

Sign Live! CC cloud suite

- Elektronische Signatur (qualifiziert und fortgeschritten)
- Starke Authentisierung
- PIN Management
- Keine lokale Installation notwendig
- Keine Admin-Rechte notwendig
- Signatur u. Authentisierung direkt in der Webanwendung
- Einfache Integration mit HTML oder JavaScript
- Nahtlose Integration - das Look & Feel kann vollständig von der Webseite definiert werden
- Unterstützung von zahlreichen Smartcards, Cryptotoken und dem neuen Personalausweis
- Gleichzeitiges Signieren mehrerer Dokumente möglich
- Basiert auf bewährter SignLive! CC Technologie
- Komfortsignatur möglich
- Trusted Viewer

Elektronische Signatur und starke Authentisierung im Web



Webanwendungen führen ihren ungehinderten Siegeszug gegenüber klassischen Client-Server Anwendungen fort. Einfache Softwareverteilung, zentrale Administration und -pflege reduzieren die Kosten. Vor diesem Hintergrund bietet die *SignLive! CC cloud suite* eine nahtlose Integration von Smartcards und eTokens in webbasierte Prozesse und Lösungen. So können ihre Prozesse sowohl von der elektronischen Signatur als auch von einer starken Authentisierung ihrer Anwender profitieren.

Elektronische Signatur

Die Erfordernis einer Unterschrift unterbricht oft digitale Prozesse, da eine rechtsgültige Unterschrift meistens handschriftlich auf Papier erfolgen muss (Medienbruch). Alternativ kann eine qualifizierte elektronische Signatur als gleichwertiger Ersatz für die handschriftliche Signatur eingesetzt werden. Die dazu benötigten Anwendungen (Signaturanwendungskomponenten) müssen aber auf dem PC schon vorhanden sein und sind zusätzlich in einer rein webbasierten Lösung nur schwer zu integrieren. *SignLive! CC cloud suite* bündelt die wichtigsten Kernkomponenten der Signaturanwendungskomponente *SignLive! CC* in ein kleines, transportables Paket, das sich einfach in Webanwendungen verwenden lässt. Es ist keine Installation oder zusätzliche Software auf dem PC notwendig. Die Webseite bringt das Paket (Java Applet) im richtigen Prozessschritt mit und der Anwender kann problemlos seine Unterschrift direkt im Browser leisten.

Bei der Verwendung einer Signaturanwendungskomponente (SAK) gibt es oft einen Anwendungswechsel von der Fachanwendung zur SAK. Der Anwender wird mit einer neuen Benutzeroberfläche konfrontiert, die viel mehr Funktionen bietet, als er im diesem Augenblick benötigt um seine Aufgabe zu erfüllen. Im Extremfall weist ihn die Anwendung noch darauf hin, dass ein neues Update zu installieren ist. Der Anwendungswechsel erhöht die Fehlerquote in diesem Prozessschritt signifikant. Die Fachanwendung kann hier auch keine Hilfestellung geben, da sie die Kontrolle an die SAK übergeben hat.

Im Gegensatz dazu bietet *SignLive! CC cloud suite* eine nahtlose Integration in die Webanwendung. Die Webanwendung führt den Anwender und zeigt ihm nur die Wahlmöglichkeiten und Funktionen der *SignLive! CC cloud suite*, die gerade in diesem Kontext sinnvoll sind. Auch die Darstellung erfolgt im gleichen Look & Feel wie die Webanwendung selbst, so dass der Anwendungswechsel für den Anwender gar nicht sichtbar ist.

Die nahtlose Integration der *SignLive! CC cloud suite* vereinfacht die Signaturvorgang für den Anwender, erhöht die Akzeptanz der elektronischen Signatur und senkt die Fehlerquote im Gesamtprozess.

Starke Authentisierung

SignLive! CC cloud suite bietet eine starke Authentisierung (Zwei-Faktor-Authentisierung) für Webanwendungen mit Smartcards oder eTokens an. Gerade wenn Sie schon eine bestehende Public-Key-Infrastruktur haben, können Sie diese mit einfachen Mitteln auch in ihren Webanwendungen verwenden. Wie auch die Signatur, benötigt die Authentisierung keine Installation oder besondere Rechte auf dem PC und lässt sich nahtlos in die Anwendung integrieren. So erhöhen Sie den Wertschöpfungsgrad ihrer PK-Infrastruktur, erreichen eines der höchsten Sicherheitslevel der Authentisierung und befreien ihre Anwender von der Notwendigkeit, sich neue Kennwörter zu merken.

Funktionen

- Elektronische Signatur (qualifiziert und fortgeschritten)
 - Einzel- und Stapelsignatur, (Massensignatur)
 - PDF und PDF/A konforme eingebettete sichtbare und unsichtbare Signaturen
 - PKCS#7 (abgesetzte Signaturen)
 - XML DSig
- Zertifikatsbasierte Authentisierung
- PIN Management
 - Initialisierung mit Transport-PIN
 - PIN ändern und zurücksetzen
- X.509 Zertifikate von Smartcard/eToken auslesen
- Kartenzustand überwachen
- Öffnen eines lokalen Trusted-Viewers
- Kryptografische Verfahren: RSA und ECC
- Unterstützte Smartcards, eToken und Kartenleser
 - Detaillierte Informationen finden Sie im zugehörigen Datenblatt
 - Grundsätzlich werden alle ISO-7816 konforme Karten und PC/SC-Kartenleser unterstützt.

Systemvoraussetzungen

- Hardware
 - Prozessor: x86-kompatible CPU
 - freier Arbeitsspeicher: empfohlen mind. 256 MB
 - Betriebssysteme
 - Windows XP, Windows Vista 7 32/64Bit
 - Linux (Ubuntu, RedHat, OpenSUSE)
 - Mac OS X
 - weitere UNIX-Plattformen auf Anfrage
 - Java Runtime Environment (JRE) Version 6 oder besser
 - Browser
 - IE 8+, Firefox 14+, Chrome 21+, Safari 5+
- Detaillierte Informationen finden Sie im zugehörigen Datenblatt.

Weitere Informationen:

www.intarsys.de

info@intarsys.de

+49 721 38479 0

Folgen Sie nebenstehendem QR-Code

