Sign Live! CC certificate manager

Produktbeschreibung

Sign Live! CC certificate manager

- Unternehmensweite Zertifikatsverwaltung
- Erstellung und Import von X.509v3-Zertifikaten
- Verwaltung von Zertifikaten
- Schnittstelle zu Fremdanwendungen wie Signtrust CERT
- Verwaltung von Root-CA und Sub-CA Zertifikaten
- Vollständige Unterstützung des Lifecycles von Antrag über Bearbeitung, Ausstellung, Folgezertifikaten und Sperrung
- Zertifikatsverteilung per E-Mail oder USB-Stick
- Versenden der Transport-Passworte per E-Mail
- Generierung und Import von Sperrlisten
- Darstellung der Detailinformationen von Zertifikaten
- Nutzung von Zertifikaten aus dem Windows-Zertifikatsspeicher
- Basiert auf bewährter, sicherheitsbestätigter Sign Live! CC Technologie

Verwaltung und Erstellung von X.509v3-Zertifikaten

Vertraulichkeit, Integrität und Authentizität von Dokumenten, Daten und Kommunikationsinhalten gewinnen im Zusammenhang mit dem Thema "Sicherheit im Internet" zunehmend an Bedeutung. Doch wie erreicht man ein Höchstmaß an Sicherheit, um sich vor den Gefahren im Internet wirkungsvoll zu schützen?

Fragen der Übertragungssicherheit und der Rechtssicherheit von Dokumenten werden normalerweise durch amtliche Ausweise und Unterschriften gelöst. Das Problem ist nun, wie man diese Konzepte auf das Internet übertragen kann. Eine praktikable und langjährig erprobte Lösung dafür sind zertifikatsbasierte PKI (Public Key Infrastructure) -Systeme.

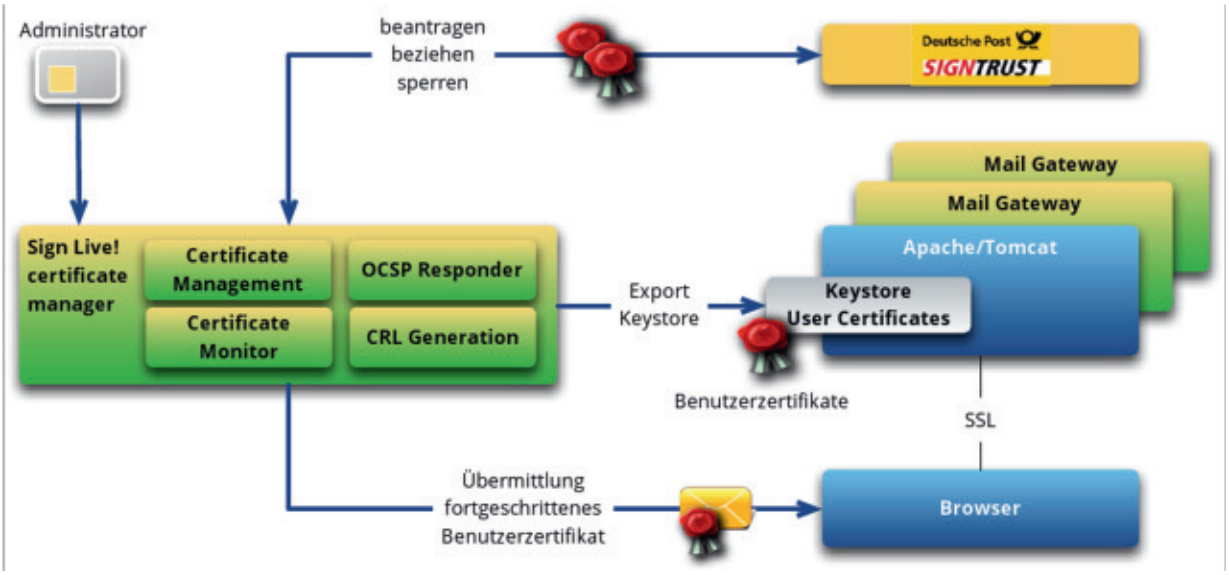
Das Zertifikat

Ein Zertifikat nach dem X.509-Standard funktioniert dabei wie ein amtlicher Ausweis, der ein Attribut oder eine Identität mit einer Person verbindet. Mit X.509-Zertifikaten können Sie Ihre IT-Infrastrukturen standardkonform, effizient und preiswert absichern. Die Technologie kann sowohl zur Absicherungen der Kommunikation im LAN und Intranet als auch im Internet verwendet werden. Eine vertrauliche Kommunikation mit Geschäftspartnern und Kunden ist damit jederzeit und ohne große Eingriffe in die bestehende Infrastruktur möglich.

Sign Live! CC certificate manager unterstützt Sie beim gesamten Prozess der Zertifikatsverwaltung. Dies beginnt bei der Erstellung von X.509v3 Zertifikaten speziell für die Mitarbeiter Ihres Unternehmens bis hin zu externen Partner wie Lieferanten und Kunden. Die damit erstellten Zertifikate können von den Benutzern u.a. in Webbrowsern, VPN-Clients und E-Mailprogrammen problemlos verwendet werden.

Sign Live! CC certificate manager

Verwaltung von X.509 Zertifikaten



Plattformübergreifend

Sign Live! CC certificate manager kann X.509v3 Zertifikate einschließlich dem Private Key erstellen. Der Zertifikatsinhaber kann diese Zertifikate anschließend auf jeder Plattform verwenden. Ob Webbrowser oder Java Runtime Environment, Smartphones unter iOS (iPhone/iPad), Android oder Blackberry OS - in der Regel reicht ein Klick und das Zertifikat wird in das gewünschte System importiert. Danach können sofort E-Mails signiert und verschlüsselt oder Anmeldungen im Browser an zertifikatsgeschützten Websites durchgeführt werden.

Integrierte OCSP- und Sperrlistenverwaltung

Sign Live! CC certificate manager erzeugt und verwaltet parallel zur Zertifikatsgenerierung auch Sperrlisten (CRLs). Über eine in den Zertifikaten abgelegte URL können diese Sperrlisten von den nutzenden Anwendungen abgerufen werden. So kann einfach und schnell die Gültigkeitsinformation aller ausgegebenen Zertifikate an Anwendungen und Portale übermittelt werden.

Über den integrierten OCSP Responder lassen sich Gültigkeit und Sperrstatus online und auf Zertifikatsebene standardisiert und schnell abrufen. OCSP Anfragen werden z.B. genutzt, um einem Anwender die Zutrittsrechte zu einem Webportal in Echtzeit zu gewähren oder zu entziehen. Moderne Application Server wie Tomcat oder JBOSS führen bei zertifikatsbasierter Authorisierung automatisch eine OCSP-Abfrage durch.

Effektive Laufzeitüberwachung

Die Behandlung von auslaufenden Zertifikaten und die rechtzeitige Benachrichtungung des Administrators ist die Aufgabe des Certificate Monitors. Folgezertifikate können zeitgerecht und unterbrechungsfrei erstellt bzw. beim Trust Center angefordert werden.

Eine Auswertung über die verbleibende Laufzeiten aller Zertifikate ist jederzeit möglich. Die Benachrichtigung kann über die Oberfläche oder per E-Mail erfolgen.

Abgesicherte Administration

Der Sicherung des Administrationszugangs kommt bei einer Zertfikatsverwaltung eine wichtige Rolle zu. *Sign Live! CC certificate manager* erlaubt den Einsatz einer Smartcard mit einem entsprechenden Klasse 3 Zertifkat

Systemvoraussetzungen

- Hardware
  - Prozessor: empfohlen Intel Core 2 Duo mit 2,0 GHz
  - freier Arbeitsspeicher: empfohlen mind. 2 GB
  - freier Festplattenspeicher: mind. 80 MB für die Installation
- Betriebssysteme
  - Windows 7 (32/64 Bit), weitere auf Anfrage
  - Java Runtime Environment (JRE) Version 6
- Soft-Zertifikate
  - X.509-konform (Trust Center, sonstige PKI)
- Lizenzierung
  - pro Arbeitsplatz/Benutzer

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