Scottish Government

Digital Identity Scotland

Market Engagement Day

Questions Annex

6 October 2020

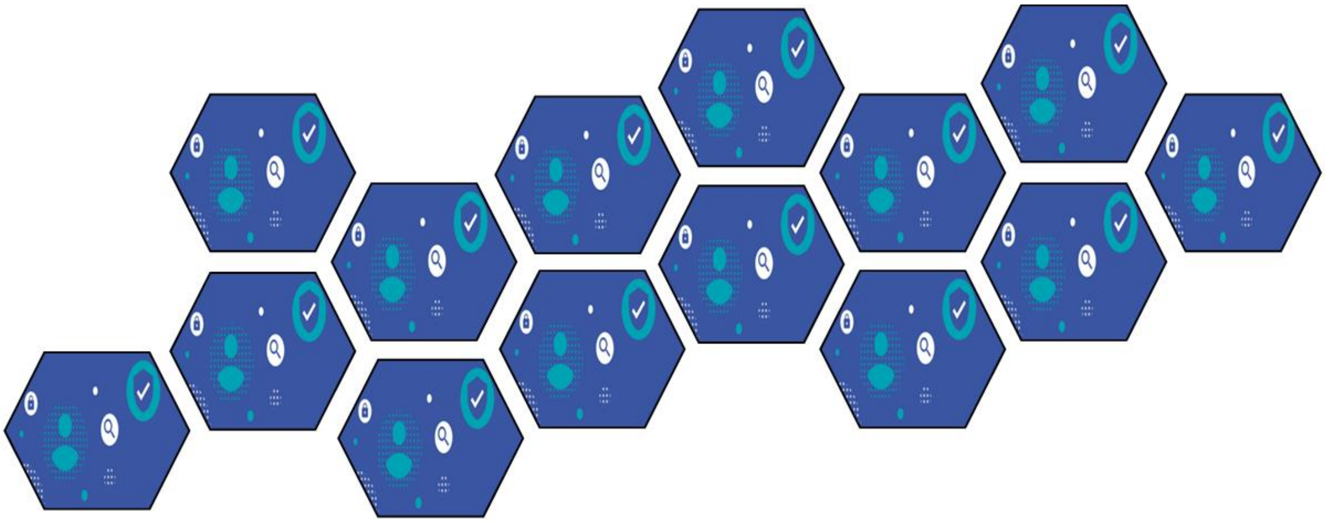

Table of Contents

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

Authorisation

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

Related Documents

Number	Title	Version/Date
1	DIS SAPS Market Engagement Indicative Requirements	**V1.0 October 2020**
2	DIS SAPS Market Engagement Presentation Slides	**V1.0 October 2020**
3	DIS SAPS Market Engagement Presentation Script	**V1.0 October 2020**
4	DIS SAPS Technical Brief for Industry	**V1.0 October 2020**
5	DIS SAPS Strategy	

1. Development Partner

1. What is the markets view on the potential benefits or drawbacks of sourcing building blocks through a development partner’s own supplier ecosystem?
2. Are there additional engineering capabilities that would be beneficial for the development of SAPS?
3. Are there additional technologies in the market that we should look for experience in from a SAPS development partner?
4. Does the market have any feedback on the proposed Principles in the context of developing SAPS?

2. Credential Provider

1. Does the market intend to certify their solutions to GPG44 Medium level, when possible?
2. How can the market support users in choosing the most appropriate authentication method?
3. What does the market use to authenticate people who do not have access to mobile phones?
4. How could we ensure that only personal data to manage the credential lifecycle is maintained?
5. Is the market able to support user names which are NOT contact handles? How would we support people who do not want to use an email address as a user name?
6. Are there mechanisms available to monitor credential use to ensure unusual behaviour is detected and support Security Operations?
7. From a market viewpoint, what could be the advantages and disadvantages of SaaS Credential Provider? What alternatives are there?
8. We want to offer a seamless service within the Credential Provider, Relying Party, and Attribute Store capabilities. One dimension of this is using the user profile in the Credential Provider to hold custom claims indicating the Attribute Store 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
9. Do you have views on these concepts, and the potential / feasibility? to work towards interoperable components and federated authorisation.

3. Attribute Store and Consent

1. What type of products and services available in the market would be suitable for use as Attribute stores?
2. Do any of these support Federated identification and how does it work?
3. What is the market view of an integral consent manager?
4. What is the market view of zero knowledge (See Section 5.4 in the Technical Brief attachment, Ref. 04) in the context of SAPS?
5. What mechanisms could be appropriate to recover a user's Attribute Store in the event of a loss of credential?
6. How could delegated access to an Attribute Store be delivered and do you think UMA2 could be applicable here?

4. Broker

1. We are interested in any feedback on our proposed broker especially in understanding the market's view on lightweight products and low-cost deployment options available in the market which minimise integration costs and would allow us to separate concerns of SAPS from those of SAPS Relying Parties as much as possible.

5. Metadata Document Management

1. We would appreciate your views on how to support metadata representation and manipulation across the ecosystem, and especially if capabilities can be readily deployed within Relying Parties and Attribute Store providers.
2. What could the market suggest as the basic / standard structure of verified attributes and should W3C's Verified Credential proposition play a role here?

6. Authorisation Services

1. Does the market agree that it is possible to implement single authorisation service for both Credential provider and Attribute Store services?
2. We note emerging standards CIBA and app2app relating to more convenient user journeys in which two domains interoperate including an authentication & authorisation journey (ref Open Banking patterns). Does the market understand these might be applied to common authentication application (of the Credential Provider) and consent manager application (of the Attribute Store)?

7. Authorisation Methods

1. Is the market aware of other Authorisation/Authentication methods which might help us achieve our SAPS aims?

8. Identity Attribute Provider

1. Do you have comments on the proposed model or wish to propose alternatives?
2. Do you believe there will be organisations committed to providing identity attributes into solutions such as SAPS?
3. Are there other suggestions on how we could deliver Identity Attributes within SAPS?

9. Identity on Demand Service

1. We invite comments on this model, in particular from respondents who may have views on or operate IDPs, or potential IAP suppliers. Do you foresee opportunities or impediments for IoDs as a service?
2. Given SAPS may provide identity assertions to external schemes (See Section 5.1 in the Technical Brief attachment, Ref .04), acting as a federated IDP to those schemes, what opportunities does this offer or modifications to the proposition might you suggest?

10. Self Sovereign Concepts

1. How does the market envisage that Self Sovereign Identity based solutions could integrate with a broker?
2. Could SSI support federated authentication by a conventional OIDC Credential Provider?
3. Could SSI support delegated access to the users Attribute Store?
4. Could SSI support less sophisticated users and recovery in the event of lost devices or compromised architecture?
5. Where, if at all, does the market see the overlap between wallets, off chain stores, identity hubs and personal data stores?
6. How can the functions of storage, authentication and authorisation/access control, and attribute 'presentations' be separated to enable composition of services with different characteristics?

11. Other Schemes

1. Does the market know of other schemes which may deliver the aims of SAPS, or which could be candidates for interworking with SAPS?
2. Does the market think that SAPS could provide verified attributes such as Identity as proofs to other public services outwith Scotland?

12. Alternative Architectures

1. Is the market aware of alternative architectures to that described which meet the user and public service needs in a Scottish Attribute Provider Service?
2. What does the market think should be changed or improved in the proposed SAPS architecture?

13. Cryptography

1. Does the market know of technical solutions to prevent the disclosure of the signature of the origin RP (the Issuer in Verified Credentials terms) to the consuming RP (the Verifier in VC/SSI terms), provided that appropriate trust in the proof (presentation in VC terms) can be demonstrated, and that such technologies meet overall integration objectives?
2. Our proposed model assumes users can decline or delete updated attributes at the Attribute Store. This means that consuming RPs will have to be designed to understand the limitations; it also gives the desired property that the user is in complete control of what verified attributes they choose to disclose to an RP. Does the market believe this is feasible?
3. Can the market suggest alternative models / technologies of attribute maintenance (public credential definitions, proof of non-revocation in VC/SSI terms, cryptographic accumulators, others).

14. Zero Knowledge Attribute Store

1. We do not want the Attribute Store provider to be able to decrypt the users verified attributes and therefore expect it to be 'Zero knowledge'. Does the market believe this is achievable and if so are there relevant examples?

15. Further Information

1. Is there any other information, feedback or suggestions relevant to SAPS that you would like to share with us? We are interested in your thoughts and challenge around our approach, concept, and thinking as well as proposed and alternative solutions.