Public-Key Infrastrukturen in der Phase der Konsolidierung und Anwendung

Detlef Hühnlein

secunet Security Networks AG
Sudetenstr. 16, 96247 Michelau
detlef.huehnlein@secunet.com

Zusammenfassung

Dieses Papier widmet sich aktuellen Entwicklungen im Umfeld von Public-Key Infrastrukturen (PKI). Insbesondere wird ein kompakter Überblick über existierende PKIs geliefert und auf einige Aspekte der technischen und rechtlichen Interoperabilität und Anwendungen dieser Infrastrukturen eingegangen.

1 Einleitung

Der Einsatz von Public-Key Mechanismen zur sicheren Implementierung elektronischer Geschäftsprozesse in Wirtschaft und Verwaltung erfreut sich zunehmender Beliebtheit. Dies dürfte unter anderem daran liegen, dass sich neben der Authentisierung, Datenintegrität und Vertraulichkeit, die für organisationsinterne Applikationen oftmals ausreichend sind, auch das Sicherheitsziel der (rechtlichen) Verbindlichkeit elegant realisieren läßt. Von zentraler Bedeutung ist hier die Verbindung zwischen der Identität einer Entität und ihren öffentlichen Schlüsseln. Diese Verbindung wird typischerweise durch das Ausstellen von X.509-Zertifikaten **[X.509]** durch eine vertrauenswürdige Stelle erreicht. Die Gesamtheit der zur Verwaltung dieser Zertifikate benötigten Systeme und Prozesse wird Public-Key Infrastruktur (PKI) genannt. So umfaßt dieser Begriff (zumindest) die Benutzerregistrierung, Zertifikatsbeantragung und -sperrung durch eine Registration Authority (RA), das Ausstellen von Zertifikaten (und ggf. vorher die Erzeugung von Schlüsseln) durch eine Certification Authority (CA), die Bereitstellung von Zertifikaten und Zertifikatsstatusinformationen in einem Directory (DIR) und natürlich entsprechende Anwendungskomponenten beim Benutzer (U). Neben diesen funktionalen Komponenten existieren - vor dem Hintergrund des geltenden öffentlichen Rechtes - organisatorische und politische Regularien für die Ausstellung und Benutzung der Zertifikate. So sind die wichtigsten Eigenschaften der Zertifikate in der Certificate Policy (CP) beschrieben. Zusammen mit dem Certification Practice Statement (CPS), das die Prozeduren bei der Ausstellung und der Verwaltung von Zertifikaten beschreibt, sind in diesen beiden Dokumenten beispielsweise auch grundsätzliche Rechte und Pflichten der beteiligten Par-

teien geregelt. Daneben existiert die Application Policy (AP)[1], die die organisatorischen und rechtlichen Rahmenbedingungen für die Nutzung der Zertifikate in bestimmten Anwendungen regelt und möglicherweise ein Subscriber Agreement (SA), das die Rechte und Pflichten der Zertifikats-Benutzer regelt. Das Zusammenspiel dieser einzelnen funktionalen und regulatorischen Komponenten ist in Abbildung 1 dargestellt.

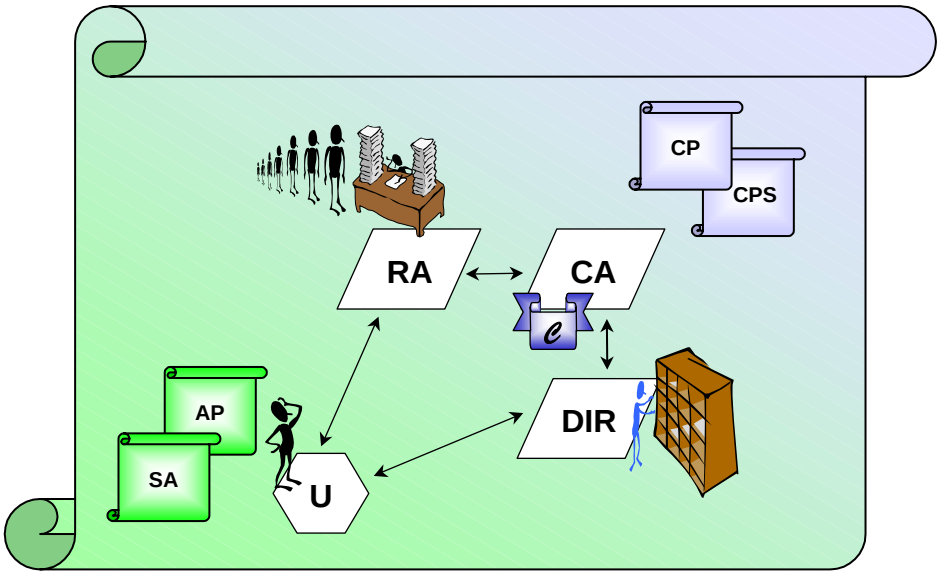

Abbildung 1: Funktionale und regulatorische Komponenten einer PKI

Nun gibt es aber nicht nur eine Klasse von zertifikats-basierten Anwendungen und eine globale PKI, die allen Anforderungen gerecht wird, sondern vielmehr eine Vielzahl von PKIs und übergeordneten PKI-Initiativen die historisch gewachsen und oft weitgehend unabhängig voneinander entstanden sind. So existieren sehr viele (noch) weitgehend unabhängige organisationsinterne PKIs und zunehmend organisationsübergreifende Initiativen, die auf ein geordnetes Zusammenspiel der einzelnen Infrastrukturen für E-Commerce- und E-Government-Anwendungen abzielen.

Dieser Beitrag liefert einen kompakten Überblick über verschiedene existierende PKI-Initiativen und beleuchtet das für eine breite Nutzung von E-Commerce und E-Government essentielle Problem der technischen und rechtlichen Interoperabilität zwischen diesen Infrastrukturen. Schließlich wird kurz zertifikatsbasierte Anwendungen eingegangen. Eine ausführlichere Darstellung existierender und sich für die Zukunft abzeichnenden Anwendungen findet sich in der vollständigen Version der Arbeit.

Dieser Beitrag ist folgendermaßen gegliedert: Abschnitt 2 liefert einen kompakten Überblick über existierende PKIs. Abschnitt 3 widmet sich dem Problem der rechtlichen und technischen Interoperabilität. In Abschnitt 4 wird auf zertifikatsbasierte Anwendungen eingegangen. In Abschnitt 5 wird schließlich der vorliegende Beitrag zusammengefasst und ein Ausblick auf zukünftige Entwicklungen gewagt.

[1] Eine mögliche Ausprägung der Application Policy ist die - in ETSI TS 101 733 (siehe **[ETSI01]**) bzw. in **[RFC3125]** definierte - Electronic Signature Policy, die festlegt unter welchen Umständen eine Signatur als gültig anerkannt wird.

2 Existierende Public-Key Infrastrukturen

Dieser Abschnitt liefert einen kurzen Überblick über einige existierende PKIs. Hierbei läßt sich grundsätzlich zwischen organisationsinternen PKIs (Abschnitt 2.1) und organisationsübergreifenden PKIs (Abschnitt 2.2) unterscheiden. Bei letzteren kann wiederum zwischen branchenspezifischen (Abschnitt 2.2.1) und branchenneutralen PKIs (Abschnitt 2.2.2) unterschieden werden.

2.1 Organisationsinterne PKIs

Für die Absicherung interner Prozesse und Systeme wird in vielen Unternehmen oder Verwaltungsorganisationen häufig selbst, bzw. in Zusammenarbeit mit Trustcenter-Dienstleistern, eine interne PKI aufgesetzt. Je nach konkreter Ausprägung kann diese interne PKI in eine konzernübergreifende Struktur eingebunden sein und/oder mehrere Vertrauensstufen berücksichtigen und ggf. auch - falls externe Parteien die so erzeugten Zertifikate als vertrauenswürdig behandeln - für die Abwicklung von Geschäften mit Kunden, Zulieferern und Partnern eingesetzt werden.

2.2 Organisationsübergreifende PKIs

Ein grundlegendes Problem der oben angedeuteten internen PKI ist, dass den von einer Organisation selbst ausgestellten Zertifikaten oft die externe Anerkennung fehlt. Deshalb müssen insbesondere auch organisationsübergreifende PKI-Architekturen berücksichtigt werden. Hierbei läßt sich wiederum zwischen branchenspezifischen PKIs und branchenneutralen PKIs unterscheiden.

2.2.1 Branchenspezifische PKIs

Im Folgenden werden einige branchenspezifische PKIs kurz vorgestellt. An diesen PKIs können branchenfremde Unternehmen oder Verwaltungseinheiten nicht als CA, sondern - unter bestimmten Voraussetzungen - bestenfalls als Endeinheit, teilnehmen.

2.2.1.1 Identrus

Identrus wurde im April 1999 von den Banken ABN AMRO, Bank of America, Bankers Trust (inzwischen von der Deutschen Bank erworben), Barclays, Chase Manhattan, Citigroup, Deutsche Bank und Hypo Vereinsbank mit dem Ziel gegründet, eine weltweite Vertrauensinfrastruktur für B2B E-Commerce zu schaffen. Als CA im Identrus-System können nur Finanzinstitute, als End-Einheit nur Geschäftskunden dieser Finanzinstitute, auftreten. Mittlerweile nehmen mehr als 50 internationale Großbanken an der Identrus-Initiative teil. Die Spezifikationen bauen auf weit verbreiteten Standards, wie **[X.509]**, **[RFC2459]**, **[RFC2311]**, **[RFC2312]** oder **[RFC2560]**, auf. Die technischen und organisatorischen Mindestanforderungen für die Teilnahme am Identrus-System sind mit den WebTrust-Kriterien (siehe Abschnitt 2.2.2.4) vergleichbar. Die rechtlichen Rahmenbedingungen sind durch ein ausgefeiltes privatrechtliches Vertragswerk definiert. Für weitere Informationen zu Identrus verweisen wir auf **[Hühn01]**.

2.2.1.2 PKI der deutschen Bundesverwaltung

Am 20.02.2001 wurde die Public-Key Infrastruktur der öffentlichen Verwaltung zur Unterstützung sicherer E-Mail durch das Bundesamt für Sicherheit in der Informationstechnik in Betrieb genommen. Eine zentrale Rolle nimmt die bereits weit verbreitete elektronische Kommunikation via E-Mail ein. Zur Absicherung dieser Kommunikation und zur Schaffung von Interoperabilität zwischen unterschiedlichen Produkten wurde das Projekt SPHINX **[BSI00]** ins Leben gerufen. Das Projekt benutzt den MailTrusT-Standard v2, der auf S/MIME (**[RFC2312]**, **[RFC2311]**), X.509v3 **[X.509]** und PKIX **[RFC2459]** aufbaut.

2.2.1.3 PKI der deutschen Sozialversicherungsträger

Die deutschen Sozialversicherungsträger betreiben eine PKI, die zur Absicherung des elektronischen Datenaustausches zwischen Trägern und Leistungserbringern in der Sozialversicherung verwendet wird.

Hier existiert eine Policy-CA (PCA) unter der weitere operative CAs existieren:

- ITSG-CA (Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH)
- DKTIG-CA (Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH)
- BfA-CA (Bundesanstalt für Arbeit)
- VDR-CA (Verband Deutscher Rentenversicherungsträger)

Alle hier aufgeführten CAs stellen X.509v1-Zertifikate aus. Als Sicherheitsmechanismus, z.B. für den Datenaustausch zwischen den Krankenkassen und Leistungserbringern **[AOK01]**, kommt das mittlerweile etwas betagte PEM **[RFC1421]** zum Einsatz.

2.2.2 Branchenneutrale PKIs

Während die oben vorgestellten PKIs nur für bestimmte Organisationen zugänglich sind, so existieren branchenneutrale PKIs, bei denen eine solche Einschränkung nicht existiert.

2.2.2.1 Herstellergetriebene PKIs

Von PKI-Systemherstellern, wie z.B. Verisign, RSA und Entrust, wird die (unter Umständen kostenintensive) Möglichkeit geboten, die unternehmensinterne PKI in "globale", herstellergetriebene Vertrauensinfrastrukturen einzubinden. Zum Teil haben sich diese Anbieter der WebTrust-Akkreditierung (siehe Abschnitt 2.2.2.4) unterzogen.

In ähnlicher Weise bieten viele TrustCenter Dienstleister beim Betrieb virtueller Zertifizierungsstellen an, dass für die Kunden-PKI vom Betreiber ein Zertifikat ausgestellt wird. Somit wird die Kunden-PKI in die "Trust-Community" des Anbieters eingebunden.

Während der Akzeptanzbereich der eigenen Zertifikate offensichtlich vergrößert wird, so sind die verschiedenen herstellergetriebenen Infrastrukturen jedoch voneinander unabhängig und - jede einzelne Initiative - weit von einer möglichen Flächendeckung entfernt.

2.2.2.2 Bridge-CA Initiative

Bei der Bridge-CA handelt es sich um eine gemeinnützige Initiative führender deutscher Industrieunternehmen und -verbände mit dem Ziel, eine globale technisch/organisatorische Vertrauensinfrastruktur, z.B. für die sichere E-Mail-Kommunikation, zu schaffen. Die Bridge-CA, deren Management-Komitee aus Deutsche Bank AG, Deutsche Telekom AG, Daimler-Chrysler AG, SKO (Sparkassenorganisation), TeleTrusT e.V. und BSI besteht, überbrückt die Lücken in den Vertrauensbeziehungen zwischen isolierten PKIs, indem zur Zeit die Root-Zertifikate der teilnehmenden Organisationen sicher verteilt werden und zukünftig eine sternförmig cross-zertifizierte Infrastruktur - mit der Bridge-CA als zentraler Instanz - aufgesetzt wird. Als E-Mail-Sicherheitsmechanismus kommt S/MIME v2 (**[RFC2312]**, **[RFC2311]**) zum Einsatz, so dass die Interoperabiltität mit Komponenten gemäß der ISIS/MTT-Spezifikation **[Tele01]** gewährleistet ist. Für weitere Informationen zur Bridge-CA sei auf **[EsHü01]** verwiesen.

2.2.2.3 Signaturgesetzkonforme PKIs

Während die rechtlichen Rahmenbedingungen und Implikationen der Zertifikatsnutzung bei den oben aufgeführten PKIs durch privatrechtliche Vereinbarungen getroffen werden müssen, ist dies bei einer signaturgesetzkonformen PKI durch öffentliches Recht geregelt. Im Folgenden werden einige Aspekte signaturgesetzkonformer PKIs in Deutschland (Abschnitt 2.2.2.3.1), Europa (Abschnitt 2.2.2.3.2) und schließlich außerhalb Europas (Abschnitt 2.2.2.3.3) beleuchtet.

2.2.2.3.1 Signaturgesetzkonforme PKIs in Deutschland

Neben dem deutschen Signaturgesetz **[SigG]**, das die EU-Richtlinie **[EGSRL]** umsetzt, und der Signaturverordnung **[SigV]**, die entsprechende Details regelt, wurden auch weitere Gesetze, wie das Gesetz zur Anpassung der Formvorschriften im Privatrecht an den modernen Rechtsverkehr **[FormVG]**, erlassen, das u.a. die Gleichstellung der gesetzeskonformen (qualifizierten) Signatur mit der eigenhändigen Unterschrift unter den dort genannten Voraussetzungen regelt.

So können, durch die Anpassung von § 126 BGB (Bürgerliches Gesetzbuch) (und Einführung von § 126a BGB) bei Einsatz qualifizierter Signaturen, nun auch Geschäftsprozessen mit gesetzlicher Schriftformerfordernis - sofern die elektronische Form nicht explizit ausgeschlossen[2] wird - elektronisch abgewickelt werden. Außerdem existieren bereits einige Gesetze und Verordnungen, die den Einsatz von qualifizierten Signaturen - oft verbunden mit einer Anbieterakkreditierung gemäß §15 SigG - explizit fordern:

- Elektronische Rechnungsstellung (siehe §14 UStG, **[StÄndG]**)
- Vergabe öffentlicher Aufträge (siehe §15 **[VgV]**)
- Rechnungslegung in der Sozialversicherung (siehe **[SVRV]** und **[SRVwV]**) und

[2] Geschäftsprozesse, die nach wie vor eine handschriftliche Unterschrift benötigen sind beispielsweise die Bürgschaftserklärung (§766 BGB), das Schuldversprechen (§780 BGB) oder der Abschluß von Kreditverträgen mit Privatpersonen (§4 Verbraucherkreditgesetz).

- weitere Verwaltungsverfahrensrechtliche Vorschriften **[VwVfÄndG]**.

Während bei diesen Geschäftsprozessen der Einsatz SigG-konformer Zertifikate zwingend nötig ist, spricht insbesondere die erhöhte Beweiskraft (siehe § 292a ZPO (Zivilprozessordnung)) bei beliebigen Transaktionen für den Einsatz signaturgesetzkonformer Zertifikate.

Derzeit, d.h. im Januar 2002, existieren folgende signaturgesetzkonforme CAs, die alle unter der von der Regulierungsbehörde für Telekommunikation und Post (RegTP) **[RegTP]** betriebenen deutschen Wurzelinstanz angeordnet sind:

- Produktzentrum TeleSec der Deutschen Telekom AG, Netphen
- Bundesnotarkammer, Köln, als von Signtrust betriebene Virtuelle CA (VCA)
- Deutsche Post Signtrust GmbH, Bonn
- DATEV eG, Nürnberg
- Steuerberaterkammer Nürnberg, als von DATEV betriebene VCA
- Medizon AG, Berlin, als von Signtrust betriebene VCA
- Steuerberaterkammer Saarland, als von DATEV betriebene VCA
- Hanseatische Steuerberaterkammer Bremen, als von DATEV betriebene VCA
- Rechtsanwaltskammer Bamberg, als von DATEV betriebene VCA
- Rechtsanwaltskammer Koblenz, als von DATEV betriebene VCA
- Steuerberaterkammer Stuttgart, als von DATEV betriebene VCA
- Steuerberaterkammer München, als von DATEV betriebene VCA
- Steuerberaterkammer Berlin, als von DATEV betriebene VCA
- AuthentiDate International AG, Ratingen, als von Signtrust betriebene VCA
- TC TrustCenter AG, Hamburg

Außerdem hat die D-Trust GmbH, Berlin, den Betrieb einer Zertifizierungsstelle gemäß SigG angezeigt; mit der freiwilligen Akkreditierung ist in näherer Zukunft zu rechnen.

Die technische Interoperabilität, z.B. bei der sicheren E-Mail-Kommunikation, zwischen den einzelnen CAs ist derzeit noch nicht vollständig gegeben. Bis Mitte 2002 ist jedoch durch die Implementierung der gemeinsam verabschiedeten ISIS/MTT-Spezifikation **[Tele01]** mit Abhilfe zu rechnen.

2.2.2.3.2 Signaturgesetzkonforme PKIs in Europa

Entscheidende Grundlage für signaturgesetzkonforme PKIs in Europa ist die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen **[EGSRL]**. Diese Richtlinie regelt grundsätzliche Aspekte der elektronischen Signatur in den EG-Mitgliedsstaaten, um einen reibungslose EG-Binnenmarkt zu gewährleisten. So enthält die Richtlinie u.a. Regularien zur

- Definition verschiedener Qualitätsstufen
  - "elektronische Signatur" (Art. 2 Nr. 1)

  - "fortgeschrittene elektronische Signatur" (Art. 2 Nr. 2)
  - "fortgeschrittene elektronische Signatur mit qualifiziertem Zertifikat und sicherer Signaturerstellungseinheit" (Art. 2 Nr. 2 und Art. 5 Abs. 1 zusammen mit Anhängen I-III) - kurz: "qualifizierte Signatur"
- Rechtlichen Gleichstellung der qualifizierten Signatur mit der handschriftlichen Unterschrift (Art. 5 Abs. 1)
- Freiwilligen Akkreditierung (Art. 3 Abs. 2)
- Option für zusätzliche Anforderung für Signaturen im öffentlichen Bereich (Art. 3 Abs. 7)

Diese Richtlinie sollte bis zum 19. Juli 2001 durch die Mitgliedsstaaten umgesetzt werden. Allerdings ist die Umsetzung der Richtlinie derzeit noch nicht vollständig abgeschlossen. Beispielsweise muß die Novellierung existierender Signaturgesetze in Italien und Portugal noch durchgeführt, und in den Niederlanden und dem Vereinigten Königreich[3] überhaupt erst ein Signaturgesetz verabschiedet, werden. Außerdem fehlen in den meisten europäischen Staaten detaillierte technische und organisatorische Umsetzungsregelungen. Hier darf erwartet werden, dass sich die noch zu schaffenden Regularien in den EU-Mitgliedsstaaten zum großen Teil auf Arbeitsergebnisse von CEN **[CEN01]**, ETSI **[ETSI01]** und EESSI **[EESSI01]** stützen werden.

2.2.2.3.3 Signaturgesetzkonforme PKIs außerhalb Europas

Auch außerhalb Europas existieren in verschiedenen Staaten bereits Signaturgesetze bzw. erste Aktivitäten mit dem Ziel ein solches zu verabschieden. Erwähnenswert scheinen hier die Aktivitäten der UNCITRAL-Kommision der Vereinten Nationen, die mit **[UNCI01]** ein Muster-Signaturgesetz bereitgestellt hat. Dieses Mustergesetz dient als Basis verschiedener Signaturgesetze - beispielsweise in den USA, Australien und Neuseeland. Bemerkenswert erscheint hier der Australische Ansatz, bei dem das nationale Signaturgesetz im Zuge der Gatekeeper-Initiative **[NOIE01]** auf internationaler Ebene mit dem Identrus-System **[Iden01]** zusammengeführt wurde.

Für einen umfassenden Überblick zur Signaturgesetzgebung in verschiedenen Ländern sei auf **[vdHof01]** verwiesen.

2.2.2.4 WebTrust for Certification Authorities

Schließlich scheint die WebTrust for Certification Authorities - Initiative **[AICPA]** des American Institute of Certified Public Accountants und Canadian Institute of Chartered Accountants (AICPA/CICA) erwähnenswert. Hier wurden auf Basis des ANSI Standards **[X9.79]** Kriterien für den vertrauenswürdigen Betrieb von CAs entwickelt, die von Wirtschaftsprüfern im Rahmen eines SAS70-Audits überprüft werden.

---

[3] In UK existiert ein Electronic Communication Bill, das Teilaspekte einer Signaturgesetzgebung gemäß **[EGSRL]** berücksichtigt. Deshalb wird derzeit noch diskutiert, ob die existierenden Regularien ausreichen, oder ein eigenständiges Signaturgesetz verabschiedet werden muss.

3 Das Problem der Interoperabilität

Wie in Abschnitt 2 angedeutet, existiert eine Vielzahl von PKIs für unterschiedliche Anwendungen in diversen Branchen in verschiedenen Ländern. Da eine Verwaltungsorganisation oder ein Unternehmen meist mehrere Anwendungen, teilweise mit unterschiedlichen, z.B. von verschiedenen CAs ausgestellten, Zertifikaten handhaben muss, führt diese Situation zwangsläufig zu Fragestellungen der Interoperabilität, die wir hier[4] folgendermaßen definieren wollen:

Interoperabilität ist die Fähigkeit zweier (oder mehrerer) Systeme, verschiedener Hersteller und Betreiber, problemlos zusammenarbeiten zu können.

Interoperabilität im Umfeld von Public-Key Infrastrukturen umfaßt (zumindest) zwei Gesichtspunkte:

- Technische Interoperabilität

  Auf der einen Seite umfaßt dieses Problem technische Aspekte der reibungslosen Zusammenarbeit zwischen PKI-Komponenten verschiedener Hersteller und Betreiber.

- Rechtliche Interoperabilität

  Auf der anderen Seite impliziert die Ausstellung und Benutzung verschiedenartiger Zertifikate oftmals unterschiedliche Rechtsfolgen für die beteiligten Parteien. Somit besteht das Problem der rechtlichen Interoperabilität in der Schaffung adäquater, für alle an der PKI beteiligten Parteien verbindlicher, rechtlicher Rahmenbedingungen für die Ausstellung und Benutzung von Zertifikaten.

Die Lösung existierender Interoperabilitätsprobleme ist insbesondere deshalb von fundamentaler Bedeutung, da durch diese der Einsatzbereich zertifikats-basierte Anwendungen stark eingeschränkt wird und sich so der tatsächliche Nutzen einer Public-Key *Infrastruktur* naturgemäß nur sehr schwer entfalten kann.

In diesem Abschnitt wird das Problem der - technischen und rechtlichen - Interoperabilität etwas näher betrachtet.

3.1 Technische Interoperabilität

Wie oben erläutert, bedeutet technische Interoperabilität bei Public-Key Infrastrukturen, dass PKI-Komponenten verschiedener Anbieter und Betreiber reibungslos zusammenarbeiten können. Hierzu ist die "Unterstützung allgemein anerkannter" Standards für Datenformate, z.B. für Zertifikate, und Protokolle notwendig aber, wie die Praxis zeigt, oft nicht hinreichend.

3.1.1 Standards sind notwendig ...

Die nachfolgende Auflistung der gebräuchlichsten Standards umfaßt die in Abbildung 1 dargestellten (funktionalen) Kernkomponenten einer PKI:

---

[4] In **[IEEE90]** findet sich beispielsweise folgende Definition: "Interoperability is the ability of two or more systems or components to exchange information and to use the information that has been exchanged."

- **CA**

  Das praktisch überall verwandte Format für Zertifikate (und Sperrlisten) ist **[X.509]**. Da in diesem Standard sehr viele Freiheiten, z.B. bzgl. der Präsenz und Kritikalität von Zertifikatserweiterungen, existieren, wird sehr oft auf das genauer spezifizierte Profil **[RFC2459]** aufgesetzt. Für qualifizierte Zertifikate existiert ein in **[RFC3039]** festgelegtes Profil, das wiederum auf RFC2459 aufbaut, und mit der Spezifikation von ETSI (TS 101 862, Qualified Signature Profile, siehe **[ETSI01]**) kompatibel ist.

  Diese Standards werden von sehr vielen Anbietern unterstützt. Außerdem darf durch die Umsetzung der ISIS/MTT-Spezifikation **[Tele01]**, die den Interpretationsspielraum in den oben genannten Standards stark minimiert, bald mit umfassender Interoperabilität in diesem Bereich gerechnet werden.

- **RA**

  Zu den Aufgaben der RA gehört neben der Identifikation des Benutzers, für die keine (technischen) Standards existieren, insbesondere Aufgaben bezüglich des Managements von Zertifikaten. Die Basis-Formate für die Beantragung von Zertifikaten sind in **[PKCS#10]** und **[PKCS#7]** spezifiziert. Ausgefeiltere Formate und Protokolle, die einer erweiterten RA-Funktionalität Rechnung tragen, finden sich in **[RFC 2511]**, **[RFC 2510]** und **[RFC 2797]**.

- **DIR**

  Für den Directory-Zugriff hat sich neben dem in **[X.500]** spezifizierten Directory Access Protocol (DAP) insbesondere das leichtgewichtige LDAP (siehe **[RFC2251]** und **[RFC2559]**) als sehr weit verbreiteter Standard herauskristallisiert. Der Standard für die Online Zertifikatsstatusabfrage ist das Online Certificate Status Protocol (OCSP) **[RFC2560]**, das - insbesondere im Zusammenhang mit werthaltigen Transaktionen - zunehmend eingesetzt wird.

- **User**

  Bei den Benutzerkomponenten hat sich insbesondere das **[PKCS#12]**-Format für das software-basierte Personal Security Environment (PSE) und die **[PKCS#11]**-Schnittstelle für Hardware-Tokens durchgesetzt.

  Neben diesen Standards (und teilweise den oben genannten Infrastrukturstandards) müssen die Benutzerkomponenten natürlich auch entsprechende Anwendungsstandards unterstützen. Eine umfassende Behandlung dieser Anwendungsstandards würde den Umfang des vorliegenden Beitrages sprengen. Deshalb sollen hier nur die gebräuchlichsten Anwendungen aufgegriffen werden:

  - SSL/TLS

    So wird zur Absicherung von HTTP-Verbindungen in Web-Browsern praktisch immer SSL/TLS (**[RFC2246]** und **[RFC 2818]**) eingesetzt. Durch die wachsende Verfügbarkeit von X.509v3-Zertifikaten, entwickelt sich SSL - meist durch (nicht in TLS **[RFC2246]** spezifizierte) Mechanismen zur Zertifikatsstatusabfrage ergänzt - zunehmend zum Standardmechanismus für die browserbasierte Authentifikation. Weitere Informationen finden sich unter **[TLS]**.

  - E-Mail

Für E-Mail-Sicherheit existieren bereits viele interoperable Produkte, die S/MIME v2 (**[RFC2312]** und **[RFC2311]**) und S/MIME v3 (**[RFC 2630]**, **[RFC2632]** und **[RFC2633]**) unterstützen. Weitere Infos finden sich unter **[S/MIME]**.

- VPN

  Zur Implementierung von VPNs wird zunehmend IPSEC eingesetzt. Die zugehörigen Standards und aktuellen Aktivitäten finden sich unter **[IPSEC]**.

- XML-Sicherheit

  Die relevanten Standards im Umfeld der XML-Sicherheit finden sich unter **[W3C-XE]** und **[W3C-XS]**. Allgemeine Informationen zu diesem - insbesondere im Hinblick auf E-Commerce und E-Government - sehr wichtigen Gebiet finden sich unter **[Geue01]**.

3.1.2 ... aber oft nicht ausreichend

Während Standards, wie z.B. die oben skizzierten, für die Interoperabilität sicherlich notwendig sind, zeigt die Praxis, dass diese oft nicht ausreichend sind.

Dies liegt beispielsweise an folgenden Umständen:

- Standards sind oft interpretationsfähig

  In vielen Bereichen sind Standards (bewußt) eher allgemein gehalten und enthalten viele Optionen von denen bei vielen Produkten nur einige unterstützt werden. Deshalb sind bei mächtigen Standards oft mehrere Profilierungsschritte bis hin zu einer "bitgenauen" Spezifikation nötig.

  Die wirklich breit unterstützte Spezifikation der X.509 Zertifikate **[X.509]** liefert ein anschauliches Beispiel. So läßt selbst die Präzisierung in **[RFC2459]** noch Spielraum für Interpretationen, so dass auf dem Weg zur Interoperabilität weitere Festlegung, wie in **[Tele01]**, nötig sind.

  Außerdem sind Standards, wie auch Produkte, keine statischen Objekte, sondern werden im Laufe der Zeit verändert und ergänzt. Viele Hersteller müssen sich, insbesondere auf Grund kurzer Innovationszyklen, mit der Unterstützung "gebräuchlicher Untermengen" eines Standards begnügen.

  So ist es heute beispielsweise kaum möglich X.509v1-Zertifikate, die keinerlei Zertifikatserweiterungen besitzen, für die SSL-Client-Authentifizierung zu verwenden, da moderne Browser, wie Netscape Navigator 4.7 oder der Microsoft Internet Explorer 5, X.509v1-Zertifikate, aufgrund der fehlenden extended key usage "authentication" nicht als "SSL-tauglich" behandeln.

  Ein anderes Beispiel ist die "Unterstützung von S/MIME" **[RFC2311]** - z.B. bei Lotus Notes 4.x (mit Mailprotect) und dem Netscape Messenger 4.7. Bekanntlich sieht dieser Standard die *Optionen* "single-signed-opaque" und "multipart-signed-cleartext" für signierte Mails vor. So unterstützt Lotus Notes nur die Variante "single-signed-opaque" und Netscape nur die Variante "multipart-signed-cleartext", so dass hier aufwendige Workarounds - oder das Ausweichen auf zusätzliche Verschlüsselung - nötig werden. Weitere Informationen finden sich in **[EsHü01]** und **[BaJH01]**.

- Oft fehlen Referenzimplementierungen und Testspezifikationen

  Wie oben erläutert, bringt die "Unterstützung bestimmter Standards" oft noch keine Garantie für die Interoperabilität der Systeme, so dass diese erst in konkreten Interoperabilitätstests nachgewiesen werden muss. Hierfür fehlen aber meist herstellerunabhängige Referenzimplementierungen und entsprechende allgemein anerkannte Testspezifikationen.

3.1.3 Initiativen zur Förderung der Interoperabilität

Wie in den beiden obigen Abschnitten erläutert, sind auf dem Weg zur technischen Interoperabilität unmißverständliche Profilierungen allgemein unterstützter Standards und ein entsprechendes Testumfeld, mit Referenzimplementierung und Testspezifikation, zu schaffen. Dies ist genau das Ziel der ISIS/MTT-Aktivitäten **[Tele01]**. Hier ist die Spezifikation, die Mehrdeutigkeiten eliminieren soll, bereits verabschiedet. Die Bereitstellung des ISIS/MTT-Testbeds soll bis Mitte 2002 erfolgen.

Außerdem existieren beispielsweise die folgenden weiteren Initiativen:

- Bridge-CA Initiative

  Bei der Bridge-CA Initiative (siehe **[EsHü01]**) ist ein - sehr pragmatischer - Interoperabilitätstest Voraussetzung für die Teilnahme.

- PKI-Challenge der EEMA

  Unter **[EEMA01]** finden sich weitere Informationen zur EEMA-PKI-Challenge, die im Rahmen eines zweijährigen, durch die EU und die Schweizer Regierung geförderten, Projektes Interoperabilitätsprobleme bei PKI-Produkten verschiedener Hersteller aufdecken und beseitigen soll.

- Interoperabiliätstests in US-amerikanischen Behörden

  Im Rahmen der US-amerikanischen Federal Bridge-CA Initiative wurde vom NIST ein PKI Testbed **[NIST01]** bereitgestellt. Außerdem existiert im Department of Defense ein Joint Interoperability Test Command (JITC), das die Interoperabilität der von der DoD-CA ausgestellten Zertifikate mit entsprechenden Applikationskomponenten testet. Weitere Informationen finden sich unter **[DoD01]**.

- Interoperabilitätstests der britischen Behörden

  Im Rahmen des Aufbaus der Root CA der britischen Behörden, wurden auch von der Communications-Electronics Security Group PKI-Interoperabiliätstests durchgeführt; die Ergebnisse dieser Tests finden sich in **[CESG01]**.

3.2 Rechtliche Interoperabilität

Unter Interoperabilität verstehen wir nach obiger Definition die Fähigkeit, dass mehrere Systeme problemlos zusammenarbeiten können. Rechtliche Interoperabilität bedeutet hier also, dass die verschiedenen - möglicherweise von unterschiedlichen Stellen betriebenen - Komponenten einer PKI, oder auch mehrere PKIs, in einer Art und Weise zusammenarbeiten können, dass die Rechte und Pflichten der Beteiligten sowie die rechtlichen Konsequenzen der Zertifikatsausstellung und Benutzung klar geregelt sind und einen verbindlichen Charakter haben.

Um ein solches Umfeld, in dem die rechtlichen Rahmenbedingungen einer PKI klar geregelt sind, zu schaffen, existieren grundsätzlich verschiedene Ansätze. So kann die PKI bestehende rechtliche Rahmenwerke des öffentlichen oder privaten Rechts als Basis benutzen oder eigene Rahmenbedingungen auf privatrechtlicher Basis schaffen.

Demnach kann folgende Unterscheidung getroffen werden:

- **Regulierung durch existierendes öffentliches Recht**

  In diese Kategorie fallen insbesondere die in Abschnitt 2.2.2.3 behandelten signaturgesetzkonformen PKIs. Hier sind die Rechte und Pflichten der an der PKI beteiligten Stellen durch öffentliches Recht, d.h. durch nationale Gesetze und Verordnungen, wie z.B. **[SigG]** und **[SigV]**, geregelt. Während hier also kein Aufwand für die Schaffung eigener rechtlicher Rahmenbedingungen entsteht, müssen die damit verbundenen technischen und organisatorischen Anforderungen berücksichtigt werden.

- **Regulierung durch existierende privatrechtliche Vertragswerke**

  In diesem Fall kann sich die PKI existierenden PKI-Initiativen, die privatrechtlich reguliert sind, anschließen. Hier existieren also vorgefertigte Vertragswerke, die die Rechte und Pflichten der an der PKI teilnehmenden Parteien durch bilaterale Verträge regeln. So kann man, sofern man die jeweiligen Anforderungen der betreffenden Initiative erfüllt, durch Unterzeichnung entsprechender Verträge an der Initiative teilnehmen.

  Beispielsweise fällt die Teilnahme am Identrus-System (siehe Abschnitt 2.2.1.1) oder an der Bridge-CA Initiative (siehe Abschnitt 2.2.2.2) in diese Kategorie. Diese Beispiele zeigen eindrucksvoll, dass die privatrechtlich definierten Rechte und Pflichten und insbesondere die für die Teilnahme nötigen Anforderungen, und der damit verbundene technische und organisatorische Aufwand zur Teilnahme, unter Umständen sehr verschieden sein können.

  Die Entscheidung, ob existierende PKIs vergleichbare Vertrauensniveaus besitzen, ist in der Praxis alles andere als trivial und derzeit (noch?) nicht automatisiert möglich. In diesem Zusammenhang darf man auf die endgültigen Ergebnisse des Forschungsprojektes "Fiducia" **[TsBD01]** gespannt sein. Dort wurden mehr als 100 Certificate Policies (CP) und Certification Practice Statements (CPS) analysiert und die relevanten Kriterien in einer CPS-Datenbank abgelegt, um schließlich eine (möglichst) automatisierte Entscheidung zu ermöglichen, ob ein entsprechendes Zertifikat in einer bestimmten Situation ausreichend vertrauenswürdig ist.

- **Schaffung eigener privatrechtlicher Rahmenbedingungen**

  Existiert kein, für die geplanten zertifikats-basierten Anwendungen, geeignetes Rahmenwerk, so können die benötigten rechtlichen Rahmenbedingungen selbst in Verträgen definiert werden. Meist werden die Rechte und Pflichten der CA in Form von CPs bzw. CPSs **[RFC2527]**, Rahmenbedingung für verschiedene Anwendungen in Application Policies (AP) und die Rechte und Pflichten der Benutzer in entsprechenden Subscriber Agreements (SA) geregelt. Während hier die Rechte, Pflichten und Anforderungen genau den Bedürfnissen der beteiligten Parteien angepasst werden können, und deshalb keine unangemessen hohen technischen und organisatorischen Aufwände zu erwarten sind, so entsteht ein unter Umständen recht hoher Aufwand für die Definition der (rechtlichen) Rahmenbedingungen. Dies ist insbesondere dann der Fall, wenn individuelle Regularien für

eine große Anzahl verschiedener Partner und Applikationen erstellt und gewartet werden müssen.

In diese Kategorie fällt übrigens auch der bewußte Verzicht auf jegliche Regulierung der PKI, z.B. bei ausschließlich organisations-interner Nutzung.

Welcher Ansatz in welcher Situation zu bevorzugen ist, läßt sich nicht pauschal beantworten. Hier ist insbesondere das geplante Anwendungsspektrum und die Struktur der Teilnehmer an der PKI zu berücksichtigen. Der zu erwartende - regulatorische und technische- organisatorische - Aufwand bei der Umsetzung der jeweiligen Variante verhält sich tendenziell wie in Abbildung 2 dargestellt. Demnach wird der erhöhte Umsetzungsaufwand bei stärker regulierten PKIs teilweise durch geringeren zusätzlich nötigen Regulierungsaufwand kompensiert. Da ausgefeiltere Regularien existieren, sind kaum Aufwände für die Gestaltung individueller Verträge nötig. So kann sich z.B. eine signaturgesetzkonforme PKI, die bei bloßer Betrachtung des technisch-organisatorischen Umsetzungsaufwandes relativ teuer ist, insgesamt - ungeachtet möglicherweise existierender Zwänge durch Schriftformerfordernisse etc. - als günstigste Variante herausstellen. Für die Entscheidung, welche Strategie gewählt werden sollte, ist dieser Aufwand genauer zu ermitteln und dem erwarteten Nutzen der PKI gegenüberzustellen.

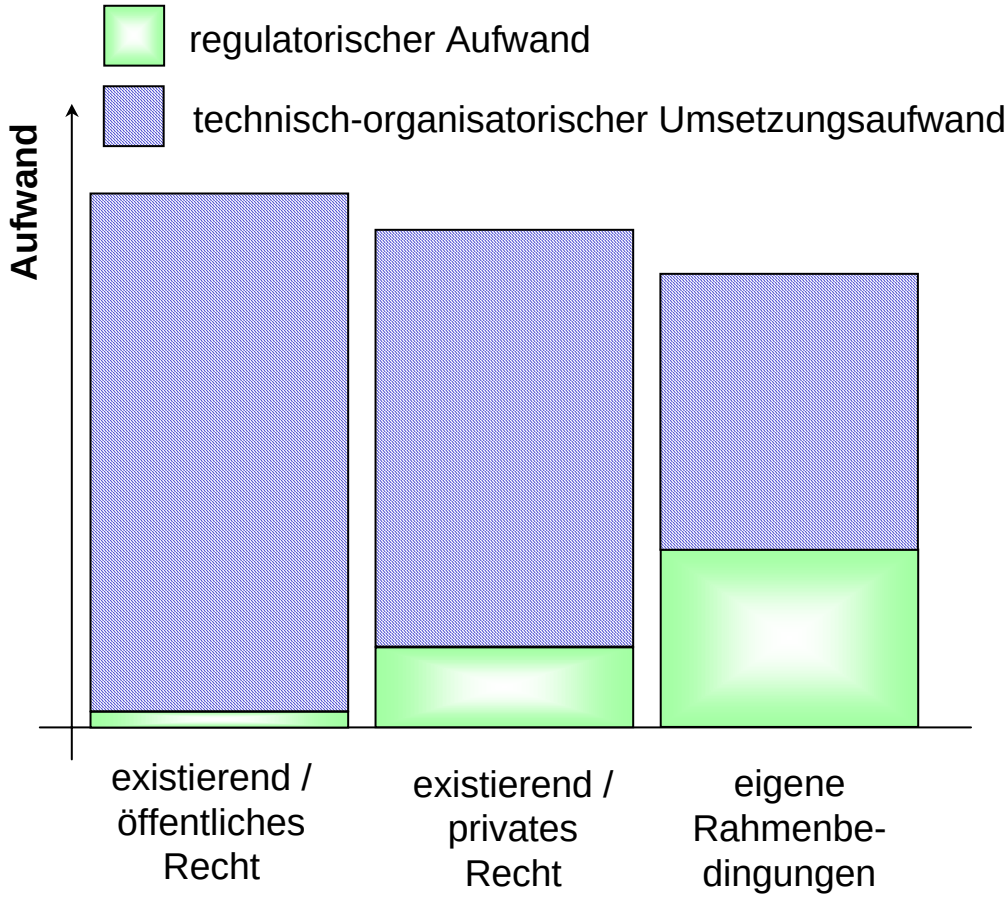

Abbildung 2: Aufwand für Regulation und Umsetzung

4 Zertifikats-basierte Anwendungen

In diesem Abschnitt gehen wir kurz auf typische zertifikats-basierte Anwendungen ein. Während wir uns in der vorliegenden Kurzfassung dieser Arbeit mit den generischen Basisapplikationen aus **[HüJa01]** begnügen, enthält die endgültige Fassung reale Beispiele, wie diese Basisanwendungen zur Absicherung existierender Geschäftsprozesse in Wirtschaft und Verwaltung eingesetzt werden.

- **E-Mail-Sicherheit**

  Durch Einsatz entsprechender Sicherheitsmechanismen für E-Mail steht eine sichere, nicht an spezielle Prozesse bzw. Anwendungen gebundene Kommunikationsplattform zum Austausch nicht-standardisierter Nachrichten zwischen einzelnen Mitarbeitern und externen Parteien zur Verfügung. Sichere E-Mails gehören derzeit zu den wichtigsten Einsatzgebieten von PKIs.

- **Datei-Verschlüsselung**

  Neben dem Schutz der Daten während der Übertragung, kann es auch wichtig sein besonders sensible Daten lediglich verschlüsselt zu speichern. Hier kann man zwischen lokaler Dateiverschlüsselung, die z.B. häufig bei mobilen Geräten eingesetzt wird, und transparenter Dateiverschlüsselung gesamter Netzwerklaufwerke unterscheiden.

- **Workflow-Signatures**

  Eine Erweiterung der o.g. E-Mail-Kommunikation sind sog. "Workflow-Signatures" mit denen auch komplexe, bisher papiergebundene (interne) Prozesse, bei denen zahlreiche Bearbeitungsschritte von unterschiedlichen Stellen vorgenommen werden, sicher elektronisch abgewickelt werden. Insbesondere kann hierdurch in sensiblen Prozessen leicht ein Mehraugenprinzip und Revisionssicherheit erreicht werden.

- **Virtual Private Networks**

  Statt der teuren Anbindung von Filialen und Zweigstellen über dedizierte Stand- oder Wählleitungen ermöglichen Virtual Private Networks (VPNs) den Zugang zum LAN der Zentrale über öffentliche Netze. Auch hier bietet eine PKI die benötigte Infrastruktur zur sicheren Authentifizierung der Gegenstelle und vertraulichen Übermittlung von Daten. Durch eine PKI lassen sich auch dynamische Extranets mit Kunden, Zulieferern und Partnern verwalten.

- **Sichere Client-Server Kommunikation**

  Während o.g. VPNs typischerweise für die Absicherung der gesamten Netzwerkverbindung einer externen Stelle und dem unternehmensinternen LAN genutzt werden, so werden oft, z.B. zum Schutz personenbezogener Daten im Personalwesen, auch Client-Server-Sicherheitsmechanismen innerhalb des LANs benötigt. So existiert beispielsweise eine zertifikatsbasierte R/3-Sicherheitslösung auf Basis der SNC-(GSS-API)-Schnittstelle von SAP. Ausserdem kann beim web-basierten Zugriff auf sensible Bereiche eines Intranets die Problematik der sicheren Benutzerauthentifizierung mit SSL-Client-Zertifikaten gelöst werden. Im Zuge der Vereinheitlichung von Inter- und Intranetanwendungen, z.B. im Bereich Content-Management, gewinnt der Einsatz von SSL, sowohl für den internen als auch externen Gebrauch, stark an Bedeutung. Langfristig wird in vielen Bereichen ein einheitliches (web-basiertes) Portal für Mitarbeiter und externe Parteien angestrebt.

- **Single Sign-On**

  Allgemeiner ist häufig - insbesondere bei heterogenen System- und Anwendungsstrukturen - eine einmalige Authentifizierung eines Benutzers angestrebt. Hier hilft eine PKI - in Verbindung mit entsprechenden Verzeichnis- und Rechteverwaltungsstrukturen - Zeit zu sparen. Dies gilt nicht nur für den Benutzer, sondern insbesondere auch für die Administratoren. Ausserdem lassen sich somit unternehmensweite Security Policies leichter durchsetzen.

- **Zusatzanwendungen bei Chipkarten-Einsatz**

  Verwendet man zum Speichern der privaten Schlüssel Hardware-Tokens (z. B. Smartcards), lassen sich damit weitere, z.B. Zutrittskontroll-, Bezahl- oder Zeiterfassungs-, Systeme einführen bzw. vereinheitlichen.

All diese Basisapplikationen befinden sich bereits zur Absicherung von Netzwerkinfrastrukturen oder Geschäftsprozessen im Einsatz. In der endgültigen Fassung des Papieres werden verschiedene reale Beispiele angegeben. Hier darf erwartet werden, dass mit der zunehmenden Lösung der oben skizzierten Interoperabilitätsprobleme zertifikats-basierte Applikationen ein noch stärkeres Wachstum erleben werden.

5 Zusammenfassung und Ausblick

In diesem Beitrag wurde ein kompakter Überblick über einige besonders interessant erscheinende Entwicklungen im Bereich PKI geliefert und insbesondere die Problematik der Interoperabilität näher beleuchtet. Wie oben erläutert, ist die (weitgehende) Lösung dieser Interoperabiliätsprobleme eine sehr wichtige Voraussetzung für die noch schnellere Verbreitung zertifikats-basierter Anwendungen.

Wie in Abschnitt 2 angedeutet, existieren bereits sehr viele - teilweise noch unabhängige - PKIs. Diese PKIs verwenden im Wesentlichen die in Abschnitt 3.1.1 aufgelisteten Standards, die von praktisch allen namhaften Herstellern unterstützt werden. Durch die vielschichtigen Initiativen zur Förderung der Interoperabilität, dürfte die technische Interoperabilitätsproblematik für Infrastrukturen und wichtige Basisanwendungen bald entschärft sein.

Etwas anders stellt sich die Situation bei der rechtlichen Interoperabilität verschiedener PKIs dar. Hier scheint - in der globalen Perspektive - der Prozeß der Konsolidierung hin zu kompatiblen Rahmenbedingungen, z.B. bezüglich der digitalen Signatur, noch weit von einem möglichen Abschluss entfernt. Während hier bereits, wie in Abschnitt 2.2.2.3 erläutert, einige Signaturgesetze existieren, die innerhalb Europas - durch die EU-Richtlinie **[EGSRL]** - auch grundsätzlich zueinander kompatibel sind, so sind die detaillierten Regelungen für die gegenseitige Anerkennung - und auch damit verbundene Fragen der technischen Umsetzung[5] - noch weitgehend ungeklärt. Bis dies geschieht, bleibt zur technischen und rechtlichen Absicherung von globalen E-Commerce-Transaktionen lediglich die privatrechtlich regulierte "Rückfall-Lösung", wie sie beispielsweise das Identrus-System bietet. Doch auch eine solche Lösung ist nicht in allen Fällen befriedigend, da in vielen Geschäftsprozessen per Gesetz Zertifikate mit

[5] So wäre beispielsweise eine cross-zertifizierte Struktur für signaturgesetzkonforme PKIs in Europa - oder gar global - denkbar.

bestimmten Eigenschaften eingesetzt werden müssen. So können beispielsweise die mit Identrus-Zertifikaten[6] signierten elektronischen Rechnungen, wegen §14 UStG[7], nicht von deutschen Finanzbehörden anerkannt werden. Dies ist insbesondere deshalb bedauerlich, weil - wie z.B. in **[Hühn01]** gezeigt - Electronic Bill Presentment & Payment (EBPP) sich auch in Deutschland bereits zu einer weit verbreiteten Anwendung für Identrus-Zertifikate entwickelt hat.

Hier bleibt derzeit nur die - mit etwas höherem Aufwand verbundene - Möglichkeit PKI-Systeme so zu entwickeln, dass die Anforderungen verschiedener regulativer Systeme, wie z.B. SigG und Identrus, gleichsam erfüllt werden, oder die Hoffnung, dass die existierenden Regularien weiter harmonisiert werden.

Reduziert man die PKI-Evolution auf die drei Phasen Entwicklung, Konsolidierung und Anwendung, so befinden wir uns derzeit schwerpunktmäßig in der Phase der Konsolidierung - verbunden mit ersten Anwendungen. Die nähere Betrachtung zeigt, dass die technische Konsolidierung auf globaler Basis bald weitgehend abgeschlossen sein wird und die rechtliche Konsolidierung bestenfalls auf nationaler Ebene ähnlich weit fortgeschritten ist.

Deshalb gilt es nun insbesondere die rechtlichen Probleme auf dem Weg einer globalen PKI-Interoperabilität anzugehen.

Literatur

[AICPA] AICPA: *WebTrust for Certification Authorities - homepage*, siehe http://www.aicpa.org/webtrust/caexec~1.htm

[AOK01] AOK Bundesverband: *Security Schnittstelle für das Gesundheitswesen für den Datenaustausch zwischen Leistungserbringern, Arbeitgebern und Krankenkassen*, Version 1.3 vom 23.07.2001, via http://www.itsg.de

[BaJH01] Bartels, M.; Jaletzke, A.; Hühnlein, D.: *Bridge-CA – Grundlegende S/MIME Interoperabilität*, 2001, verfügbar per mail an bernhard.esslinger@db.com oder detlef.huehnlein@secunet.com

[BrTe01] Bröhl G., Tettenborn A.: *Das neue Recht der elektronischen Signaturen: kommentierende Darstellung von Signaturgesetz und Signaturverordnung*, Bundesanzeiger-Verlag, ISBN 3-89817-045-4, 2001

[BSI00] BSI: *Sphinx - Pilotversuch zur sicheren E-Mail*, siehe http://www.bsi.de/aufgaben/projekte/sphinx/index.htm

[CEN01] CEN - European Committee for Standardization: *Electronic Signatures (E-SIGN) Workshop*, siehe http://www.cenorm.be/isss/workshop/e-sign/ ; Drafts via http://www.ni.din.de/sixcms/detail.php3?id=389

[CESG01] Communications-Electronics Security Group (CESG): *Secure Messaging And PKI Interoperability Demonstrator Final Report*,

[6] Die in der Identrus-Spezifikation formulierten Anforderungen sind nicht ohne weiteres mit den Anforderungen durch das SigG vereinbar. Deshalb ist ein Identrus-Zertifikat (derzeit) kein qualifiziertes Zertifikat.

[7] Hier werden qualifizierte Zertifikate mit Anbieterakkreditierung gemäß §15 SigG gefordert.

http://www.cesg.gov.uk/technology/pki/interop/media/PKIdemonstratorFinalReport.pdf

[DoD01] US-Department of Defense: *Joint Interoperability Test Command (JITC) - homepage*, siehe http://jitc.fhu.disa.mil/pki/testing.htm

[EEMA01] EEMA: *PKI challenge - Homepage*, siehe http://www.eema.org/pki-challenge/index.asp

[EESSI01] EESSI: *The European Electronic Signature Standardization Initiative - homepage*, via http://www.ict.etsi.org/eessi/EESSI-homepage.htm

[EGSRL] *Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen*, via http://europa.eu.int/comm/internal_market/en/media/sign/Dir99-93-ecDE.pdf

[EsHü01] Esslinger B., Hühnlein D.: *Global Secure E-Mail Interoperability - The Europe-based Bridge-CA*, in Horster P. (Hrsg.): Tagungsband Elektronische Geschäftsprozesse, IT-Verlag, 2001, ISBN 3-936052-00-X, SS. 22-31

[ETSI01] ETSI SEC: *Working group for Electronic Signatures and Infrastructures - homepage*, siehe http://portal.etsi.org/sec/el-sign.asp

[FormVG] *Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr*, BGBl. 2001, Teil 1, Nr. 35, (18.07.2001), via http://www.dud.de

[Geue01] Geuer-Pollmann C.: *XML Security Page- homepage*, siehe http://www.nue.et-inf.uni-siegen.de/~geuer-pollmann/xml_security.html

[vdHof01] van der Hof S.: *Digital Signature Law Survey - homepage*, via http://rechten.kub.nl/simone/ds-lawsu.htm

[Hühn01] Hühnlein D.: *Identrus-enabled applictions*, in Horster P. (Hrsg.):Tagungsband Elektronische Geschäftsprozesse, IT-Verlag, 2001, ISBN 3-936052-00-X, SS. 181-192

[HüJa01] Hühnlein D., Jaletzke A.: *Public-Key Infrastrukturen für Finanzdienstleister*, in Horster P. (Hrsg.): Tagungsband Elektronische Geschäftsprozesse, IT-Verlag, 2001, ISBN 3-936052-00-X, SS. 155-167

[Iden01] Identrus LLC: *Identrus - homepage*, siehe http://www.identrus.com

[IEEE90] Institute of Electrical and Electronics Engineers: *IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries*. New York, NY: 1990

[IPSEC] IETF: *IPSEC-charter - homepage*, siehe http://www.ietf.org/html.charters/ipsec-charter.html

[NIST01] National Institute for Standards and Technology - NIST: *NIST PKI Interoperability Testbed*, via http://csrc.nist.gov/pki/rootca/

[NOIE01] National Office for the Information Economy: *Government Public Key Infrastructure - homepage*, siehe

http://www.govonline.gov.au/projects/publickey/index.asp

[PKCS#7] RSA Labs: *PKCS #7 - Cryptographic Message Syntax Standard*, via http://www.rsalabs.com/pkcs/pkcs-7/index.html (siehe auch Kaliski B., RFC2315, via http://www.ietf.org)

[PKCS#10] RSA Labs: PKCS#10: Certification Request Syntax Standard, Version 1.5, via http://www.rsalabs.com/pkcs/pkcs-10/index.html (siehe auch Kaliski B., RFC2314, via http://www.ietf.org)

[PKCS#11] RSA Labs: PKCS#11: Cryptographic Token Interface Standard, Version 2.11, via http://www.rsasecurity.com/rsalabs/pkcs/pkcs-11/index.html

[PKCS#12] RSA Labs: PKCS #12: *Personal Information Exchange Syntax Standard*, Version 1.0, via http://www.rsalabs.com/pkcs/pkcs-12/index.html

[RegTP] RegTP - *Regulierungsbehörde für Telekommunikation und Post*: Homepage, siehe http://www.regtp.de

[RFC1421] RFC 1421: Linn, J.: Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures, via http://www.ietf.org

[RFC2246] RFC 2246: Dierks T., Allen C.: *The TLS Protocol*, Version 1.0,

[RFC2251] RFC 2251: Wahl, M.; Howes, T.; Kille, S.: *Lightweight Directory Access Protocol (v3)*, via http://www.ietf.org

[RFC2311] RFC2311: Dusse S., Hoffman P., Ramsdell L., Lundblade L., Repka L.: *S/MIME Version 2 Message Specification*, via http://www.ietf.org

[RFC2312] RFC2312: Dusse S., Hoffman P., Ramsdell L., Weinstein J.: *S/MIME Version 2 Certificate Handling*, via http://www.ietf.org

[RFC2459] RFC 2459: Housley R., Ford W., Polk W. und Solo D.: *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, via http://www.ietf.org

[RFC 2510] RFC 2510: Adams C., Farrell S.: Internet X.509 Public Key Infrastructure Certificate Management Protocols, via http://www.ietf.org

[RFC 2511] RFC 2511: Myers M., Adams C., Solo D., Kemp D.: *Internet X.509 Certificate-Request Message Format*, via http://www.ietf.org

[RFC2527] RFC 2527: Chokhani S., Ford W.: *Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework*, via http://www.ietf.org

[RFC2559] RFC 2559: Boeyen, S.; Howes, T.; Richard P.: *Internet X.509 Public Key Infrastructure Operational Protocols — LDAPv2*, via http://www.ietf.org

[RFC2560] RFC 2560: Myers M., Ankney R., Malpani A., Galperin S., Adams C.: *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol*, via http://www.ietf.org

[RFC 2630] RFC 2630: Housley R.: *Cryptographic Message Syntax*; via http://www.ietf.org

[RFC2632] RFC 2632: Ramsdell, B.: *S/MIME Version 3 Certificate Handling*, via http://www.ietf.org

[RFC2633] RFC 2633: Ramsdell, B.: *S/MIME Version 3 Message Specification*, via http://www.ietf.org

[RFC 2797] RFC 2797: Myers M., Liu X., Weinstein J.: *Certificate Management Messages over CMS*, via http://www.ietf.org

[RFC 2818] RFC 2818: Rescorla E.: *HTTP Over TLS*, via http://www.ietf.org

[RFC3039] RFC 3039: Santesson S., Polk W., Barzin P., Nystrom M.: *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*, via http://www.ietf.org

[RFC3125] RFC 3125: Ross J., Pinkas D., Pope N.: *Electronic Signature Policies*, via http://www.ietf.org

[SigG] *Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*, BGBl. 2001 Teil I Nr. 22, S. 876 ff. (21.05.2001), via http://www.dud.de

[SigV] *Verordnung zur elektronischen Signatur*, vom Bundestag am 24.10.2001 verabschiedet, via http://www.dud.de

[S/MIME] IETF: *S/MIME-charter - homepage*, siehe

http://www.ietf.org/html.charters/smime-charter.html

[SRVwV] *Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung*, (SRVwV) vom 15. Juli 1999, zuletzt geändert am 18. September 2000

[StÄndG] *Entwurf eines Gesetzes zur Änderung steuerlicher Vorschriften (Steueränderungsgesetz 2001 - StÄndG 2001)*, via http://www.bundesfinanzministerium.de/Anlage4935/Entwurf-Steueraenderungsgesetz-2001.pdf

[SVRV] *Verordnung über den Zahlungsverkehr, die Buchführung und die Rechnungslegung in der Sozialversicherung (Sozialversicherungs-Rechnungsverordnung – SVRV)*, Bgbl. Teil I, S. 1627 (15. Juli 1999), via http://www.bundesgesetzblatt.de/bgbl1f/b1findex.htm

[TsBD01] Tseng J., Backhouse J. und Dyer B.: *Fiducia - Modelling Risk in Interoperable PKI*, Präsentation am CSRC der London School of Economics, via http://www.dti-mi.org.uk/newweb/workshop2/FIDUCIAPres.pdf

[Tele01] TeleTrusT e.V.: *ISIS-MTT-Spezifikation*, Version 1.0.1, 2001, via http://www.darmstadt.gmd.de/mailtrust/

[TLS] IETF: *TLS-charter - homepage*, siehe http://www.ietf.org/html.charters/tls-charter.html

[UNCI01] United Nations Commission on International Trade Law (UNCITRAL): *UNCITRAL Model Law on Electronic Signatures (2001)*, Version der 38. Sitzung, Wien 18.-19. September, 2000, via http://www.uncitral.org/english/sessions/wg_ec/wp-88e.pdf

[VgV] *Verordnung über die Vergabe öffentlicher Aufträge* (Vergabeverordnung - VgV), Bgbl. 2001, Teil I, Nr. 3, 18.01.2001, via http://www.bundesgesetzblatt.de/bgbl1f/b1findex.htm

[VwVfÄndG] *Entwurf eines Dritten Gesetzes zur Änderung verwaltungsverfahrensrechtlicher Vorschriften (VwVfÄndG)*, Entwurf vom 16.07.2001, via http://www.dud.de

[W3C-XE] W3C/IETF: *XML-Encryption working group - homepage*, via http://www.w3.org/Encryption/2001/

[W3C-XS] W3C/IETF: *XML-Signature working group - homepage*, via http://www.w3.org/Signature/

[X9.79] ANSI X9F5: *PKI Practices and Policy Framework (X9.79)*, siehe http://www.x9.org/

[X.500] ITU-T Recommendation X.500: *The Directory—Overview of Concepts and Models*, International Telecommunication Union, Genf, Schweiz, 1997 (dies ist äquivalent zu ISO/IEC 9594-1)

[X.509] ITU-T Recommendation X.509: *Information Technology—Open Systems Interconnection—The Directory: Authentication Framework*, International Telecommunication Union, Genf, Schweiz, 1997 (dies ist äquivalent zu ISO/IEC 9594-8)