

Produktbeschreibung

Eigenschaften

Signaturen, Siegel und Zeitstempel

- qualifiziert oder fortgeschritten
- mit Smartcards und Crypto-Token
- mit Hardware Security Modul (HSM)
- als Fernsignatur über Signaturdienst

Long Term Validation für PAdES-, CAdES- und XAdES-Signaturformate

- bei der Signaturerstellung
- bei der Signaturprüfung

Zertifikatsprüfung nach eIDAS mit der EU trusted list, OCSP-Abfrage

ECC- und RSA-Signatur (PSS-Padding)

PDF/(A)-Dokument signieren

- auch mehrfach möglich, konform und kompatibel zum PDF/(A)-Standard

Über Standardschnittstellen nahtlos in (web-basierte) Workflow-/DMS-/ERP/...-Systeme integrierbar

Verwendung als Dienst unter Windows und Linux möglich

Kombinierbar mit Sign Live! CC cloud suite Komponenten als Remote Signing Lösung

Basiert auf bewährter und sicherheitsbestätigter Sign Live! CC Technologie

Erfüllt alle Anforderungen gemäß SigG, SigV, ZertES und der EU-Verordnung eIDAS

Konform zu der Definition für „Signature Creation Application“ nach ETSI

Prüfung auf gültiges Zertifikat vor der Signaturerstellung

Attributzertifikat(e) für Signatur einbetten und prüfen

Serverlösung für Massensignaturen



Elektronische Dokumente schaffen Ordnung, sparen Zeit, reduzieren Kosten und schonen die Umwelt. In Kombination mit qualifizierten elektronischen Signaturen, Siegel und Zeitstempel können Sie elektronische Dokumente rechtsgültig und medienbruchfrei erstellen, bearbeiten und im LTV-Format (long term validation) ablegen.

Sign Live! CC server erzeugt und prüft fortgeschrittene und qualifizierte elektronische Signaturen, Siegel und Zeitstempel gemäß der EU-Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt der Europäischen Union (eIDAS). *Sign Live! CC server* ist ein flexibler serverseitiger Dienst, der in der Lage ist, komplexe kryptografische Operationen auch bei sehr hohen Lasten durchzuführen. *Sign Live! CC server* ist für Trust Center-Umgebungen geeignet.

Qualität, Ordnungsmäßigkeit und Zuverlässigkeit von *Sign Live! CC server* sind durch entsprechende Prüfungen nach internationalen Sicherheitskriterien (Common Criteria) und Bestätigungen gemäß deutschem Signaturgesetz nachgewiesen. Die Bestätigungen der Gesetzeskonformität werden fortlaufend aktualisiert.

Signaturen, Siegel und Zeitstempel können mit Signaturkarten, dem elektronischen Heilberufsausweis (eHBA), der SuisseID, eToken, marktüblichen Hardware Sicherheitsmodulen (HSM) oder als Fernsignatur, z.B. mit dem „All-in Signing Service“, erstellt werden.

Alle spezifizierten Signaturformate (CAdES, PAdES, XAdES) für qualifizierte und fortgeschrittene elektronische Signaturen, Siegel und Zeitstempel, sowie alle Signaturtypen gemäß der PDF- und PDF/A-Spezifikation stehen zur Verfügung.

Die flexible Signatursoftware *Sign Live! CC server* bietet viele Einsatzmöglichkeiten und ist auf den gängigen Betriebssystemen (WIN, Linux und MacOS) auch in virtualisierten Umgebungen lauffähig.

Sign Live! CC ist verfügbar als *Sign Live! CC signature server* für die Erstellung und als *Sign Live! CC validation server* für die Prüfung von Signaturen, Siegel und Zeitstempel.

Produktbeschreibung

Erscheinungsbild der Signatur im PDF

Sign Live! CC signature server bietet bei der Signaturerstellung die zwei Optionen „mit sichtbarer Signatur“ oder „ohne sichtbare Signatur“ zur Auswahl. Für die sichtbare Signatur kann das Erscheinungsbild der Signatur umfangreich konfiguriert werden. So können z. B. die Abbildung Ihrer handschriftlichen Signatur, ein Firmenlogo oder ein Foto als Erscheinungsbild und zusätzlich weitere Texte genutzt werden. Auch auf Informationen aus dem Signaturzertifikat kann zugegriffen werden.

Optional kann das Dokument vor der Signatur PDF/A-konform für die Langzeitarchivierung aufbereitet werden.

Signaturtypen

Sign Live! CC server kann in einer PDF-Datei eine Zertifizierungssignatur und eine/mehrere Genehmigungssignaturen (Mehrfachsignatur) anbringen und prüfen. Zertifizierungs- und Genehmigungssignaturen entsprechen sowohl der ETSI-, als auch der PAdES-Norm (PDF Advanced Electronic Signature).

Zeitstempel

Sign Live! CC signature server kann in einer PDF-Datei einen separaten Dokumentzeitstempel erstellen, um Authentizität und Bestehen des Dokuments zu einem bestimmten Zeitpunkt zu bestätigen. Für qualifizierte Zeitstempel beinhaltet *Sign Live! CC signature server* eine Konfiguration, um den Zugang zu einer hochverfügbaren und hochvertrauenswürdigen Uhrzeit zu erhalten. Alle Zeitstempel entsprechen Teil 4 der ETSI 102 778 PDF-Norm für erweiterte elektronische Signaturen (PAdES).

Signaturgeräte

Sign Live! CC signature server unterstützt für die Signaturerstellung unterschiedliche Signaturgeräte auf denen sich Zertifikate befinden können, wie Smartcard, Crypto-Token, Hardware Security Modul (HSM) und entfernte Signaturdienste. Auch File-basierte Zertifikate oder Zertifikate aus dem Zertifikatsspeicher von Windows können zum Signieren verwendet werden.

Signaturkarten und Softzertifikate

Es werden gesetzeskonforme Signaturkarten aller deutschen Trustcenter und Signaturkarten aus der Schweiz, sowie aus ausgewählten EU-Mitgliedsstaaten unterstützt. Für

den automatisierten Signaturbetrieb müssen die eingesetzten Signaturkarten bestimmte technische Voraussetzungen erfüllen. Insbesondere muss die Signaturkarte die Durchführung mehrerer Signaturen bei einmaliger PIN-Eingabe gewährleisten.

Signaturformate

Sign Live! CC server unterstützt alle gängigen Signaturformate wie PAdES, CAdES, XAdES, XML DigSig, PKCS#7, CMS, PKCS#1 und S/MIME, sowie eANV-XML-Format gemäß BMU-Spezifikation. Im Fall der Signierung eines PDF/A konformen Dokumentes bleibt die PDF/A-Konformität erhalten. Die Nachweisbarkeit und langfristige Überprüfbarkeit von Signaturen kann wahlweise im Standard der Langzeit-Validierung (LTV) bei der Erstellung oder Prüfung erfolgen.

Mandantenfähigkeit

Für die Definition von mandantenspezifischen Signaturpools steht eine komfortable und intuitiv zu bedienende Benutzeroberfläche zur Verfügung. Ein Signaturpool bündelt quasi beliebig viele Kartenleser pro Mandant. *Sign Live! CC signature server* kann eine Vielzahl von Prozessen parallel abarbeiten. Die zusätzlichen optionalen Funktionen wie „Validieren“, „Zeitstempeln“, „Verschlüsseln“ und „Per E-Mail versenden“ sind miteinander kombinierbar.

Zertifikatsverwaltung

Die integrierte Zertifikatsverwaltung in *Sign Live! CC server* dient zur Generierung und zentralen Verwaltung digitaler Identitäten, kryptografischer Schlüssel und digitaler Zertifikate. Weiterhin beinhaltet die Zertifikatsverwaltung die Vertrauensliste gemäß Artikel 22 der EU-Verordnung (EU trust list), vertrauenswürdige Stammzertifikate und weitere Einträge, die für die Signaturerstellung und Prüfung herangezogen werden.

Skalierbare Lösung

Grundsätzlich ergeben sich abhängig von der Anzahl der Signaturprozesse unterschiedliche Lösungsszenarien. Als Einstiegsvariante bei geringem Volumen eignet sich die Servervariante von *Sign Live! CC signature server* mit lokalem Kartenleser. Für die zentrale automatisierte Signaturerstellung größerer Dokumentenmengen kann *Sign Live! CC signature server* mit mehreren Kartenlesern (multi card option) oder in Kombination mit externen Signaturdiensten (All-in Signing Service) eingesetzt werden. Für weitaus höhere Performance ist der Einsatz von marktüblichen Hardware Security Modulen möglich.

Produktbeschreibung

Integration und Automation

Für die Einbindung in bestehende Systeme, wie z.B. DMS und ERP-Systeme oder die Anbindung an Archivsysteme stehen umfangreiche Standardschnittstellen und Integrationsmöglichkeiten zur Verfügung.

Je nach Bedarf kann die Anbindung über Verzeichnisüberwachung, über Kommandozeilenaufruf, über Programmierschnittstellen (API) wie XMLRPC, Web-Service, SOAP, ActiveX, HTTP, Sharedlib usw. oder über Prozessintegration mit Java oder JavaScript erfolgen.

Sign Live! CC signature server ist besonders geeignet für den Betrieb im Rechenzentrum zur Massensignatur von Dokumentstapeln ohne manuellen Eingriff. *Sign Live! CC signature server* ist eine kostengünstige Anwendung, die sich in jedem Fall rechnet.

Grenzüberschreitender Einsatz

Sign Live! CC signature server ist international einsetzbar, egal ob von Deutschland, Österreich, einem anderen EU-Land oder der Schweiz aus operiert wird. Durch ihr Engagement in verschiedenen EU-Arbeitskreisen kann die intarsys dem Anwender bei der Umsetzung entsprechender Projekte umfassende Unterstützung, wie z.B. Beratung bezüglich landesspezifischer Rahmenbedingungen, anbieten.

Signaturprüfung an zentraler Stelle standardkonform und zuverlässig mit Prüfprotokoll

Mit *Sign Live! CC validation server* prüfen Sie zuverlässig, ob elektronische Signaturen korrekt sind und mit Hilfe gültiger Zertifikate erstellt wurden. So stellen Sie sicher, dass nur geprüfte Dokumente weiterverarbeitet werden und in Ihr Dokumentenarchiv gelangen. Das Prüfprotokoll gibt in einstellbarem Detaillierungsgrad das Prüfergebnis wieder und belegt, dass Sie die Prüfung durchgeführt haben. Als Formate für das Prüfprotokoll stehen HTML, PDF/A, Text und OASIS DSS zur Verfügung.

Signaturprüfung gegen EU trusted list

Die EU-Signaturverordnung eIDAS definiert die Basis für den digitalen Binnenmarkt in Europa. Eine wichtige Voraussetzung ist die vertrauenswürdige, zentrale Bereitstellung von Zertifikaten der gemeldeten Vertrauensdiensteanbieter (TSP), welche über die vertrauenswürdige Trust-Service Status List (TSL) erfolgt. *Sign Live! CC validation server* prüft die Zertifikate mittels TSL und macht Sie so wettbewerbsfähig im europäischen Wandel.

Signaturprüfung gegen OCSP und Sperrliste

Die Validierung von Signaturen kann lokal über Sperrlisten oder online per OCSP-Abfrage erfolgen. Sind beide Einstellungen aktiv, prüft *Sign Live! CC validation server* die Signatur zuerst über OCSP. War die OCSP-Prüfung erfolgreich, werden die Sperrlisten nicht mehr herangezogen. Ist die OCSP-Prüfung nicht aktiviert oder fehlgeschlagen – zum Beispiel weil keine Online-Verbindung vorhanden ist – werden die lokalen Sperrlisten herangezogen. Sperrlisten geben Auskunft darüber, ob Zertifikate zurückgezogen wurden. Aktuelle Sperrlisten sind daher unabdingbar für den Validierungsprozess. *Sign Live! CC validation server* aktualisiert Sperrlisten automatisch und ergänzt unbekannte Sperrlisten.

Signaturprüfung mit LTV-Informationen

Digital signierte Dokumente müssen oft viele Jahre archiviert werden und es muss zu jedem Zeitpunkt in der Zukunft möglich sein, die Signatur des Dokuments zu prüfen. Dieses Konzept nennt man Long-Term Validation (LTV). Mit *Sign Live! CC validation server* können Sie bei der Signaturprüfung die fehlenden Informationen für Zertifikate einbetten und so nachträglich LTV-Fähigkeit für Signaturen, Siegel oder Zeitstempel erreichen.

Systemvoraussetzungen

Betriebssysteme

- › Windows (32/64 bit) Vers. 7, 8.1, 10
- › Linux (32/64) Ubuntu, open SUSE
- › Mac OS X 10.11 / 10.12

Weitere Details siehe Datenblatt

Lizenzierung

- › Pro Server

Weitere Informationen:

🏠 www.intarsys.de

✉ sales@intarsys.de

☎ +49 721 38479 0

Folgen Sie nebenstehendem QR-Code

