



TELETRUST Deutschland e.V



Verein zur Förderung  
der Vertrauenswürdigkeit  
von Informations- und  
Kommunikationstechnik

# TELETRUST

## 1989-2004

### Bilanz und Ausblick

> information  
> security  
> solutions



Festschrift

anlässlich des  
15 jährigen Bestehens von  
*TELETRUST* Deutschland e.V.

*TELETRUST*

1989-2004

Bilanz und Ausblick

## Impressum

*Herausgeber:*  
Helmut Reimer

*Satz und Gestaltung:*  
Oliver Reimer

*Herstellung:*  
DATEV eG

© TeleTrusT Deutschland e.V., 2004

*Geschäftsstelle:*  
Chamissostraße 11, D-99096 Erfurt  
E-Mail: [info@teletrust.de](mailto:info@teletrust.de)

## Grußworte

Bundesminister des Innern

**Otto Schily** \_\_\_\_\_ 7

Bundesminister für Wirtschaft und Arbeit

**Wolfgang Clement** \_\_\_\_\_ 9

## Die Kompetenz von *TELETRUST*

Norbert Pohlmann

**Netzwerk für Informationssicherheit** \_\_\_\_\_ 13

Michael Leistenschneider

***TELETRUST* als Mittler zwischen Technologie und Anwendung** \_\_\_\_\_ 15

Jürgen Sembritzki

***TELETRUST* als Integrationsplattform für vertrauenswürdige Lösungen** \_\_\_\_\_ 17

Claudia Eckert

***TELETRUST* als Brücke zwischen Forschung und Markt** \_\_\_\_\_ 19

## Was hat *TELETRUST* bewirkt

Helmut Reimer

**Die Stunde der Wahrheit rückt näher** \_\_\_\_\_ 23

Fritz Bauspieß, Wolfgang Schneider

**Kommunikations- und Transaktionssicherheit** \_\_\_\_\_ 25

Arno Fiedler, Peter Steiert, Stephan Wappler

**Services für eBusiness & eGovernment** \_\_\_\_\_ 27

Ulrike Schulte

***TELETRUST* international** \_\_\_\_\_ 31

Volker Schneider

**Runder Tisch Kryptowirtschaft** \_\_\_\_\_ 33

Kai Hartwich

**TISP** \_\_\_\_\_ 35

## Neue Herausforderungen

Michael Hartmann, Sachar Paulus	
<b>Neue Sicherheitsarchitekturen</b>	39
Detlef Dienst	
<b>Robuste PKI-Lösungen für große Anwendergruppen</b>	43
Astrid Albrecht	
<b>Biometrie Quo Vadis</b>	45
Jörg-M. Lenz	
<b>Unterschriften im digitalen Zeitalter</b>	47
Stephan Wappler	
<b>IT-Sicherheit und Mobilität</b>	49
Bernd Kowalski	
<b>Marktgerechte IT-Sicherheitsevaluierung und -zertifizierung</b>	51
Stefan Engel-Flehsig	
<b>Rechtsrahmen: Regulierung und Märkte</b>	53
<b><i>TELETRUST</i> zur Wirksamkeit der EG-Signatur-Richtlinie 1999/93/EG</b>	55

## *TELETRUST* in der Informationsgesellschaft

Matthias Büger, Bernhard Esslinger	
<b>PKI-Life</b>	61
Willi Kafitz	
<b>Flexible Sicherheitsinfrastrukturen</b>	63
Ismet Koyun	
<b>Kooperation für IT-Sicherheitslösungen</b>	65

## Anhang

### ***TELETRUST* in Fakten 1989 – 2003**

<b><i>TELETRUST</i> – Fakten</b>	69
<b>Chronologie</b>	69
<b><i>TELETRUST</i>-Mitglieder – Stand Juli 2004</b>	78

# **Grußworte**



# Grußwort

zum 15jährigen Bestehen von *TELETRUST* Deutschland e.V.

des Bundesministers des Innern, Otto Schily



Staat und Wirtschaft haben gemeinsame Verantwortung für die IT-Sicherheit: Noch nie gab es so viele Angriffe wie heute, beispielsweise durch gefährliche und stark verbreitete Viren. Mitte des Jahres waren bereits in einem Monat – mit steigender

Tendenz – mehr Angriffe von Viren und Würmern zu verzeichnen als im gesamten letzten Jahr. Das Bundesamt für Sicherheit in der Informationstechnik berichtet über ein Schadpotenzial der Viren und Würmer, das heute größer ist als je zuvor. Hinzu kommt, dass die Ersteller der Schadprogramme zunehmend auch wirtschaftliche Interessen verfolgen und beispielsweise mit Spam-Versendern zusammenarbeiten. Teilweise werden dabei auch gefälschte Absenderadressen verwendet.

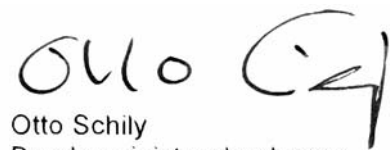
Die Bedeutung der Absicherung der IT-Systeme nimmt vor diesem Hintergrund täglich weiter zu. Insbesondere bedürfen die kritischen IT-Infrastrukturen eines besonderen Schutzes. Seit dem 11. September 2001 hat die Bundesregierung die Ausgaben für bestehende IT-Systeme der Sicherheitsbehörden und für die Erprobung und Entwicklung neuartiger IT-gestützter Verfahren im Bereich der Kriminalitäts- und Terrorismusbekämpfung deutlich erhöht und den Dialog mit den Betreibern kritischer Infrastrukturen intensiviert.

Bei der gemeinsamen Gestaltung der IT-Sicherheitskultur in unserem Land spielen die Verbände natürlich eine bedeutsame Rolle. *TELETRUST* ist deshalb auch für die Bundesregierung ein wichtiger An-

sprechpartner. Mit seinem Engagement etwa bei ISIS-MTT oder der European Bridge-CA hat sich *TELETRUST* als zuverlässiger und kompetenter Partner etabliert.

IT-Sicherheit ist bedeutsam auch für den Bereich eGovernment. Sicherheit und Vertrauen der IT haben einen festen Platz in der eGovernment-Initiative der Bundesregierung BundOnline. Das Bundesamt für Sicherheit in der Informationstechnik hat für BundOnline deshalb eine Virtuelle Poststelle als zentrale Basiskomponente zur Datensicherheit entwickelt. Diese soll die Kommunikation zwischen den Bürgerinnen und Bürgern, der Wirtschaft mit der Bundesverwaltung und der Behörden untereinander absichern. Hierbei werden Verfahren zum Schutz der Vertraulichkeit, Integrität und Authentizität, also Verschlüsselung und elektronische Signaturen eingesetzt.

Im Zuge von BundOnline werden über 100 Behörden zu Online-Dienstleistern. 268 Online-Angebote hat die Bundesverwaltung bereits realisiert. Diese 268 eGovernment-Angebote stehen für 268 Verwaltungsverfahren, die Bürgerinnen und Bürger, Unternehmen und andere Verwaltungsstellen komfortabel, aber vor allem sicher über das Internet abwickeln können. Jede dieser Dienstleistungen ist dabei ein konkreter Beitrag zum Bürokratieabbau und zur Modernisierung der Verwaltung.



Otto Schily  
Bundesminister des Innern



# Grußwort

zum 15jährigen Bestehen von *TELETRUST* Deutschland e.V.

des Bundesministers für Wirtschaft und Arbeit, Wolfgang Clement



Erfolg oder Misserfolg eines Unternehmens hängen in globalen Märkten nicht nur von herausragenden Produkten und Dienstleistungen ab, sondern auf unserem Weg in die moderne Wissensgesellschaft werden Informationen immer bedeutender für wirtschaftliches Handeln. Sie bilden die Basis komplexer

Kommunikationsprozesse zwischen Unternehmen und öffentlichen Institutionen, zwischen der Geschäftsleitung und den Mitarbeitern und vor allem zwischen Lieferanten und Kunden.

Deutschland ist bei der Verbreitung und Nutzung der modernen Informations- und Kommunikationstechnologien, vor allem des Internets, in den letzten Jahren deutlich vorangekommen. Rund die Hälfte der deutschen Bevölkerung ist online. Bei den deutschen Unternehmen sind es weit über 90 Prozent.

Die Entwicklung Deutschlands zu einem weltweit führenden Standort der Informations- und Kommunikationstechnologien stellt einen wesentlichen Beitrag für mehr Wachstum und Beschäftigung in unserem Land dar. Der vor Kurzem verabschiedete Masterplan „Informationsgesellschaft Deutschland 2006“ ist Teil des umfangreichen Reformprozesses zur Modernisierung des Arbeitsmarktes und der sozialen Sicherungssysteme.

Damit wir das Wachstumspotential der neuen Informationstechniken voll ausschöpfen können, brauchen wir Vertrauen in die Sicherheit und Zuverlässigkeit der Informations- und Kommunikationstechnik. Ziel der Bundesregierung ist, das Sicherheitsbewusstsein durch eine umfassende Aufklärung über mögliche Gefahren und Bedrohungen des Internets, vor allem über wirksame Schutzmaßnahmen, zu stärken.

Der wirtschaftliche Erfolg eines Unternehmens hängt zunehmend davon ab, inwieweit es gelingt, die betriebsinternen Datenbestände und betriebsinterne und -externe Kommunikation vor Datenverlust und Datenmissbrauch zu schützen. IT-Sicherheit ist von zentraler wirtschaftspolitischer Bedeutung.

Gerade die mittelständischen Unternehmen benötigen in besonderem Maße Hilfe und Unterstützung. Deshalb haben wir ein Frühwarnsystem für Gefahren aus dem Internet, ein sog. „Computer Emergency Response Team“, speziell für mittelständische Bedürfnisse eingerichtet. Auch mit unserer breit angelegten Sensibilisierungskampagne „Sicherheit im Internet – gerade für den Mittelstand“ ([www.mittelstand-sicher-im-internet.de](http://www.mittelstand-sicher-im-internet.de)) wollen wir das IT-Sicherheitsbewusstsein im Mittelstand schärfen und den betreffenden Betrieben das notwendige Know How über die vorhandenen Schutzmechanismen vermitteln. Dadurch beseitigen wir eine der wesentlichen Barrieren für die weitere Verbreitung des Electronic Commerce.

Seit seinem Bestehen hat der *TELETRUST*-Verein einen wichtigen Beitrag geleistet, das Vertrauen in die modernen Informations- und Kommunikationstechniken zu steigern. Dafür danke ich Ihnen. Auch für die Zukunft zähle ich auf Ihre Mitarbeit und Ihr Engagement bei der Weiterentwicklung der Informationsgesellschaft in Deutschland. Denn die breite Nutzung dieser Schlüsseltechnologie ist zu einem entscheidenden Faktor für Wachstum und Wohlstand im globalen Informationszeitalter geworden.

Ihr





# **Die Kompetenz von *TELETRUST***

Über neunzig institutionelle Mitglieder des Vereins fördern die Entwicklung von Technologien für vertrauenswürdige elektronische Geschäftsprozesse.



# Netzwerk für Informationssicherheit

Der gemeinnützige Verein TELETRUST Deutschland e.V.

Norbert Pohlmann

*Vorstandsvorsitzender des TELETRUST-Vereins*

*Chairman des Programmkomitees der ISSE (Information Security Solutions Europe)*

*Mitglied des Lenkungskreises „secure-it.nrw.2005“  
Leitprojekt des Wirtschaftsministeriums des Landes NRW*

## Globales Denken für Informationssicherheit

Wir entwickeln uns zunehmend zu einer Informations- und Wissensgesellschaft, in der Verlässlichkeit von Informations- und Kommunikationstechnik eine besondere Rolle spielt.

In den letzten Jahren des Wirkens von TELETRUST sind die Sicherheitsprobleme nicht kleiner sondern größer geworden.

Das Internet, eine der wichtigsten Infrastrukturen in unserer modernen Gesellschaft, ist sehr schnell gewachsen, und das ist auch gut so, weil die Möglichkeiten und Vorteile unbegrenzt scheinen. Das Web, die E-Mail-Kommunikation, haben z.B. enorme Vorteile gebracht, und es besteht in Zukunft noch ein sehr großes Potential, Geschäftsprozesse rationaler abzuwickeln. Jetzt besteht die größte Herausforderung darin, für eine passende Vertrauenswürdigkeit zu sorgen.

Dies ist notwendig, damit wir einerseits die schon genutzten Dienste weiterhin verlässlich nutzen können und andererseits als Enabler damit weitere neue Dienste überhaupt über das „Internet“ abwickeln können.

Da das Internet über alle geographischen und politischen Grenzen, Gesetze und Kulturen hinaus geht, stellt es neue und ungewohnte Herausforderung für die internationale Kommunikations-Gesellschaft dar.

Hier ist ein Netzwerk von unterschiedlichen Akteuren aus verschiedenen Bereichen und Disziplinen zur Lösung der anstehenden Aufgaben gefragt.

## Interdisziplinäre Lösungen

Die Probleme liegen auf sehr unterschiedlichen Ebenen:

- Internationales Recht und nationale Jurisprudenz,
- standardisierte Sicherheitstechnologie und anwendungsspezifische Anforderungen,
- Ordnung schaffen in der schnell gewachsenen Internet-Technologie (DNS, E-Mail-Gateways, Identifikations- und Authentifikationsmanagement, ...), ...

Die Einführung von Informationssicherheitssystemen, die für eine Verlässlichkeit von Informations- und Kommunikationstechnik im „Internet“ sorgen sollen, unterliegt in der Regel einem Grundproblem: Es nützt nicht viel, wenn einige wenige Fachleute diese Sicherheitssysteme kennen, sie bedienen kann und praktisch nutzen, die Masse aber nicht. Es ist wie im Straßenverkehr: Es reicht eben nicht aus, dass nur einige die Verkehrsregeln kennen und sich an sie halten: dies müssen schon die meisten tun. Aber



Prof. Dr.  
Norbert Pohlmann

Geschäftsführender Gesellschafter  
der Firma KryptoKom  
(1988 bis 1999)  
Mitglied des Vorstandes  
der Utimaco Safeware AG  
(1999 bis 2003)  
Seit 2003: Professor für  
„Verteilte Systeme und  
Informationssicherheit“

Fachbereich Informatik  
Fachhochschule Gelsenkirchen

E-Mail: [norbert.pohlmann@informatik.fh-gelsenkirchen.de](mailto:norbert.pohlmann@informatik.fh-gelsenkirchen.de)

erst, wenn sie es mit einer gewissen intelligenten Anpassungsfähigkeit machen, statt buchstabengetreu und stur dogmatischen Regeln zu folgen, kann der Verkehr fließen – in unserem Fall kann so eine ausreichende Verlässlichkeit von Informations- und Kommunikationstechnik hinsichtlich Sicherheit und Handhabbarkeit im konkreten Anwendungskontext erreicht werden.

Beispiele für Funktionskomponenten und Dienste, die diesem Grundproblem unterliegen, sind: PKI's, Elektronische Signatur, organisationsübergreifende Verschlüsselung, Ordnung im Internet (DNS, E-Mail-Server, usw.).

## Kompetenznetzwerk TELETRUST

Als TELETRUST Deutschland vor 15 Jahren unter anderem auch von mir gegründet wurde, war der Verein eher ein Club aus elitären Spezialisten der theoretischen technologischen Entwicklung.

Im Laufe der Zeit hat es, meist aufgrund praktischer Anwendungen, Erkenntnisse gegeben, die die Entwicklung von TELETRUST maßgeblich bestimmten. Dem **Anwendungsbezug** kam zunehmende Bedeutung bei der Definition und Lösung von Aufgaben zu.

Ein beispielhaftes Szenario bietet die Telematik für Medizin und Gesundheitsverwaltung. Alle am TELETRUST-Kompetenznetzwerk beteiligten haben sich entsprechende Teilaufgaben gestellt. Es geht um Infrastrukturen und darauf aufbauende Dienste, um Sicherheitstoken wie SmartCards und dazu passende Terminals und um Applikationen, die die komplexen Telematik-Prozesse zwischen Kostenträgern, Leistungserbringern und Leistungsempfängern vertrauenswürdig abbilden können. Und interoperabel soll das Gesamtsystem dann auch noch sein!

Natürlich wird eine solche Entwicklung durch prägende Persönlichkeiten mitbestimmt. Bei TELETRUST geschah dies ab 1994 durch die Arbeit des TTT-Vorstandes Dr. Otfried P. Schaefer († 1998). Durch seine Impulse wurde 1995 die AG „Medizinische Anwendungen“ von TELETRUST gegründet, die diesen Sektor bis heute kompetent betreut. Die Visionen Dr. Schaefers finden heute mit den konkreten Vorhaben um die Einführung der elektronischen Gesundheitskarte und die elektronischen Heilberufsaussweise ihre praktische Umsetzung in der Massenentwicklung.

Ein wesentlicher Aspekt der Arbeit von TELETRUST ist es, bestehende Anwendungs-Probleme überwinden zu helfen:

- wir fördern die technologische Entwicklung, auch indem wir internationale Kongresse organisieren und durchführen (ISSE),
- wir helfen, Gesetze und Richtlinien für Deutschland und Europa zu entwickeln,
- wir erarbeiten Spezifikationen, damit internationale Standards besser umgesetzt werden können (ISIS-MTT)
- wir führen im Rahmen von Projekten wissenschaftliche Begleitforschungen durch, um u.a. sozio-ökonomische und technische Perspektiven zu erkennen (z.B. BioTrusT)
- wir bieten Dienste an, um Informationssicherheit über Grenzen, Gesetze und Kulturen hinweg nutzen zu können (European Bridge-CA).

TELETRUST ist heute ein Netzwerk aus Aktivisten im Betätigungsbereich verlässlicher Informations- und Kommunikationstechnik.

Die Akteure im TELETRUST-Verein kommen aus sehr unterschiedlichen Organisationen:

- Hersteller, die für einen breiten Markt Sicherheitsprodukte und -lösungen entwickeln und zur Verfügung stellen.
- Prüfstellen, die die Qualität von Informationssicherheitslösungen feststellen
- Hochschulen/Forschungsinstitute, die im Betätigungsbereich lehren und forschen.
- Schulungsorganisationen, die Sicherheitsschulungen und Aufklärungsarbeiten durchführen
- Beratungsunternehmen, die im Sicherheitsbereich umfangreiche Beratungen anbieten
- Verbände, für die Informationssicherheit einen wichtigen Punkt ihres Wirkens darstellt
- Behörden und öffentliche Institutionen, die in unserem Betätigungsbereich öffentliche Aufgaben erfüllen.
- Anwender/Firmen, für die Informationssicherheit ein strategisches und notwendiges Thema ist.
- Dienstleister, die in unserem Betätigungsbereich IT-Sicherheitsdienste anbieten.

Die Experten, die im TELETRUST aktiv sind, vertreten sehr unterschiedliche Disziplinen: Es sind Juristen, Ingenieure, Informatiker, Kaufleute, Hochschullehrer, Erfinder, Pragmatiker, usw., die gemeinsam umfängliche und ganzheitliche Lösungen erarbeiten. Dies geschieht in einzelnen Arbeitsgruppen von TELETRUST, in Projekten oder neuerdings auch in AG-übergreifenden, auf die interdisziplinäre Erstellung einzelner Lösungen abgestellten Arbeitsstrukturen.

Der TELETRUST-Verein arbeitet auch eng mit der Politik zusammen, um gesetzliche Notwendigkeiten und gemeinsames Interesse der Informations- und Wissensgesellschaft umsetzen zu helfen. Beispielhaft für diverse Aktivitäten seien hier nur einige genannt:

- Unterstützung des Signaturlbndnisses durch 10 strategischen Thesen und technisches kontinuierliches Know How für die Leitung der AG ‚Technik‘ des SigBü
- Gemeinsame Stellungnahme mit BITKOM zum Vorhaben der Europäischen Kommission ‚ENISA‘
- Stellungnahmen zu Gesetzgebungsvorhaben im Zusammenhang mit elektronischen Signaturen, (zuletzt 1. SigÄndG)
- Unterstützung des BMGS und der Selbstverwaltung bei den Aufgaben im Zusammenhang mit der Einführung von eGK und HPC (z.B. Rolloutskizze eGK, Kartenreport)
- Auch die weiteren bevorstehenden großen Kartenvorhaben der Bundesregierung (JobCard, Elektronischer Personalausweis) werden durch TTT konstruktiv begleitet werden.

TELETRUST, das Netzwerk für Informationssicherheit, hat in den letzten 15 Jahren viele Initiativen erfolgreich durchgeführt. In den nächsten Jahren werden sicherlich viele weitere neue Herausforderungen zu bestehen sein.

Ich wünsche mir für die Zukunft, dass noch weitere Akteure aus unterschiedlichen Disziplinen im TELETRUST-Verein aktiv werden, damit wir für unsere gemeinsame Zukunft für eine passende und notwendige verlässliche Informations- und Kommunikationstechnik sorgen und damit die Möglichkeiten der Informations- und Wissensgesellschaft sicher und umfänglich erschließen können.

# TELETRUST als Mittler zwischen Technologie und Anwendung

Interoperabilität ist Voraussetzung für vielfältige Anwendungen

Michael Leistenschneider

*Stellvertretender Vorstandsvorsitzender des TELETRUST  
Deutschland e.V. sowie Mitglied des Vorstandes des  
T 7 e.V. i.G., dem Zusammenschluss der deutschen  
Trustcenter-Betreiber*

*Mitglied des Vorstandes des TelekomForum e.V., dem Ge-  
schäftskundenbeirat der Deutschen Telekom AG*

*Mitglied des Vorstandes des deutschen wissenschaftlichen  
Institutes der Steuerberater (DWS) sowie Vorsitzender des  
Arbeitskreises „Digitale Signatur“ der Berufskammern der  
Steuerberater, Wirtschaftsprüfer, Rechtsanwälte, Notare  
und Patentanwälte, der sich für die Berücksichtigung der  
besonderen Bedürfnisse der verkammerten Berufe im elekt-  
ronischen Rechtsverkehr einsetzt.*

*Vizepräsident der Steuerberaterkammer Saarland  
sowie Mitglied des Redaktionsbeirates der Zeitschrift  
„Steuern und Vermögen“*



Michael Leistenschneider

Jahrgang 1953, Studium der  
Betriebswirtschaftslehre an der  
Universität des Saarlandes

Diplom-Kaufmann, Steuerberater

Mitglied des Vorstandes der  
DATEV eG Nürnberg

E-Mail: michael.leistenschneider@datev.de

Die digitale Kommunikationsform birgt enormes Rationalisierungspotenzial für Wirtschaft, Behörden und Bürger – diese These ist unbestritten. Um den elektronischen Kommunikationsweg allerdings wirklich geschäftsfähig zu machen, müssen zwei Grundsätze eingehalten werden:

1. Inhalte müssen sich vertrauenswürdig übermitteln lassen.
2. Elektronische Transaktionen müssen auch mit rechtsverbindlichem Charakter möglich sein.

Auf elektronischem Weg kann dies nur durch Verschlüsselung und die elektronische Signatur erreicht werden. Mit dem Ziel, die Vertrauenswürdigkeit von Informations- und Kommunikationstechnik in einer offenen Systemumgebung durch angewandte Kryptographie zu fördern, ist TELETRUST Deutschland e. V. bei seiner Gründung 1989 angetreten. Seitdem hat er in diesem Bereich eine Menge erreicht.

In Bezug auf die Rechtsverbindlichkeit ist ein elementares Anliegen von TELETRUST inzwischen realisiert: Im Jahr 2002 wurde die qualifizierte elektronische Signatur in Deutschland der eigenhändigen Unterschrift gleichgestellt. Das Dritte Gesetz zur Änderung der verwaltungsverfahrenrechtlichen Vorschriften beseitigte damals die letzte rechtliche Hürde für den Einsatz der elektronischen Signatur im Öffentlichen Recht; das Formanpassungsgesetz besiegelte selbiges im Privatrecht. Demnach könnten fast alle Verwaltungsakte in Deutschland nun auch in rein digitaler Form abgewickelt werden.

## Zielvorgabe: Interoperabilität

Neben dem rechtlichen Aspekt ist die Standardisierung der Infrastruktur die maßgebliche Voraussetzung für die Akzeptanz der elektronischen Signatur bei den Anwendern. Deshalb war die Interoperabilität von IT-Sicherheitsprodukten auch für die Arbeit des TELETRUST von Anfang an eines der wesentlichen Kernthemen. Hierfür hat TELETRUST – in Kooperation mit T7, der Vereinigung der Trustcenter-Betreiber – bestehende Spezifikationen für Verschlüsselung, elektronische Signaturen und Public-Key-Infrastrukturen zu einem gemeinsamen Interoperabilitätsstandard zusammengeführt und den maßgeblichen Standard ISIS-MTT geschaffen. Durch die Bereitstellung des ISIS-MTT-Testbeds im Herbst 2002 schuf TELETRUST auch die Voraussetzung dafür, dass die Interoperabilität von Signaturlösungen sich unproblematisch in der Praxis umsetzen lässt. Unternehmen verfügen damit bereits bei der Entwicklung über ein Hilfsmittel zur praktischen Erprobung der ISIS-MTT-Konformität ihrer Signaturprodukte. So

leistet TELETRUST einen aktiven Beitrag für die Entstehung neuer interoperabler Anwendungen für den Einsatz der elektronischen Signatur. Sukzessive passen die Anbieter von Komponenten zur Erstellung elektronischer Signaturen derzeit ihre Produkte an ISIS-MTT an. Damit die Hersteller, deren Anwendungen und Dienstleistungen die ISIS-MTT-Anforderungen bereits erfüllen, dies künftig auch belegen können, hat die ISIS-MTT-Initiative ein spezielles Siegel eingeführt, das die Konformität mit der Spezifikation bestätigt. Signaturkomponenten und Lösungen, die dieses Siegel tragen, erfüllen einerseits die maßgeblichen nationalen und internationalen Kriterien und sind andererseits untereinander interoperabel.

Ein weiterer Meilenstein auf dem Weg zur Interoperabilität ist die European Bridge-CA, deren Betreiber TELETRUST ist. Das Ziel, eine Brücke des Vertrauens zwischen verschiedenen PKIs weltweit herzustellen, verfolgt sie, indem sie eine allgemeine Plattform zur Verfügung stellt, die die teilnehmenden CAs auf eine sichere, aber einfache Weise verbindet. Grundlage dafür ist bestehende Sicherheitstechnologie. Die Anforderungen und technischen Vorbedingungen für eine Teilnahme sind bewusst minimal gehalten. Sie beschreiben gewissermaßen den kleinsten gemeinsamen Nenner, der eine sichere Kommunikation über organisatorische Grenzen hinweg erlaubt. So begegnet die European Bridge-CA dem Standardisierungsproblem auf organisatorischer Ebene – Vertrauenslücken zwischen unterschiedlichen PKIs werden dadurch pragmatisch überbrückt. Dabei zeigt sich die European Bridge offen gegenüber neuen Anbietern: Sobald ein weiterer Teilnehmer sich anschließt, können alle Mitglieder seiner PKI mit allen Mitgliedern der anderen Bridge-CA-Partner sicher kommunizieren.

Wie ernst die Bestrebungen des TELETRUST und seiner Mitstreiter für die vertrauenswürdige elektronische Kommunikation inzwischen genommen werden, zeigte sich im vergangenen Jahr unter anderem am Beispiel der Gründung des Signaturländnisses. Auch bei dieser Anfang April 2003 geschlossenen Public Private Partnership aus Vertretern der Wirtschaft und der Bundesregierung ist die Interoperabilität der Signatur-Infrastrukturen eines der formulierten Ziele. Die Erkenntnis, dass sie eine unbedingte Voraussetzung ist, damit sich die elektronische Signatur als effizientes Pendant zur händischen Unterschrift durchsetzen kann, hat sich also durchgesetzt. Das ist nicht zuletzt ein Resultat des unermüdlichen Bestrebens von TELETRUST. Das Signaturländnis soll für weitere Möglichkeiten zur Anwendung, Verbreitung und Einführung chipkartenbasierter elektronischer Signaturen sorgen. Für TELETRUST bedeutet diese Initiative eine Unterstützung in seinen Bemühungen.

## Arbeit geht nicht aus

Nach 15 Jahren Bestehen kann der TELETRUST Deutschland e.V. also ein durchaus positives Fazit ziehen. Erfolgreich ist der Verein gerade durch seinen interdisziplinären Ansatz, der Vertreter aus der Wissenschaft, von Herstellern, Anwendern und Behörden

zusammenbringt und so politische und wirtschaftliche Unabhängigkeit garantiert. Kombiniert mit der technischen Kompetenz der unterschiedlichsten Hersteller von Sicherheitslösungen macht diese Mischung TELETRUST zu einem maßgeblichen Gremium, dessen Know-how in die Entwicklung von Anwendungen einfließt. Auch wenn dabei bereits beachtliche Erfolge erzielt wurden, wird die Arbeit für TELETRUST in absehbarer Zeit nicht ausgehen. Für die künftigen Aufgaben wird der Verein auch weiterhin eine Plattform sein, um wichtige Impulse für die Weiterentwicklung der vertrauenswürdigen Kommunikation zu liefern.

Denn trotz der erfreulichen Entwicklung bei der Standardisierung ist zu konstatieren, dass bei den verfügbaren Anwendungen für den Einsatz der elektronischen Signatur in Deutschland noch Nachholbedarf herrscht. Eine Bestandsaufnahme unter den Partnern des Signaturländnisses ergab, dass von ihnen derzeit insgesamt etwa 100 Anwendungen angeboten werden, die eine elektronische Signatur voraussetzen. Zu den wichtigsten gehören Behördengänge, das „Virtuelle Rathaus“, die elektronische Einreichung von Mahnbescheiden, die elektronische Abwicklung der Verfahrenskorrespondenz am Bundesgerichtshof, die elektronische Patentanmeldung beim Deutschen Patent- und Markenamt, die elektronische Klageeinreichung bei Finanzgerichten, die elektronische Steuererklärung (ELSTER), sowie die Abfrage von Steuer- und Rentenkonten.

## Massenanwendungen fehlen

Die meisten dieser Anwendungen bringen in erster Linie fest definierten Gruppen einen großen Nutzen, wie beispielsweise Rechtsanwälten oder Steuerberatern. Diese Berufsgruppen setzen auch heute schon elektronische Signaturen in größerem Maßstab ein. Denn auf Grund der berufsständischen Verschwiegenheitspflicht sind Verschlüsselung und die digitale Unterschrift für sie wichtig beim elektronischen Datenaustausch. Für diese Zielgruppen war der Nutzen daher im Vorfeld klar abzustecken, eine hohe Akzeptanz der neuen Verfahren stand also zu erwarten. Die Aktivitäten des Signaturländnisses, aber auch die in Planung befindlichen Kartenprojekte der Bundesregierung lassen hoffen, dass sich im Bereich breitenwirksamer Anwendungen in absehbarer Zeit eine Menge tun wird. Denn im Rahmen dieser Projekte wird die elektronische Signatur über kurz oder lang in die Breite gebracht werden. Damit stünde dann eine große Anzahl potenzieller Nutzer zur Verfügung, die Anbieter wiederum zur Schaffung neuer Anwendungen ermuntern würde.

TELETRUST wird dabei wie in der Vergangenheit mit Rat und Tat zur Seite stehen und technische Hilfestellung geben. Dazu werden auch künftig in den interdisziplinären Arbeitsgruppen des Vereins Vorschläge und Erfahrungen von Experten zusammengeführt und in Berichte, Ergebnisdokumente, Empfehlungen und Dienstleistungen umgesetzt, die maßgeblich zur Weiterentwicklung der vertrauenswürdigen elektronischen Kommunikation beitragen.

# TELETRUST als Integrationsplattform für vertrauenswürdige Lösungen

Jürgen Sembritzki

*Vorstandsmitglied des TELETRUST Deutschland e.V.  
Obmann des DIN NAMed Fachbereiches G „Medizinische Informatik“  
Zweiter Vorsitzender von CEN TC 251 „Health Informatics“.  
Leiter der ISO 215 „Health Informatics“ Working Group 5 „Health Cards“*

*Mitglied verschiedener europäischer Normungsgremien (CEN TC 251 „Health Informatics“ WG III „Safety, Security and Quality“, ISO TC 215 „Health Informatics“ WG 4 „Security“).  
Mitglied im Steering Committee der CEN/ISSS eHealth Focus Group*

*Mitglied (Projektleiter) in ehemaligen Europäischen Projekten wie CARDLINK, DIABCARD und NETLINK  
bis Ende 2002 Leiter des Trailblazer 11 „Health care“ der eEurope-Initiative 2002/eEuropeSmartcards  
bis Mitte 2001 Leiter der TELETRUST-AG „Medizinische Anwendungen einer vertrauenswürdigen Informationstechnik“  
bis Mitte 2000 Projektleiter zur bundesweiten Einführung des Elektronischen Arztausweises*



Dipl.-Inform.  
Jürgen Sembritzki

1983-2000 Mitarbeiter des Zentralinstituts für die kassenärztliche Versorgung (ZI), dort ab 1992 Leiter der Abt. Informatik und der EDV-Beratungsstelle  
ab 2000 beim Zentrum für Telematik im Gesundheitswesen (ZTG),  
dort seit 2001 Geschäftsführer

E-Mail: j.sembritzki@ztg-nrw.de

Der vom TELETRUST-Verein von Beginn an als äußerst wichtig erachtete Integrationsaspekt lässt sich sehr gut am Wirken im Gesundheitssektor aufzeigen. Das Gesundheitswesen mit seinen vielfältigen Einrichtungen und Kommunikationsbeziehungen wird von jeher als ein wichtiger Markt für die Industrie gesehen. Insbesondere der Aspekt der sicheren Kommunikation aller im Gesundheitswesen Tätigen hat hier eine besondere Bedeutung, werden doch in vielen Fällen sensible Patientendaten bewegt.

TELETRUST hat dies rechtzeitig erkannt und bereits im Jahr 1995 eine eigene Arbeitsgruppe „Medizinische Anwendung einer vertrauenswürdigen Informationstechnik“ gegründet. Diese Gruppe besteht bis heute. Neben Vertretern der Industrie, wie beispielsweise Kartenherstellern, Netzprovidern, Anbietern von Arztpraxissystemen sowie Krankenhausinformationssystemen etc., bietet sie vor allem auch Vertretern der Körperschaften und im Gesundheitswesen angesiedelten Institutionen, wie beispielsweise der Bundesvereinigung Deutscher Apothekerverbände (ABDA), den Kassenärztlichen und Kassenzahnärztlichen Vereinigungen, den Ärztekammern etc. ein kompetentes Forum und vereint somit eine Vielzahl der maßgeblichen „Player“ des Gesundheitssektors.

Eine der ersten bemerkenswerten Aktivitäten dieser Arbeitsgruppe war die Herausgabe des so genannten Kryptoreports im Jahre 1998, der über lange Zeit unzweifelhaft der „Bestseller“ des TELETRUST war und über das Gesundheitswesen hinaus wirkte. Darüber hinaus beschäftigt man sich über die Jahre in besonderer Weise mit sämtlichen Konzepten und Applikationen des Gesundheitswesens, die in irgendeiner Weise den Kommunikationsaspekt und den Schutz von Daten beinhalten. So haben die Vertreter dieser Gruppe insbesondere die seit 1999 geplante Einführung einer Health-Professional-Card mit ihren Anregungen und Beiträgen kritisch begleitet, mit gestaltet und in Form eines englischsprachigen Informationsblattes aus TTT-Sicht bekannt gemacht.

Da das Gesundheitswesen durch seine Struktur zwar einige Besonderheiten aufweist, ansonsten jedoch sich hinsichtlich der benötigten Sicherheitsstandards nicht unbedingt von anderen Bereichen wesentlich unterscheidet, wurde auch immer „die Vernetzung“ zu anderen Gruppen innerhalb und außerhalb des TELETRUST-Vereins gepflegt und vielfach auch durch personelle Besetzungen sichergestellt. Beispielhaft genannt seien hier die Nutzung biometrischer Identifikationsmerkmale im Gesundheitswesen, die Möglichkeit von Multiapplikationskarten oder die Adaption ganzer Konzepte aus anderen Domänen. Ein ganz herausragendes Merkmal ist sicherlich auch der ständige und konstruktive Dialog mit dem Datenschutz, um rechtzeitig Machbarkeit und Akzeptanz von Lösungen abklären zu können.

Der *TELETRUST*-Verein mit seinen Arbeitsgruppen ist darüber hinaus auch ein viel genutztes Forum verschiedenster Projektträger und der Industrie, ihre Konzepte einer vertrauenswürdigen Kommunikation mit Experten und Entscheidern intensiv bereits im Vorfeld oder auch begleitend zu diskutieren. Es ist sicher nicht vermessen, festzustellen, dass viele heute im Einsatz befindliche Applikationen aus diesem Kreis entscheidende Impulse erhalten haben.

Als aktuelles Beispiel ist die Auseinandersetzung vornehmlich mit den geplanten Neuerungen, wie sie im GKV-Modernisierungsgesetz (GMG) festgelegt worden sind, zu nennen. Dies betrifft insbesondere die Einführung einer neuen elektronischen Gesundheitskarte (eGK) sowie den dazugehörigen Heilberufsausweis und deren Zusammenspiel hinsichtlich der Zugriffsmöglichkeiten auf die gespeicherten Daten des einzelnen Bürgers. In diesem Zusammenhang wurde bspw. eine Roadmap erarbeitet und den Verantwortlichen seitens *TELETRUST* zur Verfügung gestellt, um rechtzeitig auf mögliche kritische Pfade aufmerksam zu machen. Gerade dieses Projekt, von der Bundesregierung unter dem

Titel *BIT4health* eingeführt, steht für ein hohes Maß an Integrationsfähigkeit, müssen doch Interessen des Gesetzgebers mit denen der Selbstverwaltung, der Industrie, der Wissenschaft und nicht zuletzt mit dem informationellen Selbstbestimmungsrecht des Bürgers in Einklang gebracht werden und in eine von Allen akzeptierte und praktikable Lösung umgesetzt werden. Diese Aufgabe wird u.a. durch *TELETRUST* verantwortlich wahrgenommen. Und hierin spiegeln sich auch im Wesentlichen das Selbstverständnis und die Funktion des Vereins und seiner Arbeitsgruppen wider, sich mit neuen Konzepten und Technologien rechtzeitig auseinanderzusetzen, sie kritisch zu bewerten und die Entscheider sowohl auf industrieller als auch auf ministerieller Seite entweder zu bestärken oder, falls notwendig, rechtzeitig kritische Aspekte sowie gegebenenfalls Handlungsoptionen aufzuzeigen.

In diesem Sinne wird *TELETRUST* auch weiterhin die Einführung einer Telematik-Rahmenarchitektur und der dazu gehörigen Sicherheitsinfrastruktur im Gesundheitswesen und anderen Sektoren kritisch über die nächsten Jahre begleiten und allen Akteuren eine funktionsfähige und konstruktive Integrationsplattform für vertrauenswürdige Lösungen bieten.

# TELETRUST als Brücke zwischen Forschung und Markt

Claudia Eckert

*Vorstandsmitglied des TELETRUST Deutschland e.V.*

*IT-Sicherheit von Basistechnologie über die Middleware  
und (mobilen) Netze bis in die Anwendungen*

*Networking*

*Brückenfunktionen:*

*Leiterin des Fraunhofer Institutes für Sichere Teleko-  
operation, Darmstadt*

*Vorstandsmitglied des CAST e.V.*

*Mitglieder der Leitung des Darmstädter Zentrums für  
IT-Sicherheit (DZI)*

*Mitglied des Verwaltungsrats des Deutschen For-  
schungsnetzes (DFN)*

Wachstumsmotoren der Wirtschaft sind innovative Technologien und Anwendungen, die Arbeitsabläufe verbessern, neue Anwendungsfelder erschließen und die Arbeits- und Lebensqualität verbessern. Die Sicherheitsforschung an Universitäten und außeruniversitären Forschungseinrichtungen wie z.B. den Fraunhofer-Instituten ist darauf ausgerichtet, neue Methoden, Konzepte und Technologien zu entwickeln. Hierzu gehört auch, sie prototypisch zu implementieren, um auf diese Weise einen Technologietransfer zwischen Forschung und Industrie zu ermöglichen. Von der ersten innovativen Idee über eine prototypische Realisierung einer gewünschten System-Lösung bis zur Entwicklung eines vermarktungsfähigen Produktes ist es jedoch ein weiter Weg. Der TELETRUST-Verein hat hierbei eine wesentliche Brückenfunktion. Neben der Unterstützung des Technologietransfers, so dass vorhandenes Know-how in Unternehmen nutzbar gemacht werden kann, gehört es auch zu den Aufgaben von TELETRUST, durch Studien und Projekte eine Markteinführung einer neuen Technologie vorzubereiten bzw. zu unterstützen. Auf diese Weise wirkt TELETRUST als Wegbereiter für die Einführung anwendungsbezogener neuer Technologien. Als Beispiele sind hier das ISIS-MTT-Projekt oder auch die European Bridge-CA zu nennen. Gleichzeitig wirkt TELETRUST als Vermittler zwischen Anwendern, der Industrie und der Forschung, so dass Innovationen von Unternehmen aufgegriffen und zu Produkten veredelt werden können, die den Bedürfnissen der Anwender entsprechen.

Sicherheit in der Informationsgesellschaft ist ein komplexes Problem, dessen Lösungen technische, organisatorische und gesetzgeberische Aspekte zu berücksichtigen haben. Sicherheit ist ein Gebiet, auf dem es keine optimalen Lösungen gibt. Bei jedem denkbaren Lösungsansatz muss man die richtige Balance zwischen Nutzen und Risiken und sich entgegenstehenden Anforderungen finden:

- Der Aufwand für die Sicherheit darf der Wirtschaftlichkeit des Systems nicht im Wege stehen.
- Die Anforderung der sicheren Identifizierung von Personen kann im Widerspruch zum Schutz der Privatsphäre und des Datenschutzes stehen.
- Die Sicherheitsfunktionen sollen mißbräuchliche Benutzung der Systeme möglichst ausschließen, sollen allerdings gewünschte Anwendungen nicht verhindern oder erschweren.
- Sicherheitsfunktionen sollen im besten Fall vom Benutzer gar nicht bemerkt werden, aber gegebenenfalls Willensakte nachvollziehbar machen.
- Sicherheitsfunktionen sollen Systeme nicht isolieren, sondern vielmehr zu offenen und interoperablen Systemen führen,
- Sicherheitsfunktionen sollen zu den organisatorischen Abläufen passen und skalierbar sein.



Prof. Dr. habil. Claudia Eckert

Nach dem Studium der Informatik in Bonn promovierte Claudia Eckert 1993 an der TU München und habilitierte sich dort 1999 für das Fach Informatik. Sie forschte und lehrte in den Bereichen Betriebssysteme, Rechnernetze und schwerpunktmäßig im Bereich der Informationssicherheit an den Universitäten in München, Kiel

und Bremen

Prof. Eckert ist Leiterin des Fraunhofer Instituts für Sichere Telekooperation und Inhaberin des Lehrstuhls für Sicherheit in der Informationstechnik an der TU Darmstadt

E-Mail: Claudia.Eckert@sit.fraunhofer.de

Die Forschung liefert hierzu technologische Lösungen. Um ganzheitliche Sicherheitslösungen für marktfähige Produkte in der ICT-Branche zu entwickeln, ist häufig eine interdisziplinäre Zusammenarbeit notwendig. Die Umsetzung in den Markt ist wegen der oben beschriebenen Bedingungen schwierig und erfordert oft Erprobungsphasen mit den Anwendern. In diesem Prozess zwischen Forschung, Herstellern und Anwendern spielt TELETRUST eine wichtige Rolle.

Ein Blick in die Vergangenheit zeigt, dass TELETRUST von Anfang an die Brückenfunktion zwischen Forschung und Anwendungen wahrgenommen hat. So resultierte die Gründung von TELETRUST aus einem europäischen Forschungsprojekt Mitte der achtziger Jahre, in dem mehrere europäische Forschungseinrichtungen und Anwender Online-Recherchen in kommerziellen Datenbanken mit anschließender Online-Bezahlung mit Hilfe digitaler Signaturen auf der Basis des RSA-Verfahrens in einem Feldversuch erprobten. Die Technologie wurde in den beteiligten Forschungseinrichtungen, wie dem Fraunhofer-Institut SIT (seinerzeit GMD) entwickelt. Mit TELETRUST wurde ein Netzwerk geschaffen, das es Industrie, Forschung und den Anwendern ermöglichte, diese neuen Technologien weiterzuentwickeln und in den Markt einzuführen. Der Technologietransfer aus den Forschungseinrichtungen in die Mitgliedsfirmen der beteiligten Industriepartner spielte dabei stets eine wichtige Rolle. So wurde beispielsweise auf dem TELETRUST-Stand einer großen Messe interoperable „Sichere E-Mail“ auf der Basis von S/MIME von fünf deutschen Herstellern vorgeführt. Das Projekt wurde von TELETRUST koordiniert und teilweise finanziert. Das dafür notwendige Security-Toolkit wurde in der Forschung entwickelt und den Herstellern zur Verfügung gestellt. Mittlerweile gehören diese Produkte zum Standard-Portfolio der meisten Hersteller. Dies ist ein gutes Beispiel für die Brückenfunktion von TELETRUST, ohne die ein solcher Transfer von Forschungsergebnissen in den Markt nicht so ohne weiteres möglich gewesen wäre.

Eine weitere wichtige Aufgabe ist die Verankerung von F&E-Ergebnissen in der Standardisierung. TELETRUST nimmt Entwicklungen aus der Forschung und Anforderungen der Anwenderseite auf, entwickelt in Projekten und in Arbeitsgruppen eigene Spezifikationen bzw. entwickelt bestehende Standards weiter, wie z.B. ISIS-MTT für den PKI-Bereich, und trägt dafür Sorge, dass diese Spezifikationen auch in andere relevante Normungsbereiche wie z.B. ETSI oder IETF eingebracht werden. Durch diese Arbeit von TELETRUST wird im Vorfeld eine breite Akzeptanz seitens der beteiligten Hersteller und Anwendergruppen erreicht.

Ein weiterer wichtiger Bereich, der die Brückenfunktion von TELETRUST charakterisiert, ist die neutrale Prüfung von Technologiekomponenten hinsichtlich ihrer Standardkonformität auch bei Sicherheitsfunktionalitäten und ihren Fähigkeiten zur Interoperabilität. So hat TELETRUST z.B. für den Bereich PKI in Zusammenarbeit mit Forschungseinrichtungen im Rahmen des Projektes ISIS-MTT ein Prüfkonzept und eine Testumgebung entwickelt, die allen Herstellern zur Verfügung steht. Nach erfolgreichem

Bestehen dieser Tests vergibt das ISIS-MTT-Board ein Prüfzertifikat (ISIS-MTT-Siegel) für das getestete Produkt. Durch diese Aktivitäten wird die Markteinführung von Sicherheitstechnologien unterstützt und Vertrauen bei den Anwendern geschaffen.

Das frühzeitige Aufgreifen von ökonomisch und gesellschaftspolitisch wichtigen Fragestellungen und deren an die Anforderungen der TELETRUST-Mitglieder angepasste Weiterentwicklung sowie Erprobung wird auch in Zukunft eine zentrale Aufgabe von TELETRUST sein. Auf diese Weise erhalten die TELETRUST-Mitglieder einen wichtigen Marktvorsprung, da sie innovative Technologien, deren Grundlagen im Rahmen von nationalen und internationalen Forschungsprogrammen entwickelt werden, in praxisnahen Feldversuchen erproben und mit dem Know-how der beteiligten Forschungseinrichtungen auf einem hohen qualitativen Niveau weiterentwickeln können.

Zu den zukunftssträchtigen Themen, die in naher Zukunft in enger Zusammenarbeit mit universitärer und außeruniversitärer Forschung durch TELETRUST zu bearbeiten sein werden, gehören insbesondere die Themenbereiche des Trusted Computing und des mobilen sicheren Arbeitens (Mobile Computing). Beide Themenkomplexe weisen Fragestellungen auf, die über die reinen Technologie-Fragestellungen weit hinausgehen und neben juristischen Fragen auch betriebswirtschaftliche, organisatorische sowie gesellschaftspolitische Fragen aufwerfen. Die interdisziplinäre Bearbeitung komplexer und auch für die Gesellschaft wichtiger Probleme ist ein Charakteristikum der Integrations- und Brückenfunktion des TELETRUST-Vereins.

Betrachtet man als Beispiel den Themenkomplex des Mobile Computing: Bereits heute existieren in Forschungseinrichtungen einsatzfähige Technologien für ein mobiles sicheres (Zusammen-)Arbeiten. Jedoch sind die Forschungs-Prototypen häufig nicht ausreichend auf die Bedürfnisse von Anwendern bzw. Anwendergruppen abgestimmt. Obwohl dem Marktsegment des Mobile Computing von Analysten bereits seit einiger Zeit ein großes Wachstum vorausgesagt wird, scheitert der breitflächige Einsatz mobiler Lösungen heute noch daran, dass die Forschungsergebnisse noch keinen geeigneten Eingang in die Praxis gefunden haben und die existierenden Praxis-Lösungen nicht interoperabel sind. Hier setzen die Arbeiten von TELETRUST auf diesem Gebiet an, um in bewährter Weise Synergien zwischen Forschung und Anwendung zu erzeugen.

Neben dem Technologie-Transfer wird in Zukunft in zunehmendem Maß auch der Know-How-Transfer für die beteiligten Partner im TELETRUST-Netzwerk einen Mehrwert darstellen. Angesichts der rasanten technologischen Entwicklungen sind Anwender und mittelständige Unternehmen kaum in der Lage, sich umfassend über den aktuellen Stand der angewandten Forschung im Bereich der Sicherheitstechnologie in ihrem jeweiligen Geschäftsfeld auf dem Laufenden zu halten. TELETRUST wird hier auch in Zukunft als wichtiger Vermittler zwischen den verschiedenen Interessensgruppen dienen.

# Was hat *TELETRUST* bewirkt

Die im Verein entwickelten Konzepte beruhen auf internationalen Standards, ermöglichen die Entwicklung interoperabler Anwendungen und bieten angemessene Sicherheit.



# Die Stunde der Wahrheit rückt näher

Sichere und wirtschaftliche Geschäftsanwendungen

Helmut Reimer

*Mitglied des ISIS-MTT Boards,  
Mitglied des EB-CA Boards,  
Mitglied des Programmkomitees und des Steeringkomitees  
der ISSE*

*Mitherausgeber der Fachzeitschrift „Datenschutz und  
Datensicherheit – DuD“ und  
Verfasser vieler Publikationen im Feld der Informations-  
und Kommunikationssicherheit*

## Wirtschaftlich tragfähige PKI-Anwendungen

Unter dem Dach von TELETRUST bemühen sich Experten aus rund 90 Mitgliedsunternehmen seit 15 Jahren um die Erschließung des Potentials der asymmetrischen Kryptographie für verbindliche und vertrauenswürdige elektronische Geschäftsprozesse. Keine Metapher ist dabei so oft ins Feld geführt worden wie die von ‚Henne und Ei‘, um zu begründen, warum sich das Wissen um Sicherheit und Infrastrukturen so schwer in Anwendungen einbauen lässt. Tatsächlich hat es sehr lange gedauert, bis endgültig klar wurde, dass die Vision, der Geschäftsprozess müsse sich einer Sicherheitsarchitektur unterordnen, nicht erfolgreich umgesetzt werden kann. Das Gegenteil ist richtig: So wie die gesamte IT-Landschaft müssen auch die Sicherheitslösungen und –dienste den Geschäftsprozessen dienen. Nur so werden sie Teilleistungen für den Geschäftszweck und Bestandteil von Investitionsplänen. Erfreulicherweise können wir diesen Wandel nun auch in den großen Projekten der öffentlichen Hand in Deutschland zur Kenntnis nehmen.

Im ‚Aktionsprogramm Informationsgesellschaft 2006‘ der Bundesregierung werden im Zusammenhang mit einem ‚Masterplan zum Bürokratieabbau‘ nunmehr Ziele vorgegeben, die markante Herausforderungen an die Gestaltung vertrauenswürdiger elektronischer Geschäftsprozesse und den Ausbau von Sicherheitsinfrastrukturen und –Services darstellen. Dabei geht es nicht mehr um abstrakte Sicherheit oder den Beweiswert von Signaturen, sondern um den Aufbau von komplexen Anwendungen wie z.B. das elektronische Rezept in Verbindung mit der Gesundheitskarte oder die elektronische Bereitstellung der Arbeits- und Entgeltbescheinigungen für alle Arbeitnehmer als eine der JobCard-Fachanwendungen. Die Einsparpotentiale dieser Anwendungen sind jeweils kalkuliert, und ihre IT-Architekturen befinden sich teilweise in der Erprobung. Geschäftsmodelle für die Sicherheitsinfrastruktur und die Herausgabe von ca. 80 Mio. Gesundheitskarten ab 2006 werden heftig diskutiert.

Einen Durchbruch gibt es auch bei der Bestimmung der erforderlichen Aufwendungen. So wird der Aufbau der Telematik-Infrastrukturen des Gesundheitswesens, mit der die Rationalisierungseffekte und elektronischen Anwendungen des Gesundheits-Modernisierungsgesetzes vertrauenswürdiger realisiert werden können, ca. 1,6 Mrd. EURO kosten. Diese Mittel werden von den Krankenkassen (ca. 1,0 Mrd. EURO) und den medizinischen Berufsverbänden (ca. 600 Mio. EURO) für das Projekt bereitgestellt. Letztendlich ist gerade diese Tatsache der Durchbruch, weil die Entscheidung zum Einsatz der Mittel nur auf Grundlage der



Prof. Dr.-Ing.  
Helmut Reimer

1964 Graduiert als Dr. Ing.  
seit 1971 Professor für Mikro-  
elektronik an der TU Ilmenau  
1980-1990 Leiter der Mikrochip-  
Entwicklung in einem Unterneh-  
men.  
seit 1992 Geschäftsführer von  
TELETRUST Deutschland e.V.

E-Mail: [helmut.reimer@teletrust.de](mailto:helmut.reimer@teletrust.de)

Überzeugung zum Nutzens der elektronischen Unterstützung des Gesundheitswesens erfolgen konnte.

Aus Sicht von TELETRUST ist weiter von Bedeutung, dass die Implementierung von komplexen elektronischen Lösungen inzwischen als Aufgabe angesehen wird, die effektiv nur gelöst werden kann, wenn einzelne Anwendungen stufenweise nacheinander verfügbar gemacht werden. Die TELETRUST-Gemeinschaft hat sich rechtzeitig darauf eingestellt, dafür robuste und migrationsfähige Sicherheitslösungen bereitzustellen und ihre Implementierung flexibel zu unterstützen.

## Infrastruktur und Interoperabilität

Der wirtschaftlich effiziente Betrieb von PKI-gestützten Geschäfts- oder Verwaltungsprozessen ist darauf angewiesen, dass standardgerechte Infrastrukturdienste verfügbar sind und in unterschiedlichen Anwendungsumgebungen gleichartig verwendet werden können. Gefragt sind robuste und leistungsfähige Lösungen, mit denen unterschiedliche technische und organisatorische Vorgaben erreichbar sind und die eine Optimierung der Geschäftsprozesse hinsichtlich ihrer Effektivität und ihres Sicherheitsbedarfs flexibel unterstützen. Auch über den Erfolg der Anwendung elektronischer Signaturen wird mit ihrer Integration in den Workflow der Geschäfts- oder Verwaltungsprozesse entschieden. Eine wichtige Voraussetzung für Investitionssicherheit bei Anwendern elektronischer Signaturen und bei Anbietern von Infrastrukturdiensten ist dem zu Folge die einheitliche Interpretation von Standards, mit der eine weitgehende Interoperabilität von PKI-gestützten Anwendungen erreicht werden kann. Diesem Ziel ist ISIS-MTT gewidmet, indem die universelle Nutzung der einsetzbaren kryptographischen Verfahren gebündelt unterstützt wird. Neben der elektronischen Signatur sind in elektronischen Geschäftsprozessen Verschlüsselungs- und Authentifizierungsverfahren erforderlich, da diese nicht nur dem Empfänger sondern auch dem Absender einer vertrauenswürdigen Kommunikation Nutzen bringen und somit alle Beteiligten ohne erhebliche zusätzliche Kosten zum Einsatz der Technologie motivieren.

Eine Basisfunktionalität in Unternehmensnetzen und PKI-Inseln ist stets die Authentifizierung. Sie ist Grundlage wesentlicher Kernanwendungen. Dabei muss sie aber nicht zwingend auf PKI-Zertifikaten beruhen sondern kann auch durch ‚Credentials‘ realisiert werden.

Eine besonders hochwertige Authentisierung ermöglicht die asymmetrische Kryptographie mit dem Konzept der digitalen Signatur. Sie erfolgt zertifikatsbasiert, benötigt also PKI-Services. In Unternehmensnetzen und PKI-Inseln ist ‚Single Sign On‘ eine Anwendung, die einen großen Sicherheits- und Komfortzuwachs für den Nutzer bietet und die Systemadministration deutlich vereinfacht.

Starke Authentisierungsmechanismen werden zunehmend und in den unterschiedlichsten Szenarien und Protokollen genutzt. Dadurch ist im Nutzerkreis von ISIS-MTT der Bedarf entstanden, Authentisierung als eigenständigen Bereich zu vereinheitlichen. Die Erweiterung von ISIS-MTT um ein Authentisierungsprofil trägt insbesondere auch den Migrationserfordernissen Rechnung.

## ISIS-MTT: Authentisierungsprofil

Der Bereich der elektronischen Signatur hat in ISIS-MTT inzwischen einen recht stabilen Stand erreicht. Mit der Erstellung der neuen Version 1.1 sind Anforderungen, die sich im praktischen Gebrauch ergeben haben, aufgenommen worden. Insbesondere wurden dabei auch Hindernisse ausgeräumt, die eine Nutzung von Zertifikaten für Authentisierungszwecke nach dem ursprünglichen Profil schwierig und in bestimmten Umgebungen sogar unmöglich machten.

Diese Bemühungen sind besonders wichtig vor dem Hintergrund, dass neben der elektronischen Signatur vor allem die Authentisierung als klassischer Nutzungsfall von Chipkarten in der letzten Zeit an Bedeutung gewonnen hat. Dabei werden einerseits Anwendungen neu entwickelt, andererseits sind aber inzwischen praktisch alle großen System-Plattformen für die Verwendung von Zertifikaten und oft auch Chipkarten ausgerüstet.

Daraus ist der zunehmende Bedarf entstanden, die Anforderungen von existierenden und neu zu entwickelnden Systemen speziell in Bezug auf die Authentisierung zu harmonisieren. Ohne andere Formen der Authentisierung ausschließen zu wollen, ist es das hauptsächliche Ziel von ISIS-MTT, eine einheitliche Arbeitsgrundlage in Bezug auf die zertifikatsbasierte Authentisierung zu schaffen:

- Zertifizierungsdiensteanbietern soll die Möglichkeit gegeben werden, ihre Zertifikate einheitlich so zu gestalten, dass sie in möglichst vielen Umgebungen zur Authentisierung genutzt werden können.
- Gleichzeitig sollen Anwendungsentwickler Klarheit darüber erhalten, welche Angaben in Authentisierungszertifikaten in welchen Umgebungen erwartet werden können und wie die Authentisierung in neuen Anwendungen entsprechend gestaltet werden kann.

Zu weiteren Zielen gehören:

- die Vereinheitlichung eines Zertifikatsprofils für Authentisierungszertifikate;
- die ‚Standardisierung‘ der Authentisierungsverfahren für Trustcenter-Dienste;
- die Identifikation von weiteren Authentisierungsanforderungen aus Anwendungszusammenhängen und Festlegung des Umgangs damit;
- die Beschreibung von Nutzungsszenarien, z.B. in Form von best practices

Wie im ISIS-MTT-Konzept üblich, soll auch das Authentisierungsprofil international ausgerichtet sein. Sollte es spezifische Anforderungen aus den deutschen Nutzerkreisen geben, werden diese in geeigneter Form berücksichtigt.

Statt mit dem Profil neue Protokolle, Spezifikationen oder Anforderungslisten zu erstellen, werden bestehende Anforderungen so weit wie möglich harmonisiert.

TELETRUST wird sein nationales und internationales Kompetenznetzwerk nutzen und das Authentisierungsprofil mit den Teilnehmern am Signaturlösungsprofil, den führenden Anbietern, den Arbeitsgruppen bei TELETRUST, insbesondere AG8 und AG9, dem BSI, der OSCI-Leitstelle, der ESI-Arbeitsgruppe bei ETSI und anderen europäischen Projekten abstimmen.

# Kommunikations- und Transaktionssicherheit

## Sicherheitsinfrastrukturen für offene Systeme

Fritz Bauspieß, Wolfgang Schneider

*Wolfgang Schneider ist  
Gründer der Secude GmbH,  
Leiter der TELETRUST-Arbeitsgruppe „ISIS-MTT“ und  
Mitglied im Steuerungsgremium zur PKI-Spezifikation  
„ISIS-MTT“*

*Fritz Bauspieß ist  
Gründer der Secorvo Security Consulting GmbH,  
Leiter der TELETRUST-Arbeitsgruppe „Public Key Infra-  
strukturen“ und Mitglied im Steuerungsgremium zur PKI-  
Spezifikation „ISIS-MTT“*



Dipl.-Math.  
Wolfgang Schneider

Leiter des Forschungsbereichs  
„Transaktions- und Dokumenten-  
sicherheit“ des Fraunhofer-  
Instituts SIT.

E-Mail: wolfgang.schneider@sit.fraunhofer.de



Dipl.-Inform.  
Fritz Bauspieß

Director Product Management  
Security Netweaver bei SAP

E-Mail: fritz.bauspiess@teletrust.de

Kommunikations- und Transaktionssicherheit erfordern das Zusammenwirken verschiedener technischer und organisatorischer Komponenten. Wir sprechen hier von Sicherheitsinfrastrukturen, die die Benutzung von Computern, von digitalen Inhalten und von Übertragungsnetzen schützen, wenn verschiedene Komponenten auf verschiedenen Systemen oder in verschiedenen Organisationen zusammenarbeiten müssen, um ein bestimmtes Ziel zu erreichen.

Wie müssen Sicherheitsinfrastrukturen ausgelegt werden, welche Sicherheitsfeatures werden in welcher Stärke gebraucht? Diese Fragen lassen sich nicht allgemein beantworten, obwohl in der Vergangenheit immer wieder versucht wurde, dies allein aus Sicherheitsüberlegungen hinsichtlich der technischen Komponenten heraus zu tun. Letztlich bestimmt sich die konkrete Ausgestaltung der Sicherheitsinfrastruktur aus dem Vergleich der Kosten, die im Schadenfalle entstehen können, mit den Kosten der Herstellung und des Betriebs der Sicherheitsinfrastruktur sowie der Gegenüberstellung der möglicherweise unterschiedlichen Interessen der Infrastrukturteilnehmer.

Diese Gegenüberstellung kann aber nur im Kontext der Anwendung, d.h. der Geschäftsprozesse und ihrer schutzwürdigen Bestandteile gemacht werden. Anders als bei der Sicherheitstechnik für den Flugzeug- oder Fahrzeugbau geht es hier in der Regel nicht um Menschenleben, sondern um eine reine Kostenabwägung, wie sie auch Versicherungen bei der Festlegung ihrer Prämienhöhen durchführen.

Die Kosten der Infrastruktur bestehen aus ihren Herstellungs- und ihren Einsatzkosten. Die Herstellungskosten sind oft deutlich geringer als die Einsatzkosten. Zu den Einsatzkosten gehören die Ausrollkosten, die erheblich sein können, wenn an einer großen Zahl von Arbeitsplätzen Soft- oder Hardwarekomponenten installiert oder Parameter eingestellt werden müssen. Was kostet es, einen Sicherheitsparameter (z.B. einen Root-Schlüssel) in einer Software zu ändern, die hundertausendfach ausgerollt ist?

Der größte Einzelposten bei den Einsatzkosten ist erfahrungsgemäß die Dienstleistung, die bereitgestellt werden muss, weil Schlüssel, Smartcards oder Passwörter verloren gehen, weil sich Benutzer falsch verhalten oder Dokumente nicht mehr entschlüsselt oder verifiziert werden können. Dies ist aber auch eine Problemzone, die im Widerspruch zu Sicherheitsanforderungen stehen kann. Aus Gründen der Sicherheit ist man bestrebt, die Wiedergewinnung von Schlüsseln und Nachrichten zu erschweren. Aus Gründen der praktischen Betriebsabläufe will man das so einfach wie möglich haben. Beim Design von Sicherheitsinfrastrukturen

ist es wichtig, den Wiederherstellungsfall von vornherein so einzubeziehen, dass er sich problemlos, möglichst automatisch operierend in die Betriebsabläufe bzw. die Geschäftsprozesse einfügen lässt.

Zu den Kosten, die oft nicht betrachtet werden oder die schwer bezifferbar sind, gehören auch indirekte Kosten, z.B. durch die Störung von bewährten Betriebsabläufen durch bestimmte Features der Sicherheitsinfrastruktur, durch zusätzlichen Arbeitsaufwand im täglichen Betrieb bei den Benutzern oder auch durch Umgehungsversuche von Benutzern um als unnötig und störend empfundene Sicherheitsmaßnahmen herum und den daraus entstehenden Zusatzaufwänden und Inkonsistenzen. Auch diese Faktoren sollten beim Design von Sicherheitsinfrastrukturen eine wichtige Rolle spielen.

Auf der anderen Seite kann die Bewertung der Kosten im möglichen Schadenfall je nach Anwendung sehr schwierig sein. Bei Massenphänomenen wie Viren und Spam kann man Schadenskosten und Kosten der Gegenmaßnahmen ganz gut abschätzen. Was kostet es aber, wenn eine digitale Signatur gefälscht oder ein Verzeichnisdienst kompromittiert wird? Man kann sich leicht vorstellen, dass die Kosten erheblich sein können. Allerdings ist solch eine unspezifische Vermutung wenig hilfreich für die Beantwortung der Frage, welchen Aufwand zur Vermeidung man betreiben soll. Der mögliche Einzelfall kann höchstens in Ausnahmefällen mit drohendem katastrophalen Schaden eine Entscheidungsgrundlage für Sicherheitsanforderungen sein. Der Schadenfall ist immer hypothetisch, und zur Abwägung von Schadenhöhen und Kosten der Gegenmaßnahmen operiert man in aller Regel mit Statistik, Wahrscheinlichkeit und Empirie.

Im Falle von digitalen Signaturen, beispielsweise, gibt es aber kein empirisches Material. In einem solchen Fall wäre die sinnvollste Vorgehensweise sicher die, Sicherheitsvorkehrungen schrittweise zu verbessern und im Erfahrungsfalle Sicherheitsziele zu verändern. Gerne und höchst intensiv wird hier diskutiert, welche potentiellen Schwachstellen es auf technischer oder organisatorischer Ebene prinzipiell geben kann. Aber auch hier gilt es, für den konkreten Einsatzfall eine geeignete Abwägung zwischen den drohenden Risiken – bestimmt durch die drohende Schadenshöhe und deren Eintrittswahrscheinlichkeit – einerseits und den dazu angemessenen Sicherheitsmaßnahmen andererseits zu finden. Die bestmögliche Sicherheit ist hier – wie in vielen anderen Fällen auch – nicht unbedingt die beste Lösung, weil wirtschaftlich dem Risikopotential möglicherweise nicht angemessen. Es gibt auch hier keine generell gültige Antwort, welche Sicherheitsmaßnahmen zu ergreifen sind, höchstens Empfehlungen für typische Klassen von Szenarien, wie sie beispielsweise im Signaturgesetz oder im Signaturlösungsadressiert werden.

Staatliche Initiativen oder Regulierungen spielen bei Sicherheitsinfrastrukturen natürlich auch eine große Rolle. Regulierungen können aber auch dazu führen, dass der Prozess der Risiko- und Kostenabwägung ausgeschaltet wird. „Das ist sowieso vorgeschrieben“ ersetzt dann das am Anwendungsfall oder Geschäftsprozess orientierte Entscheidungskriterium und kann sich so betriebs- und volkswirtschaftlich zu einem Kostentreiber entwickeln.

Problematisch ist auch, wenn einzelne Sicherheitsziele stark in den Vordergrund gedrängt werden und der Gesamtkontext damit

verloren geht. Als Beispiel sei hier das anonyme digitale Geld genannt. Die Bewahrung der Anonymität beim Bezahlen mit Geld ist sicherlich eine wichtige und den Verbrauchern zugute kommende Anforderung, die man an elektronische Substitute unseres Geldes stellen kann. Die technische Umsetzung ist allerdings anspruchsvoll und komplex. Es gab in den letzten Jahren eine Reihe von technisch sehr interessanten und durchaus ausgereiften Vorschlägen für anonymes digitales Geld. Realisiert wurde indes keiner dieser Vorschläge. Offensichtlich ist den Verbrauchern die Anonymität beim Bezahlen zwar wichtig, aber nicht so wichtig, als dass man die mit einer konsequenten Realisierung dieser Eigenschaft verbundenen Kosten tragen wollte. So ist anonymes digitales Geld keine Infrastruktur geworden, sondern ein Stück aus dem akademischen Schaufenster geblieben.

Neben Kostenabwägungen spielen Interessengegensätze eine wichtige Rolle für das Design von Sicherheitsinfrastrukturen. „Trusted Computing“ sei hier als Beispiel genannt. Was unter Trusted Computing zu verstehen ist, wird kontrovers diskutiert. Als kleinsten gemeinsamen Nenner kann man es als eine Sicherheitsinfrastruktur bezeichnen, die mit Hilfe von Soft- und Hardwarekomponenten den Gebrauch des PC „sicherer“ macht. In welchem Sinne ist aber hier „sicher“ gemeint? Die ursprüngliche Motivation, warum Hersteller sich zu dieser Initiative zusammengefunden haben, war „Digital Rights Management“. Content-Anbieter wollten eine Möglichkeit haben, die Benutzung der vertriebenen digitalen Inhalte stärker an bestimmte Plattformen zu binden und so eine unkontrollierte Weitergabe zu verhindern. Computer-, Software- und Chiphersteller wollten diese Plattformen anbieten. Nun ist der Schutz vor Raubkopien und vor der unkontrollierten Verbreitung von copyright-geschütztem Material sicher ein legitimes und angesichts der heutigen Situation ein notwendiges Ansinnen. Wie man dieses Ziel erreicht, ist eine andere Frage. Da gibt es nicht nur die Interessen der Content-Industrie, sondern auch die Interessen der Verbraucher, die die gekauften digitalen Güter in einer vernünftigen Weise nutzen wollen. Trusted Computing eröffnet viele Möglichkeiten, und nicht alle sind im Sinne der Endverbraucher. Konsequenz umgesetzt könnte es bedeuten, daß der Benutzer die Kontrolle über seinen Computer verliert und nur noch Softwarehersteller und Medienindustrie, die dann über die entsprechenden Codes verfügen, Änderungen an der PC-Software und den PC-Einstellungen vornehmen können. Dies könnte dann dazu führen, daß der PC nur noch Software ausführt, die er für legitim hält, nur noch Dateien bearbeitet, die er für legitim hält, Dateien automatisch löscht, die er nicht für legitim hält, ein automatisches Reporting durchführt bis hin zur automatischen Installation von Zensur- und Überwachungsmechanismen.

Dieses Beispiel zeigt, dass die technischen Möglichkeiten von Sicherheitsinfrastrukturen weitgehend sein können und dass eine ausgewogene Berücksichtigung der legitimen Interessen aller Beteiligten essentiell ist. Der Benutzer wünscht Komfort und Sicherheit, was Trusted Computing sicher bieten kann, aber er will nicht fremdbestimmt sein. Die Auflösung dieses inhärenten Gegensatzes ist sicherlich auch eine wichtige Aufgabe für TELETRUST, der sich mit der breiten Interessenlage und Unterschiedlichkeit seiner Mitglieder an der Debatte und der Entwicklung hinsichtlich Trusted Computing beteiligen kann.

# Services für eBusiness & eGovernment

## ISIS-MTT und European Bridge-CA

Arno Fiedler, Peter Steiert, Stephan Wappler

*Arno Fiedler leitet seit 2001 den Service ISIS-MTT und die AG Technik im Signaturbündnis. Er ist in ETSI aktiv.*

*Peter Steiert ist seit 2002 Leiter des Service EB-CA.*

*Stephan Wappler leitete für TTT die AG „Identitätsmanagement und PKI“ im Rahmen des GuT-Projekts. Er ist in der Open Group aktiv.*

## Einleitung

Elektronische Geschäftsprozesse müssen komplexen Anforderungen genügen. Viele resultieren aus geschäftsspezifischen Notwendigkeiten, etwa der Wahrung von angemessener Vertraulichkeit und Verbindlichkeit, andere aus dem notwendigen Transport von Daten über öffentlich zugängliche Netze und wieder andere aus der Verwendung unterschiedlicher Anwendungen bei den Geschäftspartnern. Erforderlich sind skalierbare und interoperable Mechanismen in den verwendeten Applikationen und genutzten Diensten zur Absicherung des Datentransports und der weiteren Datenverarbeitung im elektronischen Geschäftsprozess.

Durch den Einsatz von Diensten auf der Basis von Public-Key Infrastrukturen können verschiedene Teilprozesse wie z.B. Authentisierung, Autorisierung, Verschlüsselung und Elektronische Signatur einfach in Anwendungen implementiert werden. Mit der Absicht, als verbindlich betrachtete Interpretationen des Signaturgesetzes bei der Entwicklung von Produkte und Leistungen für Signaturfunktionalitäten zu berücksichtigen, sind in den vergangenen Jahren allerdings vorwiegend proprietäre Lösungen entstanden, die eine Vielzahl von spezifischen Eigenheiten aufweisen. Diese Lösungen entsprechen dann zwar den Anforderungen des (einen) spezifischen Anwendungsfalls bei einem Anwender A, sind jedoch i.d.R. nur bedingt erweiterbar (z.B. auf neue Geschäftspartner B, C, D, ...) und schwer auf andere Geschäftsprozesse übertragbar. Ursache ist die starke Einschränkung der Interoperabilität z.B. beim Einsatz von Zertifikaten und der darauf aufbauenden Teilprozesse.

Mit ISIS-MTT und der European Bridge-CA ist TELETRUST angetreten, bei PKI-gestützten elektronischen Geschäftsprozessen echte Hilfestellungen anzubieten.

## Die Herausforderung

Stand in den letzten Jahren bei den Unternehmen und in der öffentlichen Verwaltung die Entwicklung und Vereinfachung interner Geschäftsabläufe und Prozesse des elektronischen Geschäftsverkehrs im Vordergrund, wird jetzt an der Entwicklung und Umsetzung organisationsübergreifender Geschäftsprozesse gearbeitet. Getrieben wird dies sehr oft von dem Anliegen, große Kosteneinsparungen zu erzielen. Dem steht beispielsweise eine Vielzahl von Medienbrüchen entgegen, die den Daten- und Informationsaustausch unnötig verteuert. Hinzu kommt noch, dass organisationsübergreifende Geschäftsprozesse neue Geschäftsfelder entstehen lassen, die bisher nicht lukrativ sind und somit nicht oder nur teilweise bearbeitet werden.



Arno Fiedler

Inhaber der Nimbus Network Technologieberatung, Berlin.

E-Mail: arno.fiedler@teletrust.de



Peter Steiert

MitInhaber Netsys.IT GbR, Ilmenau,

E-Mail: peter.steiert@teletrust.de



Stephan Wappler

bei noventum consulting, Münster (ehemals Lynx-ctr) als Consultant im Bereich Netzwerke / IT-Sicherheit

E-Mail: stephan.wappler@noventum.de

Jedoch so schnell wie der Wunsch nach organisationsübergreifender Kommunikation geäußert wird, kann diese nicht realisiert werden. Es ist eine Vielzahl von Vorüberlegungen notwendig, und es müssen die entsprechenden technischen und organisatorischen Voraussetzungen geschaffen werden.

Wenn heute Daten auf dem konventionellen Weg (per Brief oder per Dokumentenlieferservice) ausgetauscht werden, ist sehr wohl der Transporteur bekannt. Der Empfänger ist auch in der Lage, Manipulationen zu erkennen (z.B. geöffneter Transportumschlag),

Im Internet sieht dies anders aus. Da werden die Transportwege bei jedem Transport dynamisch nach Verfügbarkeit über eine Vielzahl von Zwischenstationen bis zum Empfänger hin ausgewählt. Jede dieser Zwischenstationen bietet dabei potentiellen Dritten die Möglichkeit, einen Zugriff auf die übermittelten (unverschlüsselten) Daten zu erhalten oder diese zu manipulieren. Aus diesem Grund bedarf es der genauen Betrachtung der folgenden Sicherheitsaspekte:

- Vertraulichkeit
- Authentizitätsnachweis
- Manipulationssicherheit
- Rechtliche Verbindlichkeit

Die Vertraulichkeit kann durch den Einsatz von Verschlüsselung sichergestellt werden. Der Nachweis der Authentizität, die Manipulationssicherheit (Integrität) und rechtliche Verbindlichkeit der Daten lassen sich mit Hilfe von elektronischen Signaturen erreichen.

Als Basis für die o.g. elektronischen Signaturen am besten geeignet sind X.509-Zertifikate, die von einer eigenen Certification Authority (CA) zur Verfügung gestellt oder bei einem Zertifizierungsdiensteanbieter (ZDA) eingekauft werden. Sie stellen die vertrauenswürdige Verbindung von (personenbezogenen) Signaturwerkzeugen zur Identität dieser Person dar und sind so Voraussetzung für eine Vielzahl von Anwendungsszenarien wie z.B. HTTPS-Authentifikation, E-Mail-Verschlüsselung und -Signatur, VPN-Authentifikation und Code Signing.

Ebenso wichtig ist aber auch ein Identitätsmanagement in weiterem Sinne, das neben der Authentizität natürlicher Identitäten auch Sicherheit gegenüber juristischer Personen (Firmen und Behörden als handelnde und haftende Partner, Betreiber der Geschäftsprozesse) sowie technischer Komponenten (z.B. LDAP-Server) gewährleistet. Dies ist ein **Muss** angesichts der angestrebten Automatisierung von Teilprozesse des elektronischen Geschäftsverkehrs!

## Interoperabilitätsebenen

Ein störungsfreier Ablauf zwischen den einzelnen Anwendungen und Diensten für automatisierte Geschäftsprozesse kann nur durch den Einsatz interoperabler Protokolle und Schnittstellen sichergestellt werden. Bevor eine sichere organisationsübergreifende Kommunikation etabliert werden kann, sind dabei 4 Hürden zu überwinden:

- Organisationsübergreifend verbindende Infrastruktur  
Sie betrifft den vertrauenswürdigen Austausch von Wurzelzertifikaten, den Zugriff auf Verzeichnisdienste für den Bezug von Partner-X.509-Zertifikaten und die Möglichkeit der Validierung eingesetzter X.509-Zertifikate.

- Organisationsübergreifende Organisation der Geschäftsvoraussetzungen und –Abläufe  
Hierzu gehören die Festlegung des organisatorischen und rechtlichen Rahmens genauso wie die Prüfung der Policies der Kommunikationsteilnehmer.

- Einsatz interoperabler Hard- und Software

- Einsatz interoperabler Zertifikatsprofile

Derzeit existieren eine Vielzahl von Projekten und Initiativen, die Lösungen hierzu erarbeiten. TELETRUST Deutschland e.V. bietet seine Services „European Bridge-CA“ und „ISIS-MTT“ auf europäischer Ebene an.

## ISIS-MTT

Ziel von ISIS-MTT ist die Präzisierung der internationalen Standardisierung zu Aufbau und Einsatz von Public-Key-Infrastrukturen durch die Bereitstellung eines entsprechenden Standardisierungsprofils.

Aufgrund der langjährigen Erfahrungen von TELETRUST in diesem Umfeld hat sich im Frühjahr 2001 TELETRUST in Kooperation mit der Arbeitsgemeinschaft der Trustcenter (T7 e.V. i.G.) und mit Unterstützung durch das Bundesministerium für Wirtschaft und Arbeit (BMWA) das Ziel gesetzt, eine anwendungsorientierte, internationalen Erfordernissen entsprechende Interoperabilitäts-Spezifikation zu erstellen und am Markt durchzusetzen. Auf Grundlage vorhandener Erfahrungen bei der Spezifizierung von Diensten und Protokollen für ZDA (ISIS) und bei der Spezifizierung von Client-Funktionalitäten für E-Mail-Sicherheit (MailTrust – MTT) konnten die Experten gemeinsam bereits im November 2001 die erste Version von ISIS-MTT öffentlich bereitstellen.

Das Profil zeichnet sich durch folgende Eigenschaften aus:

- Integration bestehender internationaler Standards (S/MIME, PKIX, PKCS, X.509, ETSI, CEN ESI, XML);
- Berücksichtigung von Verfahren zur Sicherung des elektronischen Geschäftsverkehrs in verschiedenen Anwendungsfeldern auf Basis der Grundfunktionen Verschlüsselung, Authentifizierung und elektronische Signatur;
- Erweiterbarkeit um spezifische Anforderungen die des elektronischen Geschäftsverkehrs.

Von vornherein waren Investitionsschutz und Migrationsfähigkeit von Komponenten und Diensten wichtige Prämissen. ISIS-MTT wird bei Wahrung der Abwärtskompatibilität zu bereits verwendeten Zertifikatsformaten langfristig weiterentwickelt.

Erstmals werden mit ISIS-MTT die internationalen Standards für „Certification-Authority-Funktionalitäten“, Datenaustauschformate oder Clientfunktionalitäten im Zusammenhang dargestellt und, wo nötig, detailliert weiterspezifiziert, dass sie für die PKI-Anwendungsentwicklung hinreichend genaue Vorgaben machen. Da sich, zunächst in Deutschland, alle wesentlichen Entwickler, Anbieter und Nachfrager auf die ISIS-MTT-Spezifikation verständigt haben, werden nun tatsächlich herstellerübergreifend interoperable Produkte und Dienste für den Markt entwickelt und angeboten.

## Praktischer Nutzen: Testbed

Die in ISIS-MTT definierten Vorgaben zur Erreichung von Interoperabilität müssen hinsichtlich ihrer praktischen Umsetzung in zu entwickelnden Produkten und Diensten nachprüfbar sein.

Auf Basis eines detaillierten Testkonzeptes wurde ein ISIS-MTT-Testbed entwickelt, welches sich in bisher einzigartiger Weise durch einen umfassenden Funktionsumfang auszeichnet. Das Testbed wird zurzeit aktualisiert und in wesentlichen Teilen, insbesondere hinsichtlich der XML-Funktionalitäten erweitert. Aufgrund der Projektförderung durch das BMWA kann die Testbed-CD kostenfrei über die Geschäftsstelle von TELETRUST bezogen werden. Die ISIS-MTT-Konformität der in Anwendungen implementierten Verschlüsselungs-, Authentisierungs- und Signaturkomponenten kann sowohl für Produkte und Dienste verschiedener Anbieter als auch für solche, die kundenspezifischen Anforderungen genügen, getestet und ggf. nachgewiesen werden.

## Das ISIS-MTT-Siegel

Spezifikation und Testbed bilden die Grundlage für die Vergabe eines ISIS-MTT-Siegels durch das ISIS-MTT-Board, das Anwendern als Hilfestellung bei der Auswahl von Komponenten und Diensten für die organisationsübergreifende sichere Kommunikation dienen und somit Investitionsentscheidungen erleichtern kann.

Bei der Definition der Kriterien zur Vergabe dieses Siegels wurden bewusst bürokratischer Aufwand und praxisferne Testzeremonien vermieden. Das Testbed liefert durch die erstellten Prüfprotokolle pragmatisch und kostengünstig die Basis für eine Konformitätserklärung der Produkte- und Diensteanbieter. Unabhängige Prüfinstitute unterstützen bei der Durchführung der Konformitätstests. Eine Liste der ISIS-MTT-konformen Produkte und Dienstleistungen sowie die zugrunde liegenden Testergebnisse werden im Internet ([www.TELETRUST.de](http://www.TELETRUST.de)) veröffentlicht. Als Prüflabore haben sich bisher Securvo Security Consulting, TÜV-IT und T-Systems qualifiziert. Im Bereich der CA-Dienste haben Anbieter wie die Datev e.G., Entrust, Microsoft, und Nexus das Siegel bereits erworben.

Damit ist auf Basis einer öffentlich nachvollziehbaren Selbstregulierung ein flexibles und effektives System zur Sicherung von Interoperabilität geschaffen.

## ISIS-MTT Weiterentwicklung

ISIS-MTT ist von Anfang an migrationsfähig konzipiert worden. Derzeit ist eine Weiterentwicklung im Gang, die zwei Schwerpunkte hat:

- Schaffung eines Authentifizierungsprofils;
- Erweiterung des Testbeds um Tests, die das XML-Profil der ISIS-MTT-Spezifikation betreffen.

Mit der Beschreibung des Authentifizierungsprofils erfolgt in ISIS-MTT eine Harmonisierung bei der Nutzung von Chipkarten-Zertifikaten zum Berechtigungsmanagement bei Server-Systemen.

Die Nachführung des Testumfanges des Testbeds ist zum Erhalt seines praktischen Nutzens entsprechend der Weiterentwicklung von ISIS-MTT unumgänglich.

## Die European Bridge-CA – ein pragmatischer Ansatz

Als Lösungsansatz aus der Praxis stellt der TTT-Service „European Bridge-CA“ (EB-CA) eine Infrastruktur für Anwendungen zur Verfügung, die auf elektronischen Signaturen und Verschlüsselung aufbauen.

Dabei bietet die European Bridge-CA eine Lösung für die folgenden, derzeit noch verbreiteten Probleme:

- Vertrauensproblem:  
Kann der Partner-CA vertraut und wie kann der vertrauenswürdige Austausch der CA-Zertifikate realisiert werden?
- Anwendungsproblem:  
Unterstützen die eingesetzten Anwendungskomponenten X.509-Zertifikate?
- Verteilungsproblem:  
Wie kann der Zugriff auf Nutzerzertifikate kostengünstig realisiert werden?
- Validierungsproblem:  
Wie kann der aktuelle Zustand des Zertifikates des Kommunikationspartners geprüft werden?

## Lösung der Vertrauensproblematik

Eine wichtige Leistung der EB-CA ist, dem Anwender die Vertrauenswürdigkeit der einzelnen CAs zu bestätigen. Damit entfällt für den Anwender die Notwendigkeit, für jedes Trustcenter ein mehrere Seiten starkes Policy-Dokument studieren zu müssen, um Einblick in dessen Policies und somit dessen Vertrauenswürdigkeit zu erhalten.

Die EB-CA fordert von Ihren Mitgliedern die Einhaltung von Mindestanforderungen auf Basis einer Selbsterklärung. Dieser Ansatz führt zu einer wirksamen gegenseitigen Selbstkontrolle durch die Mitglieder. Die EB-CA bewertet die Policies der teilnehmenden CAs und nimmt damit dem Anwender diese komplexe und sehr zeitaufwändige Aufgabe ab. Hierdurch lassen sich die Kosten für die sichere organisationsübergreifende Kommunikation mit einer Vielzahl von Partnern erheblich reduzieren.

Die CA-Zertifikate aller beteiligten Organisationen werden durch die EB-CA erfasst und in einer signierten Liste zur Verfügung gestellt. Die Liste wird zur Gewährleistung ihrer Authentizität mit dem X.509-Zertifikat der EB-CA signiert.

Anwender, die in der Liste enthaltene Zertifikate importieren, müssen nur die Signatur der Liste prüfen, die enthaltenen Zertifikate extrahieren und in ihren Anwendungen speichern.

## Lösung der Anwendungsproblematik

Vorraussetzung für den Einsatz sicherer Kommunikation mit Hilfe von X.509 Zertifikaten ist, dass die Anwendungen dies unterstützen. Die EB-CA setzt aus diesem Grund die Durchführung eines Interoperabilitätstest voraus. Hierbei werden die eingesetzten Anwendungen gegen Referenzanwendungen geprüft, um eine objektive Aussage bezüglich der organisationsübergreifenden Interoperabilität treffen zu können. Es handelt sich dabei immer um einen anwendungsspezifischen Test, der mit den real eingesetzten Zertifikaten durchgeführt wird und die reale Nutzung der Anwendung nachbildet.

Um seine eigenen eingesetzten Anwendungen auf X.509-Tauglichkeit zu überprüfen, wird dem Anwender der vorherige Einsatz des ISIS-MTT-Testbeds bzw. bei Neuanschaffungen von Produkten auf das ISIS-MTT-Siegel zu achten, empfohlen. Mit diesen Maßnahmen kann eine Verbesserung der Qualität bei der Nutzung von Zertifikaten erzielt werden, was vor allem für weniger technikversierte Anwender von enormer Bedeutung ist.

## Lösung der Verteilungsproblematik

Die große Anzahl an Trustcentern und privaten Public Key Infrastrukturen ist schwer zu überblicken. Dies führt zu einem hohen Aufwand für den Zugriff auf und die Verteilung der bereitgestellten Zertifikate, für die in den Verzeichnisdiensten der einzelnen Trustcenter unterschiedlichste Informationen verfügbar gemacht sind (hierzu gehören z.B. Userzertifikate und Sperrlisten). Von einem Anwender kann nicht erwartet werden, dass er in seinem E-Mailclient eine Vielzahl von Verzeichnisdiensten zum Zugriff einrichtet.

Idealerweise möchte ein Nutzer nur einen zentralen Knoten in seinen Anwendungen konfigurieren, der die entsprechenden Daten bereitstellt. Als entsprechendes Vorbild ist hier die Funktionalität des Domain Name System (DNS) zu nennen.

Deshalb stellt die EB-CA einen zentralisierten LDAP-Verzeichnisdienst zur Verfügung. Durch Einbindung dieses Verzeichnisdienstes können Nutzer aus ihren Anwendungen Verschlüsselungszertifikate zu korrespondierenden Personen anfordern und Daten an diese Person verschlüsseln. Durch Nutzung dieses Dienstes entfällt für die Anwender die aufwändige Pflege einer Vielzahl von LDAP-Einträgen in den einzelnen Anwendungen, wodurch die Administrationskosten entscheidend gesenkt und Attraktivität und Akzeptanz der sicheren Kommunikation aus Sicht der Nutzer verbessert werden können.

## Lösung der Validierungsproblematik

Ähnlich wie bei der Verteilungsproblematik geht es bei eingehender signierter Daten um die Überprüfung eines X.509-Zertifikates auf dessen Gültigkeit zu einem bestimmten Zeitpunkt. Für den Anwender ist dies relativ kompliziert und es stehen derzeit zwei Alternativen zur Verfügung:

- Sperrlisten (CRLs)
- Online-Validierung mittels Online Certificate Status Protocol (OCSP)

Der Einsatz von CRLs und OCSP ermöglicht die Prüfung der Authentizität übertragener Daten. Dadurch lässt sich rekonstruieren, ob die Daten zu diesem Zeitpunkt gültig waren oder nicht, was möglicherweise zu rechtlichen Konsequenzen führen kann.

Sperrlisten bieten den Vorteil, dass sie offline bereitgestellt werden können, wohingegen der Einsatz von OCSP die Echtzeit-Überprüfung der Gültigkeit eines Zertifikats (gültig, gesperrt, abgelaufen) ermöglicht. Bei OCSP wird eine kurze Statusinformation zu einem Zertifikat angefordert und ausgewertet, was in kurzer Verarbeitungsdauer geleistet werden kann. Ein umfangreicher Download von Sperrlisten entfällt. Nachteilig ist, dass OCSP für den Validierungsvorgang immer eine Onlineverbindung zu einem OCSP-Server benötigt.

Die EB-CA stellt einen zentralen OCSP-Responder-Dienst zur Verfügung, der alle an der EB-CA teilnehmenden Trustcenter bzw. PKI's automatisiert abfragt. So können Anwendungen, die den EB-CA-OCSP-Responder integriert haben, aktuelle Statusinformationen zu einem Zertifikat mit Hilfe einer einzigen Abfrage durchführen und so eine verlässliche Echtzeit-Aussage über die transportierten Daten treffen.

## Internationale Abstimmung

Da ein wesentliches Kriterium für den Erfolg beider Services deren internationale Akzeptanz ist, wird ein konstruktiver Dialog mit internationalen Experten u.a. anlässlich von Standardisierungssitzungen relevanter Gremien geführt.

TELETRUST lud auch selbst internationale Experten ein, ihr Know How der erforderlichen Funktionalitäten einer PKI in die ISIS-MTT-Spezifikation und die Gestaltung des Betriebes der EB-CA einzubringen, um deren hohe Qualität sicherzustellen.

Da TELETRUST auch in Zukunft auf das Wissen von internationalen Experten zurückgreifen wird, kann verhindert werden, dass proprietäre, nur auf die Erfordernisse des deutschen Marktes zugeschnittene PKI-Lösungen entstehen. Dies ist im Hinblick auf ein zusammenwachsendes Europa von entscheidender Wichtigkeit und gleichzeitig Voraussetzung für die Harmonisierung und Zusammenarbeit mit anderen internationalen Aktivitäten und Initiativen (z.B. Federal Bridge-CA, IDA-BCA, BCA Japan, etc.).

## Zusammenfassung

Mit den Services EB-CA und ISIS-MTT engagiert sich TELETRUST für günstige Voraussetzungen zur organisationsübergreifenden, sicheren Kommunikation.

Die EB-CA bietet Organisationen hierzu eine gemeinsame organisatorische Plattform. Hauptsächlicher Fokus sind Investitionssicherheit und Standardkonformität. Durch die zusätzlichen Dienste kann der Aufwand bei der organisationsinternen und -übergreifenden Integration niedrig gehalten werden, ohne dabei an Vertrauenswürdigkeit zu verlieren.

Das Projekt „ISIS-MTT“ definiert ein Spezifikationsprofil zur Schaffung interoperabler PKI-Lösungen. Es wird vor allem Wert auf anerkannte Standards und bestehende Spezifikationen gelegt.

Gemeinsam ermöglichen beide Services den Anwendern und Teilnehmern eine langfristige Planung und somit Investitionssicherheit bei der Umsetzung sicherer organisationsübergreifender Kommunikation im Rahmen individueller elektronischer Geschäftsprozesse. Die zukünftig noch engere Verzahnung dieser Services unter dem Dach von TELETRUST schafft die Voraussetzung für eine konzertierte Initiative von international tätigen Unternehmen, Behörden und Institutionen für das Anbieten und Nutzen interoperabler Produkte und Dienstleistungen auf Basis pragmatischer Konzepte.

Dabei ist es nicht erforderlich, neue Standards oder technische Regulierungen auf Basis interpretationsbedürftiger Gesetze zu schaffen, sondern die bestehenden Normen- und Regelwerke im Einvernehmen mit den Markt bestimmenden Kräften zu harmonisieren und pragmatisch in Anwendungen mit breiter Nutzerakzeptanz einzusetzen.

# TELETRUST international

## ISSE, RSA, Workshops und Expertentreffen

Ulrike Schulte

*Zuständigkeiten und Kontakte:*

*ISSE, RSA und internationale Workshops  
internationales Expertennetzwerk aufgebaut über die ver-  
schiedenen Veranstaltungen  
eema, SiliconTrust, RSA Conferenc, EACC  
NIST, EC DG InfoSo, BSI, BMWA, BMI  
deutsche und internationale Fachpressekontakte  
Networking für TELETRUST Projekte*

### ISSE – erste Schritte auf den internationalen Markt

Bereits in der Gründungsgeschichte von TELETRUST ist die internationale Ausrichtung des Vereins sichtbar: Die 1983 gegründete Europäische Forschungsinitiative OASIS musste bis 1988 feststellen, dass die Aufgaben zur Schaffung geeigneter Rahmenbedingungen für Anwendungen in offenen Netzen nur mit einem sehr breiten, interdisziplinären Ansatz zu bewältigen sein würden. Da sie dies nicht leisten konnte, wurde die Initiative beendet. Statt dessen sollten in allen europäischen Staaten TELETRUST-Organisationen gegründet werden; von diesen besteht heute nur noch TELETRUST Deutschland e.V., dessen diesjährigem Jubiläum dieser Beitrag gewidmet ist.

Das Ziel von TELETRUST, die Vertrauenswürdigkeit von Anwendungen und Diensten der Informations- und Kommunikationstechnologie zu fördern, lässt sich effektiv nur in einem internationalen Rahmen umsetzen. Der elektronische Geschäftsverkehr macht an nationalen Grenzen nicht Halt und braucht Lösungen, die grenzüberschreitend Vertraulichkeit, Authentizität und Integrität der Daten, aber auch Interoperabilität und Gesetzeskonformität der verwandten Anwendungen, technischen Komponenten und Dienste sicherstellen. Dies ist ein riesiges Aufgabenfeld. Daher beschlossen 1998 die Mitglieder, das Wirken ihres gemeinnützigen Vereins TELETRUST noch stärker als bis dahin zu internationalisieren.

Eine erste Aktion war ein Vortrag des Geschäftsführers von TELETRUST, Prof. Reimer, anlässlich der RSA-Konferenz 1998 in San Francisco. Auf einem Treffen am Rande dieser Konferenz, an dem neben Prof. Reimer auch Dr. Sandl vom BMWA (damals BMWi) und Herr Eckert (damals Europäische Kommission) beteiligt waren, entstand die Idee, in Europa eine eigene IT-Sicherheitskonferenz zu gründen.

Herr Eckert rührte die Werbetrommel in Brüssel in der DG XIII „Information Society“ der Europäischen Kommission und konnte sie zur prinzipiellen Unterstützung des Aufbaus einer europäischen IT-Sicherheitskonferenz als Forum für den Austausch technischer, organisatorischer und rechtlicher Aspekte der Informationssicherheit gewinnen. Ähnliches tat Dr. Sandl im BMWA mit dem Schwerpunkt, die Schaffung eines Forums für die deutsche Kryptoindustrie zu unterstützen. Prof. Reimer erarbeitete Vorschläge, wie das Gesamtvorhaben gestartet und vorangetrieben werden könnte. Mit der EEMA (European Forum for eBusiness) fand sich ein Mitstreiter, der sich bereit erklärte, solch eine Konferenz gemeinsam mit TELETRUST auszurichten. TELETRUST, mit seiner inhaltlichen Kompetenz zum Thema, übernahm



Ulrike Schulte

Magister Kunstgeschichte, Englisch und Geschichte, RWTH Aachen  
Seit 1999 bei TELETRUST zuständig für die ISSE Konferenz.  
Seit 2003 Manager International Affairs.

E-Mail: [ulrike.schulte@teletrust.de](mailto:ulrike.schulte@teletrust.de)

die Gestaltung des Programms und den Vorsitz des Programmkomitees. Hierfür mussten zusätzliche personelle Ressourcen erschlossen werden. So wurde ich Anfang 1999 von TELETRUST als „Programm-Manager ISSE“ verpflichtet. Die Gesamtorganisation der Veranstaltung inkl. der finanziellen Verantwortlichkeit wurde in die Hände der EEMA gelegt.

Die erste ISSE (Information Security Solutions Europe) wurde 1999 in Berlin veranstaltet. Trotz der kurzen Vorlaufzeit fand die Veranstaltung großen internationalen Anklang: Über 500 Teilnehmer aus Europa und Übersee kamen in Berlin zusammen.

Auch die politische Unterstützung der ISSE war von Anfang an groß: In Berlin eröffnete Bundeswirtschaftsminister Werner Müller die erste Konferenz. Die Prominenz der Europäischen Kommission war durch ein persönliches Grußwort des Europäischen Kommissars (DG XIII) Erkki Liikanen gut vertreten.

Nach 1999 waren Barcelona, London, Paris und Wien als Europäische Weltmetropolen Anlaufpunkte dieser Konferenz. In diesem Jahr, das durch die EU-Erweiterung geprägt ist, findet die ISSE wieder in Berlin und damit in zentraler Lage für die neuen EU-Mitglieder aus Mittel- und Osteuropa statt.

Die ISSE hat sich in Europa als einer der wichtigen Events der Informationssicherheitsbranche etabliert. Über die Jahre hat sie regelmäßig ein starkes internationales Expertenpublikum angezogen. Thematisch ist die ISSE immer der gesamten Bandbreite der Informationssicherheit gewidmet – mit einem besonderen Augenmerk auf europäische Anforderungen und Entwicklungen. Man ging durchaus auf die Branchen-Hypes ein, verfolgte aber hauptsächlich die kontinuierliche Entwicklung von neusten Technologien zu wirklichen Anwendungen. Namhafte Referenten wie die Krypto-Gurus Bruce Schneier und Whitfield Diffie konnten zur ISSE gewonnen werden, und große Firmen etablierten sich als Sponsoren.

Für die deutsche Kryptobranche eröffnete die Konferenz ein gern angenommenes internationales Forum. Die Beteiligung deutscher Experten ist über die Jahre stark geblieben. Viele wichtige deutsche Initiativen wurden auf der ISSE einem internationalen Publikum präsentiert – insbesondere auch die European Bridge-CA, ISIS-MTT und die BioTrust-Ergebnisse, um nur einige TELETRUST Initiativen zu nennen.

Die ISSE bot und bietet sich für zusätzliche Aktionen und Veranstaltungen an: So organisierte TELETRUST Sonderveranstaltungen, wie z.B. International Legal Expert Meetings oder Workshops für Experten aus den baltischen Republiken, im Rahmen der Konferenz und machte so neue Experten mit TELETRUST bekannt. TELETRUST verleiht außerdem jährlich zur ISSE-Gala einen europäischen Preis für innovative und nutzbringende Anwendungen des elektronischen Geschäftsverkehrs. Last but not Least veranstaltet TELETRUST im Rahmen der Konferenz zusätzliche Abendveranstaltungen und bietet so einen gerne genutzten jährlichen Treffpunkt für Kollegen aus aller Welt!

## RSA – der Sprung in die USA

Die RSA Konferenz ist die weltgrößte Veranstaltung der Informationssicherheitsbranche. Gegründet als Tagung für Kryptoexperten, ist die Veranstaltung heute ein wichtiger Treffpunkt für die IT Sicherheitsindustrie in Nordamerika und zieht über 10.000 Teilnehmer an.

Die letzten Jahre sahen ein zunehmendes Interesse der großen Software- und Hardwarefirmen am Thema Informationssicherheit – so wurde die RSA 2004 mit einer Keynote von Bill Gates eröffnet, der die Microsoft Initiativen im Bereich Informationssicherheit darlegte. Hier zeigt sich ganz deutlich, dass Informationssicherheit nicht länger eine Domäne von spezialisierten Herstellern und Anbietern ist, sondern auch von den großen Playern in der IT Branche als bedeutender Marktfaktor gesehen wird.

Sichtbarkeit und Einfluss von europäischen Herstellern und Anbietern auf der RSA-Konferenz haben über die letzten Jahre leider stark abgenommen. Dies hängt mit der schwierigen wirtschaftlichen Lage der IT-Branche zusammen, die eine Konzentration auf den Heimatmarkt mit sich brachte. Leider bedeutet dies auch, dass europäische Impulse auf der RSA-Konferenz fehlen und wichtige Initiativen der Branche (TCG, Liberty Alliance etc.) hauptsächlich von amerikanischen Firmen vorangetrieben werden. Daher hat es sich TELETRUST seit 2001 zur Aufgabe gemacht, eine kontinuierliche Präsenz seiner Mitgliedsunternehmen auf der RSA-Konferenz – und somit auf dem amerikanischen Markt – aufzubauen.

Mit Unterstützung der AUMA e.V. und des BMWA konnte mehrfach ein Gemeinschaftsstand auf der konferenzbegleitenden Ausstellung organisiert werden, der deutschen Firmen und TELETRUST-Mitgliedern eine preisgünstige Präsenz zur RSA-Konferenz bot. Zusätzlich wurden von TELETRUST Abendveranstaltungen (mit bis zu 150 Gästen) und Expertentreffen organisiert, um für deutsche Teilnehmer mehr Networking-Gelegenheiten zu eröffnen – hier ließen sich dann auch die über die ISSE geknüpften Kontakte wieder gut nutzen, und so treffen sich internationale Experten sowohl zur ISSE als auch zur RSA-Konferenz auf TELETRUST-Veranstaltungen.

TELETRUST sieht es als unabdingbar für alle international tätigen Firmen der IT-Branche an, den amerikanischen Markt genau zu beobachten und Partnerschaften für zukünftige Aktivitäten zu knüpfen. Nur so können neuen Impulse aufgefangen und ein Markteintritt ermöglicht werden.

## Workshops und Experten Treffen

TELETRUST ist auch auf Ebene der Arbeitsgruppen und Services international aktiv. Beispielsweise organisierte die AG Recht Meetings mit internationalen Rechtsexperten und die AG Biometrie ist die Vertretung Deutschlands im European Biometric Forum (EBF). Die TELETRUST-Services European Bridge-CA und ISIS/MTT sind auch über die ISSE- und RSA-Aktivitäten in alle Welt getragen worden und werden heute zu internationalen Konferenzen in Asien, Osteuropa, und sogar UN Summits (Genf 2003) eingeladen.

Seit 2003 bemüht sich TELETRUST auch verstärkt um die neuen Beitrittsländer. So wurde im Juni 2003 in Tallinn (Estland) ein gemeinsamer Workshop zu grenzübergreifendem elektronischem Geschäftsverkehr veranstaltet. Über 50 Teilnehmer aus Deutschland, den Baltischen Staaten, Ungarn sowie Skandinavien diskutierten zwei Tage über Anwendungen und Lösungen. Die hier geknüpften Kontakte gingen in einem Nachfolge-Workshop zur ISSE 2003 auf und sind auch weiter in Einladungen zu Konferenzen und Workshops an die TELETRUST-Gemeinde zu spüren.

Kontinuität ist für internationale Kontakte das Rezept zum Erfolg!

# Runder Tisch Kryptowirtschaft

Förderung der Wettbewerbsfähigkeit  
der deutschen IT-Sicherheitswirtschaft

Volker Schneider

*Rohde & Schwarz SIT ist Mitglied im TELETRUST und  
Teilnehmer am Runden Tisch Kryptowirtschaft*

## Eckpunkte der deutschen Kryptopolitik

TELETRUST Deutschland e.V. hat seit der Legislaturperiode 1994-1998 kontinuierlich und wirksam die Entwicklung einer deutschen IT-Sicherheitspolitik unterstützt. So hat TELETRUST beispielsweise voller Enthusiasmus an der Entwicklung des Deutschen Signaturgesetzes von 1997 – dem ersten in Europa – mitgewirkt, bald danach jedoch schon auf, den Bedingungen der Praxis geschuldeten, Nachbesserungsbedarf hingewiesen. Wesentlich war und ist der unter dem Dach von TELETRUST geführte Dialog mit Vertretern der Technik und Jurisprudenz, des Daten- und Verbraucherschutzes sowie der Politik zur Notwendigkeit einer umfassenden Implementierung kryptographischer Verfahren in die Applikationen und Dienste für elektronische Geschäftsprozesse.

Am 2. Juni 1999 hatte das Bundeskabinett die „Eckpunkte der deutschen Kryptopolitik“ verabschiedet und damit das politische Gewicht der IT-Sicherheit in Deutschland unterstrichen. Der Beschluss hebt ausdrücklich hervor:

*„Die Bundesregierung beabsichtigt nicht, die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland einzuschränken.“* und *„Die Bundesregierung hält aus Gründen der Sicherheit von Staat, Wirtschaft und Gesellschaft die Fähigkeit deutscher Hersteller zur Entwicklung und Herstellung von sicheren und leistungsfähigen Verschlüsselungsprodukten für unverzichtbar. Sie wird Maßnahmen ergreifen, um die internationale Wettbewerbsfähigkeit dieses Sektors zu stärken.“*

Mit ihrem Eckpunktepapier hat die Bundesregierung nicht nur zu Fragen der Technik Stellung bezogen sondern für Deutschland auch grundsätzlich einen liberalen Umgang mit Kryptotechnologien beschlossen.

Die deutsche Kryptoindustrie hat seitdem mit hohen Aufwendungen für Forschung, Entwicklung und Zertifizierung ein leistungsfähiges Spektrum von Produkten, Lösungen und Dienstleistungen bereitgestellt und ist damit in der Lage, allen Anforderungen von sicherheitssensiblen Anwendungen vertrauenswürdig und unabhängig von internationalen politischen Einflüssen und Marktrestriktionen gerecht zu werden. Dies betrifft insbesondere

- Kritische Infrastrukturen,
- Wichtige Anwendungsbereiche der IT in der der Öffentlichen Verwaltung, in der Wirtschaft und im Finanzbereich, in Medizin und Gesundheitsverwaltung und
- Anforderungen der Inneren Sicherheit.



Diplom-Mathematiker  
Volker Schneider

Rohde & Schwarz SIT GmbH

Leiter Marketing / Vertrieb

E-Mail: volker.schneider@sit.rohde-schwarz.com

Gemessen an der Breite des Lösungsangebots steht Deutschland im internationalen Rahmen auf dem zweiten Platz nach den USA.

Im Gegensatz zu der durch die Politik hoch anerkannten Bedeutung der IT-Sicherheit hat sich ein ausreichender nationaler Markt für deutsche Lösungen nicht etabliert. Auch die internationale Wettbewerbsfähigkeit der deutschen Kryptoindustrie hat sich nicht entscheidend verbessert. Entsprechende Studien, die auch von TELETRUST unterstützt wurden, belegen die noch immer wirtschaftlich schwierige Lage der deutschen Kryptoindustrie.

Die Einrichtung des Runden Tisches Kryptowirtschaft ist ein konkreter Schritt der Bundesregierung zur weiteren Umsetzung des eingangs zitierten Eckpunktepapiers und zur strategischen Unterstützung der deutschen Anbieter von IT-Sicherheitslösungen.

## Zielstellung des Runden Tisches

Die Einrichtung des Runden Tisches Kryptowirtschaft durch die Bundesministerien des Innern (BMI) und für Wirtschaft und Arbeit (BMWA) unter Einbeziehung von TELETRUST, BITKOM und Vertretern führender Unternehmen der IT-Sicherheitsbranche erfolgte u.a. mit der Zielstellungen der Erarbeitung von geeigneten Maßnahmen

- zur strategischen Unterstützung der deutschen IT-Sicherheitswirtschaft durch die Bundesregierung,
- für die Verbesserung der internationalen Wettbewerbsfähigkeit der deutschen Kryptowirtschaft,
- zur effektiveren Nutzung der nationalen und europäischen Förderprogramme zur Entwicklung von standard- und marktgerechten Anwendungslösungen
- zur Erhöhung des Vertrauens in IT-Sicherheitslösungen durch Evaluierung und Auditierung, u.a. auch auf der Grundlage von Selbstregulierungskonzepten der Anbieter solcher Lösungen,
- zur verstärkten Sensibilisierung der Anwender in Hinblick auf die Notwendigkeit angemessener IT-Sicherheitslösungen.

## Exportunterstützung

Die Gewinnung von Exportmärkten ist angesichts der begrenzten Umsatzgröße des deutschen Marktes für die deutsche Kryptoindustrie für die Wiedererwirtschaftung der Aufwendungen für Entwicklung, Evaluierung, Vertrieb, Support und Service existentiell wichtig. In einer vom BMWA beauftragten Studie „Ausgangssituation und Chancen im Exportgeschäft der deutschen IT-Sicherheits- und Kryptowirtschaft“ werden die Regionen Mittel- und Osteuropa, Süd-Ost-Asien sowie Mittlerer und Naher Osten als wichtige Zielmärkte identifiziert.

Folgende Maßnahmen zur Exportunterstützung werden als vordringlich erachtet:

- Sensibilisierung der deutschen Botschaften und Außenhandelskammern für deutsche IT-Sicherheitslösungen,

- Roadshow zum Angebot deutscher Kryptoprodukte und Etablierung des Labels „Crypto made in Germany“ auf den Zielmärkten,
- Erarbeitung eines Produktportfolio zum marktgerechten Angebot deutscher IT-Sicherheitslösungen und Kryptoprodukte (unter Federführung des TELETRUST).

Beispielhaft für konkrete Vorhaben seien hier geplante IT-Sicherheitsworkshops in den Ländern Mittel- und Osteuropas, speziell in den Beitrittsländer der EU und der NATO genannt. In diese Workshops kann TELETRUST viele wertvolle Kontakte zu Fachleuten einbringen, die sich im Zusammenhang mit Veranstaltungen wie ISSE und CeBIT herausgebildet haben.

## IT-Sicherheitslösungen „Made in Germany“

Mit dem unter Federführung des TELETRUST entstehenden Lösungsportfolio deutscher IT-Sicherheits- und Kryptolösungen soll als Initiative der deutschen IT-Sicherheitsindustrie unter aktiver Mitwirkung der am „Runden Tisch Kryptowirtschaft“ beteiligten Unternehmen eine aussagekräftige Informationsbasis für Entscheidungsträger in Politik, öffentlicher Verwaltung und Wirtschaft geschaffen werden.

Die Broschüre, die in deutsch und englisch erstellt wird, soll beispielhaft die Leistungsfähigkeit des deutschen Kompetenznetzwerkes im Bereich der IT-Sicherheit darstellen. Sie ist ein notwendiger ergänzender Baustein für laufende und geplante Maßnahmen der Exportunterstützung.

Dargestellt werden die wesentlichen Rahmenbedingungen für die international anerkannte Vertrauenswürdigkeit von IT-Sicherheit „Made in Germany“:

- die liberale Kryptopolitik der Bundesregierung (siehe Eckpunktepapier),
- ein leistungsfähiges und international angesehenes Bundesamt für Sicherheit in der Informationstechnik (BSI),
- leistungsfähige Forschungseinrichtungen (Universitäten, Fachhochschulen, Fraunhofer-Gesellschaft) die eng mit der Wirtschaft kooperieren.

Aus Sicht der deutschen Anbieter sind insbesondere Lösungen, die die Kompetenz von einschlägigen Unternehmen zusammenführen; für folgende Marktsegmente von Bedeutung:

- Hochsicherheitslösungen für Bedarfsträger aus dem Bereich „Nationale Sicherheit“,
- Lösungen zur Sicherung von Geschäftsprozessen in Wirtschaft und Verwaltung,
- Lösungen für die Basissicherheit in Massenprodukten,
- IT-Sicherheits-Consulting und –Systemintegration.

Hinzu kommen spezielle Entwicklungen für IT-Sicherheitsinfrastrukturen wie Trust Center und Dienstleistungen wie Produktevaluierung und Zertifizierung.

Durch die Darstellung von erfolgreichen Lösungen in relevanten Anwendungsfeldern und der Kompetenz der deutschen IT-Sicherheitsindustrie soll direkt und indirekt das Marketing für IT-Sicherheit „Made in Germany“ unterstützt werden.

## Das neue TELETRUST-Experten-Zertifikat für ICT-Spezialisten

Kai Hartwich

*Insbesondere seit 1998 ist Kai Hartwich dabei, viel zu lernen.*

### Zeige mir, was Du kannst

Es ist eigentlich immer das Gleiche: Auf der einen Seite müssen von der Bundesagentur für Arbeit immer wieder wenig beruhigende Zahlen zur Arbeitslosigkeit in Deutschland veröffentlicht werden – die Halde der willigen und oft qualifizierten Anwärter auf einen guten Arbeitsplatz ist gewaltig. Auf der anderen Seite suchen Arbeitgeber händeringend nach zu ihren Unternehmen passenden, motivierten Fachkräften. Dies ist weder ein Problem bestimmter Sachgebiete noch fest umrissener geographischer Regionen. So betrifft es auch den Bereich der ICT-Sicherheit in Deutschland und Europa.

Hier gibt es hervorragende Fachleute aber auch „Experten“, deren hervorragendste Qualifikation in ihrem Glauben an die eigenen Kenntnisse und Fertigkeiten sowie der Fähigkeit, diese überzeugend darzubieten, liegt. Das Problem beider Seiten, der der Experten-Suchenden und der der sich-finden-lassen-wollenden, liegt darin, die Spreu vom Weizen zu trennen.

Im nordamerikanischen Wirtschaftsraum gibt es bereits seit Jahren anerkannte Zertifikate, mit denen ICT-Fachleute in Arbeitnehmer- und Selbständigenposition ihre Qualifikation als Experte belegen können; ein Beispiel hierfür ist CISSP (Certified Information Systems Security Professional) des Non-Profit Konsortiums (ISC)<sup>2</sup>. CISSP ist vor allem in Nordamerika ein Wertbegriff: Dem Vortrag eines CISSP wird mit erhöhter Aufmerksamkeit zugehört, CISSP ist ein Kriterium für einschlägige Auftragsvergaben.

Dieses und ähnliche Zertifikate haben bisher, aus welchen Gründen auch immer, im deutschen und europäischen Raum keine relevante Bedeutung gewonnen. Dieser Umstand führte in TELETRUST zur Idee eines unabhängigen Expertenzertifikats, das auf die deutschen und europäischen Bedingungen abgestellt ist und als Gütesiegel für hiesige ICT-Spezialisten entwickelt werden kann.

### Nomen est omen

Die Experten der sechs TELETRUST-Mitgliedsunternehmen (Applied Security, CAST, FhG SIT, GITS, secunet und Siemens), die sich in dem Entwicklungsprojekt für das neue Zertifikat zusammenfanden, hatten zunächst einen Namen für das Zertifikat zu definieren. Er sollte so klar sein, dass man aus ihm allein schon Vorstellungen seines programmatischen Inhaltes ableiten können sollte. Dies war eine erste komplexe Aufgabenstellung für Experten!



Kai Hartwich

1981-87 Diplomlehrer für Mathematik und Physik,  
1987-91 Entw.-Ing. in der mikroelektronischen F&E,  
bis Ende 1997 div. Jobs, u.a. Filialeiter im Elektrogroßhandel

seit 1998 Assistent des Geschäftsführers von TELETRUST

E-Mail: kai.hartwich@teletrust.de

Der Name sollte folgende Assoziationen vermitteln:

- Zertifikat für Experten,
- Sachgebiet: Informationssicherheit,
- Unabhängig,
- Vertrauenswürdig.

Zur Gewährleistung der letzten beiden Punkte wurde entschieden, den Namen von TELETRUST zu benutzen. Weil die Zertifikatsträger anfangs aus Deutschland, in der Tendenz aber aus ganz Europa kommen sollen, entschied man sich für eine englischsprachige Bezeichnung. Damit das neue Zertifikat nicht mit bereits etablierten verwechselt werden kann, wurde beschlossen, ein Bildzeichen dafür zu entwickeln. Im Ergebnis entstand:



## TISP-Zertifikat – für wen?

Das Zertifikat ist nicht gedacht für arbeitslose Dachdecker oder Blumenbinderinnen, die nach einer durch das Arbeitsamt oder selbst finanzierten Umschulung nach neuen Horizonten ihrer beruflichen Entwicklung Ausschau halten. Bei aller Motivation dieser Leute – das sind nicht die „fertigen“ ICT-Spezialisten, nach denen ständig gesucht wird.

Zum Erwerb des Zertifikates TISP werden bereits umfangreiches Wissen und profunde praktische Kenntnisse der Informationssicherheit vorausgesetzt. Mit der Zulassung zur Prüfung ist zu belegen, dass man über eine mindestens 3-jährige einschlägige Berufserfahrung verfügt und bei einem der zugelassenen Schulungsanbieter einen einwöchigen, zusammenfassenden Kurs belegt hat. Dieser Kurs verfolgt nicht das Ziel, alle zum Bestehen der Prüfung notwendigen Kenntnisse zu vermitteln. Er soll ggf. beim Prüfungsanwärter noch vorhandene Lücken aufdecken, die dieser dann durch zusätzliche Schulungsmaßnahmen schließen kann.

## Was kostet TISP?

TISP-Schulung und –Prüfung sind kostenpflichtig. Den Preis bestimmt der Schulungsanbieter. Derzeit liegt er bei den zugelassenen Schulungsanbietern (das sind gegenwärtig die sechs, die in dem vorbeschriebenen Projekt TISP entwickelt haben) zwischen 2.200 und 2.300 €. TELETRUST ist an dieser Einnahme nicht beteiligt.

Die bisher zugelassenen TISP-Schulungszentren bieten ihre Leistungen in Deutschland an. Daher ist Schulungs- und Prüfungssprache Deutsch.

Geplant ist jedoch, dass zu den heutigen Schulungsanbietern weitere aus Deutschland und anderen Staaten Europas hinzu kommen. Erste Interessenten aus Österreich und der Schweiz haben sich bereits gemeldet. Zur Wahrung der Qualität von TISP werden diese erst nach einem (kostenpflichtigen) Lizenzierungsverfahren von TELETRUST als TISP-Schulungsanbieter zugelassen werden. Die Lizenzierungsbeträge werden zur Deckung der Eigenkosten an TELETRUST fließen.

## Aussagekräftige Inhalte

Die Inhalte der TISP-Schulung und –Prüfung wurden in dem TISP-Entwicklungsprojekt so definiert, dass sie die europäische, besonders technologiebezogene Sichtweise bei der Bewertung der fachlichen Qualifikation von ICT-Experten berücksichtigt. Dem trägt der 18 Module umfassende Schulungs- und Prüfungsumfang differenziert Rechnung. Neben theoretischen technischen Grundlagen wie Kryptographie und Standards, spielen auch weitere Themen wie Netzwerk- und Systemsicherheit, Firewalls und VPN, Sicherheits- und Benutzermanagement aber auch rechtliche Grundlagen eine Rolle. Alles natürlich abgestimmt auf die deutschen bzw. europäischen Bedingungen.

Die Prüfung wird als Multi-Choice-Test abgenommen. In zweimal 120 Minuten sind insgesamt 180 Fragen (je 10 aus jedem Modul) zu beantworten.

## Ausblick: Anerkennung von TISP

TISP ist noch sehr jung und hat daher noch keine weite Verbreitung, geschweige denn allgemeine Anerkennung gewonnen. Heute, das ist Ende Juli 2004, haben 9 ICT-Spezialisten die TISP-Prüfung erfolgreich absolviert und das Zertifikat erhalten.

Stellt man derzeit TISP und CISSP nebeneinander, sollte man im Hinterkopf behalten, dass auch CISSP einmal klein angefangen hat.

TELETRUST wird auf seiner Webseite die Informationen zu TISP permanent aktuell halten.

Ich bin gespannt, wie TISP sich entwickeln wird. Zuversicht ist in meinen Augen nicht abwegig: In der Tendenz scheint Konvergenz zwischen TISP und CISSP möglich, vielleicht sogar eine Synthese?

# **Neue Herausforderungen**

Die Mitglieder des Vereins unterstützen die Nutzung neuer Technologien – wie Trusted Computing, RFID oder Biometrie – für künftige IT-Sicherheitslösungen.



# Neue Sicherheitsarchitekturen

Das Zusammenspiel von Bausteinen zur Erfüllung fortgeschrittener Sicherheitsanforderungen von elektronischen Geschäftsprozessen

Michael Hartmann, Sachar Paulus

*Sachar Paulus ist Chief Security Officer bei der SAP AG und verantwortlich für die Sicherheitsstrategie der SAP. Er und sein Team vertreten SAP in vielen internationalen Sicherheitsorganisationen. Er ist Mitglied im Organisations- und Programmkomitee der ISSE 2004. Für TELETRUST war er als Leiter der AG „Onlineprozesse und Identitätsmanagement“ tätig.*

*Michael Hartmann ist bei der SAP AG zuständig für die externen Kommunikationsprozesse des SAP CERT und für den Aufbau eines Product Security Bulletin Service. Für TELETRUST ist er als Leiter der AG „Personal Security Environment –PSE“ tätig.*



Dr.  
Sachar Paulus

Chief Security Officer SAP AG

E-Mail: sachar.paulus@teletrust.de



Michael Hartmann

Corporate Security Manager bei der SAP AG

E-Mail: michael.hartmann@teletrust.de

## Geschäftsprozesse

Moderne Geschäftsprozesse sind üblicherweise unternehmensübergreifend ausgelegt. Für jeden dieser Geschäftsprozesse ist eine juristische Person (z.B. Unternehmen, Behörde, eigenverantwortlich handelnde natürliche Person) verantwortlich – der Prozesseigner. Der Prozesseigner hat in der Regel ein ökonomisches Interesse an einem Geschäftsprozess – Profit oder eine kostengünstige Verwaltung. Dabei muss er selbstverständlich dafür Sorge tragen, dass der Geschäftsprozess den gesetzlichen Bestimmungen genügt.

Aus rechtlicher Sicht sind nur die Konsequenzen, die sich aus einem Geschäftsprozesses für die beteiligten juristischen Personen ergeben, relevant.

Um seinen Business Case zu realisieren, wählt der Prozesseigner unter den verschiedenen möglichen Varianten entsprechend seines individuellen Geschäftszwecks und des sich daraus ergebenden Anwendungszusammenhangs seine bevorzugte Prozessvariante primär unter ökonomischen Aspekten aus. Die juristischen oder sicherheitstechnischen Anforderungen bilden dabei nur Rahmenbedingungen, die es zu erfüllen gilt, um das ökonomische Ziel zu erreichen.

Um es ganz klar zu sagen: Der Geschäftsmann geht morgens nicht zur Arbeit, um Gesetze mit Leben zu erfüllen oder Sicherheit zu praktizieren. Er will Geschäfte machen! Die sicherheitstechnischen Maßnahmen sind dabei nur Mittel zum Zweck und daher aus Sicht des Prozesseigners nur ein Teil der ökonomischen Gesamtbetrachtung.

Die Sicherheitsverantwortlichen hingegen orientieren sich meist rein an der Infrastruktur und den zu schützenden (statischen) Assets. Eine prozessorientierte Betrachtung findet meist nicht statt, da die Sicherheitsverantwortlichen aus unterschiedlichsten Gründen selten in das Design der Geschäftsprozesse einbezogen werden.

Zur Realisierung eines Geschäftsprozesses stehen immer unterschiedliche Implementierungsvarianten zur Auswahl, die unter juristischen Gesichtspunkten als gleichwertig zu betrachten sind. Diese Implementierungsvarianten verwenden unterschiedliche Maßnahmen, um die Sicherheit des Geschäftsprozesses zu gewährleisten. Diese Maßnahmen sind stark abhängig von den beteiligten natürlichen Personen, die oft mit der Wahrnehmung einer bestimmten Rolle in einem Unternehmen oder einer Behörde beauftragt sind, also stellvertretend für eine juristische Person auftreten. Rollenspezifisch fallen dabei differierende Kosten für die von der jeweiligen Person geleisteten manuellen Beiträge an.

Je weniger natürliche Personen in einen Geschäftsprozess eingebunden und durch technische Komponenten ersetzt werden, desto mehr muss die Kontrolle von der Ausführungsphase in die Implementierungsphase verlegt werden. Beispielsweise wird die Prüfung einer händischen Unterschrift immer in der Ausführungsphase vorgenommen; zur automatisierten Prüfung einer elektronischen Unterschrift dagegen wird eine Public-Key-Infrastruktur vorausgesetzt.

Im Rahmen seiner inhaltlichen Zielsetzung – der Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik – rückt TELETRUST die Prozessimplementierungen mit hohem Automatisierungsgrad verstärkt in den Vordergrund seiner Betrachtung. Für diese Prozessimplementierungen sind Bausteine zu untersuchen, die ein optimiertes Sicherheits-Kosten-Verhältnis bieten. Gleichzeitig will TELETRUST den Prozesseigner bei der Auswahl der erforderlichen und wirtschaftlich sinnvollen Sicherheitsbausteine unterstützen.

In diesem Beitrag betrachten wir die Bausteine, die nach aktuellem und absehbarem zukünftigen Stand der Technik ein optimiertes Sicherheit-Kosten-Verhältnis bei bestmöglichem Automatisierungsgrad versprechen.

## Prozessimplementierungen

Die modernen Geschäftsprozesse und deren Implementierungen setzen sich aus vielen unterschiedlichen Bausteinen, den Anwendungen, mit einer hohen vertikalen Integration der verwendeten Technologien (beispielsweise Portal, Applikationsserver, Datenbank, Messagingserver, etc.) zusammen. Gleichzeitig nimmt auch die horizontale Integration zu, in dem diese hoch integrierten Anwendungen ebenfalls unternehmensübergreifend enger mit einander gekoppelt werden. Mit der zunehmenden Komplexität wird die Sicherstellung der erforderlichen Vertrauenswürdigkeit und Sicherheit der Geschäftsprozesse ebenfalls immer anspruchsvoller.

Abbildung 1 zeigt die Architektur heutiger Geschäftsprozesse und der zugrunde liegenden Anwendungen und Technologien. Horizontal sind verschiedene Entitäten, also Organisationen, Organisationseinheiten und Individuen angeordnet. Vertikal finden sich die unterschiedlichen Technologie-, respektive Anwendungsschichten, beginnend bei der Person bis zum Geschäftsprozess und Ihrem Eigner, der Organisation. Die abstrakteste Ebene bildet der Geschäftsprozess, der auch über mehrere Organisationen hinweg implementiert sein kann oder muss. Der Geschäftsprozess durchläuft mehrere Prozessschritte in den unterschiedli-

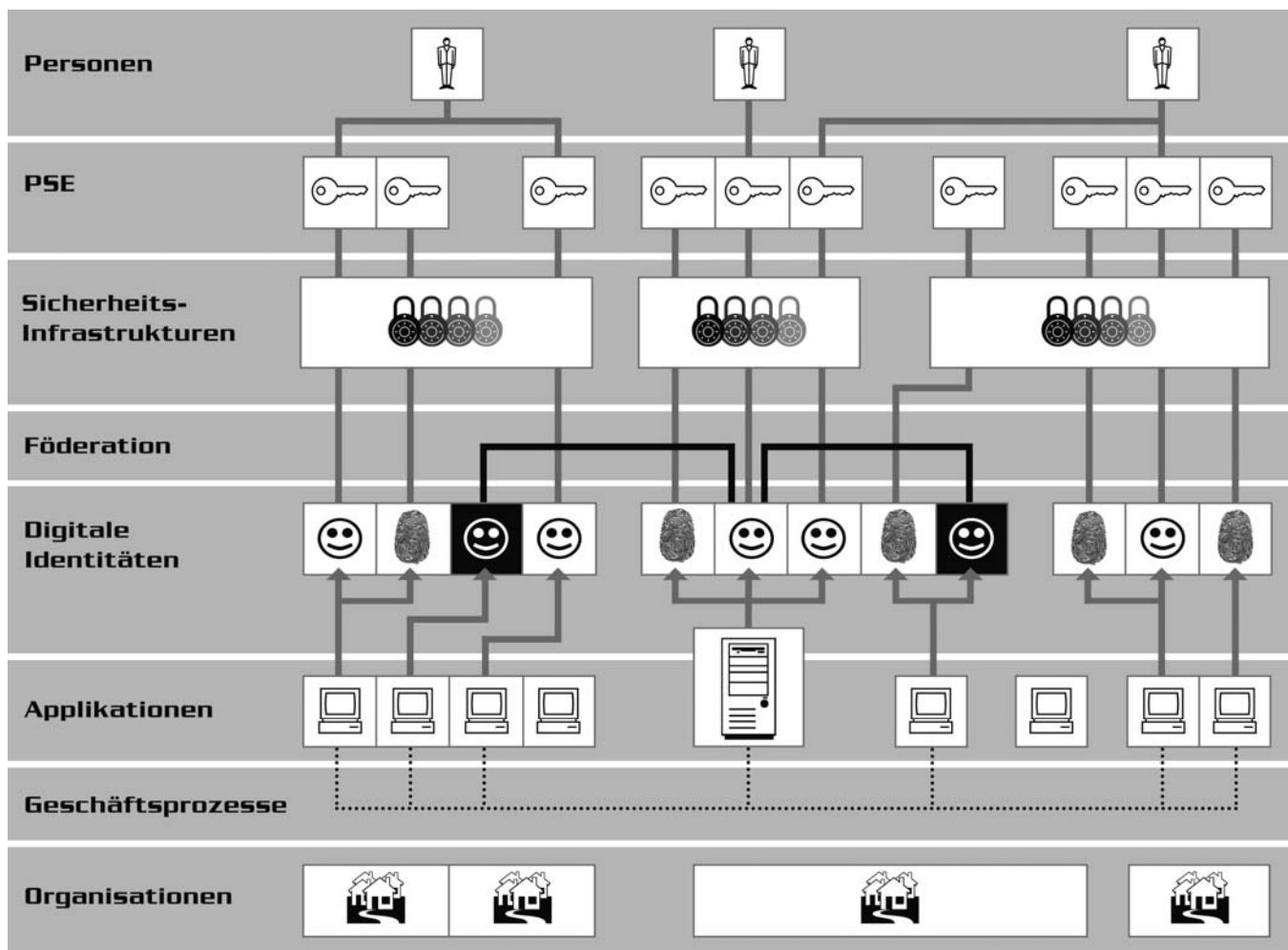


Abb. 1: Sicherheitskomponenten im Zusammenspiel unternehmensübergreifender Geschäftsprozesse

chen Applikationen, in denen die Verarbeitung der Daten stattfindet. Die einzelnen Prozessschritte wiederum werden durch Aktionen unterschiedlicher Identitäten (natürliche oder juristische Personen sowie technische Komponenten wie Server) diverser Organisationen ergänzt. Dabei wird die Verbindung zwischen elektronischen Geschäftsprozessen durch Automatisierung (siehe RFID) bzw. durch Personen in verschiedenen Rollen (siehe Identitätsmanagement) hergestellt.

Bei der Implementierung der Prozesse in elektronische Abläufe sind die unterschiedlichen Rahmenbedingungen aus ökonomischer und nationaler wie internationaler rechtlicher Sicht zu berücksichtigen. Daraus leiten sich schließlich die Anforderungen an die eingesetzten Applikationen und die mit den Applikationen verwendeten Technologien ab.

TELETRUST bearbeitet die verschiedensten Teilaspekte vertrauenswürdiger elektronischer Geschäftsprozesse in seinen unterschiedlichen, mit einander vernetzten Arbeitsgruppen.

Die wichtigsten rechtlichen Vorgaben betreffen den Schutz von personenbezogenen Daten (Datenschutzgesetzgebung) und die Eindämmung möglicher negativer Auswirkungen von elektronischen Geschäftsprozessen (Sarbanes Oxley, Basel II, GOBS, KonTraG). Bei TELETRUST werden diese Fragestellungen innerhalb der AG1 (Juristische Aspekte einer verbindlichen Kommunikation) behandelt. Die AG9 beschäftigt sich mit den Themen Online-Prozesse und Identitätsmanagement. Die Thematik der im Hintergrund erforderlichen Sicherheitsinfrastrukturen wird in der AG7 behandelt. Die aktuellen und künftigen Technologien zur Implementierung der vorgenannten Sicherheitsinfrastrukturen werden in der AG2 (PSE – Personal Security Environment) betrachtet. Die Bindung von elektronischer Identität zur Person wird durch die AG6 (Biometrische Identifikationsverfahren) behandelt. Im Folgenden schränken wir die Betrachtung auf Identitätsmanagement und vertrauenswürdige Technologiekomponenten ein.

## Online-Prozesse

Aufgrund der Responses der TELETRUST-Mitglieder in der AG9 wurde das Thema Online-Prozesse aus der inhaltlichen Arbeit dieser AG herausgelöst. Es wird aufgrund der Aktivitäten des Internen TTT-Workshops 2004 eine „Themengruppe“ gebildet, die sich AG-übergreifend dieser Thematik annehmen wird. Dabei sollen vorwiegend unternehmensübergreifende Geschäftsprozesse untersucht werden, die aufgrund verschiedener inzwischen geschaffener Rechtsrahmen in den nächsten Jahren implementiert werden sollen, so etwa:

- Elektronische Steuererklärung,
- Elektronische Rechnung,
- Verbindliche elektronische Abwicklung von Bestellungen.

Dabei geht es nicht nur um die Implementierung der Prozesse an sich, sondern ebenfalls um die „umliegenden“ Problematiken wie Revisionssicherheit und Rechtssicherheit bei der Archivierung, Anforderungen an die Sicherheitsinfrastrukturkomponenten etc.

Ergebnis soll in erster Linie eine Aggregation von Best Practices auf der Grundlage des geltenden Rechtsrahmens und unter Beachtung der Wirtschaftlichkeit sein, nicht die Beschreibung der aus Sicherheitssicht idealen Geschäftsprozesse. Beispiel: Nicht immer ist die elektronische Rechnung mit qualifizierter elektronischer Signatur betriebswirtschaftlich sinnvoll, oft genügt auch ein Sammelrechnungsmodell, in dem die einzelnen Rechnungen

elektronisch unsigniert übermittelt werden und etwa monatlich eine Sammelrechnung, die die elektronischen Rechnungen zusammenfasst, in Papierform versandt wird. Die rechtliche Grundlage dafür bildet die GdPdU (Grundzüge der Prüfung digitaler Unterlagen).

## Identitätsmanagement

Hauptproblem bei der Integration von elektronischen Identitäten, also der Kennzeichnung von durch natürliche Personen bekleidete Rollen sowie technischen Komponenten des weitgehend automatisiert arbeitenden Systems ist, dass die Identitätsdaten üblicherweise in unterschiedlichen Kontexten erstellt wurden und redundant, in nicht standardisierter Form vorliegen. Identitätsmanagement hat zum Ziel, dieses Problem durch standardisierte Zugriffs- und Austauschprotokolle zu mildern (ganz lösen wird man es nicht können). Dabei kommt hinzu, dass die Integration oft auch Aggregation von Attributen, die personenbezogen sein können und somit den Datenschutzerfordernungen unterliegen, beinhaltet (Sichere Verwaltung, Weitergabe, Bearbeitung, Austausch, Löschfristen, Zustimmung, nur unter Kontrolle des Benutzers).

Modernes Identitätsmanagement nimmt die Datenschutzproblematik in die Komplexität der integrierten Verwaltung mit auf, etwa durch die Verwendung von Föderationskonzepten. Hierbei werden Daten – statt sie zu kopieren – auch über Unternehmensgrenzen hinweg referenziert. Der Zugriff auf diese Daten (bzw. deren Kopie) können durch den Inhaber (also die beschriebene Person selbst) autorisiert werden. Als Beispiele für Prozesse, die ein standardisiertes Identitätsmanagement in diesem Sinn erfordern, seien an dieser Stelle genannt:

- Der Mobilfunkbereich ist, mit dem bereits etablierten und global ermöglichten Roaming, ein Beispiel für erfolgreiches Identitätsmanagement. Neue Herausforderungen an das Identitätsmanagement im Mobilfunkbereich ergeben sich beispielsweise durch den fließenden Übergang von WLAN zu GPRS als Datentransporttechnologie und die sich langsam etablierenden Mehrwertdienste wie Restaurantbuchungen, Internet-Provider und weitere Location-Based-Services.
- Die für Anfang 2006 geplante Gesundheitskarte ist ein weiteres Beispiel für Identitätsmanagement. Sie soll es unter anderem ermöglichen, Patientendaten elektronisch den jeweils behandelnden Ärzten zur Verfügung zu stellen. Dabei hat der Patient das berechtigte Interesse, dass seine Daten nur mit seinem Einverständnis weitergegeben werden. Die Gesundheitskarte soll nicht ausschließlich in der Beziehung Arzt-Patient den Datenaustausch ermöglichen sondern viele weitere Anwendungen z.B. im Zusammenwirken mit Apotheken oder Krankenkassen unterstützen.
- Die vom Bundesministerium für Wirtschaft und Arbeit geplanten JobCard-Fachanwendungen ermöglichen einen zeitlich begrenzten Abgleich von personenbezogenen Daten zwischen Arbeitgebern und Behörden, Behörden untereinander sowie Behörden und Anspruchsberechtigten. Die Kontrolle über bestimmte Attribute muss beim Arbeitnehmer bleiben, bei welchem diese Daten erhoben wurden. Andere Attribute werden von der BfA erhoben und sollen auch unter deren Kontrolle bleiben. Ein standardisiertes Datenaustauschverfahren ist hier bislang nicht vorgesehen.

## Vertrauenswürdige elektronische Identitätskomponenten

Personal Security Environments (PSE) sind elektronische Repräsentanten einer Identität in elektronischen Geschäftsprozessen und damit Teil der eingebundenen Sicherheitsinfrastruktur.

Die Arbeitsgruppe 2 wurde mit dem Ziel gegründet, nach einer Bestandsanalyse firmenübergreifend relevante Lösungsansätze zum interoperablen und praktikablen Einsatz von PSEs zu erarbeiten und zu unterstützen. Die Vielzahl unterschiedlicher Aspekte wie Funktionalität, technische Ausprägung, erforderliche Infrastrukturen, Verwaltung, Integration in die Anwendungslösung, Schnittstellen, Datenschutz, Bindung an die Person sowie Standardisierung beschreiben die Komplexität dieser Aufgabe und sind wichtige Voraussetzungen für einen wirtschaftlichen Einsatz. Aktuelle Anwendungsbeispiele für PSE-Szenarien:

- Sichere E-Mail (sicherer Nachrichtenaustausch, Verschlüsselung, elektronische Unterschrift ...)
- Gesundheitswesen (Health Professional Card, Elektronische Gesundheitskarte ...)
- Hoheitliche Aufgaben (Visum, Aufenthaltsgenehmigung, Bürgerkarte, Personalausweis, Pass ...)
- Marketing (Bank, Kunde, Rabatt, Verkehr ...)
- Elektronische Identität und elektronische Willenserklärung (E-Banking, Homebanking, Auktionen ...)
- Elektronische Archivierung

Ergänzend zu den Personal Security Environments werden innerhalb der AG2 die Themen Trusted Computing und RFID bearbeitet.

Eine wesentliche Voraussetzung für die erfolgreiche Abbildung elektronischer Geschäftsprozesse in Richtung einer umfassenden, vertrauenswürdigen Vernetzung aller Kommunikationsgeräte kann nur ein standardisierter Sicherheitsmechanismus sein, der den Aufbau einer sicheren Infrastruktur ermöglicht. Daher ist das Konzept des Trusted Computing – nach dem Einsatz von SmartCards – die nächste logische Entwicklung für die vertrauenswürdige Verwendung von persönlichen elektronischen Geräten wie PCs und PDAs.

Trusted Computing ist ein Konzept, das dringende multilaterale Anforderungen wie mehr Sicherheit bei online-Transaktionen, den Datenschutz (Privatpersonen), den Schutz des geistigen Eigentums oder vertrauenswürdiger Geschäftsprozesse (Unternehmen) und gesellschaftlicher Sicherheitsinteressen erfüllen kann und wird sich zwangsläufig gegen nicht-standardisierte Sicherheitsmechanismen durchsetzen. Eine frühzeitige, fundierte Beschäftigung mit der neuen Technologie ist wichtig, um eine offene Standardisierung der zugrunde liegenden Technologien durchzusetzen. Diese Offenheit ermöglicht es auch anderen, kleineren Organisationen, die nicht Mitglieder in Standardisierungsgremien wie etwa der Trusted Computing Group sind, alternative Angebote zu machen, und stellt mittelbar die freie Verwendung der Technologie sicher. Dadurch können Monopole verhindert und eine mögliche einseitige Verwendung kontrolliert werden.

Mögliche negative Folgen von Trusted Computing – wie die von den Gegnern befürchtete Kontrolle von informationellen Werten eines Unternehmens oder die Verhaltenskontrolle durch einen öffentlichen Diensteanbieter für staatliche Belange – sollten unabhängig von der technischen Diskussion betrachtet und durch aktive Mitwirkung verhindert werden.

Keinesfalls sollten aus Angst vor den möglichen negativen Folgen Entscheidungen getroffen werden, die die allgemeine technische Funktionalität beschneiden. Gleichzeitig sind das Missbrauchspotenzial klar zu beschreiben und die notwendigen Maßnahmen zu ergreifen, um dem Missbrauch der Technologie aktiv zu begegnen. Den größten Nutzen aus dieser Technologie erhält nach derzeitigem Kenntnisstand die Industrie, wobei das größte Missbrauchspotenzial zu Lasten der privaten Endanwender geht, die sich entmündigt, in ihrer persönlichen Freiheit eingeschränkt und der Monopolisierung einzelner großer Hersteller und Diensteanbieter ausgeliefert sehen. Um den möglichen Nutzen und das Mißbrauchspotenzial sauber gegeneinander abzuwägen, sollen technische und politische Interessen am Thema Trusted Computing, soweit möglich, getrennt voneinander betrachtet werden.

Das Thema RFID wird derzeit – ähnlich wie Trusted Computing – sehr kontrovers diskutiert. Unternehmen stellen die Möglichkeiten der Kostenreduzierung in den Vordergrund, während Datenschützer und Lobbyisten ein Orwellsches Schreckensszenario und den vollständig gläsernen Konsumenten befürchten, dessen gesamtes Verhalten nachvollziehbar wird; angefangen beim Einkaufen bis hin zu Bewegungsprofilen. RFID kommt nicht nur bei so genannten Smartlabels von Konsumgütern zum Einsatz, sondern wird auch für elektronisch lesbare (personengebundene) Dokumente verwendet. TELETRUST wird sich mit der RFID Technologie im positiven Sinne, als Enabler für neue Geschäftsprozesse, genauso wie im negativen Sinne auseinandersetzen und die Möglichkeiten kritisch betrachten. Nur so kann eine vertrauenswürdige Informations- und Kommunikationstechnik erreicht werden. Die AG2 versteht sich auch als Diskussionsforum, in dem der aktuelle Stand der Technik und der weitere technologische Fortschritt mit den Mitgliedern diskutiert werden und so die aktuelle Entwicklung den Mitgliedern transparent macht.

## Ausblick

Die Werkzeuge zur Gewährleistung angemessener Sicherheit im elektronischen Geschäftsverkehr existieren ebenso wie ein ausgefeilter Rechtsrahmen. Mit Trusted Computing und RFID tun sich derzeit weitere Technologien auf, die unterschiedlichste Anwendungsszenarien ermöglichen.

Weil TELETRUST es im Sinne seines Vereinszwecks als seine Pflicht ansieht, sich mit neuen Sicherheitstechnologien auseinander zu setzen, werden auch diese Technologien und die sich von ihnen ableitenden Folgen begleitet und, soweit möglich und notwendig, beeinflusst werden. Gleichzeitig wird TELETRUST die sich ergebenden Chancen bewerten und den Prozesseigner vermitteln, damit diese die neuen Technologien zur Verbesserung ihrer Prozessimplementierungen heranziehen und potenzielle neue Prozessvarianten erkennen können.

# Robuste PKI-Lösungen für große Anwendergruppen

Detlef Dienst

*Mitglied des ISIS-MTT Boards,  
Mitglied des Bridge-CA Boards,  
Vertreter des akkreditierten Zertifizierungsdiensteanbieters  
Deutsche Telekom AG (T-TeleSec Public Key Service) im  
T7 e.V. i.Gr.*

## Ausgangslage

PKI-(Public Key Infrastructure)-Lösungen werden seit einigen Jahren in verschiedenen Anwendungen erfolgreich eingesetzt. Damit sind große Erwartungen in Wirtschaft und Verwaltung verbunden:

- Steigerung der Sicherheit in der elektronischen Kommunikation,
- Verbesserung der Wirtschaftlichkeit von komplexen Lösungen,
- Nahtlose Integration der PKI-Lösungen in die Geschäftsprozesse.

IT-Sicherheit ist dabei nicht Selbstzweck sondern generischer Baustein vertrauenswürdiger Anwendungen zur Abwicklung elektronischer Geschäftsprozesse.

Bei den bereits erfolgreich eingesetzten Anwendungen handelt es sich jedoch in vielen Fällen um „Insellösungen“, d.h. um geschlossene Benutzergruppen. Interoperable PKI-basierte Kommunikation ist auf breiter Basis zwischen Wirtschaft, Verwaltung und Bürgern noch nicht Wirklichkeit geworden, obwohl die Voraussetzungen sowohl auf juristischer als auch technischer Seite gegeben sind.

## Standards

Das gemeinsam von *TELETRUST* Deutschland e.V. und T7 e.V. i. G. im Auftrag des Bundesministeriums für Wirtschaft und Arbeit entwickelte Profil ISIS-MTT hat über Deutschland hinaus Anerkennung gefunden. ISIS-MTT wird von der Bundesregierung im Rahmen der Anwendungsfelder „BundOnline 2005“, Media@Komm-Transfer, „JobCard Fachverfahren“ und „Gesundheitskarte“ favorisiert. ISIS-MTT wird in Deutschland auf breiter Basis von Zertifizierungsdiensteanbietern (ZDAs) und Entwicklern von Anwendungen unterstützt.

Die European Bridge-CA mit *TELETRUST* Deutschland e.V. als Betreiber der Dienstleistung stellt über einen zentralen Vertrauensanker ein Infrastrukturnetzwerk zwischen Wirtschaft und Verwaltung zur Verfügung.

Das Signaturlösungsmodell, eine Public-Private-Partnership von Politik und Wirtschaft im Rahmen der e-Government-Initiative „BundOnline 2005“, dient der Förderung von interoperablen Infrastrukturen und Dienstleistungen und betrachtet u.a. das Thema Geschäftsmodelle, dem in der Diskussion der vergangenen Jahre zunächst kaum Aufmerksamkeit geschenkt wurde. Trotz der genannten gemeinsamen Initiativen von Wirtschaft und Verwaltung ist es bisher nicht gelungen, dieser Technologie den Durchbruch im Massenmarkt zu ermöglichen. Dies ist darauf zurückzuführen, dass



Dipl.-Ing.  
Detlef Dienst

Studium der Elektrotechnik – Fachrichtung Nachrichtentechnik, seit Juli 1994 im Fachgebiet IT-Sicherheit tätig, Leitung des Geschäftsbereichs Trust Center Solutions und Security Products, ITC-Security, Systems Integration, T-Systems International GmbH

E-Mail: Detlef.Dienst@t-systems.com

- der wirtschaftliche Nutzen von PKI-Lösungen noch nicht auf breiter Basis nachgewiesen werden konnte,
- die Akzeptanz elektronischer Signaturen an den Kosten gar nicht oder nur unzureichend beteiligt worden sind,
- die Sensibilisierung der Anwender für die Notwendigkeit des Einsatzes neuer Sicherheitsverfahren in offenen Netzen, insbesondere des Internets, noch nicht durchgehend gegeben ist,
- Anwendungsentwickler und ZDAs darauf warten, dass jeweils die andere Seite in Vorleistung geht und dem Massenmarkt preisgünstig PKI-Lösungen zur Verfügung stellt („Henne-Ei-Problematik“).

## PKI-Lösungen für große Anwendergruppen

Um PKI-Lösungen auf breiter Basis zum Durchbruch zu verhelfen, ist es notwendig, in einer konzertierten Aktion von Wirtschaft, Bund und Ländern die „kritische Masse“ zu überschreiten; das bedeutet eine große Anzahl von Anwendern mit Komponenten zur elektronischen Signatur und Verschlüsselung (Chipkarten, Schlüsselzertifikate) auszustatten und diese Komponenten in für den „Normalbürger“ bedienbare und nutzbringende Anwendungen zu integrieren. Die Etablierung dieser Lösungen in Anwendungen und Geschäftsprozessen für große Nutzergruppen ist Voraussetzung und Chance für eine Integration der PKI-Technologie in ein breites Spektrum von elektronischen Geschäftsprozessen in Wirtschaft und Verwaltung und zwischen Bürgern und Verwaltung.

### Initiativen des Bundes

Die Bundesregierung plant mit verschiedenen Kartenprojekten, Verwaltungsabläufe zu vereinfachen und Kosten einzusparen.

Das JobCard-Fachverfahren, die elektronische Gesundheitskarte und der elektronische Personalausweis sind Teil des 2003 beschlossenen „Aktionsprogramms Informationsgesellschaft Deutschland 2006“ der Bundesregierung mit dem Ziel, einen „Masterplan für Deutschlands Weg in die Informationsgesellschaft“ vorzugeben.

Die Einführung des JobCard-Fachverfahrens ist für das Jahr 2006 vorgesehen und hat das Ziel, alle sozialversicherungspflichtigen Beschäftigten (ca. 40 Mio) mit einer Signaturkarte auszustatten, welche u.a. die elektronische Übermittlung von Arbeits- und Entgeltbescheinigungen an die Arbeitsämter ermöglicht. Das Einsparpotential durch den Wegfall von ca. 60 Mio papiergebundenen Bescheinigungen zum Informationsaustausch zwischen Arbeitgebern und Verwaltung beträgt nach Schätzungen der ITSG GmbH rund 500 Mio EUR pro Jahr. Das Gesetz zum JobCard-Fachverfahren soll noch in diesem Jahr verabschiedet werden. Z.Zt. ist die Finanzierungsfrage zur Ausrüstung der Beschäftigten mit den Karten jedoch noch nicht geklärt.

Bei einer Marktdurchdringung in der genannten Höhe von ca. 40 Mio Signaturkarten wäre die sogenannte „kritische Masse“ überschritten und der Weg frei für die Integration von PKI-Lösungen in bürgernahe elektronische Geschäftsprozesse und Basis für eine Vielzahl von Anwendungen.

## Maßnahmen zur Realisierung von PKI-Lösungen für große Anwendergruppen

Technische Interoperabilität kann man heute als gegeben annehmen; Bundesregierung und Wirtschaft haben mit ISIS-MTT gemeinsam die notwendigen Maßnahmen ergriffen und umgesetzt. Auch das Thema „Anwendungsschnittstelle zur Chipkartenintegration“ wird kein Hinderungsgrund sein. Im Sinne von juristischer Interoperabilität regeln die Richtlinie der Europäischen Union und das Signaturgesetz den Umgang mit qualifizierten Signaturen.

Die Anbieter von PKI-Lösungen haben seit Jahren ihre Kompetenz erfolgreich unter Beweis gestellt. Die Deutsche Telekom AG ist 1999 als erster akkreditierter ZDA auf den Markt gegangen und betreibt bereits seit 1996 erfolgreich eine Unternehmens-PKI.

Schwieriger zu lösen ist die Frage der Finanzierung. Nur wenn auch diese geklärt ist, können PKI-Lösungen erfolgreich realisiert werden. Anders als bisher sollten nicht nur die Anbieter von PKI-Lösungen und die Anwender (Inhaber von Schlüsselzertifikaten) die Kosten tragen, sondern alle Nutzer an den Kosten beteiligt werden. Dies sind in erster Linie diejenigen, welche, um als Beispiel die Anwendung der digitalen Signatur zu betrachten, den Nutzen aus der Prüfung der Gültigkeit und Authentizität der Signatur ziehen. Das bedeutet konkret, die Gültigkeitsauskunft (Validierung) zu bepreisen. Nichts anderes geschieht im elektronischen Zahlungsverkehr; die Händler als Akzeptanten einer Kreditkarte zahlen ebenfalls einen Beitrag an den Kartenherausgeber.

Einer der größten Kostenfaktoren bei PKI-Lösungen – insbesondere wenn die Anforderungen des SigG zu berücksichtigen sind – ist die Identifikation und Registrierung der Anwender. Hierbei sollte man – wann immer möglich – auf vorhandene Datenbestände zurückgreifen dürfen. Diese existieren in guter Qualität u.a. auf Seiten der Verwaltung (Einwohnermeldeämter), Arbeitgeber (Mitarbeiterdaten) und in der Wirtschaft allgemein im Rahmen von Kundendatenbanken. Die Anforderungen an die Identifikation und Registrierung von Kunden wird zum Beispiel durch das Geldwäschegesetz und das Telekommunikationsgesetz gesetzlich geregelt. Für die Aufbereitung dieser Daten ergeben sich folgende Leitsätze:

- Festlegung der technischen Rahmenbedingungen (ISIS-MTT)
- Festlegung der juristischen Rahmenbedingungen (elektronische Signaturen)
- Daten zur Benutzerregistrierung können vor der Ausgabe der Chipkarten und der Ausstellung der Schlüsselzertifikate gesammelt und bereitgestellt werden
- Beteiligung aller Nutzer von PKI-Lösungen an den Kosten (Kostenpflichtige Überprüfung von Schlüsselzertifikaten)
- Distribution von Kartenlesern, Chipkarten und Software an die Endverbraucher über einen fachkundigen Flächenvertrieb
- Bedarfsgerechte stufenweise Einführung (z.B. elektronische Gesundheitskarte, JobCard-Fachverfahren)

Gelingt es, mit Hilfe der genannten Maßnahmen robuste PKI-Lösungen für große Anwendergruppen im Markt zu etablieren, ist eine Erhöhung der Sicherheit in offenen Netzen und das Freisetzen von Kostensenkungspotentialen durch die Ablösung papiergebundener durch elektronische Kommunikation erreichbar.

# Biometrie Quo Vadis

## Erfolgsstory oder Mängelbericht – was war, was wird

Astrid Albrecht

*Leiterin der AG „Biometrische Identifikationsverfahren“  
und des AK „Rechtsfragen der Biometrie“*

*Mitarbeit in der AG „Juristische Aspekte einer verbindlichen Kommunikation“*

*Arbeitsfeld im Schnittstellenbereich Technik und Recht, rechtliche und soziale Aspekte neuer Informationstechnologien, elektronischer Rechts- und Geschäftsverkehr, mit regelmäßigen Veröffentlichungen und Vortragstätigkeit; Juristische Dissertation „Biometrische Verfahren im Spannungsfeld von Authentizität im elektronischen Rechtsverkehr und Persönlichkeitsschutz“*

*Aktive Mitarbeit im DIN-NI 37 zu WG 6 „Cross-Jurisdictional and Societal Aspects of Implementation of Biometric Technologies“*

*Mitbegründerin des European Biometrics Forum (EBF) als Folge des EU-Projekts BIOVISION*

*Kooperation mit BITKOM, BWG (UK), DfK, EBF, Vfs, ZVEI und weiteren*



Dr. jur.  
Astrid Albrecht

befasst sich beim Bundesamt für Sicherheit in der Informationstechnik (BSI) im Bereich Schlüsseltechnologien mit Schnittstellenfragen der IT-Sicherheit und juristischen Aspekten, schwerpunktmäßig zu Biometrie und elektronischen Signaturen.

E-Mail: astrid.albrecht@bsi.bund.de

## Biometrie zwischen Anspruch und Wirklichkeit

### Die Realität

In den vergangenen 15 Jahren hat sich die Biometrie aus ihrem vorwiegend wissenschaftlichen Forschungsdasein entwickelt und im Wettbewerb laufen gelernt. Allen Unkenrufen zum Trotz: Ja, es gibt sie, die funktionierenden biometrischen Anwendungen, auch in Deutschland. Inzwischen kann im Biergarten mit Fingerabdruck bezahlt oder das Video in der Videothek ausgeliehen werden. Trustcenter, Banken und Atomkraftwerke setzen biometrische Verfahren ein, um sicherzustellen, dass wirklich nur befugte Personen Zutritt zu sicherheitssensiblen Bereichen erhalten. In Krankenhäusern unterschreibt das Personal auf Tablet PCs.

Allerdings gilt nach wie vor, dass solche alltäglichen Anwendungen mit Biometrie immer noch ein Nischendasein fristen und vorwiegend ohne öffentlichkeitswirksame Darstellung stattfinden. Die Marktdurchdringung fällt schwer, sei es, weil in vielen Anwendungen die herkömmlichen, personenbezogenen Authentisierungsverfahren ausreichend gut funktionieren, sei es, weil der Bedarf an personengebundener Authentifizierung noch nicht erkannt wurde. Betriebswirtschaftliche Marktmechanismen wie Kosten und Nutzen erschweren – wie bei allen neuen und zunächst, im Vergleich zu den althergebrachten Mechanismen, kostenintensiveren Technologien – die Überzeugung des Anwenders, sich auf das „Abenteuer Biometrie“ einzulassen. Hinzu kommt bei biometrischen Anwendungen, dass hier besondere datenschutzrechtliche Voraussetzungen einzuhalten sind.

### Markt der (Un-?) Möglichkeiten

Nach dem 11. September 2001 hatte sich scheinbar der Markt der Möglichkeiten geöffnet. Plötzlich war die Biometrie für hoheitliche Anwendungen, insbesondere im Bereich der Terrorismusbekämpfung, salonfähig. Internationale Organisationen wie die UN-Organisation ICAO haben ihre Aktivitäten für biometrische Verfahren bei maschinenlesbaren Reisedokumenten verstärkt. Nationale Regierungen formulieren ebenfalls Anforderungen und geben entsprechende Projekte in Auftrag. Die Erkenntnisse sollen dazu dienen, auch die für die jeweilige Anforderung am ehesten geeigneten Verfahren zu identifizieren. Der verstärkte Blick auf hoheitliche Anwendungen, die naturgemäß den Schwerpunkt auf den Aspekt der wirksamen Unterstützung einer sicheren Zuordnung zwischen Ausweisdokument und Identität einer Person legen, hat auch die Hersteller vor neue Anforderungen gestellt.

Entsprechende Projekte sind zudem aus Sicht der Anbieter durchaus ambivalent: zum einen dienen sie dazu, das eigene Produkt weiterzuentwickeln, zum anderen den Markt strategisch zu erschließen. Allerdings zeigen selbst sorgfältig geplante und durchgeführte Projekte Schwachstellen und Sicherheitslücken auf. Hier hilft nur der Blick nach vorn: was kann wie optimiert werden, um letztlich allen Beteiligten zu nutzen? Die Erkenntnis, dass manche Lösungen (jedenfalls zum gegenwärtigen Zeitpunkt noch) nicht dazu geeignet sind, bestimmte Probleme zu lösen, hilft – neben dem dadurch identifizierten Optimierungspotenzial der Produkte – unwirtschaftliche Entscheidungen zu vermeiden.

## Standardisierung und Zertifizierung

Bei ISO wurde mit JTC1/SC37 ein neues Gremium für die anwendungsbezogene interoperable Standardisierung biometrischer Verfahren eingerichtet. Nationale Spiegelgremien folgten. Wie in anderen Bereichen auch stößt die Standardisierung aber nicht nur dort auf Umsetzungsprobleme, wo der Bereich der proprietären und damit wettbewerbsrelevanten Spezifikationen, ganz zu schweigen von patentrechtlichen Fragestellungen, biometrischer Produkte berührt wird. In technischer Sicht machbare Anforderungen lassen sich oft nicht unmittelbar in Spezifikationen umsetzen. Folglich wird uns die biometrische Standardisierung noch länger beschäftigen.

Schließlich wächst auch der Bereich der zertifizierten Produkte. Evaluerte Biometrie-Produkte werden in Zukunft den Markt der Möglichkeiten erweitern, da der Anwender dann von vornherein ein gewisses Maß an Vertrauen in das Produkt haben kann.

## Biometrie in aller Munde

Vermehrt formulierte Anforderungen und Einsatzszenarien hoheitlicher Anwender haben einen weiteren Effekt: Biometrie ist in aller Munde. Die Präsenz in der Presse hat stark zugenommen, seit sich nicht nur ICAO, sondern auch ISO, die EU-Kommission und nationale Regierungen verstärkt mit Biometrie beschäftigen. Sowohl Fachpresse als auch Tageszeitungen und nicht technisch ausgerichtete Magazine veröffentlichen regelmäßig zumindest kurze Berichte über Biometrie. Die dadurch allgemein entstandene Transparenz zu Biometrie auch in der nicht-fachbezogenen Bevölkerung ist durchaus zu begrüßen. Die Berichterstattung hat allerdings von nüchterner und zutreffender Information bis hin zu Euphorie oder Panikmache alles zu bieten.

## Die „Biometriker“ von TELETRUST

Die Arbeitsgruppe 6 von TELETRUST agiert seit 1997 im Bereich der Biometrie. Einzigartig ist wohl die interdisziplinäre Besetzung dieser mitgliederstarken AG. Aktuelle Entwicklungen der Technik sowie der rechtlichen und sozialen Anforderungen werden hier nicht nur im Sinne des informativen Erfahrungsaustauschs beobachtet, sondern aktiv begleitet. Dies zeigt sich nicht zuletzt in den beiden Biometrie-Sachstandsberichten des Büros für Technikfolgenabschätzung beim Deutschen Bundestag (TAB), an denen jeweils aktive AG6-Mitglieder als Gutachter fungierten – vom Unabhängigen Landeszentrum für Datenschutz über den Verbraucherzentrale Bundesverband bis zu unterschiedlichen

wissenschaftlichen Einrichtungen und Konsortien aus Systemintegratoren und Herstellern.

In dem vom Bundeswirtschaftsministerium geförderten Projekt BioTrusT wurde von 1999-2002 erstmals eine interdisziplinäre Sichtweise auf die Biometrie realisiert. Die Untersuchung verschiedener Biometrien, die direkte Einbindung der Hersteller und die erstmalige Implementierung der BioAPI-Schnittstelle weltweit machen die Praxisrelevanz des Projekts deutlich, das auch international auf erhebliches Interesse stieß; so ist der BioTrusT-Bericht auch in englischer Fassung erhältlich. Die hier erzielten vielschichtigen Ergebnisse sind nicht nur in den Kriterienkatalog der AG6 eingeflossen sondern bildeten u.a. auch das Fundament der Beteiligung der AG6 an dem EU-Projekt BIOVISION und der durch die AG6 erfolgte Mitgründung des European Biometrics Forum (EBF). Folgeprojekte wie BIOSEC auf europäischer Ebene werden weiter begleitet.

Die erfolgreiche Ausrichtung der AG6 auf die interdisziplinäre Sichtweise biometrischer Verfahren wird durch verschiedene Kooperationen ergänzt – innerhalb von TELETRUST etwa mit der AG1 in rechtlicher Hinsicht und der AG7 mit Blick auf PKI und nach außen in der Zusammenarbeit mit anderen Verbänden wie z.B. VfS, BITKOM, DfK. Die dadurch mögliche Richtigstellung der erwähnten Falsch- oder Fehlberichterstattung in den Medien ist ein positiver Nebeneffekt solcher Aktivitäten.

## Ausblick – Zuckerbrot und Peitsche

Die Mängelberichte hinsichtlich Leistungsfähigkeit und Sicherheit werden wohl auch in Zukunft Teil der Erfolgsstory Biometrie bleiben. Viele, nicht nur technische Fragen der Biometrie sind erst teilweise gelöst. Ganz nach dem Motto „Wer sucht, der findet“ ergeben sich bei der Lösung der aktuell anstehenden Probleme vor allem im Bereich der Standardisierung neue Aufgabenstellungen, die nicht von heute auf morgen gelöst werden können. Es besteht weiterhin Forschungs- und Entwicklungsbedarf, was sowohl private als auch hoheitliche Anwendungen angeht. Die Bedürfnisse der einzelnen Anwendungsbereiche sind so vielfältig und unterschiedlich wie die angebotenen Biometrien und bedürfen individuell angepasster Konzepte.

Viele Probleme sind aber auch bereits gelöst, die marktverfügbaren biometrischen Produkte haben erhebliche Fortschritte gemacht. Außerdem gilt: Die Anforderungsanalyse des einzelnen Anwenders wird stets Spezifikation und Implementation des biometrischen Produkts bestimmen.

Das zukünftige Arbeitsprogramm der Biometrie gibt also durchaus zu Optimismus Anlass. Die Überwindung der teilweise überzogenen Erwartungen und unrealistischen Marktprognosen einerseits und der Feststellung ihrer „absoluten Unbrauchbarkeit“ andererseits durch die Rückkehr zu einer neuen Sachlichkeit hat der Biometrie gut getan; sie wird zunehmend nicht mehr als Allheilmittel angepriesen. Statt dessen konzentriert man sich mit Realitätssinn auf solche Anwendungen, die eine biometrische Authentisierung sinnvoll in einen Prozess einbinden und sucht nicht mehr krampfhaft nach nicht vorhandenen Problemen für eine allein selig machende Lösung.

Auch in Zukunft wird es weiterhin auf eine vertrauensvolle Zusammenarbeit aller Beteiligten ankommen – die AG6 von TELETRUST ist hierfür nach wie vor die richtige Plattform.

# Unterschriften im digitalen Zeitalter

Vom Datenträger Papier bis zur Erfassung auf Tablet PCs

Jörg-M. Lenz

*Fachbuch in Zusammenarbeit mit Dr. Christiane Schmidt  
„Elektronische Signatur – eine Analogie zur eigenhändi-  
gen Unterschrift? (2. Auflage, 2004, Deutschen Sparkas-  
senverlag)“*

*Mitarbeit in AG „Biometrische Identifikationsverfahren“ –  
und AG „Juristische Aspekte einer verbindlichen Kommu-  
nikation“ insbesondere für Presse- und Öffentlichkeitsar-  
beit*

*Zahlreiche Veröffentlichungen in Fachzeitschriften und  
diverse Vorträge*

*Beteiligung in Projekten wie BioTruST und Biovision, Er-  
stellung der Biometrie-Landkarte Deutschland*

*Mitarbeit in Arbeitskreisen bei BITKOM zur Elektroni-  
schen Signatur und Biometrie sowie bei der Initiative D21*



Dipl. Betriebswirt  
Jörg-M. Lenz

Befasst sich seit 1999 als „Man-  
ager für Marketing und Öffentlich-  
keitsarbeit“ beim Spezialisten zur  
Prüfung von Unterschriften –  
SOFTPRO – mit der Förderung  
von Verständnis und Akzeptanz  
biometrischer Verfahren und  
korrespondierender Technologien.

E-Mail: jle@softpro.de

## Eigenhändige Unterschriften für Authentizität und Integrität auch digitaler Prozesse

### Das Comeback der Unterschrift

Authentizität der Daten ist eines der Fundamente für das Vertrau-  
en in den elektronischen Geschäftsverkehr. Nichts ist leichter, als  
an ungesicherten elektronischen Daten Veränderungen vorzuneh-  
men, ohne dabei Spuren zu hinterlassen. Dabei ist es auch heute  
noch wichtig, Vorgänge reversionssicher zu dokumentieren und  
zweifelsfrei zuzuordnen, damit sie nachträglich nicht abgestritten  
werden können.

Überraschend ist die veränderte und doch irgendwie gleich ge-  
bliebene Bedeutung, die heute wieder der eigenhändigen Unter-  
schrift in digitalen Prozessen beigemessen wird: Als in den neun-  
ziger Jahren das erste Signaturgesetz in Deutschland vorbereitet  
wurde, sollte die (papiergebundene) eigenhändige Unterschrift in  
elektronischen Prozessen vollständig durch „digitale Signaturen“  
ersetzt werden. Dabei setzte man insbesondere auf asymmetrische  
kryptographische Verfahren in Verbindung mit Chipkarten. Die  
Authentifizierung des Nutzers gegenüber der Chipkarte erfolgte  
durch Geheimzahlen (PIN), also nach dem Prinzip „Besitz und  
Wissen“ wie bei den allseits bekannten EC-Karten. Die Grenzen  
dieses Verfahrens zeigten sich spätestens im Sommer 2004: In  
zuvor ungekannter Häufung traten Fälle des Missbrauchs von  
Geheimzahlen durch Ausspähen und „Social Hacking“ auf. Ein  
weiteres Problem ist die begrenzte Merkfähigkeit der Anwender:  
Vergessene Passwörter kosten die Unternehmen im Jahr Hunderte  
von Euro pro Mitarbeiter aufgrund unproduktiver Arbeitszeiten.  
Kein Wunder also, dass andere Verfahren ohne diese Nachteile  
immer mehr an Boden gewannen. Eine ganze Gruppe davon  
stützte sich wieder auf bekannte Vorgänge aus dem papiergebun-  
denen Geschäftsverkehr: Die elektronische Renaissance der Un-  
terschrift brach an.

### Gewohnte Willenserklärung nutzen

Je eher die Technik gewohnte Vorgehensweisen unterstützt desto  
eher hat sie eine Chance, im Alltag akzeptiert zu werden. Viele  
Nutzer wollen ihre Dokumente nach wie vor „schwarz auf weiß“.  
Dabei möchten sie auf ein gewohntes Merkmal zur Authentifizie-  
rung nicht verzichten – ihre eigenhändige Unterschrift.

Zurecht: Denn eine eigenhändige Unterschrift dokumentiert eine Willenserklärung und sie kann nicht ohne das Einverständnis ihres rechtmäßigen Inhabers abgegeben werden.

Die Entwicklung neuer Verfahren zur Migration des bisherigen, schriftlich auf Papier dokumentierten Handelns in die elektronischen Verfahren hat zu verschiedenen Ergebnissen geführt. Bekannt sind elektronisch erzeugte Zusätze, die als zweidimensionaler Strichcode mit dem Dokument ausgedruckt werden und zur Überprüfung dessen Echtheit dienen können (z.B. SeCrypt), die Verwendung von Datensätzen (Templates), die aus Merkmalen der eigenhändigen Unterschrift extrahiert werden und als Schlüssel für kryptographische Verfahren dienen (z.B. von SignaturePerfect), eine mobile Signatur-Plattform (TruPoSig vom Fraunhofer Institut SIT, entstanden aus dem BMWA-Projekt „VERNET“) oder Verfahren zum automatischen Vergleich von Unterschriften (z.B. von Softpro). Letztere dienen vorwiegend der Authentisierung und werden – wie Fingerbild- oder Iriserkennung – der Biometrie zugeordnet. Sie werden im Folgenden weiter behandelt.

## Unterschrift belegt Authentizität

In vielen Fällen, wo heute elektronische Formulare ausgedruckt werden, um auf Papier die Unterschrift zu erfassen, wäre es sinnvoller, die Unterschrift schon während des Schreibens zu digitalisieren. Dabei spielt es eine entscheidende Rolle, ob die Unterschrift in einer Qualität erfasst wird, die auch einen späteren Vergleich ermöglicht. Dies betrifft sowohl die zu prüfende Unterschrift als auch die Referenz-Unterschrift, gegen die geprüft werden soll. Es ist zusätzlich sicherzustellen, dass bereits bei der Erfassung der Unterschriftsdaten feststeht, wie im Zweifelsfall eine Unterschriftenprüfung erfolgt, d.h. mit welchen Algorithmen.

## Kryptographie schützt Integrität

Elektronische Daten vor unerkannter Manipulation zu schützen ist einer der wichtigsten Aufgaben, um Vertrauen in elektronische Geschäftsprozesse zu schaffen. Die untrennbare Verbindung von Authentisierungsdaten, wie der Unterschrift, mit dem zugehörigen elektronischen Dokument ist mit kryptographischen Verfahren umsetzbar.

## Mehr Informationen als auf dem Papier

Die Digitalisierung der Unterschrift während des Schreibens ermöglicht im Vergleich zur „Speicherung“ auf Papier ein einfach nachprüfbares, hohes Sicherheitsniveau. Mit einer Reihe von Schreibtablets und Tablet PCs können Signale der Schreibbewegung erfasst werden, die im bloßen Unterschriftsbild nicht wahrgenommen werden können, etwa die sich ständig während der Unterschriftsleistung ändernden Geschwindigkeiten und Druckintensitäten, mit denen der Stift über die Unterlage fährt. Aus diesen Signalen bestimmt sich zu einem großen Anteil die Einzigartigkeit einer Unterschrift. Gespeichert werden kann ein Datensatz der Unterschrift, der aus zwei Elementen besteht: Einem statischen Bild der Unterschrift und ihren dynamischen (biometrischen) Merkmalen.

## Unterschriften hochwertig erfassen

Für Verfahren der biometrischen Unterschriftserkennung sind eine ausreichend hohe Anzahl Signalerfassungen sowie eine sehr gute Ortsauflösung während des Schreibvorganges erforderlich, sie haben nichts mit den Geräten zu tun, auf denen wir an der Tür den Empfang von Paketen quittieren.

Bei der Prüfung von Unterschriften auf dem Papier werden die unterschiedlichen Schreibdrücke im Verlauf einer Unterschrift von Schriftensachverständigen mit dem Mikroskop analysiert. Im biometrischen System werden sie bereits bei der Unterschriftsaufnahme digital dokumentiert.

Aber nicht nur die Aufnahme- und Verarbeitungsqualität der zu prüfenden Unterschrift ist wichtig. Leider noch zu oft werden der Leistungsfähigkeit biometrischer Systeme a priori durch ein zu oberflächliches Enrolment, also der Aufnahme und zuverlässigen Speicherung von Referenzdaten – der Masterunterschrift – unnötig enge Grenzen gesetzt.

## Einsatzbeispiel: Klinikum Ingolstadt

Das Klinikum Ingolstadt verwendet für die „Mobile Datenerfassung in der Notaufnahme (DNA)“ die eigenhändige Unterschrift in Verbindung mit einem Verschlüsselungsverfahren. Das Klinikum entwickelte gemeinsam mit Siemens Information and Communication Networks (ICN) eine Lösung für Tablet PCs und ersetzte dabei die Papierdokumente durch XML-basierte Formulare. Diese werden mit Microsoft Office InfoPath 2003 ausgefüllt und auf den Windows SharePoint Services unter Microsoft Windows Server 2003 gespeichert. Jetzt können Ärzte ihre Formulare auf dem Tablet PC handschriftlich ausfüllen. Zur Gewährleistung der Authentizität und Integrität erstellter Dokumente werden Daten der eigenhändigen Unterschrift erfasst und geprüft. Damit reduziert das Krankenhaus Leistungen und Zeiten, die nach den seit 2004 geltenden Fallpauschalen nicht abrechnungsfähig sind und kann die Pflege der Patienten optimieren. Der Projektverantwortliche im Klinikum – Thomas Kleemann – resümiert: „Wir bevorzugen die eigenhändige Unterschrift zur Gewährleistung der Authentizität und Integrität von Dokumenten. Sie ist für Ärzte, Krankenhauspersonal und Patienten ein vertrauter Vorgang und nicht erklärungsbedürftig. Handschriftliche Eingabe und eigenhändige Unterschrift bilden eine perfekte Synthese in der Neugestaltung mobiler Arbeitsabläufe. Der Anwender empfindet keinerlei Unterbrechung in seinen gewohnten Prozessen“.

## SmartCards zur Referenzspeicherung

SmartCards sind eine sichere Alternative als Speichermedium für biometrische Referenzdaten (z.B. von Unterschriften), wenn der Zugriff auf eine zentrale Datenbank nicht erwünscht oder nicht möglich ist. Dies hat TELETRUST in seinem Projekt BioTrust gezeigt, wo Unterschriften erstmals zur Freischaltung von Funktionalitäten der SmartCards genutzt wurden. Verschiedene Smart Card Anbieter ermöglichen mittlerweile z.B. die Freischaltung elektronischer Signaturen durch die Unterschrift (z.B. T-Systems/TeleSec, IBM und Signtrust).

So schließen sich also Chipkarten-Anwendungen und Biometrie keineswegs aus – sie ergänzen sich in vielen Fällen.

# IT-Sicherheit und Mobilität

## Neue Herausforderungen an die IT-Sicherheit

Stephan Wappler

### *Kernkompetenz:*

*Sicherer Datenaustausch basierend auf Standards to-End und to-Site, organisationsintern und -übergreifend, Einbindung mobiler Systeme in Organisationen, Verzeichnisdienstkonzepte und Umsetzung, Validierungstechniken, Sicherheitsorganisation*

### *Networking:*

*Aktive Mitarbeit in den folgenden TTT-Arbeitsgruppen:*

*AG „Public Key Infrastrukturen“*

*AG „Onlineprozesse und Identitätsmanagement“*

*Technische Arbeitsgruppe European Bridge-CA*

*Für TELETRUST Leiter der Industrie-offenen, temporären Arbeitsgruppe:*

*„Kritische Elemente einer Infrastruktur, Bereich PKI und Identitätsmanagement“ im Rahmen des Projektes GuT der Selbstverwaltung*

*Mitarbeit im Messaging Forum der The Open Group Internationaler Testkoordinator und Teilnehmer der Secure Messaging Challenge des Messaging Forums Teilprojektleiter für das Workpackage Security im durch die EU-Kommission geförderten Forschungsprojekt „Open Mobile Radio Access Network“ (whyless.com)*



Diplom Mathematiker (FH)  
Stephan Wappler

Abschluss Studium 1999  
Seit 1999 bei noventum consulting  
(ehemals Lynx-ctr, Münster) als  
Consultant im Bereich Netzwerke  
/ IT-Sicherheit tätig.

E-Mail: [stephan.wappler@noventum.de](mailto:stephan.wappler@noventum.de)

## Im Wandel der Zeit

Dem Wandel der Gesellschaft von einer Produktions- und Konsumgesellschaft hin zu einer Informationsgesellschaft ist natürlich auch die Informationstechnik unterworfen. Stand gestern noch das Produkt im Mittelpunkt, so ist es heute die Verfügbarkeit von Informationen beziehungsweise Diensten.

Nicht nur bei Wirtschaftsorganisationen sondern auch bei Privatpersonen entsteht der Wunsch und die Notwendigkeit, überall und jederzeit Informationen bzw. Dienste verfügbar oder auf diese Zugriff zu haben.

## Arten von Mobilität

Diese Wünsche und Notwendigkeiten haben natürlich einen immensen Einfluss auf die Architektur und den Betrieb von IT-Lösungen in Organisationen oder bei IT-Dienstleistern. So verschieden wie die Definition von „Mobilität“ von den Anwendern verstanden wird, so verschieden sind die Anforderungen an die Verfügbarkeit von Informationen oder Diensten.

## Offline Verfügbarkeit

Einige Anwender stellen die Anforderung, für sie relevante Informationen auf einem mobilen Gerät zu speichern und nur gelegentlich diese Informationen zu aktualisieren bzw. auf entsprechende Dienste zuzugreifen. Beispiele für derartige Informationen bzw. Diensten sind:

- Persönliche oder Gruppenkalenderinformationen
- Adressdatenbanken
- E-Mail-Datenbanken
- Zeiterfassungsinformationen
- Auftragsinformationsdatenbanken für den Außendienst
- usw.

## Online Verfügbarkeit

Jedoch nicht jede Information kann lokal gespeichert werden oder ein sporadischer Zugriff auf entsprechende Dienste, je nach Verfügbarkeit, ist für den Anwender ausreichend. Weiterhin ist eine lokale Speicherung von Informationen auf mobilen Systemen nicht immer sinnvoll, da neue Problematiken wie zum Beispiel die lokale Datensicherung gelöst werden müssen. Darüber hinaus gibt es Informationen, bei denen die Priorität auf der Aktualität liegt und es gibt Dienste, die genau für die Bereitstellung solcher

Informationen betrieben werden. Zu diesen Informationen bzw. Diensten gehören:

- Nachrichtenticker
- Börsenticker
- Zugriff über Organisationsportale auf
  - ◆ Finanzdaten von Organisationen
  - ◆ Organisations-E-Mail-Accounts
  - ◆ Managementsysteme
- Instant Messaging
- Verzeichnisdienste
- Validierungsdienste
- Aktualisierungsdienste
- usw.

## In Kombination

Oftmals ergeben sich auch Kombinationen aus Offline und Online Verfügbarkeit. Betrachtet man als Szenario den reisenden Geschäftsmann, der noch vor dem Abflug im Terminal seine neusten E-Mails auf sein Notebook geladen hat und jetzt während des Fluges seine E-Mail-Korrespondenz abarbeitet, so wird dies ersichtlich. Die E-Mails sind Offline gespeichert und darunter befinden sich auch digital signierte Mails. Um die Signatur zu prüfen, benötigt er einen Online Dienst, der ihm die entsprechende Auskunft über die Gültigkeit der Signatur gibt. Weiterhin möchte er einem Geschäftspartner eine E-Mail mit vertraulichen Daten senden. Aus diesem Grund entscheidet er sich für eine verschlüsselte E-Mail. Da er zwar die E-Mailadresse im lokalen Adressbuch gespeichert hat, jedoch das entsprechende Verschlüsselungszertifikat abgelaufen ist, benötigt er Zugriff auf einen Verzeichnisdienst, um von dort ein aktuelles Zertifikat beziehen zu können. Unter den eingegangenen E-Mails befindet sich auch ein Warnhinweis über einen neuen Virus vom seinem Organisationsadministrator. Um sich gegen den entsprechenden Schädling abzusichern, ist eine Aktualisierung der Antivirensoftware notwendig und auch dies erfordert wiederum einen Online Dienst. Da zurzeit keine Online Dienste verfügbar sind und auch der Akku des Notebooks keine Reserven mehr hat, entschließt sich der Geschäftsmann nach Sichtung aller eingegangenen E-Mails, seine formulierten E-Mails nach Ankunft in der Organisation aus dem lokalen Netzwerk zu versenden.

## Die Herausforderung

Wie an diesem kurzen Beispiel unschwer ersichtlich wird, steht die IT-Sicherheit mit der Zunahme der Mobilität von Personen und Informationen vor einer großen Herausforderung. Die über einen langen Zeitraum sorgsam entwickelten und umgesetzten Sicherheitsarchitekturen für stationäre Systeme müssen innerhalb kürzester Zeit an die neuen Anforderungen der Mobilität angepasst werden, ohne das Sicherheitsniveau zu schwächen. Zu den Herausforderungen, die bewältigt werden müssen, gehören unter anderem:

- Patchmanagement (auch für mobile Clients)
- Policy und Richtlinien Enforcement
- Einsatz von mobilen Geräten, z.B. PDA's, Mobiltelefone
- Einsatz neuer Interfaces und Übertragungstechniken, z.B. WLAN, Bluetooth, GPRS/UMTS
- Administration mobiler Clients
- Lokale Datensicherheits- und Sicherungskonzepte
- Zugriffssicherungsmechanismen und Rollenmanagement
- Sichere Kommunikation, Speicherung und Datentransfer
- Viren- und Contentmanagementlösungen
- Entwicklung und Umsetzung von Migrations- und Organisationskonzepten
- usw.

Diesen neuen Herausforderungen müssen auch entsprechende zentrale Infrastrukturen, wie zum Beispiel Bridge Infrastrukturen sich stellen und bewältigen.

## Die Kompetenz von TELETRUST

Der Kompetenzverbund TELETRUST Deutschland e.V. unterliegt auch dem Wandel und muss sich genauso wie die IT-Sicherheit in den einzelnen Organisationen diesen neuen Herausforderungen stellen und anpassen.

In Zukunft ist Kernkompetenz in Spezialbereichen, wie zum Beispiel Zugriffsschutz oder Rollenmanagement genauso gefragt, wie Kompetenz und Know-How für ganzheitliche Lösungsansätze, wie zum Beispiel für die Integration mobiler Anwender und Clients.

Die Kernkompetenz in den verschiedenen Spezialbereichen hat TELETRUST erfolgreich in den vergangenen 15 Jahren schrittweise aufgebaut und in den einzelnen Arbeitsgruppen gebündelt und etabliert.

Die Herausforderung für TELETRUST für die Zukunft besteht darin, dieses Spezialwissen aus den einzelnen Bereichen zusammen zu führen und sich als ganzheitliches Kompetenzzentrum zu etablieren. Mit der auf dem Internen Workshop 2004 besprochenen Möglichkeit von Bereichs- und Themenübergreifenden Projektteams sind die Voraussetzungen geschaffen, sich dieser Aufgabe zu stellen und die Weichen für die Zukunft in die richtige Richtung gestellt.

Die Unterstützung des Wandels zu einer Informationsgesellschaft ist eine gesellschaftspolitische Aufgabe, für die TELETRUST Deutschland e.V. die besten Voraussetzungen mitbringt und in dessen Rahmen der Verein eine wesentliche Rolle einnehmen wird.

Der Anwender hat sich in Zeiten stationärer Systeme kaum Gedanken über die Sicherheit der bereitgestellten Informationen und Dienste gemacht, sondern auf die Echtheit und die bestehenden Schutzmaßnahmen vertraut. Dieses Vertrauen auch für mobile Systeme, Informationen und Dienste zu etablieren und zu rechtfertigen ist eine wesentliche Aufgabe von TELETRUST für die Zukunft.

# Marktgerechte IT-Sicherheitsevaluierung und -zertifizierung

## Facts & Trends in der IT-Sicherheitszertifizierung

Bernd Kowalski

*Bernd Kowalski war von 1982 bis 1990 bei der Deutschen Bundespost für die Entwicklung und Normung neuer TK-Dienstleistungen zuständig.*

*Von 1990 bis 2002 baute er bei der Deutschen Telekom das Produktzentrums TeleSec auf und leitete es, bis er zum BSI wechselte.*



Dipl.-Ing.  
Bernd Kowalski

Bundesamt für Sicherheit in der Informationstechnik – Leitung Aufgabenbereich III (Zertifizierung, Zulassung, Kritische Infrastrukturen, Mobile Security, Abhörsicherheit und Marketing)

E-Mail: bernd.kowalski@bsi.bund.de

### Trends im IT-Sicherheitsmarkt

Die Stagnation des IT-Marktes der letzten beiden Jahre weicht langsam Bewegung. Die fortgeschrittene technische Überalterung in vielen Unternehmen macht sowohl im Hardware- als auch im Softwaresektor Neuanschaffungen unumgänglich. Es werden in diesem Jahr in den Bereichen Software und IT-Dienstleistung in Europa Wachstumsraten zwischen zwei und drei Prozent erwartet.

Noch viel günstiger verhält sich der IT-Sicherheitsmarkt. So hat eine Fokus-Studie gezeigt, dass z.B. Symantic den Umsatz mit Firewalls, Antivirensoftware und Filtering-Systemen im letzten Quartal um fast 30 Prozent steigern konnte, denn bei den international tätigen Unternehmen stehen diese Produkte besonders hoch im Kurs.

Vor dem Hintergrund, dass das vergangene Jahr ein Boomjahr bei den Ausbrüchen von Würmern und Viren (SoBig, Slammer, Nachi, Bugbear, Blaster usw.) war, hat der westeuropäische Markt für die IT-Sicherheit 2003 ein Volumen von rund 2,5 Mrd. Dollar erreicht. Über diese Bedrohungsszenarien hinaus sind die Unternehmen mit der Spam-Problematik einer eingeschränkten Produktivität und potentiellen Imageschäden ausgeliefert.

Nach Erhebungen des US-Marktforschungsinstitutes IDC soll der westeuropäische Security-Markt bis zum Jahr 2008 bei durchschnittlichen jährlichen Steigerungsrate von 15% ein Volumen von über 5 Mrd. Dollar erreichen.

### Trends in der IT-Sicherheitszertifizierung

Im stetigen Wachstum der IT-Sicherheitsbranche der letzten Jahren spiegelt sich auch der Trend der erteilten IT-Sicherheitszertifikate wider.

#### IT-Sicherheitszertifizierung und Prüfkriterien

Ziel der Zertifizierung ist es, IT-Produkte/-Systeme hinsichtlich ihrer Sicherheitseigenschaften transparent und vergleichbar zu bewerten, um

- einerseits Anwendern Detailinformationen und Orientierungshilfen bei der Auswahl von Produkten zu bieten und
- den betreffenden Herstellern eine Bestätigung über die Qualität der Sicherheitseigenschaften ihrer Produkte zu geben.

Die Evaluierung und Zertifizierung von IT-Produkten/-Systemen erfolgt auf Grundlage von Sicherheitskriterien. In Deutschland angewandte Kriterienwerke sind die internationalen Common Criteria (CC)<sup>1</sup> und die europäischen ITSEC<sup>2</sup>.

Die Bedeutung der beiden Kriterienwerke und die Entwicklung der beantragten Zertifizierungen im zeitlichen Verlauf der letzten 4 Jahre sind in Abb. 1 weltweit und für die BSI-Zertifikate dargelegt.

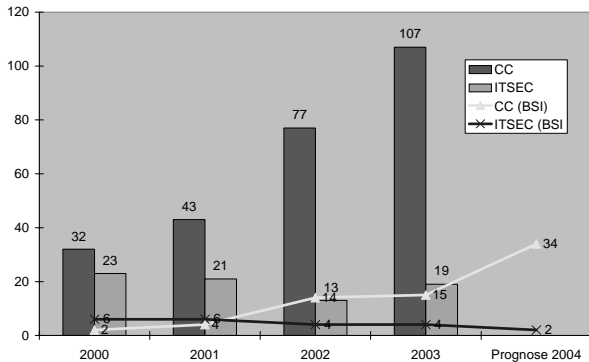


Abb. 1 Anzahl der erteilten Zertifikate weltweit und anteilig vom BSI

Aus den beiden Abbildungen lässt sich deutlich ablesen, dass zwar zum Einen die Bedeutung der europäischen Prüfkriterien ITSEC abnimmt, zum Anderen aber die Anzahl der nach CC erteilten Zertifikate deutlich steigt. Insgesamt spiegelt sich bei weltweit wachsender Anerkennung der Common Criteria als Prüfkriterienwerk der stetig steigende Bedarf an IT-Sicherheitsprodukten im Markt wider.

Die Aufteilung der erteilten Zertifikate nach Produktklassen ergibt, dass der Anteil an SmartCards sowie andere IT-Sicherheits-Produkten jeweils ca. 40 % betragen, hingegen auf die Zertifizierung von Protection Profiles (PP) ein Anteil von ca. 10 %, auf Systeme und Biometrieprodukten jeweils ca. 5 % entfallen.

Die Zertifizierung eines IT-Produkts/-Systems kann vom Hersteller oder Vertreiber eines Produkts oder von einer Bundesbehörde als Anwender bei der Zertifizierungsstelle des BSI beantragt werden.

Seit Dezember 1997 gibt es neben dem BSI in Deutschland private Zertifizierungsstellen, deren Zertifikate unter bestimmten Voraussetzungen vom BSI als Deutsche IT-Sicherheitszertifikate anerkannt werden.

Um die Mehrfach-Zertifizierung des gleichen Produktes zu vermeiden, wurde mit vielen Staaten eine gegenseitige internationale Anerkennung von IT-Sicherheitszertifikaten – sofern sie auf ITSEC oder CC beruhen – unter gewissen Bedingungen vereinbart.

Die Evaluierung der Produkte wird von derzeit 12 nach ISO/IEC 17025<sup>3</sup> lizenzierten Prüfstellen durchgeführt.

## Marktanforderungen an die IT-Sicherheitszertifizierung

Die bisherigen Zertifizierungsverfahren nach CC konzentrieren i.w. auf eine Sicherheitsprüfung in der vertikalen Tiefe und sind sehr zeit- und kostenaufwändig. Deshalb muss der Evaluierungsgegenstand weitestmöglich eingegrenzt werden. Die Prüfung einer Gesamtlösung, wie sie beim Endkunden zum Einsatz kommen muss, ist daher bisher eher die Ausnahme als die Regel.

Für den Hersteller ist eine wichtige positive Wirkung eines Sicherheitszertifikates die Verbesserung der Absatzfähigkeit seines Produktes. Mit Vorprodukt- bzw. Komponentenzertifikaten allein ist dies jedoch nicht zu erreichen. Zertifikate müssen auch dem Endkunden durch eine einfache Botschaft vermittelbar sein.

Die Erweiterung der jetzigen Produktzertifizierung des BSI zielt nicht auf die Abschaffung des bisherigen Verfahrens, sondern auf dessen Ergänzung. Ziel ist, in erster Linie die Verbesserung der IT-Sicherheit in Wirtschaft und Verwaltung durch eine flächendeckende Verbreitung von vertrauenswürdigen, also sicherheitsgeprüften Produkten einzuleiten. Erst in zweiter Linie soll die Festlegung spezifischer Sicherheitslevel (EAL-Stufen nach CC) für Prüfungen im Einzelfall zu einer erhöhten Vertrauenswürdigkeit von IT-Sicherheitsprodukten im Markt beitragen.

Die Erweiterung des Zertifizierungsverfahrens und ihre Durchsetzung im Markt wird in enger Abstimmung mit den Herstellern und im Wesentlichen über Mechanismen des Marktes und des Wettbewerbes erfolgen.

Im Markt werden Produkte nicht nach einem bestimmten vordefinierten Leistungsumfang gestaltet, sondern so, dass sich ein Optimum zwischen den für den Kunden akzeptablen Kosten im Verhältnis zur gelieferten Leistung ergibt. Das Gleiche gilt für die Sicherheitsfunktionalitäten eines IT Produktes: Führt ihre Prüfung zu Kosten, die den Absatz unverhältnismäßig reduzieren, müssen bei der Nachweistiefe (Prüftiefe) bezüglich der Korrektheit und Wirksamkeit der Sicherheitsfunktion entsprechende Abstriche gemacht werden, wenn das Produkt eine Bedeutung im Massenmarkt erhalten soll.

Die künftige Produktzertifizierung des BSI hat zwei Komponenten. Zum einen die Zertifizierung von Sicherheits-Komponenten und IT Vorprodukten, bei denen ein besonderer Wert auf die vertikale Prüfung von Sicherheitseigenschaften gelegt wird und die aufgrund ihrer modularen Eigenschaften weniger im Endkundenmarkt als vielmehr im OEM-Geschäft am Anfang der Produkt-Wertschöpfungskette zu finden sind. Zum anderen wird es ein Zertifizierungsverfahren für IT Produktlösungen im Endkundenmarkt geben, bei denen die gesamte Lösung einschließlich aller Sicherheits-Komponenten geprüft wird. Während das Zertifikat eines Vorproduktes Aussagen zu dessen spezifischen Sicherheits-Eigenschaften und ihrer Mechanismenstärke macht, wird das Zertifikat für eine IT Produkt-Lösung eine gesamtheitliche Sicht des Zusammenwirkens von Sicherheitsfunktionen und Produkteigenschaften beinhaltet.

<sup>1</sup> Common Criteria for Information Technology Security Evaluation, Version 2.1, 1999 – ISO/IEC 15408

<sup>2</sup> Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (ITSEC). Juni 1991. Brüssel: EGKS-EWG-EAG, 1991

<sup>3</sup> ISO/IEC/EN 17025 General Requirements for the Competence of Calibration and Testing Laboratories

# Rechtsrahmen: Regulierung und Märkte

Stefan Engel-Flechsigt

*Leiter der AG „Juristische Aspekte einer verbindlichen Kommunikation“.*

*Stefan Engel-Flechsigt ist Rechtsanwalt in Bonn. Er verfügt über langjährige berufliche Erfahrungen in den Bereichen Informatik, Recht und Internet, die er in der Forschung, in der Bundesregierung und in der Industrie gesammelt hat.*

*Als Mitarbeiter der Bundesregierung im Bildungs- und Forschungsministerium war er verantwortlich für die Konzeption des ersten umfassenden Gesetzeswerks zum Thema Multimedia sowie der rechtlichen Aufarbeitung der Gesamtheit neuer Technologien in der Bundesregierung. Er hat an leitender Stelle in Deutschland am Aufbau der finnischen Firma Sonera SmartTrust mitgewirkt und war verantwortlich für die Gründung von Radicchio und der Open Mobile Terminal Platform (OMTP), beides weltweite Industrie-Initiativen im Bereich der mobilen Kommunikation.*

*Neben seiner Mitgliedschaft und Tätigkeit in zahlreichen internationalen Standardisierungsgremien wie ETSI, CEN, ICTSB und GSM Association leitet er die Arbeitsgruppe von CEN/ISSS zur Standardisierung elektronischer Rechnungen im europäischen Umfeld. Als EU-Gutachter wirkt er bei der Evaluierung und Durchführung europäischer Forschungsprojekte zum Themenkreis „Trust und Security“ mit. In seiner beratenden Tätigkeit hat sich Herr Engel-Flechsigt auf den Bereich IT-Anwendungen spezialisiert.*



Stefan Engel-Flechsigt

Rechtsanwalt

E-Mail: stefan.engel-flechsigt@teletrust.de

## „Co-regulation“

### Vereinbarkeit von Regulierung, Technik und Markanforderungen am Beispiel der Gesetzgebung zu elektronischen Signaturen

Mit der fortschreitenden Anerkennung elektronischer Signaturen im Bürgerlichen Recht, im Zivilprozessrecht, im Öffentlichen Recht sowie in einer Reihe weiterer Regelungszusammenhänge sind die Grundlagen zur Gewährleistung einer rechtsverbindlichen elektronischen Kommunikation – basierend auf den jeweiligen Signaturgesetzen als technische Grundregelung – geschaffen worden. Dies gilt sowohl im nationalen wie auch im europäischen Rahmen.

Es ist nicht zuletzt ein Verdienst der Europäischen Richtlinie für elektronische Signaturen, dass die Technologie der elektronischen Signaturen sowohl in den jeweiligen Rechtsrahmen und in den Sicherheitskonzepten zahlreicher Unternehmen Berücksichtigung findet, denn:

- wesentliches Ziel der Richtlinie war es, den europäischen Markt für Zertifizierungsdienstleistungen zu öffnen;
- die Richtlinie sollte zu einer Harmonisierung der Bestimmungen zu elektronischen Signaturen in allen EU Mitgliedstaaten führen;
- die Richtlinie hat den Grundsatz der Nicht-Diskriminierung von elektronischen und handschriftlichen Unterschriften festgelegt.

Insgesamt hat die Richtlinie den nationalen gesetzgeberischen Blick erweitert und den Rahmen für eine grenzüberschreitende Tätigkeit von Zertifizierungsdienstleistern, einheitliche Grundlagen für die Zulassung, die Haftung, den Betrieb und Sicherheitsbestimmungen von Zertifizierungsdienstleistern geschaffen zu haben.

Während die Richtlinie den rechtlichen Rahmen für den Einsatz und die Nutzung elektronischer Signaturen gesetzt hat, blieb die Ausgestaltung der technischen Standards und Normen den europäischen Gremien CEN und ETSI überlassen. Dieser sog. Grundsatz der „co-regulation“ bedeutet im Kern, dass bei technologisch geprägten Rechtssetzungen auf der europäischen Ebene sich diese mit wesentlichen Prinzipien begnügt und die technische Ausgestaltung den anerkannten Standardisierungsgremien wie ETSI, CEN, CENELEC und ihren jeweiligen nationalen Mitgliedsorganisationen anvertraut wird.

Dieser Weg ist im Ansatz richtig, hat jedoch hinsichtlich der „Co-regulation“ von elektronischen Signaturen im Ergebnis zu Verzögerungen bei der Umsetzung und Verabschiedung der gefundenen Standards und zu praxisfernen Lösungen geführt:

- In der Praxis der Umsetzung der Richtlinie stellte sich die Freiheit bei der Umsetzung der Richtlinie als gravierendes Hemmnis für die europäische Anwendung heraus. Die Richtlinie ist in den Mitgliedstaaten sehr unterschiedlich umgesetzt worden. In der Praxis führt dies zur Anwendung der jeweiligen nationalen Gesetzgebung. Das nationale Auslegungsmonopol steht damit einer europäischen, grenzüberschreitenden Anwendung entgegen.
- Grenzüberschreitende Anwendungen – wie sie zum Beispiel im Bereich europäischer Unternehmen oder in Bereichen grenzüberschreitender Anwendungen zur Kostenersparnis erforderlich sind – werden durch die fehlende einheitliche Umsetzung verhindert und unnötig kompliziert. Die Entwicklung von „best-practice“ Szenarien könnte hier eher weiterhelfen als die Entwicklung von technischen Standards.
- Auch bei der Implementierung von Signaturprozessen und den damit einhergehenden unterschiedlichen Anforderungen an eine prozessorientierte Ausgestaltung treten in der Praxis Probleme auf: So ist die Richtlinie z.B. nicht für die Abbildung von Massensignaturen ausgelegt, die in der Praxis erhebliche Bedeutung erlangen können, z.B. bei elektronischen Rechnungen. Hier sollte eine Standardisierung anknüpfen.
- Durch elektronische Signaturen können medienbruchfreie Geschäftsprozesse realisiert werden. Diese haben den wesentlichen Vorteil, dass sie schneller und effizienter sind, und somit erhebliche Kosten eingespart werden können. Deshalb sollen möglichst viele Anwendungen mit der elektronischen Signatur ausgestattet werden. Zwischen Regulierung, technologi-

scher Entwicklung und Marktnähe von Anwendungen besteht deshalb ein enger sachlicher und zeitlicher Zusammenhang. Dieser Zusammenhang besteht in den rein technisch ausgerichteten Standardisierungsgremien nicht.

Unter dem Blickwinkel einer raschen und vor allem marktorientierten Sichtweise kann „Co-regulation“ daher nur dann wirksam als Regelungsprinzip eingreifen, wenn neben der rechtlichen und technischen Komponente die folgenden zusätzlichen Elemente einbezogen werden:

- Klare und einfache Verfahren müssen geschaffen werden, die transparente und rasche Verfahrensschritte erlauben und eine aktive Beteiligung aller Beteiligten erlauben.
- Die Verfahren müssen mit klaren Ziel- und begrenzten Zeitvorgaben durchgeführt werden und im Ergebnis zu einem akzeptierten europäischen Konsens führen. Die Ergebnisse müssen regelmäßig überprüft werden.
- Die sog. technische Standardisierung muss ergänzt werden durch marktwirtschaftliche und betriebswirtschaftliche Sichtweise und durch die Entwicklung von „best practice“ Szenarien, um rasch marktnahe Anforderungen an Produkte formulieren zu können.

Unsicherheiten bei Anbietern, die ihre technologischen Produkte nicht nur für einen nationalen Markt, sondern für den europäischen Markt anbieten, müssen durch eine verstärkte und formalisierte Kooperation der EU Mitgliedstaaten begegnet werden. Diese muss auch eine europäische Produktzertifizierung ermöglichen.

# TELETRUST zur Wirksamkeit der EG-Signatur-Richtlinie 1999/93/EG

*Im Sommer 2003 wurde TELETRUST neben anderen fachkompetenten Interessenvertretungen vom Bundesministerium für Wirtschaft und Arbeit (BMWA) angesprochen, eine Zuarbeit für eine vorgesehene deutsche Stellungnahme zur Evaluierung der EG-Signaturrechtlinie 1999/93/EG (EGSRL) zu erstellen.*

*Basis dieses Ersuchens war die gemäß Artikel 12 der EGSRL vorgeschriebene Überprüfung der EGSRL, bei der auch festzustellen war, ob der Anwendungsbereich der EGSRL angesichts der technologischen und rechtlichen Entwicklungen und der Marktentwicklung geändert werden sollte. Dieser Prozess wurde von der Europäischen Kommission mit der Vergabe einer Studie eingeleitet. Diese wurde unter der Leitung von Jos Dumortier (Kath. Universität Leuven) mit dem Titel „**The Legal and Market Aspects of Electronic Signatures**“ erarbeitet und im Oktober 2003 veröffentlicht (siehe auch: [www.teletrust.de](http://www.teletrust.de) → Services/Dokumente).*

*In Vorbereitung einer deutschen Stellungnahme zur Evaluierung der EGSRL hatte die Bundesregierung um Stellungnahme zu folgenden Fragen gebeten:*

- 1. Wo sehen Sie Vorteile der Einführung und Umsetzung der EGSRL in Deutschland?*
- 2. Wo sehen Sie Probleme der Einführung und Umsetzung der EGSRL in Deutschland?*
- 3. Sehen Sie notwendigen Änderungsbedarf der EGSRL?*

*Ergebnis ist die hier vorliegende Stellungnahme vom 31. Juli 2003, die im Auftrag des TELETRUST-Vorstandes, koordiniert durch die Geschäftsführung und mit der fachlichen Unterstützung der AG1 „Juristische Aspekte einer verbindlichen Kommunikation“ erarbeitet wurde. Leider ist es zu der vorgesehenen deutschen Stellungnahme zur Evaluierung der EGSRL **nicht** gekommen.*

## Präambel

TELETRUST legt im nachstehenden die Grundgedanken für eine anwendungsorientierte und praxisbezogene Umsetzung der europäischen Richtlinie in Deutschland dar.

Begleitung und Entwicklung der gesetzgeberischen Aktivitäten zur Schaffung von Grundlagen für die Anwendung elektronischer Signaturen war Schwerpunkt der Diskussionen in der AG1 von TELETRUST in den vergangenen Jahren. Mit fachkundigen Stellungnahmen sowie intensiver Beteiligung an Anhörungen der gesetzgebenden Organe hat sich TELETRUST zu Wort gemeldet. Neben dieser eher gesetzgeberischen Tätigkeit kommen in anderen Arbeitsgruppen und Projekten von TELETRUST zusätzliche weitere Aspekte hinzu, die für vertrauenswürdige Informationsverarbeitungs- und Kommunikationsprozesse wichtig sind. Hierzu zählt beispielsweise die Standardisierung, zu der TELETRUST mit ISIS-MTT einen wichtigen Beitrag geleistet hat, und auch das Projekt der European Bridge-CA. In diesem Zusammenhang sind auch die Best Practices für sicheren E-Commerce zu nennen, die von TELETRUST entwickelt wurden und der Öffentlichkeit mittlerweile zur Verfügung stehen.

Einen weiteren Gesichtspunkt möchten wir dieser Stellungnahme voranstellen:

Ein wichtiges Ziel der europäischen Regelung von elektronischen Signaturen war eine intereuropäische Optimierung der elektronischen Geschäftsprozesse und deren Sicherung. Bei der Diskussion und Umsetzung der EGSRL trat jedoch eine Fixierung auf das elektronische Dokument an die Stelle dieses Ziels. Bei den zukünftigen Diskussionen zur EGSRL und zu eventuellen neuen Gesetzgebungsinitiativen auf nationaler wie auf europäischer Ebene muss der Blick weiter gefasst werden und auch in Richtung gesicherter Prozesssteuerungen gehen.

Diese Erfahrung möchten wir in der anstehenden Evaluierung der Richtlinie einbringen. Wir stehen gerne für Rückfragen zur Verfügung und sind bereit, in künftige Evaluierungs- und Anhörungsverfahren im Bereich der elektronischen Signatur einbezogen zu werden. Unsere Anregungen werden wir auch unmittelbar in die Analyse des Ist-Zustandes durch die Universität Leuven einbringen.

## Antworten von TELETRUST:

**1. Frage:** Wo sehen Sie Vorteile der Einführung und Umsetzung der EGSRL in Deutschland?

**2. Frage:** Wo sehen Sie Probleme der Einführung und Umsetzung der EGSRL in Deutschland?

Eine sachgerechte Beurteilung dieser beiden Fragen – die gemeinsam vorgenommen werden soll – kann nicht ohne Blick auf die mit der EGSRL verfolgten Ziele erfolgen. Diese sind hinlänglich bekannt, sollen aber dennoch noch einmal kurz zusammengefasst werden:

- Wesentliches Ziel der Richtlinie ist es, den europäischen Markt für interoperable Zertifizierungsdienstleistungen und Signaturprodukte zu öffnen.
- Die Richtlinie soll zu einer Harmonisierung der Bestimmungen zu elektronischen Signaturen inkl. der Rechtsfolgeregelungen in allen EU Mitgliedstaaten führen.
- Die Richtlinie hat den Grundsatz der Nicht-Diskriminierung von elektronischen und handschriftlichen Unterschriften festgelegt.

Es ist ein Verdienst der Richtlinie, den nationalen gesetzgeberischen Blick erweitert zu haben und den Rahmen für eine grenzüberschreitende Tätigkeit von Zertifizierungsdiensteanbietern (ZDA), einheitliche Grundlagen für die Zulassung, die Haftung, den Betrieb und die Sicherheitsbestimmungen von ZDA geschaffen zu haben.

Die Richtlinie hat einen flexiblen, aber auch ausfüllungsbedürftigen Rechtsrahmen für die nationalen Gesetzgebungen zu elektronischen Signaturen vorgegeben.

Für Deutschland war es von Bedeutung, dass die bereits im SigG 1997 vorgesehene Evaluierung dieses Gesetzes sowie seine Anpassung entsprechend der EGSRL zum Anlass genommen wurde, endlich auch die Rechtsfolgeregelungen für elektronische Signaturen vorzunehmen. Heute verfügen wir über einen gesetzlichen Rahmen für viele relevanten Formen rechtswirksamen Handelns im elektronischen Geschäftsverkehr in Wirtschaft und Verwaltung sowie im Privatsektor. Allerdings betrifft die gesetzliche Regulierung im Schwerpunkt einen nur schmalen Bereich rechtswirksamen Handelns. Er bezieht sich zudem häufig explizit auf die Rahmenbedingungen für elektronische Signaturen gemäß §15 SigG 2001 und wirft damit zwangsläufig Fragen der technischen Interoperabilität von Komponenten und Diensten sowie der gegenseitigen Anerkennung im europäischen Rahmen auf. Praktisch ist diese Regulierung für die Bereiche des

E-Commerce und die Geschäftsbeziehungen zwischen Unternehmen kaum von Bedeutung. Die Warnfunktion im Verbraucherbereich beispielsweise lässt sich auch anders lösen.

TELETRUST begrüßt ausdrücklich, dass die Umsetzung in den genannten nationalen Regelwerken zügig und in engem zeitlichen Zusammenhang zu den bereits verabschiedeten gesetzlichen Grundlagen erfolgte. Damit wurde die Bedeutung der elektronischen Signaturen nachhaltig unterstrichen und ein für die in diesem Bereich tätigen Unternehmen wirtschaftlich wichtiges zusätzliches Anwendungsfeld für den Einsatz und die Nutzung elektronischer Signaturen eröffnet.

Insgesamt misst sich der Erfolg der EGSRL aber an den real erreichten Ergebnissen, also dem wirklichen Markterfolg der elektronischen Signaturen. Der Erfolgsnachweis der EGSRL wäre – gemessen an den Maßstäben für die Evaluierung – das Vorhandensein vieler praktischer und interoperabler Anwendungen von elektronischen Signaturen in Europa.

Das Fehlen deutlicher wirtschaftlicher Impulse für die ICT-Branche nach immerhin vier Jahren praktischer Umsetzung belegt aber leider trotz des Verbrauchs umfangreicher Ressourcen den **grundsätzlichen Misserfolg der EGSRL**.

TELETRUST sieht hierzu eine Reihe von Gründen:

1. **Problematik einer vorauseilenden Technikregulierung**  
Als Vorreiter in Europa hatte Deutschland bereits im Sommer 1997 ein Signaturgesetz (SigG) als Teil des Informations- und Kommunikationsdienstleistungsgesetzes (IuKDG) geschaffen. Auch Fachleute von TELETRUST waren daran voller Enthusiasmus beteiligt. Bereits Ende 1998 hatte TELETRUST jedoch erkannt und in einem offenen Brief kommuniziert, dass der Versuch der vorauseilenden Technikregulierung im SigG 1997 nicht den gewünschten Effekt eines flächendeckenden Einsatzes digitaler Signaturen im elektronischen Geschäftsverkehr hatte: „... TELETRUST hält es für wünschenswert, dass das Signaturgesetz (bzw. die SigV) schnell in einigen Bestimmungen verändert wird, um bei seiner Umsetzung mehr Flexibilität hinsichtlich innovativer Lösungen und Kompatibilität zu globalen Standards zu erreichen. Das wird dazu beitragen, dass die Investitionen in diesem Bereich ein höheres Wirkungsfeld bekommen. ...“
2. Es ist festzustellen, dass auch in der EGSRL der Versuch einer „vorauseilenden Technikregulierung“ unternommen wurde, der naturgemäß nicht technikneutral sein kann. Unterschiedliche Umsetzung der Richtlinie in EU-Mitgliedstaaten  
Die EGSRL wurde von den Mitgliedsstaaten sehr unterschiedlich in nationales Recht umgesetzt. In Deutschland erfolgte dies beispielsweise nicht so, dass das Hauptziel der EGSRL, eine europaweite Harmonisierung, im Vordergrund stand. Die in der EGSRL vorhandenen Spielräume wurden vielmehr überwiegend dahingehend genutzt, um die Vorgaben des SigG 1997 möglichst unverändert in das SigG 2001 einfließen zu lassen. Als Beispiele aus dem SigG 2001 seien hier genannt:
  - ◆ Die Bindung fortgeschrittener (und damit auch qualifizierter) elektronischer Signaturen allein an natürliche Personen; damit sind juristische Personen im Gesetzestext an dieser Stelle in Deutschland faktisch (wenn auch nicht wörtlich) ausgeschlossen, während andere EU-Mitgliedstaaten, vom weiteren Spielraum der EGSRL Gebrauch machend, elektronische Signaturen auch für juristische Personen zulassen.
  - ◆ Die gegenüber der EGSRL einschränkenden Definitionen (z.B. fortgeschrittene elektronische Signatur, Zertifizierungsdiensteanbieter)
  - ◆ Die Zulassung von Pseudonymen in Verbindung mit elektronischen Signaturen: Elektronische Signaturen sollen in der Praxis zur Identifizierung von Personen und zur Authentifizierung bei Prozessen eingesetzt werden, in denen eine **verbindliche Zuordnung zu einem Urheber** wichtig ist. Ein Anspruch auf Pseudonymität oder gar Anonymität, wie er als datenschutzrechtlicher Kern bereits im SigG 1997 geregelt war, widerspricht diesem praktischen Bedürfnis und sollte daher mit Blick auf die eigentlichen Geschäftsprozesse neu geregelt werden.
3. **Fehlende marktwirtschaftliche Fokussierung der Umsetzung in Deutschland**  
Bei der Umsetzung der EGSRL in Deutschland wurde sehr viel Gewicht auf die Regulierung der qualifizierten Signatur mit freiwilliger Akkreditierung der ZDA gelegt und weniger auf die Berücksichtigung und Förderung anwendungsbezogener Signaturen, wie sie mittlerweile im europäischen Markt anzutreffen sind, z.B. auf dem Niveau der fortgeschrittenen

Signaturen. Es hat sich als nachteilig erwiesen, dass das flexiblere „Baukastenprinzip“ bei den technischen Vorgaben der EGSRL zugunsten fest definierter Signaturqualitäten (einfach, fortgeschritten, qualifiziert, akkreditiert) im SigG 2001 aufgegeben wurde. Dies führte gemeinsam mit der vorbeschriebenen einseitigen Sichtweise zu vielen Fragen und Schwierigkeiten in der Praxis, die nach Ansicht von *TELETRUST* den geraden und schnellen Weg zu praxisbezogenen Lösungen verstellt hat.

- ◆ Es hat im Ergebnis in Deutschland zu einer **Vielzahl von Signaturprofilen** geführt, die zudem in unterschiedlichen Gesetzen Eingang gefunden haben und nun ihrerseits den klaren und eindeutigen Praxisbezug und die von der Industrie gewünschte Leitlinie vermissen lassen.
- ◆ Aus unserer Sicht hat diese Umsetzung für **wenig Durchlässigkeit des deutschen Marktes für europäische Anbieter** gesorgt. Die europäische Komponente der Zertifizierungsdienste und die damit fehlende durchgängige Einheitlichkeit der Infrastrukturen fehlt heute. Die nach deutschem Recht pauschale Anerkennung der EGSRL entsprechender, der deutschen Umsetzung jedoch nicht genügender ausländischer Signaturen widerspricht einerseits (theoretisch) dem Gleichbehandlungsgrundsatz und scheitert andererseits (praktisch) an Interoperabilitätsproblemen. Ebenso ist die gewünschte Angebotsvielfalt von ZDA anderer Mitgliedsstaaten in nationalen Märkten nicht gegeben, was auch daran liegen mag, dass die zentrale Komponente des Registrierungsdienstes vor Ort von den nationalen zuständigen Aufsichtsbehörden des Herkunftslandes nicht erfasst werden kann.
- ◆ Es hat sich erwiesen, dass die Konzentration auf den höchstmöglichen Signaturstandard und die damit für den Verbraucher verbundenen **Kosten am Markt keine Akzeptanz** finden. Für den Geschäftserfolg der ZDA ist es inzwischen maßgeblich, die ganze Bandbreite von Zertifizierungsdiensten anzubieten. Für verschiedene, durch die Geschäftsprozesse des Kunden bestimmte, Anforderungen und ihnen zugrunde liegende gesetzliche Vorgaben können so angemessene Lösungen angeboten werden.
- ◆ Leider wird in Deutschland bei öffentlichen Diskussionen des öfteren der Eindruck erweckt, nur die für Anwendungen im formgebundenen Bereich vorgesehenen Instrumentarien elektronischer Signaturen seien vertrauenswürdig. Damit wurde und wird Unsicherheit gegenüber alternativen Lösungen, deren Zulässigkeit im Gesetz ausdrücklich bestätigt ist, erzeugt und ihre Verbreitung im stark überwiegenden Bereich formfreien Handelns verhindert.
- ◆ Der elektronische Signaturen betreffende Aufgabenschwerpunkt der Regulierungsbehörde für Telekommunikation und Post (RegTP) muss den wirtschaftlichen Erfordernissen angepasst werden. Er ist von der alleinigen, technologieorientierten Umsetzung des §15 SigG (Akkreditierung von ZDA) hin zu einer vertrauensbildenden Begleitung (Aufsicht) aller Diensteanbieter für qualifizierte elektronische Signaturen zu verschieben.

Aus der Sicht von *TELETRUST* wäre es daher wünschenswert, nicht nur die rechtlichen und technischen Fragen – von denen einige noch nicht geklärt sind – in der **europäischen Praxis** zu analysieren und einer pragmatischen Lösung zuzuführen. Auch die betriebswirtschaftlichen Fragen sind auf europäischer Ebene

eingehender zu berücksichtigen, um so den potentiellen Einsatz elektronischer Signaturen und die notwendige **europäische Interoperabilität** zu verbessern. Chancen dafür bieten sich durch die ersten Impulse seit der Gründung des Signaturbündnisses in Deutschland. Hierzu zählt eine genaue Marktbeobachtung und das Feedback der Markterfahrungen in die gegenwärtigen Diskussionen.

### 3. Frage: Sehen Sie notwendigen Änderungsbedarf der EGSRL?

Die EGSRL hat ihr wirtschaftliches Ziel verfehlt. Die Marktentwicklung für Signaturanwendungen wurde nicht stimuliert.

Die EGSRL hat ihr juristisches Ziel nur zum Teil erreicht. In wesentlichen Details hat nationales Besitzstandsdenken die Umsetzung der EGSRL in national geltende Bestimmungen für elektronische Signaturen bestimmt und damit einer europaweiten Harmonisierung entgegen gewirkt.

**Eine Änderung der EGSRL in Details sollte aber aus unserer Sicht ultima ratio sein;** es sollte eher auf nationaler Ebene versucht werden, Änderungen durchzuführen und diese – wo notwendig – europäisch abzustimmen. Deutschland hat hier deutlichen Handlungsbedarf, wie wir bei der Beantwortung der Fragen 1 und 2 bereits dargelegt haben.

*TELETRUST* ist der Ansicht, dass eventuelle Detailänderungen der Richtlinie Einführung und Umsetzung elektronischer Signaturen in Europa für die Dauer des Gesetzgebungsvorhabens auf der europäischen wie auch die Umsetzung auf nationaler Ebene ganz erheblich bremsen würden.

Wenn Änderungen trotzdem vorgenommen werden sollen, sieht *TELETRUST* Änderungsbedarf, der sich zum einen auf rechtliche Vorgaben der Richtlinie, die zu verdeutlichen sind, und zum anderen auf den Prozess der sogenannten „co-regulation“, den die Richtlinien-systematik vorgibt und der sich in der Praxis als zu langsam und zu wenig flexibel erweist.

Die Erfahrung der *TELETRUST*-Mitglieder bei der Einführung der elektronischen Signatur hat gezeigt, dass rechtliche und technische Vorgaben allein eine automatische flächendeckende Verbreitung elektronischer Signaturen nicht erreichen. Für einen erfolgreichen Einsatz der elektronischen Signatur in den Geschäftsprozessen wird ein komplettes Framework mit Workflow und Archivierung unter Berücksichtigung auch betriebswirtschaftlicher Faktoren benötigt. Dies kann durch starre regulative Vorgaben nicht erreicht werden.

Aus den praktischen Erfahrungen von *TELETRUST*-Mitgliedern haben sich insbesondere folgende Aspekte ergeben, die keinesfalls abschließend sind:

- Durch elektronische Signaturen können Geschäftsprozesse medienbruchfrei realisiert werden. Dies hat den wesentlichen Vorteil, dass sie schneller und effizienter gestaltet und somit erhebliche Kosten eingespart werden können. Deshalb sollen möglichst viele Anwendungen, beginnend im formfreien Bereich, der keinerlei Regulierung bedarf, mit der Funktionalität des elektronischen Signierens ausgestattet werden. Die Regelungen der Signaturverfahren im formgebundenen Bereich können national aber nur im **intereuropäischen Konsens** ausgefüllt werden. In der Praxis der Umsetzung der EGSRL sind die vorhandenen Spielräume stets unter Wahrung der Ziele der EGSRL und nicht zur Verfolgung eigener nationaler Interessen zu nutzen. Dem kann aus unserer Sicht nur durch eine **ver-**

**stärkte und formalisierte Kooperation** der EU-Mitgliedstaaten begegnet werden, zum Beispiel im Rahmen der ENISA, deren Aufgaben entsprechend zu gestalten sind.

- Die Richtlinie ist in den Mitgliedstaaten sehr unterschiedlich umgesetzt worden. Dies haben die bislang gemachten Erfahrungen und verschiedene Studien gezeigt; zusätzlich wird die Richtlinie mittlerweile von einigen neueren Richtlinien (z.B. EU-Richtlinie für elektronische Rechnungen und MWSt, 2001/115/EC) referenziert. In der Praxis führt dies zur Anwendung der jeweiligen nationalen Gesetzgebung. Grenzüberschreitende Anwendungen – wie sie zum Beispiel im Bereich europäischer Unternehmen oder in Bereichen grenzüberschreitender Anwendungen aus **Kostenersparnis** erforderlich sind – werden durch die unterschiedlichen nationalen Umsetzungen teils verhindert und teils unnötig kompliziert. Hier muss nach Auswegen gesucht werden, die das Föderationsprinzip in der EG konstruktiver als bisher berücksichtigen.
- Bei der Implementierung von Signaturprozessen in die Abläufe des elektronischen Geschäftsverkehrs treten in der Praxis unterschiedlichste Anforderungen auf, denen durch innovative Lösungen zu entsprechen ist. Die durch den flexiblen Rahmen der EGSRRL gegebenen Möglichkeiten sind bei diesen Implementierungen soweit wie nötig auszuschöpfen; sich daraus ergebende neue Instrumentarien (Produkte, Lösungen, Dienstleistungen) sind in die Konzepte einzuordnen und anzuerkennen. Die Implementierung muss bestimmt werden durch Zweckorientiertheit, nicht durch vorauseilende Technikregulierung.
- Nach wie vor herrscht eine große Unsicherheit bei den Anwendern durch immer neue regulatorische Anforderungen oder Änderungen bestehender Verordnungen: So wird zum Beispiel zur Betrachtung des Dokumentes, das ein Anwender mit einer qualifizierten elektronischen Signatur signieren möchte, eine Anzeigekomponente benötigt. Diese soll z.B. laut RegTP mindestens E2 „hoch“ evaluiert sein, was in dieser Form weder im Signaturgesetz noch in der Signaturverordnung zu finden

ist. In der Anlage zur Verordnung zur elektronischen Signatur, Anlage 1 Nr.1 (zu § 11 Abs. 3, § 15 Abs. 5 und § 16 Abs. 2) besteht keine Veranlassung Anzeigekomponenten zu evaluieren. Allerdings, laut Aussage der RegTP, wird die Verordnung abgeändert und die Anlage 1 Nr.1 bezieht sich auf § 11 Abs. 3, § 16 Abs. 2, § 17 Abs. 2, § 17 Abs. 3 -1 und 2. Damit müssten auch Anzeigekomponenten evaluiert werden. Nun stellt sich natürlich die Frage, ob man von der jetzigen Signaturverordnung ausgeht oder von der zukünftigen, ob man sich in Deutschland dem Ziel der EGSRRL wieder nähern oder sich von ihm gar noch weiter entfernen will.

- Die Richtlinie sollte daher nach unserer Auffassung die **europäische Zertifizierung** von Produkten für elektronische Signaturen ermöglichen ohne sie vorzuschreiben. Dies ist zwar in der Richtlinie durch Art. 3 Abs. 5 angelegt und ist jetzt auch in einer ersten Entscheidung der EU Kommission vom 14.07.2003 umgesetzt worden. Dies ist im Kern ein richtiger Ansatz, müsste aber aus unserer Sicht auf weitere Komponenten ausgedehnt werden. Damit würden zahlreiche Unsicherheiten bei Anbietern, die ihre Signaturprodukte nicht nur für einen nationalen Markt, sondern für den europäischen Markt anbieten, genommen.

Der bereits angesprochene Grundsatz der „**co-regulation**“ bedeutet, dass vor allem bei technologisch geprägten Rechtssetzungen auf der europäischen Ebene sich diese mit wesentlichen Prinzipien begnügt und die technische Ausgestaltung den anerkannten Standardisierungsgremien ETSI, CEN, CENELEC und ihren jeweiligen nationalen Mitgliedsorganisationen anvertraut wird. Dieser Weg ist im Ansatz richtig, führt jedoch zu erheblichen Verzögerungen bei der Umsetzung und Verabschiedung der gefundenen Standards. Hier wäre es wünschenswert, wenn klare und einfache Verfahren geschaffen würden, die transparente und rasche Verfahren erlauben würden. Aus Sicht von TELETRUST wäre es dabei wichtig, nationale Entwicklungen, zum Beispiel ISIS-MTT, mit einzubeziehen.

# ***TELETRUST*** **in der** **Informationsgesellschaft**

Die Informationsgesellschaft braucht Sicherheit. Der Verein fördert die Entwicklung und Anwendung von aufeinander abgestimmten Produkte und Lösungen, Infrastrukturen und Dienstleistungen.



## Von der European Bridge-CA zum Signaturbündnis

Matthias Büger, Bernhard Esslinger

*Matthias Büger ist zuständig für die Mitgliedschaft der Deutsche Bank AG im Signaturbündnis.*

*Bernhard Esslinger ist zuständig für die Mitgliedschaft der Deutsche Bank AG in der European Bridge-CA.*

### Einleitung

Die Verwendung elektronischer Kommunikation im Wirtschaftsleben verspricht ein erhebliches Potenzial. Eine wesentliche Voraussetzung ist jedoch, dass neben der Vertraulichkeit auch die Authentizität und Integrität der Daten gewährleistet sind. Hieraus ergibt sich ein Bedarf für Public Key Infrastrukturen (PKI), die auch den Bereich der Kommunikation mit Behörden (E-Government) einschließt.

Dass es bis heute keine weit verbreiteten, allgemein verfügbaren Infrastrukturen gibt, hat in erster Linie wirtschaftliche Gründe: Als Netzwerkprodukt steigt der Nutzen einer PKI mit der Anzahl ihrer Nutzer (Signaturersteller und Akzeptanten); dem stehen Fixkosten für initiale Erstellung und Betrieb der Infrastruktur gegenüber. Eine allen Bürgern zugängliche PKI rechnet sich also erst bei einer hinreichend großen „kritischen“ Masse von Anwendern. Solange sich keine Infrastruktur mit großer Verbreitung abzeichnet, warten Privatpersonen wie Anwendungsanbieter lieber ab, um nicht die falsche Investition zu tätigen. Dies hat zu einer Pattsituation geführt.

European Bridge-CA (EB-CA) wie Signaturbündnis haben zum Ziel, dieses Patt zu überwinden. Dabei vereinigt sie der pragmatische Grundgedanke, auf Bestehendem (z.B. existierenden PKIs) aufzubauen und damit die Hürde für den Aufbau einer breiten PKI so niedrig wie möglich zu halten. Beide Initiativen arbeiten daran, ein Höchstmaß an Interoperabilität zu erreichen.

### Weltweit sichere E-Mail – die European Bridge-CA

Dass sich der Aufbau von Sicherheitsinfrastrukturen im ersten Schritt vornehmlich in (großen) Unternehmen vollzog, hat einfache Gründe: Der Einsatz elektronischer Kommunikation schafft Mehrwert – dies zeigt nicht zuletzt die zunehmende Bedeutung von E-Mails gerade in weltweit operierenden Unternehmen. Infrastruktur und zugehörige Anwendungen können aus einer Hand kreiert werden. Gleichzeitig besteht die Nutzergruppe aus den eigenen Mitarbeitern, auf deren Verhalten das Unternehmen Einfluss hat. Soweit nur die interne Kommunikation betroffen ist, können unternehmensinterne Richtlinien (Policies) den Einsatz der Infrastruktur regeln.

In der Folge entstanden PKIs in global agierenden Unternehmen. Im allgemeinen war es jedoch nicht möglich, diese PKIs für die sichere E-Mail Kommunikation zwischen den Unternehmen einzusetzen, auch wenn beide (technisch vergleichbare) Lösungen



Dr. Matthias Büger

Projekt Manager

Deutsche Bank AG  
Corporate Center

E-Mail: matthias.bueger@db.com



Bernhard Esslinger

Direktor

Deutsche Bank AG  
Information Risk Management

E-Mail: besslinger@web.de

einsetzen. Anschaulich gesprochen, wurden PKI-Inseln geschaffen, zwischen denen kein Austausch möglich war.

Überlegungen, diese Inseln in ein hierarchisches System einzugliedern, führen nicht zum Ziel, da nur wenige Großunternehmen gewillt sind, ihre Unternehmens-PKI einer dritten Stelle unterzuordnen. Auch sind gewachsene Strukturen in den einzelnen Unternehmen zu berücksichtigen, die Unterschiede z.B. in den Ausgabeprozessen der Zertifikate zur Folge haben.

Der pragmatische Ansatz der European Bridge-CA besteht darin, bestehende PKI-Inseln quasi durch Brücken zu verbinden, ohne eine hierarchische Struktur zu schaffen. An einer zentralen Stelle hinterlegen die Mitglieder ihre Root-CA als Vertrauensanker. Dabei verpflichten sie sich auf ein Mindestsicherheitsniveau. Die Verwendung bestehender Prozesse wird dabei ausdrücklich anerkannt, auch wenn diese von Mitglied zu Mitglied variieren.

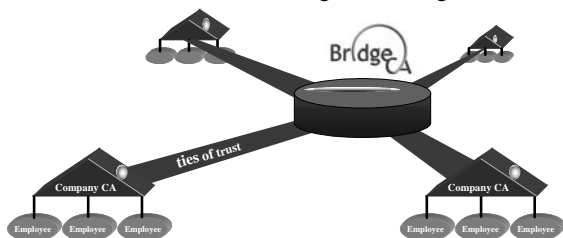


Abbildung: Das Konzept der European Bridge-CA (EB-CA)

Gemeinsam mit der Deutschen Telekom und dem BSI hat die Deutsche Bank im Jahr 2000 die EB-CA mit dem Ziel gestartet, sichere E-Mail zwischen Mitarbeitern der Teilnehmerorganisationen zu ermöglichen. Inzwischen sind der Initiative rund 30 weitere Firmen beigetreten, darunter z.B. auch die Deutsche Bundesbank, Siemens, SAP und die Telekom-Control-Kommission in Österreich. Die Mitglieder haben an ihre Mitarbeiter und Kunden inzwischen mehr als eine Million Zertifikate ausgegeben. Auch international finden Kontakte und Interoperabilitätstests statt (IDABC, The Boeing Company).

## PKI für das breite Publikum – das Signaturlbündnis

Im Vergleich zur EB-CA-Initiative ist der Fokus des Bündnisses für elektronische Signaturen (Signaturlbündnis) weiter gefasst: Ziel ist eine Smartcard-basierte Infrastruktur mit fortgeschrittenen oder qualifizierten Signaturen, in der elektronische Kanäle für alle Arten von Transaktionen genutzt werden können: vom Vertrag über Anträge bei Behörden bis hin zu Finanztransaktionen.

Eine solche Infrastruktur würde Vorteile für alle Beteiligten mit sich bringen:

- Online-Händlern wie Behörden stünde ein effizienter Kanal zur Verfügung, dessen Nutzung zu einer erheblichen Kostenersparnis führen kann.
- Privatkunden ersparen sich Behördengänge oder umständliche Versendungen – ähnlich wie beim Einsatz von Kontoauszugsdruckern in Bankfilialen.

Man darf erwarten, dass Anwendungen aus dem E-Government-Bereich (wie z.B. ELSTER) große Transaktionszahlen werden erzielen können. Für den einzelnen Bürger ist aber wichtig, dass er neben dem E-Government weitere attraktive Anwendungen vorfindet. Der Nutzen der Signaturlkarte für den Bürger liegt

gerade darin, mit nur einer Karte den Zugang zu möglichst vielen privaten und öffentlichen Anwendungen zu erhalten. Die privaten Anwendungsanbieter ihrerseits wünschen sich verlässliche Zahlen über die zu erwarteten Nutzer. Dies erfordert eine gemeinsame Initiative aus öffentlicher Hand und Privatwirtschaft (Public-Private-Partnership). Das folgerichtig gegründete Signaturlbündnis hat das Ziel,

- technische Standards zu definieren, um Interoperabilität sicherzustellen,
- bestehende Infrastrukturen wie die Kartenausgabeprozesse der Kreditwirtschaft zu nutzen, um die initialen Kosten so gering wie möglich zu halten,
- die rechtlichen Rahmenbedingungen zu schaffen, damit dieser pragmatische Weg bestritten werden kann,
- sich im Vorfeld mit großen Anwendungsanbietern z.B. aus dem E-Government-Umfeld zusammenzusetzen, um zeitgleich mit dem Ausrollen einer PKI für deren Anwendungen zu sorgen und proprietäre Entwicklungen zu vermeiden,
- ein Geschäftsmodell zu entwickeln, das einen fairen Ausgleich zwischen Betreibern und Nutzern der Infrastruktur schafft.

Das Signaturlbündnis (Logo rechts) ist auf gutem Weg, diese Ziele zu erreichen. Im Bereich der technischen Spezifikation wurden Fortschritte erzielt, eine Änderung des Signaturlgesetzes ist auf dem parlamentarischen Weg, an Geschäftsmodellen wird intensiv gearbeitet, mit der JobCard-Anwendung der Bundesregierung wurde eine wichtige Applikation einbezogen.



Als erstes Kreditinstitut bietet die Deutsche Bank bereits seit Oktober 2003 mit der db SignaturlCard jedem Kunden eine Karte an, die neben online-Banking auch im Kontakt mit der BfA, für ELSTER oder sichere E-Mail eingesetzt werden kann.

## Ausblick

Die Konzeption und der Aufbau einer Sicherheitsinfrastruktur ist unter wirtschaftlichen Gesichtspunkten – zumal in der Zeit knapper IT-Budgets – keine einfache Aufgabe. Dennoch kann sie gelingen, wenn die initialen Kosten durch pragmatisches Herangehen gesenkt und der potenzielle Nutzen durch verstärkte sektorübergreifende Zusammenarbeit vergrößert werden kann.

European Bridge-CA und Signaturlbündnis sind zwei Initiativen, die dieser Philosophie folgen – die EB-CA für Unternehmen und Organisationen mit dem initialen Zweck der sicheren E-Mail-Kommunikation und der Bereitstellung von Zertifikaten; das Bündnis für alle Bürger und möglichst viele Anwendungen vom online-Banking über Internet-Handel bis zum E-Government.

In den vorgestellten Initiativen liegt die Chance, einen Weg aufzuzeigen hin zu einer Welt, in der sich jeder Bürger im Netz genauso sicher bewegt wie in der realen Welt. Der Bürger würde sich dann unnötige Wege und Papierkrieg ersparen, jeder Handelspartner wäre nur einen ‚Klick‘ entfernt. Unternehmen wie Behörden wären in der Lage, noch weit mehr Standardprozesse effizient elektronisch abzubilden, teure manuelle Arbeitsschritte könnten weitgehend entfallen. Dies erfordert innovatives Denken und die Bereitschaft, in erster Linie die Chancen und nicht nur mögliche Probleme zu sehen.

# Flexible Sicherheitsinfrastrukturen

## IT-Sicherheit als Instrument der Unternehmenspolitik

Willi Kafitz

*Neben weiteren Projekten moderiert der Autor seit 2 ½ Jahren die Projektgruppe „Sicherheit beim elektronischen Datenaustausch“ beim Verband der Elektrizitätswirtschaft VDEW. Initiiert von dieser Gruppe haben in einer Gemeinsamen Erklärung erstmals 6 Verbände, die die deutsche Stromwirtschaft vertreten, zu organisationsübergreifenden Sicherheitsrahmenbedingungen aufgerufen. In dem Verbandsprojekt VEDIS (Verbindlichkeit und Sicherheit im Electronic Data Interchange) wird unter der Moderation des Autors von Vertretern namhafter Energieversorgungsunternehmen an einer technischen und organisatorischen Ausgestaltung gearbeitet.*

*Willi Kafitz arbeitet in der TELETRUST-Arbeitsgruppe PSE und im technischen Board der EB-CA mit.*

*Im Rahmen der AG Normierung ist er am Modellvorhaben JobCard des Bundesministeriums für Wirtschaft und Arbeit beteiligt.*



Dr. rer. nat.  
Willi Kafitz

ist seit 19 Jahren Mitarbeiter der Siemens AG in Frankfurt am Main und München in unterschiedlichen Positionen und Aufgaben. Seit ca. 6 Jahren widmet er sich ausschließlich Sicherheitsthemen mit dem Schwerpunkt PKI.

E-Mail: willi.kafitz@siemens.com

## Vernetzung korreliert mit Sicherheitsbedarf

Treibende Kraft für Sicherheitsrahmenbedingungen war in den letzten 15 Jahren die Vernetzung der Informationstechnologie. Die CERT-Organisation (Computer Emergency Response Center) meldet jedes Jahr neue Rekordzahlen an Sicherheitsvorfällen, die unmittelbar mit der weltweiten Vernetzung korrelieren. Im Jahr 2003 waren es allein wieder 137.529 Fälle und damit mehr als die Hälfte mehr, als im Vorjahr.

Als Gründe werden oft IT-Monokulturen genannt, die sicherlich ihren Anteil an der Sicherheitslage haben. Trotzdem sollte man in der Bewertung weiter gehen.

Wie Siemens haben viele national und international tätige Firmen bereits vor einigen Jahren IP-Netze aufgebaut. Durchgängige Kommunikation rund um den Globus wird innerhalb des Corporate Networks nach dem Motto möglich: „anyone, anytime, anywhere, any resource“.

Diese Netze erlauben einfachen Zugriff für alle Mitarbeiter auf eigene Daten und Ressourcen von jedem Punkt der Erde aus und sind Basis für weitere Konzerndienste wie Intranet, E-Mail und Directory Services und andere Anwendungen. Damit wird im Prinzip weltweiter Zugriff auf Informationen und Wissen im gesamten Konzern möglich und es entstand eine einheitliche Plattform für neue Geschäftsmodelle (E-Business). Aber natürlich können diese Corporate IP-Netze auch sicherheitskritisch werden, wenn sich Schwachstellen ergeben. Die Siemens AG hat sich deshalb entschlossen, neben Trustcenter, Viren Competence Center (VCC) und CERT einen 4. Dienst Intrusion Prevention and Inventory Service (IPINS) aufzubauen, der Prävention und Reaktion trennen soll.

Die fortschreitende Digitalisierung der Geschäftsprozesse, in immer mehr Fällen über Unternehmens- oder Behördengrenzen hinaus, lässt es aber nicht mehr zu, dass die eigene Institution wie eine Burg geschützt wird. Viel eher ist das Bild der Datenautobahn geeignet, die Anforderungen an diese Situation zu beschreiben. Darin müssen Begriffe wie „sichere Straßen“, „sichere Autos“ und einem Regelwerk wie der Straßenverkehrsordnung sich auch in Entsprechungen der IT-Security wiederfinden. Hier wird IT-Sicherheit nicht nur unter Schutzgesichtspunkten (Schutz vor Viren, Schutz vor Hackern usw.) gesehen werden können, sondern wird zunehmend zum Business Enabler, ohne den solche Geschäftsprozesse nicht realisierbar sind. In diesen Architekturen wird eine Absicherung über Firewalls nicht mehr ausreichen. Zusätzlich muss auf der Transportebene (z.B. über Virtuelle Pri-

vate Networking, VPN). und auf Informationsebene jeweils mit Mitteln der Public Key Kryptographie gesichert werden.

## Flexible Netze brauchen flexible Sicherheit

Insbesondere die Flexibilisierung der Netzinfrastrukturen wird dabei zu immer stärkeren Anforderungen an die Flexibilisierung der Sicherheitsinfrastrukturen führen.

Flexible Netzinfrastrukturen werden zunehmend nicht nur zur Geschäftsabwicklung, sondern auch aus unternehmenspolitischen Gründen gefordert.

Eine wichtige Forderung an eine zukünftige Knowledge-, Netz- und Sicherheitsinfrastruktur ist in manchen Unternehmen bereits die Maßgabe, auch Projekte mit Mitbewerbern durchführen zu können. Der Anglizismus ist bereits entstanden: Cooperation with Competitors, kurz Coopetition, stellt höchste Anforderungen an die Sicherheitsinfrastruktur, um diese Form von virtueller Kooperation gezielt auf bestimmte Netz- und Wissensbereiche beschränken zu können.

Auch andere Flexibilisierung auf unternehmenspolitischer Ebene, wie die schnelle Abwicklung von Mergers, Acquisitions oder Carve Outs haben ähnliche Ansprüche an Netz- und Sicherheitsinfrastrukturen.

Auch neue Flächennutzungskonzepte, z.B. Business-Park-Szenarien unter gemeinsamer Nutzung des Local Area Networks, können damit möglichst schnell, problemlos und ohne Beeinträchtigung der Betriebs- und Informationssicherheit umgesetzt werden.

Logische Konsequenz bei virtuellen Kooperationen und unternehmenspolitischer Handlungsfreiheit, ist die Mandantenfähigkeit der Netze. VPN-Zertifikate von mehreren Trustcentern müssen zusammenarbeiten können (Interoperabilität) und meist muss auch in kritischen Komponenten (z.B. IPSec-Gateways) ein Multitendorkonzept akzeptiert werden. Unter dem Begriff „Next Generation Network Architecture bzw. Infrastructure (NGNA/NGNI) werden diese und weitere zukunftsweisende, flexible Netzarchitekturen bereits in der Siemens AG vorangetrieben und durch flankierende, flexible Sicherheitsinfrastrukturen abgesichert.

NGNA ist eine qualitative Veränderung von Unternehmensnetzen und flankierender Sicherheitsinfrastruktur aufgrund von unternehmenspolitischen Anforderungen.

## Automatisierungstechnik entdeckt Vernetzung

Es gibt aber auch Bereiche, wo die Vernetzung erst „entdeckt“ wird und damit mit Macht eine Fülle von neuen Sicherheitsanforderungen entstehen. Gemeint ist die Automatisierungstechnik, die aus IT-Sicherheitsgesichtspunkten bisher weitgehend vernachlässigt wurde. Mittlerweile wird nicht mehr gefragt, ob sich TCP/IP auch in diesem Bereich durchsetzt, sondern wie lange noch existierende Bussysteme, trotz intensiver Standardisierungsbestre-

bungen, parallel überleben. Damit ist die Internetwelt mit ihren Möglichkeiten, aber auch ihren Gefahren, in der Automation. Neben sicherer Informationstechnik und Kommunikationstechnik wird Secure Teleautomation eine ganz neue Tür an Sicherheitsanforderungen aufstoßen, um die sich sicherlich auch der TELETRUST kümmern muss.

Geschäftliche Anforderungen machen in diesem Zusammenhang weitere Überlegungen nötig. Unter den Begriffen Enterprise Application Integration (EAI) oder auch Total Business Integration versteht man durchgängige, synchronisierte Prozesse über Abteilungs- und Bereichsgrenzen hinweg. So sind klassische ERP-Systeme – ganz vereinfacht ausgedrückt – „lediglich“ für die Prozesse zwischen Auftragseingang und Rechnungsausgang verantwortlich. Zur Produktionswelt gibt es in diesen Architekturen heute keine oder keine nennenswerten informationstechnischen Verbindungen. In der Produktionssteuerung wurden unter anderen Gesichtspunkten die Prozesse zwischen Zulieferung und Auslieferung behandelt. EAI möchte Daten, Applikationen, Prozesse und Mitarbeiter wesentlich stärker integrieren. Der Integrationsdruck wirkt sich besonders in Branchen aus, wo Produkte wenig Alleinstellungsmerkmale haben und deshalb optimale Kostenstrukturen und damit hohe Integration gefordert sind. Die chemische und pharmazeutische Industrie gehört dazu, aber auch die „Utilities“, z.B. die unterschiedlichen Marktrollen in der liberalisierten Stromwirtschaft, verspüren bereits diesen Marktdruck. Der Weg zur „Total Business Integration“ wirft neue Sicherheitsprobleme auf, wo Antworten nur innerhalb der Applikationen und innerhalb der Prozesse liegen können. Sicherheit wird zur Qualität der Applikation und des (organisatorischen und technischen) Prozesses und kann nicht mehr durch mehr oder weniger isolierte und sequenzialisiert eingesetzte, technische Komponenten, wie Plug-Ins etc., gelöst werden.

## Komplexität verlangt Flexibilität

„IT-Security in a networked world“ heißt der Untertitel in Bruce Schneiers Standardwerk „Secrets and Lies“. Flexiblere Sicherheitsinfrastrukturen in einer immer mehr vernetzten Welt zu etablieren, wird deshalb eine der neuen Herausforderungen sein, der sich TELETRUST, als ein Verein zur Förderung vertrauenswürdiger Kommunikation, bereits stellt und weiterhin engagiert zu stellen hat.

Die kryptographischen Grundlagen sind dazu weitgehend gelöst und in Produkten oder Software-Bibliotheken verfügbar.

Die Herausforderung an die Menschen wird der Komplexitätsgrad sein, wird die Notwendigkeit sein, nicht nur zu verstehen, „wie ein Computer unterschreibt“ sondern wie die sicheren Anwendungsarchitekturen, Trusted Computing Plattformen, Netztopologien aussehen sollen.

Die Dimension des Begriffes IT-Sicherheit muss sich dazu erweitern. Flexibilisierung der Sicherheitsinfrastrukturen wird in den Köpfen beginnen müssen.

# Kooperation für IT-Sicherheitslösungen

Flexible Security ‚Made in Germany‘

Ismet Koyun

*Gründer und Geschäftsführer der KOBIL Systems GmbH*

*Kompetenz:*

*Kryptografie, Digitale Signatur, Authentifizierung*

*Networking:*

*Mitglied bei TELETRUST*

*Strategische Partnerschaften mit Deutsche Telekom,*

*Microsoft, DG-Verlag, FlexSecure und weitere*

## Sicherheit für mobile Daten

Die Welt wird immer kleiner, weil wir Menschen immer mobiler werden. Viel unterwegs und immer erreichbar sein, wichtige Dokumente stets parat haben und sensible Daten im Zeitalter der nach allen Seiten offenen Internetwelt dennoch sicher zu schützen – das sind die Herausforderungen des 21. Jahrhunderts. Notwendig sind deshalb Security-Lösungen, die diesen Anforderungen gerecht werden und den Arbeitsplatz von heute mobiler und sicherer machen. Sicherheit bringt Einschränkungen, mobile Sicherheit bringt Freiheit und Flexibilität.

## Notebooks als Sicherheitsrisiko

Um den Forderungen nach mehr Flexibilität und Mobilität nachzukommen, statten die Unternehmen ihre Mitarbeiter zunehmend mit mobilen Geräten aus. Der Notebook-Anteil wird nach einer IDC-Prognose bis 2006 auf 44,3 Prozent ansteigen. Mit den Notebooks nehmen die Mitarbeiter aber auch vertrauliche Informationen mit auf ihre Dienstreise. Fern von der geschützten Umgebung des Unternehmens werden die mobilen Geräte oft zum Sicherheitsrisiko, durch unsichere Übertragungswege einerseits und durch Verlust oder Diebstahl andererseits. Laut einer Studie des CSI in Zusammenarbeit mit dem FBI war Notebook-Diebstahl das zweithäufigste Computerverbrechen im Jahr 2003. Oft sind die Diebe dabei nicht nur an der Hardware, sondern auch an den darauf gespeicherten Daten interessiert.

Wird einem mobilen Mitarbeiter das Notebook gestohlen, ist der materielle Schaden bei weitem nicht so groß wie der Verlust von vertraulichen Daten, die auf dem Laptop gespeichert sind, und die so in die Hände von unberechtigten Dritten fallen können. Der integrierte Passwortschutz von mobilen Geräten kann leicht geknackt werden. Insbesondere für Anwälte, Steuerberater oder Ärzte kann das sogar rechtliche Folgen mit sich bringen, wenn vertrauliche Informationen über Klienten und Patienten unzureichend gesichert sind. Ein sinnvolles Mittel, um solch sensible Daten vor dem Zugriff Unberechtigter zu schützen, ist die Verschlüsselung der gesamten Festplatte mit einem mindestens 128-Bit-Schlüssel.

Aber selbst wenn die Daten verschlüsselt wurden, sind sie im Falle eines Verlustes oder Diebstahls erst einmal weg, und es kostet Zeit und Mühe, sie wieder zu beschaffen. Die Gesamtkosten für den Ersatz des Notebooks inklusive des Aufwands für die Beschaffung der gespeicherten Daten (zum Beispiel Verträge) sowie die Einrichtung der persönlichen Umgebung (wie Desktop, Windows- und Anwendungseinstellungen, DFÜ) sind viel höher



Ismet Koyun  
Geschäftsführer Kobil Systems

Geboren in der Türkei  
Seit 1978 in Deutschland:  
Studium der Informatik  
1986 Gründung von Kobil,  
seit 1998 Fokus auf Smart Card  
Terminals und IT-Security-  
Lösungen für starke Authentifikation  
und Datensicherheit

E-Mail: ismet.koyun@kobil.com

als der Wert des Notebooks alleine. PDAs oder USB-Sticks als externe Speicher sind grundsätzlich sicherer vor Diebstahl oder Verlust, da sie meist am Körper getragen werden. Sie bieten aber dennoch keinen sicheren Speicherort für sensible Daten, da die Verschlüsselung entweder unzureichend abgesichert oder gar nicht vorhanden ist.

Kobils Erfahrungen im Security-Business haben gezeigt, dass das Sicherheitsbewusstsein beim elektronischen Datenaustausch zwar zunimmt, die Security-Produkte selbst sich aber nur schwer verkaufen lassen, da bei den unzähligen Einzellösungen der verschiedenen Anbieter keine Kunden-gerechte Ansprache stattfindet. PKI-Projekte (Public Key Infrastructure) sind beispielsweise meist sehr komplex und die darin integrierten Produkte nicht immer leicht zu bedienen. Die Herausforderung bei der Produktentwicklung bestand also darin, einen vertrauenswürdigen externen Speicher in Verbindung mit einem wirkungsvollen Verschlüsselungsmechanismus zu schaffen, der außerdem noch weitere Bereiche der mobilen Sicherheit abdecken kann und einfach in der Installation ist. So sollte dem Anwender damit auch ein zentraler Schlüssel für die Authentifikation in Netzwerke und alle Funktionen eines mobilen Offices zur Verfügung gestellt werden.

Das Ergebnis, Kobil mIdentity, ist ein handliches Produkt, das dem Anwender sämtliche Vorteile der hoch sicheren Smart Card-Technologie mit extrem einfacher Installation und Bedienbarkeit bietet. Alle Komponenten sind bereits in dem kleinen Device integriert, so dass der Anwender sofort starten kann. Es wird nicht einmal eine Installations-CD benötigt, da die Software ebenfalls „on board“ ist. Zentrale Komponenten sind die integrierte E4/hoch-evaluierte Smart Card im SIM-Format, die eine Vielzahl von Anwendungen wie Netzwerk-Authentifikation, Single-Sign-On, Passwortspeicher, digitale Signatur, Daten- und E-Mail-Verschlüsselung ermöglicht, sowie der integrierte Flash-Speicher, der den sicheren Transport von mobilen Daten durch eine 168-Bit-Verschlüsselung erlaubt.



## Mit mIdentity ins DATEV-Portal

Zum Einsatz kommt Kobil mIdentity als sichere Authentifizierungslösung für das DATEV-Web-Portal. DATEV eG ist der führende Anbieter von Software und IT-Dienstleistungen für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sowie deren Mandanten. Die DATEV bietet ihren Mitgliedern ein umfassendes Leistungsspektrum wie Software-Lösungen zur Lohnabrechnung oder den Zugriff via Internet auf Datenbanken mit steuerlichen und rechtlichen Infos. Viele dieser Informationen befinden sich im nicht-öffentlichen Bereich des Internet-Auftritts und sind nur

über einen geschützten Zugang mit einer Smart Card zu erreichen. Die bisherigen Angebote an Sicherheitspaketen, bestehend aus Smart Card, Kartenleser, Hardware-Dongle und Software, werden künftig durch mIdentity ergänzt.

Im Rahmen einer Technologie-Partnerschaft wurde mIdentity dazu in die DATEV-Umgebung integriert. Die DATEV-Kunden erhalten somit eine integrierte Lösung, da Kartenleser (bestückt mit einer DATEV SIM-Karte), Flash-Speicher und mobile Unternehmenslösungen inklusive Software-Lizenzierung in einem Gerät vereint sind. Die Mitglieder haben damit nicht nur einen gesicherten Zugang zum DATEV-Rechenzentrum und zum umfassenden Online-Angebot des nicht-öffentlichen Internet-Bereichs, sondern können auch durch den mobilen Datensafe ihre sensiblen Daten durch Verschlüsselung hoch sicher transportieren. Die Möglichkeit zur digitalen Signatur und Verschlüsselung gewährleistet dem Anwender zudem Vertraulichkeit und Rechtswirksamkeit beim elektronischen Datenaustausch.

In der gemeinsam entwickelten Version für die DATEV wird auch deren Verschlüsselungs- und Signatursoftware des Smart Card-Sicherheitspakets (inklusive der Anwendungssoftware GERVA) integriert. Kobil mIdentity unterstützt alle Smart Card-basierten Funktionen und Anwendungsszenarien, die der DATEV-Anwender bereits gewohnt ist. Und zugleich kann er von allen weiteren Einsatzmöglichkeiten des Geräts profitieren. Das Arbeiten wird sowohl für die DATEV als Anbieter als auch für deren Kunden angenehmer und einfacher, denn statt bisher Rechnerbezogene Dongles für die Freischaltung einzelner DATEV Software-Produkte verwalten zu müssen, kann jetzt jeder User mit seinem eigenen mIdentity beliebige Software-Lizenzen bei sich tragen und überall nutzen, ob zu Hause, im Büro oder unterwegs.

Insbesondere für Steuerberater, Wirtschaftsprüfer und Anwälte ist Vertraulichkeit beim elektronischen Datenaustausch aufgrund der gesetzlichen Vorgaben zur Erfüllung des Datenschutzes unabdingbar. Durch die elektronische Signatur werden E-Mails fälschungssicher und verbindlich. Sie garantiert auch, dass der Absender tatsächlich die Person ist, die sie zu sein vorgibt. Jede nachträgliche Manipulation wird sofort erkennbar. Die DATEV-Mitglieder können mIdentity somit für viele berufsspezifische Anwendungsszenarien einsetzen, die eine elektronische Signatur erforderlich machen: die vollelektronische Einkommensteuererklärung, Steuerkontoabfragen oder etwa den digitalen Mahnbescheid.

Kobil mIdentity ist eine offene Plattform, die mit internationalen Standards arbeitet und von Kobil als strategisches Produkt ständig weiter entwickelt wird. Eine Vielzahl von Einsatzszenarien sind denkbar: vom Consultant bis zum mobilen Vertriebsmitarbeiter. Die Lösung eignet sich gleichermaßen für einzelne Benutzer wie für Unternehmen. Bei Bedarf kann sie auch in eine Corporate-PKI integriert werden. Wie bei allen Smart Card-basierten Lösungen sind bei mIdentity sämtliche Funktionen durch eine starke Zwei-Faktor-Authentifikation geschützt: Der Besitz der Karte (integriert im Gerät) und das Wissen des dazugehörigen PIN-Codes sind für den Zugriff notwendig.

# Anhang



## TELETRUST – Fakten

TELETRUST hat sich in den 15 Jahren seines Bestehens von einer kleinen Gruppe hochmotivierter Fachleute zum Kompetenzverbund für angewandte Kryptographie und Biometrie entwickelt. Basis des Erfolgs ist neben der Sachkenntnis der Experten aus den derzeit 90 Mitgliedsunternehmen und –Organisationen ein hohes Maß an Zielstrebigkeit und Kontinuität der Entwicklung. Dies wird auch in Personalien deutlich:

Seit 1992 wird die inhaltliche Profilierung von TELETRUST in erheblichem Maß durch den Geschäftsführer, Helmut Reimer, forciert und seit 1993 ist der damalige Geschäftsführer von KryptoKom und Gründungsmitglieder von TELETRUST, Norbert Pohlmann, Mitglied des TELETRUST-Vorstand und seit Ende 1998 sein Vorsitzender

Der gemeinnützige Verein hat es sich durch seine Satzung zur Aufgabe gemacht,

- ◆ die Akzeptanz kryptographischer Verfahren zur Realisierung angemessener Sicherheit in Applikationen des elektronischen Geschäftsverkehrs zu verbessern;
- ◆ die Forschung zur Sicherheit des elektronischen Datenaustausches (EDI) und die Anwendung ihrer Ergebnisse sowie die Entwicklung von Standards für dieses Gebiet zu unterstützen;
- ◆ die Ergebnisse der Forschung durch Veröffentlichungen und interdisziplinäre Veranstaltungen sowie Workshops und Kurse zu verbreiten;
- ◆ mit Institutionen in anderen Ländern zusammen zu arbeiten, um Ziele und Standards innerhalb der Europäischen Union zu harmonisieren.

## Chronologie

	1989/1990	1991	1992
	Mitglieder: 13 Vorstand: Vorsitzender: Prof. Dr. Eckart Raubold, GMD Stellvertreter: Dr. Wolfgang Schröder, mbp Beisitzer: Dr. Franz Arnold, SCS Dr. Dieter Weber, DATEV Geschäftsführer: Dr. Karl Rihaczek	Mitglieder: 15 Vorstand: Vorsitzender: Prof. Dr. Eckart Raubold, GMD Stellvertreter: Dr. Wolfgang Schröder, mbp Beisitzer: Dr. Gert Bostelmann, Alcatel SEL Dr. Dieter Weber, DATEV Geschäftsführer: Dr. Klaus Truöl, GMD	Mitglieder: 17 Vorstand: Vorsitzender: Prof. Dr. Eckart Raubold, GMD Stellvertreter: Dr. Dieter Weber, DATEV Beisitzer: Dr. Gert Bostelmann, Alcatel SEL Dietrich Kruse, SNI Geschäftsführer: Prof. Dr. Helmut Reimer
Publikationen			<b>Kommunikation &amp; Sicherheit</b> Herausgeber: Reimer, Struif, TELETRUST, Bad Vilbel
Arbeitsgruppen	Gründung der AG „ <b>Juristische Aspekte</b> “ Leiter: <b>Dr. Ulrich Seidel, GMD</b>		
	Gründung der AG „ <b>Sicherheitsarchitektur</b> “ Leiter: <b>Dietrich Kruse, SNI</b>		
	Gründung der AG „ <b>Anwendungen</b> “ Leiter: <b>Dr. Stefan Jiranek, Teles</b>		
		Gründung der AG „ <b>Marketing</b> “ Leiter: <b>Hartmut Schmidt, IBM</b>	

	1993	1994
	<p>Mitglieder: 20 Vorstand: Vorsitzender: Prof. Dr. Eckart Raubold, GMD Stellvertreter: Dietrich Kruse, SNI Beisitzer: Norbert Pohlmann, KryptoKom Dr. Dieter Weber, DATEV Geschäftsführer: Prof. Dr. Helmut Reimer</p>	<p>Mitglieder: 24 Vorstand: Vorsitzender: Dr. Dieter Weber, DATEV Stellvertreter: Dietrich Kruse, SNI Beisitzer: Norbert Pohlmann, KryptoKom Dr. Otfried P. Schaefer, KVH Geschäftsführer: Prof. Dr. Helmut Reimer</p>
Veranstaltungen	<p><b>Kurs I „Kommunikations- und Datensicherheit“</b> in Ilmenau <b>Forum „Elektronischer Rechtsverkehr“</b> mit der Bundesnotarkammer in Köln (s. Publikationen)</p>	<p><b>Kurs II / III „Kommunikations- und Datensicherheit“</b> Darmstadt / Ilmenau <b>Workshop „Sicherheitsschnittstellen“</b> mit der Gesellschaft für Informatik / Fachgruppe VIS <b>„Verlässliche Informationssysteme“</b> in München (s. Publikationen) <b>1. Forum</b> mit der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung in Bonn (s. Publikationen)</p>
Publikationen	<p><b>Elektronischer Rechtsverkehr – Digitale Signaturen und Rahmenbedingungen</b> Herausgeber: Bundesnotarkammer, Otto Schmidt Verlag, Köln, ISBN 3-504-56032-0</p>	<p><b>Sicherheitsschnittstellen – Konzepte, Anwendungen und Einsatzbeispiele</b> Herausgeber: Fumy, Meister, Reitenspieß, Schäfer, Deutscher Universitäts-Verlag, Wiesbaden, ISBN 3-8244-2059-7 <b>Vertrauenswürdige Informationstechnik für Medizin und Gesundheitsverwaltung</b> <i>TELETRUST</i>, Erfurt Gedruckte Manuskripte des Forums vom 15./16.09.1994 von Bundesärztekammer, Kassenärztliche Bundesvereinigung, <i>TELETRUST</i> Deutschland e.V., Deutsche Gemeinschaft für medizinische Informatik, Biometrie und Epidemiologie</p>
Arbeitsgruppen / Projekte		<p>Neugründung der AG <b>„Juristische Aspekte einer verbindlichen Kommunikation“</b> Leiter: <b>Wolfgang Schäfer, DATEV</b></p>
	<p>Neuer Leiter: <b>Wolfgang Schäfer, DATEV</b></p>	<p>Neuer Leiter: <b>Kurt Maier, Telenet</b></p>
	<p>Umbenennung der AG in <b>„Promotions“</b> Neuer Leiter: Dr. Albert Glade, G&amp;D</p>	
	<p>Gründung der selbständigen Projektgruppe <b>„Kartenterminal“</b> Leiter: <b>Levona Eckstein, GMD</b></p>	

	1995	1996	
	<p>Mitglieder: 33 Vorstand: Vorsitzender: Dr. Dieter Weber, DATEV Stellvertreter: Dr. Albert Glade, G&amp;D Beisitzer: Norbert Pohlmann, KryptoKom Dr. Otfried P. Schaefer, KVH Geschäftsführer: Prof. Dr. Helmut Reimer</p>	<p>Mitglieder: 38 Vorstand: Vorsitzender: Dr. Dieter Weber, DATEV Stellvertreter: Dr. Albert Glade, G&amp;D Beisitzer: Norbert Pohlmann, KryptoKom Dr. Otfried P. Schaefer, KVH Geschäftsführer: Prof. Dr. Helmut Reimer</p>	
Veranstaltungen	<p><b>SYSTEMS 95</b> mit Gemeinschaftsstand „MailTrusT“ in München <b>SYSTEMS-Fachseminar „Chipkarte und vertrauenswürdige Kommunikation“</b> <b>Arbeitskonferenz „TrustCenter 95“</b> mit der Gesellschaft für Informatik / Fachgruppe VIS „Verlässliche Informationssysteme“ in Siegen (s. Publikationen)</p>	<p><b>Kurs IV „Kommunikations- und Datensicherheit“</b> in München <b>Arbeitskonferenz „Digitale Signaturen“</b> mit der Gesellschaft für Informatik / Fachgruppe VIS „Verlässliche Informationssysteme“ in Darmstadt (s. Publikationen)</p>	
Publikationen	<p><b>TrusT Center – Grundlagen, Rechtliche Aspekte, Standardisierung, Realisierung</b> Herausgeber: Horster Vieweg-Verlag, Braunschweig/Wiesbaden, ISBN 3-528-05523-5 <b>Digitale Signatur &amp; Sicherheitssensitive Anwendungen</b> Herausgeber: Glade, Reimer, Struif Vieweg-Verlag, Braunschweig/Wiesbaden, ISBN 3-528-05519-7</p>	<p><b>Digitale Signaturen – Grundlagen, Realisierungen, Rechtliche Aspekte, Anwendungen</b> Herausgeber: Horster, Vieweg-Verlag, Braunschweig/Wiesbaden, ISBN 3-528-05548-0</p>	
Arbeitsgruppen / Projekte		<p>Neuer Leiter: <b>Dr. Joachim Rieß, debis SH</b> Projekt: <b>Q-Siegel</b></p>	
		<p>Projekt: <b>MailTrusT</b> Leiter: <b>Wolfgang Schneider, GMD</b></p>	<p>Projekt: <b>MailTrusT</b> Spezifikation: <b>MailTrusT V1.1</b></p>
		<p>Umbenennung der AG in <b>„Promotions“</b> Neuer Leiter: Dr. Albert Glade, G&amp;D</p>	
			<p>Spezifikation: <b>MKT</b> (Multifunktionales KartenTerminal)</p>
	<p>Gründung der AG <b>„Medizinische Anwendungen einer vertrauenswürdigen Informationstechnik“</b> Leiter: <b>Jürgen Sembritzki, ZI</b></p>		

	1997	1998
	<p>Mitglieder: 59 Vorstand: Vorsitzender: Dr. Albert Glade, G&amp;D Stellvertreter: Stefan v. Ungern-Sternberg, DATEV Beisitzer: Norbert Pohlmann, KryptoKom Dr. Otfried P. Schaefer, KVH Geschäftsführer: Prof. Dr. Helmut Reimer</p>	<p>Mitglieder: 77 Vorstand: Vorsitzender: Norbert Pohlmann, KryptoKom Stellvertreter: Prof. Dr. Heinz Thielmann, GMD Beisitzer: Dr. Norbert Rauh, DATEV Jürgen Sembritzki, ZI f.d.k.V. Geschäftsführer: Prof. Dr. Helmut Reimer</p>
Veranstaltungen	<p><b>CeBIT 97</b> in Hannover; <b>CeBIT-Fachtagung „Digitale Signatur – Sicherheit für geschäftliche Transaktionen im Internet“</b> <b>2. Forum</b> mit der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung in Bonn.</p>	<p><b>CeBIT 98</b> unter dem Motto „Kompetenz im Verbund“ in Hannover mit TTT-Fachkonferenz <b>Internet World 98</b> IT-Sicherheitspavillon mit einigen TELETRUST-Mitgliedern, Berlin <b>Interner TELETRUST-Workshop</b> in Aachen <b>Forum „Informations- und Wissensgesellschaft – Vision und Realität“</b> mit der URANIA in Erfurt <b>Fachtagung „Biometrische Identifikationsverfahren“</b> in Bonn (s. Publikationen) <b>Arbeitskonferenz „Chipkarten“</b> mit der GI / Fachgruppe VIS, München</p>
Publikationen	<p><b>CD „Die digitale Signatur“</b> Herausgeber: TELETRUST (AG5) multimediale Erläuterung der digitalen Signatur, Signaturanwendung mit Chipkarte und diverse Informationen zu TELETRUST</p>	<p><b>Biometrische Identifikationsverfahren.</b> Handout, TELETRUST, Erfurt <b>Chipkarten – Grundlagen, Realisierungen, Sicherheitsaspekte, Anwendungen</b> Herausgeber: Horster, Vieweg-Verlag, Braunschweig/Wiesbaden, ISBN 3-528-05667-3 <b>Kryptoreport – Kryptographische Verfahren im Gesundheits- und Sozialwesen</b> Herausgeber: TELETRUST (AG3), Erfurt – Editor: Christoph Goetz (KV Bayerns) <b>Kriterienkatalog zur Bewertung der Vergleichbarkeit biometrischer Verfahren</b> Herausgeber: TELETRUST (AG6), Erfurt – Editor: Gunter Laßmann (DTAG)</p>
Arbeitsgruppen / Projekte		<p>Projekt: <b>Rechtliche Rahmenbedingungen digitaler Signaturverfahren in den USA</b> Projekt: <b>Markensatzung</b> (Eintragung der Marken MKT, MCT)</p>
		<p>Projekt: <b>Vorevaluierung Chipkarten</b> Projekt: <b>Elektronischer Dienstaussweis</b></p>
		<p>Umstrukturierung und Umbenennung der AG in „<b>Open e-commerce security</b>“ Leiter: <b>Kurt Maier, G&amp;D</b></p>
	Neuer Leiter: Arno Fiedler, Bundesdruckerei	
	Neuer Leiter: <b>Uwe Schnabel, MicroDatec</b> Projekt: UCTS	Projekt: <b>UCTS</b> Spezifikation: UCTS
	Gründung der AG „ <b>Biometrische Identifikationsverfahren</b> “ Leiter: <b>Albert Mokler, SNAT</b>	Neuer Leiter: <b>Hans-Joachim Pelka, BAPT</b> Broschüre: <b>Kriterienkatalog</b>
	Gründung der AG „ <b>MailTrusT</b> “ Leiter: <b>Wolfgang Schneider, GMD</b> Spezifikation: <b>MailTrusT V2</b>	
	Gründung der AG „ <b>Zertifizierungsinfrastrukturen – PKI</b> “ Leiter: <b>Fritz Bauspieß, Secorvo</b>	

1999	
	<p>Mitglieder: 91 Vorstand:     Vorsitzender:         Norbert Pohlmann, KryptoKom     Stellvertreter:         Prof. Dr. Heinz Thielmann, GMD</p> <p>Beisitzer:     Dr. Norbert Rauh, DATEV     Jürgen Sembritzki, ZI f.d.k.V. Geschäftsführer:     Prof. Dr. Helmut Reimer</p>
Veranstaltungen	<p><b>CeBIT 99</b> unter dem Motto „Markt bietet Lösungen“ in Hannover; mit TTT-Fachkonferenz  <b>Workshop „Vorevaluierung Chipkarte“</b> in Essen  <b>Interner TELETRUST-Workshop</b> in Essen  <b>1. Information Security Solutions Europe (ISSE)</b> in Berlin  <b>Tutorial „Internet-Security and Public-Key Infrastructures“</b> in Darmstadt  <b>Arbeitskonferenz „Sicherheitsinfrastrukturen“</b> mit der GI / Fachgruppe VIS, Hamburg  <b>Öffentliche Festveranstaltung „10 Jahre TELETRUST“</b> in Berlin</p>
Publikationen	<p><b>Sicherheitsinfrastrukturen – Grundlagen, Realisierungen, rechtliche Aspekte, Anwendungen</b>  Herausgeber: Horster,  Vieweg-Verlag, Braunschweig/Wiesbaden, ISBN 3-528-05709-2  <b>Broschüre „10 Jahre TELETRUST“</b>  TELETRUST, Erfurt  <b>Rechtliche Rahmenbedingungen digitaler Signaturverfahren in den USA</b>  Autoren: Bizer, Miedbrodt,  Herausgeber: TELETRUST (AG1), Erfurt</p>
Arbeitsgruppen / Projekte	<p>Projekt: <b>Markensatzung</b> (Eintragung der Marke UCTS)</p> <p>Projekt: <b>Vorevaluierung Chipkarten</b>  Projekt: <b>Elektronischer Dienstaussweis</b></p> <p>Broschüre: <b>Kryptoreport</b></p> <p>Projekt: <b>BioTrusT</b>  Leiter: <b>Hans-Henning Arendt, @bc</b></p>



2001	
Mitglieder: 107 Vorstand: Vorsitzender: Stellvertreter:	<p>Beisitzer: Dr. Norbert Rauh, DATEV Jürgen Sembritzki, ZTG Geschäftsführer: Prof. Dr. Helmut Reimer</p> <p>Norbert Pohlmann, Utimaco Prof. Dr. Heinz Thielmann, GMD</p>
Veranstaltungen	<p><b>CeBIT 2001</b> in Hannover; <i>TELETRUST</i> war wieder im Bereich CefIS präsent. Absolutes Highlight auf dem TTT-Stand war der Startschuss zur European Bridge-CA durch Bundesinnenminister Otto Schily, er auch die Schirmherrschaft über die EB-CA übernahm.</p> <p><b>CeBIT-Fachtagung „Verbindliche elektronische Geschäftsprozesse“</b></p> <p><b>RSA conference 2001</b> in San Francisco (USA) Erstmals war TTT mit einigen seiner Mitglieder und dem BMWi deutlich präsent: einige Vorträge in der Konferenz, durch AUMA und BMWi unterstützter Gemeinschaftsstand (200m<sup>2</sup>) in der Ausstellung, „Deutscher Abend“ auf einer Barkasse in der Bucht von San Francisco. Highlights: Besuche von Jim Bizdos und Staatssekretär Tacke bei TTT.</p> <p><b>3. Information Security Solutions Europe (ISSE)</b> in London Der TTT-Innovationspreis wurde anlässlich des GalaDinner an die bos KG für die Verwendung des „Internetportals für Bürger und Unternehmen“ übergeben.</p> <p><b>SYSTEMS 2001</b> in München <i>TELETRUST</i> war neben BITKOM und BSI ideeller Träger des IT-Security-Forums.</p> <p><b>BioTrusT-Workshop</b> in Gießen In Kooperation mit FhG SIT <b>TTT-Tutorial „Internet Security and Public Key Infrastructures“</b> mit Dr. Stephen Kent in Darmstadt</p> <p><b>Interner TELETRUST-Workshop (IWS 2001)</b> in Aachen Zwei <b>Abstimmungstreffen AG- und Projektleiter – TTT-Vorstand</b></p>
Publikationen	<p><b>Entwicklung eines neuen TTT-Layouts</b> für Flyer, Broschüren, Poster, Pressemappen etc. Fachspezifischer Flyer der <b>AG7; TTT-Image-Flyer</b> (engl.) AG4-Broschüre <b>„Trusted E-Commerce“</b> (dt. + engl.) DuD Heft 9/2001 mit Themen, die TTT-Aktionen mit europäischem Akzent beschreiben TTT-Sonderteil in <b>„Union – Kommunalpolitische Blätter“</b> <b>16 Pressemitteilungen</b> zu unterschiedlichen aktuellen Anlässen und Themen <b>ISIS-MTT-Spezifikation</b> (V1.0.1), Testkonzept, Test-Spezifikation</p>
Arbeitsgruppen / Projekte	<p>Neuer Leiter: <b>Anja Miedbrodt, DaimlerChrysler</b></p> <p>Projekt: <b>OID's</b></p> <p>Broschüre: <b>Trusted E-Commerce</b></p> <p><i>TELETRUST-Projekt: ISIS-MTT</i> Leiter: Arno Fiedler</p>

2002	
Mitglieder: 97 Vorstand: Vorsitzender: Dr. Norbert Pohlmann, Utimaco Stellvertreter: Michael Leistenschneider, DATEV	Beisitzer: Prof. Dr. Claudia Eckert, FhG SIT Jürgen Sembritzki, ZTG Geschäftsführer: Prof. Dr. Helmut Reimer
Veranstaltungen	<p><b>RSA conference 2002</b> in San José (USA) Größte ausländische Präsenz in der Ausstellung durch TTT-Gemeinschaftsstand (unterstützt durch AUMA und BMWi).</p> <p><b>CeBIT 2002</b> in Hannover; TELETRUST war wieder im Bereich CefIS präsent. Highlight auf dem TTT-Stand war der Besuch des Staatssekretärs Tacke (BMW)</p> <p><b>CeBIT-Fachtagung „PKI-gestützte elektronische Geschäftsprozesse“</b></p> <p><b>4. Information Security Solutions Europe (ISSE)</b> in Paris Der TTT-Innovationspreis wurde in diesem Jahr durch Vorstandsbeschluss wegen nur weniger Bewerbungen nicht verliehen.</p> <p><b>SYSTEMS 2002</b> in München TELETRUST war neben BITKOM und BSI ideeller Träger des IT-Security-Forums.</p> <p><b>Interner TELETRUST-Workshop (IWS 2002)</b> in Darmstadt</p> <p><b>BioTrusT-Abschluss-Workshop</b> in Berlin</p> <p><b>Abstimmungstreffen AG- und Projektleiter – TTT-Vorstand</b> in Krefeld</p>
Publikationen	<p>Thematischer TTT-Flyer zu <b>EB-CA</b> und <b>ISIS-MTT</b> (engl.)</p> <p>AG4-Broschüre „<b>Trusted E-Commerce – Die Idee wird Wirklichkeit</b>“ (dt. + engl.)</p> <p>AG6-Broschüre „<b>Kriterienkatalog zur Vergleichbarkeit biometrischer Verfahren</b>“ (V2.0)</p> <p>DuD Heft 9/2002 mit Themen, die TTT-Aktionen mit europäischem Akzent beschreiben</p> <p><b>17 Pressemitteilungen</b> zu unterschiedlichen aktuellen Anlässen und Themen</p> <p><b>ISIS-MTT-Spezifikation</b> (V1.0.2), Testbed, Kriterien für ISIS-MTT-Siegel</p> <p><b>TELETRUST-Jahresbericht 2001</b></p>
Arbeitsgruppen / Projekte	<p>Neuer Leiter: <b>RA Stefan Engel-Flehsig</b></p> <hr/> <p>Broschüre: <b>Trusted E-Commerce – Die Idee wird Wirklichkeit</b></p> <hr/> <hr/> <hr/> <p>Broschüre: <b>Kriterienkatalog V 2.0</b></p> <hr/> <hr/> <hr/>

2003	
Veranstaltungen	<p>Mitglieder: 82 Vorstand: Vorsitzender: Dr. Norbert Pohlmann, Utimaco Stellvertreter: Michael Leistenschneider, DATEV</p> <p>Beisitzer: Prof. Dr. Claudia Eckert, FhG SIT Jürgen Sembritzki, ZTG Geschäftsführer: Prof. Dr. Helmut Reimer</p>
Publikationen	<p><b>CeBIT 2003</b> in Hannover; <i>TELETRUST</i> war wieder im Bereich CefIS präsent. Themen waren insbesondere ISIS-MTT und EB-CA mit praktischen Beispielen. <b>CeBIT-Fachtagung „Informationssicherheit: Initiativen für unbeschränkte Geschäftsprozesse“</b> <b>DACH-Konferenz 2003</b> in Erfurt Die bisher erfolgreichste DACH Security wurde unter besonderer TTT-Beteiligung an der Uni Erfurt durchgeführt. <b>RSA conference 2003</b> in San Francisco (USA) Zum dritten Mal war TTT mit einigen seiner Mitglieder und dem BMWA deutlich präsent – unterstützt durch AUMA und BMWA. „Deutscher Abend“, Besuche bei US-Unternehmen Expertenmeeting waren durch TTT organisierte Randevents. <b>BSI-Kongress 2003</b> in Bad Godesberg <b>Workshop „Cross Border Certificate Services and Electronic Procurement“</b> in Tallinn <b>5. Information Security Solutions Europe (ISSE)</b> in Wien Der TTT-Innovationspreis wurde anlässlich der Conference Party an die Oberfinanzdirektion München für die Verwendung von ELSTER II übergeben. <b>SYSTEMS 2003</b> in München <i>TELETRUST</i> war neben BITKOM und BSI ideeller Träger des IT-Security-Forums. <b>Interner TELETRUST-Workshop (IWS 2003)</b> in Krefeld</p>
Arbeitsgruppen / Projekte	<p>Fachspezifischer Flyer zu <b>ISIS-MTT</b> und <b>EB-CA</b> (engl.) <b>Landkarte Biometrie</b> (gemeinsam mit BITKOM und ZVEI) <b>DuD Heft 9/2003</b> mit Themen, die TTT-Aktionen mit europäischem Akzent beschreiben (Schwerpunkt Identitätsmanagement) <b>14 Pressemitteilungen</b> zu unterschiedlichen aktuellen Anlässen und Themen <b>TELETRUST-Jahresbericht 2002</b></p> <hr/> <p>Neugründung und Umstrukturierung der AG unter Einbeziehung der selbständigen Projektgruppe Kartenterminals zur AG „<b>Personal Security Environment – PSE</b>“ Leiter: <b>Michael Hartmann, Kobil</b></p> <hr/> <p>Gründung der AG „<b>Onlineprozesse und Identitätsmanagement</b>“ Leiter: <b>Sachar Paulus, SAP</b></p> <hr/> <p>Vorbereitung der Broschüre: <b>Kartenreport</b></p> <hr/> <p>Broschüre: <b>Interoperabilität von PKI</b></p>

## TELETRUST-Mitglieder – Stand Juli 2004

ABDA – Bundesvereinigung Deutscher Apothekerverbände  
Carl-Mannich-Straße 26, 65760 Eschborn

Applied Security GmbH  
Industriestraße 16, 63811 Stockstadt

@bc@ – Arendt Business Consulting  
Malbachweg 3, 65510 Idstein

Atos Origin GmbH  
Lohberg 10, 49716 Meppen

AuthentiDate International AG  
Großenbaumer Weg 6, 40472 Düsseldorf

AWV – Arbeitsgemeinschaft für wirtschaftliche  
Verwaltung e.V.  
Düsseldorfer Straße 40, 65760 Eschborn/Ts.

BGS Systemplanung AG  
Robert-Koch-Straße 41, 55129 Mainz

Bromba GmbH  
Frankfurter Ring 193a, 80807 München

Bundesamt für Sicherheit in der Informationstechnik  
Godesberger Allee 183, 53175 Bonn

Bundesdruckerei GmbH  
Oranienstraße 91, 10958 Berlin

Bundeskriminalamt Wiesbaden  
Thaerstraße 11, 65173 Wiesbaden

CAST e.V.  
Fraunhofer Straße 5, 64283 Darmstadt

Cognitec Systems GmbH  
An der Flutrinne 12, 01139 Dresden

COMPUTAS Gisela Geuhs GmbH  
Neusser Straße 720, 50737 Köln

Computer-Communication Networks GmbH  
Steinhof 5, 40699 Erkrath

cv cryptovision gmbh  
Munscheidstraße 14, 45886 Gelsenkirchen

C1 Securos GmbH  
Postfach 100118, 55133 Mainz

DATEV eG  
Paumgartnerstraße 6, 90429 Nürnberg

Weitere Informationen sind erhältlich über  
**TELETRUST Deutschland e.V.**  
<http://www.teletrust.de>

Geschäftsstelle:

Prof. Dr. Helmut Reimer  
Chamissostraße 11, D-99096 Erfurt  
Tel: +49 361 3460531  
Fax: +49 361 3453957  
E-Mail: [info@teletrust.de](mailto:info@teletrust.de)

Debold & Lux  
Reinbecker Weg 61, 21029 Hamburg

DERMALOG Identification Systems GmbH  
Mittelweg 120, 20148 Hamburg

Deutsche Bank AG  
Frankfurter Str. 84, 65760 Eschborn

Deutsche Telekom AG  
c/o T-Systems International GmbH  
ITC Security  
Lyonerstrasse 15, 60528 Frankfurt

Deutscher Sparkassen Verlag GmbH  
Am Wallgraben 115, 70565 Stuttgart

DFN – Verein zur Förderung eines Deutschen  
Forschungsnetzes e.V.  
Anhalter Straße 1, 10963 Berlin

DGN Deutsches Gesundheitsnetz  
Service GmbH  
Heerdter Lohweg 35, 40549 Düsseldorf

DIHT / DE-CODA GmbH  
Einemstraße 5, 10787 Berlin

Dr. Fehr GmbH  
Wilhelm-Busch-Straße 16, 65479 Raunheim

D-Trust GmbH  
Kommandantenstraße 15, 10969 Berlin

Fachhochschule Gießen-Friedberg  
Fachbereich Elektrotechnik II  
Wilhelm-Leuschner-Straße 13, 61169 Friedberg

Fachhochschule Gelsenkirchen  
Neidenburgerstraße 43, 45877 Gelsenkirchen

Fraunhofer-Institut für Biomedizinische Technik  
Ensheimer Straße 48, 66386 St. Ingbert

Fraunhofer-Institut für Sichere Telekooperation  
Rheinstraße 75, 64295 Darmstadt

GAD – Gesellschaft für automatische Datenverarbeitung eG  
Weseler Straße 500-510, 48163 Münster/Westf.

Gemplus GmbH  
Mercedesstraße 13, 70794 Filderstadt

Giesecke & Devrient GmbH  
Division Zahlungsverkehrs- und Sicherheitssysteme  
Prinzregentenstraße 159, 81677 München

GITS AG  
Universitätsstraße 150, 44780 Bochum

Guardeon Solutions AG  
Rosenheimer Straße 116, 81669 München

Horst Görtz Institut- Fakultät Mathematik  
c/o Ruhr-Universität Bochum  
Universitätsstraße 150, 44780 Bochum

Infineon Technologies AG  
St.-Martin-Straße 76, 81541 München

INFORA GmbH  
Cicerostraße 21, 10709 Berlin

ITSG – Informationstechnische Servicestelle der  
Gesetzlichen Krankenversicherung GmbH  
Heinrich-Sahm-Straße 1, 63110 Rodgau

Kassenärztliche Bundesvereinigung  
Herbert-Lewin-Straße 3, 50931 Köln

Kassenärztliche Vereinigung Bayerns  
Arabellastraße 30, 81925 München

Kassenärztliche Vereinigung Hessen  
Georgi-Voigt-Straße 15, 60235 Frankfurt/Main

Kassenzahnärztliche Bundesvereinigung  
Postfach 41 01 69, 50861 Köln

KOBIL Systems GmbH  
Weinsheimer Straße 71, 67547 Worms

media transfer AG  
Dolivostraße 11, 64293 Darmstadt

MicroDatec GmbH  
Zeulenrodaer Straße 17, 99091 Erfurt

Microsoft GmbH  
Edisonstraße 1, 85713 Unterschleißheim

NEC Deutschland GmbH  
Reichenbachstraße 1, 85737 Ismaning

NetSys.IT GbR  
Weimarer Straße 28, 98693 Ilmenau

Nexus Technology GmbH  
Willhoop 1, 22453 Hamburg

Nimbus Network  
Offenbacher Straße 8, 14197 Berlin

noventum consulting  
Münstertstraße 111, 48155 Münster

ORGA Kartensysteme GmbH  
An der Kapelle 2, 33104 Paderborn

PAV Card GmbH  
Hamburger Straße 6, 22952 Lütjensee

Philips Semiconductors  
Hammerbrookstraße 69, 20097 Hamburg

PREH-Werke GmbH & Co. KG  
An der Stadthalle, 97616 Bad Neustadt a.d. Saale

ROHDE & SCHWARZ SIT GMBH  
Agastraße 3, 12489 Berlin

RSA Security GmbH  
Ziegelstraße 8, 63065 Offenbach

SAP AG  
Technology Development  
Neurottstraße 16, 69190 Walldorf

SCM Microsystems GmbH  
Sperl-Ring 4, 85276 Pfaffenhofen

SD Industries GmbH  
Äußere Günzburger Straße 2-10, 89423 Gundelfingen

Secaron AG  
Ludwigstraße 45b, 85399 Hallbergmoos

Secartis AG  
Bretonischer Ring 3, 85630 Grasbrunn

Secorvo Security Consulting GmbH  
Albert-Nestler-Straße 9, 76131 Karlsruhe

secrypt GmbH  
Bessemmer Straße 82, 12103 Berlin

SECUDE GmbH  
Dolivostraße 11, 64293 Darmstadt

Secunet – Security Networks AG  
Mergenthaler Allee 77, 65760 Eschborn

Security for Business GmbH (S4B)  
Martinskirchweg 11, 67346 Speyer

Siemens AG  
Postfach 80 17 60, 81541 München

SignCard GmbH & Co. KG  
Nürnberger Straße 1, 90546 Stein

SIZ – Informatikzentrum der Sparkassenorganisation GmbH  
Königswinterer Straße 552, 53227 Bonn

Smiths Heimann Biometrics GmbH  
Unstrutweg 4, 07743 Jena

SOFTPRO  
Software Professional GmbH & Co. KG  
Wilhelmstraße 34, 71034 Böblingen

SRC Security Research & Consulting GmbH  
Graurheindorfer Straße 149A, 53117 Bonn

STMicroelectronics GmbH  
Bretonischer Ring 4, 85630 Grasbrunn

TC TrustCenter AG  
Sonninstraße 24-28, 20097 Hamburg

Teleca Systems GmbH  
Neumeyerstraße 50, 90411 Nürnberg

THALES e-TRANSACTIONS GmbH  
Konrad-Zuse-Straße 19-21, 36251 Bad Hersfeld

TÜV Informationstechnik GmbH  
Am Technologiepark 1, 45307 Essen

T-Systems GEI GmbH  
Rabinstraße 8, 53111 Bonn

Utimaco Safeware AG  
Hohemarkstraße 22, 61440 Oberursel

Verband der Privatärztlichen Verrechnungsstellen  
Tieckstraße 37, 10115 Berlin

Verband für Sicherheit in der Wirtschaft  
Mitteldeutschlands e.V.  
Carl-Zeiss-Straße 1, 07739 Jena

VOI – Verband Organisations- und Informationssysteme e.V.  
Postfach 180160, 53031 Bonn

VOICE.TRUST AG  
Wittelsbacher Straße 2a, 82319 Starnberg

Zentrum für Telematik im Gesundheitswesen GmbH  
Campus Fichtenhain 42, 47807 Krefeld

2B Advice GmbH  
Kölnstraße 103, 53111 Bonn

Ehrenmitglieder:  
Dietrich Kruse  
Dr. Karl Rihaczek

Assoziierte Mitglieder:  
GDD e.V.  
PKI – Forum  
Silicon Trust



> [www.teletrust.de](http://www.teletrust.de)