Als führender Vertrauensdiensteanbieter in Europa ermöglichen wir die innovativsten, digitalen Geschäftsmodelle.

White Paper

Vorgehen als Siegel Partner

Swisscom Trust Services

Swisscom Trust Services

Inhaltsverzeichnis

Regulatorische Situation

Geregelte Siegel nach ZertES (Schweiz) und qualifizierte Siegel nach eIDAS (EU) können auch im Rahmen einer Fernsignatur ausgegeben werden. Die Konformitätsbewertungsstellen in Österreich für Swisscom IT Services Finance S.E. und die Zertifizierungsstelle in der Schweiz für Swisscom (Schweiz) AG verlassen sich hierbei auf eine Prüfung nach der europäischen Norm für Fernsignaturen EN 419241. Diese sieht das sogenannte „SCAL2" Verfahren (Sole Control Assurance Level, also Alleinige Kontrolle Sicherheitsniveau) vor, welches eine 2 Faktor Authentisierung verlangt. Für fortgeschrittene Siegel würde „SCAL1" also eine 1-Faktor Authentisierung ausreichen, z.B. der Besitz. Insofern können Siegel per Fernsignatur dadurch ausgestellt werden, dass eine TLS Verbindung zwischen der signierenden Organisation und Swisscom hergestellt wird, die signierende Organisation ist dann im Besitz der privaten Schlüssels zum öffentlichen Schlüssel im TLS Zertifikat. Für Stufe qualifiziert (EU), bzw. geregelt (CH) reicht das nicht mehr aus. Hier müsste beispielsweise auch der Faktor „Wissen" dazu kommen oder „Sein" (Biometrie). Z.B. könnte eine Freigabe dadurch geschehen, dass ein Vertreter der Organisation den privaten Schlüssel noch explizit freigibt mittels Passwort, biometrischem Merkmal, etc.

Verfahren für den zweiten Faktor

Swisscom hat ein gemäss CP/CPS zugelassene Vorgehensweise für die Ausstellung von Siegeln:
«Die Zertifikatausstellung läuft folgendermassen ab:

- Es wird sichergestellt, dass ein HSM eingesetzt wird,
- von Swisscom wird ein Zertifikat der gewünschten Klasse ausgestellt,
- das Zertifikat und der zugehörige kryptografische Schlüssel werden entweder
    - im Trust Center hinterlegt und das bei der Identifikation eingelieferte SSL/TLS-Client-Zertifikat wird mit dem zugehörigen Benutzerkonto verknüpft, so dass ausschliesslich durch den Besitz des zugehörigen privaten Schlüssels die Erstellung von Siegeln mittels Fernzugriff möglich ist (Signaturerstellungsdaten) oder
    - beim Kunden im HSM aufbewahrt, nachdem Swisscom sich versichert hat, dass der Kunde die erforderlichen Vorgaben einhält,
- die Zertifikatsinhaberin wird über die Bereitstellung informiert.»

Konkret heisst es dann weiter zur Authentifizierung:
„Die Registrierung und Nutzung der Authentisierungsmittel muss mit einem vom Antragssteller beschriebenen Verfahren durchgeführt werden, das von Swisscom zugelassen ist und der in [CEN/TS 419 241] beschriebenen Stufe 2 (Sole Control Assurance Level 2) entspricht."

Damit können Partner in Form eines kleinen Konzeptes darlegen, wie sie die SCAL2 Anforderungen einhalten können.

Ein Beispiel könnte eine HSM oder eine Cloud HSM mit Zugriff vor Ort beim Kunden sein, bei der in einer gemeinsamen Zeremonie das Schlüsselpaar erzeugt wird und damit auch das TLS Zertifikat, wobei der private Schlüssel unter Beisein eines geprüften Vertreters der Organisation in der HSM eingelagert wird. Damit weiterhin Batchprozesse mit Versiegelung möglich sind, empfiehlt sich dann eine z.B. zeitliche befristete Freigabe des privaten Schlüssels.

Anforderungen an das Verfahren

Der Partner sollte ein Lösungskonzept erstellen, in dem er folgende Punkte beschreibt:

- Beschreibung der Lösung und des Prozessablaufes. Hier ist wichtig, wie sichergestellt werden kann, das nur der Vertreter der Organisation letztendlich den TLS Kanal beeinflussen kann und nicht ein Dritter.
- Konformität der verwendeten Hardware oder Cloudlösung (z.B. HSM nach FIPS Schutzlevel oder vergleichbar)
- Nachweis der Zuständigkeiten und Kompetenzen der Rolleninhaber in dem Prozess. Sofern der Prozess vollständig automatisiert ist (z.B. Freigabe direkt durch den Verantwortlichen der Organisation) können hier ggfs. keine weiteren Rollen existieren. Sollte hingegen eine gemeinsame Zeremonie stattfinden, gibt es ggfs. Personen, die den Schlüssel erzeugen, Personen, die das Protokoll führen etc.
- Wie werden die Personen in Ihren Rollen regelmässig geschult?

Das Verfahren ist dann bei Swisscom zur Freigabe einzureichen.

Weiterer Ablauf

Der interessierte Partner, der zukünftig für Swisscom Siegelanwendungen verkaufen möchte sollte initial einen «Vertrag für die Bereitstellung einer Siegellösung» abschliessen, der die technische Lösung zur Aufbewahrung privater Schlüssel sowie die Vertretungsbefugnis zur Bereitstellung qualifizierter bzw. geregelter Siegel mit dieser Lösung regelt. Im Vertrag wird auf das zuvor genannte und freigegebene Konzept verwiesen.

Nach Freigabe des Verfahrens sind bei jedem Siegelprojekt folgende Prozessschritte zu beachten:

- Der Antragsteller (Endkunde), d.h. sein berechtigter und im Antrag benannter Vertreter, sollte zunächst mit der RA-App identifiziert werden. Er kann dann über eine Swisscom Signaturplattform oder eine vom Swisscom Partner betriebene Signaturplattform die notwendigen Dokumente unterzeichnen, insbesondere den Antrag und die Konfigurations- und Annahmeerklärung. Hierzu ist die Checkliste in der Bestellung durch den Partner zu beachten, da das Gesetz sehr viele Fallunterscheidungen spezifiziert und auch notwendige Beigaben (z.B. Handelsregisterauszüge) und auch die Form dazu (z.B. Beglaubigung) beachtet werden müssen.
- Swisscom prüft dann die Organisation, die Berechtigung des Vertreters (z.B. laut Registereintrag oder einer allgemeinen Vollmachtserteilung, die durch einen im Register notifizierten Vertreter der Organisation unterzeichnet wurde) und die beigefügten Dokumente und Urkunden und gibt seine Freigabe für das Aufsetzen einer Fernsignatur.
- Sofern das Lösungsverfahren eine gemeinsame Zeremonie der Schlüsselerzeugung vorsieht, sollte Swisscom bei der ersten Zeremonie beiwohnen. Siehe weitere Hinweise zu so einer Zeremonie weiter unten.
- Am Ende des Aufschaltverfahrens sollte Swisscom vom Antragsteller direkt ein TLS Zertifikat erhalten, mit dem die Kommunikation zur Fernsignatur und zur Beantragung der Signatur abgesichert wird.
- Basierend auf dem Zertifikat teilt Swisscom dem Antragsteller die ClaimedID mit.

Zeremonie

Für den Fall dass eine automatisierte Lösung basierend auf der Identifikation durch die RA-App und z.B. einer damit erstellten QES nicht möglich ist, muss ggfs. der private Schlüssel und das Zertifikat in einer protokollierten Zeremonie erzeugt und sicher abgelegt werden.

Bei dieser Zeremonie sollte der Antragsteller, also der im Zertifikatsantrag benannte Vertreter der Organisation, der befugte Vertreter des Partners sowie ggfs. der Betreiber der Teilnehmerapplikation oder zumindest der Zugriffssteuerung innerhalb der Teilnehmerapplikation zugegen sein. Ggfs. wird die Zugriffssteuerung auch vom Partner selber betrieben, aber auch dann kann es verschiedene Rollen geben: der Techniker, der z.B. ein Schlüsselpaar generiert und der befugte Vertreter, der protokolliert.

Als Abschluss der Zeremonie sollte von allen Beteiligten unterzeichnet ein Protokoll vorliegen, welches folgendes beinhaltet:

- Schritte (technisch), die durchgeführt wurden damit gemäss freigegebenen SCAL2 Lösungskonzept die Zuordnung des Zugriffsmittel (private key der SSL Verbindung) zum identifizierten Antragsteller gewährleistet ist.
- Gerätebezeichnung des kryptographischen Moduls, SW Stand Version
- Konformität der eingesetzten Lösung (muss den Anforderungen entsprechen, welches vorher im Lösungskonzept vorgelegt und freigegeben wurde)
- Teilnehmer (geprüfter Identitätsnachweis sollte vorgelegt werden, also ausgewiesen durch Pass/ID)
- Unterschriften

Das Protokoll sollte postalisch oder eingescannt und vom befugten Vertreter des Partners mit QES unterzeichnet bei Swisscom eingeliefert werden.
Wie bereits oben erwähnt sollte zumindest die erste oder die ersten Zeremonie(n) gemeinsam mit Swisscom durchgeführt werden. (Training by doing)

Für weitere Auskünfte stehen wir gerne zur Verfügung:

Swisscom Trust Services AG
Sales Support

Konradstrasse 12
8005 Zürich / Schweiz

https://trustservices.swisscom.com

Swisscom Trust Services