

Service definition document

Digital Identity strategy, trusted attributes, trust frameworks and transformational service design

Service description	2
Delivery of trusted services	2
Definition, design and delivery of digital identity solutions	2
Definition and Delivery of Trust Frameworks and Schemes	3
Undertaking Attribute assessments	3
Development of Biographic Matching strategies	3
Onboarding and engagement activities	4
Example engagement plan	4
Example Roles and responsibilities	4
Fulfilling onboarding and offboarding functions.	5
Example work package	5
Example Deliverables	6
Example reporting strategy	6

Service description

We support cloud services by defining, designing, delivering and assuring Citizen identity assurance, business identity strategies and population scale trust frameworks including identity verification processes (e.g. eID, biometric), authentication means, interoperability frameworks, risk assessments, and alignment to national and international law. We can deliver any of the following components:

Delivery of trusted services

We specialise in mitigating business and IT risks, we understand the concept of trust across the private and public sectors and recognise the numerous threat vectors including cyber attack, identity and eligibility fraud. We work with clients and help them implement processes to support their face to face, telephony and online channels through system, process review and design.

We breakdown trust into three component parts:

- Identity trust - is the person who they say they are?
- Session trust - Is the person's device and session trusted?
- Behavioural trust - Is the person behaving online as you expected?

We can help clients design cloud based services that utilise these trust components effectively, they can be used in isolation or in combination where different levels of trust can be uplifted to mitigate risk. This is achieved through the design and delivery of services relying on digital identities and trusted attributes utilising Government authentication & digital identity standards (e.g. Good Practice Guides 44/45).

Definition, design and delivery of digital identity solutions

Our expertise is centred on the design, delivery and assurance of business solutions that mitigate key risks and threats. We can help deliver solutions that are built on and aligned to international digital identity standards, allowing their use across departments, sectors and global ecosystems.

Assurance of digital identity solutions against recognised standards

It is important that the organisations relying on digital identities adopt a robust set of measures to determine whether an individual is who they say they are. It is straightforward for them to say they checked certain documents, but it is also the strength of this evidence that is important; for instance: How robust was the issuance process? Does the evidence contain any security features to make sure it is not a counterfeit? Is there a source that can be checked to determine

the evidence is valid and hasn't been revoked (such as when it was reported lost or stolen)?
Can the people checking the documents detect falsified or invalid documents?

We have contributed to digital identity standards including the UK's Good Practice Guide 45, the European Commission's eIDAS regulations and the US Government's NIST 800-63 standards. These standards are designed to assist those organisations undertaking the checks, and allow the types of evidence and the methods of checking them to be graded to determine the strength of the resulting assured digital identity

We can provide assurance to organisations delivering digital identity solutions, We can assess your identity capability and measure its compliance with the relevant digital identity standards.

Definition and Delivery of Trust Frameworks and Schemes

We are driven by a group of internationally recognised experts that have hands-on experience of creating national and international identity schemes such as GOV.UK Verify and the eIDAS Regulation as well as contributing to global identity standards published by ISO, NIST, and the UK Cabinet Office. As consultants, we have supported the World Bank's ID4D programme in an international context, defining ID Schemes and transformational government strategies for over a billion citizens.

Our services include the definition, design and delivery of trust ecosystems at population scale that support both citizens (individuals) and/or business identities.

Undertaking Attribute assessments

We can assess your organisation's datasets and methods to determine their applicability to digital identity proofing. This would focus not only on the strength of the evidence but also the monetization opportunities, demographic reach and usability considerations.

Development of Biographic Matching strategies

Biographic matching can be defined as a requirement to match individuals to a service owner's datasets where a unique identifier is not present. The key objective of matching is to produce a single matching record with the highest confidence score, this should be achieved where possible without human operator intervention. We have experience of developing biographic matching strategies at population scale.

Onboarding and engagement activities

Example engagement plan

An initial planning phase would be undertaken, which would result in a detailed plan, description of outcomes & deliverables and planned stakeholder engagements.

The research and deliverables would be based upon the needs analysis of the client and its stakeholders as detailed in the discovery phases. We will seek to understand where these user needs are currently not being met by studying the current "as-is" model, including threat vectors and fraud risks that currently exist and mapping to a "to-be" model.

We would also balance these needs against the known constraints; these might include legal, policy, security, technical (for instance legacy environments), privacy and commercial constraints.

We would produce a proposed design and architecture including user journeys that meet as many of the user needs as is practical, striking a balance between certain needs and known constraints, for example usability vs. risk mitigation, reducing friction in the channel whilst still maintaining key counter fraud principles such as checking a person's Identity to a sufficient level of assurance to mitigate the risk of impersonation. This solution would aim to utilise as many open standards as possible and HMG shared infrastructure where practical.

We would identify whether a particular constraint would inhibit the delivery of an optimal solution and make recommendations of mitigating strategies, where practical. The Alpha would test the proposed conceptual user journeys through a series of meetings/workshops with the relevant stakeholder groups. This may include A/B testing various options to determine the best approach to meet a specific user need.

The reporting of our findings & outcomes would be through oral presentations and written documentation. Project status updates will be provided on a weekly basis; including reporting actual activities against the project estimates, highlighting key issues discovered, and a high level overview of findings during the previous sprint. Any scope or resourcing issues would be identified, reported and an exception handling strategy proposed.

Example Roles and responsibilities

We can perform the a number of roles for the client, including:

- Lead consultants during Discovery.
- Intelligent customer function to oversee Alpha or Beta phases.

- Subject matters experts during procurement phases (contributing/authoring an RFI, sifting responses, writing requirements, scoring responses, assisting with contractual elements).
- Enterprise architects during design, definition and delivery of services. Designers of service onboarding and offboarding functions.

Fulfilling onboarding and offboarding functions.

We can provide a blended team to include, but not limited to, the following skills:

- Enterprise architecture and assurance
- Technical architecture and assurance
- Security architecture and assurance
- Business analysis (requirements gathering, needs analysis, use case definition, service definition and design)
- Business risk and threat analysis
- UK Identity standards and best practice
- Attributes standards and best practice
- International standards and best practice (eIDAS etc)
- Project management, artefact authors, workshop facilitators
- Stakeholder communications and management

Example work package

A typical work package would:

- Undertake a discovery on the stakeholder and user needs through business analysis practices.
- Undertake end to end analysis of the citizen identity or business identity requirements of a service that meet these needs.
- Undertake fraud risks and threat analysis.
- Deliver an 'as-is' risk and threat assessment.
- Design 'to-be' processes to mitigate threats and risks through session trust, transactional trust and identity trust.
- Determine the correct levels of identity assurance required to mitigate risks in accordance with GPG 43 (RSDOPS).
- Define a transition strategy for any legacy applications.
- Define a roadmap for design, development, testing and integration of an identity trust enabled service.
- Advise on the best methods of integration to a cloud based identity assurance scheme.

- Advise on the optimal method of delivering trusted digital identities. Advise on the optimal method of accessing attributes from authoritative sources. Advise on a matching strategy to establish best practice for biographic attribute matching with core departmental data sets.

Example Deliverables

- A common vision for the proposition
- Example use cases based upon this vision
- Enterprise architecture to include:
 - Business architecture
 - Technical architecture
- Risk and threats landscape
- Recommendations on standards implementation to mitigate risks and threats Attribute requirements
- Stakeholder and partner engagement strategy and plan
- Plan for future stages (i.e. an alpha)

Example reporting strategy

We would hold frequent check-point with the relevant project sponsors; this would highlight:

- Progress against plan
- Risks identified from current sprint and current risk register
- New Risks identified in current sprint
- Issues arising from previous sprints and progress on mitigation
- New Issues arising from current sprint
- Revisions to plan if required
- Actions and requirements on project team
- Actions and requirements on project sponsors

G-cloud Service (functional and non-functional)	See above
Pricing (including unit process, volume discounts, data extraction)	See pricing document
Service Management	Services will be provided by Layer 7 and its partners' consultants working in conjunction with the clients project requirements. All services provided by Layer 7 are delivered by experienced consultants, with demonstrable experience within Local Authorities and Government.
Service Constraints (e.g. customisation level, maintenance windows, etc.)	Service Levels, such as, when the work will be performed, agreement on out of hours working, will be defined with the customer during the planning session and documented in a plan. Any deviations by the customer from the agreed Plan should be raised at the earliest opportunity for resolution. The customer may be subject to penalty fees.
Ordering and invoicing	Please see terms and conditions document
Financial recompense model for not meeting service levels	See terms and conditions document.
Termination terms	See terms and conditions document.
On-boarding and off-boarding processes / scope etc	N/A
Trial Service	N/A
Exit process for data extraction and removal	N/A
Technical requirements (service	N/A

dependencies and detailed technical interfaces, e.g. client side requirements, bandwidth/latency requirements etc.)	
Training	N/A
Backup / Restore and disaster recovery	N/A
Data location option	N/A