Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Volkswirtschaftsdepartement EVD

Staatssekretariat für Wirtschaft SECO
Kommunikation

Mediendokumentation SuisseID

Datum 13. Januar 2011

Arbeiten der Expertengruppe Sicherheit im Jahr 2010

Ausgangslage
Unter der Leitung des Staatssekretariats für Wirtschaft SECO haben die in der Schweiz gesetzlich anerkannten Zertifizierungsdiensteanbieter gemeinsam mit Vertretern aus der IT-Wirtschaft einen Industriestandard für den elektronischen Identitätsnachweis SuisseID erarbeitet. Dieser Standard ermöglicht sowohl eine rechtsgültige elektronische Signatur wie auch eine sichere Authentifizierung. Seit Mai 2010 ist die SuisseID als Chipkarte oder USB-Token erhältlich, ausgerüstet mit digitalen Zertifikaten für die Authentisierung (IAC)[1] und qualifizierte Signatur (QC)[2].

Arbeit der Expertengruppe
Am 10. September 2010 hat das SECO eine Expertengruppe einberufen. Diese befasst sich mit der Frage, wie sich Risiken im Umgang mit Smartcards vermindern lassen. Im Rahmen eines Expertengutachtens wurde die technische Sicherheit der SuisseID untersucht. Dabei wurde die gesamte Dienstleistungskette der SuisseID bezüglich ihres Verwundbarkeitspotenzials analysiert (vom Benutzer, über das Zertifikat, Lesegerät und Client-PC, bis zur Serverapplikation). Flankierend dazu führte das SECO im November 2010 einen Workshop durch, in dem verschiedene Fragestellungen rund um die Sicherheit der SuisseID diskutiert wurden. 35 Experten aus Wirtschaft, Forschung, Lehre und Verwaltung nahmen an diesem Workshop teil. Die nachfolgend aufgeführten Sicherheitshinweise sind aus diesen Arbeiten entstanden.

Sicherheitshinweise
Unter Berücksichtigung der Tatsache, dass es in vernetzten elektronischen Umgebungen – und damit auch bei Online-Interaktionen, bei denen beliebige Gegenparteien und Intermediäre involviert sein können – keine absolute Sicherheit geben kann, ist es wichtig zu verstehen, dass die Sicherheit der SuisseID von vielen Faktoren abhängt. Zum Beispiel vom Verwendungszweck oder der Frage, wie lukrativ ein bestimmtes Angriffsziel für potenzielle Angreifer ist. Um ein klares Bild davon zu erhalten, welche Schutzmassnahmen angebracht sind, müssen im Einzelfall die Risiken und Auswirkungen betrachtet werden, die mit dem Einsatz der

---

[1] Identification and Authetication Certificate

[2] Qualified Certificate

SuisseID verbunden sind. Da es sich meistens um anwendungsbezogene Grössen handelt, können allgemeine Sicherheitshinweise nur einen Leitfaden darstellen, der eine individuelle Analyse und Bewertung der Risiken sowie geeignete Abwehrmassnahmen nicht ersetzen kann.

Die nachfolgenden Hinweise gehen von der Annahme aus, dass der Computer eines SuisseID Benutzers prinzipiell Sicherheitslücken aufweisen kann, die durch Schadsoftware (Malware) zur Kompromittierung des Computers ausgenutzt und missbraucht werden können.

Hinweise zum allgemeinen Verhalten – Mit der SuisseID soll grundsätzlich so umgegangen werden, wie mit jedem anderen elektronischen Zugangsmittel (z.B. Bankkarte). Die SuisseID muss stets sicher aufbewahrt und darf nie unbeaufsichtigt zurückgelassen werden. Die geheime PIN darf nie an Dritte weitergegeben werden. Ebenso darf sie nicht aufgeschrieben werden, erst recht nicht auf der Karte. Sollte die SuisseID kompromittiert werden oder abhanden kommen, ist sie sofort zu revozieren, d.h. für ungültig erklären zu lassen. Wie dazu vorzugehen ist, ist auf den Internetseiten des SuisseID-Lieferanten und in den Unterlagen ersichtlich, die bei der Auslieferung der SuisseID an den Inhaber abgegeben werden.

Hinweise zum Kartenleser – In vielen Ländern sind Lesegeräte für die Signatur und Authentifizierung im Einsatz, bei denen die PIN über die Computertastatur eingegeben wird (Klasse 1 Leser). Es steht ausser Frage, dass Leser der Klasse 1 gegen technische Angriffe anfälliger sind als Lesegeräte höherer Klassen, z.B. solche mit PIN-Pad und/oder eigenem Display. Dafür sind Klasse 1 Leser einfacher in der Handhabung. Benutzer, die für sich ein höheres Sicherheitsbedürfnis erkennen, können Lesegeräte einer höheren Klasse bei ihrem SuisseID-Lieferanten beziehen.

Hinweise zur elektronischen Unterschrift – Elektronische Unterschriften, wie sie die SuisseID ermöglicht, werden bereits in vielen Ländern eingesetzt. Einmal unterzeichnet, kann ein elektronisches Dokument nicht mehr unerkannt manipuliert oder die Unterschrift gefälscht werden. Eine elektronische Unterschrift sollte nur dann geleistet werden, wenn die dazu eingesetzte Signatursoftware von einer vertrauenswürdigen Stelle stammt und es für den Unterzeichneten nachvollziehbar ist, welche Inhalte effektiv signiert werden. Die Signatursoftware muss dazu alle Inhalte anzeigen und darf nichts unterdrücken. Insbesondere darf sie keine dynamischen Inhalte akzeptieren. Die Sicherheit der Signatursoftware hängt auch von der Sicherheit des Computers ab, auf dem sie installiert und betrieben wird. Besteht Verdacht, dass der Computer kompromittiert ist, darf die SuisseID nicht mehr verwendet werden, weder für die Signatur noch für die Authentisierung (Login).

Hinweise zu den Datenformaten für die Signatur – Grundsätzlich kann jedes elektronische Dokument mit der SuisseID rechtsverbindlich signiert werden. Das Signaturgesetz sieht diesbezüglich keine Einschränkung vor. PDF/A ist ein verbreitetes und geeignetes Format und zugleich das einzige, das von Behörden für elektronische Eingaben akzeptiert werden muss. Es gibt viele Werkzeuge für die Signaturerstellung und -prüfung von PDF-Dokumenten. Da die Sicherheit dieser Werkzeuge wiederum von der des Computers abhängt, gilt auch hier: Besteht Verdacht, dass der Computer kompromittiert ist, darf die SuisseID nicht mehr verwendet werden, weder für die Signatur noch für die Authentisierung (Login).

Hinweise zum Virenschutz – Die SuisseID kann durch Schadsoftware (Malware) nicht kompromittiert werden, sehr wohl aber die Umgebung, in der sie eingesetzt wird. Entsprechend gehört es zu den Sorgfaltspflichten eines Anwenders, dass er seinen Computer mit bekannten und gängigen Massnahmen schützt. Dazu gehören insbesondere Antiviren- und Antispyware-Programme sowie regelmässige Sicherheitsupdates für Betriebssystem, Anwenderprogramme und Daten. Diese Massnahmen bieten einen Grundschutz, der viele bekannte Angriffe unwirksam macht.

Hinweise zum Login auf Webseiten – Das Prinzip, das beim Login mit der SuisseID zum Einsatz kommt, gilt als sehr sicher und stellt eine deutliche Verbesserung gegenüber einem Login mittels Benutzername und Passwort dar. Eine mögliche Gefahr geht aber von der jeweils angewählten Webseite aus. Entsprechend sollte die SuisseID nur auf Webseiten eingesetzt werden, denen man vertraut. Derzeit existiert kein Gütesiegel für Webseiten, die die SuisseID unterstützen (das weit verbreitete Logo "SuisseID LOGIN" dient lediglich der einheitlichen Erkennung). Webseiten mit höherwertigen Serverzertifikaten, in vielen Browsern als grüne Adressanzeige erkennbar, gelten als seriös und vertrauenswürdig, insbesondere weil die Identität der Verantwortlichen bekannt und überprüft ist. Auch hier gilt: Besteht Verdacht, dass der Computer kompromittiert ist, darf die SuisseID nicht mehr verwendet werden, weder für die Signatur noch für die Authentisierung (Login).

Blick in die Zukunft

Auch in Zukunft will das SECO den Dialog mit den Sicherheitsexperten fortführen. Es setzt sich aktiv für eine Verminderung der Risiken beim Einsatz von Informationstechnologien ein und hat die Sicherheit zu einem Schwerpunktthema seiner E-Economy-Aktivitäten gemacht.

Im Verein „Trägerschaft SuisseID“ wurde zudem eine Arbeitsgruppe Sicherheit gebildet. Die Resultate der Untersuchung 2010 werden dort weiter verwertet und die Arbeitsgruppe wird ihre Tätigkeit in diesem Jahr danach ausrichten.

Weitere Informationen zur SuisseID finden Sie unter www.suisseid.ch.