



 **Preprint 01-09**

**Trierer Symposium
Digitale Signaturen
Abstracts**

Herausgeber:
Lutz Gollan
Christoph Meinel

ISSN 1433-8106

Editors Lutz Gollan
Dr. iur.
Christoph Meinel
Univ.-Prof. Dr. sc.

Copyright Institut für Telematik,
Trier

Trademarks All terms that are mentioned in this paper that are known to be trademarks or service marks have been appropriately capitalised. Use of a term in this paper should not be regarded as affecting the validity of any trademark and service mark. The product or brand names are trademarks of their respective owners.

Printing 2001

7. Trierer Symposium

Digitale Signaturen

15. - 16. November 2001

Themenschwerpunkte

Infrastrukturen

E-Commerce

Öffentliche Verwaltung

Zukunftserwartungen

Inhaltsverzeichnis

1. Veranstalter.....	5
2. Programm	6
3. Digitale Signaturen - Einführung in die Thematik (Thomas Engel)	8
4. SigG-Anwendungskomponenten - Lessons learned - (Torsten Henn)	9
5. Digitale Signaturen im Zahlungsverkehr (Stefan Engel-Flechsigt)	10
6. Förderung des Einsatzes von PKI-Komponenten und –Lösungen im Rahmen der Initiative D21 AG 6 "Sicherheit und Vertrauen im Internet" (Bernd Kowalski)	12
7. Nutzen und Risiken des Internet für den Handel an der Frankfurter Wertpapierbörse (Klaus-Dieter Benner)	13
8. Berufskammern als Zertifizierungsdiensteanbieter nach dem SigG (Michael Leistenschneider)	14
9. Digitale Signatur - Wirkungsweise und Anwendungen (Detlef Dienst).....	16
10. www.bremer-online-service.de Der Vorreiter und Preisträger in der Pflicht (Stephan Klein)	17
11. Elektronische Heilberufeausweise: Stand der Einführungsvorbereitungen und noch zu lösende Probleme (Reinhold Mainz)	18
12. eGovernment und Elektronische Signatur in der Landesverwaltung Rheinland-Pfalz (Gregor Schulte).....	19
13. Elektronische Signatur für sicheres eBusiness - Praktische Einsatzmöglichkeiten am Beispiel der IHK-Anwendungen (Klaus Berens).....	20
14. Das Konzept der digitalen Signatur in Theorie und Praxis (Ulrich Sandl)	21
15. Konzernweites Zertifikatsmanagement (Armin Ratz / Frank Losemann)	22

1. Veranstalter

Das Institut für Telematik e.V. ist eine gemeinnützige Forschungs- und Entwicklungseinrichtung unter der Verwaltung der Fraunhofer-Gesellschaft mit Sitz in Trier. Es wurde am 1. Januar 1998 gegründet und hat sich zu einem Kompetenzzentrum für Problemlösungen im Schnittbereich von Telekommunikation und Informatik entwickelt. Es beschäftigt ca. 50 wissenschaftliche Mitarbeiterinnen und Mitarbeiter verschiedener Fachrichtungen und Nationalitäten und ist im Ausbau begriffen.

Das Spektrum der Institutstätigkeit reicht von der anwendungsorientierten Forschung in den Bereichen Informatik und Telekommunikation bis hin zur Entwicklung maßgeschneiderter Problemlösungen und Pilotsysteme für Handel, Industrie, Medizin und Verwaltung. Darüber hinaus hat sich das Institut die Aus- und Weiterbildung im Bereich der neuen Medien sowohl von Kooperationspartnern, als auch von interessierten Mitarbeitern regionaler und überregionaler Unternehmen zur Aufgabe gemacht.

Projektpartner des Instituts sind neben High-Tech-Unternehmen und Großbetrieben vor allem auch klein- und mittelständische Firmen, in denen die wissenschaftlichen Ergebnisse in die betriebliche Praxis umgesetzt werden. Die Tätigkeitsschwerpunkte liegen insbesondere in der Entwicklung und Nutzung neuer Informations- und Kommunikationsmedien in Technik, Medizin und Gesellschaft.

Die laufenden Forschungs- und Entwicklungsprojekte sind auf die praktische Nutzbarmachung neuester wissenschaftlicher Entwicklungen in den Bereichen elektronisches Publizieren, Internet/Intranet, Telemedizin, sichere Datenübertragung, Systementwurf und –analyse gerichtet.

Das Institut für Telematik ist dabei insbesondere in folgenden Technologiebereichen tätig:

- Sicherheit in offenen Netzen (PKI, digitale Signaturen, Hardware etc.)
- Netztechnologien und Computersysteme
- Redaktionssysteme - Bereitstellung von Informationen im Internet/Intranet
- Navigationssysteme - Aufbereitung von Informationen im Internet/Intranet
- Multimedia - Darstellung und Transport multimedialer Daten
- Grundlagenforschung Informatik, Mathematik und Telekommunikation

Die überwiegend projektbezogene Finanzierung der Forschungs- und Entwicklungsvorhaben sichert dabei eine Erfolgskontrolle durch die Anwender.

Prof. Dr. sc. Christoph Meinel, der Leiter des Instituts und Inhaber des Lehrstuhls für Informatik an der Universität Trier, ist Direktor des Zentrums für Wissenschaftliches Elektronisches Publizieren (WEP) an der Universität Trier und Mitglied verschiedener Aufsichtsräte und Programmkomitees. Er gehört z.B. dem Aufsichtsrat des Internationalen Begegnungs- und Forschungszentrums für Informatik Schloß Dagstuhl an und ist Sprecher der Fachgruppe "Komplexität" der deutschen Gesellschaft für Informatik (GI). Er ist als Veranstalter verschiedener wissenschaftlicher Symposien und als Mitglied verschiedener Programmkomitees internationaler Tagungen in Erscheinung getreten.

Tagungsleitung

Prof. Dr. sc. nat. Christoph Meinel

Institut für Telematik e.V.

Bahnhofstr. 30-32

D-54292 Trier

Kontakt

Dr. iur. Lutz Gollan
Institut für Telematik e.V.
Tel: 0651 97551-20
Fax: 0651 97551-12
E-mail: gollan@ti.fhg.de

2. Programm

Trierer Symposium Digitale Signaturen

15. und 16. November 2001
im Institut für Telematik e.V., Trier

Donnerstag, 15. November 2001		
14:00 – 14:15	Univ.-Prof. Dr. Christoph Meinel, Institut für Telematik e.V., Trier	Begrüßung und Vorstellung des Instituts für Telematik
Technik und Infrastrukturen		
14:15 – 14:45	Dr. Thomas Engel, Institut für Telematik e.V., Trier	Digitale Signaturen - Einführung in die Thematik
14:45 – 15:15	Torsten Henn, Secunet AG, Siegen	SigG-Anwendungskomponenten - Lessons learned -
15:15 – 15:45	RA Stefan Engel-Flehsig, Verisign Inc.	Digitale Signaturen im Zahlungsverkehr
15:45 – 16:15	Pause	
E-Commerce und digitale Signaturen		
16:15 – 16:45	Dr. Armin Ratz / Frank Losemann, Dresdner Bank AG, Frankfurt / Institut für Telematik e.V., Trier	Konzernweites Zertifikatsmanagement
16:45 – 17:15	Klaus-Dieter Benner, Börsenaufsichtsbehörde Hessen, Frankfurt	Nutzen und Risiken des Internet für den Handel an der Frankfurter Wertpapierbörse
17:15 – 17:30	Pause	
17:30 – 18:00	Michael Leistenschneider, DATEV eG	Berufskammern als Zertifizierungsdiensteanbieter nach dem SigG
18:00 – 18:30	Detlef Dienst, T-Telesec, Netphen	Digitale Signatur - Wirkungsweise und Anwendungen

18:30	Dr. iur. Lutz Gollan / Thomas Wagner Institut für Telematik, Trier	Eröffnung des TI-Zeitstempeldienstes http://zeitstempeldienst.ti.fhg.de
ab 19:30	Konferenzdinner im Dorint Hotel Trier	

Freitag, 16. November 2001		
Digitale Signaturen und öffentliche Verwaltung		
09:00 – 09:30	Dr. Stephan Klein, Bremen Online Services	www.bremer-online-service.de - Der Vorreiter und Preisträger in der Pflicht
09:30 – 10:00	Reinhold A. Mainz, Kassenärztliche Bundesvereinigung, Köln	Elektronische Heilberufeausweise: Stand der Einführungsvorbereitungen und noch zu lösende Probleme.
10:00 – 10:30	Gregor Schulte, Ministerium des Innern und für Sport, Mainz	eGovernment und Elektronische Signatur in der Landesverwaltung Rheinland-Pfalz
10:30 - 11:00	Pause	
Erwartungen und neue Entwicklungen		
11:00 – 11:30	Klaus Berens, Deutscher Industrie- und Handelskammertag, Bonn	Elektronische Signatur für sicheres eBusiness - Praktische Einsatzmöglichkeiten am Beispiel der IHK-Anwendungen
11:30 – 12:00	Dr. Ulrich Sandl, Bundesministerium für Wirtschaft und Technologie, Berlin	Das Konzept der digitalen Signatur in Theorie und Praxis
12:00 – 12:30	Abschlussdiskussion	

3. Digitale Signaturen - Einführung in die Thematik

Dr. rer. nat. Thomas Engel
Institut für Telematik e.V., Bahnhofstr. 30-32, D-54292 Trier
Tel.: ++49(0) 651 – 97551 – 30
mailto:engel@ti.fhg.de
http://www.ti.fhg.de

Abstract

Der rasante Ausbau moderner elektronischer Kommunikationswege bringt neue Formen des Datenaustauschs mit sich. Im Zeitalter der „Globalisierung“ kommen verstärkt Netzwerkinfrastrukturen zum Einsatz, die auf Internet-Technologie basieren oder sogar teilweise das Internet selbst nutzen. Dadurch entstehen neue bisher ungelöste Sicherheitsfragen. Gefährdungs- und Missbrauch-Szenarien ausgespähter Informationen und Netzangriffe treten immer mehr in den Mittelpunkt der Diskussion um E/M-Business und E/M-Government.

Digitale Signaturen, beispielsweise als Bestandteil von Public-Key-Infrastrukturen, können vor unterschiedlichen Gefahren, die durch die Nutzung offener Netze entstehen, schützen. So sind die wünschenswerten Ziele u.a. die Integrität der Informationen, die Vertraulichkeit der Informationen, die Verbindlichkeit des Informationsaustauschs und in einigen Fällen auch die Identität des Senders.

Die verwendeten Technologien zum Erzeugen und Überprüfen digitaler Signaturen beruhen in der Regel auf Zwei-Schlüssel-Verschlüsselungsverfahren (sog. asymmetrische Kryptographie). Hierbei werden einmalige Schlüsselpaare und elektronische Zertifikate eingesetzt, die die Zugehörigkeit des jeweiligen Schlüsselpaares zu einer bestimmten Person bescheinigen.

Die Zertifikatsverwaltung erfolgt vorzugsweise in hierarchischen Systemen durch sogenannte Trust Center. Diese stellen auch die Zertifikate aus und überprüfen vor der Vergabe die Identität des Antragstellers.

Das Ziel der Verbindlichkeit des Informationsaustauschs wird dabei durch gesetzliche Regelungen wie das Signaturgesetz 2001, die Signaturverordnung 2001 und das Gesetz zur Anpassung von Formvorschriften des Privatrechts 2001 unterstützt.

Wie weit und wie schnell sich die Digitale Signatur in der Praxis durchsetzen wird, hängt von konkreten Einsatzmöglichkeiten im Alltag ab. Zur Zeit entwickelt sich eine hochdynamische Anwendungslandschaft. In den weiteren Vorträgen des Symposiums werden aus verschiedenen Sichten Technologien, Anwendungen und Erfordernisse für den erfolgreichen Einsatz der Digitalen Signatur beleuchtet.

4. SigG-Anwendungskomponenten - Lessons learned -

Dipl.-Ing. Torsten Henn
secunet Security Networks AG, Weidenauer Straße 223-225, 57076 Siegen
Tel.: ++49-271-48950-19
E-Mail: Torsten.Henn@secunet.com
<http://www.secunet.com>

Abstract

Seit August 1997 gibt es in der Bundesrepublik Deutschland ein Signaturgesetz (SigG) mit dem Ziel, einen einheitlichen Rahmen für den sicheren Einsatz digitaler Signaturen im offenen Rechts- und Geschäftsverkehr zu schaffen und damit nicht zuletzt der zunehmend elektronischen Abbildung von Geschäftsprozessen in der Welt des eCommerce und des eGovernment Rechnung zu tragen. Als weltweit erstes nationales Gesetz verlieh das SigG Deutschland eine Vorreiterrolle auf diesem Gebiet. Dieses Signaturgesetz wurde zuletzt novelliert und findet seit Mai 2001 mit der Umsetzung der EU-Richtlinie ihre derzeit abschließende Fassung. Die Entwicklung von signaturgesetzkonformen Anwendungen ist während des gleichen Zeitraumes eher mühsam vorangeschritten. Nahezu alle der derzeit auf dem Markt befindlichen Produkte wurden von den Zertifizierungsdienste-Anbietern selbst entwickelt und spiegeln folglich eine, wenngleich legitime, zertifizierungsstellenspezifische Sicht der Anwendungen wider („Geschlossene Benutzergruppe“). Zudem stellen sie primär ein „Vehikel“ dar, mit dem interessierte Endanwender die Dienste der Zertifizierungsstelle überhaupt nutzen und erste Erfahrungen sammeln zu können. Es liegt auf der Hand, dass der erwünschte Schub für die qualifizierte elektronische Signatur mit Anbieter-Akkreditierung derzeit hinter den Erwartungen zurückbleibt, wenngleich vielversprechende Initiativen (z.B. seitens der Bundesregierung) gestartet und auch entscheidende Rahmenbedingungen (Änderung der Formvorschriften) geschaffen wurden.

Betrachtet man den Fokus derzeitiger unterstützter SigG-Anwendungen, so zeigt sich schnell, dass vorrangig die „klassischen“ Anwendungsfelder „E-Mail“ und „Datei-Signierung“ im Vordergrund stehen. Für einen Endanwender ist es schwierig, hierin einen konkreten Mehrwert zu erkennen, für den es sich lohnt einen gewissen Geldbetrag zu investieren, sieht er doch für wesentlich geringere Kosten für ihn vermeintlich vergleichbare Lösungen auf dem Markt. Eine Investition impliziert immer den Rückfluss eines Gegenwertes – welcher Art auch immer – für die geleistete Einlage(n). Es benötigt daher Anwendungen, die durch Einsatz qualifizierter elektronischer Signaturen einen klaren Mehrwert erkennen lassen und hierzu vor allem Lösungen, die solche Anwendungen mit geringst möglichem Aufwand bedienen. Dies bedingt die Integration der „SigG-Technologie“ in (kostenreduzierende) Geschäftsprozesse.

Der Vortrag berichtet über die Erfahrungen, die in der Vergangenheit im Rahmen der Betreuung von Signaturanwendungskomponenten und deren Anwendungsumfeld gesammelt wurden. Er versucht die verschiedenen Gründe für die mangelnde Applikationsunterstützung (z.B. Kosten-Nutzen-Sicht, Erfahrungen in Prüf- und Bestätigungsprozessen nach SigG) zu analysieren und zeigt die notwendigen Anforderungen an mehrwertige Signaturanwendungskomponenten im Sinne des SigG auf. Hierbei wird als Ausblick ein Lösungsansatz skizziert, der mehrwertige Geschäftsprozesse durch Multiapplikationsfähigkeit unterstützt und mit einem Finanzierungs-/Lizenzierungsmodell hinterlegt wird, dass spätere „bezahlbare“ Anwendungskomponenten zulässt.

5. Digitale Signaturen im Zahlungsverkehr

RA Stefan Engel-Flechsig
VERISIGN INC. Buschkauler Weg 27 D-53347 Alfter
Telefon: ++ 172 944 70 93
E-Mail: sflechsig@verisign.com
<http://www.verisign.com>

Abstract

Der elektronische Handel im Internet verspricht Milliardenumsätze. Nach einer Studie von Forrest & Sullivan z.B. wurde das Volumen des Internet-Marktes in Europa für das Jahr 2004 mit 51,7 Mrd. US-Dollar prognostiziert. Dem deutschen Markt wird dabei in dieser wie auch in anderen Studien der größte Marktanteil prognostiziert. Sowohl aus Unternehmens- wie auch aus Endkundensicht verbindet sich mit dem wachsenden Anteil der Abwicklung von online Transaktionen die Frage nach der Richtigkeit und Vollständigkeit der übermittelten Daten, der eindeutigen Identifizierung von Absendern und Empfängern sowie der beweisbaren Übermittlung von Informationen – also kurz nach der "Sicherheit" von online-Transaktionen.

Antworten auf diese Frage können aus rechtlicher, technischer und geschäftlicher Perspektive gegeben werden.

Der Gesetzgeber hat mit dem deutschen Signaturgesetz von 1997 eine juristische Grundlage für die Anerkennung von digitalen Signaturen geschaffen. Mit der Anpassung an die EU-weiten Rahmenbedingungen für elektronische Signaturen im Signaturgesetz von 2001, dem Gesetz über die Anerkennung von elektronischen Unterschriften im Rechtsverkehr sowie mit der jüngst verabschiedeten Signaturverordnung verfügen wir heute über einen gesetzlichen Rahmen für verschiedene Formen der elektronischen Unterschriften und über ein Ranking der verschiedenen Signaturen hinsichtlich ihrer rechtlichen und gesetzlichen Anerkennung. Wir verfügen damit über ein rechtliches Instrumentarium, das in den unterschiedlichen Geschäftszusammenhängen – Vertragsschluss, Allgemeine Geschäftsbedingungen, Haftung und Beweisbarkeit – eine grundsätzlich flexible Handhabe für die Gewährleistung von Sicherheit bietet.

Folgt man der technischen Diskussion, so wird ein Aufbau der Public-Key-Infrastruktur (PKI) als angemessene Antwort auf die Gewährleistung der Sicherheit von online Transaktionen identifiziert, weil PKI die aufgeworfenen Fragen der Beweisbarkeit, der eindeutigen Identifikation, der Authentifizierung und der Vertraulichkeit mit ihren Funktionen der digitalen Signaturen und der Verschlüsselung am besten gewährleisten kann. Dies gilt für die deutschen Banken im Bereich des Endkundengeschäfts (z.B. HBCI) ebenso wie im internationalen Geschäftsverkehr (z.B. Identrus); dies gilt für weltweite Kreditkartenunternehmen wie VISA und Mastercard (z.B. EMV) ebenso wie für von internationalen Konsortien wie Radicchio oder WAP Forum identifizierten Lösungen im Bereich des mobile payments. Die technische Umsetzung dieser Lösungen gewinnt nur langsam Gestalt. Die Gründe sind vielfältig – Umbau bereits vorhandener backend Systeme, Integration in vorhandene Applikationsstrukturen und Interoperabilität, Aufbau eigener Infrastrukturen oder Nutzung einer managed PKI, Interoperabilität der Lösung im internationalen Verbund.

Aus geschäftlicher Sicht wurde lange diskutiert, ob "Sicherheit" als solche eine tragfähige Grundlage für ein erfolgreiches Geschäftsmodell darstellt. Die Investitionskosten für den Aufbau einer PKI erwiesen sich aufgrund der erforderlichen Investitionen in Sicherheitstechnologie und die Entwicklung eigener Plattformen als so hoch, dass sich ein return of investment erst nach einigen Jahren einstellen kann. Die zusätzlichen Kosten für den Endkunden machen die Refinanzierung dieses Investitionsaufwandes über den Endkunden im

Regelfälle nicht attraktiv. Es scheint sich mehr und mehr die Auffassung durchzusetzen, PKI als "enabling technology" zu verstehen und – insbesondere bei den Zertifizierungsdienstleistern – die Geschäftsmodelle mit zusätzlichen Dienstleistungen wie hosting, zusätzlichen Dienstleistungen wie SSL-Zertifikate, wireless Zertifikaten und payment Lösungen zu ergänzen. Diese Sichtweise wird unterstützt durch weltweite Standardisierungsinitiativen, die - bezogen auf das jeweilige Industriesegment – Zertifikate (und damit PKI) als notwendigen Bestandteil einer Dienstleistung festlegen – wie dies zum Beispiel im Bereich der Kabelmodems von CableLabs und tComLabs ab dem 1.1.2002 vorgesehen ist, wie dies von mehr als 30 Banken weltweit im Rahmen von Identrus vereinbart wurde oder wie dies im WAP Standard 1.2.1 für mobile payments vorgesehen ist.

Die Prognose lautet also: 2001 ist das Jahr der Gesetzgebung, 2002 wird das Jahr der Implementierung und 2003 wird das Jahr des erfolgreichen Geschäftsmodells.

6. Förderung des Einsatzes von PKI-Komponenten und –Lösungen im Rahmen der Initiative D21 AG 6 "Sicherheit und Vertrauen im Internet"

Dipl.-Ing. Bernd Kowalski
Leiter T-Systems Telesec, Untere Industriestrasse 20, D- 57250 Netphen
Telefon: ++49 (0) 0271 - 708-0
E-Mail: Bernd.Kowalski@telekom.de
<http://www.telesec.de>

Abstract

Die Initiative D21 hat sich u.a. zum Ziel gesetzt, Umsetzungshindernisse zur Einführung von Public Key Infrastrukturen für den praktischen Einsatz in Wirtschaft und Verwaltung zu beseitigen. Hierzu wurden innerhalb der AG 6 "Sicherheit und Vertrauen im Internet" zwei Projektgruppen gebildet, die in einer kooperativen Zusammenarbeit von Vertretern der Wirtschaft und Verwaltung entsprechende Lösungsvorschläge erarbeiten. Die Ergebnisse werden für Frühjahr 2002 erwartet.

In der ersten Projektgruppe "standardkonforme PKI-Lösungen" werden Konzepte diskutiert, die ein Zusammenwirken von PKI-Infrastrukturen zwischen Verwaltungen, aber auch zwischen Verwaltung und Wirtschaft sowie zwischen Verwaltung/Wirtschaft und Bürger ermöglichen. Hierbei steht die Realisierung von CA/RA-Komponenten und Client-Lösungen in Modulbauweise und die Unterstützung unterschiedlicher Sicherheitslevel im Vordergrund.

Die Projektgruppe Smartcards erarbeitet Lösungsvorschläge, um die Chipkarte als Medium für die Digitale Signatur auch beim Privatanutzer populär zu machen. Die Eigenschaft der "Multi-PKI-Fähigkeit" künftiger Smartcards ist dabei von besonderer Bedeutung, damit der Nutzer kostengünstig mit der gleichen Karte Zertifikate unterschiedlicher Trust Center unterstützen kann. Verschiedene Referenzprojekte sollen Wirtschaft und Verwaltung zum Einsatz der Smartcard motivieren und ihnen den multifunktionalen Nutzen dieses Mediums verdeutlichen.

7. Nutzen und Risiken des Internet für den Handel an der Frankfurter Wertpapierbörse

MinR Klaus-Dieter Benner
Hessisches Ministerium für Wirtschaft - Börsenaufsichtsbehörde
Börsenplatz 4, 60313 Frankfurt
Telefon: ++49 (0) 69 – 9130620
E-Mail: klaus-dieter.benner@deutsche-boerse.com
<http://www.boersenaufsicht.de/hessen.htm>

Abstract

- Nutzung des Internets am Beispiel der Frankfurter Wertpapierbörse
- Risiken fürs Internet an Beispielen der Kursmanipulation in den USA und der BRD
- Sicherheit als neues Produkt
- Finanzierung über den Kapitalmarkt
- Vertrauen in den künftigen Erfolg des E-Commerce

8. Berufskammern als Zertifizierungsdiensteanbieter nach dem SigG

Dipl.-Kaufm. Michael Leistenschneider
Datev eG, Auf der Schlicht 13, 66839 Schmelz
Tel.: ++49 (0) 6887 - 6176
E-Mail: info@leistenschneider.de
<http://www.leistenschneider.de>
<http://www.datev.de>

Abstract

Das novellierte Gesetz zur digitalen Signatur (SigG) ist am 22. Mai 2001 in Kraft getreten. Nachdem das „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsverkehr“ verabschiedet ist, können mit einer zertifizierten Signaturkarte Erklärungen genauso unterzeichnet werden, wie mit der eigenhändigen Unterschrift.

Das DATEV-Trustcenter

Die DATEV ist seit März 2001 von der Regulierungsbehörde für Telekommunikation und Post (RegTP) als Zertifizierungsstelle im Sinne des Signaturgesetzes zugelassen. Herz der Zertifizierungsstelle ist das DATEV-Trustcenter, ein eigener Hochsicherheitstrakt, in dem, von der Außenwelt abgeschirmt, zertifizierte Signaturkarten produziert werden. Neben der DATEV haben sich noch weitere Steuerberater- und Rechtsanwaltskammern zertifizieren lassen. Weitere Berufskammern wie z.B. die Wirtschaftsprüferkammer folgen. Die Berufskammern bedienen sich als Zertifizierungsdiensteanbieter den Dienstleistungen der DATEV sowie deren Trust Center.

DATEV e:secure

Mit dem Produktbündel können Dokumente rechtsverbindlich elektronisch signieren und Gewissheit über den Absender einer E-Mail erreicht werden. Und DATEV e:secure kann noch mehr: Durch die Verschlüsselung des E-Mail-Verkehrs haben Hacker und Datenspione keine Chance. Dabei ist DATEV e:secure nicht nur bei Steuerberatern im Einsatz sondern wird bereits bei Gerichten wie dem Bundesgerichtshof sowie verschiedenen Finanzgerichten erprobt. Neben dem Produktpaket DATEV e:secure gibt es das weitere Paket Kammer e:secure, das ausschließlich von den Berufskammern der Steuerberater, Rechtsanwälte und Wirtschaftsprüfer direkt an deren Mitglieder vertrieben wird. Die darin enthaltene Signaturkarte entspricht technisch dem der Karte aus dem DATEV e:secure-Paket. Allerdings enthält die Kammer-Signaturkarte, ein von der ausgebenden Berufskammer bestätigtes Berufsattribut z.B. Steuerberater.

DATEV e:secure besteht aus folgenden Komponenten:

eine zertifizierte Signaturkarte von DATEV und ein Kartenleser
die Signatursoftware GERVA (Bestandteil des SmartCard-Sicherheitspakets)
sämtliche Trustcenter Dienstleistungen wie 24-Stunden-Sperrdienst und Verzeichnisdienst.

GERVA

GERVA ist eine Anwendung, die es in Verbindung mit Chipkartensystemen ermöglicht, elektronische Dokumente mit einer Signatur im Sinne des Signaturgesetzes zu versehen. Der Prozess zum Erstellen einer Signatur nach Signaturgesetz wird auch als "*qualifiziertes elektronisches Signieren*" bezeichnet. GERVA ermöglicht es, erstellte qualifizierte elektronische Signaturen zu verifizieren.

GERVA-Viewer

Der GERVA-Viewer ist eine kostenlose Software zum Anzeigen, lokalen Prüfen und Drucken von signierten Dokumenten an PCs ohne installiertes Vollprodukt GERVA.

Dabei schließt der GERVA-Viewer die Online-Prüfung einer qualifizierten elektronischen Signatur im Verzeichnisdienst ein, so dass auch Anwender ohne das Vollprodukt GERVA und ohne zertifizierte Signaturkarte eine Überprüfung einer Signatur vornehmen können. Der GERVA-Viewer kann kostenfrei heruntergeladen werden unter:
<http://www.datevstadt.de/eseccure>

Die Vorteile auf einen Blick

höchste Sicherheit für den gesamten E-Mail-Verkehr

sensitive Dokumente und Informationen werden vor dem Zugriff Unbefugter geschützt

die Authentizität und Integrität der Daten wird überprüft

Dokumente rechtsverbindlich elektronisch signieren

9. Digitale Signatur - Wirkungsweise und Anwendungen

Dipl.-Ing. Detlef Dienst
T-Telesec, Untere Industriestraße 20, 57250 Netphen
Tel.: ++49 (0) 271 – 708-1670
E-Mail: detlef.dienst@telekom.de
<http://www.telesec.de>

Abstract

Im Rahmen der Kommerzialisierung des Internet werden immer mehr Geschäftsprozesse über das Internet abgewickelt. Die weltweite Verfügbarkeit des Internet hat entscheidend dazu beigetragen, dass dieses Medium auch für die globale Kommunikation große Bedeutung erlangt hat.

Technologie auf Basis von Internet-Standards zeichnet sich durch hohe Zuverlässigkeit und Robustheit der Kommunikationsprotokolle aus; aus dem Bereich der Internet-Anwendungen haben das World Wide Web (WWW) und E-Mail besondere Bedeutung erlangt. Die Technologie des Internet hat auch Einzug in Unternehmensnetze gehalten (Intranet), die in vielen Fällen unter Verwendung geeigneter Sicherheitskomponenten mit dem Internet verbunden werden.

Standard-Applikationen im Internet unterstützen Sicherheitsdienste nicht in ausreichendem Maße bzw. werden nur wenig genutzt. Abhören und Verfälschen digitaler Kommunikation ist für versierte Angreifer häufig kein Problem. Der Anreiz für Angreifer, sensible Informationen abzuhehren oder zu verfälschen, steigt mit dem Umfang und der wirtschaftlichen Bedeutung der Geschäftsprozesse, die über elektronische Medien abgewickelt werden. So ist Wirtschaftsspionage heute eine ernstzunehmende Bedrohung für die Unternehmen geworden.

Neben der Vertraulichkeit der Informationen, die in der Regel durch Verschlüsselung gewährleistet wird, kommt der Authentizität und Integrität von Informationen maßgebliche Bedeutung zu. Die letztgenannten Sicherheitsdienste können mittels digitalen Signaturen (Stichwort: Signaturschlüssel und digitale Zertifikate) erbracht werden. Um digitale Signaturen anwenden zu können, sind neben geeigneten Anwendungskomponenten umfangreiche Investitionen in eine Public Key Infrastruktur (PKI) notwendig. Trust Center erbringen im Rahmen dieser Infrastruktur Dienstleistungen („Zertifizierungsdiensteanbieter“) und werden nach privatrechtlichen Geschäftsbedingungen oder den gesetzlichen Richtlinien des Signaturgesetzes (SigG) betrieben.

Der Vortrag erläutert in kurzer Form technische, organisatorische und juristische (wichtige Eigenschaften des SigG) Rahmenbedingungen für einen Zertifizierungsdiensteanbieter. Anwendungsszenarien und ein Überblick über Produkte, Lösungen und Referenzen des Produktbereiches T-TeleSec (T-Systems, ITC Security) folgen. Die Präsentation benennt Voraussetzungen für einen erfolgreichen Einsatz der „Digitalen Signatur“ in Wirtschaft und Verwaltung und schließt mit einem Ausblick in die Zukunft.

10. www.bremer-online-service.de Der Vorreiter und Preisträger in der Pflicht

Dr. Stephan Klein

Bremen Online Services Entwicklungs- und Betriebs- GmbH & Co. KG, Am Fallturm 9, 28359 Bremen

Tel.: ++49 (0) 421 – 2 04 95 - 25

E-Mail: sk@bos-bremen.de

<http://www.bos-bremen.de>

Abstract

Mit der Verleihung des diesjährigen TeleTrust-Innovationspreises „Anwendungen elektronischer Signaturen in Europa“ wurde der bremer-online-service für seine vorbildlichen Internet-Anwendungen auf Basis der elektronischen Signatur ausgezeichnet.

Der bremer-online-service wird im Rahmen des MEDIA@Komm-Projektes von der bremen online services GmbH & Co. KG (bos) in enger Zusammenarbeit mit zahlreichen Dienststellen der bremischen Verwaltung entwickelt. MEDIA@Komm ist ein von der Bundesregierung initiiertes Wettbewerb mit dem Ziel, die Entwicklung und Anwendung von Multimedia, unter Einbeziehung der elektronischen Signatur, in Städten und Gemeinden zu unterstützen. 1999 wurden die Konzepte der Stadt Esslingen, des Städteverbundes Nürnberg und der Hansestadt Bremen aus 136 beteiligten Städten und Gemeinden als Sieger ermittelt.

Das Konzept der Hansestadt sieht ein Internet-Portal für Online-Behördengänge und private Dienstleistungen vor. Im bremer-online-service wurde bereits ein Großteil dieses Konzeptes umgesetzt. Der Service arbeitet mit elektronischen Signaturen nach dem deutschen Signaturgesetz. Dies ermöglicht sichere und rechtsverbindliche Transaktionen über das Internet. Bereits jetzt sind mehr als 30 Geschäftsprozesse, wie beispielsweise die Bestellung von Urkunden beim Standesamt, Adress- oder Stammdatenänderung bei verschiedenen Dienstleistern, Beantragung von Urlaubssemestern bzw. Exmatrikulation an den Bremer Hochschulen und der Universität und der Nachsendeantrag bei der Post, mit dem bremer-online-service möglich. Bis Ende 2002 ist, in Zusammenarbeit mit 27 regionalen und überregionalen, öffentlichen und privaten Dienstleistern, die Umsetzung von mehr als 100 Geschäftsprozessen geplant.

Als technische Basis dieser Online-Angebote für Unternehmen, Bürgerinnen und Bürger, dient das von bos entwickelte Produkt OSCAR (**O**nline **S**ervices **C**omputer Interface **A**rchitecture). Diese Sicherheitstechnologie ermöglicht den vertraulichen und sicheren Transport der Online-Formulare, so dass die übersandten und signierten Daten nur vom Empfänger und weder auf dem Weg durchs Netz noch von anderen Dienstleistern eingesehen werden können.

Um einen unkomplizierten und einfachen Zugang zum bremer-online-service zu gewährleisten, wurden im gesamten Stadtgebiet zahlreiche Registrierungsstellen und betreute Nutzerplätze eingerichtet. Bei den Registrierungsstellen können, gegen eine geringe Schutzgebühr, die erforderliche Signaturkarte und das zugehörige Kartenlesegerät für den Computer erworben werden. Wer keinen eigenen Computer besitzt oder sich unter fachkundiger Anleitung mit der neuen Technologie anfreunden möchte, kann einen betreuten Nutzerplatz aufsuchen. Geschultes Personal bietet dort Interessierten Unterstützung bei den ersten Schritten in die neue, sichere Online-Welt.

Nicht zuletzt aufgrund der Verleihung des Innovationspreises fühlen sich die Akteure der bremischen Verwaltung und die Crew der bremen online services GmbH & Co. KG angespornt, den bremer-online-service weiter zu einem umfassenden Angebot für Unternehmen, Bürgerinnen und Bürger auszubauen.

11. Elektronische Heilberufsausweise: Stand der Einführungsvorbereitungen und noch zu lösende Probleme

Dipl.-Inform. Reinhold A. Mainz
Kassenärztliche Bundesvereinigung, Herbert-Lewin-Str. 3, 50931 Köln
Tel.: ++49 (0) 221 – 4005-215
E-Mail: Reinhold.A.Mainz@kbv.de
<http://www.kbv.de>

Abstract

Die Landesärztekammern bereiten derzeit in Zusammenarbeit mit den Kassenärztlichen Vereinigungen die Ausgabe Elektronischer Arztausweise vor. Gemäß Absprache mit den anderen Organisationen des Gesundheitssystems sollen diese Ausweise als ein Muster für einen Heilberufsausweis dienen; deren Ausgabe an die Ärzte ist deshalb als erster Schritt einer flächendeckenden Ausstattung aller Gesundheitsberufe mit einer Chipkarte zu verstehen, die als Werkzeug einer einrichtungs- und sektorübergreifenden elektronischen Kommunikation einzuordnen ist.

Der Elektronische Heilberufsausweis soll 5 Funktionen erfüllen bzw. unterstützen, nämlich:

- Ersatz eines bisherigen Sichtausweises durch die äußere Gestaltung der Chipkarte
- elektronische Ausweisfunktion in Form einer signierten und offen lesbaren Ausweisdatei
- qualifizierte elektronische Unterschrift (Digitale Signatur)
- Ver- bzw. Entschlüsselung von Datenobjekten
- Authentisierung gegenüber Rechnern, Geräten oder Anwendungen.

Die Kammern und die anderen Körperschaften öffentlichen Rechts, welche die Berufsausübung regeln, sind Bestätigungsstellen für berufsbezogene Attribute nach Maßgabe des Signaturgesetzes (SigG). Nach dem vorliegenden Entwurf der Signaturverordnung können sie qualifizierte Attributzertifikate, die sich auf Signaturzertifikate anderer Zertifizierungsstellen beziehen können, selbst signieren, wenn sie Zertifizierungsdiensteanbieter nach den Regeln des SigG sind. Deshalb wird unabhängig von der Ausgabe Elektronischer Heilberufsausweise erwogen, selbst als (ggf. virtueller) Zertifizierungsdiensteanbieter aufzutreten.

Daneben besteht die Überlegung, als Registrierungsstelle für unterschiedliche Zertifizierungsstellen, die vom Arzt frei wählbar sein sollen, zu fungieren.

Dabei besteht in jedem Falle die Absicht, sich zur technisch-organisatorischen Durchführung der Aufgaben eines anderen (akkreditierten) Zertifizierungsdiensteanbieters zu bedienen. Jede im Gesundheitssystem zwecks Ausgabe von Sicherheitszertifikaten tätig werdende Stelle soll sich bei diesem Konzept eines anderen Zertifizierungsdiensteanbieters bedienen können.

Durch dieses marktoffene Verhalten entstehen z. B. Probleme hinsichtlich der Durchsetzung einer einheitlichen Sicherheitspolitik für das Gesundheitssystem, der Einhaltung von Standards sowohl für eine übergreifende Kommunikation als auch hinsichtlich der Verwendung unterschiedlicher Bausteine zur Konstruktion einer Kommunikations- und Sicherheitsumgebung sowie hinsichtlich des Verbunds von Verzeichnisdiensten zwecks Darstellung eines allgemeinen Adressbuchs für das Gesundheitssystem. Außerdem entstehen Probleme durch den Zwang, sich verschiedenen Sicherheitskonzepten „unterwerfen“ zu müssen und zur automatisierten Abwicklung der Geschäftsprozesse zwischen Registrierungs- und Zertifizierungsstelle unterschiedliche Schnittstellen bedienen zu müssen. Neben diesen technischen Aspekten einer marktoffenen, aber flächendeckend funktionsfähigen Kommunikations- und Sicherheitsinfrastruktur existieren auch noch offene Fragen zur inhaltlichen Ausprägung von Zertifikaten. Alle diese Probleme werden dadurch verschärft, dass die elektronische Kommunikation im Gesundheitssystem letztendlich weltweit interoperabel funktionieren soll, ohne dass dabei auf wesentliche Elemente einer definierten Sicherheitspolitik verzichtet werden kann. Dies wirft insbesondere die Frage nach einer standardisierten Beschreibung und Vergleichbarkeit von Sicherheitspolitiken auf.

12. eGovernment und Elektronische Signatur in der Landesverwaltung Rheinland-Pfalz

MinR Gregor Schulte
Ministerium des Innern und für Sport, Schillerplatz 3-5, 55116 Mainz
Tel.: ++49 (0) 6131 – 16 - 3238
E-Mail: gregor.schulte@ism.rlp.de
<http://www.ism.rlp.de>

Abstract

Die Novelle zum Signaturgesetz und die aktuellen Gesetzesinitiativen zur Gleichstellung der elektronischen Unterschrift mit der herkömmlichen Schriftform im Privat sowie im öffentlichen Verfahrensrecht weisen Richtung und die Dynamik der aktuellen Entwicklung in Richtung eGovernment auf.

Die elektronische Signatur wird nicht mit Macht kommen, aber unaufhaltsam. Die öffentlichen Verwaltungen müssen sich technisch, organisatorisch und nicht zuletzt finanziell darauf einstellen. Hier liegen Hemmnisse, die behutsam beurteilt und abgebaut werden müssen.

Rheinland-Pfalz hat seine Landesverwaltung grundlegend neu gestaltet. Die Funktionalreform eröffnet den Einstieg in eGovernment, schon im Wortlaut des Reformgesetzes.

In den letzten 2 Jahren wurden etwa 8.000 PC-Arbeitsplätze in den ehemaligen Bezirksregierungen, den Polizeidienststellen und in den Gerichten einheitlich ausgestattet und komplett über das *rlp*-Netz des Landes vernetzt.

Ein einheitliches Dokumentenmanagement-System und IT-gestützte Vorgangsbearbeitung sind die nächsten Schritte ab Januar 2002.

Die Nutzung von IP-Diensten (Mail & Surf) hat sich von Juni 2000 bis März 2001 mehr als verdreifacht. Mails sind jetzt Bestandteil virtueller Akten.

Dokumente im internen und externen Geschäftsverkehr müssen authentisierbar sein. Erste Pilot starten im Haushalts- und Kassenwesen. Die Polizei folgt mit mittelfristig rd. 10.000 Nutzern. Aber die Festlegung der Sicherheits-Standards und der Interoperabilität von Systemen steht aus.

Rheinland-Pfalz hat im März 2001 für die Landesverwaltung festgelegt, nur ein einheitliches (multifunktionales) System zu nutzen. Es baut auf den Adressstrukturen im *rlp*-Netz auf und steht auch den Kommunen offen.

(Noch) Nicht alles muss signiert und verschlüsselt werden. Pilote im Haushalts- und Kassenrecht mit 500 Arbeitsplätzen sind gestartet. Personalräte verlangen zu Recht die Verschlüsselung bei der Transfer von Personaldaten. Der Druck wird größer, wenn bei den Gerichten elektronisch signierte Klagen eingehen. Viel Zeit bleibt nicht.

Im Raum stehen Kosten von ca. 300 DM pro Arbeitsplatz und Jahr. Das bedeutet bei 20.000 Usern eine zusätzliche Haushaltsbelastung von rd. 6 Mio. DM pro Jahr.

13. Elektronische Signatur für sicheres eBusiness - Praktische Einsatzmöglichkeiten am Beispiel der IHK-Anwendungen

Dipl.-Bw. (FH) Klaus Berens
Deutscher Industrie- und Handelskammertag, Postfach 1446, 53004 Bonn
Tel.: ++49 (0) 228 – 104 - 1632
E-Mail: berens.klaus@bonn.dihk.de
<http://www.dihk.de>

Abstract

Im elektronischer Geschäftsverkehr finden geschäftliche Transaktionen derzeit noch in dem Vertrauen statt, dass der Käufer die Ware unter seinem richtigen Namen bestellt hat und auch tatsächlich haben will, und dass das Angebot des Verkäufers auch richtig übermittelt wurde. Nachprüfbar war dies bislang nicht. Die digitale Signatur im elektronischen Geschäftsverkehr ermöglicht eine genaue Identifikation des Geschäftspartners. Sie schafft außerdem die Sicherheit, dass die gegenseitig übermittelten Vertragsbedingungen keine unerwünschte Veränderung erfahren haben.

Die DE-CODA hat Anwendungen geschaffen, die die Verwendung der digitalen Signatur im Servicebereich der IHKs fördern und durchsetzen soll.

Die Anwendungen umfassen zwei Teilbereiche der IHK-Tätigkeit, die Eintragung von Berufsausbildungsverträgen in das Verzeichnis der Ausbildungsverhältnisse der Industrie- und Handelskammern sowie die Ausstellung von Ursprungszeugnissen durch die IHKs.

Die Berufsausbildungsverträge können von den Unternehmen digital an die IHK übermittelt werden. Die Unternehmen wählen sich dazu über das Internet in die entsprechende Maske <http://signatur.ihk.de> ein und füllen das dort erscheinende Formular online aus. Dieses drucken sie anschließend aus und legen es dem Auszubildenden zur Unterzeichnung vor. Wird dieser Vertrag von beiden Parteien akzeptiert und „händisch“ unterzeichnet, ruft das Unternehmen wieder die noch gespeicherten Daten in der IHK-Maske auf und unterzeichnet diese digital.

Danach wird das signierte Dokument verschlüsselt auf dem Server abgelegt. Eventuell notwendige Bescheinigungen müssen eingescannt und ebenfalls digital signiert und verschlüsselt übermittelt werden. Durch ihre digitale Signatur bestätigen die Unternehmen rechtskräftig die Übereinstimmung des elektronisch übersandten Vertrages mit dem von beiden Vertragsparteien unterzeichneten Vertrag. In der Zukunft wird es auch möglich sein, daß neben dem Auszubildenden auch der Auszubildende durch seine digitale Signatur die Richtigkeit des übersandten Vertrages bestätigt.

Anträge für Ursprungszeugnisse können von den Unternehmen digital signiert mithilfe eines zugehörigen Online-Formulars <http://signatur.ihk.de> an die IHKs verschlüsselt übermitteln. Mit der digitalen Signatur bestätigt der Unternehmer die Richtigkeit der übermittelten Daten. Des weiteren besteht für die Unternehmen die Möglichkeit, am Bearbeitungsprozess teilzunehmen, da Sie Anmerkungen des IHK-Mitarbeiters direkt einsehen und auch sofort darauf reagieren können.

Nach endgültiger Bewilligung des Antrages auf Ausstellung eines Ursprungszeugnisses druckt die IHK das Dokument aus, unterzeichnet es „händisch“ und schickt es dem Unternehmen auf dem herkömmlichen Wege zu. Dies ist notwendig, da die Zollbehörden derzeit noch keine elektronischen Dokumente akzeptieren. In Zukunft ist demnach mit einer weiteren Vereinfachung des Vorgangs zu rechnen, wenn auch die zuständigen Behörden die neuen Medien konsequent einsetzen.

14. Das Konzept der digitalen Signatur in Theorie und Praxis

RegDir Dr. Ulrich Sandl
Referat IT-Sicherheit Bundesministerium für Wirtschaft und Technologie
Scharnhorststr. 36, 10115 Berlin
Tel.: ++49 (0) 30 - 2014 - 6080
E-Mail: sandl@bmwi.bund.de
<http://www.bmwi.de>

Abstract

Am 22. Mai 2001 trat das neue deutsche Signaturgesetz in Kraft (BGBl I, S. 876). Es ersetzte das Signaturgesetz vom 22. 7. 1997 und setzte damit die europäische Richtlinie für elektronische Signaturen in nationales Recht um. Ebenso wurden mit dieser Novelle Konsequenzen aus der 1999 durchgeführten Evaluierung des damaligen Signaturgesetzes gezogen.

Ziel der Bundesregierung ist es nunmehr, "gesetzeskonforme", weil besonders sichere, digitale Signaturen dort wo möglich und nötig zum Einsatz zu bringen, um dadurch das Vertrauen der Nutzer in die Sicherheit der Informationsgesellschaft insgesamt zu erhöhen. Erhebliche Anstrengungen werden deshalb heute unternommen, um die Haupthemmnisse einer solchen Verbreitung, nämlich die mangelnde Interoperabilität der unterschiedlichen Signatursysteme sowie die bislang noch fehlenden Nutzenanwendungen (Geschäftsmodelle) zu beseitigen.

Nicht alleine die Politik und die Verwaltungen sind hier allerdings gefordert, auch und vor allem die Wirtschaft muss jetzt einen Beitrag dazu leisten, Sicherheit auf "breiter Front" im elektronischen Geschäftsverkehr durchzusetzen.

15. Konzernweites Zertifikatsmanagement

Dr. Armin Ratz
Dresdner Bank AG, Jürgen-Ponto-Platz 1, 60301 Frankfurt am Main
Telefon: ++49 (0) 96 – 26317500
E-Mail: Armin.Ratz@Dresdner-Bank.com
<http://www.dresdner-bank.com>

Dipl.-Inform. Frank Losemann
Institut für Telematik, Bahnhofstr. 30-32, 54292 Trier
Telefon: ++49 (0) 651 - 97551-60
E-Mail: losemann@ti.fhg.de
<http://www.ti.fhg.de>

Abstract

Der flächendeckende Einsatz digitaler Signaturen setzt eine leistungsfähige Public-Key-Infrastruktur voraus. Dieser Beitrag stellt eine frühe konzernweite Realisierung einer auf dem Einsatz Digitaler Signaturen basierten Authentisierungslösung vor. Der praktische Umgang mit Digitalen Signaturen bzw. das Management der Zertifikatsvergabe und -kontrolle, steht seit 1997 im Mittelpunkt einer projektbezogenen Kooperation mit der Dresdner Bank AG in Frankfurt. Die dort benötigte Anpassung der Authentikations- und Autorisationsumgebung für web-basierte Internetanwendungen bot die Gelegenheit, Zertifikate im Intranet an potentiell ca. 50.000 Mitarbeiter im In- und Ausland zu verteilen.

Die Nutzung von Zertifikaten zur Realisierung von Secure-Single-Sign-on wurde auf der Basis von SSL/TLS realisiert. Dazu war zunächst die Einrichtung und Entwicklung einer Zertifizierungsstelle im Intranet erforderlich, um die IT-Systeme und Mitarbeiter der Bank effizient und kostengünstig mit X.509v3-Zertifikaten zu versorgen.

Entscheider, Entwickler, Administratoren und nicht zuletzt die Anwender selbst mussten mit der Handhabung der bis dato unbekanntenen X.509 Zertifikate erst vertraut gemacht werden: Mit dem Zertifikat wird die sicher und nachvollziehbar authentifizierte Nutzung verschiedenster Intranet - Informationsdienste möglich, ohne sich bei jedem einzeln erneut anzumelden. Dabei wurde auf minimale Anforderungen auf Clientseite Wert gelegt, um die Reichweite auch auf Tochterunternehmen im In- und Ausland mit unterschiedlichen IT-Systemen ausdehnen zu können. Seit vier Jahren wird die von den Autoren dieses Beitrags flexibel konzipierte PKI betrieben, ständig erweitert und an veränderte Prozesse in der IT-Landschaft eines international tätigen Finanz-Konzerns angepasst.

Der Vortrag gibt einen Einblick in den Aufbau und den Betrieb einer frühen konzernweiten, heterogenen Public-Key-Infrastruktur. Er möchte die Bedeutung der Anwender-Aspekte illustrieren und stellt hierzu konkrete Maßnahmen vor und zur Diskussion.