Prepare for the Digital Operational Resilience Act (DORA) with Keyfactor

If you operate in the financial sector in the European Union, DORA entered into force on the 16th of January 2023, and will apply as of 17th of January 2025, with significant fines for noncompliance. See how Keyfactor enables your organization to stay compliant, secure, and resilient.

Achieving DORA Compliance with Keyfactor

The Digital Operational Resilience Act (DORA) is a regulation in force for organizations operating in the financial sector in the European Union aimed at ensuring operational resilience. Achieving DORA compliance is a comprehensive and multifaceted process. It involves assessing and mitigating operational risks, ensuring IT and security resilience, and complying with various regulatory obligations.

Keyfactor has a proven record and technologies that are essential to achieving DORA compliance. Working with over 1,500 enterprises globally, including many in the financial sector, and with 5 EU offices, Keyfactor has local representatives and in-region partners to assist. Keyfactor's solutions offer a true one-stop-shop for PKI, signing, and certificate management, while also making it easy to integrate into an existing technology stack.

Keyfactor offers flexibility of deployments from SaaS and cloud-hosted to on-premise or hybrid deployments for PKI, certificate lifecycle management, and signing. Organizations can also simplify complexity and reduce internal overhead even further with PKI as a Service , combining expert-run PKI with powerful certificate lifecycle automation in a single cloud platform.

Additional measures will be necessary to meet and maintain compliance with DORA, including people, process, and technology. No single vendor can provide complete DORA coverage as the legislation covers a wide array of both technology and organizational requirements. However, PKI and certificate management are key components of the regulation, and organizations must ensure they have robust processes and solutions in place.

Keyfactor solutions:

Quantum-ready PKI

Keyfactor's EJBCA platform offers a robust PKI program that offers extensive integration and powerful automation capabilities. Ensure your sensitive assets remain protected and resilient.

Certificate Lifecycle Management

Keyfactor's Command offers end-to-end certificate lifecycle management providing real-time discovery, automated renewals, and protection controls.

Secure Signing

Protect the integrity of documents, code, containers, and software identified from your ICT risk assessment with Keyfactor's Signum.

PKI as a Service

With PKIaaS, Keyfactor becomes a true one-stop shop for PKI. It combines expert-run PKI with powerful certificate lifecycle automation in a single cloud platform.

5 Key DORA Regulations and How to Approach Compliance

When it comes to PKI, certificates, keys, and signing, DORA establishes a high threshold of required controls and capabilities for compliance. With Keyfactor's longstanding expertise and experience with PKI, we can ensure your organization has the right solutions and processes in place for PKI. Section 4, Article 7 of DORA specifies what is required for cryptographic key management:

DORA Regulation Criteria	How to Approach Compliance
Financial entities shall include in the cryptographic key management policy referred to in Article 6(2), point (d), requirements for managing cryptographic keys through their whole lifecycle, including generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking, and destroying those cryptographic keys.	Having a properly set up PKI from key generation to retirement requires a PKI platform with flexibility to run as needed by your organization — in the cloud, on-prem, self-managed, or as a service. Keyfactor has years of experience implementing complex PKI deployments. Our team of experts helps set up the correct components, protocols, and software for all your organization's use cases to securely manage both internal and publicly trusted digital certificates throughout their lifecycle.
Financial entities shall identify and implement controls to protect cryptographic keys through their whole lifecycle against loss, unauthorised access, disclosure, and modification. Financial entities shall design those controls on the basis of the results of the approved data classification and the ICT risk assessment.	Centrally managing users as well as CA, SSH, and other keys is critical to security. Essential capabilities should include automating alerts for key rotation, enforcing role-based user permissions, and automating provisioning workflows. To demonstrate compliance, software should be able to produce audit log and reports on all lifecycle events. Organizations should consider signing solutions for code, documents, and other sensitive assets from the ICT risk assessment.
Financial entities shall develop and implement methods to replace the cryptographic keys in the case of loss, or where those keys are compromised or damaged.	It's important to replace existing keys and certificates that have reached end of life or have been compromised. Software should be able to generate new keys and replace old ones. Having an automated key and certificate rotation program in place reduces the likelihood of compromised keys being able to access remote servers.
Financial entities shall create and maintain a register for all certificates and certificate-storing devices for at least ICT assets supporting critical or important functions. Financial entities shall keep that register up to date.	Organizations need to discover all potential unknown certificates and keys. Look for solutions offering real-time visibility into public and private CAs, network endpoints, and key and certificate stores. Administrators should be able to view certificates from a single dashboard and move away from manual or siloed approaches that could leave blind spots or become out-of-date.
Financial entities shall ensure the prompt renewal of certificates in advance of their expiration.	Certificate lifecycle management should include automated certificate renewal. Organizations should look for solutions that can automate certificate renewal, provisioning, and installation with minimal ongoing effort to reduce the likelihood of outages, misconfigurations, or expiration.

Did you know? Keyfactor's PKIaaS makes it easy to scale your PKI and ensure resilience in the cloud with a true all-in-one solution to everything PKI.

Quantum-ready PKI

Ensuring the security of keys throughout their lifecycle starts with a trusted certificate authority (CA) and PKI platform, EJBCA Enterprise. Powered by the most trusted and widely used open-source PKI, EJBCA is fast to deploy, offers flexible deployment options, scales on-demand, and supports any use case.

Keyfactor EJBCA

Learn more ↗

End-to-end visibility and automation

Getting an accurate register starts with visibility. Establish an enterprise-wide inventory of all certificate authorities (CAs) and machine identities with Keyfactor Command. Easily take back control of your certificates and keys with automated workflows to reduce the likelihood of outages, misconfigurations, or expirations.

Keyfactor Command

Learn more ↗

Secure Signing

Protect the integrity of documents, code, containers, and software identified from your ICT risk assessment with secure signing as a service. Keyfactor Signum protects sensitive keys & documents, automates policy, and integrates with your native tools and build pipeline.

Keyfactor Signum

Learn more ↗

One-Stop PKI Solution

Keyfactor PKI as a Service combines a fully-managed PKI service and certificate lifecycle automation into a single, cloud-delivered platform. It's your PKI, built and operated by experts, to reduce your operational burden, improve efficiency, and provide unmatched security and compliance for regulations like DORA.

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)