



Digital Identity

Service Description

Securely and accountably connect people and machines to data and services



Table of Contents

1	DXC Digital Identity for UK Public Sector	3
1.1	DXC Overview	3
1.2	Identity is the New Security Perimeter	4
1.3	UK Public Sector Challenges	4
1.4	DXC Digital Identity Services	5
1.5	Service Features.....	8
1.6	Service Benefits.....	9
1.7	End-to-End Digital Identity Services.....	12
1.8	Cryptographic agility	12
1.9	User support and ticketing support.....	13
2	Case studies.....	14
2.1	DXC an Experienced Partner.....	14
2.2	Secure UK Government Delivery	14
2.3	CIAM for a Transport Ministry	16
2.4	National digital identity for 4 million citizens	16
2.5	City police digital transformation	16
2.6	UK Defence – Zero Trust and secure communications	17
2.7	Did you know?	17
3	DXC Delivery Approach.....	18
3.1	DXC IAM Capability Model.....	18
3.2	DXC IAM Delivery Methodology.....	18
3.2.1	IAM strategy definition	19
3.2.2	Identity programme	20
3.2.3	Managed operational services.	20
4	About DXC Technology.....	21

List of Tables

Table 1.	Incident Priorities and Impacts.	13
----------	---------------------------------------	----

List of Figures

Figure 1.	DXC Identity Services	3
Figure 2.	Identity is your security perimeter	4
Figure 3.	DXC IGA Services	6
Figure 4.	DXC PAM Services.....	6
Figure 5.	DXC Access Management Services	7
Figure 6.	DXC Key and Certificate Services	7
Figure 7.	DXC Decentralised Identity Services	7
Figure 8.	Erskine – Flagship UK Delivery Centre	15
Figure 9.	DXC IAM Capability Model	18
Figure 10.	DXC End-to-end IAM Methodology	19
Figure 11.	DXC Digital Identity enables public service providers and users.	22

1 DXC Digital Identity for UK Public Sector

1.1 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.
- Decentralise identity to enable use of citizen e-wallets to carry verified attributes and verified credentials to streamline access to public services for everybody while protecting their privacy and reducing the risk of data breaches.
- 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.
- Enable access by citizens and customers to public services via digital and physical channels to enable service innovation, cost effective delivery while protecting privacy and ensuring security and compliance.
- Access Management services: Single Sign-On (SSO) across applications and IT services. Adaptive intelligent authentication and authorisation. Consistent enforcement of access policies everywhere. Secure work from anywhere and on any device. Improved authentication experiences without compromising security.

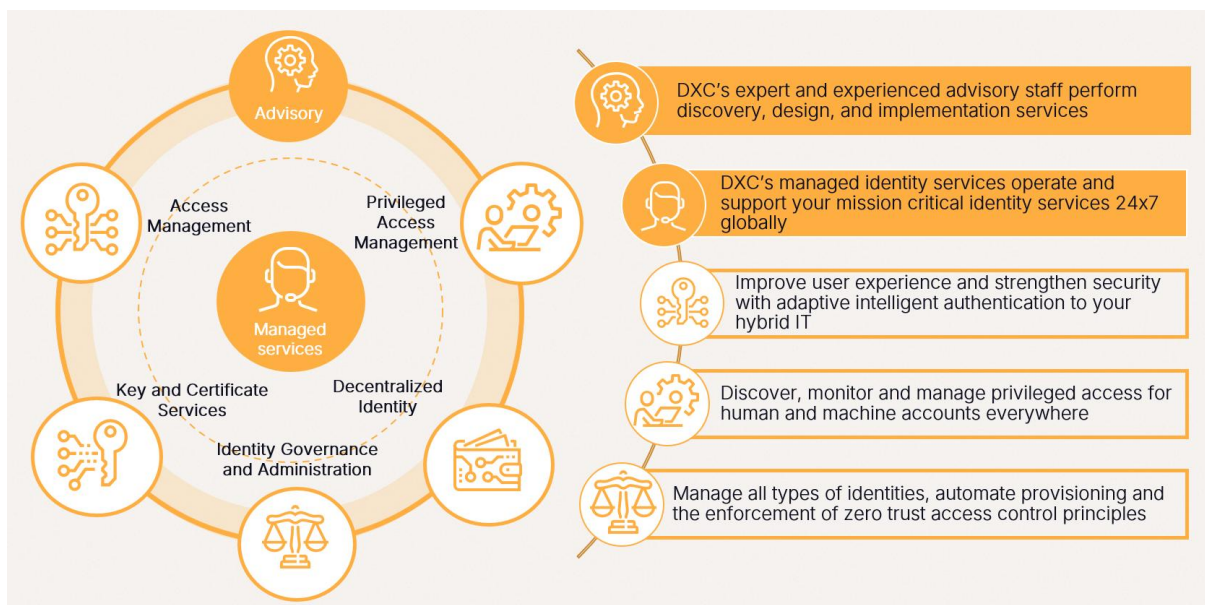


Figure 1. DXC Identity Services

1.2 Identity is the New Security Perimeter

Digital Identity is a foundation of any modern security infrastructure and a key pillar for a Zero Trust approach to security.

Digital identity is now central to how we live and work—whether logging into apps, accessing healthcare, or conducting financial transactions. DXC’s solution positions identity as a foundational element of digital transformation, enabling secure, scalable, and privacy-respecting interactions.

DXC’s Digital Identity service empowers people to take control over their personal data, enhancing privacy, digital trust, regulatory compliance, and operational efficiency across digital interactions that rely on trusted identity.

Commercial and government services have moved to digital channels to enable improved service delivery, greater efficiency and innovative service delivery. This shift to digital has also increased the focus on cybersecurity and regulatory compliance for data privacy. Identity has become increasingly the primary security control plane that determines who or what has access to which data and what they are allowed to do to that data.

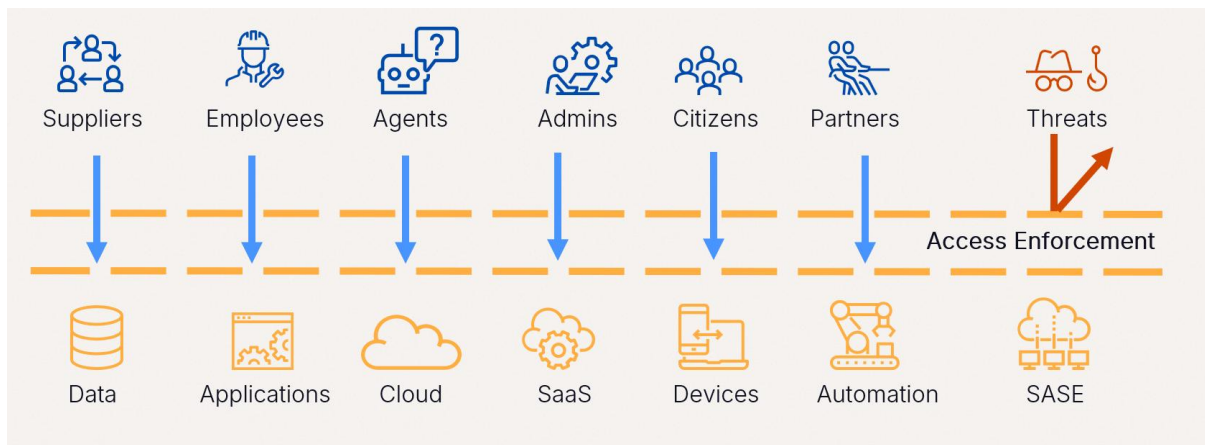


Figure 2. Identity is your security perimeter

1.3 UK Public Sector Challenges

UK Public Sector needs regulatory compliance, cost reduction, improved security stance, improved user authentication experiences, greater flexibility of service delivery, all while accelerating their shift to digital channels, and the growth in citizen adoption of digital channels and adoption of a Zero Trust security approach.

Government has complex hybrid and multi-cloud environments with geographically dispersed and remote and home working staff, citizens and a growing number of connected machines. How to deliver adaptive intelligent authentication that enforces access policies everywhere while facing fast changing threats?

People want to work from anywhere and on any device. How to Single Sign-On (SSO) across applications and IT services via any device from anywhere?

Users expect smooth authentication via any channel. How to improve user experience while strengthening authentication assurance?

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. Compliance with stringent regulations like GDPR, NHS Digital standards, and MoD security frameworks adds operational complexity.

1.4 DXC Digital Identity Services

DXC Digital Identity services enable secure access for people and machines to their data and public services, while remaining compliant with regulations, protecting privacy and defending against cyber-attacks.

DXC's services support the UK public sector to drive efficiency and service modernisation. Services that strengthen identity security by tightly controlling access through managing the provisioning of accounts, roles and access entitlements while logging and auditing all changes. Managing identities for people, machines and AI agents both on premises and in the cloud, across applications, services, and IT infrastructure of the public sector and commercial suppliers.

DXC Identity services are powered by industry-leading technology such as Microsoft, SailPoint, Ping Identity, RedHat, Okta, Thales, AWS, GCP, ServiceNow, Salesforce and CyberArk underpinned with expert advisory and managed security services.

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. Reduce the cost of regulatory compliance through centralised management of access policies and automatic enforcement across all applications and platforms.

DXC is experienced in deploying large digital identity solutions for complex clients providing mission critical services. Improving the experience for citizens, employees, partners, and suppliers by providing the right access when it is needed to support productivity and operational efficiency but not granting more access than is required for longer than is absolutely needed.

DXC ensures secure, scalable, and compliant identity security services for your mission-critical environments. DXC is qualified and experienced to design, implement and support your identity solutions:

- With 450M+ identities managed globally,
- 3,200+ security professionals,
- and UK-based SC/DV-cleared teams.

DXC's Digital Identity portfolio is composed of five main capabilities:

- Identity Governance and Administration
- Privileged Access Management
- Access Management
- Decentralised Identity
- Key and Certificate Services

The following diagrams provide an overview of these overlapping and supporting capabilities of digital identity or Identity and Access Management:

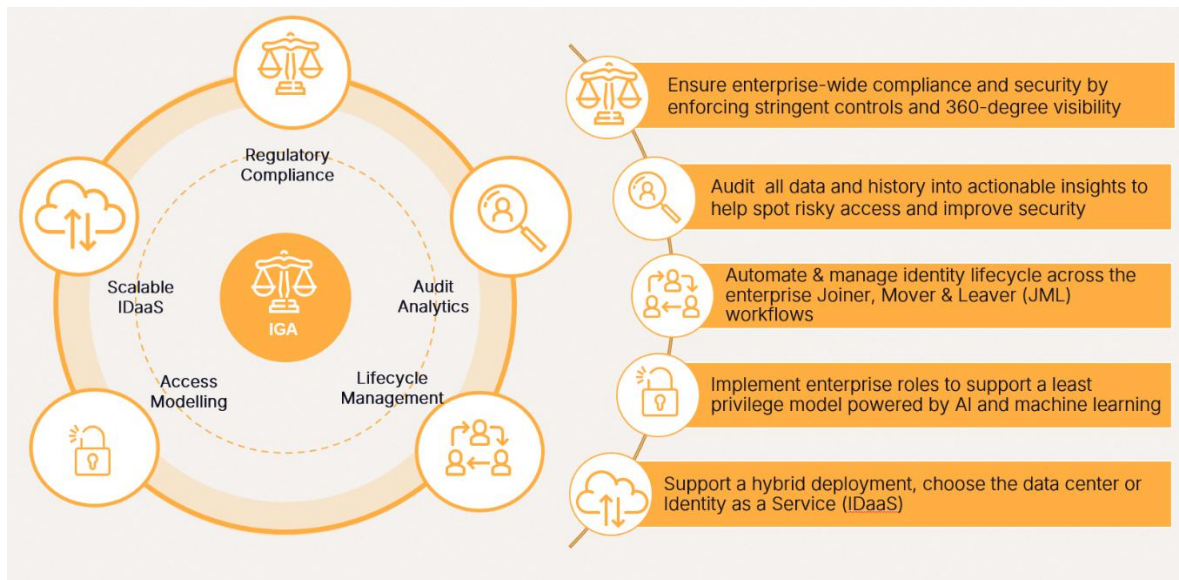


Figure 3. DXC IGA Services

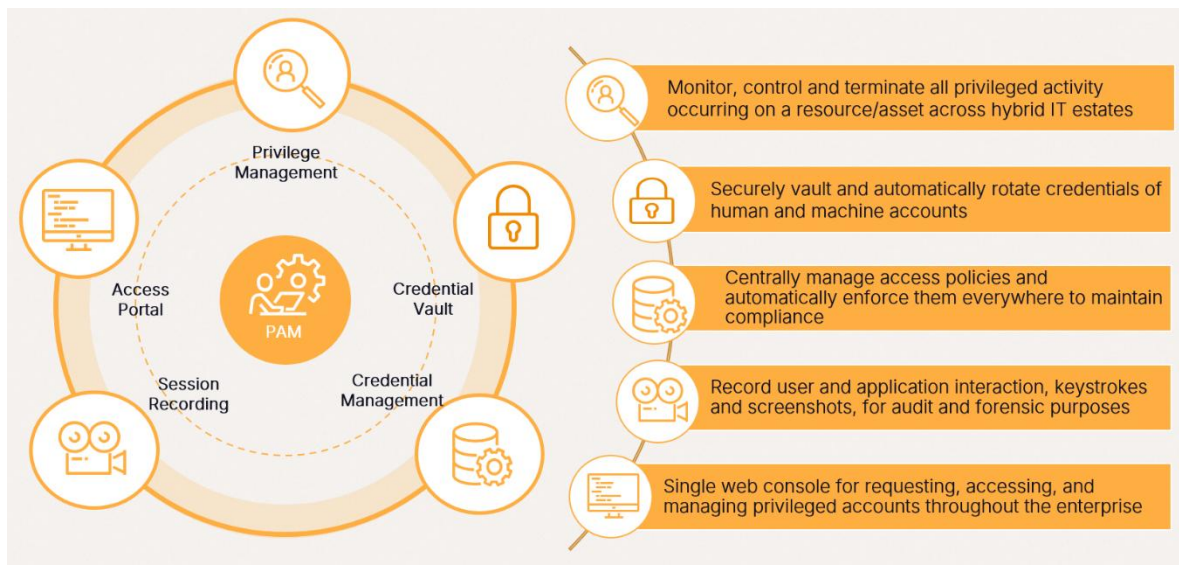


Figure 4. DXC PAM Services

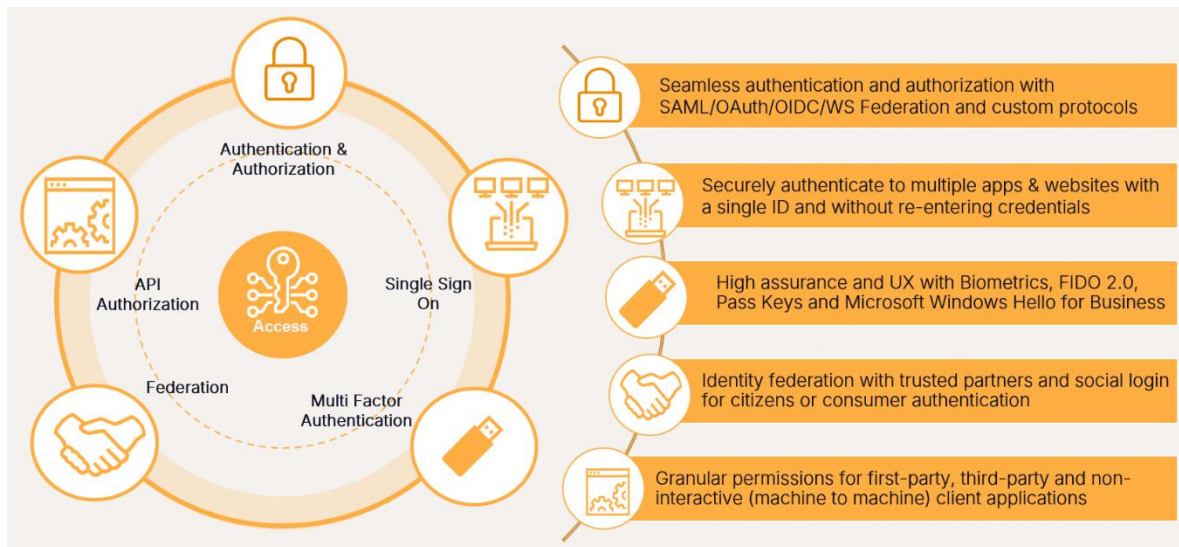


Figure 5. DXC Access Management Services

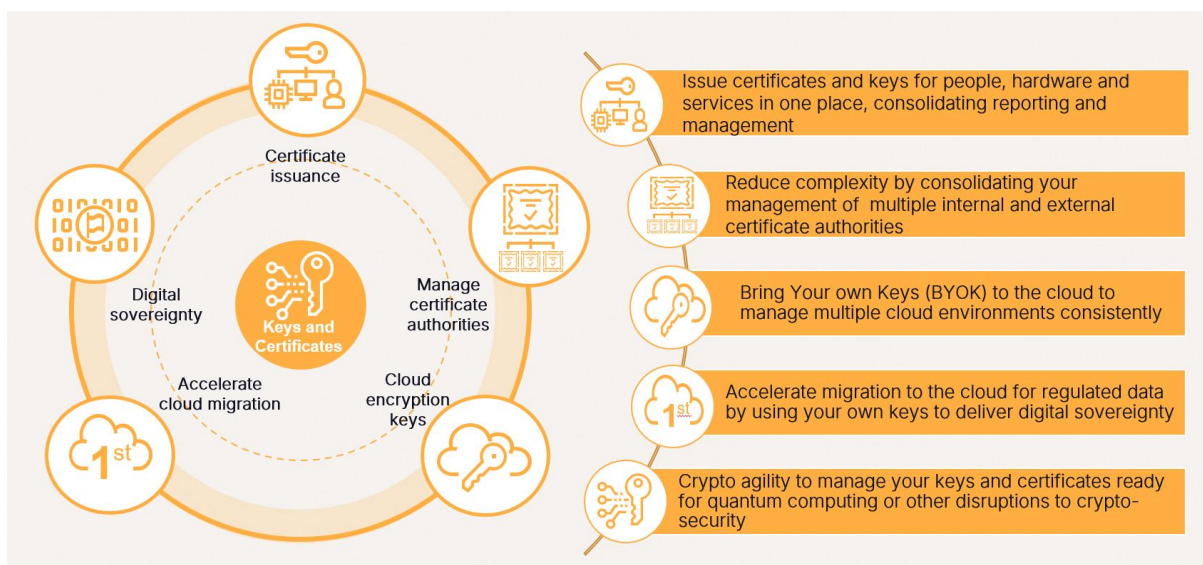


Figure 6. DXC Key and Certificate Services

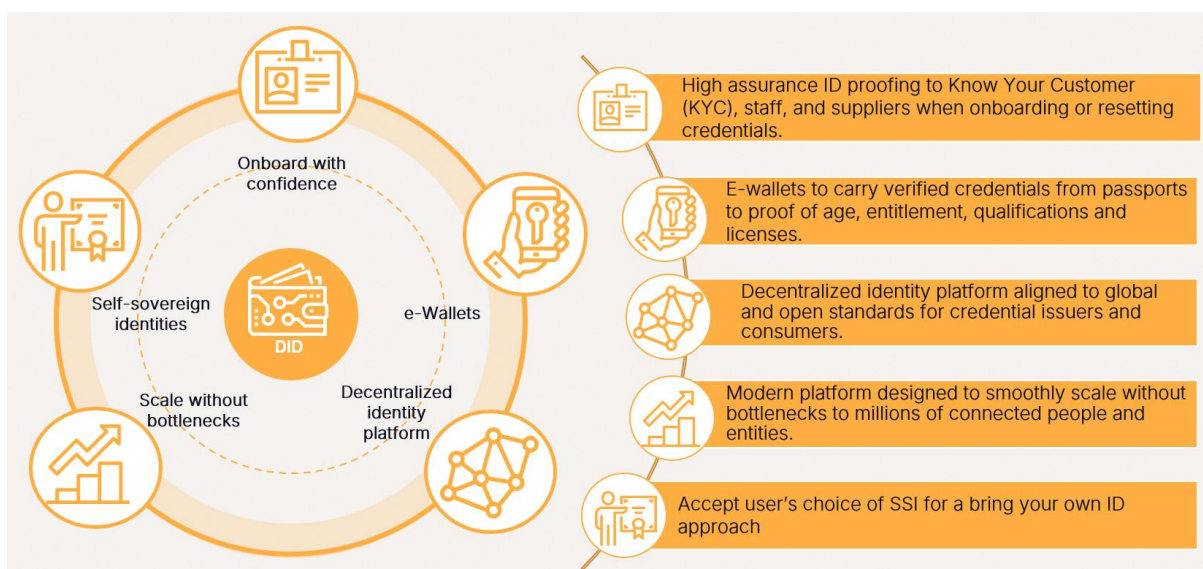


Figure 7. DXC Decentralised Identity Services

1.5 Service Features

Fundamental to successful digital government is the timely flow of data between authorized users and system, while maintaining regulatory compliance. Enable people and machines to securely access data and services. Know that the right person or machine has only the access required to accelerate your adoption of a zero-trust approach.

Deterring cyber-attacks, reducing the cost of regulatory-compliance, and enabling nimble adaptation to new ways of delivering public services is key to digital success. Capturing massive volumes of data means nothing if a user cannot access it or the latest machine learning systems process it to support timely decisions that drive efficiency and business growth.

Digital identity connects people and machines to data and IT services to enable fast and effective decision making with security and regulatory compliance.

Features and capabilities of DXC Digital Identity Services:

1. **Automation:** of identity lifecycles and provisioning flows for Joiners and Movers to Leavers (JML).
2. **Manage Access:** for employees, suppliers, partners, citizens, and machines.
3. **End to end services:** Advisory, design, implementation and operational support.
4. **Identity Federation:** Bring Your Own Identity (BYOID) for service delivery partners and suppliers.
5. **Hybrid and Flexible:** Deliver on-premises or SaaS for sovereignty and resilient scalability.
6. **Open Standards:** SAML, OAuth, OIDC, WS Federation and custom protocols.
7. **Credential Management:** Provision modern MFA, Passwordless, Biometrics, FIDO 2.0, Pass Keys and Microsoft Windows Hello for Business for high assurance security without compromise of user experience.
8. **Speedier Compliance:** Enforce regulatory changes faster by centralizing access policy management across on-premises, SaaS, APIs and legacy apps.
9. **Discover Identity Risks:** Visualize your identity risks to prioritize remediation and recertification tasks.
10. **Self-Service:** Manager identity lifecycle, enable self-service, and automate user provisioning flows.
11. **Flexible Hosting:** Identity as a service delivered to meet digital sovereignty requirements.
12. **Identity Federation:** Bring Your Own Identity (BYOID) by federating identities with partners.
13. **Dynamic identity verification:** continuous monitoring and least privileged access.
14. **Intelligent Adaptive Authentication:** intelligent context-based decisions informed by real time data signals.
15. **Privileged Credential Management:** Automatically rotate credentials for privileged accounts.
16. **Privileged Access Management:** Discover and quantify your privileged identity risks.
17. **Key and Certificate Management:** automate key and certificate lifecycles to enforce compliance and provide crypto agility and quantum readiness.

1.6 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 posture or regulatory compliance.

1. Service Innovation

Make it possible to deliver services in new ways by connecting people to services in digital and physical channels. Bring together data by connecting existing data better, linking with new data sources. Draw new insights from data by applying machine learning and AI technologies. All while enforcing privacy and access controls to protect data and the insights drawn for the data. Be able to deliver through new government and commercial partners by connecting with trusted partners to share access but only the access required and when needed.

2. Centralized Access Policies

Modern identity platforms centralize and automate management of access policies with decentralized enforcement across the protected systems, APIs and SaaS applications. So, when regulations change, or new threats emerge, rather than touch multiple applications, databases, and external systems with embedded access policies, change policy centrally and see it propagated automatically across all the protected systems on premise and in the cloud.

3. Improved User Experience

Single Sign-On (SSO) eliminates the need for multiple credentials, allowing workforce and citizens to access various government and commercial services seamlessly with the same credentials. Convenience fosters positive engagement for employees and service users. Disability access regulatory compliance and good business sense demands that we design our services with diverse stakeholders involved, not just the tech savvy people building these services. Inclusive design that involves older people, the disabled and other excluded groups to ensure our user experience and customer journeys include and delight everybody. Intelligent adaptive authentication draws on a broad set of signals to make decisions on when to ask for authentication at all or when to demand stronger step-up authentication in response to intelligence on threat actors or a high value transaction that requires additional assurances.

4. Elastic and scalable

Scale to millions reliably with secure cloud and SaaS delivery options that provide flexible on demand compute that responds to variations in demand expected for seasonal events or when responding to local incidents or national emergency that require rapid deployment of services to meet urgent needs. Providing a choice of on-premises and cloud services to meet our customers varied requirements for data residency, resilience, and scalability. A global news event or a segment on a consumer advice TV show can quickly spike visits to a website. An increasingly uncertain global situation has underlined the need for citizen services that can cope with unexpected volumes of demand without compromise to user experience or security.

1. Faster Citizen Onboarding

Automated self-service registration accelerates account creation, reducing manual intervention and improving service delivery speed. Citizens can quickly access your essential public services without delay, enhancing user satisfaction and service delivery efficiency.

2. Leverage DXC's skilled staff

Fill your identity and security skills gap by drawing on DXC's experienced and skilled identity and security specialists. Bring our experience of working in the public sector and highly regulated sectors facing rising security threats that need to maximise existing IT investments while delivering service innovations, efficiencies and new partnerships.

3. Enhanced Security Posture

Multi-factor authentication (MFA) and risk-based controls safeguard sensitive data. These measures significantly reduce the likelihood of breaches, ensuring government systems remain secure and resilient. Improve user experience and strengthen access security while reducing and removing passwords

4. Regulatory Compliance

Built-in consent management and audit capabilities help meet PCI DSS, GDPR, DORA, UK Digital Identity Trust Framework, NIS 2 eIDAS, and other public sector best practices. Compliance reduces legal risks and strengthens your credibility which builds trust in your systems and services for citizens.

5. Greater Citizen Trust

Transparent consent and privacy controls demonstrate accountability, building confidence in digital services. Citizens feel assured their data is being handled responsibly and ethically.

6. Reduced Fraud Risk

Identity proofing and verification prevent impersonation and deters unauthorized access. Strong identity assurance protects critical systems and minimizes fraudulent activities across government platforms.

7. Dynamic Risk Mitigation

Adaptive authentication adjusts security requirements based on real-time risk signals. This approach balances usability with protection, ensuring high-risk scenarios trigger stronger additional checks and verifications before access is granted to the user.

8. Interoperability Across Agencies

Federated identity enables secure collaboration between government departments and commercial suppliers for services and technology. Citizens benefit from streamlined access while organizations reduce duplication and complexity for workforce and supplier staff. Bring Your Own Identity (BYOI) for service partners and citizens.

9. Audit-Ready Operations

Comprehensive logging and reporting support compliance audits and investigations across web portals and APIs. These capabilities ensure accountability, transparency, and readiness for regulatory reviews at any time. External auditors demand more information at every audit cycle and are increasingly expensive without automation of all pervasive logging and reporting.

10. Best of Breed Partnerships

DXC's Access Management brings our experience of Microsoft Entra, Ping Identity, Thales, Okta, RedHat, and CyberArk. We provide secure, compliant access to data and IT services on any device, supported by centralized management and automated policy enforcement to lower compliance costs. DXC is experienced in large-scale deployments, including major secure portals for government.

11. Passwordless

The typical person can have 70 to 100 passwords for home and work. This degrades security and creates poor user experiences. Single sign-on is a core requirement of any access management portal. Reducing security risks from multiple weak passwords while

improving the user experience by shifting user to Passwordless and Multi-Factor authentication (MFA).

12. Federate with partners

Managing the identities and credentials of partners, suppliers and customers increases cost and complexity and damages the user experience if users are asked to register for a new account to access your systems and services. Identity federation lets you accept the authentication and attributes of trusted partners. They simply use their existing username and credentials to log on as a partner or supplier to collaborate. Customers are also able to use their preferred account such as a social media to login and access consumer and citizen services.

13. Accelerate zero trust adoption

A zero-trust approach relies on a robust identity service to authenticate access across all the edge touch points with the perimeter increasingly diffuse as data and services are increasingly distributed. An identity fabric is an enabler for organizations taking a zero-trust approach to security. Provide the right access to people and machines when it is needed but no more than the access that is required.

14. Designing for Everybody

Inclusive design promotes equal participation in digital government services. WCAG-compliant interfaces demonstrate accessibility for all citizens, including those with disabilities. Asking an older person or those with disabilities that affect dexterity to perform fiddly tasks entering selected parts of a password on a tiny on-screen keyboard, a keyboard that unhelpfully offers to autocomplete for them is not a good experience for even the most dexterous. DXC has worked with governments through user centred design that includes stakeholders to create inclusive experiences that make it easier for everybody.

15. 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.

16. Support Citizen e-wallets

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 that 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, disability status and qualifying age to deliver services. Without the need to share actual dates of birth or require people to provide evidence as proof each time they access a new public service.

1.7 End-to-End Digital Identity Services

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 an identity security strategy aligned with regulatory compliance and your organisational goals.
- Tool Selection: Recommend identity tools and identity security platforms.
- 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 interactions.
- Expert Support: Provide skilled teams to manage your identity security infrastructure.

Delivery Services

- Session Management: Enforce access policies and record credential usage.
- Workflow Integration: Integrate with ITSM tools for change management, user provisioning and credential reset.
- Automated Onboarding: Use identity proofing and credential issuance for seamless onboarding.

1.8 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 key and certificate services that operate across all endpoints that hold and interact with your data.

1.9 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 experienced in deploying large enterprise identity and access management solutions. Improving the experience for employees, partners, and suppliers. We also operate some large customer and citizen portals that allow people to interact securely through a digital channel with companies and government agencies. DXC provides complete Citizen Identity and Access Management (CIAM) solutions, Bringing our knowledge and experience of large customer or citizen IAM and their special challenges of compliance, usability and accessibility at population scale.

DXC provides end to end services from expert identity security policy advisory, design, and implementation through to managed identity security services. DXC offers integrated management of digital identities and credentials to ensure secure communication, establish trust, and streamline regulatory compliance. DXC's Digital Identity Services are powered by industry-leading technology companies such as Microsoft, Ping Identity, AWS, GCP, CyberArk, Salesforce, ServiceNow, Oracle, Okta, Thales, and DigiCert.

DXC has over 30 years of experience with modernizing identity solutions. We know how to run what you have while deploying the latest technology to maximise efficiency and service improvements in the public sector. We are helping our public sector customers run their mainframes and deploy the latest autonomous AI agents safely and effectively.

- **Trusted relationships.** We're committed to delivering mission critical access management services for customers in banking, government, healthcare, energy and manufacturing.
- **Efficiency expertise.** We help you consolidate multiple legacy solutions into a single integrated solution leveraging your existing identity security investments and the capabilities of the latest identity security platforms.

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 8. 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 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.

2.4 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.

2.5 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 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.

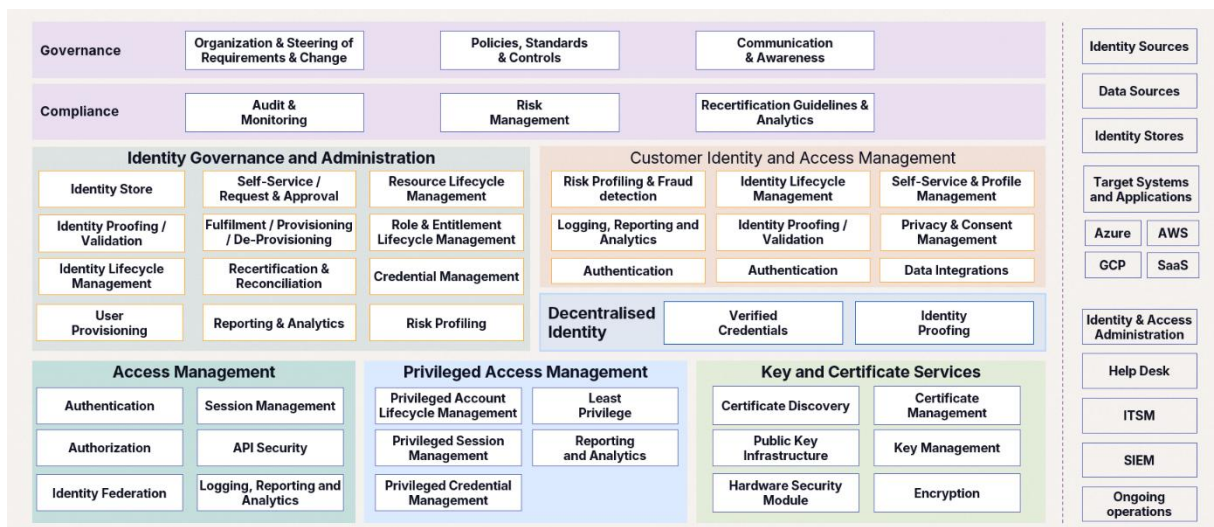


Figure 9. DXC IAM Capability Model

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 comprehensive 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.

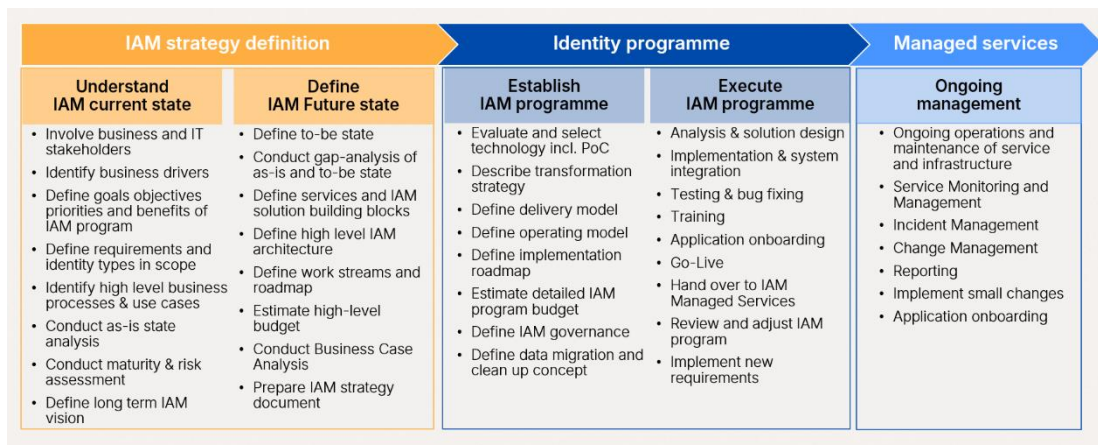


Figure 10. DXC End-to-end IAM Methodology

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 11. DXC Digital Identity enables public service providers and users.



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