



Key and Certificate Services Service Description

Trusted digital interactions for people and machines



Table of Contents

1	DXC Key and Certificate Services for UK Public Sector	3
1.1	DXC Overview	3
1.2	DXC Key and Certificate Services.....	3
1.3	Service Features.....	4
1.4	Service Benefits.....	5
1.5	Cryptographic agility	5
1.6	User support and ticketing support.....	6
2	Case studies.....	8
2.1	DXC an Experienced Partner.....	8
2.2	Secure UK Government Delivery	8
2.3	National digital identity for 4 million citizens	10
2.4	City police digital transformation	10
2.5	UK Defence – Zero Trust and secure communications	10
2.6	CIAM for a Transport Ministry	10
2.7	Did you know?	11
3	DXC Delivery Approach.....	12
3.1	DXC IAM Capability Model.....	12
3.2	DXC IAM Delivery Methodology.....	12
3.2.1	IAM strategy definition	13
3.2.2	Identity programme	14
3.2.3	Managed operational services	14
4	About DXC Technology	15

List of Tables

Table 1.	Incident Priorities and Impacts.	6
----------	---------------------------------------	---

List of Figures

Figure 1.	DXC Key and Certificate Services	4
Figure 2.	Erskine – Flagship UK Delivery Centre	9
Figure 3.	DXC IAM Capability Model	12
Figure 4.	DXC End-to-end IAM Methodology	13
Figure 5.	DXC Key and Certificate services for trusted public digital services.	16

1 DXC Key and Certificate Services for UK Public Sector

1.1 DXC Overview

DXC Technology delivers end-to-end Key and Certificate services that enable UK public sector organizations to secure communications, establish trust and streamline compliance with GDPR, NHS Digital standards, and MoD security frameworks. Consolidate onto a crypto-agile platform that delivers automation and quantum readiness.

- 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.

Our modern world relies on cryptography for trusted digital interaction and transactions.

- Secure communication. Share your data across the internet without it being tampered with or viewed by third parties.
- Data integrity and confidentiality. No matter where your encrypted data is stored, nobody can read it without your cryptographic keys. A digitally signed hash of your data alerts you when it has been altered.
- Authentication. A sender signs their document with their private key, and a receiver can verify who sent the document by checking it with the sender's public key.
- Nonrepudiation. Legally binding communications and contracts signed digitally cannot later be denied or refuted by the sender.

1.2 DXC Key and Certificate Services

Centralized management of digital identities, encryption keys, and certificates to ensure secure communication, establish trust, and streamline regulatory compliance. Accelerate the adoption of cloud and SaaS with your own private root of trust to protect the confidentiality and integrity of your data while maintaining data sovereignty.

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

Certificate Services is powered by industry-leading technologies from industry leaders such as Microsoft, 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.

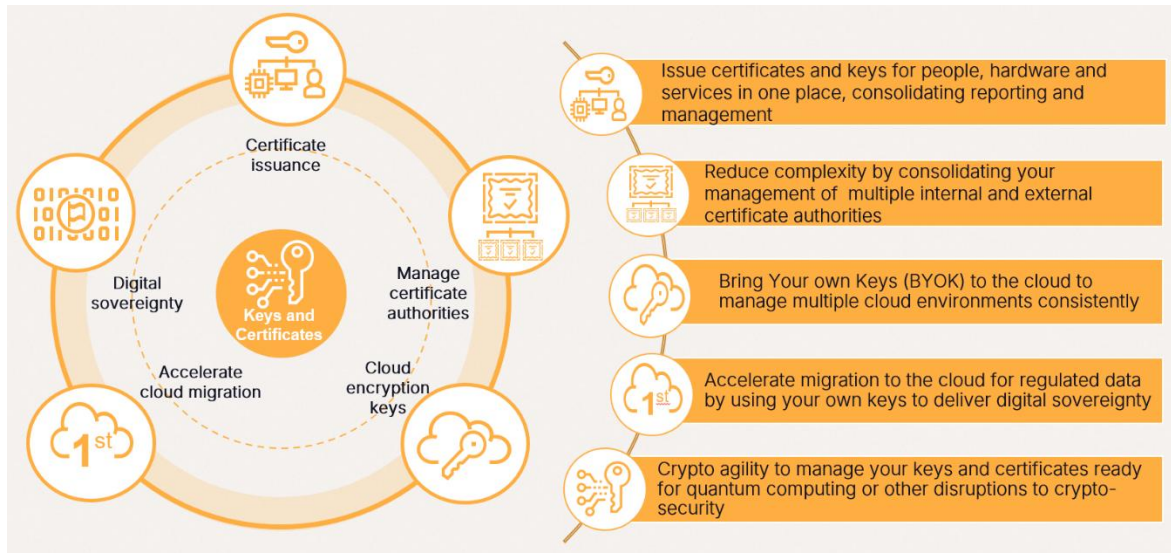


Figure 1. DXC Key and Certificate Services

1.3 Service Features

Features and capabilities of DXC Key and Certificate Services:

- Certificate issuance for people, hardware devices, and IT services.
- Consolidate multiple internal and external certificate authorities.
- Cloud encryption keys on a single platform to manage multiple cloud environments.
- Scalable delivery and management with a choice of on-premises and SaaS options.
- Elastic cloud PKI: AWS, Microsoft Azure and Google Cloud Platform.
- Issue certificates for DevSecOps to secure containers in the cloud and on-premises.
- Issue certificates for people, hardware devices and IT services.
- Consolidate multiple internal and external certificate authorities.
- Manage cloud encryption keys on a single platform for multiple cloud environments.
- Provide scalable service delivery and management for both on-premises and SaaS.
- Support Amazon Web Services, Google Cloud and Microsoft Azure encryption.
- Secure containers for DevSecOps in the cloud and on premises
- Crypto-agility advisory
- Quantum readiness
- Certificate discovery
- Public key infrastructure management

- Certificate life-cycle management
- Encryption key management
- Hardware security module management
- Operational performance tracking
- Compliance report generation
- 9-to-5 and 24x7 operational support
- Risk-based prioritization.
- Global delivery centres
- Local secure delivery

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.

- Centralized management of keys, and certificates to establish digital trust.
- Accelerate cloud migration for regulated data and streamline regulatory compliance.
- Achieve digital sovereignty to meet regulations and the challenges of an unstable globe.

1.5 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.

End-to-End Key and Certificate Services

DXC provides end to end services from expert certificate policy advisory, design, and implementation through to managed key and certificate services. DXC offers centralized management of digital identities, encryption keys, and certificates to ensure secure communication, establish trust, and streamline regulatory compliance. DXC's Key & Certificate Services is powered by industry-leading technologies from Microsoft, 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.
- 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 decentralized identity 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.

1.6 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	Limited impact on Customer's business

Priority	Operational Impact	Business Impact
	unavailable or malfunctioning, or single user failure.	
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 certificate policy advisory, design, and implementation through to managed key and certificate services. DXC offers centralized management of digital identities, encryption keys, and certificates to ensure secure communication, establish trust, and streamline regulatory compliance. DXC's Key & Certificate Services is powered by industry-leading technologies from Microsoft, 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.

DXC has over 30 years of experience with modernizing cryptography solutions, as well as established relationships with strategic suppliers of quantum-ready technology, including AWS, CyberArk, DigiCert, Google, Microsoft and Thales.

- **Trusted relationships.** We're committed to delivering mission critical cryptographic services for customers in banking, government, healthcare, energy and manufacturing.
- **Administrative expertise.** We help you consolidate management of your cryptographic keys and certificates, ensuring crypto agility for quantum safe encryption and addressing the challenges of reduced certificate validity periods in the coming years.

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 2. 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 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.

2.5 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.

2.6 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.

2.7 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.

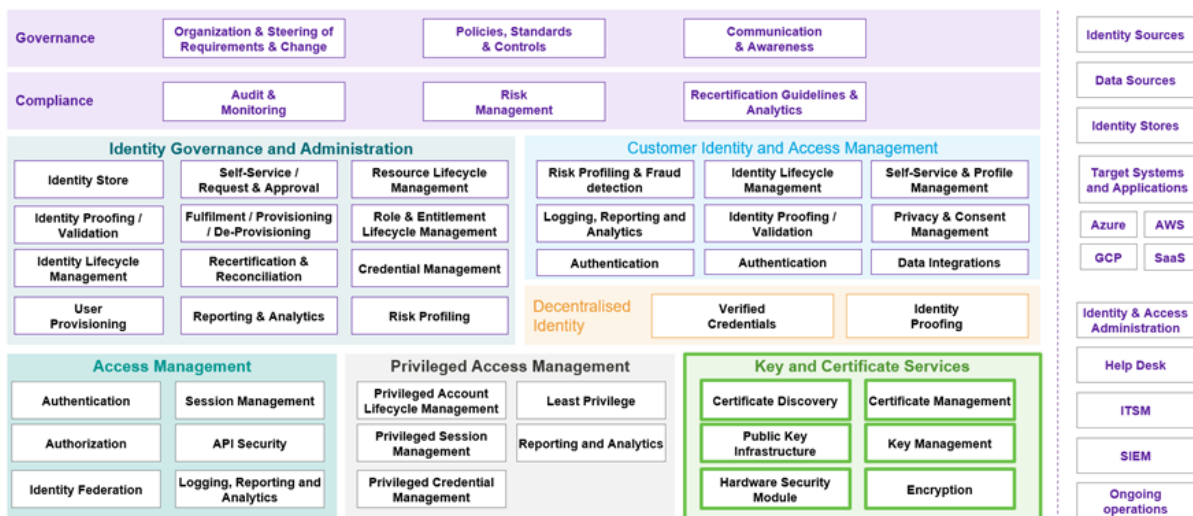


Figure 3. DXC IAM Capability Model

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.

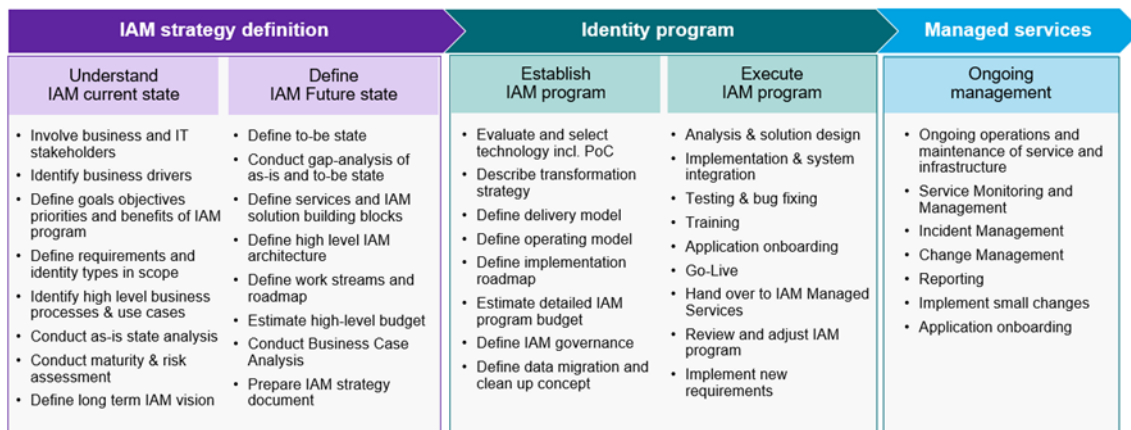


Figure 4. DXC End-to-end IAM Methodology

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 minor 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 5. DXC Key and Certificate services for trusted public digital services.



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