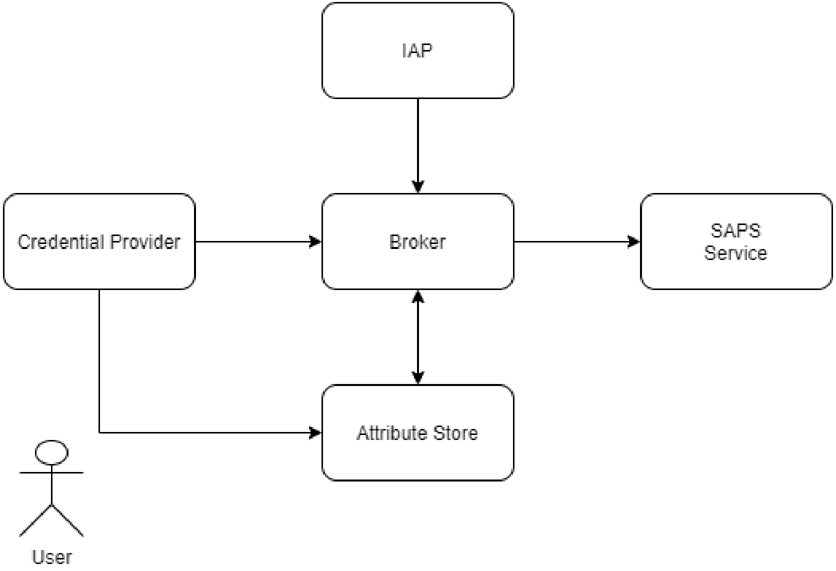


Separately, if an assertion is required for an *external* scheme or federation, the LoC verified attribute can be transformed as necessary and the SAPS service becomes an 'external Identity Provider' to that scheme.

3.8 Identity Attribute Provider (IAP)

Use case 7

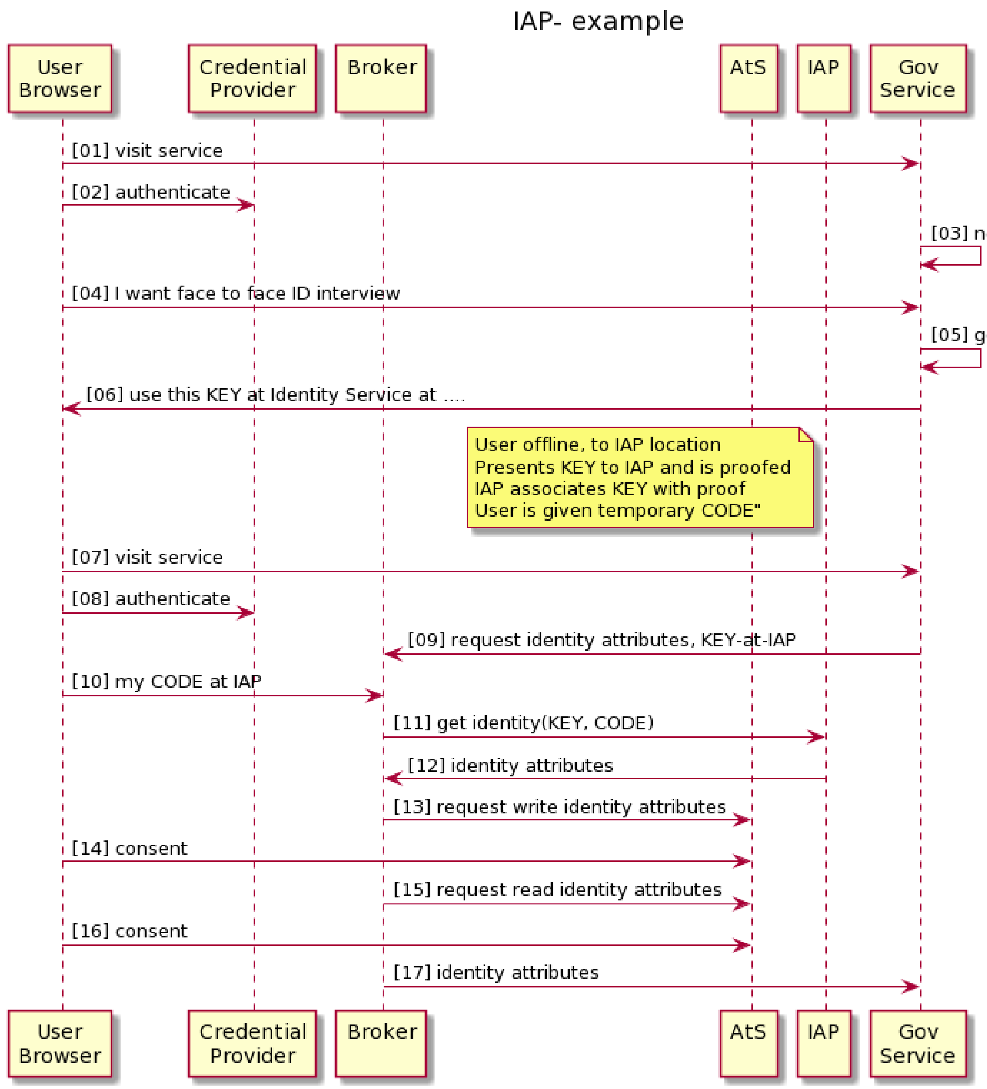
The user may be asked to undertake an identity proofing process (GPG45) producing identity attributes and a level of confidence assessment, in whatever channel is appropriate to the user. An external service (IAP) can provide these attributes into the user's AtS, from where they are subsequently disclosed with consent to SAPS consuming RPs. Having been written to the user's AtS they behave *just* *as any other SAPS Verified Attribute* - the user may consent to release them to a SAPS public service.



There are a variety of possible integration schemes which achieve transfer of trust. For instance if the IAP is a 'verify like IDP', then it will provide the user online credentials so that the user can authenticate to it later, *whilst also in session with the CP/AtS*, so that *the IAP attributes can be retrieved in a trusted context and written to the user's AtS*.

The following flow is purely for illustration.

A different flow follows as an illustration, using an out of band transfer of trust to support face to face proofing at a loosely coupled IAP. In this example we assume that the RP is responsible for the business decision to outsource a proofing activity; (other models are possible which might be administered only by SAPS broker & AtS components, enabling the RP to be completely independent of the proofing process).


IAP- example
User Browser
Credential Provider
Broker
AtS
IAP
Gov Service
[01] visit service
[02] authenticate
[03] needs identity proof
[04] I want face to face ID interview
[05] generate and keep key
[06] use this KEY at Identity Service at ....
User offline, to IAP location
Presents KEY to IAP and is proofed
IAP associates KEY with proof
User is given temporary CODE"
[07] visit service
[08] authenticate
[09] request identity attributes, KEY-at-IAP
[10] my CODE at IAP
[11] get identity(KEY, CODE)
[12] identity attributes
[13] request write identity attributes
[14] consent
[15] request read identity attributes
[16] consent
[17] identity attributes
User Browser
Credential Provider
Broker
AtS
IAP
Gov Service

A service determines that an authenticated user needs an ID proof and agrees the user's needs, in this example, for a face to face ID service. A key is generated (05) which will be recognised by the IAP which may also serve as a billing code after the identity is proofed. The service keeps the key so that the authenticated identity from the CP (the user identifier) can be correlated with the returning identity attributes in a future online session, and the user is given the key in some useable form QRcode, post, etc, (06).

The user visits the IAP and is proofed and given a code to enable retrieving the attributes, and then returns to the service and authenticates (08). The service can then initiate a request for identity attributes by redirecting to the broker (as for normal attribute disclosure). The user gives their code (10) and the broker obtains the attributes (11, 12). Before they are returned to the service, the user consents to updating the AtS (13, 14), and disclosing the identity attributes to the service (15,16,17).

(See also '4.8' for more detail on IAP.)

4. Market Engagement – Capabilities

This section highlights each capability for which we are seeking information. Each capability has a sub-heading here, so that respondents can be clear under which capability(ies) they are commenting and answering questions in the separate Market Engagement Questions (Ref. 04) related to that capability.

4.1 Development/Delivery Partner

In order to help DIS create and initially deliver SAPS, we may require the services of a partner with the requisite skills and experience to work with us.

The characteristics DIS currently believe will be important in a Development Partner are listed below. We would welcome feedback, challenge and alternative approaches as part of your response to this market engagement exercise.

4.1.1 Capacity and Skillbase

We believe we may need a team of between 10 and 20 people over the next 2 years to help deliver SAPS. This may include Programme/Delivery Managers, Technical Architects, Business Analysts, Developers, Testers, Service Managers and Support Analysts.

We prefer to work in an agile manner, and believe a partner would need to demonstrate technical capability in a range of technical areas to support the integration of composite solutions and services to form SAPS, including Cloud technologies, standards such as OIDC and OAuth, DevOps practices. Any partner is likely to have extensive Identity experience and a pool of data analysts to call upon as required. Given the likelihood of integrating several constituent services, we would expect any partner to have demonstrable, relevant commercial expertise.

We are considering whether it may be advantageous if any Development Partner has access to the building block services of DAPS through its own supplier ecosystem. As such, this could provide an option to simplify the management and development/delivery of those building blocks into SAPS overall. DIS and the Development Partner would agree the specification/requirements for the building block, but then the Development Partner can secure the appropriate solution and integrate into SAPS.

More specific expectations are shown below.

4.1.2 Engineering

The partner should demonstrate capability and routine delivery of solutions using:

- CI/CD – continuous delivery to live
- Continuous Test, including security testing
- Cloud Native architecture and delivery
- Infrastructure as Code
- DevOps and SecOps
- Cloud (preferably AWS) experience of the above

4.1.3 Technology

The partner should be able to demonstrate capability and delivery of solutions which include the following technologies.

- OAuth2, OIDC, UMA2
- Structured Tokens in protocols
- Open Banking protocols including CIBA, app2app, sender constrained tokens
- Cryptography & PKI, JOSE, *and preferably* Proofs and Zero Knowledge proofs
- Authenticator design / application
- Native mobile app technologies
- *and preferably* SSI, DIDs, DIDComm, DPKI, VCs

4.1.4 Design

The partner should be able to demonstrate capability and availability (on their staff roll) of persons with the following capabilities.

- Architecture and Design capability - to integrate with the client design team including specialist identity and open standard protocol architects with a deep knowledge of Customer Identity and Access Management (CIAM).
- Security Architecture - specialising in ecosystems and multi-component distributed architectures, perimeter-less security models, zero trust solutions
- MetaData Design – support client design of the metadata of verified attributes, including working with business service owners. Application of no-sql and graph technologies to support search and in integration with legacy software environments.
- Integration Architecture – distributed brokers, protocol management, integration with complex existing services.
- Trust Frameworks – ecosystem wide inter-organisational agreements and technical solutions for trust framework delivery, e.g. distributed security architectures, PKI, distributed trust mechanisms.

4.1.5 Culture and Ways of Working

- Supporting open collaboration across all functions and especially with Scottish Government staff which form part of the team to focus on delivery of value (iteration, design, engineering)
- Embracing user-centred design and co-design concepts, accepting and interpreting iterative feedback from Scottish Government user experience and service design teams and working to iterate products
- Willingness to work with novel technologies and SME suppliers to engineer a solution in line with Scottish Government/Supplier co-architecture/co-design team.
- Lack of a ‘change control’ commercial culture – collaborative delivery expecting change and discontinuity.
- Management of delivery and of financials which is compatible with co-design teams and iterative delivery, transparency of true cost and resource consumption and clear shared value arrangements.
- IPR to be solely and only vested in and owned by Scottish Government, although we are open to alternative options which can help to de-risk development/delivery and leverage value.

4.1.6 Operating

Whilst the key attributes of a development partner cover working with us to develop the DIS SAPS solution, we appreciate that there is a need to operate and deliver the service, both through development and beyond into go-live and continuous improvement. As such, potential development partners who can demonstrate they have the key skills and proven experience in operating services such as DIS SAPS could offer added value.

Whatever, we would seek to develop the solution with the flexibility for the Scottish Government to take a final decision on the long term operation of the service without having to be tied into any particular development partner.

4.1.7 Experience

We would likely seek a partner with a demonstrable track record of successful delivery of similar size programmes, across both public and private sectors, with the ability to reference such success. Whilst there may not be identical programmes to reference, we would expect potential development partners to be able to demonstrate real and recent applicable experience which our programme can build upon. Especially relevant here is a track record of effective knowledge sharing and transfer across customer teams, to reduce ongoing reliance and give us the flexibility in determining the ongoing operating model for DIS SAPS.

4.1.8 Principles

The Architectural Principles which we'd expect any partner to work within include:

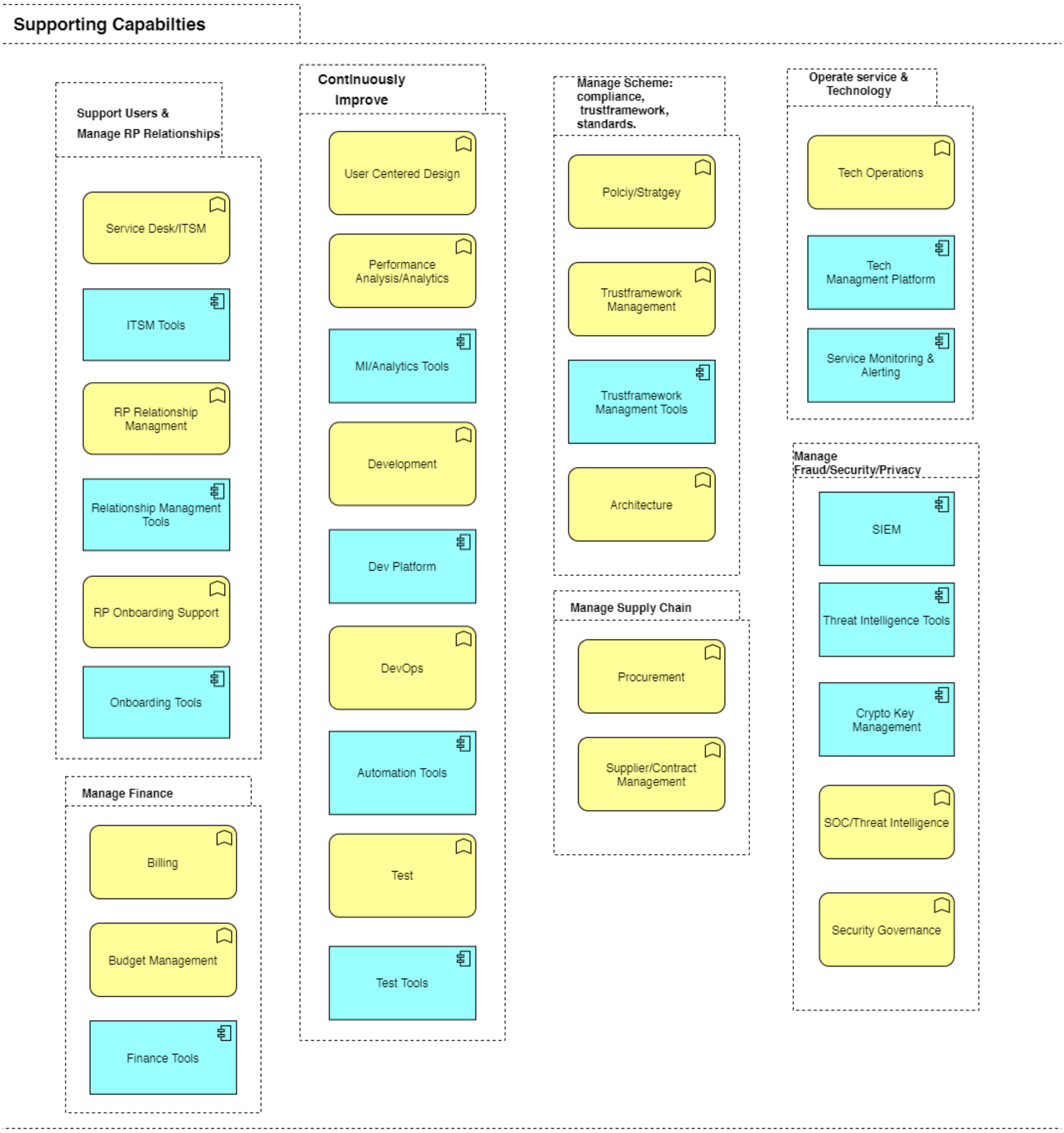
No	Principle	Meaning	Rationale
1	Reuse before build, before buy	Where appropriate services exist within the public sector these should be re-used. This re-use could range from reusing an existing platform service to re-use of a service design pattern or technical component. DIS is assuming that reusable identity/attribute components of the service do not already exist. Therefore DIS has a strong preference to buy the majority of the core identity components as cloud based SAAS services. Where re-use and SAAS are not viable DIS will consider building or customising.	Re-use of existing services is financially efficient and also increases delivery speed and reduces delivery risk. The use of carefully integrated SAAS services will provide increased delivery speed and reduced risk while allowing future flexibility. Building software while higher risk may be the best way of achieving the innovation required to deliver DIS and we appreciate that a level of software development is likely with any solution.
2	Architect for flexibility and continuous change	The architecture will be designed as a set of loosely integrated components which can be able to safely and easily changed in a continuous manner. An architecture composed of smaller decoupled and functionally cohesive services is preferred. DIS will avoid the unnecessary use of vendor specific features. Commercial arrangements need to be flexible. This principal indicates DIS will use hyperscale public cloud services for both SAAS services and any dev/test/integration/ops capabilities it	The understanding of user needs will evolve and DIS requires to continuously improve the service as these learning emerge. Digital identity and verified attributes is a rapidly evolving area. DIS wishes to maximise its opportunity to capitalise on technology innovations which would improve the service. Market changes may occur which are not innovative but provide more attractive service

		requires. Public clouds offer the flexibility , breadth of capabilities, capacity and security required. The trade-offs between flexibility, performance and complexity will need to be understood and managed. In terms of build, integration and test these need to be automated using DevOps practices to support safe predictable change. See 'Automate Everything'.	offerings . DIS wants the flexibility to benefit from these.
3	Maximise Automation	All aspects of the technical solution should be automated and available on demand. This includes build, test, configuration, environment provision, user & RP provisioning. A consequence of this DIS SAAS services or other capabilities will likely be hosted in public cloud providers. DevOps practices will be used. DIS recognises building automation is an initial complexity but one that will provide good foundations on which to proceed.	Automation facilitates predictable delver, consistent quality and enables safe change.
4	Just Enough Architecture	The design approach is not "big design upfront". The architecture will stay sufficiently ahead of delivery to ensure strategic alignment with the business objectives. The design will be continuously iterated based on changes in the overall service strategy and learnings from users and the delivery teams. Areas of highest technical risk will be architected and built (perhaps a proof of concepts) earlier in the delivery. Architects will work as part of delivery teams and ensure a collaborative two way feedback loop exists in the technical design process.	Allows architecture to easily adjust based on real world feedback . Reduces overall risk by addressing high risk areas early. Given we have a hard, significantly cutting edge set of problems to address, we appreciate this may not always be feasible.
5	Technology Based on Standards	DIS will prefer to use proven standards where these exist over developing new standards. Where existing Scottish government standards apply DIS will follow these e.g. Digital Service Standard. DIS will also likely either adopt or align to the UK government identity standards including and any emerging GDS standards. In some areas where no relevant standards exist, e.g. MetaData, DIS will develop standards.	Using proven standards reduces the risk associated with developing new standards which may not work. Interoperability and flexibility are enhanced by use standards. Transparency around the use of standards builds public and stakeholder trust and confidence.

		DIS will be transparent about the standards it uses and develops and ensure appropriate compliance across the SAPS ecosystem.	

4.1.9 Service Capabilities Scope

Any development partner will be required to work beyond the boundaries of the core identity block to support the development of the wider capabilities required to run an operational service. DIS' initial analysis of the supporting capabilities required are outlined in the diagram below.



4.2 Core SAPS - Credential Provider

The CP might be operated as SaaS (an example of this was mentioned in blog https://blogs.gov.scot/digital/2020/05/13/digital-identity-scotland-prototype-draws-to-a-close/). Such a capability offers OIDC Authorisation Server, authenticator choice, authentication methods, (minimal data) registration, and credential life cycle management in the remit of the outsourced supplier. Clearly there are many market participants in this area, so we are specifically interested in responses to the questions posed in the accompanying attachment.

We want to offer a seamless service within the CP, RP, and AtS capabilities. One dimension of this is using the user profile in the CP to hold custom claims indicating the AtS instance. Another is a desire to ensure a common app or inter-app protocol for Authentication and Consent Management (Authorisation). Another potential collaboration is to use a common Authorisation Service which might also support appropriate fine-grained authorisation and delegation using the UMA open standard (see '4.5').

Respondents are also requested to see Indicative Requirements (Ref. 01).

4.3 Core SAPS - Attribute Store & Consent Manager

A key component of the user managed SAPS eco-system is the Attribute Store.

An attribute store instance may be provisioned for a user on request by a user (web interface) or via an API from SAPS infrastructure.

An attribute store may have a mechanism of authentication and / or recovery as provisioned by the AtS provider.

An attribute store must accept federated authentication from a SAPS CP, enabling its owner to be in a single session with SAPS CP, RP, and the AtS.

When an owner is disclosing attributes to a SAPS RP the AtS offers capability for the user to select from attributes in the store which 'match' the requirement as expressed by the RP.

The user is in sole control of their permissions to disclose attributes from their store, to write and to maintain attributes to their store, and to delegate access to their store. Such control is exercised by the user, when authenticated to their store in a Consent Manager which is an integral part of the AtS. The consent manager UI may be via a web or via a native mobile app.

Only owners or their delegates may access data in the store. Only owners may set consent policy for RPs to read or write data. Delegates may not access / browse attributes in the store.

Data in the AtS must be encrypted so that only the user or their delegate can decrypt it.

AtS capability should include the creation (and signing) of derived attributes (see '2.9' above).

Respondents are also requested to see Indicative Requirements (Ref. 01).

4.4 Infrastructure – Broker

It is vital that the integration cost and skills are manageable for SAPS services. We plan to provide an internal capability which minimises integration costs and separates concerns of SAPS from those of SAPS RPs as much as possible.

We expect that an integration capability will be required. This should be a minimal lightweight broker, managing protocol flows, session state (supporting SSO across CP, RP and AtS), orchestrating calls and redirections to AtS. It must also support orchestration of concurrent sessions with external IDPs or IAPs ('4.8'), and associated calls to *separate* internal services to transform and sign attribute payloads. These elements are expected to be stateless i.e. persistence only for a session.

To minimise (i.e. avoid) aggregate data in the broker, we expect to keep the user's AtS instance and related (encrypted and sender constrained) tokens in the CP as custom claims.

Externally facing protocols are OIDC to the CP and AtS and OAuth to the related APIs. Note the aspiration to support UMA for AtS access see '4.5'. Protocols internally to SAPS RPs can be assumed to be based on redirection and OAuth APIs.

RPs will want to support options to authorise AtS access for users who are web based (front channel) and native mobile app based (back channel, api). User journeys which involve the browser remaining focused on the service page, whilst the user selects attributes and consents to disclosure on their mobile device are likely to be preferred, but SAPS will have to support browsers and hence redirection models for other users. Thus, the broker orchestrates such calls / redirections to support these needs using protocols above (notably all within a single session whilst the user is authenticated).

In addition, a logical queue of (encrypted) verified attributes is needed, keyed by an account identifier, to support writing of attributes to the user's ATS when they next authenticate to a public service (via the broker). This queue *could* be simply implemented using a database, so although logically is an integration capability, it is not necessarily part of a 'broker' *product.* A broker product is likely to be better focused on the previous functionality, and only if a suitable queuing element is coincidentally a constituent, might we consider its deployment for outbound attributes.

4.5 Infrastructure – Metadata document management

The SAPS ecosystem will represent Verified Attributes as a signed combination of both the data item itself and associated metadata as described in '2.10' above. We expect that a SAPS standard will be developed and will iterate as services on-board and use cases are added; we expect that the metadata will be represented in standard formats (JWT/JSON/JSON-LD) to ease integration and to support manipulation and search tools.

4.6 Infrastructure – Authorisation Services

One implementation route we are considering is to separate the Authorisation Service from the Authentication Methods. (C.f. combined services mentioned in '4.1' above.) Both the CP and the AtS sections above have mentioned SSO across these components, and the support for fine-grained authorisation (e.g. UMA). Federated authentication and authorisation services would enable SAPS to deliver such services across CP and AtS, and/or deploy solutions which have a greater range of user options and/or contractual control of suppliers.

4.7 Infrastructure – Authentication Method

As mentioned in the previous section, we are considering separating the Authorisation Service from Authentication Method so that suppliers of novel and user-focused authentication methods and authenticators can more easily be integrated into the ecosystem, so improved security characteristics and improved usability (including accessibility, digital assistance, offline, and novel tech) are facilitated.

4.8 Identity Attribute Provider (IAP)

DIS expects that private sector identity proofing services may support its vision over the medium term. Such identity proofing services (Identity Attribute Providers, IAPs) may operate across multiple channels, and in particular may choose to offer face to face proofing of a person.

An IAP transaction is initiated by a referral from a SAPS RP. The requirement is that the identity attributes including metadata for that person, an assessment of the Level of Confidence in the proofing and related metadata will be returned to SAPS, according to appropriate standards and accreditation (GPG45 and certification). SAPS will (with consent of the subject) store these as Verified Attributes in the user's AtS, *and then* return them to the referring RP.

Mechanisms for transfer of trust will be developed so that the RP's user can present to the Identity Attribute Providers using an appropriate credential (suitable for use in whatever channel is to be used).

One option is a temporary credential issued by the RP to the user and presented to the IAP, which then proofs and associates its internal records with the temporary credential, and issues another temporary credential (for the digital channel) to the user. The results of the proof will be fetched by the user when in session with the RP, via SAPS infrastructure, using the temporary credential.

Another option *may* be for an IAP to provide a *SAPS compliant* service (acting as a 'RP' in ecosystem terms) to which the user authenticates using their SAPS CP, and quotes the referral code issued by the RP. This model might be suitable for digital only journeys, but requires tighter integration and attendant security and contractual control of the IAP.

Such Identity Attribute Providers (IAPs), may also be Identity Providers (IDPs) in a more traditional sense in which the user also is issued with digital credentials to access their IDP account and potentially to federate identity to other services. SAPS will permit the transfer of trust, specifically Identity Attributes, perhaps using the mechanism of a contemporaneous user session with both SAPS CP and the IDP. However, SAPS will *not* support the IDP *as the SAPS CP*. (Since by definition IDPs are outside the SAPS public service ecosystem.)

SAPS does not foresee mechanisms to purchase verified attributes more generally from the private sector market-place; that is, SAPS expects that Identity Attribute Providers will be the limit of its interest in commercially sourced verified attributes, but see also sections '2.12' '4.8' for related needs. (In addition, note that existing API and other mechanisms of the provision of services to RPs will no doubt continue independently of the programme.)

4.9 Identity on Demand Service (IoDS)

Over time a SAPS user will build extensive verified attributes, including a history over time. These data and metadata are likely to be sufficient to base claims against GPG45 evidence strength and validity (cryptographically controlled and origin at authoritative source), and verification (incremental trust, long term ownership by the same owner), and activity history. Only counter-fraud checks against external data sources remain to provide all the elements of a formal Level of Confidence proof. A stateless specialised SAPS derived attribute service could issue an assertion containing MDS and LoC back to the user's AtS *on request by a user*, so the user could use the resulting Verified Attribute 'my standard identity package' at any RP.

4.10 Exploratory – Self Sovereign Concepts

SAPS is proposing a form of decentralised identity in which the user is in control of their verified data. Incremental trust is anchored in a strong credential and federated authentication serving as a ubiquitous mechanism of access to public services. We acknowledge that it has compromises, notably: the closed ecosystem decision so that we can control governance, manage risks, manage privacy, and limit liability within the public sector; and the conscious choice of an incremental technology route with a view to enabling take-up by public sector RPs. We are inviting your comment in this market engagement exercise.

To present a polarised view, to solicit your comment, SSI/VC is said to be:

- immature (standards and interop, tools and end to end solutions);
- requires sophisticated users and end user devices;
- is based on 1 to 1 direct authentication and communications which require invasive integration and result in many to many architectures;
- relies on intermediate processing which is really 'just another middleware' (agents, resolvers and the like) on which all function depends and which has uncertain non-functional characteristics including cost models;
- requires distributed storage capabilities, rare skill sets, and complex cryptographic techniques for revocation and proofs.

We acknowledge potential upsides – privacy, agency, potential vendor/solution independence, potentially openness, potentially ubiquity, hence this request for your comments.

We are aware of terminological differences, and will be pleased to accept terms used as respondents from the SSI/DID/DIF/VC community might wish. For example, we note that the term 'credential' in the SSI community is used differently from that used in this document for 'credential provider'; 'verified credential' may be (very roughly) equated with 'verified attribute' although the latter is specific to SAPS ecosystem and is focused on eco-system specific metadata, and the former is (almost) a standard focused on discovery, proof and ownership.

If you believe that a totally different architecture could deliver the SAPS proposition, please see section '5.2' below.

5. Market Engagement – Other Points for Consideration

5.1 Other Frameworks and Schemes

We note that there are other initiatives, trust frameworks and schemes in development and consideration elsewhere.

SAPS is a deliberately closed ecosystem, serving the needs of the Scottish public service.

We have outlined that IAPs (external to SAPS) may provide verified identity attributes (section '4.7') and the capability to generate standardised forms of verified identity attribute package for consumption within and out-with SAPS RPs (section '4.8').

Such inbound and outbound transfers of verified attributes enable interoperation with other frameworks and may be of interest to respondents engaged in activities or of enabling infrastructures aligned with those frameworks. Examples are: DIU/AIX framework, financial sector schemes such as TISA or bank identities or transaction networks, non-standard identity schemes (based on personal documents such as passports).

5.2 Alternative Architectures

This market engagement pack has presented considerable levels of detail covering our intentions, and of our current architectural thinking to meet those needs. We have successfully undertaken a proof of concept which has been well received and continues in private user testing. Nevertheless, we remain open to ideas and to counter-proposals.

We are aware of SSI concepts and interested in any illustration of how such concepts can be applied to DIS context.

5.3 Cryptography, Maintenance, Revocation and Privacy

1. One of the issues raised in our proposition is the potential to track if an RP abuses the signatures of the origin of the Verified Attribute. We clearly have governance and control over all RPs but are also considering technical controls.

2. Our current model also models maintenance (and revocation) of Verified Attributes as *optional* updates to the AtS. Thus, it is possible that a user (who has sole control of their AtS) could decline (or delete) updated attributes. The user will be aware that doing so will *also* tag all versions of that attribute in their AtS as being potentially out of date, so that if the user chooses to disclose one of them, the tag will be disclosed to the consuming RP.
   This means that consuming RPs will have to be designed to understand the limitations; it also gives the desired property that the owner user is completely in control of what verified attributes they disclose to a consuming RP.

5.4 Zero Knowledge AtS Storage

It is an ideal property of the solution that the service provider offering the AtS capability cannot decrypt the user's persisted verified attributes (literally cannot, even under circumstances of successful insider attack, or external attackers owning their platform). In this sense the AtS platform may be said to be 'zero knowledge' in respect of persisted owner-user personal data.

We recognise that this is very hard to achieve, especially in the context of users who may not be able to look after their own keys, and in the light of a need to support delegation.