Christian Leupi*

Erste Praxiserfahrungen mit der SuisseID

Stichworte: Inbetriebnahme SuisseID, Umgang mit PIN-Codes, Signieren von E-Mails

Die SuisseID ist mittlerweile lanciert und hat auf Basis der Initiative des SAV in Anwaltskreisen bereits ansehnliche Verbreitung gefunden. Es wäre nun allerdings bedauerlich, wenn die SuisseID – nachdem sie von den Anwältinnen und Anwälten bereits rege bestellt wurde – ihr Dasein ungenutzt in den Schubladen der Schreibtische fristen würde.

Der vorliegende Artikel soll deshalb über die ersten Praxiserfahrungen mit der SuisseID berichten, welche der Autor dieses Artikels als «Testnutzer» des SAV machen konnte. Er möchte den Mitgliedern des SAV einerseits Anregungen für den täglichen Einsatz der SuisseID geben und andererseits denjenigen Kolleginnen und Kollegen, welche bisher dem Thema SuisseID keine Beachtung geschenkt haben, beziehungsweise diesem etwas skeptisch gegenüberstehen, etwas die Angst vor dem Unbekannten nehmen.

Bestellvorgang

Der Bestellvorgang wurde erfreulicherweise seit der Lancierung der SuisseID stetig verbessert und dürfte für alle, welche bereits einmal in einem Onlineshop eingekauft haben, kein Problem darstellen. Die «Beglaubigung» der Identität durch eine Kanzleikollegin oder -kollegen vereinfacht und strafft den Bestellprozess erheblich, kann doch damit der sonst obligatorische Gang zur Gemeinde beziehungsweise Post für die Identifizierung vermieden werden.

Obwohl der Bestellprozess an sich nunmehr ausgereift erscheint, ist aus Anwendersicht eine Detailkritik an den Versandmodalitäten angebracht. Da die SuisseID quasi die elektronische Identität des Anwenders darstellt, wäre sicherlich zu wünschen, dass sowohl die SuisseID als auch die Zugangsdaten mit eingeschriebener Post und nicht mit A-Post versendet werden. Zu überlegen ist, ob der Versand sogar nur gegen persönliche Aushändigung erfolgen sollte, wie dies z.B. Mobilfunkanbieter praktizieren.

Inbetriebnahme

Die Mitteilung der Zugangsinformationen mag den unbedarften Anwender auf den ersten Blick etwas überfordern, ist der Inhalt doch sehr technisch (PIN, PUK, Transport PIN, Revokationspasswort etc.). Hier stellt sich sofort die Frage, welches Sicherheitselement zu welchem Zweck dient und was in welcher Form aufbewahrt werden sollte. Allerdings erschliesst sich der Zweck der einzelnen Sicherheitselemente nun besser, da mittlerweile ein Merkblatt beiliegt, welches die einzelnen Begriffe verständlich erklärt und auch über den sicheren Umgang mit PUK und Revokationspasswort aufklärt.

Die PIN der SuisseID ist vergleichbar mit einer herkömmlichen PIN bei Bankkarten und Ähnlichem. Allerdings ist zu beachten, dass die SuisseID zwei PINs enthält. Eine PIN dient zur Authentifikation, also beispielsweise zum sicheren Login auf Webplattformen. Eine weitere PIN – die Signatur-PIN – ist notwendig, um die digitale Signatur freizugeben, das heisst um das elektronische Dokument zu signieren. Ob es hier tatsächlich – wie vom Anbieter empfohlen – sinnvoll ist, für beide PINs dasselbe Passwort bzw. dieselbe Zahlenkombination zu verwenden, muss aus Sicht des Benutzers in Frage gestellt werden. Der vorsichtige Benutzer setzt wohl eher zwei unterschiedliche PIN ein, was das Missbrauchspotenzial wesentlich verringert.

In der Startphase der Auslieferung der SuisseID tauchten diverse Fragen im Zusammenhang mit der Installation auf, für welche sich nun im Online-Supportbereich des Anbieters die entsprechenden Antworten finden.

Anwendung allgemein

Im Allgemeinen ist bei der täglichen Anwendung nicht ohne weiteres erkennbar, welche dieser beiden PINs wann erforderlich ist, da die Software einheitlich von PIN spricht. Wird die falsche PIN genutzt, so gibt die Software eine Warnung aus, dass nur noch wenige Versuche zur Verfügung stehen. Dies kann beim Benutzer durchaus etwas Nervosität auslösen. In der Regel ist aber zuerst die PIN zu benutzen, welche den Zugriff auf die Zertifikate freigibt und erst im zweiten Schritt die Signatur-PIN. Dies lässt sich auch daran erkennen, dass das zweite Eingabefenster darauf hinweist, dass nun eine digitale Signatur angebracht wird.

Hier schafft die Empfehlung des Anbieters, für beide PINs denselben Code zu benutzen, natürlich Abhilfe. Allerdings ist nicht auszuschliessen, dass dies auf Kosten der Sicherheit geht, da mit Bekanntwerden des einheitlichen Codes die gesamte Anwendung der SuisseID kompromittiert wäre – allerdings immer unter der Voraussetzung, dass zusätzlich physischer Zugriff auf die Karte besteht.

Die Terminologie ist aber kein Problem der SuisseID an sich, sondern eine Frage der softwaremässigen Umsetzung der Signierung. Es wäre zu wünschen, dass die Anwendungen den Benutzer klar darauf hinweisen, welche der beiden PINs gefragt ist.

Signieren und Verschlüsseln von E-Mails

Einer der Hauptanwendungsbereiche der SuisseID ist das Signieren von E-Mails. Mit der Signatur kann der Empfänger nachvoll-

* Lic. iur., Rechtsanwalt, MAS Business Information Technology, *christian.leupi@gr-law.ch*

ziehen, dass einerseits die E-Mail tatsächlich vom Absender stammt und andererseits die Nachricht nicht verändert wurde.

Das Signieren von E-Mails ist vom Anbieter grundsätzlich nachvollziehbar erklärt und verständlich erläutert. Es dürfte auch ohne detaillierte Informatikkenntnisse umsetzbar sein. Allerdings beschränkt sich dies momentan auf den Einsatz von Windows-Betriebssystemen und Microsoft Outlook. Sofern der Anwender Windows und Outlook einsetzt, geht das Einrichten der Signaturfunktion mit wenigen Mausklicks vonstatten. Falls andere Betriebssysteme oder E-Mail-Software eingesetzt werden, sieht die Sache schon etwas anders aus. Diese bedingen mehr Konfigurationsaufwand und technisches Know-How. Die Signaturfunktion ist unter der neuesten Version des Apple-Betriebssystems (OS X 10.6.) mit dem integrierten Mailprogramm leider (noch) nicht nutzbar.

Der Anbieter der Anwalts-SuisseID bietet ein Secure E-Mail-Zertifikat an, welches zusätzlich zur Signierung von E-Mails und elektronischen Daten auch die Verschlüsselung von E-Mails und Anhängen ermöglicht. Dieses Zertifikat, welches allerdings in der technischen Spezifikation der SuisseID nicht vorgesehen ist, wurde standardmässig nicht implementiert. Es ist aber auf Anfrage erhältlich und kann manuell auf der SuisseID installiert werden.

Wer die SuisseID mittels Secure-E-Mail-Zertifikat zum sicheren Austausch von E-Mails und elektronischen Daten einsetzen will, muss allerdings mit diversen Einschränkungen leben. Die wichtigste Einschränkung besteht in der Notwendigkeit, dass sowohl Absender als Empfänger von E-Mails eine SuisseID mit Secure-E-Mail-Zertifikat einsetzen müssen, damit der verschlüsselte Informationsaustausch in beide Richtungen klappt. Die Einsatzbreite der Verschlüsselung ist dementsprechend erheblich von der Verbreitung der SuisseID abhängig.

Weiter ist zu berücksichtigen, dass mit dieser Variante der Verschlüsselung die elektronische Nachricht als solche verschlüsselt wird und dementsprechend auch in verschlüsselter Form elektronisch aufbewahrt wird. Dies birgt die Gefahr, dass die Daten irgendwann nicht mehr entschlüsselt werden können, da diese untrennbar mit dem jeweiligen Zertifikat des Empfängers verknüpft sind. Es ist deshalb aus Sicht der Anwaltskanzlei, welche auf die verschlüsselte E-Mail-Kommunikation setzt, etwas fraglich, ob sich die E-Mail-Verschlüsselung mittels Secure-E-Mail-Zertifikat wird etablieren können.

Im Kanzleibetrieb momentan sicherlich mit weniger Einschränkungen einsetzbar ist die sichere E-Mail-Kommunikation über Zustellplattformen wie z.B. PrivaSphere, welche im Vergleich zur vorerwähnten Verschlüsselung der einzelnen Nachrichten einen etwas anderen Ansatz verfolgen. Diese verschlüsseln nicht die Nachricht bzw. die Daten, sondern den Transportweg der Daten (analog E-Banking). Aus Anwendersicht hat dies den nicht zu unterschätzenden Vorteil, dass die Nachrichten im Klartext empfangen werden und sich die Anwaltskanzlei deshalb keine Gedanken um die Entschlüsselung machen muss. Allerdings setzt der komfortable Einsatz dieser Technologie (z.B. Integration in bestehende Mailserver) erhebliche Investitionen voraus. Die Anwendung der Zustellplattform über den Web-Browser entpuppt sich im Kanzleialltag momentan noch als wenig komfortabel und flexibel.

Signieren von PDF-Dokumenten

Ein weiterer Hauptanwendungsbereich der SuisseID stellt das Unterzeichnen elektronischer Daten wie beispielsweise PDF-Dateien mittels der qualifizierten Signatur dar. Aus Anwaltssicht sind natürlich in diesem Zusammenhang die elektronischen Eingaben an Behörden zu erwähnen.

Zu diesem Zweck stellt der Bund eine Software zum Signieren von PDF kostenlos zur Verfügung – den eGov LocalSigner. Grundsätzlich ist diese Initiative des Bundes zu loben. Allerdings kann der Funktionsumfang des eGov LocalSigner nicht mit kostenpflichtiger PDF-Software mithalten. Nebst dem eGov LocalSigner benötigt der Anwender nämlich zusätzlich noch eine Software zum Erstellen von PDF-Dateien (wobei auch kostenlose Angebote erhältlich sind) sowie sinnvollerweise eine Applikation für das Zusammenführen mehrerer PDF-Dateien zu einer Datei.

Diese Funktionen sind bei kommerziellen Produkten (wie z.B. Adobe Acrobat) meist in einer Software integriert, zusammen mit weiteren Komfortfunktionen wie beispielsweise dem Erstellen von Inhaltsverzeichnissen. Wer also voll auf elektronische Eingaben setzen will, ist mit einer kommerziellen PDF-Software sicherlich besser bedient.

Immerhin hat die Software des Bundes den kostenpflichtigen Produkten etwas voraus. Standardmässig ist nämlich bereits ein Zeitstempeldienst – derjenige der Bundesverwaltung – vorkonfiguriert. Dies ist bei den kommerziellen PDF-Lösungen nicht der Fall. Hier muss der Zeitstempeldienst manuell installiert werden, was aber den Benutzer nicht vor grosse Herausforderungen stellen sollte.

Wie auch der Schweizerische Anwaltsverband auf seiner Webseite empfiehlt, sollte der SuisseID-Anwender standardmässig einen Zeitstempeldienst installieren. Ohne Zeitstempeldienst wird der Zeitpunkt der Signierung des elektronischen Dokuments durch die Systemzeit des Benutzer-PCs gesetzt. Allerdings ist nur mit dem Einsatz eines Zeitstempeldienstes gewährleistet, dass der Zeitpunkt der Signierung des elektronischen Dokuments nachvollziehbar und von unabhängigerStelle bestätigt nachgewiesen werden kann.

SuisseID und Login bei Online-Angeboten

Ein weiterer Anwendungsbereich der SuisseID ist die Authentifikation gegenüber Online-Angeboten. Die Anmeldung erfolgt in diesem Falle mittels zweier Elemente, erstens durch die SuisseID als physisches Element und zweitens durch die PIN. Dies erhöht die Sicherheit des Logins, da ein Anmelden nur mit Vorliegen der SuisseID geschehen kann. Allerdings ist zu berücksichtigen, dass damit unter Umständen auch der Einsatzradius beschränkt wird, da die Nutzung nur mit SuisseID und Kartenlesegerät erfolgen kann. Gerade der Sicherheitsgewinn eines Logins per SuisseID

auf einem fremden Computer wird dann unter Umständen durch das Fehlen des Kartenlesegerätes verhindert.

Für die Authentifikation mittels SuisseID ist aus Anwendersicht zu wünschen, dass der Anmeldeprozess möglichst einfach und ohne Benutzerinteraktion in technischer Hinsicht verläuft.

Als Beispiel sei vorliegend die Buchhaltungsanwendung «Abaweb Treuhand» erwähnt, welche über die Internetverbindung als Software-as-a-Service angeboten und genutzt werden kann. Während der Loginprozess im Internet Explorer ohne Konfiguration des Browsers und vorgängige technische Vorkehren auf Anhieb funktioniert, erfordert die Benutzung im Firefox eine vorgängige manuelle Installation des Kryptographiemoduls. Diese ist zwar auf den Supportseiten von Quovadis gut erklärt, stellt aber für den Durchschnittsanwender sicherlich eine gewisse Hürde und potenzielle Fehlerquelle dar.

Etwas verwirrend sind zudem die Begriffsbestimmungen im Firefox. Dieser verlangt im Zuge des Loginprozesses ein «Master-Passwort», womit allerdings die PIN gemeint ist. Eine einheitliche Terminologie wäre deshalb sehr wünschenswert.

Zu beachten ist zudem, dass für die Authentifikation das korrekte Zertifikat benutzt werden muss («Authentication» und nicht «Qualified Signature»). Der Internet Explorer wählt das richtige Zertifikat automatisch aus, Firefox präsentiert dem Anwender standardmässig das Signaturzertifikat. Nach Auswahl des Authentisierungszertifikats klappt die Anmeldung auch im Firefox, ansonsten erhält der Anwender eine Fehlermeldung.

Fazit

Der Bestell- und Installationsprozess ist ausreichend dokumentiert und sollte auch für den durchschnittlichen PC-Benutzer zu bewerkstelligen sein. Erste Anlaufstelle sollte im Zusammenhang mit Fragen der Online-Supportbereich des Anbieters sein, welcher bereits eine Vielzahl von Antworten bereithält. Auch die vom Anwender vorzunehmenden Installationen sind nachvollziehbar erklärt.

Momentan scheint aber die Integration der SuisseID hauptsächlich in die Microsoft-Produktpalette gelungen zu sein. Die Installation im Windows-Betriebssystem sowie die Anwendung in Outlook und im Internet Explorer gestaltet sich einfach, während die Anwendung auf Apple-Rechnern sowie in alternativen Webbrowsern und E-Mail-Anwendungen momentan noch zu viele Benutzereingriffe und technisches Verständnis voraussetzt.

Hier sind sicherlich primär die Hersteller gefordert und es wird für die Verbreitung der SuisseID entscheidend sein, dass auch die Anwendung im Nicht-Microsoft-Bereich möglichst benutzerfreundlich gestaltet wird.

Adrian Rufener*

Mit der SuisseID zum beweiskräftigen Mailverkehr

Stichworte: sicherer Mailverkehr, digitale Signatur, E-Mail als Beweismittel

In der Anwaltsrevue 4/2009 wurde ausführlich dargestellt, wie der Mailverkehr abgesichert werden kann. An dieser Stelle kann auf Wiederholungen weitgehend verzichtet werden. Mit der SuisseID wird per 1. Januar 2011 nicht bloss der Rechtsverkehr mit den Zivilgerichten und den Strafverfolgungsbehörden möglich sein. Vielmehr sind die Einsatzmöglichkeiten der SuisseID sehr vielfältig, da digitale Zertifikate verschiedene Eigenschaften aufweisen, welche den elektronischen Rechtsverkehr erheblich erleichtern und vor allem auch mehr Rechtssicherheit schaffen. Digitale Zertifikate weisen folgende Eigenschaften auf:

Authentizität/Identifikation (Authentication)

Der Empfänger muss den Absender eindeutig identifizieren und überprüfen können, ob die Nachricht wirklich vom Absender stammt.

Autorisierung (Authorization)

Rechte, Befugnisse und Privilegien eines Benutzers müssen zugeteilt und überwacht werden.

Integrität (Integrity)

Die Nichtveränderbarkeit und Unverfälschbarkeit von Informationen muss garantiert werden, Veränderungen müssen automatisch festgestellt werden können.

Vertraulichkeit (Confidentiality)

Nur der Berechtigte darf eine verschlüsselte Information lesen können.

Nicht Anfechtbarkeit/Unleugbarkeit (Non-Repudiation)

Der Verfasser darf nicht in der Lage sein zu bestreiten, dass er die Information so geschrieben hat.

Allein dieser «Leistungskatalog» zeigt die Vorteile des Einsatzes von digitalen Zertifikaten im Mailverkehr auf. Der ungesicherte Mailverkehr lässt unter anderem weder den Absender des Mails

* Lic. iur. HSG, Partner Schoch, Auer & Partner, St. Gallen, Geschäftsführer des St.Gallischen Anwaltsverbandes.