



Decentralised Identity

Service Description

Protect privacy, build digital trust and streamline operations



Table of Contents

1.1	DXC Decentralised Identity for UK Public Sector	3
1.2	DXC Overview	3
1.3	Decentralized Identity	3
1.4	Service Features.....	4
1.5	Service Benefits.....	5
1.6	End-to-End Decentralized Identity Services	6
1.7	A New Paradigm for Digital Trust.....	7
1.8	The Problem with Centralized Identity Systems	8
1.9	e-Wallets.....	8
1.10	Distributed Identity Framework (DIF)	8
1.11	Trust Framework.....	8
1.12	ID Proofing.....	9
1.13	Population Scale.....	9
1.14	UK Public Sector Challenges	9
1.15	Growing Threat Landscape.....	10
1.16	Cryptographic agility	10
1.17	User Support and Ticketing Support	11
2	Case studies.....	12
2.1	DXC an Experienced Partner.....	12
2.2	Secure UK Government Delivery	12
2.3	National digital identity for 4 million citizens	14
2.4	CIAM for a Transport Ministry	14
2.5	City police digital transformation	14
2.6	UK Defence – Zero Trust and secure communications	14
2.7	Streamline Travel Experiences	15
2.8	Did you know?	15
3	DXC Delivery Approach.....	16
3.1	DXC IAM Capability Model.....	16
3.2	DXC IAM Delivery Methodology.....	16
3.2.1	IAM strategy definition	17
3.2.2	Identity programme	18
3.2.3	Managed operational services	18
4	About DXC Technology.....	19

List of Tables

Table 1.	Incident Priorities and Impacts.	11
----------	---------------------------------------	----

List of Figures

Figure 1.	DXC Decentralised Identity Services	4
Figure 2.	Growing Threat Landscape with Rising Number and Type of Identities	10
Figure 3.	Erskine – Flagship UK Delivery Centre	13
Figure 4.	DXC IAM Capability Model	16
Figure 5.	DXC End-to-end IAM Methodology	17
Figure 6.	Identity enables public service users and providers	20

1.1 DXC Decentralised Identity for UK Public Sector

1.2 DXC Overview

DXC Technology delivers end-to-end Identity and Access Management services that enable UK public sector organizations to secure digital identities, enforce Zero Trust principles, and meet stringent compliance requirements such as GDPR, NHS Digital standards, and MoD security frameworks.

- Identity Governance and Administration (IGA) for compliant and accountable identity lifecycle management.
- Privileged Access Management (PAM) for safeguarding the privileged accounts that control your critical systems.
- Passwordless adaptive authentication for frictionless user experiences, making secure access easy to use access.
- DXC Key and Certificate Services provide centralized management of encryption keys and certificates on a crypto agile platform to ensure secure communication, establish trust, and streamline regulatory compliance.
- Decentralised Identity services built on a privacy protecting approach to personal data that enables people to carry their personal data in their own e-wallet and decide when and with whom to share their verified credentials and verified attributes.

Government has complex hybrid and multi-cloud environments with geographically dispersed staff and citizens working remotely and from home. A growing number of connected machines from IoT, RPA Bots and AI agents. UK Public Sector needs regulatory compliance, cost reduction, improved security stance, quantum readiness, greater flexibility of service delivery, all while accelerating the growth of digital channels and adoption of a Zero Trust security approach.

1.3 Decentralized Identity

DXC Decentralized Identity services help UK public sector organizations to shift service delivery to digital channels while raising levels of identity assurance and delivering services with a privacy by design approach to digital identity security.

DXC provides:

- ID-proofing to onboard with the confidence of high assurance identity.
- Distributed identity platform for open standards, scale and resilience.
- Scales without centralized bottlenecks for speed and resilience.
- e-Wallets to carry verified credentials and verified attributes.
- Flexibility of self-sovereign identities or government issued.
- Privacy by design technology backed with compliance to digital identity trust frameworks and regulations.

The trend has been for a shift to digital channels for delivery of services and interaction with customers and citizens. The move accelerated with the pandemic as people shifted to remote working, customers to online retail and citizens to electronic government services.

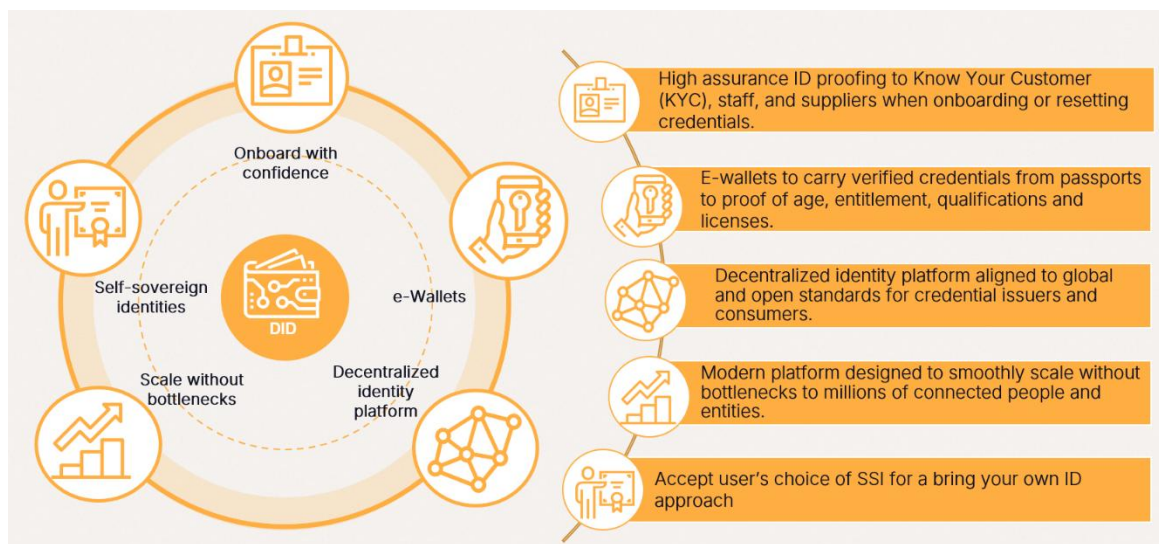


Figure 1. DXC Decentralised Identity Services

1.4 Service Features

Features and capabilities of DXC's Decentralised Identity services:

1. Secure Digital Wallet

Enable citizens and staff to store verified credentials such as IDs, licenses, and certificates in a secure e-wallet accessible via smartphone or cloud, ensuring convenience and strong encryption for sensitive identity data.

2. Blockchain based Identity framework

A decentralised, standards-driven identity system leveraging blockchain to guarantee trust, transparency, and security without retaining personal information in centralised repositories, reducing risk and enhancing compliance.

3. Selective credential sharing

Allow individuals to share only the necessary verified attributes for applications, access requests, or identity checks, maintaining privacy and meeting UK GDPR and data minimisation principles.

4. Remote Digital ID proofing

Verify identities remotely using document capture and facial recognition technologies, eliminating physical presence and manual paperwork for faster, secure onboarding of citizens and employees.

5. Zero Trust Security model

Enforces least-privilege access and continuous authentication, safeguarding sensitive public sector data while enabling secure collaboration across departments, agencies, and third-party suppliers.

6. Scalable SaaS architecture

A modern, cloud-native platform designed to scale seamlessly to millions of users and entities without performance bottlenecks, ensuring reliability and agility for nationwide services.

7. Self-Sovereign Identity enablement

Empowers citizens and staff to bring and manage their own digital identity, giving them full control over what data to share and with whom, supporting user-centric government services.

8. Identity risk assessment

Comprehensive evaluation of identity and access workflows to identify vulnerabilities, exposure points, and compliance gaps, enabling proactive risk mitigation across critical public sector systems.

9. Strategic roadmap development

Tailored plans for implementing decentralised identity solutions aligned with UK regulatory requirements, government digital strategies, and future scalability needs.

10. Technology advisory and tool selection

Expert guidance on choosing decentralised identity platforms, verifiable credential tools, and integration strategies for seamless adoption across government departments and agencies.

11. Privacy by design

Eliminates centralised data storage to minimise breach risks, ensuring citizen trust and compliance with UK GDPR and other privacy regulations.

12. Verified credentials and digital proofing

Secure identity validation without manual document submission or physical presence, leveraging advanced verification technologies for efficiency and accuracy in public service delivery.

13. Non-Repudiation assurance

Guarantees secure, auditable, and tamper-proof digital transactions, ensuring accountability and trust in every identity-related interaction across government systems.

14. End-to-End implementation services

From strategy and architecture to deployment and operational support, delivering complete lifecycle services for decentralised identity adoption in the UK public sector.

15. Regulatory compliance enablement

Ensures adherence to UK and global standards like GDPR, ISO 27001, NIS2, and DORA, reducing compliance risks and strengthening governance for critical public services.

1.5 Service Benefits

Extend collaboration by securely connecting anybody and anything to data and services, securely and accountably. Transform to operate from anywhere, regardless of device or channel without compromising your security or regulatory compliance.

1. Faster Onboarding

Automates identity proofing and verification, enabling rapid, high-assurance onboarding for citizens, employees, and partners without manual document checks or delays.

2. Open Standards Compliance

Built on globally recognized standards like DIDs and Verifiable Credentials, ensuring interoperability with credential issuers and consumers across sectors and borders.

3. Eliminate Data Honeypots

Sensitive identity attributes remain locally controlled and cryptographically secured, reducing centralized storage risks and minimizing exposure to breaches and ransomware attacks.

4. Accelerate Digital Transformation

Empowers trusted digital interactions and transactions while safeguarding privacy, supporting seamless service delivery across government, healthcare, education, and financial ecosystems.

5. Regulatory Alignment

Meets stringent requirements of DORA, UK Digital Trust Framework, eIDAS 2.0, GDPR, and NIS2, reducing compliance complexity and associated costs.

6. Privacy by Design

Implements decentralised identity principles and self-sovereign models, giving individuals full control over personal data and consent-driven sharing.

7. Zero Trust Security

Enforces continuous authentication, identity verification, and least-privilege access policies, strengthening resilience against insider threats and unauthorized access.

8. Reduce Identity Risk

Mitigates risks of credential theft, insider breaches, and ransomware by decentralizing identity storage and enforcing cryptographic security measures.

9. Support for Digital Wallets

Enables citizens to carry verified credentials—such as age, qualifications, and entitlements—in secure wallets, simplifying cross-sector authentication and reducing fraud.

10. Cross-Border Interoperability

Issues credentials aligned with eIDAS 2.0, supporting European Digital Identity Wallets for seamless authentication across borders and sectors.

1.6 End-to-End Decentralized Identity Services

Secure and manage digital interactions that rely on trusted identity while enhancing privacy, digital trust, regulatory compliance, and operational efficiency. Secure and manage digital interactions that rely on trusted identity while enhancing privacy, digital trust, regulatory compliance, and operational efficiency.

Advisory Services

- Identity Risk Assessment: Identify exposure points in identity and access flows.
- Strategy and Roadmap: Define a decentralized identity strategy aligned with regulatory compliance and business goals.
- Tool Selection: Recommend decentralized identity and verifiable credential tools.
- Regulatory Compliance: Alignment with DORA, UK Digital Trust Framework, eIDAS 2.0, GDPR, and NIS2.

Managed Services

- 24/7 Monitoring: Continuous oversight of identity usage and system access.

- **Audit and Activity Logs:** Maintain immutable logs of access and credential interactions.
- **Credential Lifecycle Management:** Automate issuance, revocation, and renewal of credentials.
- **Expert Support:** Provide skilled teams to manage decentralized identity infrastructure.

Delivery Services

- **Automated Onboarding:** Use identity proofing and credential issuance for seamless onboarding.
- **Credential Issuance:** Issue and manage verifiable credentials securely.
- **Access Session Management:** Enforce access policies and record credential usage.
- **Workflow Integration:** Integrate with ITSM tools for change management and credential reset.

Decentralized identity offers a transformative shift in digital trust by placing control of identity data in the hands of individuals, reducing reliance on centralized databases and mitigating risks of breaches and fraud. Solutions like Microsoft Entra Verified ID enable secure, user-controlled credentialing using open standards such as DIDs and Verifiable Credentials, streamlining onboarding, access management, and compliance.

In Europe, the eIDAS 2.0 regulation mandates the rollout of European Digital Identity Wallets (EUDI) by 2026, empowering citizens to store and share verified attributes such as age, residency, entitlements, qualifications and payment details. Enabling seamless cross-border authentication and reducing identity related fraud.

Blockchain-based support for +100 million decentralized identifiers, enhancing user privacy and reducing friction in digital interactions. DXC's enables scalable, privacy-preserving identity verification, lowering compliance costs and improving customer trust.

Enhance security, privacy, and user experience while aligning with global regulatory trends, making it a strategic imperative for government agencies and commercial enterprises navigating successful digital transformation.

1.7 A New Paradigm for Digital Trust

DXC Technology's Decentralized Identity solution is designed to revolutionize how individuals and organizations manage digital identities in an increasingly interconnected world. At its core, the offering aims to protect privacy, build trust, and streamline compliance in digital transactions by shifting control of personal data from centralized systems to the individual user.

Helping UK government organizations modernize systems, strengthen security, and ensure compliance across hybrid and multi-cloud environments. DXC's digital identity services:

- **Modernize legacy systems** with scalable solutions for hybrid and multi-cloud environments.
- **Provide expert advisory and managed services** to streamline identity provisioning and access management.
- **Automate policy enforcement** and enable real-time auditing for compliance reporting.
- **Leverage leading technology providers** to deliver identity security. (Microsoft Entra, Ping Identity, Thales, DigiCert, AWS, Google GCP, ServiceNow, Oracle, and many others)

With 450M+ identities managed, 3,200+ security experts, and UK-based SC/DV-cleared teams, DXC delivers secure, scalable identity services for mission-critical environments.

1.8 The Problem with Centralized Identity Systems

Traditional identity management systems rely on large, centralized databases that store sensitive personal information. These systems are vulnerable to data breaches, expensive to maintain, and often fail to meet evolving privacy regulations. DXC's decentralized approach eliminates these risks by enabling self-sovereign identities—where users control their own verified credentials and decide what information to share and with whom.

1.9 e-Wallets

Widely used to download tickets, membership cards, retail loyalty cards and payment methods into the e-wallets we have on our Android and Apple devices. All part of the rapid shift to digital channels. e-Wallets can also be hosted in the cloud for those without mobile devices. Look in your mobile phone e-wallet at the payment cards, loyalty cards, tickets and vouchers that we now carry in our phone and present when required. The EU is rolling citizen e-wallets for all EU citizens starting in 2026 under the eIDAS 2.0 framework. USA has deployed e-ID for TSA airport checks with a digital driving license in participating states. ICAO has agreed international standards for Digital Passports. The UK is rolling a citizen e-wallet in 2025 with a UK veteran's card and UK digital driving licence as the first two verified credentials on a new UK citizen e-wallet. The NHS app has largely been a successful demonstration of the adoption of a mobile application to access public services. There are plans to roll out a UK digital national identity in the coming years. Many parts of government will want and need to consume verified credentials and verified attributes carried in e-wallets as well as issue verified credentials and verified attributes to people's e-wallets.

1.10 Distributed Identity Framework (DIF)

There is a technical framework for managing these verified credentials in an open and interoperable manner. Distributed Identity Frameworks (DIF) provide a platform that uses a block chain to hold a cryptographic record that your credential was issued or validated by a trusted party, but importantly the personal data is not held on the block chain. You hold your personal data in your personal wallet protected with strong cryptography and your biometrics. There is no need for a central store of such sensitive personal data, an attractive target for hackers. It is hard to steal every smart phone and unlike a physical purse or wallet dropped in the street your e-wallet is cryptographically locked and can be protected with biometrics and PINs.

Governments are issuing digital drivers licenses and developing standards for digital passports and vaccine certifications. Educational institutions are issuing digital qualifications and digital safety certifications for regulated and safety critical sectors like banking, healthcare, transportation, and construction to quickly validate new employees and contractors. Visas and travel documents issued to tourists and businesspeople can increase tourism and international business investment by making travel easier while raising the quality of identity assurance.

1.11 Trust Framework

The technology cannot exist without a robust legal framework that defines responsibilities and liabilities and operational rules for the service providers, identity and attribute verifiers and for the people using the e-wallets to interact with government and commercial entities. Citizens need to understand the way their data is handled, how it is protected and that they can have confidence in the protection of their privacy and cybersecurity.

Countries across the world have legislated for Digital Identity Trust Frameworks and created organisations to operate and enforce the standards and certification processes. So that citizens can trust their e-wallets and be confident to use them across government and commercial service providers. The Office for Digital

Identities and Attributes (OfDIA) enables the use of trusted digital identity services in the UK.

1.12 ID Proofing

Government agencies and public service providers and companies in regulated sectors, such as banks, need to follow Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations when onboarding citizens or customers. Employers need to verify that the person who turns up on the first day as a remote worker is the person they interviewed, background checked and they are compliant with right to work legislation.

Digital ID proofing allows a person to hold up a photo ID to a web camera or mobile phone camera and have the contents captured and validated. The person's photography on the validated document can be matched against the live capture image of the person being ID checked and onboarded. Having validated them as an employee, public service user or a "known" customer then a verified credential can be stored on the person's e-wallet.

High assurance verified credentials stored in a personal e-wallet avoid the need to revalidate and verify the person's identity each time they want to share it via digital channels. This cuts costs for service providers for expensive manual ID verification in-person and the cost of repeated digital ID proofing over digital channels.

Decentralized identity allows people to decide who they share their verified credentials or verified attributes with and revoke access in future. The option to share just a verified attribute, such as address can be a significant cost saving for organizations that need trusted data attributes such as address and age to deliver services.

Self-sovereign Identities

A decentralized model also supports Self Sovereign Identities (SSI) where anybody can create their own identities from scratch and through sponsorship of trusted individuals or the building of reputation these identities become as trusted as any centrally issued credential. Addressing use cases for often socially excluded groups, "thin-file-people", who lack official records but still need to access government and financial services providers. The growing number of gig economy workers often building their valuable reputations from completing thousands of small tasks.

1.13 Population Scale

The decentralized approach scales easily to meet the demands of large citizen and IoT applications where the bottle neck of centralized transaction processing is impractical as the number of connected entities and the complex web of interconnected relationships expands. Old hub and spoke models reach their limit as peer to peer and increased edge processing deliver on these new opportunities.

A decentralised approach is innately more resilient and better able to keep critical services running smoothly and securely through natural and civil disasters and periods of cyber and kinetic conflict.

1.14 UK Public Sector Challenges

UK Public Sector needs regulatory compliance, cost reduction, improved security stance, quantum readiness, greater flexibility of service delivery, all while accelerating the growth of digital channels and adoption of a Zero Trust security approach.

Government has complex hybrid and multi-cloud environments with geographically dispersed staff and citizens working remotely and from home. A growing number of connected machines from IoT, RPA Bots and AI agents.

Managed Citizen IAM services for the UK public sector face constraints such as tight budgets, complex procurement rules, and legacy IT systems that hinder rapid modernization. Compliance with stringent regulations like GDPR, NHS Digital standards, and MoD security frameworks adds operational complexity.

Multi-cloud and hybrid environments, combined with geographically dispersed users and growing IoT ecosystems, require advanced orchestration and zero-trust security. Integration across fragmented government systems and data silos remains challenging, while balancing cost efficiency, scalability, and user experience. Additionally, skills shortages and risk-averse governance often slow adoption of innovative features like Passwordless authentication and decentralized identity.

1.15 Growing Threat Landscape

Identity is the gateway into your IT systems, networks, citizen data and services. In a world where you can login to any system from anywhere on any device the gateway to all your systems is behind your logon and only as good as your weakest account. Identity is often described as the new security perimeter as it is the critical control plane for access and organisational security.

Identities belong not just to people but to machines, connected devices, IoT, operational technology, systems accounts, cloud workloads, RPA bots and autonomous AI agents. Attackers target users with privileged access or system accounts with elevated access rights to steal data or deploy ransomware to disrupt operations and extort money. Attackers will also find ways to escalate the privileges on ordinary user accounts to give them the additional access required to achieve their targets.

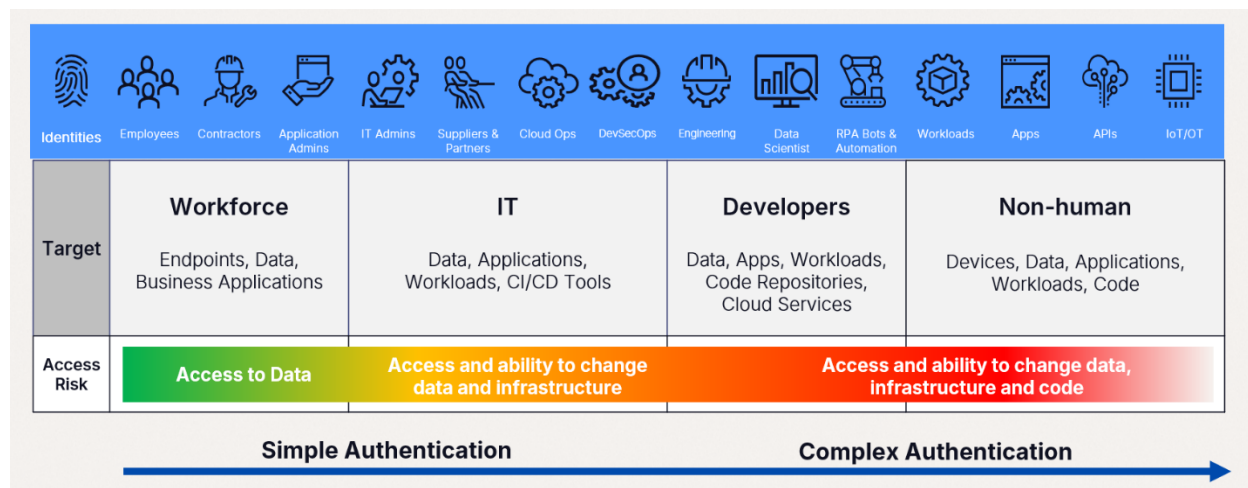


Figure 2. Growing Threat Landscape with Rising Number and Type of Identities

1.16 Cryptographic agility

Cryptographic agility, or crypto agility, enables your organization to quickly and seamlessly adapt your cryptographic mechanisms in response to new threats, vulnerabilities or changes in standards. You can change cryptographic algorithms, update key lengths, modify protocols, switch cryptographic libraries and rotate keys efficiently.

Visibility of cryptographic assets with automated management of keys and certificates allows you to address the following challenges:

- **Quantum readiness.** Quantum computers will revolutionize drug discovery, material science, forecasting and optimization. They will also break the public key cryptography that protects your data and communications, allowing criminals, competitors and governments to intercept and read your confidential data or impersonate anybody or anything. Being quantum ready requires cryptographic modernization to keep your data security ahead of the advancing capabilities of quantum computers.
- **Certificate expiration.** Today's TLS certificates that secure your web servers expire after 398 days. This will be reduced to 200 days in 2026, 100 days in 2027 and 47 in 2029. Shorter certificate validity improves your security but raises operational challenges that require automating certificate management.
- **Cloud-first strategy.** Control your own encryption keys (BYOK/HYOK) to retain data sovereignty for data residency laws. Protect the integrity and confidentiality of your data while maintaining the resilient and elastic computing capabilities of public cloud.
- **Identity and access management.** Certificates allow people and machines to authenticate and authorize as they connect to each other in our increasingly distributed and interconnected world.
- **Zero trust security.** Stop trusting and start verifying everyone and everything, everywhere, with Passwordless and MFA services that operate across all endpoints that hold and interact with your data.

1.17 User Support and Ticketing Support

Users can manage the status and priority of their support tickets. When Incidents are either detected by DXC or reported by authorized Customer personnel, DXC will classify them according to the priorities listed in the table below.

Table 1. Incident Priorities and Impacts.

Priority	Operational Impact	Business Impact
Critical (P1)	Failure on multiple Devices, systems, or user accounts.	Major impact on Customer's business
High (P2)	Failure of single system or Device.	High impact on Customer's business
Medium (P3)	Specific feature of system or Device unavailable or malfunctioning, or single user failure.	Limited impact on Customer's business
Low (P4)	No operational impact.	No business impact

2 Case studies

2.1 DXC an Experienced Partner

DXC is working with European governments on the EIDAS 2.0 citizen e-wallet and is one of the 8 providers of an approved reference e-wallet. We are helping a large European car makers pilot digital ID proofing to onboard new employees remotely. DXC has a long history of working with the UK government on issuing identity documents for travel, background checks for education, healthcare, work and volunteering with vulnerable service users.

DXC provides end to end services from expert decentralised identity policy advisory, design, and implementation through to managed decentralised identity services. DXC's management of digital identities, encryption keys, and certificates to ensure secure communication, establish trust, and streamline regulatory compliance. DXC's Decentralised Identity services are powered by industry-leading technologies from Microsoft, RedHat, Ping Identity, Google, AWS, Salesforce, ServiceNow, Thales, and DigiCert.

- **Trusted relationships.** We're committed to delivering mission critical identity security services for customers in banking, government, healthcare, energy and manufacturing.
- **Administrative expertise.** We help you streamline management of identities and credentials, ensuring existing systems and services run smoothly while accelerating digital transformation with modern user friendly, privacy protecting e-wallets, verified credentials and decentralised identities.

2.2 Secure UK Government Delivery

DXC Technology provides secure, accredited delivery capabilities across three UK locations (Newcastle, Farnborough and Erskine), ensuring compliance with government security standards and supporting mission-critical programmes.

Our Erskine Delivery Centre is a flagship facility designed for high-assurance services to UK Public Sector clients.

Comprehensive Service Portfolio:

- Networks and Testing – Secure network design, validation, and performance assurance.
- Service Management – ITIL-aligned operations for consistent, reliable service delivery.
- Cybersecurity Services – Advanced threat protection, monitoring, and incident response.
- Identity Services – End-to-end IAM solutions for citizen and workforce security.
- Operational Account Delivery – Dedicated teams for account governance and continuity.
- Peripheral Packaging – Secure configuration and deployment of end-user devices.
- Project and Programme Management – Agile and waterfall methodologies for complex initiatives.
- Architecture and Engineering Design – Scalable, secure solutions tailored to government requirements.



Figure 3. Erskine – Flagship UK Delivery Centre

Identity Services Expertise at Erskine includes:

- Microsoft Entra – Cloud identity and access management for secure digital services.
- CyberArk – Privileged Access Management to protect critical accounts and credentials.
- SailPoint – Identity governance for compliance and lifecycle management.
- Thales – Encryption and key management for data protection and trust assurance.

Physical and Operational Capabilities at Erskine:

- Build Labs – Secure environments for solution development and integration.
- Visitors Centre – Controlled access for client engagement and demonstrations.
- 544,000 ft² Campus – Large-scale facility supporting complex government programmes.
- Data Centre (170 racks) – High-capacity infrastructure for hosting secure workloads.
- Accreditations: ISO 27001 & ISO 9001 – Certified for information security and quality management.
- Modern Workplace Build Centre – End-to-end deployment of secure digital workplace solutions.

- 24/7 Network Operations Centre (NOC) & Shared Service Desk – Continuous monitoring and support for critical services.

2.3 National digital identity for 4 million citizens

Protecting the privileged access for the high security critical infrastructure which provides the signing keys and digital identity certificates for 4 million people.

- Achieved GDPR, ETSI, and eIDAS compliance, ensuring secure and trusted digital identity services for 6,500+ government and commercial services.
- Improved operational efficiency with automated privileged account lifecycle, credential rotation, and streamlined workflows.
- Enhanced security posture by eliminating privileged threats and providing full visibility of risks to management.

2.4 CIAM for a Transport Ministry

Citizen identity and access management for 2.5 million citizens and 20k civil servants for access to 20 transport ministry applications. DXC designed and delivered a CIAM solution which integrated with the citizen electronic identity scheme and supported SAML and OpenID standards for application integration.

Business Challenge:

- Lacked authentication methods that integrated with the citizen e-ID scheme.
- Poor user experience and complex registration and authentication journeys.
- Need for enhanced security to meet external cyber threats.

How DXC helped:

- Provided an experienced security architect to design and lead the delivery.
- Enabled national e-ID scheme (SPID) as primary access mechanism.
- Strong authentication with smart card and mobile authenticator integration.
- Onboarded 2.5 million citizens, 20 K civil service identities and 20 Applications.

Business Outcomes:

- Consistent user experience across four IT environments and 20 applications.
- National e-ID supported for citizens, companies and professionals.
- SSO to multiple citizen transport services.
- Improved security posture with strong Passwordless and multi-factor authentication.

2.5 City police digital transformation

DXC secured a 9-year contract to modernize the UK's largest police force:

- Implemented cloud-based ERP and AI-driven workforce planning.
- Delivered real-time resource allocation, reducing administrative overhead and improving frontline policing.
- Expected multi-million-pound savings through streamlined operations.

2.6 UK Defence – Zero Trust and secure communications

DXC deployed Zero Trust architecture and quantum-safe encryption for UK defence clients:

- Introduced Hermes private 5G platform for secure battlefield communications.
- Enabled continuous identity verification in contested environments.
- Supported coalition interoperability and mission readiness at scale.
- Did you know?
- DXC applied machine learning to vastly improve a cumbersome manual process of transformer station installations for an electricity supplier.
- DXC deployed an innovative security strategy and solution for a national institute for insurance against accidents at work to strengthen resiliency to malware attacks.
- DXC simplified IT infrastructure and increased automation to help a railway engine and carriage maker achieve a 62% reduction in critical IT incidents.
- DXC implemented a vision for smart factories using a next-generation digital manufacturing execution system and the digital thread framework for an international aeronautics company.

2.7 Streamline Travel Experiences

Airports are excited by the opportunity for people to perform their ticketing, passport checks, visas and vaccine certification on the sofa at home, downloading their verified credentials to their mobile device, and then experience an “open gate” journey through an airport. Giving back time for the shopping and dining that an airport would rather we did than the long queues they currently manage at peak times.

Decentralised identity enables innovation in the business travel and tourism space to reduce costs and improve travellers journey experiences. It avoids travel operators building up massive databases of sensitive personal data and travel documents. Many airlines have been the victims of successful hacking into their databases of customer travel documents and payment details. Transport operators like airlines and airports just need to know a traveller has valid documents for their destinations border controls and not keep a copy of them.

2.8 Did you know?

- DXC applied machine learning to vastly improve a cumbersome manual process of transformer station installations for an electricity supplier.
- DXC deployed an innovative security strategy and solution for a national institute for insurance against accidents at work to strengthen resiliency to malware attacks.
- DXC simplified IT infrastructure and increased automation to help a railway engine and carriage maker achieve a 62% reduction in critical IT incidents.
- DXC implemented a vision for smart factories using a next-generation digital manufacturing execution system and the digital thread framework for an international aeronautics company.

3 DXC Delivery Approach

3.1 DXC IAM Capability Model

DXC's Identity and Access Management (IAM) capability model delivers a robust framework designed to secure digital identities and uphold zero-trust principles across hybrid and multi-cloud environments for UK public sector organizations. Our approach ensures secure and accountable connectivity between people, devices, applications, and critical data systems, granting access only to authorized entities.

By integrating advanced Identity Governance and Administration (IGA), Access Management (PAM), and Adaptive Authentication, DXC enables public sector bodies to minimize risk, achieve stringent regulatory compliance, and provide seamless user experiences. This model supports:

- Centralized policy enforcement for consistent security controls.
- Federated identity management to enable secure collaboration across agencies.
- Scalable solutions capable of managing millions of identities across on-premises and cloud environments.

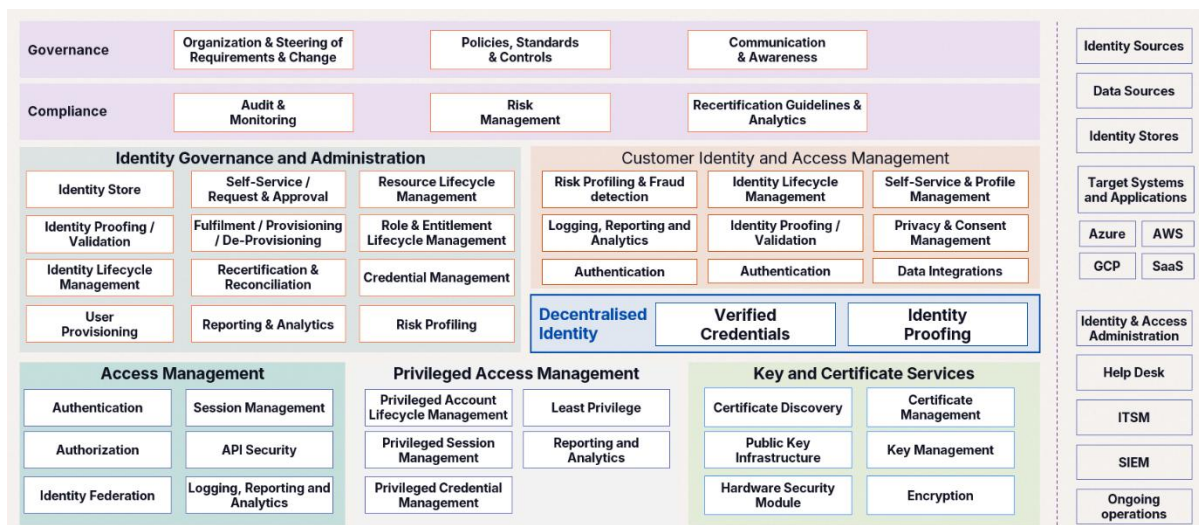


Figure 4. DXC IAM Capability Model

Beyond technology, DXC's IAM services deliver strategic value through a maturity-assessed roadmap that aligns identity capabilities with your technology and service objectives. We assess current-state identity processes, define a future-state architecture, and implement best practices using our extensive library of security blueprints. Our zero-trust adoption accelerators and identity fabric approach ensure resilience against evolving threats while enabling digital transformation. With deep expertise in Microsoft Entra, SailPoint, CyberArk, Ping Identity, BeyondTrust, Azure, AWS, GCP, Oracle, ServiceNow, and leading IAM platforms, DXC provides end-to-end advisory, implementation, and managed services to help clients modernize identity management and maintain compliance in complex, dynamic environments.

3.2 DXC IAM Delivery Methodology

DXC has defined a holistic approach for the definition and execution of IAM programmes based on decades of experience operating identity services for our customers.

This best-practice approach allows DXC to support customers at any maturity level during the whole IAM program from defining the IAM vision and strategy through design and implementation of the selected solution right up to fully managed IAM operational services.

DXC has defined blueprints and reusables from other projects which include:

- Framework for IAM governance,
- Framework for application onboarding,
- Automated build
- Deployment framework
- and others.

Identity is complex and a multi-year programme of work. DXC's experience of designing, implementing and then supporting, sometimes for decades, IAM solutions, directly informs our practical and pragmatic approach to successful service delivery. Our advisory is directly informed by our practical long-term delivery experience. DXC has been there with our customers running many generations of IT technology in our 50-year history while also deploying the latest technology and modernizing while squeezing value from the legacy assets.

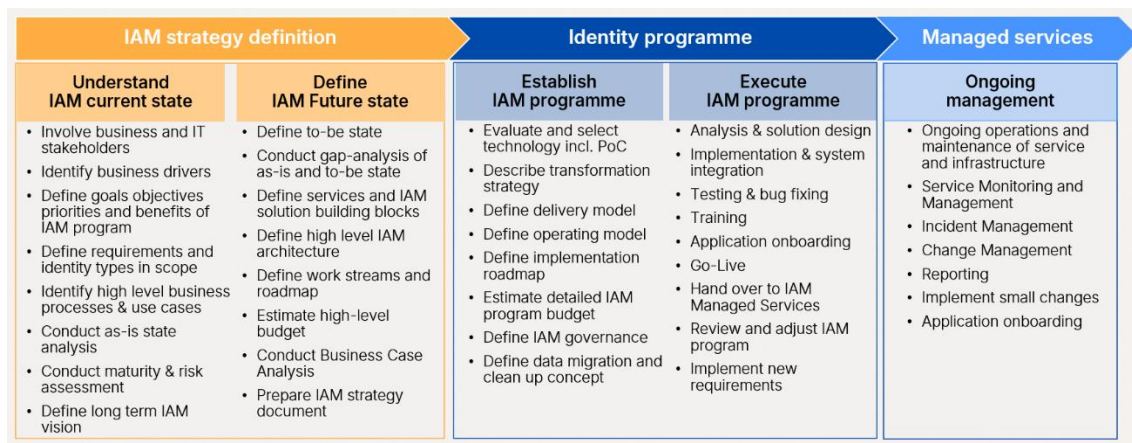


Figure 5. DXC End-to-end IAM Methodology

3.2.1 IAM strategy definition

Understand Identity and Access Management (IAM) current state:

1. Involve business and IT stakeholders
2. Identify business drivers
3. Define goals objectives priorities and benefits of IAM program
4. Define requirements and identity types in scope
5. Identify high level business processes & use cases
6. Conduct as-is state analysis
7. Conduct maturity & risk assessment
8. Define long term IAM vision

Define IAM Future state:

9. Define to-be state.
10. Conduct gap-analysis of as-is and to-be state.
11. Define services and IAM solution building blocks.
12. Define high level IAM architecture.

13. Define work streams and roadmap.
14. Estimate high-level budget.
15. Conduct Business Case Analysis.
16. Prepare IAM strategy document.

3.2.2 Identity programme

Establish IAM programme

17. Evaluate and select technology incl. PoC
18. Describe transformation strategy
19. Define delivery model
20. Define operating model
21. Define implementation roadmap
22. Estimate detailed IAM program budget
23. Define IAM governance
24. Define data migration and clean up concept

Execute IAM programme

25. Analysis & solution design
26. Implementation & system integration
27. Testing & bug fixing
28. Training
29. Application onboarding
30. Go-Live
31. Hand over to IAM Managed Services
32. Review and adjust IAM program
33. Implement new requirements

3.2.3 Managed operational services

Ongoing management:

34. Ongoing operations and maintenance of service and infrastructure
35. Service Monitoring and Management
36. Incident Management
37. Change Management
38. Reporting
39. Implement small changes
40. Application onboarding

4 About DXC Technology

DXC Technology (NYSE: DXC) is a leading global provider of information technology services. We're a trusted operating partner to many of the world's most innovative organizations, building solutions that move industries and companies forward. Our engineering, consulting and technology experts help clients simplify, optimize and modernize their systems and processes, manage their most critical workloads, integrate AI-powered intelligence into their operations, and put security and trust at the forefront. Learn more on dxc.com.

Every day we deliver excellence for our customers and colleagues. We use the power of technology to deliver mission-critical IT services that move the world. Our customers entrust us to deliver what matters most. We are DXC.

An Employer of Choice

We inspire and take care of our people. We work to create a culture of learning, diversity and inclusion for all our people to grow and reach their full potential.

A Trusted Technology Partner

We understand technology and are committed to delivering excellence for our customers.

A Company that Cares

We are committed to improving the communities in which we live and work. We are good stewards of our company, our customers and the world.

Deliver Mission Critical

We deliver the mission-critical IT services that move the world.

Entrusted to Deliver

Every day, we earn our customers' trust by delivering transformative technologies to ensure the success, safety and well-being of businesses and people worldwide.

Delivery Excellence

Our delivery excellence gives planes flight, helps patients heal, and increases the scale and speed of commerce.

Deliver What Matters Most

We are proud of the work we do and the trust and confidence our customers place in us to deliver what matters most.

Start planning now for crypto-agility and a post-quantum future.

Learn more at

dxc.com/digital-identity

dxc.com/key-and-certificate-services



Figure 6. Identity enables public service users and providers



DXC Technology
110 Pinehurst Road,
Farnborough Business Park,
Farnborough, Hampshire,
England, GU14 7BF

[DXC.com](https://www.dxc.com)

About DXC Technology

DXC Technology (NYSE: DXC) is a leading enterprise technology and innovation partner delivering software, services, and solutions to global enterprises and public sector organizations — helping them harness AI to drive outcomes at a time of exponential change with speed. With deep expertise in Managed Infrastructure Services, Application Modernization, and Industry-Specific Software Solutions, DXC modernizes, secures, and operates some of the world's most complex technology estates. Learn more on [dxc.com](https://www.dxc.com).

© 2025 DXC Technology Company. All rights reserved. Public