

# Sign Live! CC signature server



## Produktbeschreibung

### *Sign Live! CC signature server*

- Fortgeschrittene/Qualifizierte Signaturen und Zeitstempel
- Kontinuierliche Massensignatur
  - bis zu 19.000 Signaturen/h je Signaturkarte (ECC)
  - bis zu 80.000 Signaturen/h mit Hardware Security Modul (HSM)
- Externe Signaturdienste
  - Swisscom All-in Signing Service für Massensignaturen, On Demand Signaturen und Zeitstempel
  - Signtrust NET für Massensignaturen
- Erfüllt alle Anforderungen gemäß SigG/SigV, ZertES und EG-Signaturrichtlinie
- Basiert auf bewährter und sicherheitsbestätigter Sign Live! CC Technologie
- Administration über eine komfortable und intuitiv zu bedienende Benutzeroberfläche
- Kostengünstige und einfache Integration in bestehende Prozesse
- Flexibel einsetzbar durch Standard-schnittstellen und Signaturformate
- Permanente Anpassung an aktuelle gesetzliche Anforderungen und internationale Standards
- Der *Sign Live! CC signature server* läuft auch als Dienst

## Inhouse-Lösung für alle Anwendungen bei der Signaturerstellung



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

### Skalierbare Lösung

Grundsätzlich ergeben sich abhängig von der Anzahl der Signaturprozesse und dem geforderten Automatisierungsgrad in der Produktion unterschiedliche Lösungsszenarien. Als Einstiegsvariante bei geringem Volumen eignet sich die Servervariante von *Sign Live! CC* mit lokalem Kartenleser. Für die zentrale automatisierte Signaturerstellung großer Dokumentenmengen kann *Sign Live! CC signature server* mit mehreren Kartenlesern (multi card option) oder in Kombination mit externen Signaturdiensten (Signtrust NET, Swisscom AIS) eingesetzt werden. Eine weitere Möglichkeit für weitaus höhere Performance ist der Einsatz von Hardware Security Modulen (SafeNet).

### Signaturkarten und softwarebasierte Zertifikate

Es werden gesetzeskonforme Signaturkarten aller deutschen Trustcenter und Signaturkarten aus verschiedenen EU-Mitgliedsstaaten sowie der Schweiz 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. Daneben sind – im Rahmen der einfachen und fortgeschrittenen Signatur – auch softwarebasierte Zertifikate einsetzbar. Zertifikate aus dem Zertifikatsspeicher von Windows können für fortgeschrittene Signaturen ebenfalls verwendet werden.

# Sign Live! CC signature server

Gesetzeskonforme Signaturlösung nach SigG/SigV und ZertES



## Signaturformate

*Sign Live! CC signature server* erstellt alle gängigen Signaturformate, einschließlich PDF, 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) erfolgen.

*Sign Live! CC signature server* bietet über Konfigurationsmechanismen die Möglichkeit, beim Signaturvorgang zusätzliche XML-Daten in das zu signierende Dokument zu integrieren und optional PDF/A-konform für die Langzeitarchivierung aufzubereiten. Der Anwender kann frei wählen, welche Dokumentenformate, PDF-Formulare oder "Transaktionen" er signieren möchte.

## 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.

## Integrationsmöglichkeiten

Für die Einbindung in bestehende dokumenterzeugende und dokumentführende Systeme, wie z.B. DMS und ERP-Systeme oder die Anbindung an Archivsysteme stehen umfangreiche Standardschnittstellen und Integrationsmöglichkeiten zur Verfügung. Je nach Bedarf erfolgt die Anbindung über Verzeichnisüberwachung, Kommandozeilenaufruf, Programmierschnittstellen (API) wie XMLRPC, SOAP, ActiveX, HTTP usw. oder Prozessintegration mittels Java oder JavaScript.

*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 – egal, ob Sie sie in einem Rechenzentrum betreiben oder in kleineren Institutionen.

## 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.

## Signaturerstellung

### Signaturalgorithmus:

- ECC (Elliptic Curve Cryptography),
- RSA (Rivest-Shamir-Adlerman)

### RSA-Hashalgorithmen:

- SHA1, SHA-2 (-224, -256, -384, -512), RIPEMD160/256

### Zeitstempelunterstützung:

- gemäß IETF RFC 3161 Time-Stamp Protocol für Trustcenter in D-A-CH, wie z.B. D-TRUST, Signtrust, TeleSec, Swisscom, SwissSign, QuoVadis
- Einsatz als RFC3161-konformer Zeitstempeldienst möglich

### Mehrfach-Signaturkarten:

- Signaturkarten gängiger Trustcenter/CAs in D-A-CH wie z.B. D-TRUST, Telesec, Signtrust, S-TRUST, DATEV, Bundesnotarkammer, medisign, dgnservice, QuoVadis, Swisscom, SwissSign, A-Trust

### ASP-Signaturdienste:

- Signtrust NET, Swisscom AIS

### Hardware Security Module:

- SafeNet PSE und Luna

### Betriebssysteme:

- Windows 7 / 8 (32/64 bit)
- Windows 2008/2012 Server (32/64 bit)
- Ubuntu 10.04/12.04, Open SUSE 12.3
- SUSE Linux Enterprise Server 11, CentOS 6
- Mac OS X (ab 10.8)
- VMware, Citrix XenApp, Windows TS

### Systemvoraussetzungen:

- IBM-kompatibler PC ab Pentium 4 / 2 GHz
- ab 4/8 GB Arbeitsspeicher (RAM)
- Festplattenspeicher: mind. 200 MB für Basis-Installationspaket

### Java

- Java Runtime Environment (JRE) Version 7

### Weitere Informationen:

[www.intarsys.de](http://www.intarsys.de)  
[info@intarsys.de](mailto:info@intarsys.de)  
+49 721 38479 0

Folgen Sie nebenstehendem QR-Code

