DATENBLATT **proNEXT Signature Activation Module**

QSCD für eIDAS-Fernsignatur

- ✓ QSCD als elementarer Baustein für Fernsignaturlösungen
- ✓ Fernsignatur als benutzerfreundliche Form der elektronischen Signatur
- ✓ Einfache Integration der Fernsignatur in spezielle Prozesse für Vertrauensdiensteanbieter (VDAs)
- ✓ Cloudbasierte, standortunabhängige Anwendung – senkt die Einstiegshürde für VDAs in den Fernsignaturmarkt

Digitale Signatur aus der Cloud

Die Fernsignatur, auch Remote Signature genannt, ermöglicht die Anbringung einer fortgeschrittenen oder qualifizierten elektronischen Signatur ohne Signaturkarte und ohne spezielle Software direkt aus dem Browser heraus. Eine vorherige Identitätsprüfung ist dabei vorgeschrieben. Der Aufenthaltsort – ob Arbeitsplatz oder Homeoffice – spielt dabei keine Rolle, der Signaturprozess kann von unterwegs auf mobilen Endgeräten vorgenommen werden. Vor allem bei Vertragsangelegenheiten, welche zwingend eine Signatur erfordern, aber auch bei Verträgen, die von mehreren Personen unterzeichnet werden müssen, ist diese Art der Fernsignatur empfehlenswert und stellt eine zeitliche Erleichterung dar. Die Abbruchraten von Vertragsunterzeichnungen sinken somit enorm.

Abbildung oben: CryptoServer CP5 von utimaco, Eigentum & copyright: utimaco

Herausforderung

Mit der seit 2016 gültigen eIDAS-Verordnung wurden grundlegende und bindende Rahmenbedingungen geschaffen, um elektronische Kommunikation in rechtsverbindlicher Form europaweit zu ermöglichen. Insbesondere in der höchsten Form, also den qualifizierten Ausprägungen von Zertifikaten und Siegeln, sind konkrete Sicherheitsanforderungen an VDAs formuliert, die einerseits Anwendungsformen ermöglichen, andererseits aber die Verantwortung der VDAs erhöhen.

Daher sind VDAs verpflichtet, die Umsetzung dieser Anforderungen für den Betrieb im qualifizierten Umfeld und der dabei verwendeten Lösungskomponenten zur Erzeugung von qualifizierten Signaturen und Zeitstempeln aber auch Validierungs- und Aufbewahrungsdiensten nachzuweisen.

ETSI Signature Creation Protocols & Policy Requirements

→ *CEN Standards for remote signing systems*:

- EN 419 241 1: Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements
- EN 419 241 2: Trustworthy Systems Supporting Server Signing - Part 2: Protection profile for QSCD for Server Signing
- EN 419 221 5: Protection Profiles for TSP cryptographic modules – Part 5: cryptographic module for Trust Services
- TS 119 431 : Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1-2
- TS 119432: Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation

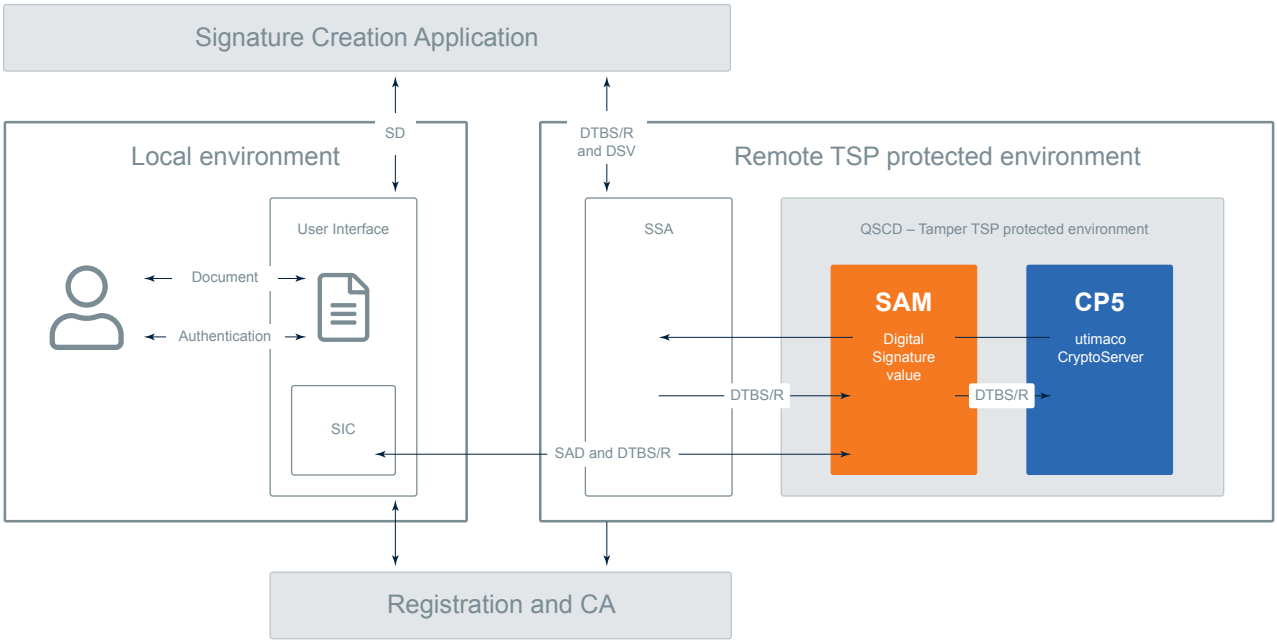
Deutliche Vorteile für Anwender, die rechtsverbindliche digitale Prozesse verwenden wollen, ergeben sich dank eIDAS aus der Nutzung der Fernsignatur, welche damit zu einem wesentlichen Enabler zur Verbreitung der elektronischen Signatur wird. Allerdings weist die Fernsignatur den VDAs auch eine neue Rolle zu, denn ab jetzt stellt er zusätzliche Infrastruktur für den Signaturprozess zur Verfügung. Das dafür notwendige QSCD liegt in seinem Verantwortungsbereich, wird über vollständig neue Technologiekomponenten genutzt und kann sehr flexibel in Anwenderprozesse eingebunden werden.

DATENBLATT **proNEXT Signature Activation Module**

QSCD für eIDAS-Fernsignatur

Lösung

Vertrauensdienstanbieter, die einen Fernsignaturdienst anbieten möchten, müssen sicherstellen, dass der Signaturschlüssel des Unterzeichners ausschließlich unter dessen alleiniger Kontrolle und auch nur für den beabsichtigten Zweck verwendet wird. Das System für diese Art von Diensten besteht aus einer lokalen und einer entfernten Umgebung. Der Unterzeichner befindet sich in der lokalen Umgebung und interagiert mit der Server Signing Application (SSA) und dem kryptografischen Modul (HSM) in der Remote-Umgebung.



Die Signaturoperation wird mithilfe eines Signaturaktivierungsprotokolls ausgeführt, für das Signaturaktivierungsdaten (SAD) in der lokalen Umgebung bereitgestellt werden müssen. Um sicherzustellen, dass der Unterzeichner die alleinige Kontrolle über seine Signaturschlüssel hat, muss der Signaturvorgang autorisiert werden. Ist dies erfolgreich, wird von einem Signaturaktivierungsmodul (SAM) der Signaturschlüssel innerhalb eines kryptografischen Moduls (HSM) aktiviert. Sowohl das Kryptographiemodul als auch das SAM müssen sich in einer dedizierten, geschützten Umgebung befinden.

Für Fernsignaturlösungen ist also das Zusammenspiel von SAM und HSM als vollständiges QSCD eine zentrale Komponente und von elementarer Bedeutung. Utimaco bietet eine leistungsstarke Kombination aus CryptoServer CP5 und CryptoServer CP5 SDK, mit der die SAM-Firmware in der manipulationsgeschützten Umgebung des HSM ausgeführt werden kann.

Der CryptoServer CP5 SDK ist die ideale Wahl für Entwickler solcher „internen SAMs“ und VDAs, welche eine solche Serversignaturlösung betreiben.

Fazit

Für VDAs ist es existentiell wichtig, die eingesetzten Technologiekomponenten hinsichtlich der Konformität zu den ETSI-Normen zu prüfen und auszuwählen. Die ETSI Konformität der Komponenten von utimaco und procilon wurden vom TÜV IT bestätigt und zertifiziert. Die leistungsstarke Kombination aus Hard- und Software-Komponenten von utimaco und procilon ermöglicht die elektronische Unterschrift mittels qualifizierter Signatur in Echtzeit. Im Rahmen eines Pilotprojektes wurde diese Fernsignaturlösung bereits getestet und genießt derzeit ein Alleinstellungsmerkmal auf dem Markt.

Kontakt

procilon GmbH
Leipziger Straße 110
04425 Taucha

+49 342 98 48 78-31
anfrage@procilon.de
www.procilon.de

copyright by procilon GmbH | Alle Warenzeichen gehören den jeweiligen Eigentümern. | Technische Änderungen und Irrtümer vorbehalten.