

Zentrale Signaturdienste revolutionieren die SuisseID

Das Schweizerische Signaturgesetz regelt die Gleichstellung der elektronischen Signatur mit der eigenhändigen Unterschrift. Am 1. August 2011 traten die überarbeitete Verordnung zum Signaturgesetz sowie die technischen und administrativen Vorschriften in Kraft, welche neben Smartcards neu auch zentrale Signaturdienste für die Erstellung von elektronischen Signaturen ermöglichen. Die neuen Möglichkeiten werden den Einsatz der SuisseID revolutionieren und erstmals im nationalen Projekt Terravis angewendet.

Autor und Referent



René G. Eberhard

CEO keyon AG

eberhard@keyon.ch
www.keyon.ch

Referent



Fabrizio Pescosolido

SIX Securities Services, Head of
Division Customer Relations

Fabrizio.Pescosolido@six-group.com

Vortrag 11. Oktober 2011

**C8: Cloud Signature in
Terravis, 12:00 Uhr**

Neue Gesetzesgrundlage

Das Bundesgesetz über Zertifizierungsdienste im Bereich der elektronischen Signatur (SR 943.03, ZertES) fordert, dass qualifizierte elektronische Signaturen nur mit Mitteln erzeugt werden können, die die Inhaberin oder der Inhaber unter ihrer oder seiner alleinigen Kontrolle halten kann (Art. 2 Bst. b Ziff. 3 ZertES). Zudem muss der Signaturschlüssel von der rechtmässigen Inhaberin oder vom rechtmässigen Inhaber vor der missbräuchlichen Verwendung durch andere verlässlich geschützt werden (Art. 6 Abs. 2 Bst. c 2 ZertES).

Bisher durfte nach Art. 11 Abs. 1 VZertES die Inhaberin oder der Inhaber eines qualifizierten Zertifikats die Signaturerstellungseinheit keiner anderen Person anvertrauen. Sie oder er musste diese auf sich tragen oder wegschliessen. Die bisherigen gesetzlichen Vorgaben waren ausschliesslich auf die Verwendung von tragbaren Signaturerstellungseinheiten wie Smartcards oder USB Tokens abgestimmt.

Zentrale Signaturdienste im Gesetz verankert

Seit vielen Jahren existieren bereits sichere technische Lösungen für die Bereitstellung von sicheren Signaturerstellungseinheiten, welche die Anforderungen der ZertES erfüllen und für zentralisierte Signaturdienste eingesetzt werden könnten. Hierbei werden die Signaturschlüssel der Inhaberin oder des Inhabers in der gesicherten Infrastruktur eines Unternehmens oder eines vertrauenswürdigen Dritten gespeichert und verwendet. Die Inhaberin oder der Inhaber identifizieren und authentisieren sich sicher gegenüber dem zentralen Signaturdienst und erhalten so Zugriff auf die entsprechenden Signaturschlüssel.

Um dieser Entwicklung Rechnung zu tragen, wurde der Art. 11 Abs. 1 VZertES sowie die entsprechenden technischen und administrativen Vorschriften (TAV ZertES) angepasst. Die neuen Bestimmungen wurden per 1. August 2011 in Kraft gesetzt und ermöglichen den Einsatz von zentralen Signaturdiensten im Rahmen der ZertES resp. SuisseID.

Hemmschwelle Smartcard

Elektronische Signaturen gewinnen mehr und mehr an Bedeutung. Grund hierfür sind laufende Ergänzungen gesetzlicher Bestimmungen, die den elektronischen Datenverkehr fördern. Unternehmen profitieren von dieser Entwicklung in vielerlei Hinsicht. Sie erhalten Rechtssicherheit im elektronischen Geschäftsverkehr, können ihre Prozesse optimieren und dadurch Kosten sparen.

Die aufwändigen organisatorischen und technischen Prozesse und Abhängigkeiten im Zusammenhang mit Smartcards haben den Einsatz von elektronischen Signaturen in Unternehmen bisher wenig gefördert.

▪ Verteil- und Verwaltungsprozesse

Neue Standard- und Notfallprozesse im Zusammenhang mit der Verteilung und Verwaltung der Smartcards und der entsprechenden PIN Briefe mussten umgesetzt werden. Problematisch waren vor allem Prozesse im Zusammenhang mit der Erneuerung von Zertifikaten, verlorengegangenen oder gestohlenen Smartcards.

▪ Technische Installation

Auf den Arbeitsstationen der Nutzer musste eine Treibersoftware installiert werden, welche die Smartcard ansprechen konnte. Die Installation solcher Treiber verlief nicht immer problemlos, da es verschiedene Abhängigkeiten zum Betriebssystem oder bereits bestehenden Smartcard Installationen gab.

Zudem mussten die eigentlichen Signaturapplikationen auf den Arbeitsstationen installiert werden. Allfällig etablierte Workflowprozesse mussten unterbrochen werden und der Mitarbeiter musste in der Handhabung der Smartcard und der Signaturapplikation geschult werden.

▪ Keine Kontrolle

ZertES konforme Zertifikate werden nur für natürliche Personen ausgestellt. Falls ZertES konforme Signaturen im Umfeld von Unternehmen eingesetzt werden, ist es üblich oder gar zwingend notwendig, dass der Name des Unternehmens im Organisationsfeld des Zertifikats festgehalten wird. Hiermit bestätigt das Unternehmen, dass der Mitarbeiter in einer Beziehung zur Organisation steht (Art. 5. Abs. 2 VZertES). Zudem verpflichtet sich das Unternehmen im Rahmen der SuisseID (Spezifikation V1.3, Kapitel 2.3.4), das Zertifikat des Mitarbeiters zu revozieren, falls der Mitarbeiter beispielsweise das Unternehmen verlässt oder dieser in einer anderen Rolle tätig ist, als im Zertifikat vermerkt. Diese Anforderung muss in den etablierten HR Prozessen der Unternehmen entsprechend berücksichtigt werden.

Da die Organisation für jedermann sichtbar im Zertifikat eingetragen ist, möchte sie sicherstellen, dass solche elektronischen Signaturen nur im Kontext des Unternehmens und nicht für allerlei private Zwecke eingesetzt werden können. Mit Smartcards konnte dies bisher nur über Wei-

sungen, nicht aber technisch sichergestellt werden.



Zentrale Signaturdienste

Seit dem 1. August 2011 besteht die Möglichkeit, zentrale Signaturdienste innerhalb der eigenen Organisation oder bei vertrauenswürdigen Dritten sicher zu betreiben.

Ein zentraler Signaturdienst stellt hierbei Schnittstellen zur Verfügung, über welche Dokumente bereitgestellt werden, die elektronisch signiert oder validiert werden sollen. Benutzer verwenden hierfür beispielsweise einen Web-Browser während Applikationen eine SOAP Schnittstelle verwenden. Über solche Schnittstellen können qualifizierte elektronische Signaturen direkt in etablierten Workflows erstellt und validiert werden.

Ein wesentliches Element des zentralen Signaturdienstes ist die sichere Verwaltung der Signaturschlüssel sowie deren Zuordnung zu den jeweiligen Benutzern. Die Signaturschlüssel werden sicher und zentral in einem Hardware Security Module (HSM) generiert und verwaltet. Die Authentisierung der Benutzer erfolgt über einen 2-Faktor Identifizierungs- und

Authentifizierungsmechanismus
(TAV ZertES, Kapitel 3.3.3 b)

Zahlreiche Vorteile

Zentrale Signaturdienste bieten neben dem eigentlichen Signieren und Validieren von Dokumenten weitere Vorteile an. Folgend ein paar Beispiele:

▪ **Zentrale Verwaltung**

Benutzer und Signaturschlüssel können zentral verwaltet werden. Zertifikatsbezogene Standard-, Erneuerungs- und Notfallprozesse können auf der Basis etablierter Unternehmensprozesse umgesetzt werden.

▪ **Kontrollierte Verwendung**

Der Zugriff auf die Signaturschlüssel kann eingeschränkt und kontrolliert werden. Beispielsweise kann ein bestimmter Signaturschlüssel nur innerhalb einer bestimmten Applikation verwendet werden. Zudem kann, für einen bestimmten Zeitraum, jedes signierte Dokument zentral für Audit-Zwecke gespeichert werden.

▪ **Kontrollierte Prüfung**

Zentrale Signaturdienste können zur Prüfung elektronisch signierter Dokumente verwendet werden. Das Ergebnis der Prüfung wird verständlich dargestellt und in einem Prüfprotokoll festgehalten. Weiter können Eigenschaften wie beispielsweise Unterschriftenberechtigungen, Rollen oder spezifische Verantwortlichkeiten angezeigt werden.

▪ **Konvertierung**

Bevor Dokumente signiert werden, können diese zentral in ein einheitliches Format (beispielsweise PDF/A) konvertiert werden.

Erster praktischer Einsatz bei Terravis

Terravis ist das erste schweizweite Auskunftsportal, über den institutionelle Kunden Zugang zu topaktuellen Informationen aus dem Grundbuch und der Amtlichen Vermessung erhalten. Ab 2012 wird Terravis als Drehscheibe den elektronischen Geschäftsverkehr zwischen den Grundbuchämtern, den Notaren, den Banken und Pensionskassen ermöglichen.

Verschiedene elektronische Geschäftsfälle wie beispielsweise die Grundbuchanmeldung verlangen zwingend qualifizierte elektronische Signaturen auf der Basis der SuisseID / ZertES.

Um die Verwendung der qualifizierten elektronischen Signatur zu vereinfachen, stellt Terravis einen zentralen Signaturdienst auf der Basis von keyon / trueSign bereit, der die zuvor aufgeführten Eigenschaften aufweist und von den institutionellen Kunden genutzt werden kann.

Im Praxisreferat vom 11. Oktober stellen Fabrizio Pescosolido und René Eberhard auf die Lösung Terravis mit dem zentralen Signaturdienst vor.