Digital Scotland
Digital Identity Scotland

Scottish Government
Riaghaltas na h-Alba
gov.scot

Scottish Government

Digital Identity Scotland

SAPS

Engagement Day

Presentation Script

6 October 2020

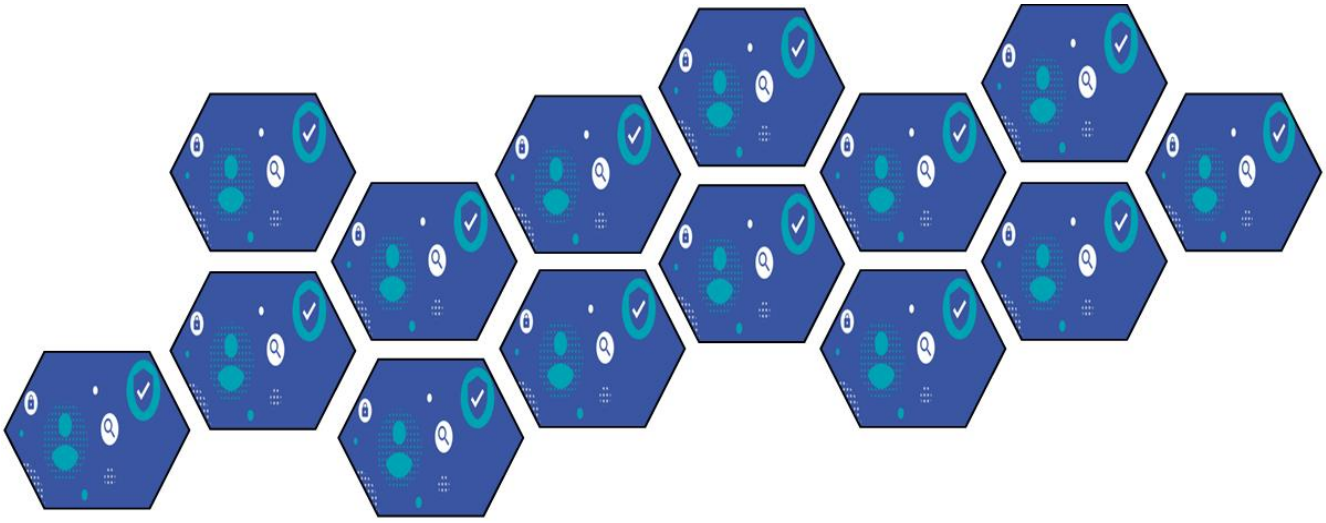

Table of Contents

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**	**6/10/2020**

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 Technical Brief for Industry	**October 2020 v1.0**
4	DIS SAPS Market Engagement Questions	**October 2020 v1.0**
5	DIS SAPS Strategy	**June 2020 v1.0**

[TITLE SLIDE 1]

1. Welcome – Mike Crockart (MC)

'Hi my name is Mike Crockart and I am the Service Owner for Digital Identity Scotland and as such you're going to hear far too much of my voice over the next 30 minutes or so. We'd like to welcome you to our Industry Engagement Event for the Digital Identity Scotland Beta phase. Under normal circumstances, we had hoped to host a face to face session, with the chance for you to engage with our team, and for us to share our intentions, and pose some questions, to you directly.

Given the new normal, we decided to pull together this 'shrink-wrapped' package, adopting a format which has proven successful within the Scottish Government's Digital Directorate programmes. We hope this briefing will help to inform you, stimulate feedback with commentary on our plans and give you the opportunity to enhance our thinking with innovative, low risk and high value alternatives.'

[SLIDE 2]

2. Format (MC)

'Whilst this presentation will be available for access over the next few months, we are still in the process of developing the next phase of the project and plan to use feedback from today's session to shape the final requirements and finalise our invitation to tender. We have provided some questions and more detail on our draft requirements in the attachments sent in your invitation email. We will endeavour to respond promptly to any questions posed within the next 2 weeks.'

Please email your feedback/questions to 'digitalidentityscotland@gov.scot'

[URL TO YOUTUBE VIDEO RESTATED - SLIDE 3]

3. Introduction by the Scottish Government Director of Digital (Colin Cook)

'Hi, I'm Colin Cook, the Director of the Digital Directorate for the Scottish Government. We really appreciate your interest in our programmes and welcome your feedback, thoughts and guidance on how we do the best for Scotland, to help realise Scotland's full potential in a digital world.

Digital Identity Scotland is a high priority programme for us all as part of our Digital Transformation journey. Ensuring that service users can access public services across Scotland as easily as possible, with appropriate security for their information and the services they are accessing, will be enabled by the effective application of digital technology, but always with a user centred focus.

I encourage you to challenge and to innovate, along with our team, with the common aim of making access to public services easier and better for all concerned. Thank you for taking time to engage with us and I look forward to working more closely with some of you in the near future.'

[CC INTRODUCTION - SLIDE 4]

4. Agenda (MC)

Today's agenda is supported by the additional information provided by email.

'Firstly, we will present our vision of the DIS Scottish Attribute Provider Service (SAPS). Throughout this presentation we will refer to SAPS - this is a working name and the service will be renamed before it becomes public facing, based on user research.

Secondly, we will summarise progress to date and the expected timeline moving forward.

Thirdly, we will focus on our User Centred Design approach – everything we do is focussed on making it easier, accessible and usable for our service users.

Fourthly, we'll present our High Level Solution and Requirements overview.

Next, we'll cover security concerns and the applicable standards.

Then, we'll talk about the expected procurement process.

Finally, we'll discuss next steps and how you can interact more with our team.'

[AGENDA SLIDE AS PER THE WORDS – SLIDES 5 TO 12]

5. SAPS Vision (MC)

'Our Vision is to develop and establish a trusted and secure service for users to prove who they are, or that they are eligible for a service. Users will be able to store their verified information and choose to share it when applying to public services. This will improve a user's access to services by providing a safe and secure way to prove their identity, while reducing time and cost for the public sector.

SAPS will be founded on user-centric principles only allowing the sharing of data with the active consent of the service user.

No data will be shared for commercial purposes, nor will data be stored in a centralised database. It will ensure that a service user's data remains under their own control so they can store and consent to share their data with public sector organisations where needed.

[VISION - SLIDES 13-15]

A key concept in our vision is that data that has been assured or proven by a trusted public sector organisation is considered to be verified data. Reusing verified data delivers benefits to the individual service user by removing repetition and friction such as the repeated need to provide varied evidence when accessing public services, and can help to solve governmental data-sharing challenges. Additionally, reuse of verified data also reduces costs and burden on the public sector associated with the unnecessary re-checking of data which has already been verified by other trusted organisations.

[VERIFIED ATTRIBUTES - SLIDE 16 - 18]

SAPS has seven key principles:

Inclusivity: Everyone has a right to a digital identity and the benefits it can provide

Ownership: Individuals always own their identity and personal data

Control: An individual's digital identity/data should not be used or shared without their explicit consent. Individuals should have a choice of the data held, who can access it and the right to opt out or to change where they store their data. Individuals maintain control of their data with the right to access, correct, and delete it as they choose

Simplicity: An individual's use of their digital identity should be simple and intuitive

Portability: An individual should be able to access/use their digital identity anywhere. This also means we need to ensure enough consistency with other systems and standards being developed across the world

Transparency: Individuals have the right to understand how their digital identity data is stored, used and shared

Privacy and Security: Identity data and transactions that involve an individual's data should be held with the highest standards of privacy and security.

[KEY PRINCIPLES - SLIDE 19-25]

SAPS will deliver a range of benefits as it develops over time. We have developed a prioritised roadmap for releasing these benefits in phased stages.

SAPS1 gives the user the ability to use a digital sign on for services. This enables users to save and resume part way through their journey, so they can return to a complex application to provide supplementary information or track its progress.

SAPS2 gives the ability to save verified attributes for future use and supports a quicker, easier user journey.

SAPS3 enables users to have their identity verified by trusted parties leading to the possibility of a digital only experience

As more verified attributes become available from more organisations contributing to the solution, SAPS4 delivers an easier user journey reducing the amount of data a user has to submit during each interaction, leading to a better user experience and reduced effort. It also reduces costs by removing any dependence on 3rd party identity providers.

[BENEFITS - SLIDE 26]

6. DIS Timeline (MC)

In 2017, the Programme Team and Governance groups were established.

In 2018 an initial Discovery was undertaken between January and May 2018. The Programme completed a landscape review of identity models (including Gov.Verify) and current/emerging technologies. In depth user research was undertaken including privacy interests and initial high level personas were developed. There was initial engagement with relying parties and other UK departments including GDS, DWP and HMRC.

In 2019, an Alpha ran from January to June 2019 in conjunction with the Open Identity eXchange. This included successful testing of a technical architecture using a Broker integrating two public sector Relying Parties with two Identity Providers, one a commercial provider to GOV.UK Verify and one from the Scottish public sector. The full output report is available on the OIX website.

In 2020 the programme re-focussed on a service user controlled, verified attribute strategy - Scottish Attributes Provider Service (SAPS), completing a successful Prototype Alpha in May 2020, working with a commercial Credential Provider and a Personal Data Store provider. In parallel, the programme also investigated suitable candidates to deliver the first building block of the SAPS solution. The SAPS Strategy was published in June 2020 with the aim to establish SAPS1 (secure digital sign on) through Credential Provider/Authentication capability.

2021 – the programme aims to procure the Attribute Store and enhanced broker capability in the first half of 2021, allowing us to integrate with the Credential Provider and deliver the SAPS 2 (save/use attributes) service during 2021. Later in 2021, dependant on the market response to the replacement for GOV.UK Verify, we aim to introduce verified identity attributes from third party providers (e.g. Verified Identity to GPG45 Medium Level) which can be made available through a service user's personal attribute store for use by public sector bodies. This forms SAPS 3 (verify identities). All this will allow us to on-board Relying Parties through 2021 and into 2022.

2022 – with all the building blocks in place, the service operating, and service users building up a set of comprehensive verified attributes in their personal attribute stores, we expect to reduce the reliance on third party verified attribute providers, and be able to generate more derived attributes from the data available, creating a virtuous circle and self perpetuating model of more verified attributes, more Relying Parties and more service users benefitting from SAPS and the easier user journey of SAPS4 (proliferation)

[TIMELINE - SLIDE 27]

'This slide provides a cut down version of the roadmap shown over the next two years.'

[ROADMAP - SLIDE 28]

7. User Centred Design – Fiona Maclellan (FM)

[personas - slide 29]

Building a service with the users needs at the centre is key to success. We know that "one size does not fit all" and so we are working to create an adaptable design which meets the range of user needs. To give you some of the flavour of what our users are looking for we have organised our user need statements into 5 themes:

[list of theme headings - slides 30-34]

1. catering for Multiple user groups: we want to build a service that supports the member of the public and the organisation

2. Clearly add value: communicating the benefits of the programme is important for buy in and to help the different audiences engage

3. Ease of integration: we want to utilise current solutions and work closely with the organisations' existing user journey and systems to make sure we can integrate our designs

4. Accessibility: Something we hear repeatedly in workshops and research sessions is that the solution needs to work well for everybody. This chimes with the idea that any solution will seamlessly plug into the service provider's existing journey.

5. Futureproof: The solution needs to be forward looking and allow for innovation and proactivity in the public service.

Here are three key examples of these user needs statements which guide our iterative designs:

[quote against photo background - slide 35]

As a service user who values ease of access, I need to be able to prove my identity or entitlement online in a way and at a time that suits me so I find it easy to do and stay in control of my time and my data.

[quote against photo background - slide 36]

As a service provider, I need a solution which is flexible so that it fits into our user journey and we aren't forced to integrate something that doesn't work for our users.

[quote against photo background - slide 37]

As a service provider, I want the solution to allow future services to be created easily so that we can be joined up and proactive public services.

[research timeline - slide 38 - 39]

Our findings come from extensive exploratory research with service users and providers. Recently, 26 people within the Digital Directorate participated through a prototype survey. We have conducted 8 in-depth usability sessions with individuals and couples and our wireframes went through an initial accessibility review.

[research timeline - slide 40]

There is still plenty to do, our ambition in the next phase is to work closely with organisational partners to understand in more detail their business processes and needs. This will inform the next iteration of the full end-to-end service design.

8. High Level Solution – Claire Lumsdaine (CL)

8.1 High Level Solution

'One proposed High Level Solution for SAPS is shown in this slide. This is still an evolving solution, and we are looking for your feedback, comments and suggestions to improve on this solution, approach and design.

For the detail that sits behind this high level summary, please see the attachments you have been provided with.

The Scottish Attributes Provider Service (SAPS) will be a closed ecosystem for public service providers. SAPS will enable value from one public service, in the form of 'things proved about me', to be reused in other services improving users' experience by reducing both friction and effort.

This will always be in partnership with the service user who will own and control all of their 'verified attributes'.

Each user will be given a single sign in, without needing to prove any personal identity attributes. Their sign in gives access to a secure place to store and control their attributes that only the user can access. Only the user can control their otherwise encrypted store; only when in session with a service will their consent be actioned.

If a user consents to reusing attributes, form filling becomes effortless and errorless and they do not have to provide evidence to reprove their data. Relying Parties 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.

[HIGH LEVEL SOLUTION - SLIDE 41]

The three key building blocks of SAPS are the Credential Provider (which provides common secure sign in), Attribute Store and Broker. More information on each of these is available in the supporting documentation, and we would welcome your feedback and questions about our proposed approach.'

[CORE ELEMENTS & INTERACTIONS - SLIDE 42]

8.2 Incremental Trust and a Strong Credential

'SAPS will provide a mechanism for growing trust over time, unlike previous approaches to online identity in which the user experienced significant and often insurmountable friction at the start of their journey when asked to prove their identity.,

In SAPS, the user will have a strong authentication credential from the outset, without proving their identity. A strong credential is one which complies with GPG44 at least Medium (level 2)

Trust in the credential is an element of this trust, but is incremented over time by the association of data and the proof of this data by services using it.

[CP/INCREMENTAL TRUST - SLIDES 43 - 45]

8.3 Attribute Store

'SAPS Relying Parties will offer users the ability to store and control their Verified Attributes in the Attribute Store.

Each instance is provided free to the user and is controlled by the data subject of the Verified Attributes.

Only the owner can view the contents, manage their consents or decrypt the contents of their Attribute Store - not the Scottish Government, nor the supplier of the Attribute Store service.'

An attribute store must accept federated authentication from a SAPS Credential Provider, enabling its owner to be in a single session with SAPS Credential Provider, Relying Party, and the Attribute Store.

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

Attribute Store capability should include the creation (and signing) of derived attributes'

[ATTRIBUTE STORE - SLIDES 46 - 49]

8.4 The 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 the concerns of SAPS from those of SAPS Relying Parties as much as possible.

We expect that an integration capability will be required, potentially a minimal lightweight broker, managing protocol flows, session state (supporting SSO across Credential Provider, Relying Party and Attribute Store) as well as orchestrating calls and redirections to Attribute Store.

[HIGHLIGHT BROKER - SLIDE 50 - 55]

8.5 Further Functions

'Other expected functions/features include the following:

Consent Management

This is where consent for attribute receipt and disclosure is managed and enforced at the Attribute Store via a user-facing Consent Management capability, for viewing and maintaining consents.

Derived Attributes

Relying Parties 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, or is resident of local authority from residential postcode.

Standard metadata

When verified attributes are created, they are assigned metadata by the origin Relying Party. This metadata (e.g. name of attribute class, timeliness of proof, minimum assurance level) is then matched against requests from consuming Relying parties to match whether available attributes might match their needs. The attributes are not disclosed without explicit consent of the owner.

Delegation

Some SAPS users may wish to appoint another SAPS user for the purposes of administering their affairs with a particular Relying Party.

Attestation

A SAPS user may ask 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 Relying Party.

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.

More information on detailed, draft SAPS requirements is provided in the email attachments sent with your invite.'

[FURTHER INFORMATION - SLIDE 56 - 60]

9. Key Use Cases (CL)

'The key Use Cases for SAPS are:

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 all of the parts of my journey 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.

[SUMMARY WITH HEADINGS ON 5 USE CASES - SLIDE 61 - 65]

'Additional Use Cases may be:

6. Given that I need to prove my identity to a standard for a service (SAPS or maybe a UK GOV service), 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 (maybe a future Verify 2 Identity Provider).'

Draft detail on these use cases and expected message flows is provided in the email attachments sent with your invite.

[ADDITIONAL 2 CASES ABOVE - SLIDE 66 - 67]

10. Technical Design Principles (CL)

'In order to deliver SAPS, we intend to follow a series of design principles which we believe will ensure a robust, credible and sustainable service can be delivered. These principles can be summarised as follows:

1. Re-Use, before Buy, Before Build

Where appropriate services, platforms, approaches or components exist within the public sector these should be re-used. DIS is assuming that reusable identity/attribute components of the service do not already exist. Therefore there is a strong preference to buy the majority of the core identity components as cloud based Software As A Service (SAAS) services.

2. Architect for flexibility and Continuous Change

The architecture will be designed as a set of loosely integrated components which can be 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 and the commercial arrangement needs 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 requires.

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.

As a consequence of this DIS SAAS services or other capabilities will likely be hosted in public cloud providers.

DevOps practices will be used.

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 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.

5. Technology Based on Standards

DIS will prefer to use proven standards over developing new standards. Where existing Scottish government standards apply DIS will follow these, e.g. Digital Service Standard, Scottish Approach to Service Design.

DIS will also likely either adopt or align to the UK government identity standards including any emerging GDS standards.

[TECHNICAL DESIGN PRINCIPLES - SLIDE 68 - 72]

11. Security Considerations – Laurie Brown (LB)

Privacy is a fundamental user need within the Digital Identity Scotland ecosystem and there are robust cyber security and privacy framework expectations placed both on the Digital Identity Scotland team itself, and of all Partners supporting the design, delivery and operation of the service.

DIS is committed to the Scottish Government's Public Sector Action Plan on Cyber Resilience and the Scottish Public Sector Cyber Resilience Framework which is part of that.

The Cyber Resilience Framework provides a common, effective way for Scottish public sector organisations to assess their cyber resilience levels/maturity, gain reasonable confidence that they are adhering to minimum cyber resilience requirements, and take decisions on how/whether to achieve higher levels of cyber resilience on a risk-based and proportionate basis.

The framework also helps to provide clarity and assurance to individual organisations, Ministers, the Scottish Parliament and the public that appropriate levels of cyber resilience are in place.

Given the importance of Security and Privacy in the DIS programme and taking into account the threat landscape and business impact a security incident could cause, DIS will pursue the highest level of compliance possible within the Cyber Resilience Framework, including alignment to the ISO27001 standard and compliance with NIS Regulations

DIS are also considering formal certification with the IASME Governance and IASME GDPR standards to be able to allow for external assurance of our security and privacy controls.

Development Partners will be expected to fully support DIS on this Standards alignment, compliance and certification journey, and in some cases, may be expected to hold appropriate alignment, compliance and certification in some of these standards.

Indeed, it is worth stressing that any preferred Credential Provider should be Level 2 Certified with the Cloud Star Alliance Security, Trust and Assurance Registry, or CSA STAR for short, and that this mandates ISO27001 certification as a baseline into that Standard. It is reasonable to expect a similar level of assurance to be considered for other platform services within the core Trust Domain (including the Broker and any Attribute Store).

[SECURITY STANDARDS - SLIDE 73]

We believe that Standards can help Digital Identity Scotland meet Privacy needs.

Equally important to Privacy is Trust. Trust from the Relying Parties, Trust from our Citizens, Trust from Privacy Expert Groups and Trust from key development partners. Trust will be a key success factor for Digital Identity Scotland as without Trust the service simply won't be used.

Standards will help Digital Identity Scotland with Trust, but that Trust can dissolve instantly were there to be a serious security incident within the service. Reputationally, Digital Identity

Scotland may never fully recover were that to occur, and Trust may never be fully regained, affecting the sustainability of the service.

It is anticipated that the service will be a high value target from various Threat Sources and Threat Actors, and as the service scales through an increase in uptake, the likelihood of attack and impact from attack will only increase.

It is therefore essential that a highly resilient security architecture is deployed and maintained with extensive defence in depth layers. DIS will need support from a Development Partner to ensure appropriate security controls are in place, including but not limited to advanced protective and transaction monitoring, utilisation of the latest high end encryption and cryptographic key management capabilities, world leading threat intelligence and counter fraud services, and so on.

To deploy a secure DIS service, one that is also highly accessible and usable as covered by other slides in today's presentation, we believe we can gain and sustain Trust in the service, and protect Privacy rights to the highest level.

[SECURITY THREAT ASSESSMENT - SLIDE 74]

12. Procurement Timelines – Suzanne Reid (SR)

'The Digital Commercial Service (DCS) is supporting DIS in the Beta procurement, bringing the teams wealth of experience on recent Digital Programmes to bear.

At this point in time, our expectation is that we will come to market to secure the services of a capable Development Partner, who can work with our team to plan, select and integrate the different functional components necessary to create and deliver SAPS over the next 24 months. Beyond that period, there may be an opportunity for a Service Support partner to help deliver the service on an ongoing basis.

As such, the current procurement routes under consideration are shown on screen.

DPS Lot 1, all things being equal, would be our preferred route and interested parties are encouraged to register with DPS using the link. This is not an onerous process and has the added advantage of making your services available for other Scottish public bodies.

The second option would be to consider a New Agreement advertised via OJEU.

Thirdly, we could use another Scottish Government or UK (e.g. Crown Commercial Services) framework. This would only be more likely where we needed to narrow down our options beforehand.

Whatever route, the Public Contract Scotland website will be used and appropriate guidelines issued.'

[DCS - SLIDE 75 - 77]

'As part of any tender process, we would expect to provide the documents, as shown on the screen. This engagement exercise will be a significant contributor to the shape of the final documentation issued with any tender as we are confident that the interested parties can make a real and positive difference to our thinking moving forward.'

Documents	Description	Action
Terms and Conditions	Scot Govt ICT Model Ts&Cs including Schedules	Bidder to agree to the Ts and Cs set out. *No changes will be accepted
Specification	Specification and SLAs etc., set out as part of the procurement.	Bidder to read and understand document – cross referenced to Questions.
Tender Response - Technical	Questions set out to bidders	Bidder to complete and return as part of the tender process.
Commercial Response	Pricing information for the project	Bidder to complete and return as part of the tender process.
Instructions to Tenderers	Information explaining how to complete the tender and advises weightings of the technical questions, and information on using PCS-T	Bidder to read and understand document.
Form of Tender	Acknowledgement of process and agreement, confirming understanding of the tender process and responses required	Bidder to complete and return as part of the tender process.

[PROCUREMENT DOCUMENTATION - SLIDE 78]

'Our current, provisional timetable is shown. We want to get this as right as possible, so it's more important to consider the options available to us and to build on the positive engagement we are sure we will have with suppliers like yourselves. As such, if we move dates, it's because we have the opportunity to deliver a better outcome rather than stick rigidly to a pre-defined calendar.

If any of these dates change during the bidding process, all suppliers will be updated'

Action Date

ITT Published 30/11/2020

ITT Return date 25/01/2021

ITTs evaluation complete 22/02/2021

Contract award 15/03/2021

Beta development commences 29/03/2021

[PROCUREMENT TIMETABLE - SLIDE 79]

13. Q&A Process

'So how do you engage with us to feedback your thoughts, views and suggestions on what we've shared today. Well, we have provided some additional detail around our requirements and some questions we would like to pose to yourselves as the people in this space who have many of the answers and solutions.

We'd appreciate your feedback at several levels:

1. Have we been clear enough on our current thinking?

2. Where do you agree/differ from that thinking especially with respect to our Intentions, High Level Solution and proposed Procurement approach.

3. Are there options/solutions/approaches you think we are missing and could benefit from ?

4. On the individual questions we pose, can you feed back your responses please?

Please email your thoughts to digitalidentityscotland@gov.scot

We will endeavour to respond to any questions before the end of October, and will also look to provide an update on our plans at that time. We are not looking for any formal responses at this time but would appreciate it if you indicate whether any feedback you provide can be shared with other interested parties.'

[Q&A PROCESS - SLIDE 80]

14. Thank You

'We'd like to thank you for your time today and in the coming days and weeks. This presentation will remain accessible for at least the next 4 weeks, plus we have provided copies of the content and supporting information in the accompanying email invite.

Our success will be based on our ability to work with, and learn from, you. We look forward to engaging further and working with you to the benefit of service users across Scotland.

Thank You.’

[THANK YOU - SLIDE 81]