**Invitation and Instructions to Tender –**

**Provision and Ongoing Support of a Digital Identity Solution**

**Tender Ref: CP17/05/532**

**Statement of Requirements.**

[1 Invitation to tender. 4](#_Toc488654698)

[2 INTRODUCTION 5](#_Toc488654699)

[2.1 Background 5](#_Toc488654700)

[3 Context 6](#_Toc488654701)

[3.1 Concept 6](#_Toc488654702)

[3.2 Scope 7](#_Toc488654703)

[4 Functional Requirements 10](#_Toc488654704)

[4.1 Definition of a Digital Identity Service 10](#_Toc488654705)

[4.2 Identification 11](#_Toc488654706)

[4.3 Authentication 14](#_Toc488654707)

[4.4 Authorisation 16](#_Toc488654708)

[4.5 User Experience 18](#_Toc488654709)

[4.6 Integration 19](#_Toc488654710)

[4.7 Other 19](#_Toc488654711)

[5 Non-functional Requirements 20](#_Toc488654712)

[5.1 Compliance 20](#_Toc488654713)

[5.2 Security 21](#_Toc488654714)

[5.3 Performance 22](#_Toc488654715)

[5.4 Operation 23](#_Toc488654716)

[5.5 Monitoring and reporting 24](#_Toc488654717)

[6 States of Jersey Information 26](#_Toc488654718)

[6.1 Roadmap 26](#_Toc488654719)

[6.2 Volumes 26](#_Toc488654720)

[6.3 States of Jersey Data Sources 28](#_Toc488654721)

[7 Tenderer specific Information 30](#_Toc488654722)

[7.1 Onboarding and migration strategy 30](#_Toc488654723)

[7.2 Tenderer Constraints 30](#_Toc488654724)

[7.3 Governance 31](#_Toc488654725)

[7.4 Maturity and longevity 31](#_Toc488654726)

[7.5 Commercials 31](#_Toc488654727)

[Appendix A SOJ Systems 33](#_Toc488654728)

[A.1 States of Jersey Directories 33](#_Toc488654729)

[A.2 eGov Services Platform 34](#_Toc488654730)

[Appendix B GLOSSARY OF TERMS 35](#_Toc488654731)

[Appendix C REFERENCES 36](#_Toc488654732)

# Invitation to tender.

This statement of requirements documents the detailed requirements relating to the Digital Identity solution under tender reference CP17/05/532.

Tenders are advised to read and assess these requirements thoroughly and to address any requirements within any tender proposal.

# INTRODUCTION

## Background

The States of Jersey wishes to procure a Digital Identity Service as a key enabler for the eGovernment services. The Digital Identity Service will enable individuals to establish trusted digital identities that enable them to access digital government services.

This document defines the scope of the Digital Identity Service and defines the business requirements of the service. It forms part of an ITT for the Digital Identity Service.

# Context

## Concept

The objective of the Digital Identity Service is to provide individuals (acting in either personal or occupational capacities) with digital identities that can be used to access digital government services (referred to as Relying Parties or RPs).



Figure 1, Concept

Figure 1 illustrates the role that the Digital Identity Service as follows:

* The individual requests to access a States of Jersey online service – referred to in the diagram as RP (“Relying Party”) as the service will be relying on the “Digital Identity Service” to meet its digital identity requirements.
* The RP interacts with the Digital Identity Service to establish the identity of the individual. This will include:
  + Obtaining verified data about the individual
  + Establishing a unique reference for the individual
  + Authenticating the user during subsequent interactions with the RP service.
* The Digital Identity Service will enable the individual to manage their identity. It will perform various tasks:
  + Use approved methods to verify identity data about the individual to the required level.
  + Provide the individual with an appropriate and approved means to authenticate themselves to the required level
  + Actually perform the authentication in the context of access to the service
  + Maintain the identity accounts, data and authentication means.
  + Provide the individual with appropriate tools to view and self-manage their digital identity.

The Digital Identity Service could be specific to the States of Jersey or part of a wider digital identity service used in other contexts.

## Scope



Figure 2, Types of RP

Figure 2 illustrates at a high-level how the Digital Identity Service will be used by the States of Jersey. Two types of RP are envisaged:

* Direct RPs, where the individual accesses the RP directly and the RP interacts directly with Digital Identity Service.
* Indirect RPs, where the individual accesses the RP via a States of Jersey portal, such as the customer service portal being delivered as part of the eGovernment programme. The portal then interacts with the Digital Identity Service. The portal would then be responsible for providing identity data back to the Indirect RPs.

RP services will be offered over browser, mobile app and assisted digital channels and therefore it must be possible for the Digital Identity Service to be invoked and operate within those channels as well.

|  |  |
| --- | --- |
| Channel | Description |
| **Browser** | The primary channel, initially, with individuals accessing services via a browser on a range of devices (PC, tablet, mobile etc.) |
| **Mobile App** | A channel that is required to be supported and expected to grow in the future, with apps being provided on the major mobile platforms (currently iOS and Android) |
| **Assisted Digital** | An in-person channel but where the customer service representative uses a digital channel to take the in-person customer through the process of accessing a service. |

Table 1, Channels

The Digital Identity Service will manage the digital identities of individuals, but those individuals could be of differing types as shown in the table below. Throughout this document, the term “individual” is used as a generic term for a person with any of the role types supported.

|  |  |
| --- | --- |
| Type | Description |
| **Personal Customers** | Individuals accessing customer-facing government services, including both residents and non-residents. |
| **Business representatives** | Individuals who are authorised officers or directors of a business customer |
| **Agents** | Individuals authorised to act on behalf of another such as accountants performing tax returns online for personal and business customers. |
| **Others** | Other individuals permitted to access government services, for example, doctors requiring access to health records |

Table 2, Identity Types

Where an individual has multiple roles (e.g. a personal customer and an agent) the individual should be able to create different digital identities for each role.

The States of Jersey intends to provide many services digitally. The following table lists examples of the currently proposed early adopters of the Digital Identity Service.

|  |  |
| --- | --- |
| RP | Use Cases |
| **Social security** | * Current benefit recipients * Businesses completing manpower and social security contributions (similar to national insurance) contributions schedules |
| **States Greffier** | * Voter registration * e-Petitioning |
| **Income Tax** | * New tax system * Agent access to multiple personal accounts |
| **Health and Social Services** | * Access to health records (Jersey Care Record) by private sector (GPs), third sector (hospices) and community (nursing) |
| **Department for Infrastructure & Parishes** | * New driving licence and DVS (similar to DVLA) system |

Table 3, Example Use Cases

# Functional Requirements

This section describes the functional requirements of the Digital Identity Service. The intention is not to suggest any one solution but rather describe the desired scope leaving room for the different approaches that exist in the marketplace.

## Definition of a Digital Identity Service



Figure 3, Digital Identity Service

A Digital Identity Service performs three primary functions:

* **Identification (also referred to as “Verification”)**: The process of establishing the digital identity (i.e. the unique individual and their associated attributes). Typically, this is achieved through examining reliable source documents, referring to external sources and demonstrating that they correspond to the individual in question. Identification can be relatively expensive and often introduces an amount of friction into the user experience. Often it is performed during onboarding although it can be performed at other times. For example if the individual loses their authentication token and they may, in effect, need to be re-onboarded. Also, if there is a need to increase the level of assurance of an individual’s digital identity, additional identification steps may be necessary.
* **Authentication**: The process of demonstrating that access to a service is being requested by the previously identified individual. Typically, this is achieved through the use of authentication methods and technologies under the control of the individual including passwords, devices, biometrics and behaviour. Authentication methods should be designed for frequent transactional use. They allow the individual to claim the previously established identity.
* **Authorisation**: Once an individual has been successfully authenticated within the context of accessing an RP, authorisation is concerned with the usage of the identity. There are two aspects:
  + **What the individual is permitted to do**, including what data or services within the RP the individual can access. It also includes delegation or power of attorney arrangements, where an individual can act on behalf of another person or business. This aspect of authorisation will primarily be a function of the RP. The RP will apply its business rules to determine who can see and do what within its system
  + **How the digital identity is used**: Providing the individual with visibility and control over how their data is shared. This is a function of the Digital Identity Service for the personal data that it manages.

There is no universally agreed definition of digital identity. For the purposes of this document the following definitions are used:

* **Identifier**: a number that is unique to the individual and can be used to refer to them without reference to any additional personal data.
* **Attribute**: any piece of personal data relating to an individual, such as name, address, date of birth and so on.

As per Figure 1, it will often be the case that identification will happen before authentication as part of the process of onboarding the individual. There are solutions which reverse this sequence. For example, if the digital identity service is mobile app based, the first step in onboarding may be to download and secure the app (including establishing authentication methods with the individual) before then taking the individual through the identification process.

The intent of this document is not to suggest any one solution but rather describe the desired scope of the Digital Identity Service leaving room for the different approaches that exist in the marketplace

## Identification

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 1 | Mandatory | **First time identification**  The first time the individual arrives at the Digital Identity Service, the Digital Identity Service shall identify the individual as part of its onboarding service. This shall involve an approved combination of:   * Asking the user to claim attributes (see below) * Examining approved identity documents (which can potentially be done digitally) to corroborate the claimed attributes * Accessing recognised third party or States of Jersey data sources to corroborate the claimed attributes and gain confidence that the individual’s identity is active and has not be compromised. * Verifying that the identity of the user present in the onboarding processed corresponds to the identity being claimed, for example using biometric, knowledge-based or other means.   The level of identification (see below) of the first-time identification will be determined from the RP request. |
| 2 | Mandatory | **Subsequent identification**  If an RP requests a level of identification (see below) greater than that achieved so far for the individual in question, then the Digital Identity Service will perform additional identification steps to achieve the required level. |
| 3 | Mandatory | **Digital Identity Service identifier**  Once onboarded the Digital Identity Service shall assign a unique identifier (a persistent reference) to that individual that can be shared with relying parties for use in subsequent authentication transactions.  This requirement does not preclude solutions where an individual has multiple unique identifiers – one per RP that the individual has a relationship with. In this case, identifiers will be unique numbers that are specific to the Digital Identity Service and not to be confused with other references or identifiers used within the States of Jersey services. |
| 4 | Mandatory | **Detecting duplicate identities**  The Digital Identity Service shall be able to detect and prevent attempts by individuals to create multiple identities for identity types where this is not permitted by business rules agreed with the Authority. |
| 5 | Mandatory | **Identity theft detection**  The Digital Identity Service shall be able to detect and prevent attempts by individuals to create false identities or identities to which they are not entitled. |
| 6 | Mandatory | **Removal of identities**  The Digital Identity Service shall include processes to manage the removal of identities according to business rules agreed with the States of Jersey and in compliance with regulation. For example, this could include processes to remove dormant identities. |
| 7 | Mandatory | **Core Attributes**  The core attributes that shall be verified for every personal customer shall be:   * Full name * Date of birth * Full address * Email address * Phone number |
| 8 | Mandatory | **Additional Attributes**  The Digital Identity Service shall be flexible and able to support the verification of additional attributes, for example (but not limited to):   * Gender * Qualification * The Digital Identity Service shall have the flexibility to be able to verify and store additional attributes such as gender that are mutually agreed with the Authority. |
| 9 | Mandatory | **Ongoing identification**  The Digital Identity Service shall perform ongoing verification of the established identity. Often this will be invisible to the individual with third party sources being accessed at appropriate times to re-confirm attribute data and to ensure the identity has not become at risk of compromise.  The ongoing identification shall be at a level corresponding to the highest level against which the individual has been identified. |
| 10 | Mandatory | **Re-identification**  If an individual loses their authentication token (see below), the Digital Identity Service shall provide a mechanism to re-identify the individual prior to provisioning a new authentication token for that individual. |
| 11 | Mandatory | **Level of Identification**  The Digital Identity Service shall support configurable levels of identification that can be published to RPs. These levels (which the States of Jersey will work with the chosen Tenderer to define) will provide a range of identification levels for each of the attributes supported by service. Each level will provide a different combination of identification methods.  Digital identity providers shall support at least 3 configurable levels.  RPs will specify the required level when making a service request to the Digital Identity Service.  ITT responses shall include details of any existing accreditations against recognised levels of authentication (NIST, CC, GPG45, eIDAS etc).  It is envisaged that some RPs will require a level of identification equivalent to “high” in eIDAS terms. |
| 12 | Mandatory | **Method of Identification**  The Digital Identity Service shall describe the identification methods they will support, being clear about any cost implications and showing how they will meet the coverage requirements for the service (see the “Coverage” requirement below).  Identification methods could include:   * Face-to-face identification methods * Identification performed entirely through a mobile device * Other methods of online or digital identification   If mobile identification is not currently supported, then a roadmap should be provided to indicate when it will be supported.  The Tenderer should describe the range of identification methods they currently support and provide a roadmap of future methods that they plan to support. |

## Authentication

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 13 | Mandatory | **Authentication token definition**  An authentication token is a means through which an individual can digitally assert ownership of a previously established digital identity.  An authentication could include something the individual knows (e.g. a password), something the individual has (e.g. a card or appropriately secured mobile device application), something the user is (e.g. a biometric) or some combination of these elements.  In some circumstances, it may be possible to gain sufficient assurance in the identity being asserted through other contextual information such as transaction data, location and behaviour. |
| 14 | Mandatory | **Authentication token creation and issuance**  The first time the individual arrives at the Digital Identity Service, the Digital Identity Service shall create an authentication token for the individual as part of its onboarding service.  The authentication token shall have a level of authentication determined from the RP request. |
| 15 | Mandatory | **Binding**  The authentication token issuance process shall be tightly coupled (or “bound”) to the identification process to ensure there is no exploitable gap between the two processes that would permit an attacker to take over an individual’s identity or otherwise subvert the system.  The authentication token shall be linked to the individual’s identifier (or identifiers) such that RPs can authenticate an individual’s identifier based on their identity as opposed to any particular attributes needing to be passed with every transaction. |
| 16 | Mandatory | **Authentication token maintenance**  The Digital Identity Service shall manage the full lifecycle of the authentication token, as appropriate to the level of authentication of the token and the type of token in question.  This may, for example, include device management, card management, cryptographic key management, enforcing PIN or password policies and so on. |
| 17 | Mandatory | **Authentication token compromise detection**  The Digital Identity Service shall employ systems to detect the compromise of authentication tokens, appropriate to the tokens in question.  This shall include monitoring appropriate third-party lists of known security issues and ensuring access to vendor specific security information. |
| 18 | Mandatory | **Authentication token revocation**  The Digital Identity Services shall have mechanisms in place to support the revocation and re-issuance of authentication tokens in the event of loss, theft or other compromise. This may include needing to re-identify the individual to prevent malicious attempts to take over an individual’s identity. |
| 19 | Mandatory | **Authentication process**  The RP shall be able to request authentication of an individual. The individual shall assert their identity through the presentation of an identifier (in some cases this could be transparent to the user, if for example the identifier is held within a mobile application). The Digital Identity Service shall authenticate the individual to the level of authentication (see below) requested by the RP, using the authentication token previously issued to the individual. |
| 20 | Optional | **Single Sign On**  The Digital Identity Service should be able to support single sign-on to allow for implicit authentication of the individual when the individual is already authenticated within the channel being used. This should include the ability to support single sign-off.  The RP shall be able to specify whether single sign-on is permitted for access to its service and under what circumstances. |
| 21 | Mandatory | **Authentication token enhancement**  If a RP requests a level of authentication higher than the level of the authentication token currently issued to the individual, the Digital Identity Service shall, according to its business rules (which must be agreed by the States of Jersey), go through the necessary identification and authentication token creation steps to provide the individual with a high assurance authentication token. |
| 22 | Mandatory | **Authentication step-up**  The Digital Identity Service shall support authentication step-up where a RP party initially requests one level of authentication but then requests a higher level of authentication within the same session.  This will allow RPs to offer services requiring lower levels of authentication with less friction, and only require the additional friction that may be associated with higher levels of authentication, when necessary. |
| 23 | Mandatory | **Level of authentication**  The Digital Identity Service shall support configurable levels of authentication that can be published to RPs. These levels (which the States of Jersey will work with the chosen Tenderer to define) will provide a range of authentication levels. Each level will provide a different combination of authentication tokens or methods.  Digital identity providers shall support at least 3 configurable levels.  RPs will specify the required level when making a service request to the Digital Identity Service.  ITT responses shall include details of any existing accreditations against recognised levels of authentication (NIST, CC, GPG44 etc).  It is envisaged that some RPs will require a level of authentication equivalent to “high” in eIDAS terms. |
| 24 | Mandatory | **Method of authentication**  The Digital Identity Service shall provide authentication methods appropriate to the channels over which services will be delivered: web, mobile or assisted digital.  The Tenderer should describe the range of authentication methods they currently support and provide a roadmap of future methods that they plan to support. |

## Authorisation

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 25 | Mandatory | **Consent to share data**  Attributes shall not be shared with RPs until consent has been obtained from (and not subsequently withdrawn by) the individual, if required under GDPR |
| 26 | Mandatory | **Sharing of data**  When requesting authentication of an individual an RP shall be able to request attribute data as well.  Typically, on first use of an RP’s digital service, attribute data will be required in order to provision an account within the RP service or to link the identity to an existing account. |
| 27 | Mandatory | **Types of attribute request**  RPs shall be able to request attribute data in different ways, including:   * Attribute data itself (e.g. name, date of birth etc) * Information derived from attributes (e.g. age bracket derived from date of birth) * Enquiry on value of attribute (to get yes/no answer)   Acceptable use guidelines shall advise the RPs on which type of attribute request should be employed in which circumstance. |
| 28 | Mandatory | **User view of data**  The individual shall be able to view the personal data managed by Digital Identity Service on their behalf and the consents they have given to share data with RPs.  Access to these functions shall require authentication of the individual to a level of authentication agreed by the States of Jersey. |
| 29 | Mandatory | **User management actions**  The individual shall be able to perform the relevant management actions pertaining to their personal data managed by the Digital Identity Service, such as:   * Revoke a sharing consent previously given. This will result in the RP being notified of the consent withdrawal. * Initiate the correction or updating of attribute data maintained by the Digital Identity Service. * Self-service maintenance on the individual’s identity within the Digital Identity Service such as authentication token reset and account termination.   Access to these functions shall require authentication of the individual to a level of authentication agreed by the States of Jersey. |
| 30 | Mandatory | **Linking attributes to RP records**  The Digital Identity Service shall provide a mechanism to allow the RP to link the identity being used to the corresponding account within the RP service.  Typically, this will be required on first use (of an RP) but may also be required at other times. For example, a compromised identity will need to be reset or recreated and the new identity linked to the corresponding RP accounts. |

## User Experience

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 31 | Mandatory | **User Journey**  The Digital Identity Service shall support different user journeys including:   * Identification initiated from web-based RP (initially), with subsequent authentication on app or web-based RPs. * Identification initiated from app-based RP (initially), with subsequent authentication on app or web-based RPs. * Identification initiated from assisted digital RP, with subsequent authentication on app, web-based or assisted digital RPs   The proportion of individuals who will use assisted digital channels is not currently known. |
| 32 | Mandatory | **Optimal User Experience**  For all aspects of the Digital Identity Service (identification, authentication and authorisation), the service should provide an excellent user experience. This should include:   * Providing a clear, consistent and intuitive user interface * Removing unnecessary friction * Providing assurance to the individual of the safety and security of the service   The Tenderer should demonstrate the typical user experience their service will provide.  The Tenderer should describe what role user research has played in their product and service development. |
| 33 | Mandatory | **Customer Service**  The Digital Identity Service shall include the necessary customer service capabilities. This should include online support, a call centre and in-person customer service capabilities as required.  Services should be designed to maximise self-service, however there should be appropriate fall-back arrangements for when customer service issues arise that cannot be resolved through self-service and for those individuals who require additional assistance. | |

## 

## Integration

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 34 | Mandatory | **Interfaces**  The Digital Identity Service shall provide a clear and straightforward interface for Direct RPs to integrate with.  The Tenderer should provide details of the interfaces that they would offer. |
| 35 | Mandatory | **Interaction with eGov Services Platform**  For Indirect RPs, the Digital Identity Service shall integrate with the eGov Services Platform (ESP), details of which can be found in [ESP].  The Tenderer should describe how they would anticipate integrating with the ESP, with particular focus on the Portal, Integration Platform and People Directory. This should show information flows between components of the identity service and ESP, the messaging standards used, and how end-to-end security is achieved. |
| 36 | Mandatory | **Use of Standards**  The Digital Identity Service will interact with all RPs using open messaging standards including both Open ID Connect and SAML. |

## Other

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 37 | Optional | **Digital Signatures**  The digital identity should have the potential to support digital signature services compliant with eIDAS in the future. |

# Non-functional Requirements

## Compliance

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 38 | Mandatory | **Data protection**  Jersey expects to introduce legislation equivalent to the General Data Protection Regulation (GDPR) before May 2018. The Digital Identity Service therefore shall comply with GDPR.  Tenderers should provide details of how they will comply with GDPR including:   * The data sources that they propose to use and how they will be accessed, cleansed and governed. * Where personal data will be held. Ideally personal data should be held in Jersey or the UK. Alternatively, personal data may be held within the EU. * The basis for processing personal data. * Any sharing of personal data with third parties and the basis for doing so. |
| 39 | Optional | **AML/CFT**  The Digital Identity Service shall support the creation and maintenance of digital identities that meet the identification requirements of the States of Jersey AML/CFT regulations.[[1]](#footnote-1) |
| **40** | Mandatory | **Independent Audit**  The Digital Identity Service shall undergo independent audit at least annually covering all aspects of the service including performance against the States of Jersey requirements. The auditor’s report shall be made available to the States of Jersey. |

## Security

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 41 | Mandatory | **Security Management**  The Digital Identity Service shall be managed securely in line with industry best practice (e.g. ISO 27000). This shall ensure a holistic approach to security covering all aspects of the service. Details of the approach and scope including copies of relevant certifications shall be provided.  A named senior person within the Digital Identity Service organisation shall be responsible for the security of the service. That person shall be ultimately accountable for all aspects of the service security. |
| 42 | Mandatory | **Security by design**  The Digital Identity Service shall have been demonstrably designed and built to be secure. The Tenderer shall provide relevant architecture and design information as evidence of this. |
| 43 | Mandatory | **Security standards**  The Digital Identity Service shall have appropriate security certifications for both the end-to-end service and specific security enforcing components within the service, as appropriate.  Examples of relevant certifications are ISO 27000, PCI DSS, Common Criteria and FIPS 140-2.  Copies of relevant certifications shall be provided.  The Tenderer shall also comply with the States of Jersey Security Standards, [SEC]. |
| 44 | Mandatory | **Risk based**  The security of the Digital Identity Service shall have been determined from a thorough risk assessment.  Ongoing risk assessments shall be performed by the Tenderer using an established risk management framework (e.g. ISO27005) and at appropriate intervals (at a minimum annually) to determine the appropriate security controls that should be employed by the service.  The ITT response should provide summary of key risks and primary controls that will be employed. |
| 45 | Mandatory | **Independently assessed**  The security of the Digital Identity Service shall be independently assessed. The Tenderer shall provide details of the type, scope and frequency of independent assessments performed.  These may include, for example, security audits and security testing.  The States of Jersey reserves the right to request further independent security assessments should the scope not be sufficient. |

## Performance

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 46 | Mandatory | **Coverage**  The Digital Identity Service shall be able to perform identification on 90% of individuals aged 15 and over who are resident in Jersey (including residents with other nationalities) by the time it is fully live. This shall include ensuring that the individuals who use States of Jersey most frequently are supported.  The Digital Identity Service shall be able to perform identification on at least 75% of non-resident potential users of government services within 12 months of being fully live.  The service should also be able to perform identification on newcomers to the island from EU countries, potentially prior to their arrival in Jersey.  This implies ability to identification of individuals that are not physically located in Jersey. |
| 47 | Mandatory | **Availability**  The Tenderer shall provide details of their historic and target availability, expressed as a percentage. The Tenderer shall provide a justification of the claimed availability such as, for example, an overview of the infrastructural and operational measures employed.  Details should be provided on any unplanned outages experienced together with the recovery times achieved. |
| 48 | Mandatory | **Throughput**  The Digital Identity Service shall be able to support the anticipated loads that will be generated. See section 5.2 below.  The Tenderer should provide details of throughput limits to their service and ability to scale the service appropriately. |
| 49 | Mandatory | **Peak loads**  The Digital Identity Service shall be able to support the anticipated peak loads that will be generated. See section 5.2 below.  The Tenderer should provide details of peak load limits to their service and ability to scale the service appropriately. |
| 50 | Mandatory | **Concurrency**  The Digital Identity Service shall be able to support the anticipated peak concurrent requests that will be generated. See section 5.2 below.  The Tenderer should provide details of peak concurrent request limits to their service and ability to scale the service appropriately. |
| 51 | Mandatory | **Response times**  The Digital Identity Service shall detail their historic and target response times including:   * Technical response times for identification and authentication services from the perspective of the RP. This should include pertinent information regarding interfaces with RPs including, for example, whether APIs are synchronous or asynchronous. * End user response times from the perspective of the individual, including detailing any point in the delivery of services where the individual would be required to wait. |

## Operation

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 52 | Mandatory | **Single point of contact**  The Tenderer shall provide the States of Jersey with a single point of contact for the management and operation of the Digital Identity Service.  Ideally this should be a dedicated single point of contact. Where a dedicated single point of contact is not provided the Tenderer shall explain how it will ensure the States of Jersey receives responsive support. |
| 53 | Mandatory | **Change management**  The Tenderer shall employ best practice change management processes. Details of these shall be provided. Where the Digital Identity Service is not specific to the States of Jersey, the Tenderer shall describe how changes will be managed to ensure that the States of Jersey are properly engaged in the change process and not adversely affected by changes made for other service users.  The States of Jersey has a template change management process as part of its standard contract. |
| 54 | Mandatory | **Incident management**  The Tenderer shall employ best practice incident management processes. Details of these shall be provided. Where the Digital Identity Service is not specific to the States of Jersey, the Tenderer shall describe how incidents will be managed to ensure that the States of Jersey receives responsive support.  The Tenderer shall detail their historic and target SLAs for resolving incidents.  The Tenderer should consider all incident types in their response including service and security issues. |
| 55 | Mandatory | **Environments**  The Tenderer should describe the number of technical environments that they will operate (e.g. for development, test and production). This shall include describing how environments are segregated, the level of security control applied to each environment and how change management is performed across the environments. |
| 56 | Mandatory | **Roles**  The Tenderer shall describe the operational roles and responsibilities within the Digital Identity Service including access controls, segregation of duties and use of dual controls where appropriate. |
| 57 | Mandatory | **Testing**  The Tenderer shall describe its approach to testing including functional and non-functional testing, regression and ongoing testing. |

## Monitoring, Management and Reporting

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 58 | Mandatory | **Management reporting**  The Tenderer should provide details of the standard management reports they would provide to the States of Jersey.  In addition, the Tenderer should describe the level of support they would provide for bespoke reports to meet the States of Jersey’s specific requirements and any limitations on such reporting.  Management reports should include summary and detailed statistics on the usage of the service (e.g. usage of particular authentication methods, performance of particular identification methods and so on), feedback from users and performance against SLAs. |
| 59 | Mandatory | **Security reporting**  The Tenderer should provide details of the standard security reports they would provide to the States of Jersey including, for example, identification and authentication failures (indicating malicious activity), detected cyber-attacks, availability of security systems, impact of new discovered vulnerabilities on the Digital Identity Service. |
| 60 | Mandatory | **Service development**  The Tenderer will be expected to regularly brief the States of Jersey of the developments and changes it plans to make to the Digital Identity Service. This shall include providing advanced notice of planned maintenance periods with the right of veto from the States of Jersey.  The Tenderer may also receive requests from the States of Jersey to change or enhance the Digital Identity Service.  The Tenderer shall describe how such changes shall be managed in particular for changes that could negatively impact or limit the delivery of digital identity services to the States of Jersey. |
| 61 | Mandatory | **Service Management Meetings**  The Tenderer shall support regular service review and planning meetings with management and operational stakeholders from the States of Jersey. |

# States of Jersey Information

## Roadmap

When service needs to be available – pilot, full rollout, scaling up etc.

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 62 | Mandatory | **Timescales**  The Digital Identity Service shall be available as follows:   * Q4 2017: Proof of Concept * Q1 2018: First live RPs * Q2 2018 onwards: Continued rollout to other services |
| **63** | Optional | **Future interoperability**  The Digital Identity Service should have the potential for future interoperability with the UK and EU digital identity schemes. |
| **64** | Optional | **Private sector reuse**  The Digital Identity Service should have the potential for re-use in the private sector, for example, by the financial services industry. |
| **65** | Optional | **Economic benefit to Jersey**  The Digital Identity Services may help position Jersey as an innovator and early adopter of technology.  The Digital Identity Service may provide commercial opportunities for the Jersey digital industry, such as export of IPR or provision of services. Tenderers are requires to respond to requirements 86-89. |

## Volumes

|  |  |  |  |
| --- | --- | --- | --- |
| # | Type | Requirement | |
| 66 | Mandatory | **Individuals**  The headline statistics relating to individuals that will use the Digital Identity Service are:   * ~125,000 potential users of government services including Islanders who are non-resident such as university students and people who have moved to the UK but are still entitled to access services in Jersey. * ~104,000 resident population * ~75% of personal customers hold a current valid passport. Jersey-born individuals have British passports. * ~40% (12,000) of pensioners are non-resident   A significant number of residents were born in other countries:   * Jersey: 50% * British Isles: 31% * Portugal / Madeira: 7% * Poland: 3% * Republic of Ireland: 2% * Other European country: 3% * Elsewhere: 4%   Additional statistics on the resident population and demographic data can be derived from the 2011 Census, which can be found here:  <https://www.gov.je/Government/Census/Census2011/Pages/index.aspx> | |
| 67 | Mandatory | **Individuals with multiple identities**  As indicated above some individuals may have more than one identity, for example a personal customer identity and an occupational identity. Exact figures are not available at this point. It is assumed that this will affect less than 10% of the population and that the majority of affected individuals will only have 2 identities.  The priority of the States of Jersey is to support personal customer identities with a view to extending services to other identity types if technically and commercially viable. | |
| 68 | Mandatory | **Number of Relying Parties**  Indicatively the States of Jersey anticipates the following range of RPs:   * The customer services portal which will be the means of accessing the services of a number of Indirect RPs * Parish systems including electoral, rates, driving licences, dog licences and gun licences. Some of these are available through a parish services portal (<https://services.parish.gov.je/>) * Direct RPs including CAESAR, jerseylaw.je, health, court registry, e-petitioning and potentially others.   The intention is to allow the Digital Identity Service to be used beyond government to provide greater utility to individuals and additional value to the Tenderer. | |
| 69 | Mandatory | **Hours of Service**  It is envisaged that the Digital Identity Service should be available 24x7. The States of Jersey will be willing to consider appropriate maintenance windows.  Customer service support may only be required during normal service usage hours, as agreed with the States of Jersey. |
| 70 | Mandatory | **Identification volumes**  The identification volumes will be determined from the population size and planned rollout given above, together with periodic re-identification.  It is anticipated that the States of Jersey will work with the chosen Tenderer to find an optimal plan for onboarding individuals. | |
| 71 | Optional | **Authentication volumes**  The authentication volumes will be determined by the population size and the growth in usage of the service. Typically, individuals are expected to access States of Jersey services several times per year for customer-facing services.If the usage of the Digital Identity Service extends into the private sector, personal customer usage may increase to weekly.  Occupational access to States of Jersey services (for example by Medical Professionals and Agents) could occur multiple times per day. | |

## States of Jersey Data Sources

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 72 | Mandatory | **People Directory**  The States of Jersey is in the process of establishing a single directory of personal customers (referred to as the “People Directory”) that will include core attribute data.  The Digital Identity Service shall be capable of integrating with the People Directory.  Appendix A explores how the People Directory and Digital Identity Service could interoperate. |
| 73 | Mandatory | **Other Directories**  In the future, other directories may be established for non-customer identity types (e.g. a business directory, a register of medical practitioners).  The Digital Identity Service shall be capable of integrating with the other directories, following a similar model to the People Directory. |
| 74 | Optional | **Other Data Sources**  Other data sources which could leveraged by the Digital Identity Service include the driving license database (which includes photographs of drivers) and the electoral roll. |

# Tenderer specific Information

## Onboarding and migration strategy

|  |  |  |
| --- | --- | --- |
| # | Type | Information Requested |
| 75 | Mandatory | **On-boarding**  The Tenderer shall describe how they intend to on-board individuals in a manner that ensures a rapid take-up of the service.  This shall include any marketing support that the Tenderer can provide and examples of how onboarding has been achieved elsewhere. |
| 76 | Optional | **User migration**  In some cases, individuals will have existing digital access credentials (e.g. legacy user IDs and passwords). The Tenderer shall describe how they will support the migration of those individuals to the Digital Identity Service. |
| 77 | Mandatory | **Ongoing development**  The Tenderer shall explain how they will evolve and enhance their service over time, especially to support new identification methods and authentication tokens.  This shall include obtaining feedback from users, that is used to continually improve the service. |
| 78 | Mandatory | **Track record**  The Tenderer shall provide details of case studies and reference implementations relevant to the States of Jersey including, for example, implementation of government-to-citizen services. |

## Tenderer Constraints

|  |  |  |
| --- | --- | --- |
| # | Type | Information Requested |
| 79 | Mandatory | **Dependencies of the States of Jersey**  As part of any service boundary, the Tenderer shall detail any dependencies it will have on the States of Jersey for the provision and operation of the Digital Identity Service and where applicable, the cost of the Tenderer to meet those dependencies on behalf of the States of Jersey. Examples include:   * States of Jersey being required to provide face-to-face identification support. * States of Jersey being required to host all or part of the service * States of Jersey being required to provide customer or counter services * APIs required to access States of Jersey data * Provision and operation of a trusted national root certificate authority (for a PKI based Digital Identity Service). |

## Governance

|  |  |  |
| --- | --- | --- |
| # | Type | Information Requested |
| 80 | Mandatory | **Governance**  The States of Jersey envisage several potential approaches to the delivery and operation of the Digital Identity Service, such as:   * An on-premise Digital Identity Service that is specific to the States of Jersey * A hosted Digital Identity Service that is specific to the States of Jersey * A Digital Identity Service that is not specific to SoJ but to some extent shared with other users.   In all cases the Tenderer should explain the proposed governance arrangements for the Digital Identity Service. |

## Maturity and longevity

|  |  |  |
| --- | --- | --- |
| # | Type | Information Requested |
| 81 | Mandatory | **Roadmap**  All Tenderers shall describe their future roadmap. For new solutions, yet to achieve maturity or scale, this shall include details of the strategy to achieve maturity and scale. |
| 82 | Mandatory | **Continuity**  The Tenderer shall describe the arrangements they would put in place, in the event that they are no longer able to support the Digital Identity Service being proposed. |

## Commercial Requirements

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| # | Type | | | Requirement | | |
| 83 | | | Mandatory | | | Commercial model  The annual charge for the scheme over a seven-year period must be estimated (based on a user take-up model provided within Appendix Four to the ITT). This must include the charge to Jersey of initial and ongoing development, implementation, independent assessment against standards, initial and ongoing verification, issuance of identities (including any physical aspect such as a card), integration, initial and ongoing security, ongoing management and support (including helpdesk etc.). States of Jersey staff costs must be included and calculated with reference to the Jersey civil service pay scale (<https://www.gov.je/SiteCollectionDocuments/Working%20in%20Jersey/GD%20Civil%20Service%20pay%20scales%20pay%20scales%20JM%2007032017.pdf>) Where costs for any commercial 3rd party services will be incurred these should be detailed and included. | | |
| **84** | | Mandatory | | | **Liability Model**  The Tenderer shall describe their approach to liability including defining clearly the level of liability the Tenderer will accept and for what. The description shall include considering liabilities relating to identification, authentication and authorisation, as well as those relating to the protection of data.  The Authority is particularly interested in the level of liability the successful tenderer will accept for incorrectly identifying individuals as well as the overall security of the solution.  The Authority is very alert to the sensitivity of both the proposed service and the data that it will authenticate and enable to be accessed and wishes to fully understand the liability models being proposed.  Where Tenderers wish to significantly limit their liability, additional consideration should be given to steps that can be taken to mitigate the additional risks this may present to the States of Jersey. | | |

## Jersey Digital Capabilities

|  |  |  |
| --- | --- | --- |
| # | Type | Requirement |
| 85 | Mandatory | **Digital Jersey Engagement**  The States of Jersey has a Digital Policy Framework, which sets out six main objectives  · a thriving digital sector  · digital skills for all  · advanced digital infrastructure  · government digital transformation  · robust cyber security  · secure data protection  Further information can be found at <http://digitalpolicy.gov.je/>  In support of these objectives, the States of Jersey have created Digital Jersey. Established in 2012, Digital Jersey is the principal driver of government efforts to establish Jersey as an internationally recognisable centre for the digital industries. One of Digital Jersey’s primary aims is to foster growth in digital employment, increase the sector’s local value and build brand awareness.  Further information can be found at <https://www.digital.je/>  The States of Jersey recognises that there is potential for bidders to explore and, where appropriate, leverage and further develop Jersey’s inherent digital capabilities.  To this end, tenderers are required to contact Digital Jersey to explore the value that may be accrued by engaging with or developing inherent skills.  Tenderers shall include evidence of this engagement within their tender. |
| 86 | Mandatory | **On-island Presence**  Tenderers shall confirm and provide detail of whether they believe there is any potential to establish a presence within Jersey with the objective to create digital capabilities and economic benefit for the Island. If so, details of the timing, scope and accrued benefits shall be provided. |
| 87 | Mandatory | **Partnership Working**  Tenders shall provide details of whether, after full consideration, there is any potential for working with potential local capabilities and skills, recognising that the overall responsibility for any contract and end-to-end service integrity will be retained by the main contractor. |
| 88 | Mandatory | **Investing in Jersey**  In the event that Tenderers have identified that there is potential for local engagement, then full details shall be provided confirming the likely scope, value and term of any engagement and whether the bidder believes this could represent wider potential to the sub-contractor(s) beyond any potential agreement resulting from this tender. |
| 89 | Mandatory | **Strategic Synergy**  Bidders are required to confirm and explain how they can support the strategic objectives of the States of Jersey. They are also required to confirm any price premium that is being incurred to underpin these innovations and the demonstrable benefits that are anticipated. |

**Appendix A - SOJ Systems**

* 1. States of Jersey Directories

The States of Jersey is in the process of establishing a single directory of customers (referred to as the “People Directory”) that will include core attribute data. It is envisaged that other directories will be established for other identity types.

Where a States of Jersey directory exists, it is envisaged that it will be the system of record for the corresponding identity type.

There will need to alignment between the Digital Identity Service and the States of Jersey Directories. This will include determining what part the directory can play in the Digital Identity Service’s identification and authentication processes.

The following diagram illustrates one way in which a States of Jersey directory could be leveraged for identification:



Figure 4, Illustration of use of States of Jersey Directories for Identification

The flow could be as follows:

1. (Not shown on the diagram) The individual attempts to access the RP service and is redirected to the Digital Identity Service.
2. The individual asserts their identity (e.g. name, address etc) to the Digital Identity Service providing the necessary evidence.
3. The Digital Identity Service verifies the evidence and confirms it corresponds to the individual.
4. The Digital Identity Service submits the established identity (e.g. name, address etc) to the SoJ Directory in the form of an enquiry.
5. The SoJ Directory responds with a “Y” or “N” depending on whether a matching record is found. If the response is a “Y” then a Ref (identifier) is also provided. The business rules concerning when a “Y” or “N” response is given will be determined with the directory
6. Assuming the response from the directory is “Y”, the Digital Identity Service would pass the Ref to the RP. The Digital Identity Service would also provide the user with an authentication token, storing any necessary authentication data in its database.
7. Where the RP is within the States of Jersey, it will interact directly with the SoJ Directory, using the Ref to retrieve the RP specific identifier and any required data.

Subsequent RP service access would then only require the Ref (or another Digital Identity Service specific identifier it that is appropriate) to be asserted and authenticated and the Ref replayed to the RP.

This flow illustrates one possible flow only. Other approaches may be possible depending on the capabilities of the Digital Identity Service Tenderer. The flow does reflect the States of Jersey current thinking about how it will provision its directories within the context of the eGov Services Platform (see below). Specifically:

* States of Jersey RPs would be able to access the relevant directories.
* RPs will have RP specific identifiers that they use within their systems.
* The eGov Portal will use a Ref (which is different to the RP identifiers) to reference the individual.
* The directory will provide the linkage between the identifiers
* External services will only be able to interact with a directory using enquiries, as opposed to querying for or searching data.
  1. eGov Services Platform

The States of Jersey is delivering a platform for providing government digital services in a consistent way, referred to as the “eGov Services Platform” (ESP).

The States of Jersey is employing a “services oriented architecture”. The Digital Identity Service will be a key component of the ESP and will need to integrate with it at an appropriate level. Further information is available in [ESP].

1. GLOSSARY OF TERMS

|  |  |
| --- | --- |
| Term | Definition |
| AML/CFT | Anti-Money Laundering / Countering Financing of Terrorism |
| CC | Common Criteria |
| eIDAS | EU regulation on electronic identification and trust services for electronic transactions (2014) |
| ESP | eGOV Service Platform (based on Firmstep) |
| FIPS | Federal Information Processing Standards (US) |
| GDPR | General Data Protection Regulation |
| GPG44 | Good Practice Guide 44 |
| GPG45 | Good Practice Guide 45 |
| IPR | Intellectual Property Rights |
| ISO | International Standards Organisation |
| NIST | National Institute of Standards and Technology (US) |
| RP | Relying Party: A service provider (public or private sector) using the Digital Identity Service for the identification and authentication of the individuals using its services. |
| ITT | Request For Proposal |
| PCI DSS | Payment Card Industry Data Security Standard |
| PKI | Public Key Infrastructure |
| SAML | Security Assertion Markup Language |
| SLA | Service Level Agreement |
| SoJ | States of Jersey |
| Tenderer | A vendor or other organisation responding to the States of Jersey open tender for the supply of digital identity services. |
| UID | User Identifier |

1. REFERENCES

|  |  |
| --- | --- |
| Reference | Document Title |
| ESP | eGov Components and Usage, States of Jersey, v1.0 |
| SEC | Security Standards, States of Jersey, v1.3 |



END OF DOCUMENT

1. <https://www.jerseyfsc.org/anti-money_laundering/regulated_financial_services_businesses/aml_cft_handbook.asp>  
   <https://www.jerseyfsc.org/the_commission/general_information/latest_news/Customer-Due-Diligence.asp> [↑](#footnote-ref-1)