



SERVICE DEFINITION DOCUMENT

*Digital Identity, IAM,
Verification & Trust Services*

73 Church View, Hollywood,
BT18 9LN – United Kingdom
+44 (0)2890 394 431
info@cranmo.re

Contents

1. Purpose of this Document	3
2. Service Description	3
2.1 Overview.....	3
2.2 Service Components	3
2.3 Service Benefits.....	4
3. Delivery Approach.....	4
3.1 Strategy & Discovery	4
3.2 Implementation	5
3.3 Deployment & Go-Live.....	5
3.3 Operations (Ongoing Support).....	5
4. Service Constraints	5
5. Ongoing Support	6
5.1 Support Services.....	6
5.2 Support Response Levels	6
6. Security and Compliance.....	6
6.1 Security Accreditations	6
6.2 Mobile Application Security	6
7. Pricing	7
8. Contact Information	7

1. Purpose of this Document

This document provides comprehensive information about Cranmore Consulting's Digital Identity, IAM, Verification & Trust Services and defines how these services are delivered to UK public sector organisations.

This Service Definition is required as part of Cranmore's listing on the G-Cloud 15 framework and conforms to the requirements specified in the Crown Commercial Service's guidance on service definition documents.

These services are designed for central government departments, local authorities, NHS organisations, and other public bodies seeking end-to-end digital identity services from strategy and early-stage problem definition through solution implementation and ongoing operational support, including UK Digital Identity and Attributes Trust Framework compliance.

2. Service Description

2.1 Overview

Cranmore delivers complete digital identity lifecycle services covering strategy, implementation, and ongoing operations. Our comprehensive approach spans early-stage problem definition and feasibility assessment, identity solution architecture and development, IAM platform implementation, identity verification system deployment, trust service integration, and continuous operational support. We help organisations establish trustworthy, secure, and user-friendly digital identity capabilities enabling reliable electronic transactions across systems and jurisdictions aligned with UK Digital Identity and Attributes Trust Framework.

Services encompass problem definition, feasibility assessment, and solution architecture ensuring clear understanding of identity challenges before implementation. Implementation delivers IAM platforms identity verification solutions, federation and SSO capabilities, trust service integration, and custom identity applications. We also provide ongoing support including monitoring, security management, user administration, and continuous enhancement ensuring identity solutions remain secure, performant, and aligned with evolving requirements.

Our technology-agnostic, standards-based approach ensures vendor independence, interoperability, and future-proof architecture. Proven ASSURED Agile methodology delivers identity solutions iteratively through two-week sprints with continuous stakeholder engagement. ISO 27001 and Cyber Essentials Plus certifications ensure security throughout strategy, implementation, and operations. Public sector experience ensures compliance with Government security classifications, accessibility standards, and UK GDPR requirements.

2.2 Service Components

Digital Identity, IAM, Verification & Trust Services include:

- **Identity strategy and discovery:** Strategic planning, discovery, and readiness assessment to define digital identity vision, principles, and transformation roadmaps.
- **Trust and compliance alignment:** Mapping identity approaches to relevant UK guidance, including the UK Digital Identity and Attributes Trust Framework, where applicable.
- **Identity and access architecture:** Definition of IAM architecture covering authentication, authorisation, governance, and identity lifecycle management.
- **Identity verification strategy:** Planning of identity proofing and verification approaches, including assurance levels and user journey considerations.

- **IAM platform implementation:** Implementation and configuration of identity and access management platforms using buyer-selected technologies.
- **Federation and single sign-on:** Design and configuration of federation and SSO to support cross-organisation identity and access.
- **Identity integration and security:** Integration of identity services with applications and data sources, including zero-trust and MFA-aligned security controls.
- **Identity and organisation checking:** Design and delivery of identity and organisation checking capabilities, including onboarding, identity verification workflows, and assurance-level considerations, using buyer-approved approaches and providers.
- **Testing and assurance:** Functional and security testing of identity solutions, proportionate to service risk and context.
- **Operational support options:** Optional support for identity operations, monitoring, administration, and continuous improvement, agreed as part of the engagement.

2.3 Service Benefits

Organisations engaging Cranmore for digital identity services realise substantial advantages:

- **End-to-end capability:** Support across the digital identity lifecycle, from strategy and discovery through to implementation and operational handover.
- **Regulatory and trust alignment:** Identity approaches informed by relevant UK digital identity and trust guidance, including the UK Digital Identity and Attributes Trust Framework, where applicable.
- **Reduced delivery risk:** Structured discovery and strategy reduce the risk of false starts and misaligned investment.
- **User-centred identity design:** Identity solutions that balance security, assurance, and usability to support positive user experiences.
- **Technology independence:** Platform-agnostic approaches enable informed technology selection and reduce vendor lock-in.
- **Standards-based and interoperable:** Use of open standards and federation approaches supports interoperability across systems and organisations.
- **Security by design:** Identity architectures aligned to zero-trust and modern authentication practices support secure and resilient services.
- **Privacy-aware delivery:** Privacy-by-design principles support compliance with UK GDPR and data minimisation expectations.
- **Public sector expertise:** Experience delivering identity services within public sector contexts, including central government and regulated environments.

3. Delivery Approach

Cranmore's Digital Identity, IAM, Verification and Trust Services cover full cycle provision.

3.1 Strategy & Discovery

Strategy establishes clear understanding of identity challenges and target architecture:

- Problem definition workshops exploring current state, pain points, user needs, and constraints
- Stakeholder engagement identifying requirements across user groups and organisations
- User research understanding authentication experiences, friction points, and accessibility needs
- Regulatory review assessing trust framework, security standards, and compliance requirements

- Threat modelling identifying identity-related security risks and attack vectors
- Feasibility assessment evaluating technical readiness, organisational capability, and implementation risks
- Architecture design defining IAM components, integration approach, and security controls
- Implementation roadmap phased approach with quick wins and long-term transformation

3.2 Implementation

Implementation delivers identity solutions through Agile sprints:

- Sprint planning prioritising features for two-week sprints based on business value
- IAM platform deployment implementing chosen identity platform with core authentication
- Federation configuration enabling SSO and cross-organisation identity recognition
- Verification system implementation deploying identity proofing and document verification
- Backend integration connecting identity systems to applications and directories
- Security configuration implementing MFA, zero-trust controls, and threat protection
- Custom development building bespoke identity workflows and applications
- Testing comprehensive quality assurance including security testing and penetration testing
- Sprint reviews demonstrating working functionality gathering stakeholder feedback
- User training preparing administrators and end-users for identity system usage

3.3 Deployment & Go-Live

Deployment transitions identity solutions to production:

- Pilot deployment releasing to limited user group validating core functionality
- Migration planning defining approach for transitioning users from legacy systems
- Production deployment executing phased rollout with monitoring and support
- Hypercare four-week enhanced support following go-live with rapid issue resolution
- Performance monitoring tracking system performance, authentication success rates, and user experience

3.3 Operations (Ongoing Support)

Operations provides continuous support and enhancement:

- Monitoring of identity services using automated alerts to support service availability and incident detection
- Incident response rapid resolution of authentication issues and security incidents
- User administration managing identity lifecycle, provisioning, and deprovisioning
- Access reviews periodic certification ensuring appropriate access controls
- Security operations continuous threat monitoring, vulnerability management, and patching
- Performance optimisation continuous improvement based on analytics and user feedback
- Enhancement delivery implementing new capabilities through iterative Agile sprints

4. Service Constraints

To support successful digital identity outcomes:

- **Stakeholder and system access:** Effective delivery is supported by Buyer access to relevant stakeholders, users, and existing identity and access management systems, subject to appropriate security controls.
- **Coordination and engagement:** Cranmore works collaboratively with the Buyer to coordinate workshops, testing activities, and migration planning.

- **Documentation availability:** Implementation is informed by access to existing system documentation, configuration information, and assurance artefacts, where available.
- **Subject matter expertise:** Availability of security, compliance, identity, and architecture subject matter experts supports informed decision-making and risk management.
- **Buyer participation:** Regular Buyer participation in sprint reviews, validation, testing, and migration activities supports effective delivery and alignment.
- **Change and adoption support:** Buyer involvement in user communications, training, and change management activities supports adoption of new identity capabilities.

5. Ongoing Support

5.1 Support Services

Cranmore provides comprehensive identity services support:

- **Expert Leadership** – Identity Architect providing technical leadership and strategic guidance
- **Round-the-Clock Support** – 24/7/365 monitoring and incident response for production identity systems
- **24/7 Phone Support** – Telephone support 24 hours, seven days per week (028 9042 1238)
- **Ticketing System** – Email and ticketing via Atlassian helpdesk for queries and issues
- **Service Reviews** – Regular service reviews with performance metrics and improvement recommendations

5.2 Support Response Levels

Incident response based on business impact:

- **Priority 1 (Major Impact):** 15 minutes response, 6 hours resolution target
- **Priority 2 (High Impact):** 1 hour response, 8 hours (one working day) resolution target
- **Priority 3 (Moderate Impact):** 4 hours response, 3 working days resolution target
- **Priority 4 (Minor Impact):** 1 day response, 10 working days resolution target

6. Security and Compliance

6.1 Security Accreditations

Cranmore maintains:

- **ISO 27001** – International standard for information security management
- **Cyber Essentials Plus** – Independently verified cyber security controls
- **Security Clearance (SC)** – Key personnel hold UK Security Check clearance enabling work with OFFICIAL and OFFICIAL-SENSITIVE data

6.2 Mobile Application Security

All services apply security best practices including zero-trust architecture, defence-in-depth strategies, modern authentication methods (FIDO2, biometrics, MFA), identity threat protection, secure credential storage, audit logging, and UK GDPR privacy by design. Trust framework compliance ensures digital identities meet minimum quality standards for reliable, secure electronic transactions.

7. Pricing

Digital identity services priced based on lifecycle phase and scope:

- **Strategy and Discovery:** Typically delivered on a fixed-price basis, agreed in advance based on the defined consultancy scope and timebox.
- **Implementation:** Priced separately on a fixed-price basis, based on the agreed solution scope, assurance requirements, and delivery complexity.
- **Third-party identity and organisation checking:** Integration and coordination activities are priced as part of implementation or enhancement scope. Any third-party provider fees are excluded and are contracted and paid directly by the Buyer to the relevant provider.
- **Operational support (optional):** Optional support services may be provided under a fixed recurring fee, based on the agreed support model and service levels.
- **Enhancements:** Time and Materials pricing may be used for agreed enhancements or extensions, where appropriate.
- **Payment terms:** Payment terms are 30 days from invoice date. Invoicing arrangements are agreed as part of the call-off.

See pricing documents for more information.

8. Contact Information

Primary Contact

Fergus McGrath
Sales Director
Cranmore Consulting
Mobile: 07912 777717
Email: fergus@cranmoreconsulting.com

Service Desk

Telephone: 028 9042 1238
Email: info@cranmoreconsulting.com

Registered Office

Cranmore Consulting Ltd
73 Church View, Holywood
BT18 9LN
United Kingdom

G-Cloud 14 Listing

<https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/479964968691217>