Sign Live! CC validation server

Produktbeschreibung

Sign Live! CC validation server

- Kontinuierliche Massenvalidierung mit sehr hohem Durchsatz (bis zu 17.000 Validierungen pro Stunde)
- Administration über eine komfortable und intuitiv zu bedienende Benutzeroberfläche
- Fortgeschrittene und qualifizierte elektronische PDF(/A)-Signatur, PKCS#7- und XMLDSig-Signatur
- Prüfprotokoll als HTML, PDF/A oder XML gemäß OASIS DSS1.0
- Integrierte Zertifikats- und Sperrlistenverwaltung
- Prüfung von PDF-Dateien oder sonstige Dateien auf Veränderung und Zertifikatsvalidierung (OCSP, Sperrliste)
- Basiert auf bewährter und sicherheitsbestätigter Sign Live! CC Technologie
- Anzeige der Detailinformationen eines Zertifikats/Zeitstempels
- Umfangreiche Scripting- und Reportfunktionen
- Proxy-Unterstützung
- Hohe Sicherheit durch Installationsprüfroutine / Trusted Mode
- Erfüllt die Anforderungen nach SigG/SigV und der EG-Signaturrichtlinie

Zuverlässige und vielseitig einsetzbare Signaturvalidierung

Bei Erhalt von elektronisch signierten Dateien werden alle Signaturen und somit die Unterzeichner sowie die Integrität des unterzeichneten Inhalts geprüft. Abhängig von der Konfiguration des *Sign Live! CC validation server*s kann dies vollautomatisch ablaufen. Die Gültigkeitsprüfung der Signatur erfolgt durch Echtheitsprüfung des Zertifikatsstatus der digitalen ID des Unterzeichners und der Integritätsprüfung der Datei. Die Echtheitsprüfung bestätigt, dass das Zertifikat des Unterzeichners oder das entsprechend übergeordnete Zertifikat in der Liste vertrauenswürdiger Identitäten des Prüfenden vorhanden ist. Ferner wird geprüft, ob das Unterschriftszertifikat gültig ist. Mit der Prüfung der Dokumentintegrität wird kontrolliert, ob der unterschriebene Inhalt nach der Unterschrift geändert wurde. Bei Inhaltsänderungen wird bei Prüfung der Dokumentintegrität kontrolliert, ob die Inhaltsänderung vom Unterzeichner genehmigt wurde.

Mit *Sign Live! CC validation server* sind alle gängigen standardkonformen Signaturformate und Zeitstempel automatisiert verifizierbar. Geprüft werden können auch Signaturen, die in PDF-Dokumenten enthalten sind - sogenannte PDF-inline-Signaturen. Bei Bedarf kann eine GDPdU-konforme Prüfdokumentation im HTML-, PDF/A- oder XML-Format erzeugt werden.

Die Signaturverifikation erfolgt automatisch auf Basis von Sperrlisten (CRL). Über die Sperrlistenaktualisierung können stets aktuelle Sperrlisten aus dem Internet herunter geladen werden. Zusätzlich ist die Verwendung des OCSP Protokolls möglich, um Informationen zur Gültigkeit des Signaturzertifikates einzuholen. Die Signaturprüfung erfolgt im ersten Schritt immer nach dem Schalenmodell und im zweiten Schritt nach dem Kettenmodell, sofern es sich um ein qualifiziertes Zertifikat handelt. Das Produkt kann Signaturen verifizieren, die mit den bereits aufgezählten Algorithmen erzeugt wurden. Die Konfiguration von Sperrlistendownload, OCSP Abfragen und LDAP Verzeichnisdiensten ist über Konfigurationsdateien möglich. OCSP-Anfragen können individuell konfigurierbar zur Durchsatzoptimierung kurzfristig im Cache abgelegt werden.

Sign Live! CC validation server

Detaillierte Signaturvalidierung und Zeitstempelprüfung

Zentrale Verwaltung öffentlicher Zertifikats-sperrlisten

Falls erforderlich, kann *Sign Live! CC* durch einfache Konfiguration als Sperrlistenserver eingesetzt werden und für alle Arbeitsplätze im LAN automatisch die gültigen Sperrlisten akkreditierter sowie angezeigter Trustcenter sicher und schnell zur Verfügung stellen. Dies erfolgt unabhängig vom Erzeuger oder der Art der erzeugten Signatur.

Allen Arbeitsplätzen hinter dem Proxy oder der Firewall der Organisation stehen die notwendigen Sperrlisten einfach und effizient ohne den jeweiligen Aufbau einer Verbindung via Internet zum ZDA zwecks Prüfung einer signierten Datei zur Verfügung.

Dadurch ist eine massive Steigerung der Verifikationsleistung im Unternehmen möglich und auch eine Entlastung der Internet-Zugänge für die Online-Abfragen der internen Arbeitsplätze.

Erweiterbarkeit

Sollte die reine Validierung von Signaturen zukünftig nicht mehr ausreichend sein, können dank der offenen Schnittstellen und der flexiblen Komponentenarchitektur des *Sign Live! CC validation servers* schnell und einfach Erweiterungen angeschlossen werden. Damit können intelligente Zusatzfunktionen wie die Extraktion von Rechnungs- und Indexdaten, PDF/A-Prüfung und ggf. –Konvertierung, Stempeln von PDF-Dokumenten sowie die Anbindung an elektronische Archive realisiert werden

Skalierbarer Server und flexible Architektur

Sign Live! CC validation server kombiniert Flexibilität und Funktionalität skalierbar und sicher. Auch verteilte Serverumgebungen, die einen reibungslosen Betrieb mit Hochverfügbarkeit durch Load-Balancing in geschäftskritischen Systemen sichern, werden unterstützt.

- Als Plugin-Lösung einfach in jeden bestehenden Webdienst einzubinden
- Online API für high level integration mit Webanwendungen
- Web Services/SOAP Schnittstellen und Java API

Integration

- Konfigurierbare Dateisystemüberwachung mit mehreren Verzeichnisebenen
- Synchronisieren via Markierungsdatei oder Änderungsüberwachung der zu prüfenden Datei
- Nicht zu prüfende Dateien verschieben
- Kollisionsbehandlung
- Kommandozeilenaufruf, ActiveX, SOAP, HTTP, XMLRPC, JDBC, P9100, TN3270, Integration in Tomcat
- Betrieb mit/ohne Benutzeroberfläche im Hintergrund, z.B. als Windows Dienst, Linux Service

Unterstützte Standards:

- X.509v3 – Zertifikats- und CRL-Format
- RSA – Asymmetrische Verschlüsselung
- MD5 und SHA1 – Hash Algorithmen
- PKCS#1 – RSA Verschlüsselung
- PKCS#7 – für Signaturen
- PKCS#12 – für Speicherung der Schlüssel
- CAdES/XAdES – für erweiterte Signaturen
- CBT XMLDigSig – für Signaturen
- OCSP – für Zertifikats-Statusprüfung
- OSIF – Standard-Identifizierungs-Funktion
- LDAP – für den Zugang zu Zertifikatssperrlisten öffentlicher Verzeichnisse und der Firmenverzeichnisse.

Systemvoraussetzungen

- Hardware
  - Prozessor: Intel/AMD mit mind. 2,0 GHz
  - Arbeitsspeicher: mind. 2/4 GB
  - Festplattenspeicher: mind. 150 MB für die Installation
- Betriebssysteme
  - Windows 7 (32/64Bit), Windows Server 2003, 2008, Mac OS X, verschiedene Linux Distributionen
- Java
  - Java Runtime Environment (JRE) Version 6
- Lizenzierung
  - Pro Server/CPU/Institut-Durchsatzanforderung

Weitere Informationen:
www.intarsys.de
info@intarsys.de
+49 721 38479 0
Folgen Sie nebenstehendem QR-Code