

Eine Nummer, eine Person, ein Passwort = SuisseID

Die SuisseID ist ein elektronischer Identitätsnachweis, der zur sicheren Authentisierung gegenüber Online-Applikationen oder zum rechtsverbindlichen Unterschreiben von elektronischen Dokumenten genutzt werden kann. Sie ist ab Mai 2010 erhältlich und wird durch das Staatssekretariat für Wirtschaft (SECO) gefördert.

Die SuisseID soll dem elektronischen Geschäfts- und Behördenverkehr in der Schweiz zum Durchbruch verhelfen. Bisher realisierten Anbieter von Online-Applikationen eigene Authentisierungsmechanismen, da verbreitete und standardisierte Identifikationsmerkmale fehlten. Auf der anderen Seite setzten sich keine standardisierten Identifikationsmerkmale durch, da zu wenig Online-Applikationen bereitstanden, die ein standardisiertes Authentisierungsverfahren unterstützten. Mit der SuisseID, dem ersten standardisierten Produkt für einen sicheren elektronischen Identitätsnachweis in der Schweiz, soll die Huhn-Ei-Problematik durchbrochen werden. Die SuisseID ist eine signaturgesetzkonforme Smartcard oder ein USB-Token mit einem qualifizierten Signaturzertifikat (SuisseID QC) nach ZertES und einem standardisierten Authentisierungszertifikat (SuisseID IAC).

Solides Fundament

Das Signaturgesetz (ZertES) regelt die technischen und organisatorischen Rahmenbedingungen im Zusammenhang mit rechtsverbindlichen elektronischen Unterschriften. Entsprechend unterliegt das ZertES konforme Signaturzertifikat der SuisseID

diesen Vorgaben, welche im Rahmen der SuisseID-Spezifikation partiell, innerhalb der Möglichkeiten des Signaturgesetzes, erweitert wurden. Ein analoges Gesetz im Bereich der sicheren Authentisierung gegenüber Online-Applikationen fehlt.

Die Qualität einer elektronischen Identität ist abhängig von der Generierung und Verwaltung des elektronischen Schlüsselpaares (Private und Public Key) sowie Registrierung der Person und der Verknüpfung seiner Personalien mit dem öffentlichen Schlüssel im Zertifikat. Beide zuvor genannten Eigenschaften erfüllen im Zusammenhang mit dem qualifizierten Signaturzertifikat höchste Anforderungen.

3 Jahre gültig

Da das Authentisierungszertifikat die identischen Personenangaben enthält wie das qualifizierte Signaturzertifikat und die 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 qualifi-

zierte Signaturzertifikat. Eine SuisseID hat eine maximale Gültigkeitsdauer von drei Jahren. Danach muss sie erneuert werden. Zudem sind personenspezifische Angaben im Zertifikat nicht zwingend eindeutig. Im Minimum muss das Zertifikat den Namen und Vornamen des Zertifikatsinhabers beinhalten.

Damit Online-Applikationen ihre Nutzer eindeutig und unabhängig vom Lebenszyklus eines Zertifikats authentifizieren können, wurde die SuisseID-Nummer als integraler 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 Online-Applikationen 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. Aus gesetzlichen Gründen konnte die neue AHV-Nummer resp. Sozialversiche-



rungsnummer nicht im Umfeld der SuisseID verwendet werden.

Identity Provider

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

Verschiedene Online-Applikationen haben die Anforderung, zusätzliche Informationen über den Zertifikatsinhaber einzufordern. Beispielsweise muss ein Online-Anbieter von alkoholischen Getränken oder elektronischen Spielen das Alter seines Kunden kennen. Ebenfalls kann im Zusammenhang mit elektronischen Signaturen beispielsweise die Funktion resp. die Zeichnungsberechtigung gemäss Handelsregister von Interesse sein. Personenbezogene Attribute, welche nicht im Zertifikat enthalten sind, können vom Zertifikatsinhaber unter Einbezug des SuisseID Identity Providers an die Online-Applikation übermittelt werden. Die Über-

mittlung der zusätzlichen Attribute erfolgt unter vollständiger Kontrolle des Zertifikatsinhabers und nur durch seine jeweilige, explizite Zustimmung. Eine Online-Applikation kann ohne Einbezug des Zertifikatsinhabers keine personenbezogenen Attribute über den SuisseID Identity Provider beziehen.

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, welche aufgrund der damit verbundenen Prozesse idealerweise von einer Corporate PKI ausgegeben werden.

Integration der SuisseID

Im Rahmen des SuisseID-Projekts werden interessierten Anbietern von Online-Applikationen Toolkits bereitgestellt, welche eine einfache Integration der SuisseID-Funktionalitäten in die entsprechenden Applikationen ermöglicht. Bereits existieren auch schon

kommerzielle Applikationen und Module, welche es Online-Applikationen ermöglichen, die SuisseID-Funktionalitäten einfach zu integrieren.

Vergleich mit dem Ausland

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

Fazit

Die SuisseID ist eine pragmatische, auf etablierten und verbreiteten Standards aufbauende Lösung, welche einen sicheren elektronischen Identitätsnachweis ermöglicht. Die Funktionalitäten der SuisseID sind gut dokumentiert und können einfach über die bereitgestellten Toolkits oder kommerzielle Module integriert werden. Es liegt nun an den Anbietern von Online-Applikationen, diese entsprechend zu integrieren und so zum Erfolg der SuisseID beizutragen.



Autor:
René Eberhard ist CEO der Keyon AG und arbeitete als Beauftragter des SECO aktiv an der Spezifikation der SuisseID mit. E-Mail: eberhard@keyon.ch
www.keyon.ch

SuisseID Testzertifikate bereits bei QuoVadis erhältlich

Mit der vom SECO lancierten SuisseID können Privatpersonen und Firmen ihre Geschäfte künftig zeitunabhängig und sicher über das Internet abschliessen. Zudem kann die SuisseID auch von Bürgern zur Erledigung von Amtswegen bzw. zur sicheren Online-Kommunikation mit der öffentlichen Verwaltung verwendet werden.

Vom SECO gefördert

Die SuisseID ist ab Mai 2010 in Form einer Chipkarte oder eines USB-Sticks mit einem qualifizierten Signaturzertifikat und einem standardisierten Authentisierungszertifikat erhältlich. Für die Ausstellung der Zertifikate ist man bei QuoVadis Trustlink Schweiz AG schon jetzt bestens gerüstet.

In enger Zusammenarbeit mit dem renommierten Herausgeber von ID-, Bank- und Kundenkarten, der Firma Trüb AG in Aarau, wird QuoVadis als sehr leistungsfähiger SuisseID-Anbieter sowohl Einzelpersonen wie auch ganze Firmen und Organisationen effizient und kostengünstig beliefern. Speziell beraten und betreuen will QuoVadis künftige SuisseID-Anwendungsanbieter. So können

bei QuoVadis per sofort SuisseID-Zertifikate zu Testzwecken bezogen werden.

«Dieses kostenlose Angebot richtet sich an SuisseID-Anwendungsanbieter, Entwickler, Integratoren und Beratungsunternehmen, welche die SuisseID in ihre Projekte integrieren wollen. Firmen, die sich für die Anwendung der SuisseID interessieren, können sich dem Angebot von QuoVadis ebenfalls anschliessen», erklärt QuoVadis CEO Carl Rosenast.

Die SuisseID schafft eine rechtsverbindliche Verknüpfung zwischen einer natürlichen Person und deren Rollen und Bevollmächtigungen in Unternehmungen und anderen juristischen Körperschaften. Durch einen Entscheid des Bundesrats im August 2009 werden 17 Millionen Schweizerfranken für die subventionierte Erstausgabe der SuisseID an natürliche Personen sowie 4 Millionen für den Aufbau der entsprechenden Infrastruktur zur Verfügung gestellt.

Weitere Informationen dazu finden Sie auf der Website von QuoVadis: www.quovadis.ch



QuoVadis ist ein international akkreditierter Zertifizierungsdienstleister (CSP Certification Service Provider) mit weltweiter Anerkennung (WebTrust). Angeboten werden elektronische Zertifikate nach Schweizerischer (ZertES) und europäischer Gesetzgebung (ETSI). Das QuoVadis Root Zertifikat ist weltweit in allen gängigen Browsern und Betriebssystemen verteilt.

QuoVadis Trustlink Schweiz AG
Teufenerstr. 11, 9000 St.Gallen
Tel. +41 71 272 60 60
info.ch@quovadisglobal.com
www.quovadis.ch



keyon

Corporate PKI = Identity & Access Management
Software Engineering = Legal Archiving = ISMS - ISO 2700X

SuisseID-Enabling von Web-Applikationen

phion

SuisseID Authentication Service for phion airlock

Wir unterstützen Sie bei der Integration der SuisseID und anderen Fragen im Bereich Identity & Access Management

keyon AG
Schlüsselstrasse 6
8645 Jona
Switzerland

Tel: +41 55 220 64 00
Fax: +41 55 220 64 01

www.keyon.ch
info@keyon.ch

1. Name
Muster

2. Vorname
Sandra

3. SuisseID-Nummer
0000-1234-1234-1234