e-billing, digitale Signatur, ein Statusbericht

Hans G. Zeger, A-CERT

DSAG: AG SRM Linz, 16. 3.2011

A-CERT CERTIFICATION SERVICE

ARGE DATEN als Zertifizierungsdienstleister

Zertifizierungsdienste seit 1997

Zertifizierungsanbieter gem. SigG 2000

- **A-CERT ADVANCED**
  fortgeschrittene Signatur gem. § 2 Z 3 SigG
- **A-CERT GLOBALTRUST**
  technische Zertifikate (Serverzertifikate gem. X509v3)
- **A-CERT COMPANY**
  Public Key Infrastructure (PKI) für Unternehmen
- **A-CERT TIMESTAMP**
  Zeitstempeldienst für revisionssichere Archivierung
- **A-CERT GOVERNMENT**
  Amtssignaturzertifikate für die öffentliche Verwaltung gem. § 19 e-Government-Gesetz
- **GLOBALTRUST QUALIFIED (in Planung)**
  qualifizierte Signatur gem. § 2 Z 3a SigG

A-CERT CERTIFICATION SERVICE

©ARGE DATEN 2011

Referenzen A-CERT Zertifizierungsprodukte

A-CERT CERTIFICATION SERVICE

Digitale Signaturen und Zertifikate sind Instrumente zur Herstellung von Vertrauen zwischen "unbekannten" Teilnehmern im Online-Rechtsverkehr

A-CERT CERTIFICATION SERVICE

©ARGE DATEN 2011

Grundlagen Signaturgesetz (SigG)

Signaturgesetz 2000

- jeder kann Signaturverfahren nach eigenem Ermessen einsetzen
- jedes Signatur-Verfahren ist rechtlich gültig
- "qualifizierte" Signaturdienste für Dritte sind registrierungs- bzw aufsichtspflichtig
- Verschiedene Signaturformen
  - gewöhnliche (technische) Signatur
  - "fortgeschrittene" Signatur § 2 Z 3 SigG
  - Amtssignatur, Verwaltungssignatur
  - "qualifizierte" Signatur § 2 Z 3a SigG
- Umfang der Gültigkeit richtet sich nach gesetzlichen Bestimmungen oder privatrechtlicher Vereinbarung
- "qualifizierte" Signaturen müssen von Behörden als eigenhändig anerkannt werden

Grundlagen Signaturgesetz (SigG)

Fortgeschrittene Signatur und Zertifikat (§ 2 Z 3 SigG)

Signatur ...

- ... ist ausschliesslich dem Signator zugeordnet (lit. a)
- ... erlaubt die Identifizierung des Signators (lit. b)
- ... steht unter alleiniger Kontrolle des Signators (lit. c)
- ... erlaubt nachträgliche Veränderung der Daten zu erkennen (lit. d)

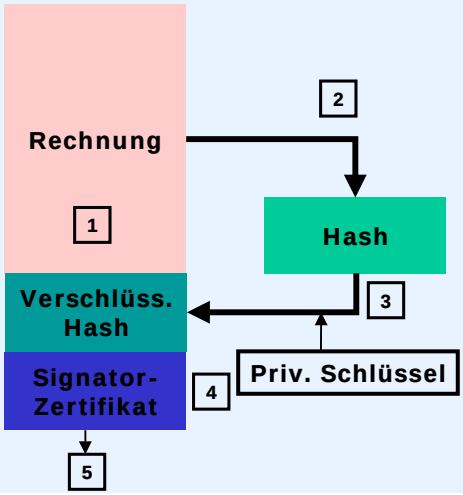
Was tut A-CERT als Zertifizierungsstelle?

- identifiziert den Signator (lit.b)
- stellt Techniken zur Signatur bereit (lit. a,d)
- unterstützt und berät Signator (lit.c)

A-CERT CERTIFICATION SERVICE
©ARGE DATEN 2011

Grundlagen Signatur

Wie die Signatur auf einem Dokument aufgebracht?

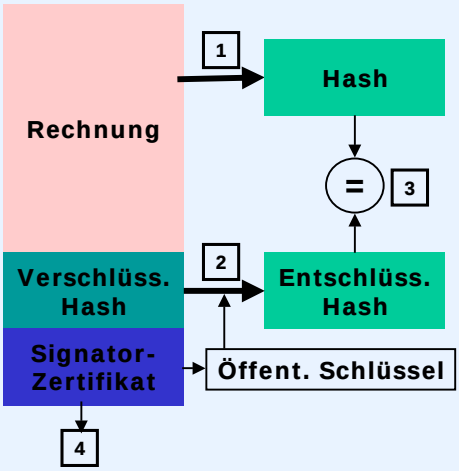


- 1. Dokument (Rechnung)
- 2. Erzeugen eines Hash des Dokuments (Rechnung)
- 3. Verschlüsseln des Hash mit privatem Schlüssel des Absenders
- 4. Signatorzertifikat + öffentlichen Schlüssel beifügen
- 5. signiertes Dokument (Rechnung) versenden

A-CERT CERTIFICATION SERVICE

Grundlagen Signatur

Wie wird die Signatur geprüft?



- 1. Empfänger berechnet aus der Rechnung Hash
- 2. Empfänger entschlüsselt den verschlüsselten Hash mit dem öffentlichen Schlüssel des Absenders
- 3. Empfänger vergleicht die beiden Hashwerte
- 4. Empfänger prüft Online die Gültigkeit des Zertifikats

A-CERT CERTIFICATION SERVICE

kleine (Kultur-)Geschichte zu eBilling

- 2001: EU-RL 2001/115/EG (Mehrwertsteuerrichtlinie)
- 2003: Verordnung 583/2003 des BMF zur elektronischen Rechnungslegung
- 2004: Registrierung des fortgeschrittenen Zertifizierungsdienstes A-CERT ADVANCED bei RTR/TKK
- 2005-10: mehrere - im Kern gleichbleibende - Richtlinien des BMF zur Verordnung
- 2010: EU will weitere Authentisierungsverfahren zur elektronischen Rechnungslegung ermöglichen
- 20??: Ende der unsignierten Fax-Rechnung

alle Dokumente Online unter:
http://www.a-cert.at/static/a-cert-advanced-praesentation-komplett.pdf

Inhalt der BMF-Richtlinie (Auszug)

- Zustimmung des Empfängers erforderlich (reicht aber auch stillschweigende Billigung oder Praxis)
- es muss "fortgeschrittene" Signatur verwendet werden (Ausnahmen bei EDI und Rechnungsübermittlung an Bund)
- Signatur + Verfahren müssen leicht nachprüfbar sein, es dürfen aber externe Prüfstellen verwendet werden (etwa https://pruefung.signatur.rtr.at/)
- Ausdruck als vorläufiger Nachweis einer Rechnung zulässig
- Signatur mus auf eine natürliche Person ausgestellt sein
- Signatur durch Dritte (Dienstleister) ist zulässig
- mehrere Rechnungen können mit einer Signatur unterschrieben werden

derzeitige Version BMF-010219/0288-VI/4/2010 Stand 18.11.2010

Warum elektronische Rechnung?

Nutzen des Ausstellers

- Integration des Rechnungsversands in Rechnungslegung/Buchhaltung
- vereinfachtes Handling (Drucken, Kuvertieren, ...)
- raschere Zustellung ⇨ frühere Bezahlung??
- geringere Zustell- und Materialkosten (Porto, Papier)

Nutzen des Empfängers

- Integration der Rechnungübernahme in Rechnungslegung/Buchhaltung (kein OCR, Scannen, ...)
- Automatisierung der Rechnungsprüfung
- vereinfachte Archivierung, bessere Terminkontrolle,

Grenzen der elektronischen Rechnung

- Konsumenten: erwarten Papierrechnung, sind mit elektronischer Archivierung überfordert
- kleine Unternehmen, ohne integriertes Buchhaltungs- und Archivierungswesen haben keine Vorteile
- kleine Unternehmen, mit geringen Belegszahlen bei denen Papierhandling und Versand "nebenbei" erfolgen
- Unternehmen, bei denen Rechnung nur Teil des Gesamtbelegs ist (Parkhäuser, Eintrittskarten, Kinokarten, ...)
- Unternehmen, bei denen Rechnung persönlich übergeben wird: klassische Freizeitbetriebe, Restaurants, Taxis, ...
- Unternehmen, bei denen Rechnungen nicht üblich sind: Marktfahrer, "kalte Hand-Regel", ...

Fragen aus der täglichen Praxis

- Wer darf signieren?
  Jeder Mitarbeiter, der im Unternehmen beauftragt wurde
- Wer sollte signieren?
  Jemand im Unternehmen der tatsächlich den technischen Prozess beaufsichtigt
- Ist Dienstleistersignierung zulässig?
  Jeder Rechnungsleger kann sich eines Dritten für die Signatur der Rechnung bedienen
- Muss der Dritte spezifische Anforderungen erfüllen?
  Nein, er muss nur fortgeschrittene Signaturverfahren verwenden
- Darf automatisch signiert werden?
  Ja, die Willenserfordernis wie bei der "qualifizierten" Signatur ist nicht gegeben

Besonderheit des Signaturmarktes

- Abweichend von anderen IT-Lösungen (Buchhaltung, Archivierung, Kommunikationstechnik, ...) ist dieser Markt stark gesetzlich reguliert

Einige Lösungen jedoch wenig erfolgreich

- Akzeptanzgründe (Bürgerkarte)
- unklare gesetzliche Vorgaben, siehe GTelG
- wirtschaftliche Interessen und bestehende alternative Lösungen, siehe Online-Banking
- mangelnde Investitionssicherheit, kurze Laufzeiten

Ist damit die Idee der digitalen Signatur gescheitert?

digitale Signatur vs. Unterschrift

NEIN - aber man sollte die Unterschiede zur "natürlichen" Unterschrift kennen

Fehlende unmittelbare Einsichtigkeit
- einer konventionellen Unterschriftenleistung kann man zuschauen, einer digitalen darf man nicht zuschauen

Wiederholbarkeit
- konventionelle Unterschriften sind nicht wiederholbar, Identität gilt als Beweis für eine Fälschung, bei der DigSig ist Wiederholbarkeit zentrales Qualitätsmerkmal

Beschränkte Gültigkeit
- konventionelle Unterschrift ist unbeschränkt gültig und kostenfrei, bei der DigSig ist die Gültigkeit unbestimmt

Möglichkeit der exakten Zeitinformation
- konventionelle Unterschriften enthalten keine sicheren Zeitinformationen, DigSig können diese enthalten

Signaturmarkt und Alternativen

... und man sollte die Alternativen zur digitalen Signatur kennen

- Applikationsplattformen, wie Portalverbund, eBilling-Plattformen, Zustell- und Validierungsservices
- propriäteres IT-Sicherheits-Management, wie derzeit bei den meisten DocumentManagementSystemen
- Token-Lösungen, wie Handy-PIN/TAN, SecurityCard, ...

- bestehende Anmeldeverfahren (Login/PSW) werden erhalten bleiben, insbesondere beim privaten Enduser, der vielleicht 3-5 Kennungen zu verwalten hat

Einsatzmöglichkeiten fortgeschrittene Signatur

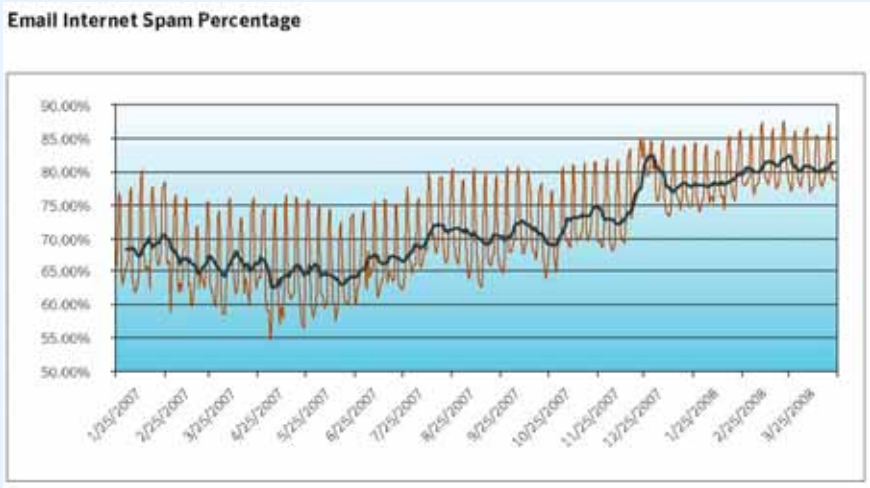
- elektronische Rechnungslegung, inkl. Gutschriften, Bestellungen, Auftragsbestätigungen, Lieferscheine, ...
- Signatur von Bescheiden, behördlichen Mitteilungen
- signieren von Mails
- Softwaresignatur
- Dokumentenmanagement (Vidierung elektronischer Dokumente)
- Vergabe von Zeitstempel für Dokumente

unabhängig vom Dateiformat einsetzbar

- beliebige Dokumentenformate, wie .xml, .pdf, .txt, .html, .doc, ...

.pdf ist bei Rechnungslegung derzeit beliebtestes Format

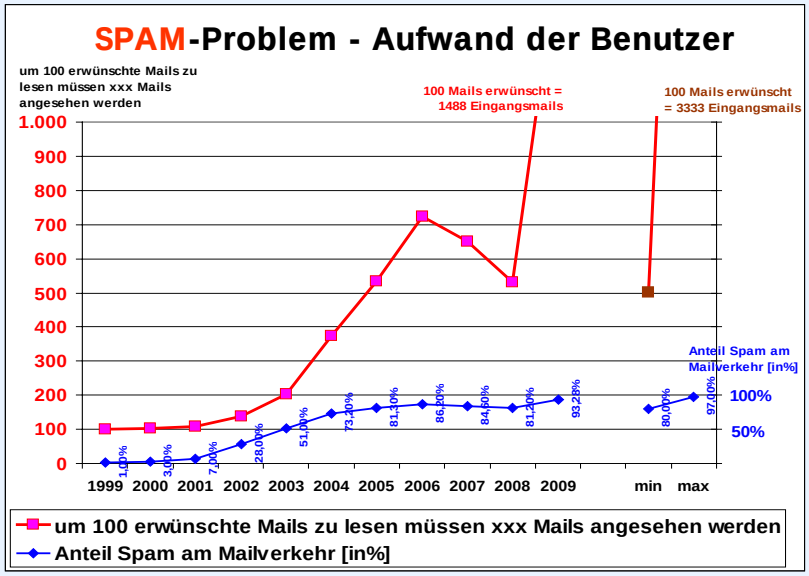
SPAM-Problem - Ausmaß



The trend line demonstrates a 7-day moving average.

Quelle: Symantec

Signaturanwendung Mailserver

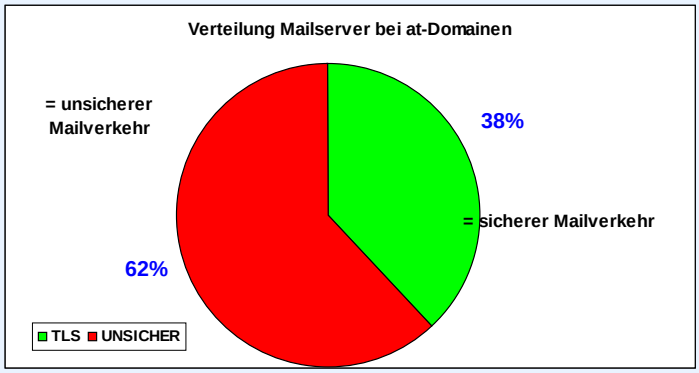


A-CERT CERTIFICATION SERVICE

Signaturanwendung Mailserver

TLS-Mailserver als Spam-Antwort?

TLS = Transport Layer Security (TLS) :
Standardisierung des sicheren Datenverkehrs auf Transportebene, Nachfolger von SSL (Secure Socket Layer)



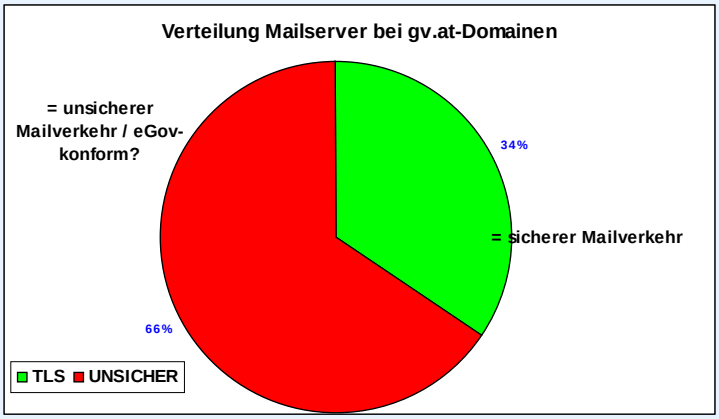
Ausgewertet wurde der Mailverkehr des eines Monats (Mailserver aus 910 at-domains)

A-CERT CERTIFICATION SERVICE

Signaturanwendung Mailserver

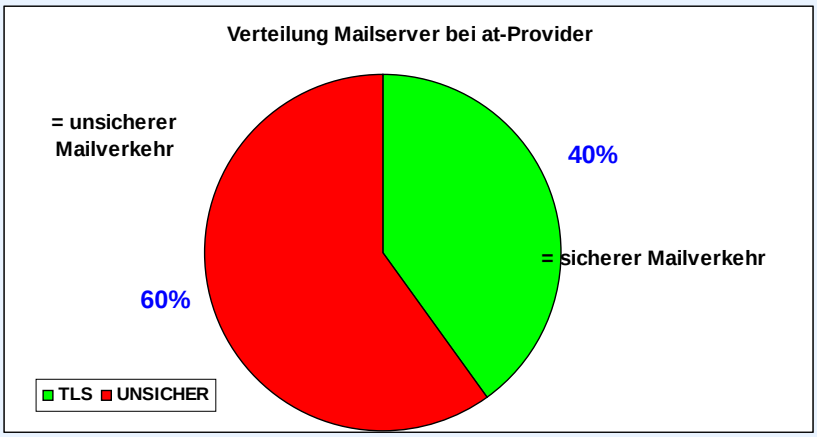
... und was machen die Vorbilder?

eGovernment-Sektor (*.gv.at-Mail-Server)



Signaturanwendung Mailserver

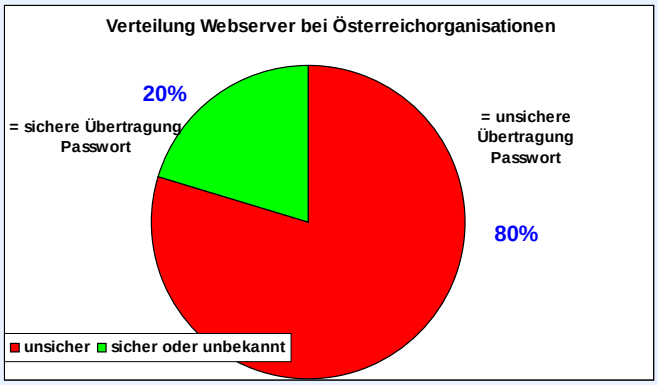
Vorbilder II: Internet-Service Provider



Signaturanwendung Web/eCommerceserver

Sichere Übertragung vertraulicher Daten

Seit 2002 schreibt EG-Richtlinie Telekommunikation sichere und identifizierte Datenübertragung vor



Ausgewertet wurden Formulare von etwa 600 österreichischen Organisationen

Signaturmarkt im Umbruch

Nischen und Märkte, abseits von eBilling ...

- Verschlüsselte Mailübertragung durch Mailserver (TLS statt Individualsignierung)
- zertifizierte Webseiten, sichere Webkommunikation
- longterm Dokumentenmanagement (Online-Tresore) (Vidierung und Archivierung elektronischer Dokumente)
- zeitliche Synchronisation von Geschäftsprozessen
- Signatur von Programmen
- Signatur von Protokollen (z.B. gem. §14 DSG erstellte Protokolle)
- Unternehmens-PKIs (z.B. Stromhandel, Lebensmittelhandel)
- "Web der Dinge", Ausstattung "smarter" Geräte mit Zertifikaten zur sicheren Identifikation (z.B. SmartMeter, SmartPhones, ...)

... und wenn das alles funktioniert ...

- Online-Identifikation von Maschinen und Menschen ("Single Sign On")

... danach kann man weiter schauen ...

Signaturmarkt im Umbruch

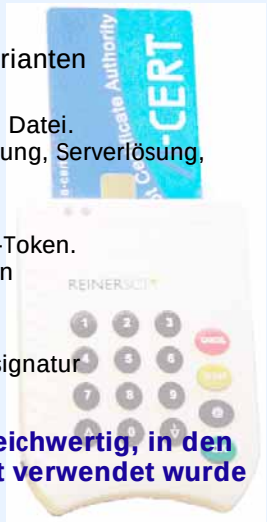
Digitale Signatur sollte dort verwendet und gefördert werden, wo sie schon funktioniert

A-CERT fortgeschrittene Signatur

A-CERT ADVANCED Lösungen

Fortgeschrittene Signatur gem. SigG in drei Varianten

- **Version I: Crypto-Datei**
  Die Signatur erfolgt mittels einer verschlüsselten Datei.
  Typischer Anwendungsfall: gesicherte IT-Umgebung, Serverlösung, Massensignatur
- **Version II: eToken**
  Die Signatur erfolgt mittels Smart-Chip auf USB-Token.
  Typischer Anwendungsfall: mobile Anwendungen
- **Version III: Smartcard**
  Die Signatur erfolgt mittels Smartcard.
  Typischer Anwendungsfall: Workstations, Einzelsignatur



Signaturtechnisch sind alle Varianten gleichwertig, in den Zertifikaten ist vermerkt, welches Produkt verwendet wurde

A-CERT Entwicklungen

A-CERT Projekte

GLOBALTRUST QUALIFIED

"Qualifizierte" digitale Signatur gemäß SigG
derzeit Vorbereitung der österreichischen Registrierung
spezifische Anwendungsbereiche, wie elektronische Ausschreibungen

A-CERT COMPANY

Unterstützung von Unternehmen im Aufbau eigener Public Key Infrastrucutures, insbesondere beim Einsatz in "smarten" Geräten
Schwerpunkt sind Langzeitzertifikate bis 2036

Kontaktinformationen

Vortragender: Hans G. Zeger
ARGE DATEN - Österreichische Gesellschaft für Datenschutz
A-1160 Wien, Redtenbachergasse 20

Tel.:	0676 / 9107032
Fax.:	01 / 4803209
Mail A-CERT:	info@a-cert.at
Mail persönlich:	hans.zeger@a-cert.at
Zertifizierung:	http://www.a-cert.at
WWW-Verein:	http://www.argedaten.at

alle rechtlich relevanten Dokumente zu eBilling:
http://www.a-cert.at/static/a-cert-advanced-praesentation-komplett.pdf

Ich danke für Ihre Aufmerksamkeit