cryptas

we establish trust.

Trust, but validate.

primeID VALIDATE

ÜBERPRÜFUNG DER GÜLTIGKEIT
VON DIGITALEN ZERTIFIKATEN IN ECHTZEIT.

Digitale Zertifikate auf Laptops, Handys oder Smart Cards stellen bei Verlust oder Diebstahl ein hohes Sicherheitsrisiko für Unternehmen dar. Um Missbrauch von Zertifikaten zu verhindern, muss deren Gültigkeit in Echtzeit abgerufen und diese bei Bedarf schnellstmöglich widerrufen werden können. Eine Zunahme an gesicherten Webanwendungen und Kommunikationswegen in Unternehmen lassen dies jedoch schnell zur Herausforderung werden. primeid VALIDATE ist eine zuverlässige, sichere und skalierbare Lösung, um Sperrinformationen und Statusänderungen von Zertifikaten lückenlos und in Echtzeit abzufragen.

PRÜFUNG VON X.509 ZERTIFIKATEN IN UNTERNEHMEN

Für gewöhnlich müssen für jedes ausgestellte X.509 Zertifikat Sperrinformationen verfügbar sein. primeid VALIDATE ist eine einfache, effiziente und sichere Lösung, um entsprechende Sperrinformationen sofort und in Echtzeit abzufragen.

WIDERRUFEN VON SCHLÜSSELMATERIAL

Um Zertifikate vor Missbrauch zu schützen, ist verlorenes oder gestohlenes Schlüsselmaterial schnellstmöglich zu widerrufen. Mit primeid VALIDATE kann eine weitere Verwendung von verlorenen und gestohlenen Schlüsselmaterial schnell und einfach unterbunden werden.

Um ein Höchstmaß an Sicherheit zu garantieren, müssen Sperrinformationen zu digitalen Zertifikaten in Echtzeit abgerufen werden können. Authentifizierungs- oder Signaturvorgänge beispielsweise verlangen eine Sicherstellung der Gültigkeit von zugrundeliegenden Zertifikaten zu jeder Zeit und ohne für NutzerInnen spürbare Verzögerungen. Eine direkte Anbindung unterschiedlicher Certification Authorities sowie ein skalierbares Lösungsdesign werden hier oft als entscheidend angesehen.

UNSERE LÖSUNG

primeid VALIDATE ist eine zuverlässige, sichere und skalierbare Lösung, um Sperrinformationen von digitalen Zertifikaten in Echtzeit abzufragen. Am primeid VALIDATE Server werden Statusänderungen von Zertifikaten sofort und in Echtzeit hinterlegt und alle unternehmensrelevanten Zertifikate gesichert. Dies gewährleistet eine Betriebsfortführung und Wiederherstellung im Desaster-Fall. Relevantes Schlüsselmaterial wird sicher in Hardware Security Modulen (HSMs) gespeichert, die ein Höchstmaß an Sicherheit garantieren und einen Durchsatz von >950 signierten Antworten pro Sekunde pro Node erlauben. Zusätzlich ermöglicht der primeid VALIDATE Proxy eine Zonentrennung und Vorvalidierung von Requests sowie Caching-Mechanismen.

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

cryptas

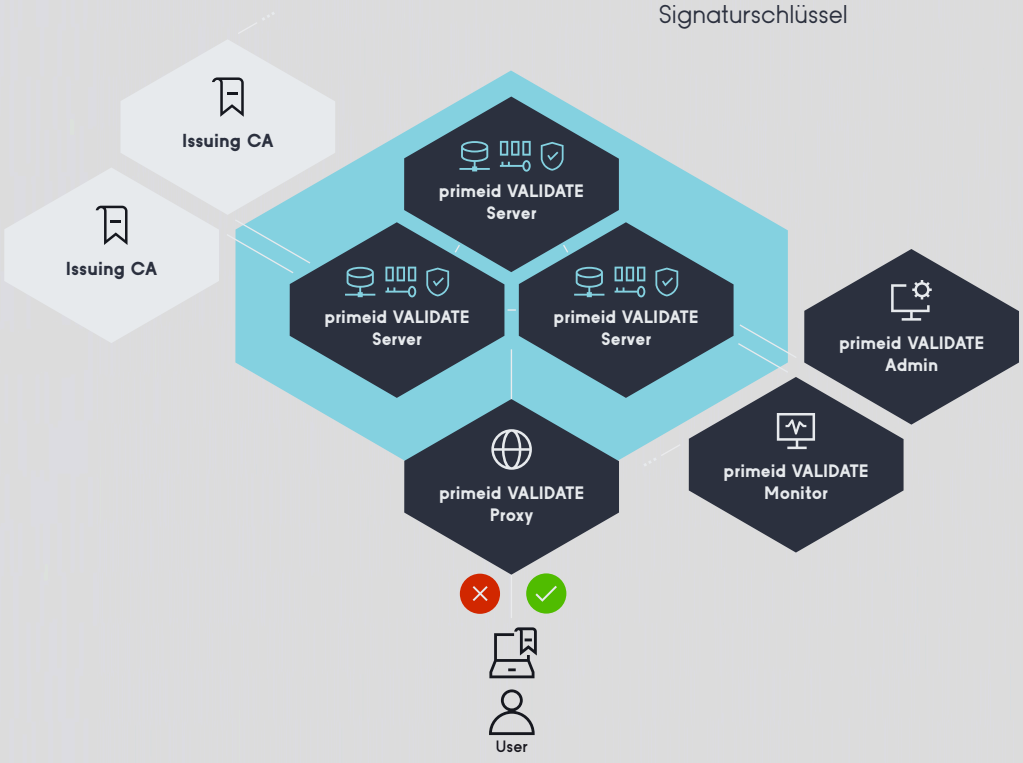
we establish trust.

VORTEILE

- Abruf von Sperrinformationen in Echtzeit
- Clusterbetrieb mit replizierter Datenhaltung auf jedem Node
- Lastverteilung und Skalierung
- Appliance-Lösung für einfache Installation und Erweiterbarkeit
- Physische Appliance
- primeid VALIDATE Admin zur Übersicht und Konfiguration aller Nodes und Zertifikate
- primeid VALIDATE Monitor für statistische Auswertungen (Auslastung, Zertifikatsverwendung, etc.)
- Diverse Anbindungsmöglichkeiten an externes Monitoring (SNMP, etc.)
- Logging-Tools für detaillierte, individuelle Auswertung und Analyse
- Toolset für eine einfache Migration und initialem Import bei Inbetriebnahme
- primeid VALIDATE Proxy für die Vorvalidierung von Requests und eine sicherheitsrelevante Zonentrennung

FEATURES

- OSCP-Protokoll nach RFC-6960
- Lightweight-OCSP-Profil für High-Volume-Umgebungen (RFC-5019)
- primeid VALIDATE Proxy
- primeid VALIDATE Admin Web GUI
- primeid VALIDATE Monitor Web GUI mit Health und Metrics Endpoints
- Response Signing mit HSM, PKCS#11 Library, Keystore
- SNMP Notifications
- Zertifikats-Management API für CA-Integration
- Unterstützung unterschiedlicher Cas (z.B. Microsoft CA mit ExitModule)
- Cluster Unterstützung
- Hohe Performance ab 950 signierten Antworten pro Sekunde pro Node
- Physische CRYPTAS Secure Hardware Appliance (19", 1U, redundant power supply, 2x GbE RJ45) mit Hardware Security Module (HSM) zum Schutz und Anwendung der Signaturschlüssel



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