

Atlantic Data - Digital Identity Service

1. Service Overview

The Digital Identity Services provide cloud-based software services that support the creation, verification, management, and controlled reuse of digital identities and associated attributes. The services enable organisations and individuals to establish trusted digital identity evidence in support of regulated processes, while maintaining appropriate security, privacy, and governance controls.

The services are designed to support use cases where reliable identity verification and assurance are required, including employment, safeguarding, and statutory compliance processes. Individuals retain control over the sharing of their identity information through explicit consent and authentication.

The Digital Identity Services are delivered in alignment with UK government standards and guidance, including the UK Digital Identity and Attributes Trust Framework (UKDIATF), and are intended to support secure, auditable, and privacy-preserving identity interactions.

Atlantic Data is certified under the UK Digital Identity and Attributes Trust Framework (UKDIATF) as both an **Identity Service Provider (IDSP)** and a **Holder Service Provider (HSP)**. This enables the creation of reusable digital identities that are securely stored and managed on behalf of individuals. Digital identities and associated attributes may be shared with relying organisations only following explicit individual consent and authentication, including biometric facial verification in line with higher levels of assurance under GPG44.

This service definition describes the Digital Identity Services offered by Atlantic Data. The specific service configuration, delivery model, and optional modules applicable to a customer are determined by the Digital Platform item selected and the agreed service configuration.

2. Service Scope

The Digital Identity Services provide software-based capabilities to support digital identity verification, identity holding, and controlled sharing of verified identity attributes. The services are modular and may be configured to support different operating models and use cases.

Included

The Digital Identity Services include:

- Digital identity verification and management software (Mobile / Web)
- Capture and verification of identity evidence in line with applicable standards
- Creation and management of reusable digital identities and associated attributes
- Secure storage of identity evidence and verification outcomes
- Consent-based sharing of identity attributes with relying organisations

- Audit and reporting to support governance and compliance

3. Customer Journey (End-to-End Workflow)

The Digital Identity Services support a structured end-to-end journey for identity verification and reuse.

3.1 Service Setup and Configuration

The service is configured in line with the selected Digital Platform item, including organisational structure, user access, permitted use cases, and identity assurance requirements.

3.2 Identity Initiation

An individual is invited to create or use a digital identity as part of a customer-defined process. The individual is provided with clear information about the purpose of identity verification and the use of their data.

3.3 Identity Evidence Capture

Identity evidence is captured using approved methods, which may include document capture, biometric checks, or other verification techniques appropriate to the selected assurance level.

3.4 Identity Verification

Captured identity evidence is verified in accordance with applicable standards and guidance. Verification outcomes are recorded and associated with the individual's digital identity.

3.5 Digital Identity Creation and Holding

Where applicable, verified identity evidence and attributes are retained within a digital identity holder service, enabling reuse across multiple interactions subject to consent and eligibility.

3.6 Consent and Attribute Sharing

Individuals are able to share selected identity attributes with relying organisations through explicit consent and authentication. Attribute sharing is logged to support audit and transparency.

3.7 Ongoing Use and Management

Digital identities and associated attributes may be reused for subsequent interactions, subject to validity, assurance requirements, and customer configuration.

4. Service Features and Capabilities

The Digital Identity Services provide a set of core features to support secure identity verification and management.

Core Features

- Digital identity verification and management platform
- Support for multiple identity verification methods
- Secure storage of identity evidence and verification outcomes
- Consent-based sharing of identity attributes
- Role-based access controls and audit logging
- Management information and reporting

Identity Holder Capabilities

Where configured, the service supports identity holding capabilities, including:

- Retention of verified identity evidence and attributes
- Support for reuse of identity evidence across multiple interactions
- Individual control over consent and disclosure

5. Service Delivery Model

The Digital Identity Services are delivered as a mobile app and private cloud-based software service. Atlantic Data is responsible for the availability, security, and maintenance of the software platform.

Customers configure the service to align with their specific use cases and assurance requirements.

6. Support and Service Management

Support is provided through the following channels:

- Service Desk Support – for day-to-day operational queries, user assistance, and system usage support
- Email Support – for non-urgent requests, reporting queries, and follow-up communication
- Telephone Support – for time-sensitive or safeguarding-related issues

Support channels are available during published support hours. Contact details and access arrangements are provided during onboarding.

Incident Escalation

Incidents and service issues are managed using a defined incident management process. Issues are assessed, prioritised, and progressed based on their impact and urgency.

Escalation routes are in place for:

- Issues affecting processing or result delivery
- Safeguarding-critical incidents
- Service availability or performance concerns

Where appropriate, incidents are escalated internally to specialist teams to ensure timely investigation and resolution.

Service Monitoring and Management

The service is actively monitored to support availability and performance. Atlantic Data maintains oversight of platform operation, managed service activities, and support demand to identify trends and areas for improvement.

Service management activities may include:

- Monitoring of application processing and exception volumes
- Review of support requests and incident trends
- Ongoing service improvement and optimisation

Customer Engagement

Customers are provided with a named point of contact appropriate to the service configuration. Engagement may include:

- Onboarding support and service familiarisation
- Periodic service reviews, where appropriate
- Communication of service updates or changes

The level of engagement is proportionate to the selected service and customer requirements.

7. Service Availability and Performance

The Digital ID Services are designed to provide reliable and consistent availability to support safeguarding-critical operations. Availability and performance are managed to ensure customers can access the service when required and that Digital ID processing activities are not disrupted unnecessarily.

Service Availability

The services are delivered via a private cloud-hosted platform that is available to authorised users through mobile app and standard web browsers.

The platform is designed to support continuous access for operational use, subject to:

- Planned maintenance activities
- Unplanned incidents or external dependencies outside Atlantic Data's control

Where maintenance is planned, customers are notified in advance where reasonably practicable.

Performance and Reliability

The platform is designed to support the expected volumes and usage patterns of Digital ID processing and safeguarding oversight. Performance is monitored to ensure that:

- Applications can be initiated, processed, and tracked efficiently
- Reporting and management information remain accessible
- Managed service activities can be carried out without undue delay

Performance management focuses on service stability and operational effectiveness rather than transaction speed alone.

Resilience and Continuity

Measures are in place to support service resilience and continuity, including:

- Redundancy within the hosting environment
- Data backup and recovery processes
- Business continuity and incident response planning

These measures are designed to reduce the risk of service interruption and support timely recovery where incidents occur.

Dependencies and External Services

Certain aspects of the service depend on third-party systems and external bodies such as CRA's, Fraud Databases etc. Availability and processing times for these external services are outside Atlantic Data's direct control and may affect end-to-end timelines.

8. Security and Compliance

The Digital ID are designed and operated with security, data protection, and regulatory compliance as core principles. Controls are in place to protect personal data, support safeguarding obligations, and meet the expectations of public sector and regulated organisations.

Information Security

Atlantic Data maintains an information security management framework designed to protect the confidentiality, integrity, and availability of service data.

Security controls include:

- Access controls based on defined user roles
- Segregation of environments and duties
- Secure authentication and authorisation mechanisms
- Monitoring and logging of system access and activity
- Regular review and improvement of security controls

Data Protection and Privacy

The services are operated in compliance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Personal data is processed solely for the purposes of delivering Digital ID services on behalf of customers. Data handling practices are designed to support:

- Lawful, fair, and transparent processing
- Data minimisation and purpose limitation
- Appropriate retention and secure disposal
- Support for data subject rights

Certifications and Assurance

Atlantic Data holds and maintains relevant certifications and assurance measures to support service security and reliability, including:

- ISO/IEC 27001 certification for information security management
- Atlantic Data is an IDSP, ISP and HSP under the UKDIATF
- Regular independent penetration testing conducted by accredited providers
- Compliance with payment security standards where payment processing is applicable

Evidence of certifications and assurance measures can be provided on request.

9. Hosting and Data Residency

The Digital ID services are delivered using a secure, private cloud-hosted infrastructure designed to support availability, resilience, and compliance with UK data protection and public sector expectations.

Hosting Environment

The services are hosted within a managed private cloud environment that supports the secure operation of the software platform and associated managed service components.

The hosting environment is managed and maintained by Atlantic Data. Infrastructure is monitored and maintained to support service availability, security, and performance.

Data Residency

Personal data processed as part of the Digital ID Services is hosted within the United Kingdom.

Data residency arrangements are designed to support compliance with UK data protection legislation and public sector requirements, including those applicable to safeguarding organisations.

Access and Connectivity

The service is accessed via the public internet using secure connections. Access is restricted to authorised users through authentication and role-based controls.

Backup and Recovery

Backup and recovery processes are in place to support data integrity and service continuity. Backups are managed in line with defined retention and recovery procedures and are tested periodically.

10. Data Management and Retention

The Digital ID service manage personal and operational data in a controlled and transparent manner to support DBS processing, safeguarding oversight, and compliance with legal and regulatory obligations.

Data Categories

The services may process the following categories of data:

- Applicant personal information required for Digital ID
- Identity verification information and supporting evidence
- Digital ID application status and outcome data
- Consent records and audit information
- Service usage, reporting, and management information

Data processed is limited to what is necessary to deliver the selected service and support safeguarding and governance requirements.

Data Processing Roles

Atlantic Data acts as a data processor on behalf of customers for the purposes of delivering the Digital ID service. Customers/Applicants act as data controllers and determine the lawful basis and purposes for processing personal data.

Data Retention

Personal data is retained in accordance with:

- Applicable legal and regulatory requirements
- DBS guidance and audit obligations
- Customer-defined retention periods, where permitted

Retention periods and data handling arrangements are agreed during service onboarding and may be reviewed periodically. Data that is no longer required is securely deleted or anonymised in line with defined procedures.

Data Access and Control

Access to personal data is restricted to authorised users and personnel based on defined roles and responsibilities. Controls are in place to prevent unauthorised access, alteration, or disclosure of data.

Data Subject Rights

The services support customers in meeting their obligations in relation to data subject rights, including access, rectification, and erasure, in line with applicable data protection legislation.

11. Onboarding and Implementation

Onboarding Approach

Onboarding typically includes:

- Confirmation of the selected Digital Platform item and service configuration
- Set-up of organisational details, user roles, and access controls
- Configuration of workflows, safeguarding requirements, and reporting
- Agreement of identity verification methods and operational processes

The onboarding process is managed collaboratively to ensure clarity of roles and responsibilities.

Implementation Activities

Implementation activities may include:

- System configuration and environment setup
- User account creation and role assignment
- Data or configuration where applicable
- Testing of workflows and reporting

The scope and duration of implementation activities depend on the selected service and organisational complexity.

User Enablement

Users are supported during onboarding through:

- Guidance on system use and Digital ID processes
- Access to user documentation and supporting materials
- Initial support to ensure users can operate the service effectively

User enablement is designed to support consistent and compliant use of the service.

Go-Live and Early Support

Following onboarding, the service moves into live operation. Additional support may be provided during the early stages of use to address queries, confirm correct configuration, and support a smooth transition into business-as-usual operation.

12. Offboarding and Exit Planning

Offboarding from the Digital ID Services is managed in a controlled and transparent manner to support continuity, data protection, and safeguarding obligations. Offboarding arrangements are designed to minimise disruption and support an orderly transition at the end of the contract period.

Offboarding Approach

Offboarding is initiated in line with contractual arrangements and agreed timelines. The approach is proportionate to the selected service configuration and the nature of the customer's Digital ID activity.

Offboarding activities may include:

- Confirmation of offboarding scope and timetable
- Controlled closure of user access
- Agreement of data handling and transfer requirements
- Coordination of any required transition support

Data Handling on Exit

On exit, personal and operational data is handled in accordance with:

- Applicable data protection legislation
- Digital ID audit and record-keeping requirements
- Customer-defined retention instructions, where permitted

Data may be:

- Returned to the customer in an agreed format
- Retained where legally required
- Securely deleted or anonymised in line with defined procedures

A record of data handling actions may be provided to support audit and governance requirements.

Continuity and Safeguarding Considerations

Where offboarding occurs while Digital ID activity is in progress, reasonable steps are taken to ensure continuity and avoid unnecessary safeguarding risk. This may include completion of in-flight applications or agreement of handover arrangements, subject to contractual terms.

13. Customer Responsibilities

Customers using the Digital ID Services have defined responsibilities to ensure the services are used appropriately, lawfully, and in line with safeguarding requirements.

Organisational Responsibilities

Customers are responsible for:

- Maintaining accurate organisational and user information within the service
- Ensuring users are authorised and trained to use the service appropriately

Applicant Engagement and Information

Customers are responsible for:

- Engaging applicants and providing clear instructions
- Ensuring information submitted by applicants is accurate and complete

Safeguarding and Decision-Making

Customers remain responsible for:

- Applying their own safeguarding policies and procedures

The services support safeguarding decisions but do not replace customer responsibility or judgement.

Compliance Responsibilities

Customers are responsible for complying with applicable laws, guidance, and policies relevant to their use of Digital ID services, including data protection and safeguarding obligations.

14. Optional Modules

Optional modules may be added where explicitly included in the selected Digital Platform item, including integration with other separately listed G-Cloud services.