emudhra
Trust Delivered

Futureproofing Cybersecurity with emCA

PKI FOR ANY USE CASE:

- Migrate from legacy CAs to a modern multi-tenant, high performance flexible enterprise PKI
- Automate PKI deployment and certificate issuance for DevOps and microservices
- Issue trusted identities for IoT devices and connected manufacturing environments
- Enable secure government-issued and verified ePassports
- Enable EMV based PKI for payment card industry including central/retail banks

emCA is a robust certificate authority (CA) solution that is quick to implement, capable of scaling as needed, and adaptable to any application scenario.

In a landscape where every node is connected yet trust is scarce, public key infrastructure (PKI) stands out as a tested digital identity solution, enabling safe, encrypted, and verified connections for each user, device, and workload. However, the complexity and outdated nature of many PKI systems, which necessitate advanced expertise and struggle to scale with contemporary use cases, have made managing PKI a challenging task.

emCA transforms the way organizations handle PKI operations, offering a streamlined process for issuing, managing, and maintaining digital certificates, even at a vast scale. Built on open-source principles and platforms, emCA has earned its place as the most extensively used and trusted CA software in many uses case globally.

emCA has changed the game:

Allowing you to operate multiple PKI hierarchies on a single platform, centralize the configuration and administration of certificate policies, and access detailed (and if required, signed) audit and transaction logs from one centralized location. Furthermore, configuring CAs and certificate templates becomes a straightforward task, eliminating the need for administrators to be PKI specialists.

KEY BENEFITS:

- Protect critical systems and data and support zero-trust architecture with PKI-based identity
- Enable developers and IT admins to move faster with sub-second certificate issuance
- Meet stringent security and compliance requirements with a best practice and trusted PKI
- Solution scalable in both horizontal and vertical infrastructures

KEY FEATURES:

- A unified PKI platform that accommodates multiple Certificate Authorities (CAs), Validation Authorities (VAs), and Registration Authorities (RAs) concurrently
- Exhibits superior scalability, capable of handling vast deployments via database-tier clustering and High Availability (HA) setups
- Presents flexible deployment options such as PKI as a software, container, cloud instance, or managed services
- Certificate lifecycle management is automated through the CLM platform, emDiscovery
- Seamless integration capability with Active Directory (AD) and Azure AD, Kubernetes, among others
- Provides trusted and compliance-ready solutions, validated by Common Criteria, and already operational in WebTrust and ETSI/eIDAS compliant environments

Launch swiftly — operate universally

Every organization is faced with distinct operational obstacles, encompassing security necessities, budget constraints, and available IT assets. emCA is a platform agnostic application that works seamlessly on any operating system, application servers and database. It is a modular application that can be effortlessly deployed on complex environments.

Safeguard every machine and workload

The evolution of containerization, DevOps, IoT devices, and remote work has inflated the number of devices and users that an internal PKI must secure. To that end, emCA integrates seamlessly with a host of third-party applications and systems, broadening your PKI to adapt to emerging use cases. This is achieved through support for commonly adopted protocols and several pre-configured plugins spanning various platforms and applications.

Supported technologies

Certificate formats and standards:

- RFC5280 compliant X.509 certificates and CRLs
- PKCS#10, CRMF and SPKAC certificate requests
- PKCS#12, JKS, PEM and PKCS#11 keystores
- EN 319 412 eIDAS compliant certificates
- OCSP compliant with RFC6960 and RFC5019
- ICAO 9303, EAC 1.11 and EAC 2.10 ePassport and eID
- RFC6962 compliant Certificate Transparency

Protocols:

- ACME, CMP, EST, and SCEP enrollment/management protocols
- Rest / SOAP API
- Web Services

Hardware security modules (HSMs):

- Thales Luna, Entrust nShield, Utimaco, AWS CloudHSM, Azure Key Vault Managed HSM, Fortanix, and other PKCS#11-compliant modules

Cryptography:

- RSA, ECDSA and EdDSA keys, CVC, EMV compliant