



Passwordless and Multi-Factor Authentication (MFA)

Service Description

From Password Risk to Passwordless protection



Table of Contents

1	DXC Passwordless and MFA for UK Public Sector	3
1.1	DXC Overview	3
1.2	UK Public Sector Challenges	3
1.3	Service Features.....	4
1.4	Service Benefits.....	5
1.5	End-to-End Passwordless and MFA Services	7
1.6	Passwords are not enough	8
1.7	Evolving Threat landscape.....	9
1.8	The shift to Passwordless and MFA.....	9
1.9	Cryptographic agility	10
1.10	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	CIAM for a Transport Ministry	14
2.4	National digital identity for 4 million citizens	14
2.5	City police digital transformation	14
2.6	UK Defence – Zero Trust and secure communications	14
2.7	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. Build Trust with Seamless Authentication Experiences 7

Figure 2. DXC Access Management Services 8

Figure 3. Growing Threat Landscape with Rising Number and Type of Identities 9

Figure 4. Erskine – Flagship UK Delivery Centre 13

Figure 5. DXC IAM Capability Model 16

Figure 6. DXC End-to-end IAM Methodology 17

Figure 7. DXC Passwordless and MFA enables public service providers and users 20

1 DXC Passwordless and MFA for UK Public Sector

1.1 DXC Overview

DXC provides the full spectrum of digital identity services including:

- 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.

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. DXC Passwordless and Multi-Factor Authentication

DXC Technology delivers end-to-end Passwordless and Multi-Factor Authentication (MFA) services that enable UK public sector organizations to secure communications, establish trust and streamline compliance with GDPR, NHS Digital standards, and MoD security frameworks.

Increase trust in your digital interactions with Passwordless authentication designed for ease of use by real people. Enforce continuous and adaptive authentication, no matter who or what is accessing your data, wherever that data is stored. Powered by industry-leading technology such as Microsoft Entra, Ping Identity, Thales, Okta, and CyberArk.

DXC provides end to end services from expert certificate policy advisory, design, and implementation through to managed Passwordless and MFA services. DXC offers centralized management of authentication credentials, digital identities, encryption keys, and certificates for high assurance identity verification, to ensure secure communication, establish trust, and streamline regulatory compliance. DXC's Passwordless and MFA Services are powered by industry-leading technologies such as Microsoft, Ping Identity, CyberArk, SailPoint, AWS, GCP, Thales, and DigiCert.

DXC is helping our clients shift workloads to hybrid and multi-cloud environments while keeping data secure and compliant, using suitable encryption and private key services that lets workloads and data reside on the cloud without being accessible to the cloud service provider. DXC is experienced in deploying large mission critical systems that span hybrid cloud environments and existing data centres.

1.2 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.

1.3 Service Features

Features and capabilities of DXC's Access Management services for Passwordless and Multi-factor Authentication:

1. End-to-end professional services: advisory, design, implementation, operational support and managed services.

DXC provides comprehensive support from initial strategy and design through implementation and ongoing operational management. This ensures a seamless experience for organizations adopting MFA and Passwordless solutions.

2. Push authentication and challenge codes via mobile authenticator.

Users receive secure push notifications or challenge codes on their mobile devices, enabling quick and convenient verification without relying on passwords. Such out of band authentication methods provide an extra layer of verification as an attacker needs access to the mobile device.

3. FIDO2 authentication with mobile device authenticators, hardware tokens, and passkeys.

Fast ID Online (FIDO) is a secure authentication standard supported by Microsoft, Google, Apple, Thales, W3C and many more technology companies to provide easy to use and secure authentication online. DXC supports FIDO2 standards across multiple platforms, enabling strong, phishing-resistant authentication using passkeys and hardware tokens. Raising the level of assurance with cryptographically strong authentication which is also easier for end users.

4. Risk-based and continuous authentication enforcement.

Authentication policies dynamically adjust based on user behaviour, device health, and contextual risk factors, providing stronger security without impacting usability. Context matters and drawing on many data signals allows for step up authentication to be enforced when an ongoing attack is detected or intelligence shows a user is compromised in a third party data breach or the pattern of location, device and tasks is unusual and raises a red flag even if the methods of authentication were successful as an attacker may have compromised the users credentials or device to gain access.

5. Biometrics: face, fingerprint, palm, and voice authentication options.

Biometric authentication offers a frictionless, secure alternative to passwords, leveraging unique physical traits for identity verification. They are also a highly convenient method to unlock cryptographic keys that can be tightly bound to

credentials stored on a personal device. Avoiding the need to centrally store sensitive biometric data while allowing a easy shift to cryptographically strong authentication in the form of FIDO2 tokens and Passkeys.

6. Windows Hello for Business (WHfB) integration on Windows devices.

WHfB enables Passwordless sign-in using PIN, facial recognition, or fingerprint on a Windows device. Unlock the private authentication keys stored in the secure hardware of the Trusted Processing Module (TPM) enhancing enterprise security with cryptographically strong authentication that is phishing resistant. Many organizations have Windows widely deployed and are often licenced for Microsoft Entra allowing them to quickly deploy Microsoft MFA and WHfB.

7. USB hardware security keys and smart card support.

Hardware-based authentication adds a physical layer of security, protecting critical systems and privileged accounts from compromise. An attacker must steal the hardware and discover the PIN or biometric used to unlock the authentication keys stored in the secure chip. Stolen tokens and cards can be quickly cancelled and new certificates issued to the hardware and old certificates revoked. It is very difficult for an attacker working remotely and from overseas to cheat such hardware security.

8. User Behaviour Analytics (UBA) with One-Time Password capability.

UBA detects anomalies in user activity, such as accessing out of their regular hours on a never seen before device and attempting to download large amounts of data after resetting their credentials recently. While OTP provides an additional verification layer for sensitive transactions with a code generated by a device or software application based on a secret key held by that device alone and either a challenge string that needs to be entered or very simply the current time is used to generate a unique passcode that changes every constantly.

9. Certificate-Based Authentication (CBA) for high-assurance transactions.

Certificates provide cryptographic proof of identity, ensuring secure access for sensitive data and privileged operations. CBA provides people with high assurance authentication but requires they have a piece of hardware; smart card, USB keys, FIDO hardware token which contains a secure chip on which private keys are stored and sensitive cryptographic algorithms can be run privately to provide high assurance authentication.

10. Seamless integration with Microsoft Entra, Ping, Thales, Okta and legacy identity tools.

DXC leverages leading identity platforms to deliver scalable, interoperable solutions tailored to public sector needs. Our 50+ years of experience of working with government and secure clients means we know how to run what you have and get the most from previous generations of technology while helping organisations mature their security stance as technology advances and new innovative threats emerge.

1.4 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. Simplifies secure access with expert-led end-to-end delivery.

DXC's comprehensive approach reduces complexity by managing every stage of the authentication journey—from advisory and design to implementation and ongoing

operations. This ensures organizations achieve strong security without burdening internal teams, accelerating deployment and improving overall efficiency.

2. Enhances user convenience with mobile-based authentication challenges.

Push notifications and challenge codes on mobile devices provide a fast, intuitive way for users to verify identity. This eliminates password fatigue and streamlines access, improving user satisfaction while maintaining robust security controls.

3. Future-proof security using global FIDO2 standards and passkeys

By adopting FIDO2 and passkey technology, DXC delivers phishing-resistant authentication aligned with industry standards supported by major vendors. This ensures interoperability, long-term viability, and compliance with modern security frameworks such as Zero Trust.

4. Reduces fraud through intelligent adaptive, context-aware authentication policies.

Adaptive authentication dynamically adjusts based on user behaviour, device health, and global risk signals. This proactive approach minimizes fraud and unauthorized access while maintaining a seamless experience for legitimate users.

5. Improves user experience with biometric login for seamless but secure access.

Biometric authentication—such as facial recognition or fingerprint scanning—offers a secure, Passwordless experience that is both fast and user-friendly. It strengthens identity assurance while reducing reliance on vulnerable credentials such as passwords.

6. Strengthen enterprise security with WHfB Passwordless authentication.

Windows Hello for Business enables secure sign-in using PIN, facial recognition, or fingerprint, eliminating passwords entirely. This reduces credential theft risks and enhances compliance for organizations using Windows environments. Many already have Windows deployed widely and hold the licences to quickly realise the security and user productivity benefits.

7. Protects critical systems using hardware-based security tokens.

USB security keys and smart cards add a physical layer of protection for privileged accounts and sensitive systems. It poses a major challenge to attackers who need to access or steal the hardware devices, much harder than stealing or simply guessing a password. These hardware-based methods deliver high-assurance authentication for critical operations. They are also recommended for any member of the workforce who works remotely. MFA and Passwordless access is also a must for most when shifting to a Zero Trust approach to security.

8. Detect anomalies with advanced user behaviour analytics.

User Behaviour Analytics (UBA) monitors patterns and flags suspicious activity, helping organizations identify insider threats and compromised accounts early. Combined with OTP or other forms of MFA this adds an extra layer of security for high-risk transactions. A user might be compromised, or their MFA credentials may have been stolen so even when they have successfully authenticated, they cannot be trusted if their behaviour indicates compromise or breach.

9. Ensure regulatory compliance with strong certificate-based identity assurance.

Certificate-based authentication provides cryptographic proof of identity, meeting stringent compliance requirements for regulated environments. This approach secures sensitive data and privileged access with high-assurance credentials.

10. Leverage DXC's trusted technology partnerships for scalable, secure authentication solutions.

DXC integrates leading platforms such as Microsoft, AWS, GCP, Salesforce, ServiceNow, Oracle, Ping Identity, CyberArk, DigiCert and Thales to deliver scalable, interoperable solutions. This reduces vendor lock-in and ensures organizations benefit from proven, industry-leading technologies.

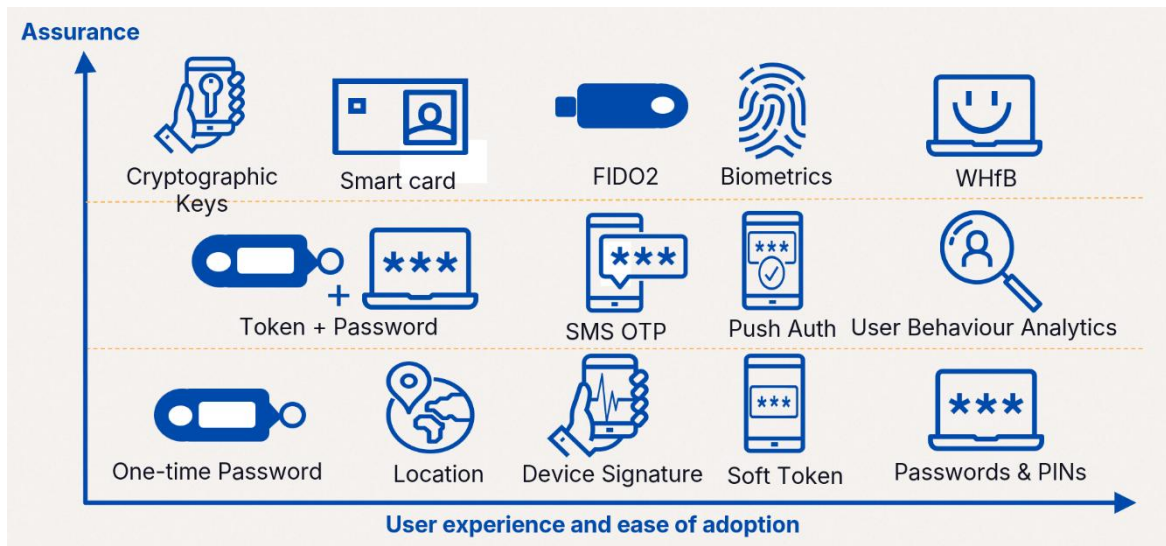


Figure 1. Build Trust with Seamless Authentication Experiences

1.5 End-to-End Passwordless and MFA Services

DXC provides end to end services from expert certificate policy advisory, design, and implementation through to managed Passwordless and MFA services. DXC offers centralized management of digital identities, encryption keys, and certificates to ensure secure communication, establish trust, and streamline regulatory compliance.

DXC's Passwordless and MFA services are powered by industry-leading technologies from technology providers such as Microsoft, Ping Identity, CyberArk, RedHat, AWS, GCP, Thales, and DigiCert.

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 access management strategy aligned with regulatory compliance and business goals.
- Tool Selection: Recommend access management tools and identity security platforms for Passwordless and MFA services.
- 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 access management infrastructure.

Delivery Services

- Access Session Management: Enforce access policies and record credential usage.

- Workflow Integration: Integrate with ITSM tools for change management and credential reset.
- Automated Onboarding: Use identity proofing and credential issuance for seamless onboarding.

DXC Passwordless and MFA services are typically delivered as part of a wider Access Management solution as organisations usually want to federate identities, single sign-on and apply conditional access (including MFA) for access to applications, APIs and IT services. Authentication is tightly integrated with authorisation.

It is also common to provide a full Identity and Access Management (IAM) suite of products or an Identity Security platform that provides:

- Access management, including Passwordless and MFA.
- Identity Governance and Administration (IGA) for user provisioning and audit reporting.
- Privileged Access Management (PAM) to provide additional controls and protections for elevated and privileged access.

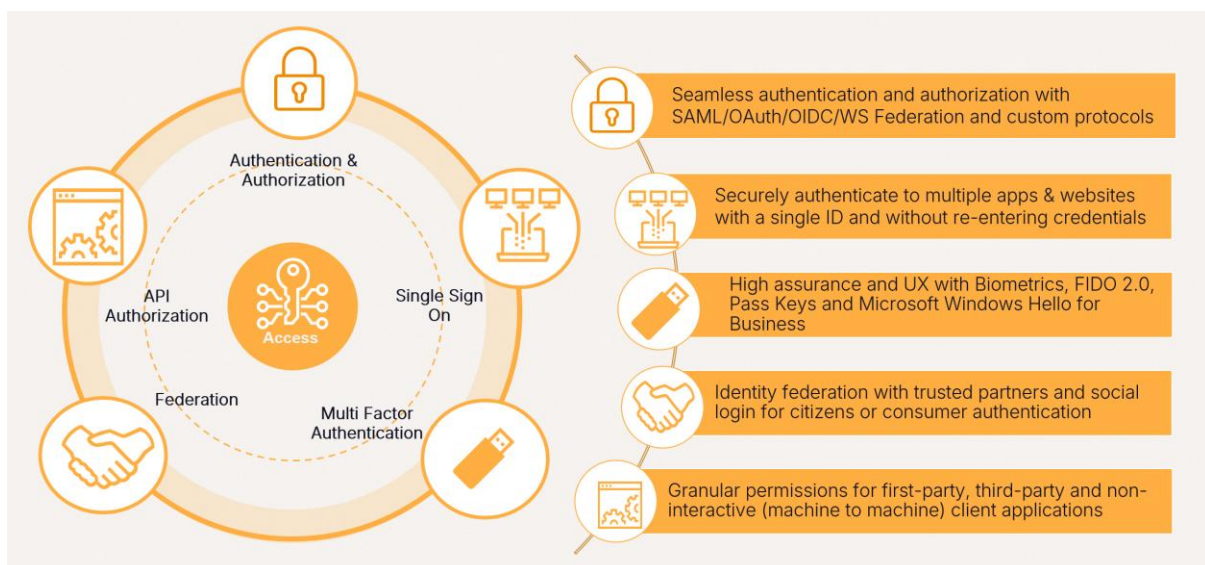


Figure 2. DXC Access Management Services

1.6 Passwords are not enough

Our modern world relies on digital interactions and transactions which depend upon high assurance authentication if they are to be trusted.

- Despite years of awareness, poor password practices—like reuse, sharing, and weak credentials—remain widespread and easily exploited by attackers.
- Phishing and credential-based attacks continue to be highly effective, especially when users reuse the same default password in many places. Their password can be stolen once and used in many other places.
- It's increasingly difficult to validate that users are who they claim to be, especially with remote and home working workforces.
- Complex user-unfriendly security controls can frustrate users, leading to poor adoption, work arounds and customer churn—especially when competitors offer smoother experiences. Outdated requests to change passwords frequently and to as people to create passwords with complexity rules are neither practical nor effective

security measures and are not recommended as best practice though still widely practiced and pointlessly enforced on users.

1.7 Evolving Threat landscape

Criminals, hackers, state actors, disgruntled or incompetent staff are all likely sources of cyber risk.

Passwords are weak and prone to many forms of long-standing attacks:

- Automated password cracking
- Keylogging and malware
- Social engineering
- Stolen credentials
- Dictionary attack
- Phishing

Attackers have access to increasingly sophisticated tools to steal or compromise weak credentials. Attack methods are evolving rapidly, demanding a new approach to authentication.

- AI powered social engineering to manipulate individuals into giving up access.
- Automated bots are increasingly effective at guessing passwords.
- AI is helping to automate sophisticated credential attacks.
- Stolen credentials are frequently traded on the dark web.

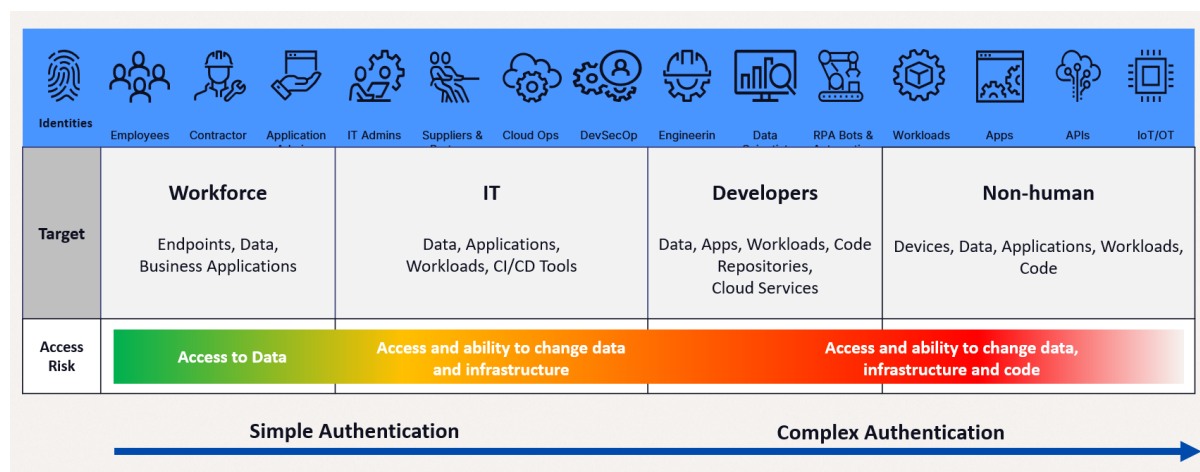


Figure 3. Growing Threat Landscape with Rising Number and Type of Identities

1.8 The shift to Passwordless and MFA

Many organisations have adopted multi-factor authentication for remote access or high-risk system administrator accounts or high value transactions. This approach often involves adding an additional method of authentication alongside passwords. This improves the security stance but still relies on the use of passwords which are innately not secure and inconvenient to use for a human being. Reserving MFA just for high-risk user accounts is also not sufficient as attackers will acquire the password of a regular user and having gained access will find a means to raise its privileges and entitlements so it can be leveraged to steal data or disrupt operations with ransomware.

The other driver for Passwordless authentication solutions is a focus on ease of use without compromise to security. Yes, it is possible to make authentication more secure and yet make it easier for a human being to use and stay secure.

Key benefits of Passwordless and MFA:

- Breach Mitigation – No passwords to steal reduces breach risk.
- Phishing Protection – No password to trick you into sharing.
- No Forgotten Passwords – Eliminates reset requests freeing up help desk staff.
- Stronger Hacking Defence – More secure than passwords for authentication.
- Reduced Attack Surface – Fewer vulnerabilities to exploit.
- No Password Reuse – Because there are no passwords to reuse.

The outcome:

- Improved user experience aligned with the needs of modern digital enterprises.
- A proactive step toward Zero Trust digital identity management.
- Improved identity security while reducing user friction.

1.9 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.

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

DXC is helping our clients shift workloads to hybrid and multi-cloud environments while keeping data secure and compliant, using suitable encryption and private key services that lets workloads and data reside on the cloud without being accessible to the cloud service provider. DXC is experienced in deploying large mission critical systems that span hybrid cloud environments and existing data centres.

- **Trusted relationships.** We're committed to delivering mission critical authentication services for customers in banking, government, healthcare, energy and manufacturing.
- **Administrative expertise.** We help you consolidate management of your identities and credentials, ensuring existing systems and services run smoothly while accelerating digital transformation with modern user friendly Passwordless authentication.

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 4. 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.

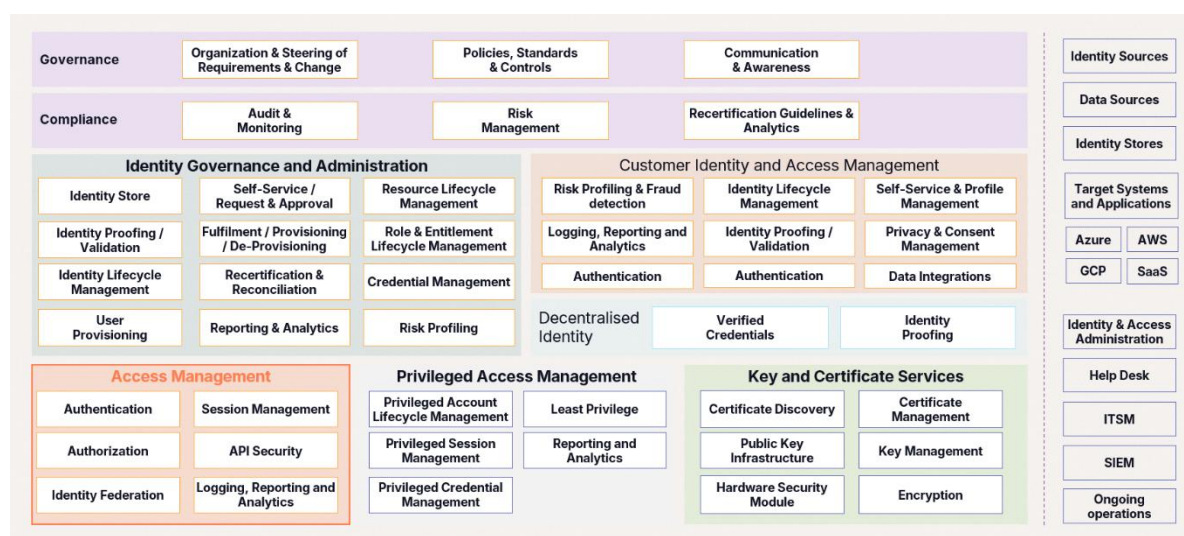


Figure 5. DXC IAM Capability Model

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.

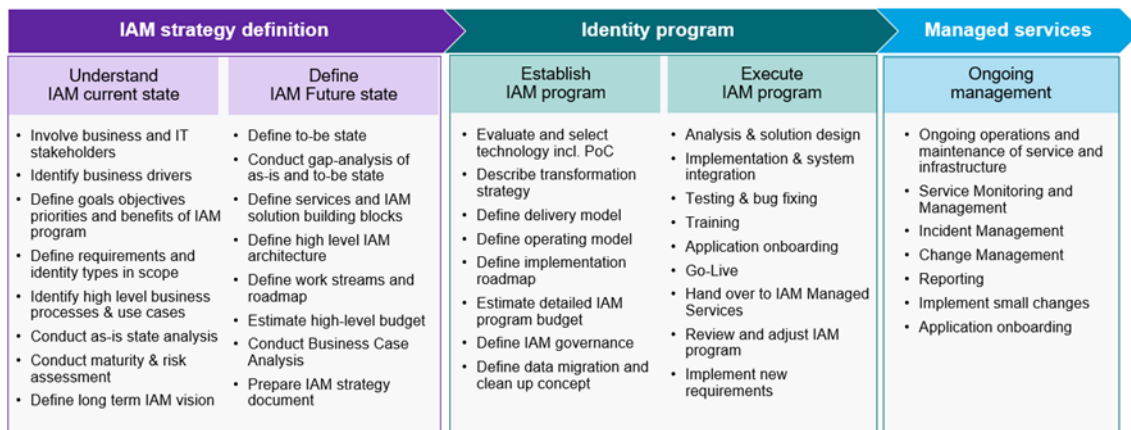


Figure 6. DXC End-to-end IAM Methodology

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 7. DXC Passwordless and MFA enables public service providers and users



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

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.

© 2025 DXC Technology Company. All rights reserved. Public