

Open eGov LocalSigner und SuisselD – von der elektronischen Signatur zum Identitäts- und Funktionsnachweis in Dokumenten

Adrian Blöchlinger

Der Schweizerische Anwaltsverband (SAV) rüstet in diesem Jahr seine Mitglieder mit einer Verbandskarte inklusive qualifizierten Zertifikats und SuisselD-Funktionalität aus und sorgt auch für die Ausbildung der Anwaltschaft. Der Schweizerische Notarenverband (SNV), die Fondation Notariat Suisse und die Association des notaires vaudois investieren in einen Modellversuch im Kanton Waadt, rüsten das Waadtländer Notariat mit Zertifikaten aus und bauen ein Register für Urkundspersonen auf, das künftig auch elektronische Funktionsnachweise ausstellen soll. Das Bundesamt für Justiz (BJ) sorgt im Rahmen der Sachenrechtsrevision dafür, dass ab 2012 auch elektronische Ausfertigungen öffentlicher Urkunden Realität werden. Praktischer Beitrag des BJ zur Abwicklung des elektronischen Rechtsverkehrs mit Behörden ist das auf die Bedürfnisse der Verwaltung, der Anwaltschaft und des Notariats optimierte Freeware-Programm Open eGov LocalSigner, das hier vorgestellt werden soll.

Mit diesen partnerschaftlichen Initiativen und Massnahmen steigt die Wahrscheinlichkeit, dass der elektronische Rechtsverkehr unter Einsatz von qualifizierten Zertifikaten ab 2011 im Rahmen von Verwaltungs- und Zivilverfahren in der Praxis dann auch stattfinden wird.



Adrian Blöchlinger
Fachbereich Rechtsinformatik
Bundesamt für Justiz
adrian.bloechlinger@bj.admin.ch

Unter dem Namen Open eGov (www.openegov.ch) haben das BJ und das Staatssekretariat für Wirtschaft (SECO) über mehrere gemeinsame Projekte seit 2004 sukzessive eine serviceorientierte Plattform für den Aufbau von Onlineprozessen mit der Verwaltung geschaffen. Die Innovations- und Entwicklungsplattform umfasst im Wesentlichen ein Framework für den Aufbau von Benutzerdialogen, standardisierte modulare Bausteine und Services für die elektronische Signatur, die Validierung elektronisch signierter Dokumente und Services für sichere Übermittlung.

Open eGov LocalSigner: ein ausgereiftes Produkt

Im Bereich der elektronischen Signatur wurde 2007 die erste Version des Programms Open eGov LocalSigner (www.openegov.ch/localsigner) bereitgestellt und seither kontinuierlich verbessert und ausgebaut. Mit der Version 2.5 wird Ende November 2010 ein auf Behörden, Anwaltschaft und Notariat optimiertes Produkt zur unentgeltlichen Nutzung bereitgestellt. Das Produkt läuft unter allen bekannten Betriebssystemplattformen.

Massnahme(n) zur Förderung des elektronischen Rechtsverkehrs ab 2011

Sinn und Zweck der Entwicklung von LocalSigner war es, die finanzielle Hürde für den Einstieg in den elektronischen Rechtsverkehr für Verwaltung und Gerichte, aber auch für die Bürgerinnen und Bürger tief zu halten: Es soll nebst dem Zertifikat nicht noch teure Software für das Signieren beschafft werden müssen. Ergänzt wird diese Förderungsabsicht im Jahr 2010 durch die Subventionierung der Zertifikate (SuisselD) im Rahmen des Konjunkturpaketes III und durch das Konzept des Identitätsnachweises über die SuisselD, das neue Perspektiven für die Weiterentwicklung des LocalSigner eröffnet.

Basisfunktionalität für das sichere Signieren von PDF-Dokumenten...

Mit dem LocalSigner können PDF- und PDF/A-Dokumente, das heisst Eingaben bei Behörden, Urteile und Verfügungen und auch elektronische Ausfertigungen von notariellen Urkunden, unter Einsatz eines ZertES-konformen qualifizierten Zertifikats rechtsgültig signiert und mit Zeitstempel versehen werden. Diese Dokumente müssen danach gemäss den Verordnungen zu den elektronischen Verfahren an die Verwaltung, die Register und an die Justiz sicher und nachvollziehbar übermittelt werden.

...ergänzt mit weiteren Sicherheits- und PDF-Bearbeitungsfunktionen

Die neue Version 2.5 erweitert die bereits vorher gute Funktionalität noch einmal bei der Sicherheit und bringt neu auch PDF-Bearbeitungsfunktionen:

- Unterstützung mehrerer Kartenleser, automatische Middleware-Erkennung und Signatur mit dem stärkeren Hash-Algorithmus SHA256 (Anforderung z. B. des deutschen Signaturgesetzes, für eine noch sicherere Signatur) über die PKCS#11-Schnittstelle;
- automatische Unterstützung aller qualifizierten schweizerischen Zeitstempeldienste und eines frei definierbaren weiteren Zeitstempeldienstes;
- Analyse des zum Signieren geladenen Dokuments zur Ermittlung versteckter Inhalte oder dynamischen Verhaltens (JavaScript usw.) mit Warnfunktion, Analyse und Anzeige, ob und in welcher PDF- oder PDF/A-Version das zu signierende Dokument erstellt wurde und in welcher PDF- oder PDF/A-Version das Dokument nach Bearbeitung und Signatur vorliegt;
- Der bisherige integrierte Betrachter für das zu signierende Dokument dient lediglich noch der Positionierung der sichtbaren Signatur. Es kann jederzeit zwischen integriertem Betrachter und

dem Referenzbetrachter Adobe Reader hin und her geschaltet werden, sodass die Dokumentanalyse- und Validierfunktionen des Referenzbetrachters während des Signierprozesses jederzeit genutzt werden können;

- Dokumentbearbeitungsfunktionen wie das Anfügen einer leeren Seite, das Einfügen von Seiten aus einem anderen PDF-Dokument, das Löschen von Seiten aus dem zu signierenden Dokument, das Einfügen von (signierten) Beilagen in das zu signierende Dokument und das Einfügen von Text aufseiten des zu signierenden Dokuments.

Für die genannten Dokumentbearbeitungsfunktionen war bisher der Kauf der teuren kommerziellen Produkte notwendig. Die Dokumentbearbeitungsfunktionen interessieren vor allem das Notariat für die Erstellung elektronischer Ausfertigungen öffentlicher Urkunden. Natürlich profitieren auch Anwaltschaft und die Verwaltung, indem nun mit LocalSigner eigentliche PDF-Dossiers zusammengestellt und signiert werden können.

Lokale Installation, zentrale Serverinstallation und Einbindungsmöglichkeiten

Dank einer vom Schweizerischen Bundesgericht finanzierten Erweiterung kann LocalSigner auch zentral auf einem Server installiert werden. Die meisten Funktionen und Einstellungen können dabei so festgelegt werden, dass alle Benutzerinnen und Benutzer mit den gleichen Einstellungen und im gleichen Corporate Design ihre Signaturen auf dem Dokument anbringen. Dadurch ist LocalSigner für den Einsatz in der Verwaltung besonders geeignet. Und natürlich verfügt LocalSigner auch über Aufrufschnittstellen, die seine Einbindung zum Beispiel in Gerichtsapplikationen oder Geschäftsverwaltungssysteme erlauben.

Version 3.0 bereits im Frühjahr 2011!

Für die bereits geplante Version 3 soll im Frühjahr 2011 die Erweiterbarkeit über sogenannte Plug-ins hinzugefügt werden. Dadurch soll etwa ermöglicht werden, ein in LocalSigner signiertes Dokument direkt über eine gemäss den Verordnungen anerkannte Zustellplattform als elektronisches Einschreiben zu versenden oder eine sog. diskrete Validierung bereits signierter Dokumente mit dem zentralen Open eGov Validator Service (www.openegov.ch/validator) vorzunehmen (zur Validierung siehe auch «Von elektronischen Urkunden zu elektronischen Justizarchiven», in: «eGov Präsenz» 1 [2010], S. 70). Die Funktionalität des Anfügens von Beila-

gen bildet unter anderem die Grundlage der geplanten Weiterentwicklungen für das Einfügen von Identitäts- und Funktionsnachweisen, einer weiteren wichtigen Erweiterung der Version 3.0.

Unterschrift als Identitätsnachweis?

Der schweizerische elektronische Rechtsverkehr, insbesondere die Verfahren mit der Justiz, gehen von einem auf Dokumente zentrierten Modell aus. Bürgerinnen und Bürger, die Anwaltschaft und das Notariat produzieren ein Dokument, das in PDF konvertiert, unterschrieben und anschliessend an die Behörde übermittelt wird.

Die einfache Schriftlichkeit im juristischen Sinne beinhaltet die eigenhändige Unterschrift in Sinne der Zurechenbarkeit und damit auch der Identität des Unterzeichnenden. Ausgehend von diesem Konzept wurde zunächst diese Form der Schriftlichkeit elektronisch abgebildet und findet sich in Art. 14 Abs. 2^{bis} OR als anerkannte elektronische Signatur gemäss ZertES wieder. Auf diesem Prinzip basiert auch die Gesetzgebung zum elektronischen Rechtsverkehr: Im Signaturzertifikat findet sich aber lediglich der Name des Unterzeichnenden. Nur mit grossem Aufwand kann im Bedarfsfall bei der sogenannten anerkannten Anbieterin von Zertifizierungsdiensten die genaue Identität des Unterzeichnenden über dessen hinterlegte Ausweisschrift in Erfahrung gebracht werden.

Problematik beim dokumenten- und signaturzentrierten Ansatz

Dieses Konzept stösst jedoch hinsichtlich einer automatisierten Verarbeitung der Eingaben an seine Grenzen, weil aus dem Zertifikat des Unterzeichnenden ausser dem Namen und einer allfälligen Organisationszugehörigkeit keine weiteren zertifizierten Daten ausgelesen werden können. Es fehlen Angaben zu Person, Geburtsdatum und Nationalität oder auch sogenannte Admissions (Zulassungen), zum Beispiel zu einer Funktion wie Notar oder Anwalt gemäss BGFA oder gar Zeichnungsberechtigungen.

Mit den ergänzenden Konzepten der SuisseID, die nach internationalen Standards Attribute zu Identität und künftig auch zu Funktionen über sogenannte Providerservices im Netz bereitstellen, lässt sich in synchronen Prozessen über Webapplikationen bereits heute problemlos arbeiten. Ein solcher Identitätsnachweis ist im Artikel «Sicherer Identitätsnachweis im Strafregister mittels SuisseID» in dieser Ausgabe beschrieben. In Zukunft wird der Funktionsnachweis analog funktionieren.

Wie packen wir aber einen Identitätsnachweis in ein PDF-Dokument?

Wie beim Bestellvorgang für einen Strafregisterauszug braucht es dazu zuerst einen Prozess, der die identifizierenden Attribute der hinterlegten Ausweisschrift (Pass, Identitätskarte) elektronisch bereitstellt. Dies erfolgt durch einen SuisseID Identity Provider Service (IdP) nach Eingabe des Karten-PIN und in Form der – anlässlich der Hinterlegung signierten – sogenannten QC-Attribute.

Die signierten QC-Attribute werden vom IdP oder einem Intermediär in einem zum Ausgabezeitpunkt erneut signierten Datenpaket (elektronisches Token) an die Signierapplikation weitergereicht, von dieser überprüft und als Metadaten in das zu signierende PDF-Dokument eingefügt. Anschliessend wird das Dokument selbst signiert. Die im Dokument eingefügten QC-Attribute sind bei dieser Variante zwar maschinell auslesbar, für den Menschen beziehungsweise den Empfänger aber nicht direkt sichtbar.

Handelt es sich beim Dokument, in das der Identitätsnachweis eingefügt werden soll, um ein Formular, kann der Inhalt der QC-Attribute zusätzlich von der Signierapplikation in entsprechend normierte Formularfelder (Formularkopf) eingefügt werden. Damit werden sie auch für den Menschen sichtbar.

Handelt es sich um ein aus einem Textdokument erstelltes PDF-Dokument, wie dies beim Rechtsverkehr oder bei elektronischen Urkunden üblich ist, so lässt sich ein auch für Menschen sichtbarer Identitätsnachweis in Form eines signierten PDF-Attachment in das zu signierende Dokument einfügen. Dieses signierte Attachment wird vom IdP oder dem allfälligen Intermediär erstellt, signiert und von der anfordernden Signierapplikation in das zu signierende Dokument eingefügt.

Damit eine maschinelle Verarbeitung und die automatisierte Validierung von Identitäts- und Funktionsnachweisen möglich werden, müssen die Struktur und die Codierung der in das PDF eingefügten Metadaten für Funktionsattribute noch normiert werden.

Unsere Absicht ist es, den Open eGov LocalSigner so auszugestalten, dass die Bedienbarkeit der geschilderten komplexen technischen Vorgänge so einfach wie gewohnt bleibt.