cryptas

we establish trust.

Trust, but validate.

primeID VALIDATE

VALIDATE DIGITAL CERTIFICATES
IN REAL-TIME.

Lost or stolen laptops, mobile phones, or smart cards pose a high-security risk for companies, as cryptographic keys on these devices can lead to misuse. To prevent misuse, it must be possible to validate digital certificates in real-time, and revocation should be as fast as possible. However, the increasing number of web applications and secure communication channels in companies make the real-time validation of certificates challenging. primeid VALIDATE offers a secure and scalable high-performance solution to request revocation information in real-time.

VALIDATION OF X.509 CORPORATE CERTIFICATES

Revocation information must be available for every X.509 certificate. primeid VALIDATE is a simple, efficient, and secure solution to request revocation information in real-time.

REVOCATION OF COMPROMISED KEYS

If keys have been compromised, the corresponding certificate must be revoked as soon as possible. primeid VALIDATE offers a solution to prevent the further use of lost or stolen certificates and keys.

To guarantee maximum security, revocation information for digital certificates must be retrievable in real-time. Authentication and signature processes, for example, require assurance of the validity of underlying certificates at any time and without significant delay. Here, direct integration of different certification authorities, as well as a scalable solution design, are often seen as key.

OUR SOLUTION

primeid VALIDATE offers a secure, robust, and scalable solution to retrieve revocation information of digital certificates in real-time. Certificate status changes are immediately and in real-time transmitted to the primeid VALIDATE Server. All corporation-relevant certificates are also backed up on this server, ensuring disaster recovery and business continuity. Relevant cryptographic keys are stored in hardware security modules (HSMs), providing the highest security and transaction rates of >950 requests per second per node. The primeid VALIDATE Proxy enables advanced network zone architecture as well as the pre-validation of request and caching mechanisms.

PUBLIC

06/2024

cryptas

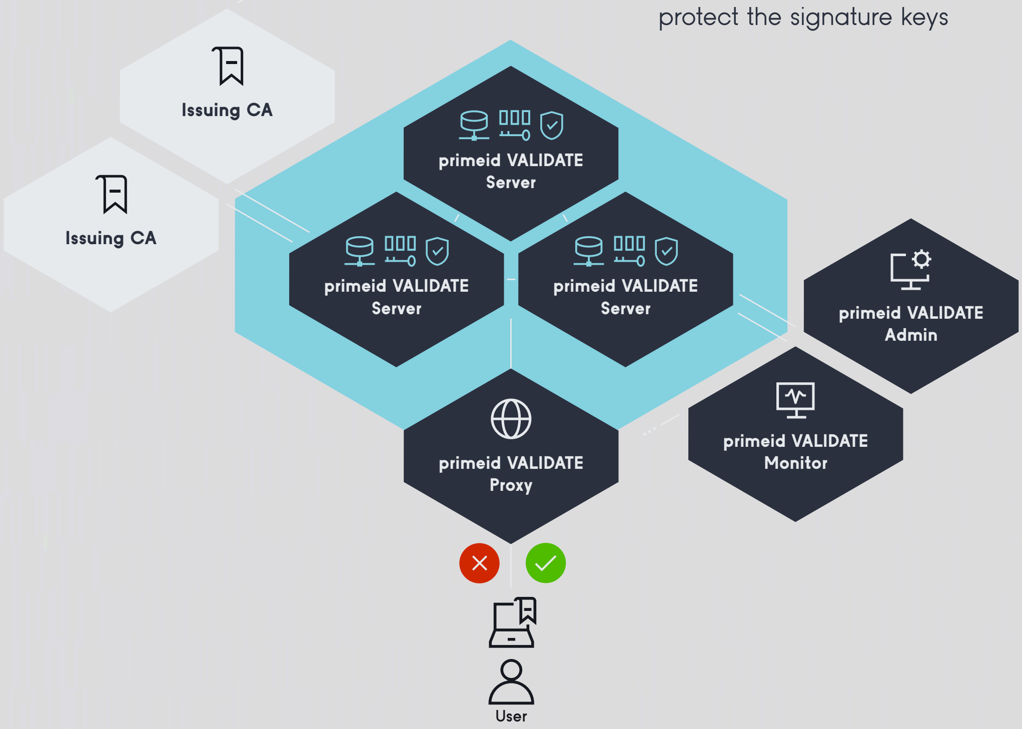
we establish trust.

BENEFITS

- Retrieval of revocation information in real-time
- Cluster operation with data replication on every node
- Load balancing and scalability
- Appliance solution for easy installation and extensibility
- Available as a physical appliance
- primeid VALIDATE Admin to manage nodes, configuration, and certificates
- primeid VALIDATE Monitor for statistical analysis (load, usage of certificates, etc.)
- Connectivity to external monitoring systems (e.g. SNMP)
- Detailed logging, enabling individual reporting and analysis (external tool support)
- Toolset for easy migration and initial import at the initial operation
- primeid VALIDATE Proxy for pre-validation of requests and establishing network zone separation

FEATURES

- OCSP protocol specification RFC-6960
- Lightweight OCSP protocol for High-Volume Environments (RFC-5019)
- primeid VALIDATE Proxy
- primeid VALIDATE Admin with Web UI
- primeid VALIDATE Monitor with Web UI and health und metrics endpoints
- Multi-CA support
- Response signing with HSM, PKCS#11 Library, keystore
- SNMP notifications
- Certificate Management API for certification authority integration
- Support of different Cas (e.g. Microsoft CA with ExitModule)
- Cluster support
- High performance starting at 950 requests per second per node
- Physical CRYPTAS Secure Hardware Appliance (19", 1U, redundant power supply, 2x GbE RJ45) with a hardware security module (HSM) to protect the signature keys



PUBLIC

06/2024

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

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