PKI for Central Government Organisations in the UK

Discover the critical role of identity and public key infrastructure (PKI) in enhancing security for Central Government Organisations in the United Kingdom

The era of digital government is here. The shift to cloud computing and fast-developing technologies, including artificial intelligence (AI) and IoT devices, creates new opportunities — and complexity. Adopting modern technology and sunsetting legacy systems helps government organisations improve productivity, better connect citizens to essential services, and drives efficiency, but not without security.

In an increasingly connected world, improving security and resilience of critical national infrastructure and services is essential to protect the UK's national security and economic prosperity. Disruption or failure of services can have a significant impact on businesses, governments, and citizens that rely on those services.

The National Cyber Security Center (NCSC) states in their 2023 Annual Review that "the new frontline is online," citing a multitude of threats from bots undermining democracy, to hacks disrupting public services, to ransomware attacks on businesses. To thrive in this always-on, connected age while safeguarding against threats, government security strategies must evolve.

Traditional security perimeters are no match for sophisticated threats from hostile state and non-state actors. Mission success demands an identity-first approach, ensuring authentication of every connected person, device, and workload, and encryption of data transmitted between them.

Threats and challenges for central government organisations in the UK:

- The rapid use of artificial intelligence is compounding threats and lowering the barrier to entry to malicious actors
- Supply chain attacks by nation-state and non-state actors undermine trust in systems and software
- Adoption of connected IoT devices and cloud services increases the attack surface of government services
- Ransomware and denial of service attacks increasingly aim to disrupt critical infrastructure and essential services
- Traditional security perimeters and legacy systems are inadequate defense against sophisticated threats

PKI: the foundation of digital trust

Public key infrastructure (PKI) serves as the foundation of digital trust — a critical layer in the security of government organisations that ensures authentication, confidentiality, and integrity in digital communications.

For trust to work, it has to extend to every connected device, digital interaction, and application. That's what makes PKI so effective: it binds a trusted and verifiable identity to digital objects like websites, users, devices, emails, networks, and software. PKI forms the foundation of a Zero Trust strategy. By implementing a resilient and scalable PKI, these departments can significantly enhance their resilience against threats like malware and ransomware.

Authentication

PKI enables strong authentication by verifying humans, machines, workloads, services, and anything connected with a cryptographically unique identity.

Encryption

PKI facilitates secure communication by encrypting data transmitted between connected people and devices using robust encryption mechanisms.

Integrity

PKI and signing mechanisms deliver tamper-proof software, code, and digital content by verifying their source and integrity to mitigate threats.

Why PKI is a time-critical project for government organisations

The UK government's increasing reliance on digital services demands a robust PKI to strengthen communications and data protection. Disruptive changes in the technology and threat landscape mean that government organisations must re-assess the capabilities of their PKI solutions to ensure they can support the velocity and volume of digital certificates they require.

There are several compelling events driving government organisations to focus on PKI as a core project, which include:

End of support

PKI hardware components and software, such as Active Directory Certificate Services, often reach end of support or end of life (EOL) within 5 to 8 years. For instance PKI deployments running on Microsoft Server 2016 must be migrated to a new version no later than the end of extended support in 2027.

CA expiration

Certificate Authority (CA) expiration is a critical component of PKI best practice. As outlined by the NCSC, a CA lifespan should be as short as reasonably practical. Central government organisations require between 12-24 months to migrate when an Issuing CA or Root CA expires.

Skills shortage

It's no secret that there is a major skills shortage in cybersecurity, with the UK government citing that 50% of businesses have a basic cyber skills gap. PKI is fundamental security infrastructure, but specialized skills are difficult to find and retain.

Cloud migration

In accordance with the Government Cloud First policy, when procuring new or existing services, public sector organisations should default to Public Cloud first. It is strongly recommended to adopt a highly resilient and flexible PKI solution capable of supporting cloud-based workloads and services.

The risks and challenges of mismanaged PKI:

- Unknown and untracked certificates expire unexpectedly and lead to disruptive service outages
- Misconfiguration and excessive privileges result in significant vulnerabilities to critical infrastructure
- Legacy PKI solutions cannot support modern protocols, architecture, and automation required for cloud migration
- Staff shortages and employee churn increase the risk of PKI misconfiguration and audit failures
- Quantum computing will break classic algorithms and protocols that existing PKI deployments are built upon

Growing pains

Government organisations have adopted strategic initiatives, such as DevOps and IoT devices, that demand short-lived certificates at high volume. PKI must be able to scale and meet these requirements with lifecycle automation to enable application teams to move quickly, without compromise to security.

Security risk

Legacy PKI deployments are no longer fit for purpose to meet today's security and regulatory requirements, often lacking modern security design principles and highly susceptible to misconfiguration. This leaves government organisations vulnerable to disruptive outages and audit failures.

Shorter lifespans

The lifespan of digital certificates has decreased over time, putting increased workload on teams responsible for managing them, and rendering manual certificate management practices obsolete. While shorter lifespans improve security and reduce the impact of private key compromise, automation is required to keep pace.

Crypto-agility

Vulnerabilities arise, algorithms evolve, and with the advent of quantum computing, government organisations must proactively prepare for the transition to post-quantum cryptography, which will require a complete overhaul of PKI infrastructure to modern solutions that can support resilient algorithm, and easily adapt to future changes.

Keyfactor for UK Central Government Organisations

The era of digital government is here. The shift to cloud computing and the changing security landscape present big challenges and opportunities. Every government organisation must invest in mission-critical security infrastructure — including PKI — to operate in todays connected world.

Keyfactor helps central government organisations build the foundation of digital trust necessary to advance cyber resilience while enhancing digital experiences. Trusted by more than 1,500+ leading organisations and government institutions, Keyfactor provides a complete solution stack from certificate issuance (PKI) and lifecycle automation to digital signing and quantum-resilient cryptography.

As organisations continue to phase out legacy PKI systems and software, such as Active Directory Certificate Services (ADCS) and Entrust Certificate Services, Keyfactor works with government organisations to successfully migrate and modernize their PKI, alongside ecosystem partners that provide SC & DV cleared resources to support professional services and architect resource requirements.

Keyfactor's product suite aligns with strategic government mandates, such as the Cyber Assessment Framework, and holds certifications required by third parties to work with government organisations, such as ISO 27001, and is working towards alignment to the GCloud 14 Framework and tScheme approval to better support the needs of procurement and security teams.

Why Keyfactor

- → Modernize PKI infrastructure to enable cloud-first and Zero Trust initiatives
- → Deploy your PKI as a turnkey hardware or software appliance, in the cloud, or as a service with secure facilities and regional availability within the UK
- → Ensure your PKI is designed to best practice with the deepest bench of PKI and cryptography expertise in the industry
- → Reduce the risk of outages, security incidents, and audit failures with full visibility and control of digital certificates
- → Align with industry standard certifications, including Common Criteria, ISO 27001, and PCI DSS

Modern and flexible PKI

Powered by the most trusted and widely used open source-based PKI in the world, EJBCA Enterprise enables government organisations to establish trust in every human and machine with an identity-first approach. With EJBCA Enterprise, you have the flexibility to run in the cloud or on-prem, self-managed or as a service. It is a complete turnkey PKI platform, pre-packaged with all the components, protocols, and software you need to get up and running, and scale seamlessly.

Keyfactor EJBCA

Learn more ↗

Certificate lifecycle automation

Keyfactor Command is a certificate lifecycle management and automation solution that delivers complete visibility of all digital certificates across even the most complex environments. The solution enables teams to prevent disruptive outages and avoid unexpected audit failures with the ability to discover, manage, and automate the lifecycle of certificates, all from one centralized console. Keyfactor Command is CA and platform-agnostic, integrating with all major HSMs, identity providers, public and private CAs.

Keyfactor Command

Learn more ↗

Secure digital signing

Keyfactor Signing Solutions protect the integrity and authenticity of code, software, and digital content – from e-passports and electronic IDs to sensitive legal and government documents. Our solutions are trusted by government organisations globally and designed to maximize the operational productivity, while protecting sensitive keys and safeguarding access to critical signing processes.

Keyfactor Signum

Learn more ↗

KEYFACTOR

Keyfactor brings digital trust to the hyper-connected world with identity-first security for every machine and human. By simplifying PKI, automating certificate lifecycle management, and securing every device, workload, and thing, Keyfactor helps organizations move fast to establish digital trust at scale — and then maintain it. In a zero-trust world, every machine needs an identity and every identity must be managed.

For more, visit keyfactor.com or follow @keyfactor.

Contact us

- www.keyfactor.com
- +1 216 785 2946 (North America)
- +46 8 735 61 01 (Europe)