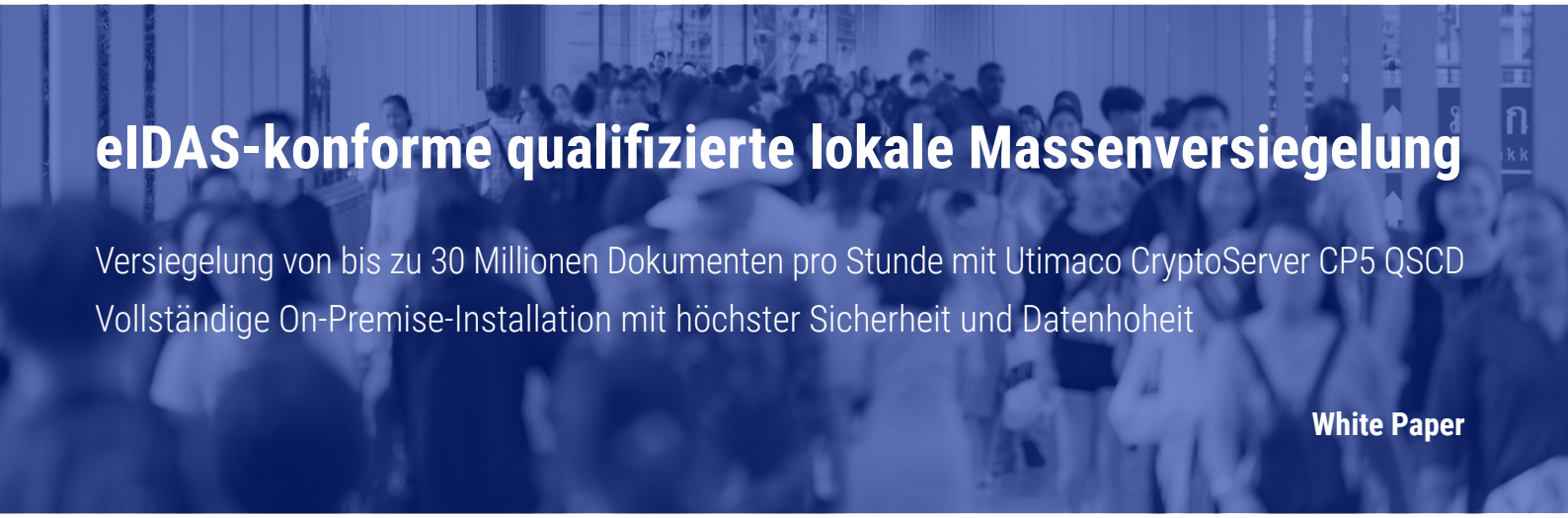


eIDAS-konforme qualifizierte lokale Massenversiegelung

Versiegelung von bis zu 30 Millionen Dokumenten pro Stunde mit Utimaco CryptoServer CP5 QSCD

Vollständige On-Premise-Installation mit höchster Sicherheit und Datenhoheit

White Paper

Qualifizierte lokale Massenversiegelung

Qualified Local Mass Sealing (QLMS) ist eine umfassende Lösung, mit der Sie bis zu 30 Millionen Dokumente pro Stunde digital signieren können. Die Vor-Ort-Lösung verwendet qualifizierte elektronische Siegel, die mit der Verordnung über elektronische Identifizierung, Authentifizierung und Vertrauensdienste (eIDAS) konform sind. Sie ist eine ideale Lösung für die Massenverarbeitung von Dokumenten oder Daten mit einem hohen Automatisierungsgrad.

Unternehmen, Finanz-, Verwaltungs- und Gesundheitsorganisationen, die eigene Rechenzentren betreiben, können QLMS für hochperformante Versiegelungsprozesse lokal implementieren, z. B. für die Versiegelung von Auftragsbestätigungen, Rechnungen, digitalen Kontoauszügen, amtlichen Bescheinigungen, Krankenakten usw. sowie für die Authentifizierung von Kontozugängen für FinTechs gemäß PSD2 (Payment Services Directive 2).

Die herkömmliche Methode bestand und besteht darin, qualifizierte E-Siegel auf Smartcards mit Kryptochips für Smartcard-Lesegeräte oder USB-Tokens oder in der Cloud für Remote-Prozesse einzusetzen.

Erst seit der Änderung der Verordnung am 1. März 2019 ist es rechtlich zulässig, Hardware-Sicherheitsmodule (HSM) als QSCD für die interne digitale Versiegelung von Dokumenten zu verwenden, womit dies nicht mehr allein Vertrauensdienste-anbietern vorbehalten ist.

Basierend auf dem QSCD unseres Technologiepartners Utimaco kann unsere Lösung für Qualified Local Mass Sealing bis zu 8.600 Operationen pro Sekunde mit einem 2048bit RSA-Schlüssel verarbeiten.

Was Sie wissen müssen

QSCD

Qualifizierte Siegelerstellungsgeräte sind nach EN 4192215 zertifiziert und entsprechen der eIDAS (EU) Verordnung 910/2014.

Fernidentifizierung

Die Fernüberprüfung der Identität des gesetzlichen Vertreters der Organisation ist obligatorisch, um das Antragsverfahren für das Qualifizierte Siegel der Organisation zu beginnen.

Versiegelung Server

Für Unternehmen, die eine schlüsselfertige Lösung für die qualifizierte Versiegelung von Dokumenten suchen, kann ein leistungsstarker und vielseitiger Sealing Server in einem Vor-Ort-Bereitstellungsmodell implementiert werden.

Qualifiziertes Siegel

Das Qualifizierte Siegel kann mit einer ein-, zwei- oder drei-jährigen Gültigkeit versehen werden und wird von einem akkreditierten Qualified Trust Service Provider (QTSP) ausgestellt.

Bereitstellung, Integration und Schulung

Mit unserer Erfahrung aus zwei Jahrzehnten HSM-Beratung unterstützen unsere Experten Sie bei der Schlüsselübergabe und der Integration der Lösung in die bestehende IT-Infra-struktur.

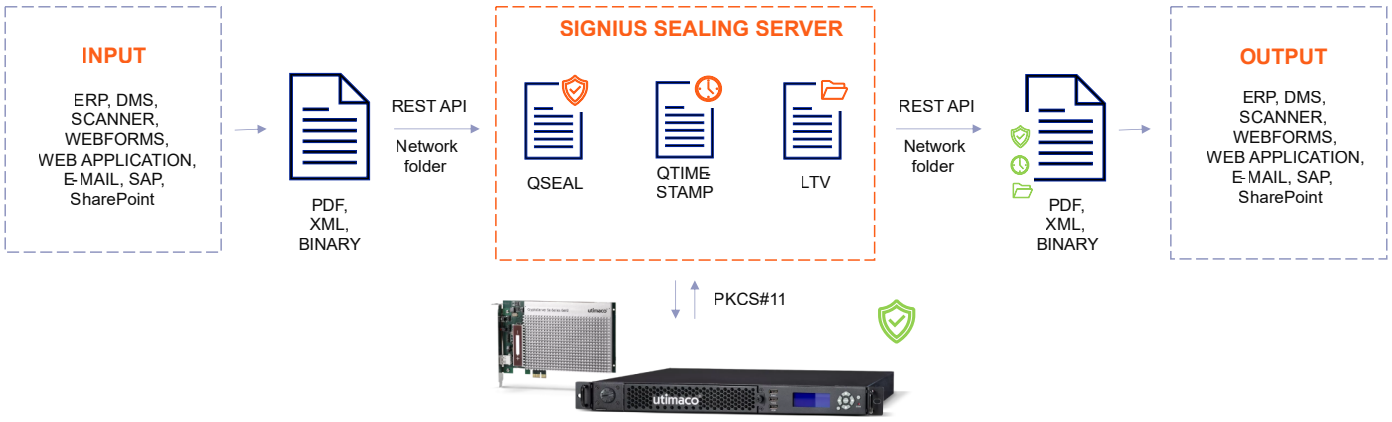
eIDAS

Alle von SIGNIUS implementierten Technologien und Prozesse sind vollständig konform mit eIDAS und den allgemeinen Datenschutzbestimmungen.

Vorteile eines eIDAS-konformen QLMS

- Unbegrenzte Versiegelung von Dokumenten ohne volumenabhängige Gebühren, die vom Vertauensdiensteanbieter erhoben werden
- Massensiegelung von bis zu 30 Millionen Unterschriften pro Stunde
- eIDAS-zertifizierte und fälschungssichere qualifizierte Signaturerstellungseinheit (QSCD)
- Unleugbarkeit, bestätigte Authentizität und garantierte Integrität
- Ideal für die Massenverarbeitung von Dokumenten oder Daten mit höchstem Automatisierungsgrad
- Ersatz von alten, schlecht funktionierenden Chipkarten und Kartenlesegeräten
- Flexible Integration in bestehende Signaturlösungen
- Breite Unterstützung für verschiedene Dokumentenmanagement-, CRM- und ERP-Systeme
- Die Vor-Ort-Einrichtung garantiert ein Höchstmaß an Datenschutz und Einhaltung der GDPR
- In der EU und darüber hinaus anerkannte Rechtskonformität
- Langzeitarchivierung und qualifizierte Zeitstempel sind auf Anfrage erhältlich

Der Versiegelungsprozess



UTIMACO CRYPTOSERVER CP5
CC-CERTIFIED QUALIFIED SIGNATURE CREATION DEVICE (QSCD)
FOR QUALIFIED ELECTRONIC SIGNATURES AND SEALS

Qualifizierte elektronische Signaturen und Siegel

Eine qualifizierte elektronische Signatur ist die elektronische Unterschrift einer natürlichen Person.
Gemäß den eIDAS-Verordnungen bieten qualifizierte elektronische Signaturen (QES) - im Gegensatz zu "einfachen" (z. B. gescannten händischen Unterschriften) und "fortgeschrittenen" Signaturen - die höchste Gewähr und Sicherheit. Eine QES hat die gleiche rechtliche Wirkung wie eine handschriftliche Unterschrift.

Ein qualifiziertes elektronisches Siegel wird an juristische Personen ausgegeben und von diesen verwendet, um die Herkunft und Integrität von Daten und Dokumenten zu gewährleisten; ein elektronisches Siegel ist daher keine elektronische Signatur einer natürlichen Person. Unter einer juristischen Person versteht man gemeinhin eine Gesellschaft, ein Unternehmen, eine Vereinigung und eine Behörde. In Verbindung mit qualifizierten Zeitstempeln bieten Dokumente, die mit einer qualifizierten Signatur oder einem qualifizierten Siegel signiert sind, die höchste Sicherheitsstufe der Unleugbarkeit, Authentizität und Integrität vergleichbar dem Status einer notariellen Beglaubigung.

Qualifizierte elektronische Siegel, Signaturen und Zeitstempel können nur von einem Vertauensdiensteanbieter erstellt und verwendet werden, der von einer Konformitätsbewertungsstelle geprüft und von einer nationalen Aufsichtsbehörde zertifiziert und schließlich in der EU Trust Service List (EU TSL) aufgeführt ist.

eIDAS und CEN/TS 419221-6

Die am 1. März 2019 veröffentlichte technische Spezifikation (CEN/TS 419221-6) legt die Anforderungen für lokale Anwenungen der EN 419221-5 für qualifizierte elektronische Signaturen oder Signaturerstellungseinheiten fest, d.h. für den Fall, dass der Unterzeichner oder Signaturersteller direkte lokale Kontrolle über das kryptographische Modul hat. Ziel ist es, die qualifzierten Siegelerstellungseinheiten und/oder Signaturerstellungseinheiten (QSealCD / QSignatureCD) nach der (EU) Verordnung 910/2014 zuzulassen. Für die organisationsinterne Massenversiegelung ist eine entsprechende Zertifizierung der HSM/ QSCD und deren Unterbringung in einem sicheren Serverraum oder Rechenzentrum (z.B. mit Zugangskontrolle) erforderlich.

In diesem Fall ist der Betrieb von Hardware-Sicherheitsmodulen (HSM) als QSCD für die interne qualifizierte digitale Versiegelung von Dokumenten rechtlich und technisch nicht mehr nur qualifizierten Vertrauensdiensteanbietern vorbehalten.

Utimaco CryptoServer CP5 (QSCD)

Der Utimaco CryptoServer CP5 ist nach Common Criteria EAL4+ gemäß dem Schutzprofil EN 419 221-5 "Kryptografisches Modul für Vertrauensdienste" zertifiziert. Diese Zertifizierung ermöglicht die konforme Erzeugung von qualifizierten digitalen Signaturen, Siegeln und Zeitstempeln gemäß der eIDAS-Verordnung.

Eine Erneuerung der Zertifizierung ist im Dezember 2023 geplant, die dann bis 2028 gültig sein wird. Der CryptoServer CP5 kann mit Hilfe des CryptoServer SDK Entwicklungskits um ein Signaturaktivierungsmodul (SAM) erweitert werden, das innerhalb der zertifizierten HSM-Grenze läuft und die Anforderungen des Schutzprofils EN 419 241-2 erfüllt.

Technische Daten des Utimaco CryptoServer CP5 QSCD

Die eIDAS-konforme CC-zertifizierte qualifizierte Signaturerstellungseinheit (QSCD)

Wesentliche Merkmale

- Sichere Schlüsselspeicherung und -verarbeitung innerhalb der sicheren Grenzen des HSM
- Umfangreiche Schlüsselverwaltung mit Schlüsselautorisierung
- Schlüsselautorisierung API und Tool (nach PP EN 419 221-5)
- "m von n" Quorum-Authentifizierung (z.B. 3 von 5)
- 2-Faktor-Authentifizierung mit Smartcards
- Konfigurierbare rollenbasierte Zugriffskontrolle und Aufgabentrennung
- Unterstützung mehrerer Mandanten
- Fernverwaltung
- Dedizierter Softwaresimulator für Bewertungs- und Integrationstests
- Unterstützte Betriebssysteme: Windows und Linux
- Mehrere Integrationen mit PKI-Anwendungen usw.
- Alle Funktionen sind im Produktpreis enthalten

Unterstützte kryptographische Algorithmen

- RSA, ECDSA mit NIST- und Brainpool-Kurven
- ECDH mit NIST- und Brainpool-Kurven
- AES
- CMAC, HMAC
- SHA2-Familie, SHA3
- Hash-basierter deterministischer Zufallszahlengenerator (DRG.4 nach AIS 31)
- Echter Zufallszahlengenerator (PTG.2 nach AIS 31)
- Bis zu 3.000 RSA- oder 2.500 ECDSA-Signiervorgänge im Massenverarbeitungsmodus
- Alle Algorithmen im Produktpreis enthalten

Verfügbare Modelle und Leistungen

	KryptoServer CP5					
Hardware-Plattform-Modell	**KryptoServer CP5 Se12**	**KryptoServer CP5 Se52**	**KryptoServer CP5 Se500**	**KryptoServer CP5 Se1500**	**KryptoServer CP5 Se15000**	**KryptoServer CP5 Se40000**
RSA-Operationen pro Sekunde	16 RSA 2K Sig/s (18 im Bulk-Modus)	80 RSA 2K Sig/s (90 im Bulk-Modus)	800 RSA 2K Sig/s (2.300 im Bulk-Modus)	1,100 RSA 2K Sig/s (3.600 im Bulk-Modus)	15000 RSA 2K sigs/s	40000 RSA 2K sigs/s

Kontaktieren Sie uns für eine DEMO oder ein Gespräch mit unserem eIDAS-Experten

Über SIGNIUS

SIGNIUS hat sich der digitalen Transformation der Gesellschaft verschrieben. Als Systemintegrator, Entwickler und Technologieanbieter für verschlüsselungsbasierte Lösungen unterstützt SIGNIUS seine Kunden dabei, die Herausforderungen der Digitalisierung zu meistern und ihre wirtschaftlichen Potentiale zu realisieren.

Über Utimaco

UTIMACO ist ein globaler Plattformanbieter von vertrauenswürdigen Cybersecurity- und Compliance-Lösungen und -Dienstleistungen mit Sitz in Aachen (Deutschland) und Campbell, CA (USA).

UTIMACO entwickelt On-Premises- und Cloud-basierte Hardware-Sicherheitsmodule, Lösungen für Schlüsselmanagement, Datenschutz und Identitätsmanagement sowie Data Intelligence-Lösungen für regulierte kritische Infrastrukturen und öffentliche Warnsysteme. UTIMACO ist einer der weltweit führenden Hersteller in seinen wichtigsten Marktsegmenten.

www.utimaco.com

https://signius.de **connect@signius.eu** **+48 61 415 22 12**