



primeID CERTIFY

The foundation for certified security

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
- Scalability for large-scale deployments through database-tier clustering and HA configurations
- Seamless integration with Active Directory, Azure AD, Kubernetes, primeID AUTOMATE, VALIDATE, Intercede MyID and other systems

primeID CERTIFY CHANGES THE GAME

It allows 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.

primeID CERTIFY 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 proven digital identity solution, enabling secure, 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 However, the complexity and outdated nature of many PKI systems, which necessitate advanced expertise and struggle to scale with contemporary use cases, have made managing PKI a challenging task.

primeID CERTIFY transforms the way organizations handle PKI operations, offering a streamlined process for issuing, managing, and maintaining digital certificates, even at a large scale. Built on open-source principles and platforms, **primeID CERTIFY** is a trusted PKI platform used worldwide across a wide range of use cases.

PUBLIC



we establish trust.

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 proven, 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 large deployments via database-tier clustering and High Availability (HA) setups
- Presents flexible deployment options such as PKI as software, container, cloud instance, or managed service
- Certificate lifecycle management is automated through the CLM platform primeID AUTOMATE
- Seamless integration capability with Active Directory (AD) and Azure AD, Kubernetes, and many more
- Provides trusted and compliance-ready solution, Common Criteria certified, and already operational in WebTrust and ETSI/eIDAS compliant environments

LAUNCH SWIFTLY — OPERATE UNIVERSALLY

Every organization is faced with distinct operational obstacles, encompassing security requirements, budget constraints, and available IT resources. **primeID CERTIFY** 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 in complex environments.

PUBLIC

CRYPTAS International GmbH
Franzosengraben 8 · 1030 Wien · Austria
+43 (1) 3 555 3-0 · info@cryptas.com

SAFEGUARD EVERY MACHINE AND WORKLOAD

The evolution of containerization, DevOps, IoT devices, and remote work has increased the number of devices and users that an internal PKI must secure. To that end, primeID CERTIFY integrates with a lot 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

- RFC 5280 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 RFC 6960 and RFC 5019
- ICAO 9303, EAC 1.11 and EAC 2.10 ePassport and eID
- RFC 6962 compliant Certificate Transparency

Protocols

- ACME, CMP, EST, and SCEP enrollment/management protocols
- REST 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
- **PQC:**
 - FIPS 203, ML-KEM, based on CRYSTALS-Kyber
 - FIPS 204, ML-DSA, based on CRYSTALS-Dilithium
 - FIPS 205, SLH-DSA, based on SPHINCS+
 - Coming soon:
 - FIPS 206, FN-DSA, based on FALCON

10/2026

cryptas.com
Vienna | Graz | Düsseldorf | Hengelo | Stockholm