Zeitschrift für Datenrecht und Informationssicherheit

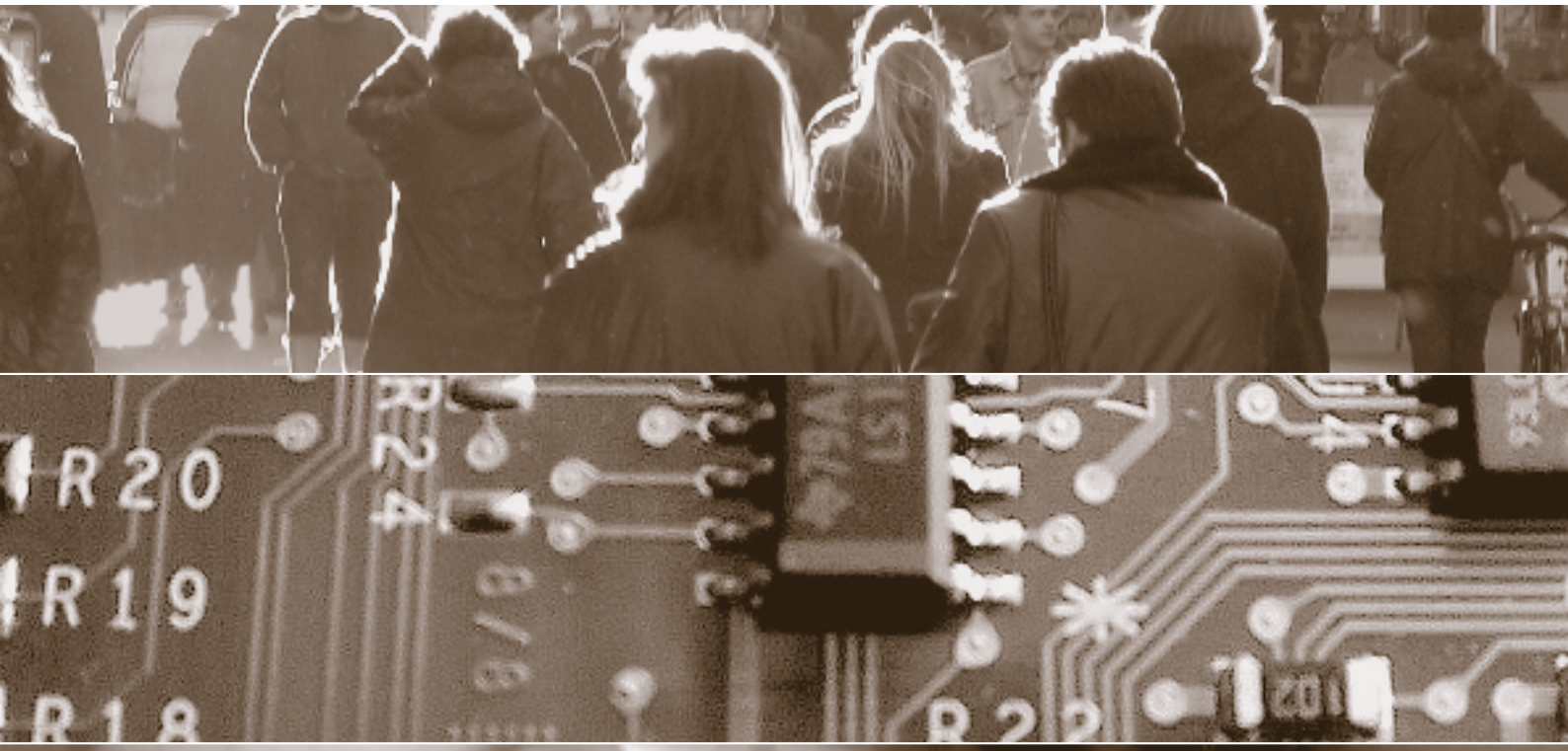
digma

www.digma.info 10. Jahrgang, Heft 3, September 2010

Schwerpunkt:

Governance Risk and Compliance (GRC)

fokus: Compliance in Informatiksystemen
fokus: Risiken im Outsourcing und Off-shoring
report: 10 Jahre Safe Harbor: Grund zum Feiern?



Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth

Schulthess §

fokus

Schwerpunkt:
Governance Risk and Compliance (GRC)

Compliance in Informationssystemen

Die zunehmende Erfassung und Speicherung von Personendaten erfordert neue Strategien im Sicherheits- und Risikomanagement. Das Prozess-Rewriting bietet eine Reihe von Vorteilen, insbesondere bei der Durchsetzung von Compliance in flexiblen Prozessen. Der Einsatz dieser Technologie wird in einem Krankenhausinformationssystem untersucht.

Risikomanagement und Wertschöpfung

Aktives Risikomanagement sollte mehr sein als blosser Schutz vor Verantwortlichkeitsansprüchen bei Vorfällen. Eine zu stark compliance-lastige Sichtweise kann dazu führen, dass ein Unternehmen die Chance aufgibt, die Geschäftstätigkeit durch die Optimierung des Risiko-/Ertrag-Verhältnisses für das Generieren von Wert aktiv zu steuern.

Risiken im Outsourcing und Off-shoring

Mit Outsourcing/Off-shoring sollen im Stammland Kosten eingespart werden. Wie wirtschaftlich ist Outsourcing/Off-shoring wirklich, wenn die nachträglich zur Einhaltung der rechtlichen und (branchen-)regulatorischen Anforderungen notwendig werdenden kostenintensiven Korrekturen miteinberechnet werden?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. Dr. iur. Rainer J. Schweizer, Dr. Günter Karjoth

Redaktion: Dr. iur. Bruno Baeriswyl und Dr. iur. Beat Rudin

Zustelladresse: Redaktion digma, per Adr. Datenschutzbeauftragter des Kantons Basel-Stadt, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, Fax +41 (0)61 201 16 41, redaktion@digma.info

Erscheinungsplan: jeweils im März, Juni, September und Dezember

Abonnementspreise: Jahresabo Schweiz: CHF 158.00, Jahresabo Ausland: Euro 99.00 (inkl. Versandspesen), Einzelheft: CHF 42.00

Anzeigenmarketing: Publicitas Publimag AG, Mürtschenstrasse 39, Postfach, CH-8010 Zürich
Tel. +41 (0)44 250 31 31, Fax +41 (0)44 250 31 32, www.publimag.ch, service.zh@publimag.ch

Herstellung: Schulthess Juristische Medien AG, Arbenzstrasse 20, Postfach, CH-8034 Zürich

Verlag und Abonnementsverwaltung: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach, CH-8022 Zürich
Tel. +41 (0)44 200 29 99, Fax +41 (0)44 200 29 98, www.schulthess.com, zs.verlag@schulthess.com

Man wird immer weniger lügen können

Reiserouten planen und vorab schon im Internet sehen können, wie die Gegend rund ums Hotel sich ausnimmt – das ist praktisch. Was sollen dann bloss die vielen Bedenken gegen Google Street View? Der Autor warnt davor, die Gegnerschaft vorschnell als Hinterwäldler mit der Mentalität bornierter Kleingärtner zu denunzieren. Es geht um mehr: um unsere Furcht vor unerwünschter Neugierde und der Schubladisierung durch fremde Blicke, vor Selbstpreisgabe und Statusverlust.

10 Jahre Safe Harbor: Grund zum Feiern?

Um den Datenaustausch mit Empfängern in den Vereinigten Staaten zu erleichtern, haben die EU und die Schweiz mit den USA je ein Safe-Harbor-Abkommen getroffen. Verbessert dies den Datenschutz oder ist es bloss ein Deckmäntelchen, hinter dem sich Unternehmen zu Unrecht verstecken können? Die Meinungen gehen auseinander.

Datenschutzkontrolle im Staatsschutz

Im Bereich des Staatsschutzes ist eine unabhängige und wirksame Datenschutzkontrolle nicht möglich. privatim, die Vereinigung der schweizerischen Datenschutzbeauftragten, beanstandet, dass eine Kontrolle der Datenbearbeitungen der Staatsschutzorgane von der Zustimmung des Bundes abhängig ist und damit die zu kontrollierenden Organe über den Umfang der Kontrollen bestimmen. privatim fordert deshalb die Aufhebung des Zustimmungserfordernisses.

report

forum

Transfer

SuisseID – die Lösung aller Probleme?

Roland Portmann, Prof., Dozent für IT-Security, Hochschule Luzern – Technik & Architektur, roland.portmann@hslu.ch

Anfang Mai wurde vom Staatssekretariat für Wirtschaft Seco die SuisseID vorgestellt. Mit der Entwicklung der SuisseID war eine Initiative im Rahmen der konjunkturellen Stabilisierungsmassnahmen, die der Bundesrat im letzten Jahr beschlossen hat, und ist der erste standardisierte elektronische Identitätsnachweis in der Schweiz. Privatpersonen können die SuisseID bei SwissSign und QuoVadis bestellen. Schon bald nach der Vorstellung der SuisseID wurden einige kritische Stimmen laut. So erschien in der Weltwoche vom 4. Mai 2010 ein sehr kritischer Artikel von Andreas Von Gunten mit dem Titel «Teure Lösung für nichtexistente Probleme» und verneint den Nutzen der SuisseID mit teilweise durchaus diskussionswürdigen Argumenten.

Was ist die SuisseID?

Grundsätzlich ist die SuisseID eine Smartkarte mit mehreren X.509 Zertifikaten, die auch in der Form eines Memorysticks bestellt werden kann. Gemäss der Spezifikation enthält eine SuisseID mindestens ein qualifiziertes Zertifikat, das für rechtsgültige Unterschriften verwendet werden kann und ein Authentisierungszertifikat. Auf den ersten Blick unterscheidet sich die SuisseID nicht von früheren Angeboten, wie beispielsweise dem Postzertifikat, das seit einigen Jahren erhältlich ist.

Eine wesentliche Erweiterung ist die Integration einer «SuisseID-Nummer» im Zertifikat. Die Spezifikationen von SuisseID stellen sicher, dass eine SuisseID-Nummer genau einer Person zugeordnet werden kann und damit eine eindeutige Identifizierung einer Person erlaubt. Die SuisseID-Nummer ist in allen Zertifikaten eines Inhabers gleich und kann auch bei Erneuerungen der Zertifikate beibehalten werden. Bei Bedarf (z.B. aus Datenschutzüberlegungen) kann eine Person auch mehrere SuisseID-Nummern bekommen. Diese SuisseID-Nummer erlaubt eine langfristige und sichere Authentisierung von Personen, auch wenn sich der Zertifikatsinhalt (z.B.: die E-Mail-Adresse) ändert.

Der X.509 Standard bietet eine recht grosse Freiheit bei der Gestaltung des Zertifikatsinhaltes. Für eine applikations- und organisationsübergreifende Verwendung von Zertifikaten ist eine weiter gehende Standardisierung des Zertifikatsinhaltes sinnvoll und notwendig. In der Spezifikation der SuisseID ist genau definiert, welche Informationselemente in den Zertifikaten vorhanden sein müssen.

Eine weitere wesentliche Erweiterung der SuisseID ist, dass die SuisseID-Anbieter zwingend die Internet-Dienste eines Identity Provider und einer Claim Assertion anbieten müssen. Mit diesen Diensten, die auf zeitgemässen, sicheren Protokollen aufbauen, können Anbieter von Dienstleistungen im Internet (z.B. Webshops) die Authentisierung dem jeweiligen SuisseID-Anbieter übergeben und erhalten bei Bedarf vom Anbieter weitere Informationen über die Person. Die SuisseID-Anbieter verwalten dazu alle Informationen, die auf den herkömmlichen Identitätsnachweisen (Pass oder Identitätskarte) enthalten sind. Dieser zusätzliche Informationsaustausch ist für den Benutzer transparent, d.h., vor der Informationsübertragung wird dem Benutzer mitgeteilt, welche zusätzlichen Informationen der Anbieter vom Identity Provider wünscht. Es wurde darauf geachtet, dass nur minimale Informationen übertragen werden. Für eine Altersüberprüfung muss beispielsweise nicht das Geburtsdatum übertragen werden, sondern nur das Attribut «isOver18».

Was kann die SuisseID?

Auf der Webseite von SuisseID (<http://www.suisseid.ch>) wird für Endkunden mit fünf Anwendungsfällen für die SuisseID geworben. Diese Anwendungsfälle dürften Endkunden kaum motivieren, sich eine SuisseID zu beschaffen.

Sicherstellen des Absenders von E-Mails

Heute werden im privaten und im geschäftlichen Umfeld erst sehr wenige E-Mails signiert. Es gibt kaum Anwendungsfälle, die auf einer korrekten Signierung einer E-Mail aufbauen. Die Implementation eine solchen Anwendungsfalles dürfte für eine Organisation mit recht hohen Kosten verbunden sein, da dann auch die Archivierung der signierten Mails geregelt werden müsste. Ein Anwendungsfall wäre allenfalls der E-Mail-Verkehr mit

den Banken, die zunehmend die entsprechende Infrastruktur aufbauen. Für diesen Mailverkehr wäre aber eine Verschlüsselung wichtiger als eine Signierung. Ein Zertifikat für die E-Mail-Verschlüsselung fehlt bei der aktuellen Version der SuisseID.

Dokumentenunterschrift elektronisch rechtsgültig

Falls eine Firma Verträge mit elektronischen Unterschriften akzeptieren will, müssen die entsprechenden organisatorischen und technischen Voraussetzungen in der Firma geschaffen werden. Schon die Ablage von Papierverträgen ist in vielen Firmen ein Problem. Kaum eine IT-Infrastruktur einer Firma in der Schweiz dürfte in der heutigen Konfiguration eine sichere und effiziente Überprüfung, Ablage und Archivierung von elektronischen unterschriebenen Dokumenten beherrschen.

Zugang zum Firmen-Intranet von zuhause aus

Dies kann durchaus in vielen Fällen eine sinnvolle Anwendung sein, bedingt aber, dass die Firma die Authentisierung der Intranet-Anwendung entsprechend anpasst. Dies kann mit hohen Investitionen verbunden sein.

Elektronisch amtliche Dokumente bestellen

Dies ist eine Anwendung, die für den Endkunden durchaus bequem ist. Die meisten Einwohner in der Schweiz dürften eher selten amtliche Dokumente benötigen, bei denen ein Gang zum Amt notwendig ist. Auf der (sehr guten!) Webseite der Gemeinde Horw beispielsweise, die bereits SuisseID unterstützt, bringt die Verwendung der SuisseID noch keine echten Vorteile.

Jugendschutz im E-Commerce

Der Altersnachweis kann mit der SuisseID sicher vereinfacht werden. Hier muss aber beachtet werden, dass das Internet stark zunehmend international wird und die SuisseID eine rein schweizerische Lösung darstellt. Ob viele Anbieter eine Altersüberprüfung mit der SuisseID anbieten werden, wird sich in Zukunft zeigen.

Welche Probleme löst die SuisseID?

Für die oben dargestellten Anwendungsfälle dürfte der Nutzen für den Endkunden klein sein und kaum zu einer starken Verbreitung der SuisseID führen.

Die SuisseID könnte aber zur Lösung eines der grösseren Problembereiche im Internet-Business führen. Auf sehr vielen Webseiten muss man sich als Endkunde anmelden. Sei es beim Internetshopping, sei es beim Lösen eines SBB-Tickets, sei es für den Zugang zu einem Social Network: man muss einen Benutzernamen und ein Passwort eintippen. Es kann davon ausgegangen werden, dass nur sehr wenige Internetbenutzer die für eine ausreichende Sicherheit notwendigen Regeln einhalten. Mit einem Web Single Sign On, wo man sich nur beim ersten Zugriff auf eine geschützte Webseite bei meinem Identity Provider anmelden muss, könnte das Leben der Internetbenutzer stark vereinfacht werden. Dieser Anwendungsfall ist auf der SuisseID-Seite für einen möglichen Einsatz bei Unternehmungen aufgeführt. Single Sign On wird aber nur nebenbei erwähnt.

Als Internetanwender und Internetkäufer würde ich mir zudem wünschen, dass ich nicht auf jedem Internet-Shop meine Adresse und meine Kreditkartennummer eintippen muss. Die Spezifikation der SuisseID erlaubt die Integration von weiteren Datenbanken mit personenbezogenen Daten. Auch in diesem Fall ist der Datenaustausch für den Endbenutzer transparent.

Im kommerziellen Umfeld sind für die SuisseID viele Anwendungsfälle denkbar. Insbesondere wenn der Benutzerkreis klar definiert ist, kann eine Verwendung der SuisseID zu Projekteinsparungen führen, da die Verwaltung der Identitäten mit den zugehörenden Business-Prozessen (z.B. Ersatz bei Verlust) an die Anbieter von SuisseID ausgelagert werden kann.

SuisseID International ?

Das Internet kennt keine Landesgrenzen. Die SuisseID ist eine rein schweizerische Lösung. Damit ist ein Einsatz der SuisseID im internationalen Umfeld eingeschränkt, aber nicht grundsätzlich unmöglich, da mit standardisierten Protokollen gearbeitet wird. Es wäre beispielsweise durchaus möglich, dass ein deutscher Web-Anbieter der Authentisierung von Identity-Providern von mehreren Ländern vertraut.

Die SuisseID könnte auch für digitale Unterschriften verwendet werden, falls sich dies im internationalen Geschäftsumfeld etablieren würde.

Schlussfolgerung

Im Internet bestehen durchaus ernsthafte Probleme, die mit einem Einsatz der SuisseID mindestens teilweise gelöst werden können. Aufgrund des geplanten Angebotes werden sich kaum viele Endkunden eine SuisseID beschaffen. Die auf der SuisseID-Webseite dem Endkunden präsentierten Einsatzbereiche lösen keine grösseren Probleme eines typischen Internetbenutzers. Da aber zeitgemässe und standardisierte Protokolle eingesetzt werden, sind noch viele weitere Anwendungsfälle denkbar, die für den Endkunden echte Vorteile bieten würden. Insofern hätte der Titel dieses Artikels auch heissen können: «SuisseID: Interessante Lösung für andere Probleme». ■

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement digma (4 Hefte des laufenden Jahrgangs)
à **CHF 158.00** bzw. bei Zustellung ins Ausland **EUR 123.00** (inkl. Versandkosten)

Name Vorname

Firma

Strasse

PLZ Ort Land

Datum Unterschrift

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8022 Zürich
Telefon +41 44 200 29 19
Telefax +41 44 200 29 18
E-Mail: zs.verlag@schulthess.com
Homepage: www.schulthess.com

Schulthess §