

Die elektronische SuisseID – eine Idée Suisse

Die SuisseID ist ein elektronischer Identitätsnachweis, der zu sicheren Authentisierung gegenüber Onlineapplikationen oder zum rechtsverbindlichen Unterschreiben von elektronischen Dokumenten genutzt werden kann. René Eberhard



René Eberhard

ist CEO der Keyon AG und arbeitete als Beauftragter des SECO aktiv an der Spezifikation der SuisseID mit.
eberhard@keyon.ch

Die SuisseID soll dem elektronischen Geschäfts- und Behördenverkehr in der Schweiz zum Durchbruch verhelfen. Sie ist eine signaturgesetzkonforme Smartcard oder ein USB-Token mit einem qualifizierten Signaturzertifikat (SuisseID QC) nach dem Signaturgesetz ZertES und einem standardisierten Authentisierungszertifikat (SuisseID IAC). Das ZertES regelt die technischen und organisatorischen Rahmenbedingungen im Zusammenhang mit rechtsverbindlichen elektronischen Unterschriften. Entsprechend unterliegt das ZertES-konforme Signaturzertifikat der SuisseID diesen Vorgaben, die im Rahmen der SuisseID-Spezifikation partiell, innerhalb der Möglichkeiten des Signaturgesetzes, erweitert wurden. Ein analoges Gesetz im Bereich der sicheren Authentisierung gegenüber Onlineapplikationen fehlt.

Die Qualität einer elektronischen Identität ist abhängig von der Generierung und Verwaltung des elektronischen Schlüsselpaares (Private- und Public Key) sowie der Registrierung der Person und der Verknüpfung ihrer Personalien mit dem öffentlichen Schlüssel im Zertifikat. Beide zuvor genannten Eigenschaften erfüllen im Zusammenhang mit dem qualifizierten Signaturzertifikat höchste Anforderungen. Da das Authentisierungszertifikat die identischen Personenangaben enthält wie das qualifizierte Signaturzertifikat und der Verpflichtung der Zertifikatsanbieter, für die Ausgabe und Verwaltung vom Authentisierungszertifikat die gleichen organisatorischen und operativen Verfahren anzuwenden wie für das qualifizierte Signaturzertifikat, hat das Authentisierungszertifikat eine vergleichbare Qualität wie das gesetzlich geregelte qualifizierte Signaturzertifikat.

Eine Nummer, eine Person, ein Passwort

Eine SuisseID hat eine maximale Gültigkeitsdauer von drei Jahren. Danach muss sie erneuert werden. Zudem sind per-

sonenspezifische Angaben im Zertifikat nicht zwingend eindeutig. Im Minimum muss das Zertifikat den Namen und Vornamen des Zertifikatsinhabers beinhalten. Damit Onlineapplikationen ihre Nutzer eindeutig und unabhängig vom Lebenszyklus eines Zertifikats authentifizieren können, wurde die SuisseID-Nummer als integralen Bestandteil eines Zertifikats eingeführt. Sie ist eine eindeutige, sechzehnstellige Nummer, die bei der Ausgabe eines Zertifikats einer spezifischen Person zugeordnet wird. Die SuisseID und somit die entsprechende SuisseID-Nummer kann bei mehreren Onlineapplikationen genutzt werden. Der Zertifikatsinhaber muss sich so keine applikationsspezifischen Passwörter mehr merken.

Um eine Profilierung von Nutzern auf der Basis der SuisseID-Nummer zu vermeiden, kann eine Person mehrere Zertifikate mit unterschiedlichen SuisseID-Nummern beantragen.

Identity Provider

Aus Gründen des Datenschutzes wurden die Angaben zu einer Person, die im Zertifikat enthalten sein müssen, auf ein Minimum beschränkt. Aktuell müssen lediglich der Name und der Vorname sowie ihre SuisseID-Nummer enthalten sein. Weitere personenbezogene Attribute sind optional.

Verschiedene Onlineapplikationen haben die Anforderung, zusätzliche Informationen über den Zertifikatsinhaber einzufordern. Beispielsweise muss ein Onlineanbieter von alkoholischen Getränken oder elektronischen Spielen das Alter seines Kunden kennen. Ebenfalls kann die Funktion respektive die Zeichnungsberechtigung gemäss Handelsregister von Interesse sein.

Personenbezogene Attribute, die nicht im Zertifikat enthalten sind, können vom Zertifikatsinhaber unter Einbezug des SuisseID Identity Providers an die Onlineapplikation übermittelt werden. Die Übermittlung der zusätzlichen Attribute erfolgt unter vollständiger Kontrolle des Zertifikatsinhabers und nur durch seine jeweilige, explizite Zustimmung.

Corporate SuisseID

Die SuisseID kann im Corporate-Umfeld im Bereich der Authentisierung von natürlichen Personen und im Zusammenhang mit rechtsgültigen elektronischen Signaturen genutzt werden. Die SuisseID unterstützt keine Verschlüsselung von Daten oder Authentisierung von Systemen (z.B. 802.1X). Diese Anforderungen müssen über zusätzliche Zertifikate abgedeckt werden, die aufgrund der damit verbundenen Prozesse idealerweise von einer Corporate PKI ausgegeben werden.

Integration der SuisseID

Im Rahmen des SuisseID-Projekts werden interessierten Anbietern von Onlineapplikationen Toolkits bereitgestellt, die eine einfache Integration der SuisseID-Funktionalitäten in die entsprechenden Applikationen ermöglicht. Bereits existieren auch schon kommerzielle Applikationen und Module, die es Onlineapplikationen ermöglichen, die SuisseID-Funktionalitäten einfach zu integrieren.

Ein Blick ins nahe Ausland zeigt, dass Deutschland und Österreich ähnliche Ziele verfolgen wie die Schweiz. Die «Bürgerkarte» aus Österreich basiert auf einem vergleich-



Die Personenangaben, die im Zertifikat enthalten sein müssen, sind auf ein Minimum beschränkt.

baren Konzept wie die SuisseID, jedoch ohne den Identity Provider für die Bereitstellung von zusätzlichen Personenattributen. Die «Bürgerkarte» beinhaltet zwei X.509-Zertifikate für die qualifizierte elektronische Signatur und für die einfache elektronische Signatur. Der «elektronische Personalausweis» aus Deutschland folgt dem Standard der European Citizen Card und beinhaltet, analog zur SuisseID, zwei X.509-Zertifikate für die qualifizierte Signatur und den elektronischen Identitätsnachweis (Authentisierung). Zusätzliche Attribute werden statisch auf dem elektronischen Personalausweis gespeichert. Diese können nur von speziell zertifizierten Applikationen unter expliziter Einwilligung des Zertifikatsinhabers ausgelesen werden. Darüber hinaus ist der elektronische Personalausweis ein sicheres Reisedokument für hoheitliche Kontrollen im In- und Ausland.

Es liegt nun an den Anbietern von Onlineapplikationen, die Funktionalitäten der SuisseID entsprechend zu integrieren und so zum Erfolg der SuisseID beizutragen. ■

Merkmale der SuisseID

- Die SuisseID ist eine signaturgesetzkonforme Smartcard oder ein USB-Token mit einem ZertES-konformen Signatur- und standardisierten Authentisierungszertifikat.
- Die Zertifikate enthalten eine eindeutige SuisseID-Nummer, die dem Zertifikatsinhaber, einer natürlichen Person, zugeordnet ist.
- Personenspezifische Merkmale wie beispielsweise das Geburtsdatum können, mit jeweils expliziter Freigabe durch den Zertifikatsinhaber, standardisiert und sicher an Onlineapplikationen übermittelt werden.

Weitere Informationen unter: www.suisseid.ch