telekom control

Aufsichtsstelle für elektronische Signaturen

Konsultation zu den Anforderungen des SigG an die Geräte der Benutzer – Zusammenfassung der Stellungnahmen

03.04.2000

Aufsichtsstelle für elektronische Signaturen
Telekom-Control-Kommission und Telekom-Control GmbH, Mariahilfer Straße 77–79,
1060 Wien, Tel. 01/58058-0, Fax: 01/58058-9191, http://www.tkc.at, signatur@tkc.at

Einleitung

In ihrer Sitzung vom 06.12.1999 hat die Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen die Telekom-Control GmbH beauftragt, eine Konsultation zur Frage der Anforderungen des Signaturgesetzes an die Geräte der Benutzer durchzuführen. Das Konsultationsdokument wurde in der Sitzung der Telekom-Control-Kommission vom 10.01.2000 erörtert und am 12.01.2000 auf dem Website der Aufsichtsstelle veröffentlicht. Zur Stellungnahme eingeladen wurden über eine Mailing-List alle der Aufsichtsstelle bekannten Interessierten – insbesondere die Anbieter von Zertifizierungsdiensten und alle potenziellen Nutzer sicherer elektronischer Signaturverfahren – vor allem Behörden und E-Commerce-Anbieter.

Auf mehrfachen Wunsch hat die Telekom-Control GmbH das Ende der Stellungnahmefrist bis zum 15.03.2000 verlängert. Bis zu diesem Zeitpunkt sind Stellungnahmen von A-Trust, Card Solutions, Concord-Eracom, Datakom, Globalsign, iTA, Amt der Oberösterreichischen Landesregierung und Siemens eingelangt, die im Anhang dieses Dokuments im vollen Wortlaut wiedergegeben wurden.

Im folgenden hat die Telekom-Control GmbH die Stellungnahmen redaktionell zusammengefasst. Dabei wurde die im Konsultationsdokument gewählte Gliederung beibehalten. Die blau markierten Namen sind jeweils mit Hyperlinks auf die zitierte Passage der Stellungnahme hinterlegt.

Allgemeines

Zu einer Reihe von Fragen, die im Konsultationsverfahren erörtert wurden, werden nach Art. 3 Abs. 5, Art. 9 und Art. 10 der Signaturrichtlinie 1999/93/EG europaweit allgemein anerkannte Normen festgelegt werden. Im Rahmen der EESSI (European Electronic Signature Standardisation Initiative) arbeiten CEN/ISSS und ETSI/SEC an Protection Profiles nach den Common Criteria für die Evaluierung sicherer Signaturerstellungseinheiten.

Auch in den Stellungnahmen wurde betont, dass die in der Praxis eingesetzten technischen Lösungen sich an internationalen Standards orientieren sollen und österreichspezifische Lösungen unbedingt vermieden werden sollen (z. B. IBM, iTA).

Dokumentenformate

Gibt es beim gegenwärtigen Stand der Technik – abgesehen von simplen Formaten wie Ascii (text/plain) – bereits „sichere“ Dokumentenformate, deren Spezifikation allgemein verfügbar ist und mit denen dynamische Veränderungen und unsichtbare Daten ausgeschlossen oder doch zumindest in ihrer Problematik reduziert werden können – etwa Subvarianten von RTF oder von Postscript?

Unstrittig ist in den Stellungnahmen die hohe Bedeutung sicherer Dokumentenformate, wenngleich es auch viele Anwendungen geben wird, in denen auch „nicht sichere“ Dateien signiert werden (vgl. IBM). Die Stellungnahme von iTA fasst die Bedeutung sicherer Dokumentenformate markant zusammen: „Gibt es kein sicheres Format, so ist die sichere Unterschrift nahezu wertlos!“

Ein wirklich universell einsetzbares Dokumentenformat, das die Anforderungen des § 7 Abs. 2 SigV erfüllt, scheint es nicht zu geben (vgl. iTA). Es gibt aber einige Ansätze für die wichtigsten Anwendungsfälle in der Praxis.

A-Trust verweist darauf, dass das Problem sich nicht alleine dadurch lösen lässt, dass Spezifikationen für Dateiformate frei verfügbar sind, denn ohne eine sinnvolle Verbreitung, bzw. Implementierung in Standardsoftware helfe das beste Format nichts. Ein Zertifizierungsdiensteanbieter müsse daher immer in Kontakt mit der Softwareindustrie stehen, um Produkttests bzw. auch Implementierungen der eigenen Signaturtools in Standardsoftware, in die Wege leiten zu können.

Ähnlich argumentiert auch IBM: Hersteller zukünftiger Business-Anwendungen werden Signierfunktionen clientseitig integrieren und somit selbst über Erscheinungsbild und Datenformat entscheiden (Beispiel: Web-Banking).

Bei der Durchsicht der Stellungnahmen fällt auf, dass zwar eine sehr genaue Spezifikation gefordert wird (Siemens: „Die Spezifikation muss so detailliert sein, dass ein Anzeigeprogramm (Viewer) gemäß dieser (nach-)implementiert werden kann. Als weitere Vorgabe gilt, dass der Signator den gesamten Inhalt der Daten visuell überprüfen (und verstehen) können muss.“), dass aber andererseits teilweise sehr salopp über Dokumentenformate gesprochen wird und etwa „Ascii“ ohne näheren Verweis auf die konkreten Spezifikationen als geeignet angesehen wird, obwohl durch „Ascii“ nur ein kleiner Umfang eines gewöhnlichen Texteditors spezifiziert wird (z. B. nicht einmal die Umlaute der deutschen Sprache). Der geforderte Detaillierungsgrad und Umfang einer „Spezifikation“ im Sinne des § 7 Abs. 2 SigV scheint noch weitgehend ungeklärt zu sein. Klar ist, dass anhand der Spezifikation nachvollziehbar sein muss, wie die Darstellung des Dokumentenformates zu erfolgen hat. Eine konkrete Evaluierungsprozedur für diese „Nachvollziehbarkeit“ scheint es aber noch nicht zu geben.

Beispiele für Dokumentenformate

Reiner Text

Reiner, unformatierter Text, wird für zahlreiche Anwendungen das am einfachsten einsetzbare Dokumentenformat sein. Oft werden diese Dokumentenformate (ein Byte = ein dargestelltes Zeichen) umgangssprachlich „Ascii“ genannt. Der Ascii-Code definiert von den 256 möglichen Zeichen aber nur die Darstellung der Codes von 32 bis 126. In der Praxis wird daher nicht Ascii verwendet, sondern verschiedene andere Codierungen, auf deren Unterschiede man achten wird müssen.

IBM: Plain-ASCII-Text ist natürlich überall dort verwendbar, wo kürzere Informationen, wie Formularinhalte, formlose Anträge, Aufzählungen, Bestellungen nach Artikelnummern, etc. signiert werden. In diese Kategorie fallen auch einfache Web-/HTML-Formulare, deren Inhalt so gestaltet sein sollte, dass die Formatierungsinformation nicht den Inhalt / die zu signierende Nutzinformation „erschlägt“.

iTA: Wie richtig erwähnt, stellt sich auch bei Ascii (text/plain) die Frage nach dem verwendeten Charakterset. Diese Information müsste im signierten Dokument sichtbar sein und in geeigneter Form mitgespeichert sein.

Grafikformate

Eine Möglichkeit, ein Textdokument so darzustellen, dass es auf beliebigen Systemen gleich aussieht, besteht darin, den Text in einem Grafikformat zu speichern. iTA bezeichnet diese Möglichkeit, sogar als „einzige Möglichkeit, ein Textdokument darstellungssicher und frei von Manipulationen darzustellen“. Siemens verwendet eine Variante des TIFF-Formats.

Der Nachteil dieser Variante besteht im großen Speicherverbrauch und darin, dass ein Text nach der Konvertierung in ein Grafikformat nicht mehr als Text weiter verarbeitbar ist. Daher

greifen die Anbieter dieser Technologie oft darauf zurück, neben der „sicher signierten“ Version auch eine weiter verarbeitbare Version des Textes zu versenden, wodurch natürlich das Problem entsteht, dass die beiden Versionen sich unterscheiden könnten.

Vorteile eines Grafikformates bestehen sicherlich in der hohen Dokumentenechtheit und damit verbundenen Glaubwürdigkeit (sogar das Schriftbild bleibt erhalten) und in der einfacheren Möglichkeit, das Dokument auch in ferner Zukunft in identischer Form darzustellen.

Portable Document Format (PDF)

IBM: „Es ist heute üblich, Dokumente, die i. a. mit Textverarbeitungsprogrammen erzeugt werden ... – wenn diese vor Veränderung zu schützen sind – in das Acrobat PDF-Format zu konvertieren. Fehlerhafte Konvertierungen sind i. a. deutlich erkennbar. Eine Überprüfung der korrekten Konvertierung vor Anbringung der Signatur ist natürlich zu empfehlen.“ (vgl. auch iTA, die für die Konvertierung in PDF noch „einige zusätzliche Überprüfungen (Filter)“ für erforderlich hält.

Extensible Markup Language (XML)

Siemens gibt an, dass für das Produkt TrustedDoc XML verwendet wird. Details der Spezifikation des Dokumentenformates bleiben jedoch offen. An der von Siemens genannten URL ist zwar abrufbar, dass das Produkt die „WYSIWYS (What You See Is What You Sign) requirements“ erfülle, aber nicht, wie dies konkret umgesetzt wird.

Formularmanagementsystem Webform

Globalsign verweist in seiner Stellungnahme auf das Formularmanagementsystem Webform, welches speziell für Signaturanwendungen entwickelt wurde und auch von BSI und TÜV evaluiert werden soll. Zum Produktumfang gehört auch ein Dokumentenformat und ein Secure Viewer. Durch den speziellen Formulardarstellungsmechanismus sei geeignet sichergestellt, dass ein Formular in seinem gesamten Umfang vor dem Unterzeichnen gelesen werden könne. Es werde explizit auf Formularteile hingewiesen, welche die Sichtbarkeitskriterien in irgend einer Form (z.B. durch Schriftgröße, Farbe, Überdeckung, Art der Gestaltung) verletzen können (vgl. die Leistungsbeschreibung).

Gibt es beim gegenwärtigen Stand der Technik praktikable Konvertierungsprogramme, mittels derer Dokumente aus Standardformaten in solche „sicheren Formate“ konvertiert werden können? Inwieweit besteht die Möglichkeit, Dokumente in „sicheren Formaten“ elektronisch weiterzuverarbeiten?

Das Problem, dass das Dokumentenformat einerseits die Anforderungen an ein sicheres Dokumentenformat erfüllen sollen, andererseits aber die signierte Nachricht manchmal beim Empfänger weiterbearbeitet werden soll, wird manchmal dadurch „gelöst“, dass die Datei doppelt versandt wird: einmal sicher elektronisch signiert und einmal im unsicheren Format. (vgl. Globalsign, iTA). Dabei entsteht natürlich das Problem, dass die Version, die weiterbearbeitet wird, sich unter Umständen von jener Version unterscheidet, die rechtlich gültig sein soll. Auch IBM erwähnt die Möglichkeit, dass dem Empfänger eines signierten Dokumentes auch eine weiterbearbeitbare Fassung mitgeschickt wird wobei IBM offenbar davon ausgeht, dass auch dieser weiterbearbeitbare Fassung signiert werden könne. Ebenso werde sich an heutigen Gepflogenheiten, Dateien in signierten Mails zu verschicken, nichts wesentlich ändern.

Bedauerlicher Weise gibt es offenbar noch kaum Formate, die Sicherheit und leichte Weiterverarbeitbarkeit gewährleisten. Bei den im Konsultationsverfahren bekannt-

gewordenen Ansätzen für die Konvertierung in ein sicheres Dokumentenformat wird in der Regel so vorgegangen, dass ein Textformat in etwas ganz anderes (z. B. das Grafikformat TIFF, die Seitenbeschreibungssprache PDF oder die Formularsprache des Produkts Webform) vorgenommen wird. Konvertierungsprogramme, die aus einem „unsicherem“ Textformat ein „sicheres“ Textformat machen (z. B. aus Word eine RTF-Variante), sind im Konsultationsverfahren nicht bekanntgewordenen.

Aus den Stellungnahmen sind zwei Ansätze zu erkennen, wie die Anforderungen an sichere Dokumentenformate umgesetzt werden können.

- Einerseits ist es möglich, dass das Anwendungsprogramm selbst das sichere Dokumentenformat erstellt, verarbeitet und anzeigt. Die Signaturfunktion wird dann vom Signatur z. B. durch Eingabe seines PIN-Codes oder Fingerabdrucks mit diesem Programm ausgelöst, ohne dass eine gesonderte Darstellung erforderlich wäre.

  z. B. IBM: „Hersteller zukünftiger Business-Anwendungen werden Signierfunktionen clientseitig integrieren und somit selbst über Erscheinungsbild und Datenformat entscheiden (Beispiel: Web-Banking).“

  Der Vorteil dieser Variante liegt darin, dass keine umständliche Konvertierung und gesonderte Darstellung erforderlich ist. Der Nachteil besteht in der schwierigeren Evaluierung einer solchen Software.

- Andererseits kann ein „unsicheres“ Dokumentenformat aus der Anwendungssoftware übernommen und in einer eigenen Signatursoftware in ein sicheres Format konvertiert und angezeigt werden. Die Signatursoftware wendet dazu einen Formatfilter an, der die Konvertierung durchführt. Anschließend ermöglicht sie dem Signatur die Anzeige im gesicherten Format. Der Signator löst dann z. B. mit einem PIN-Code oder seinem Fingerabdruck die Signatur aus.

  z. B. A-Trust: „Konvertierungsprogramme gibt es wohl von jedem Dateiformat in jedwedes x-beliebig andere Format. Die Frage stellt sich hier nach einer sinnvollen, anwenderfreundlichen Einbindung solcher Konvertierungsprogramme in ein Signaturerstellungsprogramm das für „sichere Signaturen“ geeignet ist und vom ZDA zur Verfügung gestellt wird.

  In diesen Signaturerstellungsprogrammen, auch „Signaturclients“ genannt, werden keine Daten bearbeitet, sondern diese nur zur reinen Anzeige gebracht, um dem Signator dem Signaturgesetz entsprechend, die zu signierenden Daten anzuzeigen und so die „sichere Signatur“ zu ermöglichen.

  Wie oft ich also Daten konvertiere, zur Anzeige bringe, wieder konvertiere, etc. bleibt außerhalb des Signaturgesetzes und ist einzig eine Frage der anwenderfreundlichen Bedienbarkeit der vom ZDA angebotenen Programme.“

  Der Vorteil dieses Ansatzes besteht darin, dass der Signaturclient leichter evaluierbar ist und wahrscheinlich eine größere Zahl „unsicherer“ Dokumentenformate bearbeiten kann. Ein mögliches Problem könnte darin bestehen, dass bei der Konvertierung Inhalte verlorengehen, die dem Signator nicht auffallen, weil er das nach dem Konvertierungsvorgang dargestellte „sichere Dokumentenformat“ nicht sorgfältig liest.

Wie sind die Kosten „sicherer“ Dokumentenformate und von Konvertierungs- oder Codeprüfungsprogrammen für die Anbieter, die Signatoren und die Empfänger signierter Nachrichten einzuschätzen?

Konkrete Kosteneinschätzungen wurden durch das Konsultationsverfahren nicht bekannt.

Zwischen dem Signator und seinem Zertifizierungsdiensteanbieter gibt es ein vertragliches Naheverhältnis, im Rahmen dessen der Signator vom Anbieter über die Problematik „sicherer“ und „unsicherer“ Dokumentenformate informiert werden kann und in dem der Anbieter den Signatoren Software zur Verfügung stellen kann. Wie aber kann der Empfänger signierter Nachrichten überprüfen, ob es sich um sichere Dokumentenformate handelt und wie erlangt er Zugang zu Software, mit der er diese Überprüfung vornehmen kann?

A-Trust betont, dass es im natürlichen Bestreben eines Zertifizierungsdiensteanbieters sein werde, sichere Dokumentenformate zu empfehlen und die Verbreitung solcher Formate voranzutreiben. Denn das Produkt des Zertifizierungsdiensteanbieters sei die Ermöglichung der „sicheren Signatur“.

Nach Ansicht von Datakom soll dem Empfänger des elektronischen signierten Dokuments die Software nötigenfalls „für non-commercial use“ unentgeltlich zur Verfügung gestellt werden.

iTA: „Wenn es eine Veröffentlichung der behördlich zugelassenen sicheren Dokumentenformate gibt, kann auch jeder Marktteilnehmer überprüfen, ob das jeweilig signierte Dokument in einem sicheren Format dargestellt ist. Damit erscheint der Vertrauensschutz in geeigneter Form gewährleistet.“ (Anzumerken ist, dass das SigG kein behördliches Zulassungsverfahren für Dokumentenformate vorsieht.)

Ein technischer Distributionsmechanismus für sichere Dokumentenformate ist offenbar noch in weiter Ferne.

Die Signaturverordnung trifft keine Aussage darüber, welche Rechtsfolgen entstehen könnten, wenn der Signator die Pflichten des § 7 Abs. 2 nicht einhält und „unsichere“ Dokumentenformate signiert. Welche Rechtsfolgen könnte dies haben bzw. welche Rechtsfolgen wären im Sinne des Vertrauensschutzes geboten?

Die Stellungnahmen enthalten keine juristischen Ausführungen zu dieser Frage. A-Trust verweist auf die freie Beweiswürdigung (thematisiert aber nicht die Schriftform), iTA nimmt auf mögliche Missbrauchsfälle Bezug.

Aufbewahrung der privaten Schlüssel

Soweit der Aufsichtsstelle bekannt ist, gibt es am Markt bereits eine Reihe von Chipkarten, die nach ITSEC bzw. nach FIPS 140-1 evaluiert wurden. Decken diese Evaluierungen alle Anforderungen der Signaturverordnung ab?

Die Stellungnahmen zu dieser Frage waren teilweise widersprüchlich. Es gibt eine Reihe von Chipkarten, die nach dem deutschem Signaturgesetz ITSEC E4 hoch evaluiert wurden bzw. werden, wohingegen die österreichische Signaturverordnung bei im wesentlichen den selben Sicherheitsanforderungen lediglich eine Evaluierung nach den Kriterien von ITSEC E3 hoch verlangt.

Concord-Eracom und Globalsign sowie Siemens gehen davon aus, dass die von ihnen eingesetzten bzw. angebotenen Chipkarten, welche nach deutschem Signaturgesetz evaluiert wurden bzw. werden, auch die österreichischen Anforderungen erfüllen.

A-Trust ist der Ansicht, dass mit den Zertifikaten der zur Zeit erhältlichen Chipkarten nicht die notwendige Sicherheit garantiert werden könne. Diese Evaluierungen hätten nicht das Ziel gehabt, die umfassende und der Signaturverordnung entsprechende Sicherstellung der Aufbewahrung der privaten Signaturschlüssel zu gewährleisten. Dies werde sich erst ändern, wenn die ersten Chipkarten nach ITSEC E3 zertifiziert sein würden, bzw. wenn die notwendigen Common Criteria Profile im Rahmen der EU-Richtlinie bereitgestellt würden und dann nach diesen evaluiert werden könne.

Ob eine konkrete Evaluierung die Anforderungen der SigV erfüllt, ist gemäß § 18 Abs. 5 SigG und § 9 SigV von einer Bestätigungsstelle zu bescheinigen. Die Bestätigungsstelle A-SIT geht davon aus, dass die von den maßgeblichen Herstellern angebotenen Chipkarten nach diesen Bestimmungen bescheinigbar sind.

Sind in diesem Zusammenhang Sicherheitsprobleme bekannt, die noch nicht in ausreichender Weise gelöst wurden?

In den Stellungnahmen wurden keine grundsätzlichen ungelösten Sicherheitsprobleme bekannt. Es könnten aber im Einzelfall Sicherheitsprobleme bekannt werden, auf die ein Anbieter mit dem Widerruf von Zertifikaten reagieren müsste. Card Solutions: „Es sind in diesem Zusammenhang derzeit keine Sicherheitsprobleme bekannt, die noch nicht in ausreichender Weise gelöst wurden. Bei den umfangreichen Versuchen Chipkarten zu attackieren können sich aber im Laufe der Zeit vereinzelt neue Sicherheitsprobleme ergeben. Diese wurden in der Vergangenheit meist rasch gelöst, wobei in der Regel nur neue Chipkartenversionen davon profitieren.“ Auch Datakom gibt an, dass derzeit keine Sicherheitsprobleme bekannt seien.

IBM und iTA sehen als zusätzliche Sicherheitsmaßnahme für die Zukunft einen auf der Karte integrierten Zähler, der bei jeder Verwendung des Signaturschlüssels um eins erhöht wird und dem Signator bei jedem Signiervorgang angezeigt wird. Nach Ansicht von iTA könnte die Sicherheit darüber hinaus erhöht werden, indem die Eingabe des PIN-Codes oder des Fingerabdruckes direkt auf der Karte erfolgt. Nach Ansicht von Card Solutions sollte die Möglichkeit der Autorisierung durch Fingerabdruck auf der Chipkarte oder am Kartenleser forciert werden. Siemens schlägt vor, dass die Bildung des Hashwerts teilweise mit Hilfe der Chipkarte erfolgt.

Die vermeintlich höhere Sicherheit biometrischer Karten wird von Siemens kritisch beleuchtet: Das Überprüfen von biometrischer Information (Minutien) mit Referenzdaten sei ein vergleichsweise sehr aufwändiger Vorgang und bedürfe einer sogenannten Matcher-Software. Es gäbe Bestrebungen, diese Software möglichst kompakt zu gestalten (Micro-Matcher), so dass sie auf einem 8-Bit-Chip-Betriebsystem ablauffähig sei, um die Überprüfung der präsentierten Daten mit den gespeicherten Referenzdaten vom Chip selbst vornehmen zu lassen. Derzeit gäbe es keine bekannten Chipkarten und Chipkarten-Betriebsysteme, die sowohl das Matchen von biometrischen Daten als auch asymmetrische kryptographische Verfahren böten. Erst wenn diese Kriterien beide erfüllt seien, könne man von einem PIN-Ersatz durch Fingerprint sprechen – alle anderen Softwareimplementierungen außerhalb des Chip stellten eine Bedrohung des Sicherheitsniveaus dar. Siemens weist außerdem auf das Problem hin, dass bei Multiapplikationskarten verschiedene PIN-Codes erforderlich sind, der Fingerabdruck aber global sei.

Zu bedenken ist auch, dass man seinen eigenen Fingerabdruck im Gegensatz zu einem PIN nicht ändern oder widerrufen kann. Daher werden biometrische Systeme oft nur in Kombination mit einem PIN eingesetzt, um das Problem des PIN-Weitersagens einzudämmen (vgl. Siemens).

Inwieweit gibt es bereits Alternativlösungen zu Chipkarten, die geeignet wären, die Anforderungen des Signaturgesetzes und der Signaturverordnung zu erfüllen?

Alle Stellungnahmen gehen davon aus, dass die Sicherheitsanforderungen zum gegenwärtigen Zeitpunkt nur durch eine Hardwarelösung erfüllt werden können (vgl. z. B. Siemens). Der Einsatz von Chips empfehle sich dadurch selbst, dass er ein völlig unabhängiges System darstelle – ein von der sonstigen weltweiten Vernetzung abgetrenntes Rechnersystem also, das individuell verwaltet und personalisiert werden könne (A-Trust). Alternativprodukte seien derzeit am Markt für einen breit gestreuten Einsatz noch nicht einsetzbar (vgl. IBM, iTA).

Siemens verwies darauf, dass die Karte nur das Trägermedium für das eigentliche Sicherheitsmodul, den Chip, sei. Diese Art von Sicherheitsmodul könne sich auch in einem Handy, auf einer Steckkarte im PC oder in einem Organizer (PDA) befinden. Das Scheckkartenformat, das meistens mit dem Begriff Chipkarte assoziiert werde, sei also sekundär.

Card Solutions wies darauf hin, dass die elektronische Signatur zunehmend auch in Handys zum Einsatz kommen werde. In den neuesten Ausarbeitungen für GSM-Erweiterungen sei eine gesicherte und authentische Übertragung von Daten mittels Handy enthalten. Dieser Standard (Wireless Identification Module, WIM) regle einerseits die Herstellung und Verwaltung von gesicherten Übertragungskanälen (Wireless Transport Layer Security, WTLS) und basiert andererseits auf dem Konzept der elektronischen Signaturen. WIM werde in der Regel in die heute verwendeten SIM-Chipkarten integriert, könne aber bei Dual-Slot Handys auch als eigene Chipkarte ausgeführt sein. Ein WAP-Handy mit WIM-Funktion könne eine bequeme und vor allem preisgünstige Alternative zu den herkömmlichen Chipkartenlesern darstellen. Card Solutions verwies dazu auch auf ein eigenes Produkt.

Wie sind die Kosten der jeweiligen Möglichkeiten, private Schlüssel sicher zu verwahren, einzuschätzen?

Konkrete Kosteneinschätzungen wurden durch das Konsultationsverfahren nicht bekannt.

Kontrolle des Signiervorganges

Inwiefern ist es beim gegebenen Stand der Technik möglich, die unbefugte Verwendung von privaten Schlüsseln verlässlich zu verhindern? Für wie praktikabel werden die im Konsultationsdokument dargestellten Sicherheitsmaßnahmen eingeschätzt bzw. welche anderen Sicherheitsmaßnahmen gibt es?

Zu den im Konsultationsdokument angesprochenen Sicherheitsmaßnahmen (Auswahl des Betriebssystems, Auswahl der Anwendersoftware, Verwenden von Virenprüfprogrammen, spezielle Sicherheitsfunktionen der Signatursoftware, Eingabe des PIN-Codes in eine Spezialtastatur/Biometrie) waren die Stellungnahmen erstaunlich wenig konkret. A-Trust ist sogar der Ansicht, dass sich diese Frage für sichere Signaturen gar nicht stelle. Die technische Umsetzung der sicheren Verwendung der privaten Schlüssel sei durch den 6-stelligen PIN gewährleistet.

In einigen der Stellungnahmen wurde allgemein festgehalten, dass eine 100-prozentige Kontrolle des Signaturvorgangs nicht möglich sei und jede Hardware- oder Softwarekomponente ein Sicherheitsrisiko berge (iTA) bzw. dass eine Signaturerstellungssoftware allen Gefahren einer missbräuchlichen Verwendung ausgesetzt sei (IBM). IBM betonte in diesem Zusammenhang die Information und Aufklärung des Benutzers über Gefahren und korrekte Nutzung der Signaturkarte. Siemens äußerte den Wunsch, die Telekom-Control oder A-SIT sollten eine Standardkonfiguration für einen PC definieren, an Hand derer Trust-Center-Anbieter ein Bündel aus Hardware und Software zusammenstellen können, und für dessen Komponenten eine (kostenpflichtige?) Wartung – d. h. Evaluierung von neuen Versionen angeboten wird. Dazu muss angemerkt werden, dass die rechtlichen Anforderungen sich nur auf die Signaturerstellungseinheiten beziehen, die aber nur einen Teil der Systemumgebung abdecken (vgl. EG 15 der Signaturrichtlinie 1999/93/EG). Eine sichere Systemumgebung ist wichtig, es gibt aber keine konkreten Anforderungen des Signaturgesetzes und der Signaturverordnung dazu.

Die folgenden konkreten Sicherheitsmaßnahmen kamen im Konsultationsverfahren hervor:

Siemens sprach zur Verbesserung der Sicherheit Möglichkeiten der Verschmelzung von Chipkarte und Signatursoftware an. Eine Möglichkeit bestehe darin, dass die Signatursoftware selbst signiert werde. Vor dem Zugriff auf die Chipkarte erfolge eine Prüfung der Signatur, um das Einschleusen von „Trojanern“ zu erkennen. Eine weitere von Siemens angesprochene Möglichkeit besteht darin, den Hashwert teilweise auch auf der Chipkarte zu errechnen.

Siemens hält aber auch fest: „Alle Konfigurationsvorschriften inklusive zwingender Verwendung eines Virenschutzprogrammes sind berechtigt und richtig, wie kann jedoch der Empfänger einer signierten Nachricht die Zustände zum Zeitpunkt des Signierens am System des Signators überprüfen und die Echtheit der Signatur verifizieren? Diese Vorschläge und Empfehlungen sind also letztlich als (Selbst)Schutz des Senders/Signators zu sehen, helfen dem Empfänger aber nicht, ein höheres Maß an Sicherheit über die Signatur zu erlangen.“

Die Stellungnahme von Card Solutions geht detailliert auf einige Möglichkeiten ein, die Freigabe der Chipkarte mittels PIN oder biometrischer Daten technisch abzuwickeln. Einige der Vorschläge von Card Solutions stellen aber Eingabeerleichterungen dar, die für sichere elektronische Signaturen durch § 7 Abs. 3 SigV ausgeschlossen werden.

Es ist klar, dass jeder einzelne Signator die Sicherheit seines eigenen Rechners nach seinen Bedürfnissen nach Belieben steigern kann – je nachdem wie viel Aufwand er dafür betreibt und zu welchem Verlust an Funktionalität er bereit ist. Inwieweit gibt es aber praktikable Sicherheitsmaßnahmen, die sich standardisieren und auf eine größere Zahl von Signatoren anwenden lassen?

Aus den Stellungnahmen ergeben sich praktisch ausschließlich Verbesserungsmöglichkeiten im Bereich der Chipkarte (vgl. oben).

IBM und iTA sehen als zusätzliche Sicherheitsmaßnahme für die Zukunft einen auf der Karte integrierten Zähler, der bei jeder Verwendung des Signaturschlüssels um eins erhöht wird und dem Signator bei jedem Signiervorgang angezeigt wird. Nach Ansicht von iTA könnte die Sicherheit darüber hinaus erhöht werden, indem die Eingabe des PIN-Codes oder des Fingerabdruckes direkt auf der Karte erfolgt. Nach Ansicht von Card Solutions sollte die Möglichkeit der Autorisierung durch Fingerabdruck auf der Chipkarte oder am Kartenleser forciert werden. Siemens schlägt vor, dass die Bildung des Hashwerts teilweise mit Hilfe der Chipkarte erfolgt.

Aus der Sicht des Empfängers einer signierten Nachricht betrachtet, ist vor allem interessant, ob Sicherheitsmängel dem Signator zugerechnet werden können (gibt dieser z. B. die Chipkarte samt PIN-Code weiter, was sich vom Zertifizierungsdiensteanbieter nicht verhindern lässt, dann haftet der Signator dennoch). Inwieweit können Sicherheitsmaßnahmen es sicherstellen, dass die Kompromittierung der Sicherheitsmaßnahmen dem Signator zugerechnet werden kann?

Zu dieser Frage brachte das Konsultationsverfahren keine neuen Erkenntnisse.

Eine weitere Steigerung der Sicherheit aus der Sicht des Empfängers einer signierten Nachricht besteht darin, dass gewisse Sicherheitsmaßnahmen vom Signator nicht einmal dann außer Kraft gesetzt werden können, wenn er es wünscht (beispielsweise kann der Signator selbst an den eigenen privaten Schlüssel nicht heran, wenn dieser in einer entsprechenden Chipkarte gespeichert ist). Gibt es in diesem Zusammenhang weitere mögliche Sicherheitsmaßnahmen?

Diese Frage bringt einen der wesentlichsten Auffassungsunterschiede hinsichtlich der technischen Realisierung der sicheren elektronischen Signatur zum Ausdruck. Es gibt zwei mögliche Positionen, die ungefähr folgendermaßen charakterisiert werden können.

- Die eine Auffassung sieht die einzelnen technischen Komponenten als Bausteine an, die nach internationalen Standards frei kombinierbar zusammenarbeiten. Der Signator kann eine „sichere“ Chipkarte auch mit einer „unsicheren“ Software verwenden. IBM etwa geht davon aus, dass die Anbieter zukünftiger Anwendungssoftware die Signierfunktion in ihre Anwendungen einbauen werden und daher auch nicht bereitgestellte oder empfohlene Signatur-Clients verwendet werden. Eine Folge dieser freien Kombinierbarkeit: „Der Empfänger eines signierten Dokumentes hat keine Möglichkeit, die Art der Erstellung der Signatur (außer der Zertifikatsinformation, die ihm versichert, dass die Signatur auf einer SmartCard erstellt wurde) zu erkennen. Aufgrund gängiger und akzeptierter Normen kann und muß die Smartcard auch von COTS (Commercial off the shelf software) angesprochen werden.“

- Nach der anderen Auffassung hingegen müssen die eingesetzten technischen Komponenten in irgendeiner Form miteinander verschmolzen werden. Die Chipkarte darf demnach nur mit einem „sicheren“ Signaturclient zusammenarbeiten, welcher wiederum nur „sichere“ Dokumentenformate verarbeitet. Nicht einmal der Signator selbst darf in der Lage sein, den „sicheren“ Signaturclient durch eine nicht vom Zertifizierungs-diensteanbieter zu ersetzen oder einer nicht vom Zertifizierungsdiensteanbieter freigegebenen Anwendungssoftware eines anderen Anbieters den Zugriff auf die Chipkarte ermöglichen. Dies bringt dem Empfänger der Nachricht die Sicherheit, dass die Signaturerstellung auch wirklich unter Verwendung eines den Anforderungen der SigV entsprechenden Signaturclients und Dokumentenformates erfolgte (wenngleich auch keine Sicherheit gegeben ist, dass am Rechner des Signators keine „trojanische“ Software eingesetzt wurde). Für den Zertifizierungsdiensteanbieter bedeutet diese technische Lösung ein Abgehen von technischen Standards, die die freie Kombinierbarkeit von Produkten ermöglichen, und eine dementsprechend große Einschränkung am Markt.

  Wohl auch deshalb wird die Verschmelzung der Komponenten von keiner Stellungnahme verlangt. Siemens erwähnt einige Möglichkeiten (Hashwertbildung teilweise auf der Karte, Signierung der Signatursoftware), sieht sie aber nicht als zwingend, sondern als Möglichkeiten der Verbesserung der Sicherheit an. A-Trust wird das Padding des Hashwerts zwingend auf der Karte vorsehen (das bedeutet, dass die Karte nur für Signatur, nicht aber für Entschlüsselung eingesetzt werden kann), verhindert aber nicht,

dass andere als die von A-Trust selbst bereitgestellten Signaturprodukte aufdie Karte zugreifen.

Es wird diskutiert, dass die sichere elektronische Signatur auch Personen zur Verfügung stehen soll, die nicht über einen eigenen PC und Internetzugang verfügen. Diese Personen könnten an öffentlichen Terminals – etwa in Gemeindeämtern oder Banken – am elektronischen Rechts- und Geschäftsverkehr teilnehmen. Welche Anforderungen müsste man an solche Terminals stellen bzw. wie könnte der Signator erkennen, ob er dem Gerät vertrauen kann?

In den Stellungnahmen werden verschiedene Möglichkeiten von Empfehlungen öffentlicher Terminals erwähnt. A-Trust hält Hinweise vom Zertifizierungsdiensteanbieter, welche Terminals als vertrauenswürdig gelten, für die beste Möglichkeit. Card Solutions schlägt ein gesetzlich geschütztes Piktogramm vor, welches von den Anbietern von Zertifizierungsdiensten mit Genehmigung der Telekom-Control (oder einer von ihr beauftragten Organisation wie A-SIT) vergeben werden könnte. (Anm.: Diese gesetzliche Möglichkeit gibt es nicht, vgl. aber § 17 SigG und § 18 Abs. 6 SigV.) Nach Ansicht von IBM kann die elektronische Signatur mit heutiger Technik nur auf Geräten in einem kontrollierten Umfeld (vergleichbar den Selbstbedienungsautomaten im Finanzdienstleistungsbereich) zum Einsatz kommen.

Wie sind die Kosten der jeweils vorgeschlagenen Sicherheitsmaßnahmen einzuschätzen?

Konkrete Kosteneinschätzungen wurden durch das Konsultationsverfahren nicht bekannt.

Verwendung von Schlüsseln für andere Zwecke

Wie viele Schlüsselpaare sollte man typischerweise verwalten, um die wesentlichen Funktionen abzudecken (z. B. eines für sichere elektronische Signatur – also starke Rechtswirkungen, eines für Verschlüsselung und ein drittes für Authentifizierung und automatisierte Signaturen mit schwachen Rechtswirkungen, z. B. für automatisierte Empfangsbestätigungen)?

SigG und SigV enthalten keine Vorschriften über andere Anwendungen als Signaturanwendungen. § 3 Abs. 4 SigV legt aber fest, dass die Signaturerstellungsdaten nur für jene Zwecke verwendet werden dürfen, für die sie bestimmt sind. Um auch andere Zwecke (in der Praxis sind derzeit vor allem SSL- und S/MIME-Verschlüsselung und die SSL-Authentifizierung relevant) abdecken zu können, halten manche Autoren der Stellungnahmen zwei Schlüsselpaare (IBM), andere Autoren drei Schlüsselpaare (Siemens, Concord-Eracom) für erforderlich bzw. zweckmäßig.

Dass für Verschlüsselung und für Signatur unterschiedliche Schlüsselpaare verwendet werden müssen, wird offenbar als selbstverständlich vorausgesetzt und daher in manchen Stellungnahmen gar nicht explizit angesprochen.

Deutlich zu unterscheiden ist nach den Stellungnahmen auch zwischen der Authentifizierung und der Signaturfunktion. Siemens bezeichnet den im Konsultationsdokument beschriebenen Angriff über den SSL-Handshake als durchaus ernst zu nehmen.

Siemens: „Die Anzahl der Schlüsselpaare scheint zumindest 3 zu betragen:

Erstes Paar: Digitale Signatur nach dem SigG, gleichgestellt der eigenhändigen Unterschrift.

Zweites Paar: Verschlüsselung (wobei der private Schlüssel für Backup-Zwecke exportierbar sein muß)

Drittes Paar: Authentisierung im allgemeinen (z.B. für Kerberos Anmeldung an Windows 2000, SSL-Authentisierung, e-commerce Anwendungen)“

Nach der Stellungnahme von IBM würde es genügen, neben dem Signaturschlüssel ein weiteres Schlüsselpaar für Authentifizierung und Verschlüsselung (SSL, S/MIME) einzusetzen.

Siemens spricht in der Stellungnahme Probleme mit der Handhabung im Chipkartenbetriebssystem an, die entstehen, wenn mehrere Schlüsselpaare mit unterschiedlichen PIN-Codes auf der selben Chipkarte verwaltet werden sollen.

Wie kann der Anbieter verhindern, dass der Signator seine Schlüssel zweckwidrig nutzt? Der X.509-Standard erlaubt die Angabe der keyUsage im Zertifikat. Gibt es darüber hinaus praktikable Methoden?

A-Trust bringt zu Recht vor, dass die Angabe der keyUsage die zweckwidrige Verwendung technisch nicht verhindern kann. Wie A-Trust an anderer Stelle ausführt, wird A-Trust das Padding des Hashwerts zwingend auf der Karte durchführen. Die Nutzung des privaten Schlüssels zur Entschlüsselung (nicht aber die Nutzung zur Authentifizierung) ist dadurch technisch ausgeschlossen.

Sichere Signaturprüfung

Aus § 9 Abs. 2 und § 7 Abs. 5 des Entwurfs der SigV ergibt sich ein Unterschied zwischen einer „normalen“ Signaturprüfung und einer „sicheren“ Signaturprüfung, welche nach ITSEC E3 „hoch“ evaluiert wurde. Inwieweit besteht ein Bedarf an einer solchen „sicheren“ Signaturprüfung und gibt es technische Komponenten, die eine sichere Signaturprüfung vornehmen und ITSEC E3 „hoch“ evaluiert sind?

Ein Bedarf an sicherer Signaturprüfung wird vor allem für Gerichtsverfahren gesehen (vgl. A-Trust). Dazu müssen Zertifizierungsdiensteanbieter die Prüfung der auf ihren qualifizierten Zertifikaten basierenden sicheren elektronischen Signaturen anbieten (§ 7 Abs. 6 SigG). iTA bezeichnete die sichere Signaturüberprüfung durch andere als Signatoren als wünschenswert und für die breite Anwendung der elektronischen Signatur als notwendig, dies entspräche nach Ansicht von iTA aber einer in der Praxis nicht durchsetzbaren Kann-Bestimmung. Die Qualität einer Überprüfung von Signaturen müsse dem Ermessen des jeweils Betroffenen überlassen bleiben.

IBM geht davon aus, dass der breite Einsatz von ITSEC E3 hoch zertifizierter Software zur Signaturprüfung nicht zu erwarten sei. Serverseitig würden die Signaturprüfung überwiegend in Business-Applikationen eingebaut werden und daher kaum einer Evaluierung zugeführt werden. Das heiße aber nicht, dass nicht signaturgesetzkonforme Komponenten zum Einsatz kämen (wie z. B. die FIPS 140-1 Level 4-evaluierten Crypto-Hardwarekomponenten in allen IBM-Großrechnern).

iTA und Siemens verwiesen darauf, dass es „inkompatibel“ (iTA) bzw. eine „punktuell unrealistisch hohe Hürde“ (Siemens), dass § 9 SigV an die sichere Signaturprüfung eine höhere Anforderung (ITSEC E3 hoch) als an den secure viewer (ITSEC E2 hoch) stellt.

Noch sehr schlecht scheint bei den meisten Programmen die Überprüfung der Gültigkeit der Zertifikate zu funktionieren. Das automatisierte Nachschlagen in Verzeichnissen und Überprüfen von CRLs sowie das automatisierte Überprüfen

von Zertifikatshierarchien ist noch kaum implementiert. Die Überprüfung der Gültigkeit des Zertifikates ist daher meist händisch vorzunehmen. Inwieweit gibt es bereits Produkte, bei denen die Überprüfung automatisiert abläuft?

In den Stellungnahmen wird eine Automatisierung und Vereinfachung der Signaturprüfung erwartet (vgl. A-Trust). Siemens verweist insbesondere auf das OCSP-Protokoll, welches eine einfache, automatisierte Möglichkeit schaffen werde, fremde Zertifikate und Signaturen einfach, unkompliziert und sicher prüfen zu können. Derzeit befinde sich das Protokoll aber in einem sehr frühen Stadium und es gäbe nach dem Wissensstand von Siemens kein Produkt, das diesen neuen Standard bereits implementiert hätte.

Weitere Fragen

Zu den im Konsultationsdokument gestellten Fragen nach dem Bedarf an Verschlüsselungssoftware und nach Dokumentenverwaltungssystemen, die die sichere Aufbewahrung von signierten Dokumenten in großer Zahl ermöglichen, wurden keine konkreten Stellungnahmen abgegeben.

A-Trust betont für Verschlüsselungssoftware die Bedeutung weltweiter Akzeptanz und die weit verbreitete Integration in Standardsoftware sowie die bestmögliche kryptographische Sicherheit. Globalsign kündigte an, ein Langzeitarchiv und einen Zeitstempeldienst anbieten zu wollen.

Aus der Stellungnahme von Siemens: „Die Anforderungen, die zumeist von Kunden an den Hersteller von Kryptographie-Produkten herangetragen werden, widersprechen oft den sicherheitstechnischen Anforderungen. Im Vordergrund stehen dabei meistens die minimale Anzahl von notwendigen PIN Eingaben, das transparente Agieren im Hintergrund (der Anwender soll in seinem Arbeitsprozeß so gut wie nichts merken), das Offenhalten von fall-back Konzepten („wenn der Administrator schnell etwas nachsehen muß, soll er sofort und jederzeit trotzdem in das System kommen, eine Datei lesen können, etc.“) und die völlige Wiederherstellbarkeit im Fall von Ausfällen, Crash aber auch nach dem Ausscheiden von Mitarbeitern.“

Zu verweisen ist auch auf die ausführliche Stellungnahme des Amtes der oberösterreichischen Landesregierung, in dem der praktische Einsatz elektronischer Signatur in der Landesverwaltung erörtert wird.

Anhang

Im Folgenden sind die im Konsultationsverfahren eingelangten Stellungnahmen wiedergegeben. Sämtliche Stellungnahmen sind – mit Ausnahmen der Beilagen zu den Stellungnahmen von Concord-Eracom und von Globalsign Austria – ungekürzt wiedergegeben. Von der Telekom-Control GmbH wurde lediglich das Layout vereinheitlicht. Weiters wurden die in Begleitschreiben oder auf Deckblättern enthaltenen Informationen über die Autoren der Stellungnahmen redigiert und jeweils ans Ende der Stellungnahme gestellt.

A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH i. Gr.

Die A-Trust sieht sich in erster Linie als Zertifizierungsdiensteanbieter (=ZDA), der „qualifizierte Zertifikate“ ausgibt und weist darauf hin, daß sich die Stellungnahme immer auf den Einsatz dieser Zertifikate bezieht.

zu Dokumentformate

Gibt es beim gegenwärtigen Stand der Technik – abgesehen von simplen Formaten wie Ascii (text/plain) – bereits „sichere“ Dokumentenformate, deren Spezifikation allgemein verfügbar ist und mit denen dynamische Veränderungen und unsichtbare Daten ausgeschlossen oder doch zumindest in ihrer Problematik reduziert werden können – etwa Subvarianten von RTF oder von Postscript?

A-TRUST: Hierbei läßt sich das Problem nicht alleine dadurch lösen, daß Spezifikationen für u.U. neue Dateiformate frei verfügbar sind, denn ohne eine sinnvolle Verbreitung, bzw. Implementierung in Standardsoftware hilft das beste Format nichts im Sinne der Probleme des Einsatzes der „sicheren Signatur“. Selbst wenn diese Formate infolge in Standardsoftware implementiert wird, ist es dem ZDA (=Zertifizierungsdiensteanbieter) auferlegt Hinweise über Programme zur Verfügung zu stellen, mit denen eine „sichere Signatur“ möglich ist.

Ein ZDA wird daher immer in Kontakt mit der Softwareindustrie stehen müssen, um Produkttests, bzw. auch Implementierungen der eigenen Signaturtools in Standardsoftware, in die Wege leiten zu können.

Gibt es beim gegenwärtigen Stand der Technik praktikable Konvertierungsprogramme, mittels derer Dokumente aus Standardformaten in solche „sicheren Formate“ konvertiert werden können? Inwieweit besteht die Möglichkeit, Dokumente in „sicheren Formaten“ elektronisch weiterzuverarbeiten?

A-TRUST: Konvertierungsprogramme gibt es wohl von jedem Dateiformat in jedwedes x-beliebig andere Format. Die Frage stellt sich hier nach einer sinnvollen, anwenderfreundlichen Einbindung solcher Konvertierungsprogramme in ein Signaturerstellungsprogramm das für „sichere Signaturen“ geeignet ist und vom ZDA zur Verfügung gestellt wird.

In diesen Signaturerstellungsprogrammen, auch „Signaturclients“ genannt, werden keine Daten bearbeitet, sondern diese nur zur reinen Anzeige gebracht, um dem Signator dem Signaturgesetz entsprechend, die zu signierenden Daten anzuzeigen und so die „sichere Signatur“ zu ermöglichen.

Wie oft ich also Daten konvertiere, zur Anzeige bringe, wieder konvertiere, etc. bleibt außerhalb des Signaturgesetzes und ist einzig eine Frage der anwenderfreundlichen Bedienbarkeit der vom ZDA angebotenen Programme.

Bei einer weiteren Bearbeitung der Daten verliert die ursprüngliche Signatur allerdings die Gültigkeit und muß abermals signiert werden.

Wie sind die Kosten „sicherer“ Dokumentenformate und von Konvertierungs- oder Codeprüfungsprogrammen für die Anbieter, die Signatoren und die Empfänger signierter Nachrichten einzuschätzen?

A-TRUST: Je stärker verbreitet die Tools sein werden, desto einfacher und günstiger können diese an die Anwender weitergegeben werden.

Zwischen dem Signator und seinem Zertifizierungsdiensteanbieter gibt es ein vertragliches Naheverhältnis, im Rahmen dessen der Signator vom Anbieter über die Problematik „sicherer“ und „unsicherer“ Dokumentenformate informiert werden kann und in dem der Anbieter den Signatoren Software zur Verfügung stellen kann. Wie aber kann der Empfänger signierter Nachrichten überprüfen, ob es sich um sichere Dokumentenformate handelt und wie erlangt er Zugang zu Software, mit der er diese Überprüfung vornehmen kann?

A-TRUST: Der ZDA muß, dem Signaturgesetz folgend, die Informationen bereitstellen, die dem Anwender, bzw. dem Signator, erkennen lassen, ob es sich bei dem von ihm zu signierenden elektronischen Datenformat um ein Sicheres handelt.

Da die „sichere Signatur“, neben der Ausgabe von „qualifizierten Zertifikaten“, in erster Linie auf der Sicherheit beruht, daß die Unveränderlichkeit der zu signierenden Daten gewährleistet ist, wird es im natürlichen Bestreben eines ZDA sein, diese Formate zu empfehlen und die Verbreitung solcher Formate voranzutreiben. Denn das Produkt des ZDA ist die Ermöglichung der „sicheren Signatur“.

Die Signaturverordnung trifft keine Aussage darüber, welche Rechtsfolgen entstehen könnten, wenn der Signator die Pflichten des § 7 Abs. 2 nicht einhält und „unsichere“ Dokumentenformate signiert. Welche Rechtsfolgen könnte dies haben bzw. welche Rechtsfolgen wären im Sinne des Vertrauensschutzes geboten?

A-TRUST: Dies stellt die Judikatur in jedem individuellen Falle im Rahmen der freien Beweiswürdigung fest. Denn durch den Einsatz von nicht sicheren Dokumentenformaten gilt nicht die Annahme der „sicheren Signatur“ wie sie im Signaturgesetz definiert wurde.

zu Aufbewahrung der privaten Schlüssel

Soweit der Aufsichtsstelle bekannt ist, gibt es am Markt bereits eine Reihe von Chipkarten, die nach ITSEC bzw. nach FIPS 140-1 evaluiert wurden. Decken diese Evaluierungen alle Anforderungen der Signaturverordnung ab?

A-TRUST: Nein – da mit den Zertifikaten der zur Zeit erhältlichen Chipkarten nicht die notwendige Sicherheit garantiert werden kann. Diese Evaluierungen hatten nicht das Ziel die umfassende und der, Signaturverordnung entsprechenden, Sicherstellung der Aufbewahrung der privaten Signaturschlüssel zu gewährleisten. Eine Kompromittierung, also ein Auslesen eines privaten Schlüssels für ein ausgegebenes „qualifiziertes Zertifikat“ hätte fatale Folgen für den ZDA, der alle bisher ausgegebenen Zertifikate widerrufen müßte. Somit muß auch der ZDA, auch wenn dies eine Verteuerung der einzusetzenden Hardwaretechnologie bedeutet, auf die Sicherheitskriterien der Signaturverordnung bestehen.

Dies wird sich ändern, wenn die ersten Chipkarten nach ITSEC-3 zertifiziert sein werden, bzw. wenn die notwendigen Common Criteria Profile im Rahmen der EU-Richtlinie bereitgestellt werden und dann nach diesen evaluiert werden kann.

Sind in diesem Zusammenhang Sicherheitsprobleme bekannt, die noch nicht in ausreichender Weise gelöst wurden?

A-TRUST: Das Leitmotto eines ZDA sollte lauten „Wer Sicherheit anbietet, muß auch selbst sicher sein“! Daraus resultiert, das schon die Möglichkeit einer Kompromittierung auszuschließen sein sollte und nicht auf den Ernstfall und deren Wahrscheinlichkeit spekuliert werden darf.

Inwieweit gibt es bereits Alternativlösungen zu Chipkarten, die geeignet wären, die Anforderungen des Signaturgesetzes und der Signaturverordnung zu erfüllen?

A-TRUST: Der Einsatz von Chips empfiehlt sich dadurch selbst, dass er ein völlig unabhängiges System darstellt. Ein von der sonstigen weltweiten Vernetzung abgetrenntes Rechnersystem also, das individuell verwaltet und personalisiert werden kann. Erst wenn neue technische Errungenschaften diesen Anforderungen entsprechen können und im finanziell vernünftigen Rahmen verfügbar sind, werden sich hier Alternativen empfehlen.

Wie sind die Kosten der jeweiligen Möglichkeiten, private Schlüssel sicher zu verwahren, einzuschätzen?

A-TRUST: Da ihre privaten Schlüssel die Signaturerstellungseinheit, also die Chipkarte, niemals verlassen können, stellt sich die Frage nach der Möglichkeit die Smartcard sicher zu verwahren. Eine Handhabung ähnlich der Kreditkarten und ihren Ausweisen ist hier wohl die beste Lösung.

zu Kontrolle des Signiervorganges

Inwiefern ist es beim gegebenen Stand der Technik möglich, die unbefugte Verwendung von privaten Schlüsseln verlässlich zu verhindern? Für wie praktikabel werden die oben dargestellten Sicherheitsmaßnahmen eingeschätzt bzw. welche anderen Sicherheitsmaßnahmen gibt es?

A-TRUST: Für „sichere Signaturen“, also private Schlüssel die einem „qualifizierten Zertifikat“ zugeordnet sind, stellt sich diese Frage nicht.

Das Signaturgesetz verbietet sowohl ein Backup eines privaten Schlüssels des ZDA – ebenso wie die Vervielfältigung desselben. Die Verantwortung über den Token, der den privaten Schlüssels eines „qualifizierten Zertifikates“ enthält, obliegt dem Zertifikatsbesitzer.

Es handelt sich dabei also um Probleme der menschlichen Einflußnahme und nicht der technischen Realisierbarkeit.

Die technische Umsetzung der sicheren Verwendung, wird durch den 6-stelligen PIN gewährleistet. Zukünftig werden sicherlich Entwicklungen bei biometrischen Verfahren, in Kombination mit der Chiptechnologie, weitere Sicherheitsanforderungen erfüllen.

Es ist klar, dass jeder einzelne Signator die Sicherheit seines eigenen Rechners nach seinen Bedürfnissen nach Belieben steigern kann – je nachdem wie viel Aufwand er dafür betreibt und zu welchem Verlust an Funktionalität er bereit ist. Inwieweit gibt es aber praktikable Sicherheitsmaßnahmen, die sich standardisieren und auf eine größere Zahl von Signatoren anwenden lassen?

A-TRUST: Für die Massendatenverarbeitung empfehlen sich Signatursysteme, die in die Sicherheitsbereiche der Netzwerke integriert werden. Für solche Signatursysteme sollten die gleichen technischen Anforderungen gelten, wie für die Smartcards und die

Systemumgebung des ZDA, auch wenn diese dann infolge nicht als „qualifizierten Zertifikate“ auszuweisen sind, da sie an keine natürlichen Personen gebunden werden können.

Aus der Sicht des Empfängers einer signierten Nachricht betrachtet, ist vor allem interessant, ob Sicherheitsmängel dem Signator zugerechnet werden können (gibt dieser z. B. die Chipkarte samt PIN-Code weiter, was sich vom Zertifizierungsdiensteanbieter nicht verhindern lässt, dann haftet der Signator dennoch). Inwieweit können Sicherheitsmaßnahmen es sicherstellen, dass die Kompromittierung der Sicherheitsmaßnahmen dem Signator zugerechnet werden kann?

A-TRUST: Wenn der ZDA allen Auflagen des Signaturgesetzes nachkommt, also den Karteninhaber über alle möglichen, wahrscheinlichen und unwahrscheinlichen Notwendigkeiten informiert und die dementsprechende Signaturerstellungsumgebung bereitstellt, ist die rechtliche Verantwortung erfüllt.

Sollte der Signator seine Smartcard und seinen PIN weitergeben, liegt es auch in seiner vollen rechtlichen Verantwortung. Für dieses etwaige menschliche Problem, kann die A-Trust leider keine Sicherheitsmaßnahmen anbieten.

Eine weitere Steigerung der Sicherheit aus der Sicht des Empfängers einer signierten Nachricht besteht darin, dass gewisse Sicherheitsmaßnahmen vom Signator nicht einmal dann außer Kraft gesetzt werden können, wenn er es wünscht (beispielsweise kann der Signator selbst an den eigenen privaten Schlüssel nicht heran, wenn dieser in einer entsprechenden Chipkarte gespeichert ist). Gibt es in diesem Zusammenhang weitere mögliche Sicherheitsmaßnahmen?

A-TRUST: Der Signator hält mit der Smartcard seinen privaten Schlüssel in Händen und dieser ist für "sichere Signaturen" nach Signaturgesetz, nur brauchbar, wenn er in einem geschützten Token aufbewahrt wird. Die Freischaltung der Signaturfunktion durch PIN-Eingabe gilt jeweils nur für einen Signaturvorgang. Weiters implementiert die A-Trust eine Beschränkung der Verwendbarkeit des Signaturschlüssels durch zwingendes Padding des Hash-Wertes in der Karte.[1]

Es wird diskutiert, dass die sichere elektronische Signatur auch Personen zur Verfügung stehen soll, die nicht über einen eigenen PC und Internetzugang verfügen. Diese Personen könnten an öffentlichen Terminals – etwa in Gemeindeämtern oder Banken – am elektronischen Rechts- und Geschäftsverkehr teilnehmen. Welche Anforderungen müsste man an solche Terminals stellen bzw. wie könnte der Signator erkennen, ob er dem Gerät vertrauen kann?

A-TRUST: Am Besten geeignet scheinen im Moment Hinweise direkt vom ZDA, welche Terminals als vertrauenswürdig gelten. Der ZDA wird gerne diese Informationen bereitstellen.

[1] Abgedruckt ist eine Präzisierung gegenüber der ursprünglichen Stellungnahme, welche A-Trust mit E-Mail vom 27.03.2000 vorgenommen hat.

Wie sind die Kosten der jeweils vorgeschlagenen Sicherheitsmaßnahmen einzuschätzen?

A-TRUST: Dies läßt sich zur Zeit nicht beziffern. Da die Verbreitung dieser Systeme auch von der Kundenakzeptanz anhängt, wird sich hier wohl schnell eine verträgliche Preisbasis etablieren.

zu Verwendung von Schlüsseln für andere Zwecke

Wie viele Schlüsselpaare sollte man typischerweise verwalten, um die wesentlichen Funktionen abzudecken (z. B. eines für sichere elektronische Signatur – also starke Rechtswirkungen, eines für Verschlüsselung und ein drittes für Authentifizierung und automatisierte Signaturen mit schwachen Rechtswirkungen, z. B. für automatisierte Empfangsbestätigungen)?

A-TRUST: Dies obliegt den Anwendern. Die „Public Key Infrastructure“ läßt sich wohl in jedem Bereich andenken, der in Zusammenhang mit manuellen Bestätigungen und Signaturen betrachtet werden kann.

Wie kann der Anbieter verhindern, dass der Signator seine Schlüssel zweckwidrig nutzt? Der X.509-Standard erlaubt die Angabe der keyUsage im Zertifikat. Gibt es darüber hinaus praktikable Methoden?

A-TRUST: Die keyUsage im Zertifikat bringt nichts, da trotzdem jeder den öffentlichen Schlüssel einfach aus dem Zertifikat extrahieren kann und dann damit machen kann, was er will. Aber das ist, wie gesagt nur der öffentliche Schlüssel. Der private Schlüssel ist einzig und allein durch die Attribute, die ihm bei der Erzeugung in der Chipkarte mitgegeben werden, in seiner Verwendung eingeschränkt, in Falle A-Trust eben auf Signieren von Daten im PKCS#11- oder ISO9796-Format. Damit kann verhindert werden, daß der Schlüssel z. B. für Datenverschlüsselung eingesetzt wird. Nicht beeinflussbar bleibt natürlich was der Signator mit dem Schlüssel signiert.[2]

zu Sichere Signaturprüfung

Aus § 9 Abs. 2 und § 7 Abs. 5 des Entwurfs der SigV ergibt sich ein Unterschied zwischen einer „normalen“ Signaturprüfung und einer „sicheren“ Signaturprüfung, welche nach ITSEC E3 „hoch“ evaluiert wurde. Inwieweit besteht ein Bedarf an einer solchen „sicheren“ Signaturprüfung und gibt es technische Komponenten, die eine sichere Signaturprüfung vornehmen und ITSEC E3 „hoch“ evaluiert sind?

A-TRUST: Fast täglich erscheinen neue Signaturapplikationen am Markt. Auch hier orientieren sich die Hersteller immer mehr an der EU Richtlinie und den nationalen Gesetzgebungen für digitale Signaturen.

In Österreich ist die Signaturverordnung bereits in Kraft getreten, daher werden Technologieanbieter und Trust Center so rasch als möglich Hard.- u. Software anbieten, die die Anforderungen der „sicheren Signaturprüfung“ erfüllen. Die rechtlichen Notwendigkeit

[2] Abgedruckt ist eine Präzisierung gegenüber der ursprünglichen Stellungnahme, welche A-Trust mit E-Mail vom 27.03.2000 vorgenommen hat.

einer „sicheren Signaturprüfung“ ist außer Frage gestellt, da diese für Gerichtsverfahren etc. unerläßlich ist.

Noch sehr schlecht scheint bei den meisten Programmen die Überprüfung der Gültigkeit der Zertifikate zu funktionieren. Das automatisierte Nachschlagen in Verzeichnissen und Überprüfen von CRLs sowie das automatisierte Überprüfen von Zertifikatshierarchien ist noch kaum implementiert. Die Überprüfung der Gültigkeit des Zertifikates ist daher meist händisch vorzunehmen. Inwieweit gibt es bereits Produkte, bei denen die Überprüfung automatisiert abläuft?

A-TRUST : Hier werden in den kommenden Wochen und Monaten immer neue Produkte am Markt erhältlich sein, die diese Funktion(en) automatisieren und vereinfachen.

zu Weitere Fragen

Wie stellt sich der Bedarf nach Verschlüsselungssoftware dar (Transportverschlüsselung, verschlüsselte Aufbewahrung von Dokumenten)? Welche Anforderungen sind an Produkte zur Verschlüsselung zu richten?

A-TRUST: Die weltweite Akzeptanz und weitverbreitete Integration in Standardsoftware. Die Basis sollte auch hierbei die bestmögliche kryptographische Sicherheit sein.

Um signierte Dokumente in großer Zahl sicher aufbewahren zu können, werden spezielle Dokumentenverwaltungssysteme notwendig sein. Das Dokumentenformat soll auch noch nach langer Zeit lesbar sein. Die Dokumente sollen vor unabsichtlicher Zerstörung der Signatur geschützt sein (die Signatur kann z. B. zerstört werden, wenn ein signiertes Dokument geöffnet, ausgedruckt und wieder gespeichert wird, und die Anwendungssoftware dabei ein neues Datum „zuletzt gedruckt am:“ einfügt). Wie stellt sich der Bedarf nach Dokumentenverwaltungssystemen dar und welche Anforderungen werden an solche Produkte zu richten sein?

A-TRUST: Wie schon von ihnen erwähnt, müssen diese Programme auch nach extrem langen Zeitspannen sicherstellen, dass die Signaturen und die signierten Dokumente einwandfrei nachvollziehbar sind und das Erkennen von „sicher signierten Dokumenten“ ermöglichen.

Auch in diesem Bereich erwarten wir eine ständig wachsende Anzahl von Anbietern solcher Produkte, ebenso wie eine Vielzahl von Archivierungsapplikationen die in bestehende Software implementierbar sein wird.

A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH in Gründung; Kontakt: APSS GmbH, Hintere Zollamtsstrasse 17, 1031 Wien, Tel. 01/71773-3535, e-sign@apss.at, http://www.a-trust.at/

Card Solutions Chipkartensysteme-Entwicklungs- und BeratungsgmbH

Als unabhängiges Entwicklungs- und Beratungsunternehmen auf dem Gebiet der Chipkarten und Chipkartenlösungen und Marktleader in Österreich auf diesem Gebiet konzentriert sich CARD SOLUTIONS bei der Stellungnahme auf die Chipkarte und den Chipkartenleser. Eine ausführliche Stellungnahme war auf Grund der sehr kurzen zur Verfügung stehenden Zeit nicht möglich.

Zu den Fragen in Kapitel 2: Aufbewahrung der privaten Schlüssel

Es sind in diesem Zusammenhang derzeit keine Sicherheitsprobleme bekannt, die noch nicht in ausreichender Weise gelöst wurden. Bei den umfangreichen Versuchen Chipkarten zu attackieren können sich aber im Laufe der Zeit vereinzelt neue Sicherheitsprobleme ergeben. Diese wurden in der Vergangenheit meist rasch gelöst, wobei in der Regel nur neue Chipkartenversionen davon profitieren.

Es gibt natürlich auch Alternativlösungen zu Chipkarten, die geeignet wären, die Anforderungen des Signaturgesetzes und der Signaturverordnung zu erfüllen. Wenn man aber auch die wichtigen Faktoren Preis, Portabilität und Verfügbarkeit am Markt (inklusive der notwendigen Peripheriegeräte) berücksichtigt, existiert noch keine geeignete Alternative zur Chipkarte.

Zu den Fragen in Kapitel 3: Kontrolle des Signiervorganges

Es ist beim aktuellen Stand der Technik möglich, die unbefugte Verwendung von privaten Schlüsseln verläßlich zu verhindern. Voraussetzung dazu ist aber, daß der Signator vor jedem einzelnen Signaturvorgang der Chipkarte eine gesicherte Freigabe erteilt. Dies erfordert vor dem Signaturvorgang die Eingabe einer PIN oder biometrischer Daten und kann über die Peripheriegeräte eines PCs wie Tastatur, PC-Maus, Chipkartenleser etc. erfolgen. Die weiteren Freigaben eines Signaturvorganges könnten bis zum Ziehen der Chipkarte aus dem Chipkartenleser auch durch eine Taste am Chipkartenleser erfolgen. Wenn der Chipkartenleser in eine PC-Tastatur integriert ist, könnte sich diese Taste auch auf der PC-Tastatur befinden und diese Taste bei Bedarf direkt mit dem Chipkartenleser kommunizieren. Wichtig dabei ist, daß kein Programm im PC in der Lage ist, diesen Schutz zu umgehen. Derartige Chipkartenleser und PC-Tastaturen sind von verschiedenen Herstellern am Markt preisgünstig und in ausreichenden Stückzahlen zu bekommen. Die derzeit in der Signaturverordnung (§ 7) vorgesehene Ausschließung von Eingabeerleichterungen bei wiederholter Eingabe von Autorisierungscodes verbietet aber diese Art der Eingabe. Sie erscheint bei Einhaltung bestimmter Anforderungen (siehe u. a. oben) unbegründet und kann sogar die Sicherheit wesentlich reduzieren. Eine oftmalige Eingabe einer PIN erhöht die Gefahr einer Ausspähung, z.B. durch „über die Schulter schauen“, und eine Freigabe des Signaturvorganges vom PC aus ist, im Gegensatz zur Freigabe am Chipkartenleser, derzeit noch vielfältigen Manipulationsmöglichkeiten ausgesetzt.

Die Sicherheit kann noch wesentlich verbessert werden, wenn anstatt einer Taste die gesamte PIN oder das biometrische Merkmal mindestens einmal pro Steckvorgang der Chipkarte in den Chipkartenleser und von dort direkt an die Chipkarte übertragen wird oder direkt in die Chipkarte eingegeben wird. Chipkartenleser und PC-Tastaturen, die diese Anforderung erfüllen, sind von verschiedenen Herstellern am Markt preisgünstig und in ausreichenden Stückzahlen zu bekommen. Sie sind außerdem auch bei anderen sicherheitssensiblen Anwendungen wie z.B. im Zahlungsverkehr und der Ladefunktion von elektronischen Geldbörsen von großer Bedeutung und wären daher grundsätzlich für alle PCs zu empfehlen.

Solange Chipkarten keine Freigabe des Signaturvorganges durch eine Funktionstaste (oder ähnliches) auf der Chipkarte oder eine direkte PIN bzw. biometrische Eingabe ermöglichen, können für sichere elektronische Signaturen nur kontaktbehaftete Chipkarten (nach ISO/IEC 7816) zugelassen werden.

Bei kontaktbehafteten Chipkarten könnte nach einer erfolgreichen Eingabe der PIN (bzw. biometrischen Daten) auch der reine Steckvorgang in den Chipkartenleser als Freigabe für den Signaturvorgang dienen und damit auch die Funktionstaste beim Chipkartenleser eingespart werden. In diesem Fall muß dann aber die Chipkarte vor jedem Signaturvorgang aus dem Chipkartenleser herausgezogen und dann sofort wieder gesteckt werden. Wenn die Chipkarte nicht sofort wieder gesteckt wird, muß der Chipkartenleser diese vereinfachte Freigabe sperren (Löschen der PIN bzw. des biometrischen Merkmales im Chipkartenleser). Da bei dieser Methode mit einer erhöhten Anzahl an Steckvorgängen zu rechnen ist, muß dies zur Reduktion der Abnutzung der Chipkartenkontakte bei der Auswahl des Chipkartenlesers berücksichtigt werden.

Bei den biometrischen Daten zeigt der Markt, daß Fingerabdrucksysteme auf Chipkartenterminals, PC-Mäusen und PC-Tastaturen schon relativ preisgünstig verfügbar sind. Alle anderen biometrischen Daten sind vergleichsweise dazu noch teuer, bei richtiger Anwendung aber auch geeignet. Man sollte daher die aktuellen Möglichkeiten im Bereich des Fingerabdruckes forcieren. Der Fingerabdruck sollte aus Sicherheitsgründen und eventuellen „Fingerabdruckängsten“ des Signators nur am Chipkartenleser oder direkt in die Chipkarte eingegeben werden können und er darf den PC nie passieren. Der Fingerabdruck kann im Gegensatz zur PIN nicht vergessen werden und er bietet eine hohe Sicherheit bei der Freigabe der Signaturfunktion, wenn alle Zusatzanwendungen der multifunktionalen Chipkarte mit PINs oder anderen biometrischen Merkmalen authentisieren.

Die elektronische Signatur wird zunehmend auch in Handys zum Einsatz kommen. In den neuesten Ausarbeitungen für GSM-Erweiterungen ist eine gesicherte und authentische Übertragung von Daten mittels Handy enthalten. Dieser WIM (Wireless Identification Module) - Standard regelt einerseits die Herstellung und Verwaltung von gesicherten Übertragungskanälen (Wireless Transport Layer Security, WTLS) und basiert andererseits auf dem Konzept der elektronischen Signaturen. Die WIM-Funktionalität erweitert die elektronischen Signaturen auf die Mobilkommunikation. WIM wird in der Regel in die heute verwendeten SIM-Chipkarten integriert, kann aber bei Dual-Slot Handys auch als eigene Chipkarte ausgeführt sein.

In ein paar Jahren werden voraussichtlich mehr als die Hälfte WAP-Handys sein, d.h. Millionen von Handys allein in Österreich, und bei diesen die WIM-Funktion eine wichtige Rolle spielen. Es ist möglich, daß in ein paar Jahren die elektronische Signatur auf Handys stärker verbreitet ist als bei Personalcomputer. Bei der Betrachtung der elektronischen Signatur sollten daher WIM und Handy berücksichtigt werden. Die ersten WIM-Prototypen sind schon für Handys verfügbar (auch CARD SOLUTIONS hat in Wien eine eigene WIM auf einer JAVA-Card entwickelt). Ein WAP-Handy mit WIM-Funktion hat den Vorteil, daß es sowohl als eigenständiges Gerät mit sicherer elektronischer Signaturfunktion und Internetzugang operieren kann, als auch als externer Chipkartenleser (mit Tastatur und Bildschirm) eines PCs. Damit können relativ schnell Millionen von PCs mit sicheren, multifunktionalen Chipkartenlesern ausgestattet werden. Gerade für private Anwender oder mobile Außendienstmitarbeiter von Firmen stellt dies eine bequeme und vor allem preisgünstige Alternative zu den herkömmlichen Chipkartenlesern dar.

Es sollte die sichere elektronische Signatur über öffentlich aufgestellte Geräte auch Personen zur Verfügung gestellt werden, die nicht über einen eigenen Internetzugang verfügen. Der Signator sollte dabei durch ein gesetzlich geschütztes Piktogramm, das leicht ersichtlich an den öffentlich aufgestellten Terminals aufgeklebt ist, erkennen, ob er einem

Terminal vertrauen kann oder nicht. Die Vergabe dieser Piktogramme könnte z.B. von den Anbietern von Zertifizierungsdiensten mit Genehmigung der Telekom-Control (oder einer von ihr beauftragten Organisation wie A-Sit) erfolgen. Das Piktogramm bietet keine technische Sicherheit, ermöglicht aber bei strenger Vergabe und regelmäßiger Kontrolle eine akzeptable Lösung zum Beispiel in Banken und Postämtern.

CARD SOLUTIONS Chipkartensysteme- Entwicklungs- und BeratungsgesmbH, Pfeiffergasse 2, 1150 Wien, Univ.-Doz. D.I. Dr. Ernst Piller, e-mail: piller@cardsol.at, Tel.: 89934

Concord-Eracom Computer Security GmbH

1. Einleitung

Im folgenden werden auf die Fragen des Dokuments „KonsultationSignatoren.doc", welches von der TKC zur Kommentierung veröffentlicht wurde, Stellung bezogen. Dabei wird unsere Sicht als Hersteller von SigG konformen Produkten dargestellt. Dem Dokument ist eine umfassende Produktbeschreibung unserer PKI-Produktfamilie beigefügt.

2. Stellungnahme

- zu Kapitel 2, erste Frage:

Derzeit werden in den beiden Deutschen SigG-konformen und akkreditierten Trust Centern Chipkarten mit dem Betriebssystem TCOS V2.0 (Rev. 2) und SETCOS V4.3.0 eingesetzt. TCOS ist nach ITSEC E4/hoch evaluiert und nach dem Deutschem SigG/SigV bestätigt worden. SETCOS befindet sich in der Endphase der Evaluation/Bestätigung oder hat diese bereits abgeschlossen. Die Anforderungen des Deutschen SigG/SigV stimmen weitestgehend mit den Anforderungen des Österreichischen SigG/SigV überein. Insofern sollten alle Anforderungen der Österreichischen SigV abgedeckt sein.

- Zu Kapitel 2, dritte Frage:

Unsere neue Produktfamilie PKI-8 und PKI-ESM (siehe beigefügte Produktbeschreibung) können während der Initialisierung vom Security Officer so konfiguriert werden, daß die Anforderungen des SigG/SigV (Deutschland, Österreich) erfüllt werden. Sie sind im wesentlichen für Anwender mit hohen Performanceansprüchen konzipiert.

- Zu Kapitel 4, erste Frage:

Das akkreditierte Trust Center der Deutschen Post AG speichert drei RSA Schlüsselpaare mit 1024 Bit Länge in unterschiedliche Verzeichnisse auf der Chipkarte. Die Verwendung der Schlüssel ist jeweils mit einer PIN gesichert. Die erwähnten 3 Einsatzmöglichkeiten bzw. Schlüsseltypen sind nach meinem Kenntnisstand ausreichend, um zukünftige Anwendungen abzudecken.

- Zu Kapitel 4, zweite Frage:

Die Einschränkung der Nutzungsmöglichkeiten obliegt der Software/Hardware des Herstellers des Signierprodukts. Unsere Produktfamilie PKI-8, PKI-ESM erlaubt die Einschränkung des Gebrauchs der Schlüssel für den vorbestimmten Zweck.

Anm. d. TKC: Die in der Stellungnahme erwähnte Beschreibung der Produkte von Concord-Eracom wurde aus Platzgründen nicht wiedergegeben. Sie ist unter http://www.eracom.com.au/products/pcasm.html abrufbar.

Ilja Ohliger, Concord-Eracom Computer Security GmbH (Deutschland). Kontakt Österreich: Concord Eracom Information Security Systems Austria GesmbH, Wolfganggasse 20, 1120 Wien, Tel. 01/8155700-0, jbogad@concord-eracom.at, http://www.concord-eracom.at

Datakom Austria GmbH

Die Datakom Austria hat das Konsultationspapier der Telekom Control mit Interesse aufgenommen und begrüßt die Möglichkeit als Zertifizierungsdiensteanbieter Stellung zu nehmen. Es soll im Rahmen dieser Stellungnahme bewußt auf die Nennung von Produkten und Herstellern verzichtet werden (um ungewollte Interpretationen zu vermeiden).

ad Dokumentenformat, Verwendung von Schlüsseln für andere Zwecke, sichere Signaturprüfung und Verschlüsselungsprodukte

Das österreichische Signaturgesetz schafft Rechtssicherheit durch die verbindlichen Regelungen für Erbringer von Signatur- und Zertifizierungsdiensten sowie die Erstellung von elektronischen Signaturen, insbesondere im Bereich der qualifizierten Zertifikate und sicheren elektronischen Signaturverfahren.

Aufgrund dieser Regelungen ist es wünschens- und begrüßenswert, dass sichere elektronische Signaturen jedenfalls auf Basis eines qualifizierten Zertifikates geleistet werden müssen. Qualifizierte Zertifikate sollen daher – auch im Sinne der Rechtssicherheit – ausschließlich für sichere elektronische Signaturen genutzt werden. Dies soll auch ins Zertifikat aufgenommen werden (key usage). Für andere Zwecke, d.s. einfache/gewöhnliche Signaturen, Authentisierung und Verschlüsselung werden einfache/gewöhnliche Zertifikate herangezogen. Ob und inwieweit für die im letzten Satz genannten Verwendungszwecke ein oder mehrere Zertifikate verwendet werden, muß dem Zertifikatsinhaber überlassen sein. Im Unternehmensbereich empfiehlt sich hier im Bereich der Verschlüsselung (iSv Vertraulichkeit) jedenfalls die Nutzung eines „company-encryption-keys“ (symmetrisch oder asymmetrisch) um Probleme, z.B. aufgrund von Mitarbeiterwechseln uä zu vermeiden.

Für den Bereich „sichere Dokumentenformate“ und Überprüfung der sicheren elektronischen Signatur sei auf die entsprechenden Hersteller verwiesen. Dem Empfänger des auf Basis eines qualifizierten Zertifikats (sicher?)elektronischen signierten Dokuments sollte diese SW nötigenfalls „für non-commercial use“ unentgeltlich zur Verfügung gestellt werden. Anbieter von Businessapplikationen werden anzunehmenderweise entsprechende Signaturclients in Lösungen integrieren (z.B. Web-Banking, Web-Bestellungen uä). Sollte die Signaturprüfung „Unregelmäßigkeiten“ liefern, so wird wahrscheinlich Rücksprache mit dem Signator nicht zu umgehen sein – wie im traditionellen Bereich (kann vom ZDA nicht beeinflußt werden)

ad Aufbewahrung privater Schlüssel

Zur Frage, inwieweit die am Markt befindlichen, nach ITSEC bzw. FIPS 140-1 evaluierten Chips, die Anforderungen der Signaturverordnung abdecken, muß auf die internationalen Normungsgremien verwiesen werden. Sicherheitsprobleme sind zum gegenwärtigen Zeitpunkt nicht bekannt

ad Kontrolle des Signiervorganges

Für die Weitergabe von PINs kann der Zertifizierungsdiensteanbieter unter gewissen Bedingungen nicht haftbar gemacht werden können: Beim a-sign Zertifizierungsdienst erfolgt die Initialisierung/Personalisierung der Signaturkarten, in Anwesenheit und unter Aufsicht des Zertifikatswerbers/Signators in der lokalen Registrierungsstelle. Weiters muß der Zertifikatswerber/Signator im Rahmen dieses Personalisierungsprozesses auch die PIN, die dem Schutz seines privaten Schlüssels dient, vergeben. (Der Prozeß wird hier aufs wesentliche verkürzt und läßt daher technische Tatsachen außer acht. Die genaue Vorgehensweise würde den Rahmen der Stellungnahme sprengen) Es erfolgt also keine

zentrale Schlüsselgenerierung bzw. keine zentrale PIN-Vergabe durch Datakom, sondern immer vom Signator selbst. Die Karte wird nach dreimaliger Falscheingabe gesperrt.

Bei Bereitstellung öffentlicher Terminals müssen die Provider die Anforderungen des Signaturgesetzes (damit auch Signaturverordnungen) sowie die Vorgaben der ZDAs erfüllen und die auf diesen Terminals zulässigen ZDAs erkennbar machen.

Datakom Austria GmbH, Wiedner Hauptstraße 73, 1040 Wien, Tel. 01/50145-0, Fax. 01/50260, kunden.service@datakom.at, http://www.datakom.at/, http://a-sign.datakom.at/

Globalsign Austria GmbH i. Gr.

1. Globalsign Austria verwendet Smartcards von Gemplus, die nach dt. Signaturgesetz E4 hoch zertifiziert werden und damit auch dem österr. Signaturgesetz entsprechen. Die ersten Karten sollen Ende Mai verfügbar sein.

2. Die Applikation Webform (siehe beiliegendes attachment) ist ein Formularmanagementsystem, das für verschiedene Anwendungen geeignet ist. Wichtig ist, dass Webform am Beginn einer Zertifizierung steht (mit BSI u. TÜV) um dem Signaturgesetz zu entsprechen. Dabei sind vor allem die Komponenten Signaturerstellungssoftware, Prüfsoftware, Secure Viewer, Mehrfachsignaturen zu prüfen.

Wichtig ist hier vor allem, dass Daten aus anderen (auch nicht sicheren) Formaten in das .esd Format von Webform übernommen werden können, wobei esd für electronic signed document Format steht.

Mit Webform können diese Daten dann sicher signiert und verschickt werden und auch beim Empfänger wieder in ein anderes Format übernommen werden (nach erfolgreicher Überprüfung der sicheren Signatur mit zertifizierter Software). D. h. der signaturgesetzkonforme Teil läuft dann unter der zertifizierten Software Webform ab, die Daten können aber in andere Formate übernommen und weiterverarbeitet werden. Im rechtlichen Sinn ist aber immer das .esd file heranzuziehen.

3. Wir sind auch mit Partnern dabei einen signaturgesetzkonformen Zeitstempeldienst aufzubauen und auch ein sog. Trusted Archiv, ein Langzeitarchiv für signierte Dokumente, um diese auch nach langer Zeit für z. B. Beweise vor Gericht etc. verfügbar zu haben.

Ich sehe genauso wie im Papier beschrieben noch eine Menge offener Fragen bez. sicherer Digitaler Signatur die sich erst im Laufe der Zeit klären werden. Um dem User eine bedienerfreundliche Umgebung für sichere Digitale Signaturen zu ermöglichen, überlegen wir eine Reihe von Maßnahmen innerhalb des Globalsign Netzwerkes.

Anm. d. TKC: Das in der Stellungnahme erwähnte Attachment beschreibt das von Globalsign Austria angebotene Formularsystem w-form. Aus Platzgründen wird im Folgenden nur ein Auszug aus dieser Beschreibung wiedergegeben.

Leistungsmerkmale des elektronischen Formularsystems w-form

- Einfache, rasche Gestaltung von sämtlichen Formularen der internen Unternehmenskommunikation, des Geschäftsverkehrs mit Kunden, der Standardisierung von Verwaltungs- und sonstigen Unternehmensabläufen, von öffentlichen Institutionen intern für die eigene Administration und extern im Verkehr mit Kunden.

- Integrierte Signaturanbindung in den Formularen sowohl in Form von Software-Zertifikaten (GlobalSign, u.a.) als auch durch Einbindung spezifischer Hardware zur Unterstützung von Smartcardsystemen (Chipkarte und Code), sowie Biometrics-Systemen für die Fingerabdrucksignatur und andere Identifikationssysteme wie z.B. Identifikation via Armbanduhr (Swatch, etc.).

- Standardmäßige Integration der Software-Zertifikate einschließlich der Zurverfügungstellung von geeigneten Schnittstellen mit einem Signaturdataport-Modul.

- Spezieller Formulardarstellungsmechanismus, der geeignet sicherstellt, daß ein Formular in seinem gesamten Umfang vor dem Unterzeichnen auch gelesen werden kann. Sämtliche weitere Signatursysteme können optional angebunden werden. Dabei wird explizit auf Formularteile hingewiesen, welche die Sichtbarkeitskriterien in irgend einer Form (z.B. durch Schriftgröße, Farbe, Überdeckung, Art der Gestaltung) verletzen können. Durch diesen Viewer (Formulardarstellungsmechanismus) wird im Normalfall bei der Formulargestaltung nur mehr auf Viewer-verträgliche Elemente zurückgegriffen.

- Integrierte Datenbankanbindung samt der Zurverfügungstellung einer Reihe von allgemeinen Schnittstellen (SQL, DBF, ASCII, ODBC, LDAP) wie auch speziellen Schnittstellen (SAP, OAX, BAAN, Concord, Navision) an das System des Anwenders eines Formulars und an das System des Empfängers eines Formulars. Damit wird ein möglichst automatisches Formularausfüllen und eine automatische Übernahme der Daten von ausgefüllten signierten Formularen auf der Empfängerseite ermöglicht.

- Intelligente Formularprüfung als integrierter Bestandteil eines jeden Formulars nach dem objektorientierten „Formular prüfe dich“ Prinzip. Dabei wird ein detaillierter Prüfmechanismus für das korrekte Ausfüllen von Pflichtfeldern und für eine syntaktisch und semantisch sowie plausibiltätsmäßig korrekte, sowie vollständige Formularerfassung unterstützt. Diese Formularprüfung ist essentiell für eine reibungslose Datenübernahme ins System des Formularempfängers. Geprüft wird detailliert (Feld für Feld und Zusammenhänge zwischen mehreren Eingaben in verschiedenen Feldern) mit den umfassenden Möglichkeiten der Formularsprache w-script. Dabei ist eine syntaktische und logische Prüfmöglichkeit vorhanden und es wird auch eine Datenbankanbindung via SQL unterstützt und Resultate von Datenbankabfragen ausgewertet. Darüberhinaus wird für noch speziellere Prüfungen, die in einem externen System stattfinden oder vom Dateiformat her von w-script nicht unterstützt werden, die Integration einer externen Formularprüfungsfunktion (Java, JNI C++) gewährleistet. Diese Funktion wiederum kann die gesamte oder Teile der Prüfung eines oder mehrerer Formularfeldinhalte oder Zusammenhänge zwischen Formularfeldinhalten prüfen. Ein Beispiel dafür wäre die Prüfung eines Internet-Kreditwerbers bei einer Bank auf dessen Bonität oder hinsichtlich Vermerken auf KSV-/UKV-/Schufa-Auskunftslisten.

- Unterstützung von Online-Informations- und Dokumentenbeschaffung. Künftige Informationsanbieter werden genormte Schnittstellen (z.B. via JAVA Socket) anbieten, mit denen eine Online-Informationseinholung möglich ist. Anwendungen wie Grundbuch, Telefonbuch, Bonitätsauskünfte, Auskünfte über die Richtigkeit oder Existenz von Dokumenten sind geeignete Vorreiter dieses IT-Trends. Damit wird vielen Institutionen ermöglicht, teure Verwaltungsabläufe, bei welchen vom Leistungswerber eine Liste von Dokumenten beizubringen ist, via Internet abzuwickeln (z.B. Ansuchen zur Ausstellung eines Reisepasses im öffentlichen Bereich; automatische Bonitäts- und Grundbuchsinformationseinholung bei einer Bank.

- Garantiert ausreichende Sicherheit während der Übertragung im Internet durch das Modul w-transaction. Dieses Software-Modul stellt sicher, daß während der Übertragung im Internet niemand das Formular lesen oder erfolgreich verändern bzw. durch die Ausweisung mit einer falschen IP-Nummer im Internet erfolgreich widerrechtlich empfangen kann. Durch ein gegenseitig zertifiziertes System, das vor der Übertragung die Identität der Server prüft und erst danach das Formular sendet, wird ein Manipulationsversuch erschwert. Durch die asynchrone Verschlüsselung mittels public und private key wird Sicherheit vor unbefugten Manipulationen erreicht. Nur nichtmanipulierte Dokumente erhalten einen Eingangsstempel (Zeitstempel). Manipulierte Formulare werden mit dem entsprechenden Vermerk an den Sender zurückgesandt. Zusätzlich wird der Sender zu zwei verschiedenen Zeitpunkten via email über diese Manipulation verständigt.

- Plattformunabhängigkeit: das elektronische Formularsystem läuft systemübergreifend, kann ein business administration system integrieren und ist plattformunabhängig. Ein Einsatz des elektronischen Formularsystems kann überall dort erfolgen, wo Java 1.2 verfügbar ist. Lösungen für X-Windows unter UNIX, Windows NT und Windows 98 sind Standard.

- E-commerce-Eignung der elektronischen Formulare um auch höherpreisige Bestellungen rechtsverbindlich im Internet abwickeln zu können. Die elektronischen Formulare eignen sich hervorragend für jede Versandhaustätigkeit im Internet.

- Eignung der elektronischen Formulare für die Vertragsabwicklung via Internet. Durch die ausgezeichnete Darstellungs-, Erfassungs-, Gestaltungs-, Signatur- und Übertragungsmöglichkeit wird eine rechtsverbindliche Vertragsabwicklung via Internet ermöglicht und dadurch das gemeinsame Gestalten und Abändern eines Vertragswerks von zwei Vertragsparteien via Internet entscheidend erleichtert. Es soll dabei ein Mechanismus unterstützt werden, der zwei Formulare vergleicht und dabei die Änderungen von einer Vertragsversion zur nächsten hervorheben kann.

- Wenn ein via Internet eingereichtes Formular beim Empfänger einlangt, sind sämtliche automatischen Prüfungen bereits durchgeführt und die Dokumente als Anlagen zum Formular verpackt. Beispielsweise wäre die Bonitätsauskunft, Staatsbürgerschaftsnachweis, Meldenachweis und ein Grundbuchauszug schon beim eingereichten Formular als Anlage dabei. Mit dieser Auskunft kann der Kreditreferent nun seine Arbeit beginnen. Im öffentlichen Bereich wäre die Einrichtung einer electronic registration Stelle denkbar, sodaß jeder Bürger sich einmalig elektronisch registrieren läßt und sämtliche weiteren Behördenwege mittels seines elektronischen Zertifikats via Internet vornehmen kann und seine Unterlagen (Dokumente) automatisch elektronisch als Anlagen beigefügt werden. Vom elektronischen Formularsystem wird jedenfalls eine Schnittstelle für ein solches Online-Informations- und Dokumenten-Beibringungs-System unterstützt.

Dipl.-Ing. Gerald Stickler, Globalsign Austria GmbH in Gründung. Kontakt: Innovation Systems Informationstechnologie GmbH, Hauptstraße 2, 2630 Ternitz, 02630/39699, office@innosys.at, http://www.innosys.at/

IBM Österreich

Das österreichische Signaturgesetz fördert den elektronischen Geschäftsverkehr und bietet der Wirtschaft und den Bürgern die Basis für neue Entwicklungsmöglichkeiten.

e-Business expandiert mit einer Eigendynamik, die in kurzen Abständen neue Produkte und Standards etabliert. Diese Standardisierungen geben lokalen Eigenentwicklungen und Vorschriften, die über die allgemeinen europäischen oder weltweiten Gepflogenheiten hinausgehen, keine Chance auf Akzeptanz.

Wichtige internationale Konsortien, wie z.B. Netzwerke von Finanzdienstleistern (IDENTRUS, SET, etc.) haben bereits hochsichere und trotzdem praktikable und wirtschaftliche Technologien für elektronischen Geschäftsverkehr im Einsatz. Diese Technologien sollten der Anhaltspunkt dafür sein, was Gesetze und Verordnungen zum jeweiligen Zeitpunkt als sicher anerkennen. Da sich die Technologien rasch weiterentwickeln, sollten die gesetzlichen Anforderungen mit dem technologischen Fortschritt steigen, jedoch nicht versuchen, lokale Zusatzanforderungen zu stellen.

IBM bietet eine umfangreiche Palette an e-business Hard- und Softwareprodukten sowie Dienstleistungen. Im speziellen ist IBM Österreich der Technologie-Provider für a-sign, dem Trustcenter der DATAKOM Austria. IBM arbeitet auch international eng mit SmartCard-Herstellern (Gemplus, Siemens, Schlumberger, u.a.) sowie Herstellern von sicherheitsrelevanten Softwarekomponenten zusammen. Besondere Erfahrung stammt auch aus der Zusammenarbeit mit und der Erstellung von Lösungen für IDENTRUS und GTA (Global Trust Authority), sowie der Kooperation mit den meisten großen Bankinstituten. Weiters ist IBM Gründungsmitglied der International Security Trust and Privacy Alliance (ISTPA), deren Aufgabe es ist, die Interoperabilität von Zertifikaten, Produkten und Plattformen sicherzustellen.

1.) Dokumentenformate

Es ist heute üblich, Dokumente, die i. a. mit Textverarbeitungsprogrammen erzeugt werden und – wenn diese vor Veränderung zu schützen sind – in das Acrobat PDF-Format zu konvertieren. Fehlerhafte Konvertierungen sind i. a. deutlich erkennbar. Eine Überprüfung der korrekten Konvertierung vor Anbringung der Signatur ist natürlich zu empfehlen.

Wie im „normalen“ schriftlichen Geschäftsverkehr sollten die Geschäftspartner darauf achten, dass das Dokument keine nachträgliche Manipulation und Missinterpretation ermöglicht.

Benötigt der Empfänger eines signierten Dokumentes auch eine weiterbearbeitbare Fassung, dann kann diese ja auch (signiert oder unsigniert) mitgeschickt werden. Ebenso wird sich an heutigen Gepflogenheiten, Dateien in signierten Mails zu verschicken, nichts wesentlich ändern.

Plain-ASCII-Text ist natürlich überall dort verwendbar, wo kürzere Informationen, wie Formularinhalte, formlose Anträge, Aufzählungen, Bestellungen nach Artikelnummern, etc. signiert werden. In diese Kategorie fallen auch einfache Web-/HTML-Formulare, deren Inhalt so gestaltet sein sollte, dass die Formatierungsinformation nicht den Inhalt / die zu signierende Nutzinformation „erschlägt“.

Hersteller zukünftiger Business-Anwendungen werden Signierfunktionen clientseitig integrieren und somit selbst über Erscheinungsbild und Datenformat entscheiden (Beispiel: Web-Banking).

2.) Aufbewahrung der privaten Schlüssel

Bei der Frage von ITSEC / FIPS-zertifizierten Chipkarten verweisen wir auf die Angaben der jeweiligen Hersteller von Signaturkarten. Verschiedene Anbieter von SmartCards versprechen entsprechende Zertifizierungen in näherer Zukunft.

Aus Kostengründen und wegen der erfolgten Standardisierung und Marktakzeptanz der Smartcards gibt es heute kaum Alternativen für einen breitgestreuten Einsatz.

3.) Kontrolle des Signiervorganges

Die Signatur wird zwar mit Hilfe von zertifizierten Smartcards erfolgen, eine Signaturerstellungs-Software ist natürlich allen Gefahren einer mißbräuchlichen Verwendung ausgesetzt. Die Nutzung der digitalen Signatur muß auf den heute üblichen (und unsicheren) Plattformen erfolgen können. Auch die kurzen Update-Zyklen von wenigen Monaten (Betriebssysteme, Browser, Mail-Systeme, etc.) tragen nicht zur Erhöhung der Sicherheit bei und verhindern eine Festlegung auf gewisse Produkte und Funktionalitäten. Daher werden auch bereitgestellte Signier-Client-Funktionen laufend Ergänzungen / Updates erfahren. Anbieter zukünftiger Anwendungssoftware (z.B. Homebanking-Anwendungen) werden die Signierfunktion in ihre Anwendungen einbauen und daher auch nicht bereitgestellte oder empfohlene Signier-Clients verwenden.

Information und Aufklärung des Benutzers über Gefahren und korrekte Nutzung der Signaturkarte sind wichtig. Da missbräuchliche Nutzung des Signaturschlüssels verhindert werden soll, sollten auch zusätzliche Nutzungen der Signaturkarte (zum Verschlüsseln, für andere Applikationen, etc.) mit entsprechender Vorsicht behandelt werden.

Der Empfänger eines signierten Dokumentes hat keine Möglichkeit, die Art der Erstellung der Signatur (außer der Zertifikatsinformation, die ihm versichert, dass die Signatur auf einer SmartCard erstellt wurde) zu erkennen. Aufgrund gängiger und akzeptierter Normen kann und muß die Smartcard auch von COTS (Commercial off the shelf software) angesprochen werden.

Eine Zusatzfunktion könnte in Zukunft ein auf der Karte integrierter Zähler sein, der bei jeder Verwendung des Signaturschlüssels um eins erhöht wird und dem Signator bei jedem Signiervorgang angezeigt wird.

Geräte mit öffentlichem Zugang (Kioske, etc.) sollten – wenn auf diesen die digitale Signatur verwendet werden soll – mit einem dem jeweiligen Stand der Technik entsprechenden Schutz versehen sein: Firewall-gesichert, Intrusion-überwacht, virengeschützt, etc.. Daher wird die Signatur (mit heutiger Technik) nur auf Geräten in einem kontrollierten Umfeld (vergleichbar den Selbstbedienungsautomaten im Finanzdienstleistungsbereich) zum Einsatz kommen.

4.) Verwendung von Schlüsseln für andere Zwecke

Im allgemeinen genügt neben dem Signaturschlüssel ein weiteres Schlüsselpaar für Authentizierung und Verschlüsselung (SSL, SMIME).

5.) Sichere Signaturprüfung

Der breite Einsatz von (E3hoch) zertifizierter (Client-)Software zur Signaturprüfung ist nicht zu erwarten, da die Zertifizierungen nicht mit den raschen technologischen Entwicklungen und fortschreitenden Standardisierungen Schritt halten könnten.

Serverseitig werden die Signaturprüfungen überwiegend in die Business-Applikationen eingebaut werden und daher kaum einer Zertifizierung zugeführt werden. Das heißt nicht, dass nicht signaturgesetzkonforme Komponenten zum Einsatz kommen (wie z.B. die FIPS 140-1 Level 4 zertifizierten Crypto-Hardwarekomponenten in jedem IBM-Großrechner und optional in den mittleren und kleineren Rechnersystemen).

Herbert Jochum, IBM Österreich, Obere Donaustraße 95, 1020 Wien, Tel. 21145-2360, e-mail: herbert_jochum@at.ibm.com

iTA – Information Technology Austria

Österreichischer Verband der Informationstechnologie Industrie

Der iTA, der Österreichische Verband der Informationstechnologie Industrie, hat das Konsultationspapier der Telekom-Control mit großem Interesse aufgenommen und begrüßt die Möglichkeit, damit auch als Interessenvertretung der in Österreich tätigen Unternehmen der IT-Industrie Stellung zu diesem, für die weitere Entwicklung der elektronischen Kommunikationsformen wichtigen, Fragenkomplex beziehen zu können. Wir wollen in unserer Stellungnahme bewusst auf die Nennung einzelner Produkte verzichten und vielmehr die grundsätzlichen Positionen und Vorschläge kommunizieren.

Unsere Mitgliedsunternehmen stehen bei der Implementierung von richtungsweisenden Anwendungsprojekten an vorderster Front und sind daher nicht nur interessiert, sondern auch in der Lage, in der Diskussion die notwendige Orientierung an der Praxis einzubringen.

Aus diesem Grund haben wir auch die Frage hinsichtlich der Gründung einer geeigneten gemeinsamen Institution als potentielle Bestätigungsstelle ventiliert, dies aber zum gegenwärtigen Zeitpunkt – in Anbetracht der mit Gesetzesbeschluss erfolgten Gründung des Vereins “Zentrum für sichere Informationstechnologie” (A-SIT) – vorerst nicht weiter verfolgt, obwohl A-SIT für die einschlägige Industrie und ihre Fachleute nicht zugänglich ist.

Mehrere Initiativen der EU sowie auch der österreichischen Bundesregierung sind von dem Bemühen geprägt, den potentiellen Nutzern von neuen Technologien eine weitgehende Rechtssicherheit im Zusammenhang mit deren Nutzung zu gewähren, so auch die Verabschiedung des Signaturgesetzes und der Signaturverordnung. Damit soll ermöglicht werden, die bereits vorhandenen technischen Möglichkeiten der elektronischen Kommunikation einer breiten Nutzung zuzuführen, was eine der Grundvoraussetzungen für das Funktionieren der Informationsgesellschaft darstellt.

Das österreichische Gesetz und auch die EU-Richtlinie gehen von verschiedenen Stufen der Signatur zugeordneten Rechtssicherheit aus, wobei die höchste Stufe die (nahezu volle) Gleichsetzung mit der eigenhändischen Unterschrift erfährt. Es ist jedoch notwendig darauf hinzuweisen, dass für viele Anwendungsfälle dieses Höchstmaß an Sicherheit nicht unbedingt erforderlich ist. So müssen die Sicherheitsaufwendungen in einer vernünftigen Relation zu den abzudeckenden Risken stehen.

Es erscheint uns daher auch wesentlich darauf hinzuweisen, dass die entsprechenden verbindlichen Vorschriften, die unter anderem auf dem Ergebnis dieser Konsultation aufbauen, unserer Meinung nach nur für die Handhabung der „Sicheren Signatur“ entsprechend § 2 Z 3. SigG gelten.

Es ist uns jedoch wohl bewusst, dass die grundsätzlich bestehenden Sicherheitsprobleme natürlich auch bei normalen elektronischen Signaturen von Relevanz sind, aber in diesem Fall in die notwendige Aufklärung für Signatoren eingehen müssen.

Die entscheidende Frage wird wohl immer bleiben: „Sind die Kosten für die erkaufte zusätzliche Sicherheit in Einklang mit dem abzudeckenden Restrisiko?“

Dies zu betonen, ist unseres Erachtens nach deswegen so wichtig, weil die nach dem Wortlaut des Gesetzes und der dazugehörigen Verordnung geforderten Voraussetzungen nach unserer Marktkenntnis derzeit - und wahrscheinlich für eine absehbare Zukunft - nicht bzw. nur ungenügend abgedeckt werden können und es daher im Sinne einer raschen Verbreitung der elektronischen Unterschrift notwendig ist, die Verwendung von nicht

zertifizierten (zertifizierbaren) Produkten oder Produktzusammenstellungen nicht zu stigmatisieren.

Zu dem Konsultationspapier:

Wir teilen grundsätzlich die von der TKC aufgeworfenen Probleme und sehen, wie oben bereits erwähnt, derzeit keine am Markt erhältliche Lösung, um die Anforderungen von Gesetz und Verordnung nach dem Wortlaut derselben zu erfüllen. Wir bieten der TKC und dem A-SIT die Mitarbeit bei der Lösung der offenen Probleme an.

Wir regen an, zu einzelnen Themenkreisen, die in dem Papier gut abgegrenzt sind, Arbeitskreise einzusetzen, um praxisorientierte Lösungen zu erarbeiten, die sich auch im internationalen Gleichklang bewegen.

Was wir unbedingt vermeiden sollten, sind österreichspezifische Lösungen. Dies nicht nur wegen der Wahrscheinlichkeit der Inkompatibilität mit der einschlägigen EU-Richtlinie, sondern auch wegen der für die Entwicklung und Vermarktung zu kleinen Marktgröße Österreichs. Denn neben den gesetzlichen Bestimmungen wird nicht zuletzt der Preis über die Nutzung solcher Produkte entscheiden. Wir müssen zwischen zwingenden Erfordernissen und Empfehlungen differenzieren.

Im folgenden finden Sie unsere Positionen zu den einzelnen Punkten des Konsultationspapiers:

Zu 1. Dokumentenformate:

Wie richtig erwähnt, stellt sich auch bei Ascii (text/plain) die Frage nach dem verwendeten Charakterset. Diese Information müsste im signierten Dokument sichtbar sein und in geeigneter Form mitgespeichert sein.

Ein allen Anforderungen entsprechendes Programm ist am (Welt-)Markt nicht verfügbar. Eine Neuentwicklung müsste zumindest EU-weit gemeinsam erfolgen. Für die breite Nutzanwendung ist das Übersetzen in PDF-Files mit einigen zusätzlichen Überprüfungen (Filter) eine tragbare Lösung, die sich aber nach dem Buchstaben des Gesetzes nicht für die sichere Signatur eignet.

Die einzige Möglichkeit, ein Textdokument darstellungssicher und frei von Manipulationen darzustellen, ist, es als Bitmap zu speichern. Dies hat jedoch den gravierenden Nachteil, dass eine direkte Weiterverarbeitung nicht möglich ist. Eine zugegebenermaßen aufwendige Erweiterung der Sicherheit ist es, das Dokument in (irgend-)einem Dokumentenformat gemeinsam mit einem Bitmapabbild des Dokumentes gemeinsam (kombiniertes Dokument) zu signieren. Die Bitmapdarstellung hätte im Falle einer allfälligen Diskrepanz zwischen beiden Darstellungen die höhere Beweiskraft.

Eine mit Warnung versehene ”sichere Lösung” ist im Gesetz nicht vorgesehen. Gemäß §9 SigG muss der Zertifizierungsanbieter ein Zertifikat unverzüglich widerrufen, wenn die Gefahr einer missbräuchlichen Verwendung des Zertifikats besteht. Wenn kein sicheres allgemein verfügbares Dokumentenformat (von der Aufsichtsstelle beglaubigt) verfügbar ist, muss davon ausgegangen werden, dass eine nach dem Gesetz missbräuchliche Verwendungsgefahr besteht. Daher darf in diesem Fall bereits kein sicheres Zertifikat ausgegeben werden. Die Rechtsfolgen hätte in diesem Fall die TKC beziehungsweise die Bestätigungsstelle zu tragen.

Die hohen Anforderungen des Gesetzes und der Verordnung betreffen die „Sichere Signatur“. Gibt es kein sicheres Format, so ist die sichere Unterschrift nahezu wertlos! Wenn

es eine Veröffentlichung der behördlich zugelassenen sicheren Dokumentenformate gibt, kann auch jeder Marktteilnehmer überprüfen, ob das jeweilig signierte Dokument in einem sicheren Format dargestellt ist. Damit erscheint der Vertrauensschutz in geeigneter Form gewährleistet. Eine allfällige Ahndung wird durch die Sorgfaltspflicht des Anwenders hinfällig.

Eine Verfolgung einer trotzdem eingetretenen Verwendung eines „unsicheren" Formates erscheint nicht zielführend. Dies wird ja erst im konkreten Anlassfall wirksam und kann im Falle einer nachgewiesenen echten missbräuchlichen Verwendung entsprechend der bestehenden Rechtsordnung geahndet werden.

Die Information, um welches Datenformat es sich handelt, sollte im Dokument selbst angegeben werden.

Zu 2. Aufbewahrung der privaten Schlüssel

Es scheint uns zum heutigen Zeitpunkt keine praktisch einsetzbare Alternative zur Chipkarte zu geben.

Es sollte überdacht werden, ob man nicht einen Zähler auf der Chipkarte einführt, der die Signaturvorgänge hochzählt, um so auch dem Benutzer ein zusätzliches Sicherheitsgefühl gegenüber einer missbräuchlichen Verwendung zu geben.

Andere Verfahren und Techniken sind in Entwicklung und Erprobung, aber derzeit noch nicht generell am Markt einsetzbar.

Zu 3. Kontrolle des Signiervorganges

Eine 100 %-ige Kontrolle des Signiervorganges ist nicht möglich.

Jede HW-Einrichtung und jede SW-Komponente birgt ein Sicherheitsrisiko. Auch der in die Tastatur integrierte Chipkartenleser oder das Biometriklesegerät lassen sich nur dort sicher verwenden, wo die gesamte Installation einem entsprechenden, laufend überprüften, Sicherheitskonzept unterliegt. Dies ist bei den Zertifizierungsdiensteanbietern, aber auch bei großen institutionellen Rechenzentren gegeben, bei einem beliebigen Signator oder bei Selbstbedienungsterminals jedoch kaum.

Es ist anzunehmen, dass bei vielen dieser Institutionen dem jeweiligen Benutzer, der üblicherweise in einem Vertragsverhältnis mit der Institution steht, die Software für die Signaturerstellung integriert in einem Gesamtsoftwarepaket, wahrscheinlich sogar on-online (immer auf dem letzten Stand) erhält. Dabei wird die vereinbarte Sicherheitsstufe (höchste Sicherheit?), ebenso wie die Haftung für das Restrisiko, im gegenseitigen Vertragsverhältnis geklärt/festgelegt werden.

Im Bereich „any to any" ist diese Vorgehensweise nicht zu erwarten.

Die Funktionalität der Chipkarte könnte sich technologisch so weiter entwickeln, dass alle Verschlüsselungsvorgänge in der Karte und die Eingabe des PINS oder des Fingerabdruckes auf der entsprechenden Karte selbst erfolgen können.

Die bewusste oder leichtfertige Weitergabe von sicherheitsrelevanten Informationen, wie Passwörter oder PINS, kann sicherlich nicht wirksam technisch verhindert werden.

Da die Signatur nicht auf ein definiertes Gerät (Gerätekonfiguration) beschränkt ist, ist die Frage der Verwendung eines „öffentlichen" Terminals (Signierstation) Vertrauenssache: Wer ist der Betreiber?

Von verpflichtenden Bestimmungen ist jedoch abzusehen, da sich die gleiche Problematik bei der Benutzung unterschiedlicher Terminals durch ein und denselben Benutzer ergibt: Home, Office, Bank, Freund, Uni,....

Empfehlungen über Ausstattung und Kontrolle der Zugangsmöglichkeit zu öffentlichen Terminals sind aber sicher angebracht.

Zu 5. Sichere Signaturprüfung

Es erscheint inkompatibel, wenn einerseits die Signaturprüfung mit E3 „hoch“, der „Secure Viewer“ aber mit E2 zu evaluieren ist.

Die in diesem Zusammenhang entstehenden hohen Kosten können sich als Hemmschuh für die allgemeine Verbreitung erweisen.

Die sichere Signaturüberprüfung durch andere als Signatoren ist wünschenswert und für die breite Anwendung der elektronischen Signatur notwendig, entspricht unserer Meinung nach einer in der Praxis nicht durchsetzbaren Kann-Bestimmung. Die Qualität einer Überprüfung von Signaturen muss dem Ermessen des jeweils Betroffenen überlassen bleiben.

Es wird nicht zuletzt die Aufgabe der TKC sein, auch „Nicht-Signatoren“ darüber aufzuklären, welcher Aufwand für die sichere Überprüfung einer „sicheren“ Unterschrift notwendig ist.

Als Voraussetzung eines reibungslosen Ablaufes von Signaturprüfungen jeder Art ist die online-Zugriffsmöglichkeit auf alle Verzeichnisse notwendig, um die Gültigkeit von Zertifikaten zu überprüfen. Das automatische Nachschlagen zur Überprüfung der Gültigkeit von Zertifikaten ist nicht nur eine technische, sondern vielmehr eine organisatorische Herausforderung. Dies muss ja auch zumindest innerhalb der EU, sinnvollerweise aber weltweit, möglich sein.

In diesem Zusammenhang stellen sich noch einige zusätzliche Fragen:
- Wird die Überprüfung der Gültigkeit auf Internetzugang beschränkt?
- Wird sichergestellt, dass alle Zertifikate Online überprüfbar sind?
- Muss der Überprüfer eines Zertifikates selbst ein Zertifikat besitzen?
- Wer zahlt wem was für die Überprüfung?

Zu 6. Weitere Fragen

Wir sind der Meinung, dass die Weiterverbreitung der elektronischen Signatur nur durch die Verwendung international anerkannter und einsetzbarer Standards gewährleistet werden kann.

Es ist anzunehmen, dass auch andere Institutionen, einschließlich der öffentlichen Stellen, den Nutzern die jeweiligen Programme für die Abwicklung der eigenen Transaktionen wahrscheinlich sogar online zur Verfügung stellen werden.

iTA – INFORMATION TECHNOLOGY AUSTRIA, Österreichischer Verband der Informationstechnologie Industrie, Mariahilfer Straße 37 - 39, 1060 Wien
Bearbeiter: Werner H. Rauch, Geschäftsführer, Tel.: + 43 1 588 39 DW 39, Fax: + 43 1 586 69 71, E-Mail: rauch@feei.wk.or.at

Amt der Oberösterreichischen Landesregierung

Allgemeines

Das öst. Signaturgesetz (SigG) hält sich im Wesentlichen an die Vorgaben der EU-Richtlinie. Es wird daher keine Personal Key Infrastructure (PKI) normiert, sondern lediglich eine Authentifizierungsinfrastruktur. Der Bereich der Vertraulichkeit bleibt auch im SigG ausgespart. Vom Bundesministerium für Justiz wurde in diesem Zusammenhang stets betont, dass es den Zertifizierungsdienstleistern freistünde, neben Authentifizierungszertifikaten auch andere Zertifikate - etwa zur Verschlüsselung - auszugeben. Diese Tätigkeit sei durch das SigG nicht untersagt, sondern liegt lediglich außerhalb dessen Anwendungsbereichs.

Wie die EU-Richtlinie sieht auch das SigG ein mehrstufiges System von Zertifikaten vor. Neben den „einfachen“ gibt es „qualifizierte“ Zertifikate, die von besonders vertrauenswürdigen Zertifizierungsstellen ausgegeben werden dürfen, welche besonderen Bestimmungen unterliegen. Nachrichten, die nun mit diesen Zertifikaten auf besonders sichere technische Weise signiert sind (sogenannte „sichere elektronische Signaturen“) genießen das Privileg, ausdrücklich schriftlichen Dokumenten iSd § 886 ABGB gleichgestellt zu sein.

Zertifizierungsstellen für qualifizierte Zertifikate können im Gegenzug für strengere Kontrollen ihren Kunden sichere elektronische Unterschriften mit besonderen Rechtswirkungen bieten. In Österreich sind aber im Vergleich zu anderen Ländern zivilrechtliche Formvorschriften selten, es überwiegt die Formfreiheit. Die Gleichstellung wird daher nur in Nischenbereichen einen ausreichenden Anreiz bieten, Anbieter von qualifizierten Zertifikaten zu werden.

Das Signaturgesetz regelt nun grundsätzlich folgendes:

- Zulassung und Nichtdiskriminierung elektronischer Signaturen im Geschäfts- und Rechtsverkehr

- Weitgehende Gleichstellung der Rechtswirkungen einer sicheren elektronischen Signatur mit den Rechtswirkungen einer eigenhändigen Unterschrift

- Einführung eines Aufsichtssystems über Zertifizierungseinrichtungen einschließlich der Schaffung eines Systems zur freiwilligen Akkreditierung

- Einführung von Haftungsregeln für Zertifizierungseinrichtungen und

- Regelung der Voraussetzungen einer Anerkennung ausländische Zertifikate und elektronischer Signaturen

Die vollwertige rechtliche Anerkennung sicherer elektronischer Signaturen im Geschäftsverkehr und im Verkehr mit Behörden stellt das Hauptanliegen des SigG dar. Die Kombination von organisatorischen und personellen Maßnahmen zur Qualitätssicherung sowie eine Reihe sicherheitstechnischer Maßnahmen rechtfertigt nun die Gleichstellung der sicheren elektronischen Signatur mit der eigenhändigen Unterschrift.

Das SigG schafft aber auch ein Mindestmaß an Rechtssicherheit für diejenigen Signaturen, die nicht die – in manchen Fällen unerlässlichen – hohen Sicherheitsanforderungen für sichere Signaturen erfüllen. Im elektronischen Alltag können grundsätzlich alle, also auch einfache Signaturverfahren zulässigerweise verwendet werden. Vor Gerichten oder Behörden sind auch mit solchen Signaturen versehene Erklärungen als Beweismittel

zulässig. Somit kommt den nicht sicheren elektronischen Signaturen die gleiche Rechtswirkung wie dem herkömmlichen E-Mail zu, und bieten darüber hinaus noch ein zusätzliches Qualitätskriterium hinsichtlich der Identität des Absenders und der Authentizität der Nachricht.

Das Signaturgesetz gilt grundsätzlich im öffentlichen Bereich, es sei denn im jeweiligen Verfahrensgesetz wird Besonderes geregelt. Der Justizausschuss geht hier aber davon aus, dass dies nicht notwendig ist. Dies bedeutet, dass seit 1.Jänner 2000 die eigenhändige Unterschrift durch eine elektronische Signatur ersetzt werden kann und zwar immer dann, wenn Schriftlichkeit im Sinne von Unterschriftlichkeit gefordert ist.

Bedeutend ist in diesem Zusammenhang auch die bereits vorhin angesprochene Nicht-Diskriminierungsklausel des § 3 Abs. 2 woraus hervorgeht, dass einfache sichere elektronische Signaturen nicht rechtsunwirksam sind. Daher entfalten diese die gleiche Rechtswirkung wie ein normales E-Mail und es können somit Anträge rechtswirksam auf diesem Weg eingebracht werden. Die gesetzliche Grundlage für den öffentlichen Bereich ist hier der § 13 AVG.

Für den Bereich der Eingangspost bedeutet dies, dass die Bürger Anträge grundsätzlich auch elektronisch einbringen können und die Behörde nur bei Zweifel über die Identität die eigenhändige Unterschrift fordern muss; was bei der sicheren digitalen Signatur ex lege wegfallen würde. Die einfache digitale Signatur bietet hier immerhin noch ein Plus an Sicherheit hinsichtlich Identität und Authentizität gegenüber dem herkömmlichen E-Mail. Zu erwähnen ist hier noch, dass § 13 AVG immer unter der Voraussetzung der „technischen Möglichkeit“ steht. Die Bestimmung des § 1 Abs. 2 SigG, also die grundsätzliche Anwendbarkeit des Signaturgesetzes im öffentlichen Bereich, bedeutet nun - wie sich aus den erläuternden Bemerkungen zum Gesetzesentwurf ergibt – aber nicht, dass im öffentlichen Bereich die technische Ausstattung zum Austausch signierter Erklärungen vorhanden sein muss. Somit besteht kein rechtlicher Druck auf die Verwaltungen, Vorsorge für die erforderlichen technischen Einrichtungen zu treffen.

Im Gegensatz dazu kann die Behörde nur dann selbst die elektronische Kommunikation verwenden (Ausgangspost), wenn diese Kommunikationsweise (E-Mail) vom Bürger im konkreten Verwaltungsverfahren bereits verwendet und der Verwendung durch die Behörde nicht ausdrücklich widersprochen wurde. Auf die Zustellproblematik sei hinzuweisen, weshalb die praktische Anwendung nicht allzu groß sein wird.

Insgesamt kann daher festgehalten werden, dass die sichere bzw. überhaupt die elektronische Signatur keine Voraussetzung für die herkömmliche elektronische Kommunikation zwischen Bürger und Verwaltung darstellt. Nur in jenen Bereichen, in denen die Identifikation des Bürgers eine besondere Voraussetzung ist, wird eine sichere Signatur notwendig werden. Zu denken wird hier in Hinkunft an die elektronische Akteneinsicht oder die Einbindung des Bürgers in Verwaltungsapplikationen sein.

Im Unterschied zum öffentlichen Bereich ist im Privatrecht für die Anwendbarkeit der elektronischen Kommunikation eine vorherige Vereinbarung notwendig. Der Austausch von Visitenkarten mit einer E-Mail-Adresse dürfte beispielsweise hier noch keine kompetente Zusage sein. Zum Privatrecht ist noch zu sagen, dass die Schriftlichkeit nur in bestimmten Bereichen notwendig ist, wie z. B. bei der Bürgschaft. Wo dies nicht der Fall ist, sind keine elektronischen Signaturen notwendig. Es kommt auch so, also durch ein herkömmliches E-Mail, ein Rechtsgeschäft zustande.

§ 1 Abs. 2 SigG sieht vor, dass das Signaturgesetz auch in sogenannten geschlossenen Systemen anzuwenden ist, sofern dies von den Teilnehmern vereinbart wird. Dabei handelt es sich um Systeme, in denen die angebotenen elektronischen Dienste einem

eingeschränkten Personenkreis zur Verfügung stehen. Musterbeispiel sind die von Kreditinstituten angebotenen elektronischen Netze.

Vorgangsweise im Land Oberösterreich

Auch wenn keine rechtliche Verpflichtung zur Ermöglichung der Kommunikation mittels digitaler Signatur zwischen Bürger und Verwaltung besteht, gehört es zur Bürgerfreundlichkeit und Modernität der Verwaltung sich dieser Technologie nicht zu verschließen.

Für die oö. Landesverwaltung wird daher folgende Vorgangsweise eingeschlagen:

1. Eingehende Nachrichten

Es ist davon auszugehen, dass bereits seit 1. Jänner 2000 Bürger elektronisch signierte Nachrichten übermitteln können. Zwar wird es zu diesem Zeitpunkt noch keinen akkreditierten österreichischen Zertifizierungsdiensteanbieter geben, doch ist es auf Grund der Anerkennungsregeln im Signaturgesetz möglich, dass österreichische Bürger bereits digitale Signaturen von ausländischen Anbietern verwenden. Sofern es sich hier um elektronische Signaturen von in EU-Staaten niedergelassenen Zertifizierungsdiensteanbietern handelt, sind diese ohne weiteres den österreichischen Signaturen gleichgestellt.

Seitens der oö. Landesverwaltung wird daher angestrebt, für den Empfang eingehender digital signierter Nachrichten technisch und organisatorisch gerüstet zu sein, weshalb alle offiziellen E-Mail-Postfächer (also die offizielle Landes-E-Mail-Adresse „post@ooe.gv.at“ sowie die offiziellen Dienststellen-Postfächer „dienststelle.post@ooe.gv.at“), entsprechend ausgerüstet werden sollen.

Voraussetzung dafür ist jedoch, dass die in der oö. Landesverwaltung vorhandenen und eingesetzten Produkte, also die Mail-Clients der Microsoft-Produktpalette (MS Outlook) den Anforderungen an die elektronische Signatur gerecht werden. Bei den derzeit laufenden Teststellungen hat sich jedoch vorläufig ergeben, dass die eingesetzten Produkte nicht 100% kompatibel mit der für die elektronische Signatur eingesetzten sind Technologie (Probleme mit dem 1024-kbit-Schlüssel).

2. Ausgehende Nachrichten

Da mit der digitalen Signatur weder die Problematik der Zustellung gelöst wird, noch damit eine sichere Übertragung vertraulicher Nachrichten (z. B. Bescheide) zwingend verbunden ist und andererseits das AVG im Verwaltungsverfahren die elektronische Übermittlung ohnehin nur dann zulässt, wenn die Verfahrenspartei im konkreten Verfahren bereits das Medium E-Mail benutzt hat und nicht ausdrücklich einer Übertragung widersprochen hat, scheint es derzeit noch verfrüht, die Möglichkeit einzuräumen, dass die Landesverwaltung selbst Erledigungen mit einer digitalen Signatur verschickt.

Dazu gesellt sich noch das Problem, dass das Signaturgesetz davon ausgeht, dass nur natürliche Personen eine digitale Signatur beantragen können. Zwar ist es rein rechtlich nach dem Signaturgesetz möglich, dass in eine digitale Signatur auch ein entsprechender Hinweis über Umfang der Vertretungsmacht etc. aufgenommen wird, doch scheint es aus unserer Sicht derzeit nicht notwendig, die Mitarbeiter des Landes mit einer „dienstlichen“ digitalen Signatur auszustatten.

3. Interne digitale Signatur

Rein theoretisch bestünde natürlich mit einer digitalen Signatur auch die Möglichkeit, intern Nachrichten zu signieren um sicher zu stellen, wer welche Nachrichten übermittelt bzw. von wem bestimmte Nachrichten geändert werden. Dieser Aspekt ist durchaus auch interessant für den elektronischen Workflow.

Es ist hier aber festzuhalten, dass dazu nicht eine digitale Signatur im Sinne des Signaturgesetzes notwendig ist, sondern dass man dabei auch wie bisher über in Verbindung mit Passwörtern vorgehen kann.

Seitens des Landes Oberösterreich stellt sich hier insbesondere die Frage ob die anderen Bundesländer beabsichtigen, selbst einen öffentlichen Schlüssel zur Verfügung zu stellen, sodass der Bürger somit auch grundsätzlich die Möglichkeit besitzt, an die Verwaltung verschlüsselt Nachrichten zu übermitteln. Unserer Ansicht nach sollte dies entsprechend den Bestimmungen des SigG (vgl. insbesondere die Ausschussbemerkungen zu § 2 Z. 11) rechtlich und technisch möglich sein. Allenfalls könnte hier die Ansicht des zuständigen Bundesministeriums eingeholt werden.

Amt der Oö. Landesregierung, Präsidium, Klosterstraße 7, 4010 Linz, Aktenzeichen: PräsS-680662/7-2000-Heu, Bearbeiter: Mag. Karl Heuberger, Telefon: 0732/7720-1174, Fax: 0732/7720-1621. E-mail: praes.post@ooe.gv.at

Siemens AG Österreich

Einleitung

Die Siemens AG Österreich beschäftigt sich in den unterschiedlichsten Geschäftsbereichen mit den Anforderungen des Österreichischen Signaturgesetzes. Die hier abgegebene Stellungnahme repräsentiert eine akkumulierte Teilsicht einiger betroffener Bereiche, unter anderem die technische Stellungnahme der Siemens Business Services GmbH & Co (SBS).

Darüber hinaus möchten wir auf die Position der iTA (iTA Information Technology Austria, Österreichischer Verband der Informationstechnologie Austria), bei der SBS Mitglied ist, verweisen.

Ad 1 Dokumentenformate

Das Österreichische Signaturgesetz und dessen Durchführungsverordnung schlägt keine konkreten Formate der zu signierenden Daten vor. Dateiformate von Daten, die signiert werden, müssen allerdings genau spezifiziert werden. Die Spezifikation muss so detailliert sein, dass ein Anzeigeprogramm (Viewer) gemäß dieser (nach-)implementiert werden kann. Als weitere Vorgabe gilt, dass der Signator den gesamten Inhalt der Daten visuell überprüfen (und verstehen) können muss. Das gewählte Datenformat und die dazugehörigen Anzeigeprogramme werden vom Zertifizierungsdiensteanbieter (ZDA) evaluiert und müssen von der Bestätigungsstelle genehmigt werden.

Im Rahmen von aktuellen Siemens Entwicklungen werden das TIFF (Tag Image File Format) und das XML (eXtensible Markup Language) Format zur Speicherung elektronisch signierter Daten verwendet. In beiden Fällen wird jeweils nur ein Teilbereich des Formates verwendet.

TIFF

TIFF (Tag Image File Format) ist ein steuerzeichen-basiertes Dateiformat zur Speicherung und zum Austausch von Rastergrafiken und wurde im Jahre 1986 erstmals von Aldus Corporation publiziert. 1994 wurde die Pflege des Formats von Adobe Systems Incorporated übernommen, als die Firma Aldus von Adobe übernommen wurde. Die letztgültige Version von TIFF ist die Version 6.0, die seit 1995 besteht (Spezifikation unter http://partners.adobe.com/asn/developer/PDFS/TN/TIFF6.pdf). TIFF beschreibt Bilddaten, die typischerweise von Scannern, Frame-Grabbern, Photo- und Zeichenprogrammen kommen. Es ist aber keine Seitenbeschreibungssprache (wie XML) oder Druckersprache (wie Post Script). TIFF wird zum Teil in den Geräten selbst unterstützt, da Datenkomprimierung im Format enthalten ist und diese die Kommunikation beschleunigt. Die Implementierung von TIFF ist relativ leicht umsetzbar, da die Anzahl der Steuerzeichen (Tags) und Felder beschränkt ist. Trotzdem bietet TIFF eine leichte Erweiterbarkeit für zukünftige Versionen.

Das TIFF Format ist zwar kein anerkannter Standard, wurde aber durch seine weite Verbreitung zu einem De-Facto Standard im Bereich Electronic-Publishing. Da TIFF ein anerkanntes, auf mehreren Plattformen verfügbares Grafikformat ist, in dem außerdem Datenkomprimierung als Teil des Formates definiert ist, wird dieses Format für die Speicherung von Bilddaten bevorzugt.

XML

Extensible Markup Language (XMLTM) ist ein einfaches, flexibles Textformat, das von SGML (ISO 8879) abgeleitet wurde. Es wurde dazu entwickelt, den weiten Bereich des

Electronic Publishing abzudecken. XML wird insbesondere für den Datenaustausch im Web zunehmend an Bedeutung gewinnen. Mit einer Standardisierung des Formates ist in der nächsten Zeit zu rechnen.

Die Siemens Tochter SSE verwendet daher XML als Format für signierte Dokumente in ihrem Produkt TrustedDoc. (http://www.sse.ie/trusteddoc/index.html)

Nähere Informationen zu XML unter http://www.w3.org/XML/Activity und http://inf2.pira.co.uk/top011a.htm.

Ad 2 Aufbewahrung der privaten Schlüssel

Auf den Begriff „Chipkarte“ als derzeit „praktikabelste Lösung“ zur Aufbewahrung privater Schlüssel sowie die Zertifizierung derselben soll näher eingegangen werden:

Die Chipkarte ist tatsächlich nur ein Trägermedium für das eigentliche Sicherheitsmodul, den Chip. Diese Art von Sicherheitsmodul kann sich auch in einem Handy, auf einer Steckkarte im PC oder in einem Organizer (PDA) befinden. Das Scheckkartenformat, das meistens mit dem Begriff Chipkarte assoziiert wird, ist also sekundär.

Das Modul selbst muß in 2-facher Hinsicht hohen Sicherheitsstandards genügen: auf der einen Seite die physikalische Bauart des Moduls inkl. ROM-Code und andererseits das darauf laufende Betriebssystem. Eine Komponente kann die andere kompromittieren – darum ist eine gleich starke Evaluierung der Sicherheitsmechanismen sinnvoll.

Die Chip-HW wird an Hand einer bestimmten Maske evaluiert (Bauart der Schaltung, Verlauf der Leiterbahnen, Anordnung der Speicherzellen, Löschvorgänge, Verhalten bei Manipulationen (z.B. Taktfrequenz, Temperatur, Spannung, ...), Transportschutz der Maske), beim Betriebssystem nur einzelne Teile, die für die sicherheitsrelevanten Aktionen ausschlaggebend sind: Schlüssel erzeugen, signieren, Hash-Berechnung, Zufallszahl erzeugen, PIN prüfen. Andere Funktionen wie beispielsweise das Selektieren eines Files oder das Lesen eines Feldes werden in diesem Rahmen nicht evaluiert.

Die Tochterfirma der Siemens AG Berlin-München, Infineon Technologies AG (ehemals Siemens Halbleiter (HL)) hat für diese Anforderungen das Modul SLE66CX160S nach ITSEC E4 hoch evaluieren lassen, um auch den Anforderungen des deutschen Signaturgesetzes entsprechen zu können. Aus unserer Sicht decken diese sehr aufwendigen und ins Detail gehenden Evaluierungen (die auch ein hohes Maß an Zeit (ca. 6 Monate) und Geld (mindestens 3 Mio. ATS erfordern) die Anforderungen des Signaturverordnung hinreichend ab.

Bereits bei der Entwicklung einer Chipgeneration wird angenommen, daß die Raffinesse der Attacken zunimmt und – wenn auch bereits sehr aufwendige – Angriffe bekannt werden. Dazu können bereits beim Design Maßnahmen eingeplant werden, mittels Patches im Betriebssystem gewisse Schwächen zu beheben.

Das sichere (tamper-proof) Aufbewahren eines privaten Schlüssels erfordert zum heutigen Stand der Technik zwingend eine HW-Maßnahme – wie diese konkret aussieht, darüber kann diskutiert werden (z.B. Cryptoboxen, Chipkarten, SIM-Karten, ...).

Die Kosten eines Sicherheitsmoduls sind stark stückzahlabhängig; das Preis-Leistungs-verhältnis ist durchaus gut, wenn dieses auch nicht direkt honoriert wird, da der unmittelbare Nutzen nicht angreifbar, meßbar oder anderweitig erfahrbar ist.

Ad 3 Kontrolle des Signiervorganges

Anmerkungen zum Text:

Zunächst ist die Bildung des Hashwertes nur in Software nicht zwingend nötig; es sind auch Verfahren implementierbar, die zumindest eine (z.B. die letzte) oder auch mehrere Runden der Hashwertberechnung mit Hilfe der Chipkarte durchführen. Dies ist lediglich eine Performancefrage. Der Vorteil besteht darin, daß der eigentliche Hashwert, der schließlich mit dem privaten Schlüssel verschlüsselt wird, niemals im Klartext im System vorliegt sondern im Sicherheitsmodul verbleibt.

„Noch sicherer sind biometrische Karten“: diese Aussage muß sehr kritisch beleuchtet werden! Eines der wichtigsten Vorgänge ist die Authentisierung des Benutzers gegenüber der Karte; im klassischen Fall über eine 4-8 stellige PIN. Das wichtigste Element dabei ist die Überprüfung der eingegebenen PIN mit den gespeicherten Referenzdaten im Sicherheitsmodul selbst (und das Behandeln von Falscheingaben, Fehlbedienzähler!). Das bedeutet, daß keine außenstehende (Prüf-)Instanz involviert ist, sondern das Betriebssystem des Sicherheitsmoduls selbst entscheidet, ob eine bestimmte „Access Condition“ erfüllt ist oder nicht.

Das Überprüfen von biometrischer Information (Minutien) mit Referenzdaten ist ein vergleichsweise sehr aufwendiger Vorgang und bedarf einer sogenannten Matcher-SW. Es gibt Bestrebungen, diese Software möglichst kompakt zu gestalten (Micro-Matcher), so daß sie auf einem 8-bit Chip Betriebsystem ablauffähig ist, um die Überprüfung der präsentierten Daten mit den gespeicherten Referenzdaten vom Chip selbst vornehmen zu lassen. Derzeit gibt es keine bekannten Chipkarten und Chipkarten Betriebsysteme, die sowohl das Matchen von biometrischen Daten als auch asymmetrische kryptographische Verfahren bieten. Erst wenn diese Kriterien beide erfüllt sind, kann man von einem PIN-Ersatz durch Fingerprint sprechen – alle anderen Softwareimplementierungen außerhalb des Chip stellen eine Bedrohung des Sicherheitsniveaus dar.

Qualitativ gibt es noch das Argument, daß eine PIN-Prüfung immer ein exaktes Ergebnis gibt: richtig oder falsch. Beim Matchen von Minutien ist das Kriterium das Unter- oder Überschreiten eines Schwellwertes, der jedoch nicht exakt vorgebbar ist sondern zwischen 2 Extremen gesetzt wird (False Acceptance Rate, False Rejection Rate). Damit ist das Ergebnis nicht binär exakt (1 oder 0, exakt richtig oder falsch) sondern bietet immer nur eine gewisse Wahrscheinlichkeit der Richtigkeit.

Heute ist nur eine zwingende Kombination („AND“, nicht „OR“) als zusätzliche Hürde denkbar, um das Problem des PIN-Weitersagens einzudämmen, das hauptsächlich ein Philosophie oder Awareness Problem ist.

Lösungen, bei denen das Überprüfen (Matchen) der biometrischen Information in Software oder aus dem Sicherheitsmodul ausgelagerter Firmware (z.B. ASIC, ROM Bausteine) passiert und dem Sicherheitsmodul nur das Ergebnis dieser Überprüfung mitgeteilt wird, sind als unsicher zu betrachten; ein Stück Software/Firmware, das immer ein Übereinstimmen der Daten an das Sicherheitsmodul weitergibt, ist relativ einfach herzustellen und korrumpiert den gesamten Authentisierungsmechanismus. Die Überprüfung (Matching) muß in der Hoheit des Chipkartenbetriebssystems liegen.

Der Problemkreis „Softwarekonfiguration am Client-PC im Feld“ ist eines der ungeklärtesten Bereiche der Durchführungsverordnung. Sowohl was das Betriebssystem als auch die Anwendersoftware und die allgemeine Konfiguration zusammen mit den notwendigen Evaluierungen betrifft ist ein starker Widerspruch zwischen Sicherheit, Anwendbarkeit und Praktikabilität aber auch Kontrollierbarkeit gegeben.

2 Punkte seien besonders angesprochen:

- Eine Möglichkeit besteht darin, die Signatursoftware selbst signieren zu lassen; vor dem Zugriff erfolgt eine Prüfung der Signatur, um das Einschleusen von „Trojanern“ zu erkennen.

- Alle Konfigurationsvorschriften inklusive zwingender Verwendung eines Virenschutzprogrammes sind berechtigt und richtig, wie kann jedoch der Empfänger einer signierten Nachricht die Zustände zum Zeitpunkt des Signierens am System des Signators überprüfen und die Echtheit der Signatur verifizieren? Diese Vorschläge und Empfehlungen sind also letztlich als (Selbst) Schutz des Senders/Signators zu sehen, helfen dem Empfänger aber nicht, ein höheres Maß an Sicherheit über die Signatur zu erlangen.

- Wie ist die Frage der Beweislast und der Beweiswürdigung zum Zeitpunkt der Erstellung der Signatur rechtlich zu sehen?

Es scheint daher wünschenswert, eine Standardkonfiguration für einen signaturgesetzkonformen Personal Computer von Seite der Telekom Control oder der A-SIT zu definieren, an Hand derer Trust Center Anbieter ein Bündel aus HW und SW zusammenstellen können, das den gesetzlichen Auflagen genügt und für dessen Komponenten eine (kostenpflichtige?) Wartung (d. h. Evaluierung von neuen Versionen) angeboten wird.

Ad 4 Verwendung von Schlüsseln für andere Zwecke

Der beschriebene Angriff über den SSL Handshake ist durchaus ernst zu nehmen – daraus wird klar ersichtlich, daß die Mitverwendung des Signaturschlüssels für weitere Anwendungen aus Gründen der Praktikabilität und „ease – of – use“ Sicherheitslücken öffnet. Insbesondere wird oft (sinnvollerweise) im Zusammenhang mit e-commerce oder e-business Szenarien von der Verwendung einer Chipkarte gesprochen, um die Verwendung von „wirklich privaten“ Schlüsseln zu forcieren und beispielsweise im Zusammenspiel mit sog. „smart card based cryptographic service provider“ auch starke Kryptographie im Internet anwenden zu können.

Die Verwendung von applikationsspezifischen Schlüsseln ist hingegen eine 2-fache Herausforderung: einerseits sind die meisten Chipkartenbetriebssysteme bis jetzt mit globalen PINs versehen gewesen (und damit ergab ein Reset Security State auch einen globalen Reset); die Logik in den Anwendungen war damit relativ einfach. Nun muß bei jedem Umselektieren der Anwendung eine Überprüfung der PIN erfolgen – sehr unkomfortabel.

Andererseits mußte sich der Anwender nur eine PIN merken, die scheinbar (siehe Marketing von biometrischen Systemen) schon schwierig genug zu beherrschen war (insbesondere wenn man 5 verschiedene Karten für unterschiedliche Anwendungen hat). Wenn nun noch auf einer Karte 3 unterschiedliche PINs (zumindest 1 PIN Applikation gesetzeskonforme digitale Signatur, 1 PIN global für weitere Applikationsschlüssel, 1 globale Unblock-PIN) gemerkt und verwaltet werden müssen, stellt sich eine gewiß große Herausforderung an die Gedächtnisleistung (wie soll das übrigens mit biometrischen Systemen harmonisiert werden? Hier ist der Fingerabdruck auch global...).

Die Anzahl der Schlüsselpaare scheint zumindest 3 zu betragen:

Erstes Paar: Digitale Signatur nach dem SigG, gleichgestellt der eigenhändigen Unterschrift.

Zweites Paar: Verschlüsselung (wobei der private Schlüssel für Backup-Zwecke exportierbar sein muß)

Drittes Paar: Authentisierung im allgemeinen (z.B. für Kerberos Anmeldung an Windows 2000, SSL-Authentisierung, e-commerce Anwendungen)

Ad 5 Sichere Signaturprüfung

Das OCSP Protokoll, das sich noch in einem sehr frühen Stadium befindet, sollte diesbezüglich eine einfache, automatisierte Möglichkeit schaffen, fremde Zertifikate und Signaturen einfach, unkompliziert und sicher prüfen zu können. Derzeit gibt es nach unserem Wissenstand kein Produkt, das diesen neuen Standard bereits implementiert hat.

Bemerkenswert ist die höhere Anforderung (ITSEC E3 hoch) an die sichere Signaturprüfsoftware – eine aus unserer Sicht punktuell unrealistisch hohe Hürde.

Ad 6 Weitere Fragen

Die Anforderungen, die zumeist von Kunden an den Hersteller von Kryptographie-Produkten herangetragen werden, widersprechen oft den sicherheitstechnischen Anforderungen. Im Vordergrund stehen dabei meistens die minimale Anzahl von notwendigen PIN Eingaben, das transparente Agieren im Hintergrund (der Anwender soll in seinem Arbeitsprozeß so gut wie nichts merken), das Offenhalten von fall-back Konzepten („wenn der Administrator schnell etwas nachsehen muß, soll er sofort und jederzeit trotzdem in das System kommen, eine Datei lesen können, etc.“) und die völlige Wiederherstellbarkeit im Fall von Ausfällen, Crash aber auch nach dem Ausscheiden von Mitarbeitern.

Ansprechpartner: Dr. Peter Klein, Siemens Business Services, Dietrichgasse 27-29, 1030 Wien, peter.h.klein@siemens.at