Für E-Commerce und andere Datenkommunikation

Mehr Unternehmenssicherheit durch Trustcenter?

Trustcenter[1] werden häufig als zentrale Komponente einer Sicherheitsinfrastruktur gesehen. Doch was kann ein solches Trustcenter für ein Unternehmen tatsächlich leisten? Wo sind seine Grenzen? Was sind die Voraussetzungen für den Einsatz eines Trustcenters und welche Kosten entstehen? Dieser Beitrag gibt konkrete Antworten auf diese Fragen.

Von Claus Stark, Karlsruhe

Zum Schutz digitaler Daten werden heute moderne Kryptoverfahren eingesetzt, die auf individuellen Schlüsseln für die Teilnehmer basieren. Eine leicht verständliche Darstellung dieser der „Public Key-Kryptographie" zugehörigen Verfahren findet sich zum Beispiel in [BEU97].

Eine solche Absicherung ist auch ohne Trustcenter möglich, etwa durch den bei Pretty Good Privacy (PGP) verfolgten „web-of-trust"-Ansatz, bei dem sich die Nutzer selbst gegenseitig Vertrauen aussprechen – oder auch durch die Nutzung von „pre-shared keys", beispielsweise in einem VPN. Solche Ansätze eignen sich, wenn die Architektur sehr einfach und die Anzahl der potenziellen Teilnehmer klein ist. Sollen aber sehr viele Mitarbeiter miteinander sicher elektronisch kommunizieren und sollen auch Geschäftspartner, Kunden und Behörden mittels sicherer Kommunikation erreicht werden, kann das Management der für die Sicherung benötigten Schlüssel sehr schnell komplex werden:

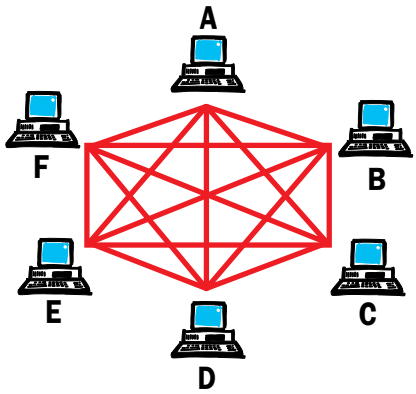

Abb1. Potenzielle Kommunikationsbeziehungen zwischen sechs Personen

Abbildung 1 zeigt, dass ohne Trustcenter bereits zwischen sechs Personen bis zu 15 individuelle Schlüsselvereinbarungen unter den Teilnehmern zur Absicherung ihrer IT-Kommunikation notwendig sein können. Dieser Aufwand steigt quadratisch mit der Zahl der Nutzer: Bei n Nutzern sind n*(n-1)/2 paarweise vereinbarte Schlüssel erforderlich. Bedenkt man, dass große Unternehmen leicht mehrere tausend Mitarbeiter haben, bei denen die Fluktuation oft auch hoch ist, wird klar, dass ohne geeignete Systematik das Schlüsselmanagement sehr schnell unhandlich werden kann. Zudem basieren diese individuellen Vereinbarungen oft auf keiner gemeinsamen „Policy", das heißt Vertrauensbildung wird hier oft sehr unterschiedlich gehandhabt: Nur selten wird ein fremdes Zertifikat adäquat anhand seines „Fingerprints" überprüft, oft wird es einfach ungeprüft akzeptiert.

Ein Trustcenter hingegen unterstützt die notwendige Vertrauensbildung zwischen den Nutzern zentral, indem es die für die sichere IT-Kommunikation benötigten Schlüssel „beglaubigt" und sie in Form von „Zertifikaten" den Nutzern zur Verfügung stellt. Die Zertifikate (also die „beglaubigten" Schlüssel) können nun ohne aufwändige individuelle Absprachen direkt genutzt werden. Die Policy zur Vertrauensbildung läßt sich so sehr wirksam zentral durchsetzen, zum Beispiel indem nur Zertifikate von als vertrauenswürdig akzeptierten Trustcentern von den Mitarbeitern genutzt werden dürfen.

Vertrauen die Nutzer dem Trustcenter, impliziert dies das Vertrauen in die von diesem ausgestellten Zertifikate. Um dieses Vertrauen zu rechtfertigen, muss ein Trustcenter folglich sehr vertrauenswürdig sein.

Trustcenter...

Über unseren Autor:

Claus Stark ist Diplom-Informatiker der Medizin, arbeitet seit fünf Jahren im Bereich IT-Sicherheit / PKI und ist seit über zwei Jahren Security-Consultant bei Secorvo Security Consulting GmbH in Karlsruhe. Publikationen von Mitarbeitern der Secorvo GmbH sind im Internet unter: www.secorvo.de/publikat/ hinterlegt. Kontakt zum Autor: stark@secorvo.de

1 Neben der Bezeichnung „Trustcenter" haben sich eine Reihe weiterer Begriffe für diese Art Einrichtung etabliert. Man spricht oft auch von „Zertifizierungsstelle" oder „CA" („certification authority"). Eine miteinander in direkter Beziehung stehende Anzahl von Trustcentern wird in der Regel als „PKI" („public key infrastructure") bezeichnet. In diesem Beitrag wird der Einfachheit halber nur der Begriff „Trustcenter" verwendet.

Abkürzungen

CA	Certification Authority
CPS	Certification Practice Statement
DIR	Directory
IPsec	Internet Protocol Security
IT	Informationstechnologie
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
RA	Registration Authority
RegTP	Regulierungsbehörde für Telekommunikation und Post, Mainz
S/MIME	Secure Multipurpose Internet Mail Extension
SSL	Secure Socket Layer Protocol

Viele Bereiche der IT-Kommunikation sind inzwischen „Trustcenter-fähig“, insbesondere sind die verbreiteten Anwendungsbereiche E-Mail („S/MIME“), Client-Server- („SSL“) und VPN-Kommunikation („Virtual Private Network“, „IPsec“) bereits sehr gut dafür gerüstet. Und andere Anwendungsbereiche wie Single-Sign-On sowie Workflow-, Dokumentenmanagement und Archivsysteme ziehen nach.

Was kann ein Trustcenter leisten?

Ein Trustcenter stellt einem Unternehmen Dienste rund um die Verwaltung von Schlüsseln bereit, die zur Absicherung des elektronischen Geschäftsverkehrs benötigt werden. Die Basisdienste eines Trustcenters umfassen in der Regel die eindeutige und sichere Identifikation von Personen, Servern und „Services“ sowie die Verwaltung von Schlüsseln und Zertifikaten (Ausstellung, Veröffentlichung, Überprüfung und gegebenenfalls auch Sperrung beim Ausscheiden von Mitarbeitern aus dem Unternehmen). Ein Trustcenter kann darüber hinaus auch sehr differenzierte Spezialdienste anbieten (zum Beispiel einen Zeitstempeldienst für Unternehmen, die einen „elektronischen Eingangsstempel“ für ihr digitales Archiv benötigen; s. WIK 01/3).

Ein Unternehmen kann dieses Schlüsselmanagement prinzipiell selbst durch ein eigenes, unternehmensinternes Trustcenter erbringen. Aufbau und Betrieb eines solchen Trustcenters können jedoch aufwändig und teuer werden – eine Investition, die sich für viele mittelständische Unternehmen nicht lohnt. Daher haben sich mittlerweile eine Reihe von kommerziellen Anbietern etabliert, die alle relevanten Trustcenter-Dienste als Dienstleister anbieten.

Ein Trustcenter besteht in der Regel aus verschiedenen Komponenten (Abb.2). Identifikation und Registrierung erfolgt in der „Registration Authority“ (RA), die eigentliche Zertifikatausstellung in der „Certification Authority“ (CA), die Veröffentlichung von Zertifikaten und gegebenenfalls Sperrlisten im „Verzeichnis“ (Directory, DIR).

Heutige Trustcenter-Dienstleister richten ihr Angebot teilweise an verschiedene Zielgruppen:

■ Soll die Kommunikationssicherung mit Digitaler Signatur gemäß Signaturgesetz erfolgen, muss der Trustcenter-Dienstleister eine entsprechende SigG-Akkreditierung durch die Regulierungsbehörde (RegTP) in Mainz besitzen.

■ Sollen unternehmenseigene Zertifikatsformate zum Einsatz kommen, sollte der Trustcenter-Dienstleister den individuellen Aufbau und Betrieb von „Virtuellen Trustcentern“[2] unterstützen.

■ Und werden lediglich Standardzertifikate für E-Mail oder VPN benötigt, muss das Trustcenter entsprechende Registrierungs-, Zertifizierungs- und Sperrdienste entlang dem gesamten „certificate lifecycle“ dieser Standardanwendung anbieten.

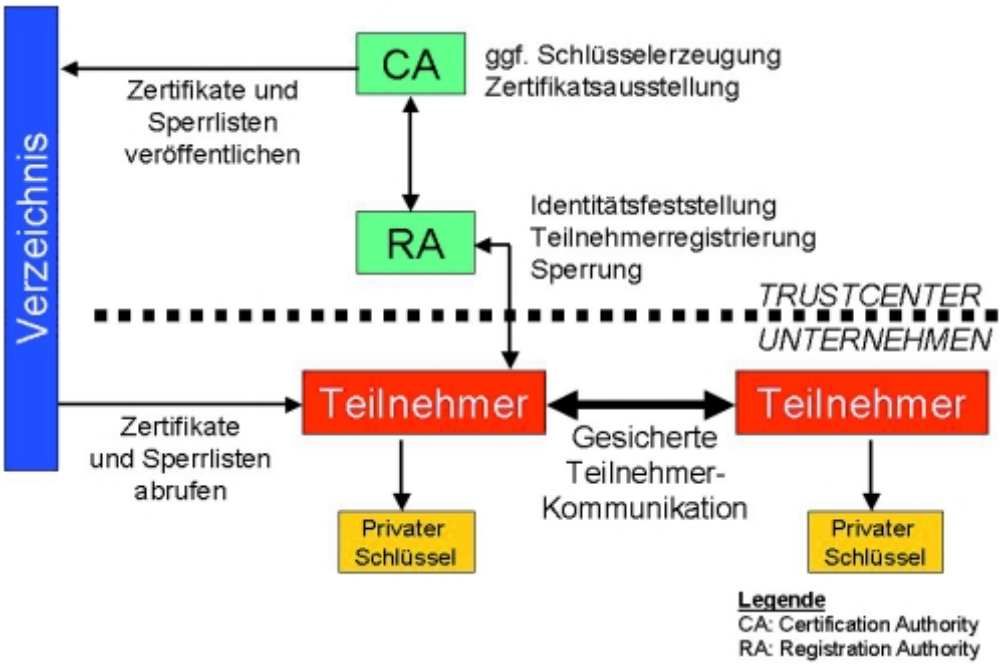

Abb.2: Vereinfachtes Modell einer möglichen Trustcenter-Nutzung im Unternehmen

Nicht alle Trustcenter-Dienstleister bieten alle Dienste an und es werden meist auch nicht alle Trustcenter-Dienste benötigt. Möchte beispielsweise ein Unternehmen einige der Dienste selbst erbringen, etwa seine Mitarbeiter identifizieren und registrieren, findet er bei einigen Trustcentern hierfür entsprechende „RA-Software“ für die Registrierung vor Ort. Möchte ein Unternehmen seine Schlüssel unter Eigenregie auf Smartcards erzeugen, ist dies auch oft möglich („dezentrale Schlüsselgenerierung“). Die Einbindung bereits vorhandener Infrastruktur des Unternehmens – zum Beispiel eines zentralen Verzeichnisservers – ermöglichen einige Anbieter ebenfalls.

Die Auswahl eines geeigneten Trustcenter-Dienstleisters hängt also vom konkreten Bedarf des Unternehmens ab und muss stets individuell und sehr sorgfältig erfolgen.

Das Beispiel in Abbildung 2 zeigt eine Lösung, bei der Identifikation, Registrierung, Zertifikatsausstellung, Zertifikatsveröffentlichung und der Sperrdienst vom Trustcenter erbracht wird. Die Mitarbeiter des Unternehmens nutzen die Schlüssel und Zertifikate für eine gesicherte Kommunikation.

Was kann ein Trustcenter nicht leisten?

Durch die Nutzung eines Trustcenters werden nicht alle Sicherheitsprobleme des Unternehmens gelöst. Im Gegenteil: Das eigene Trustcenter beziehungsweise die Dienste des Trustcenter-Dienstleisters müssen im Gesamtsicherheitskonzept des Unternehmens berücksichtigt werden. Dabei sind technische, organisatorische, infrastrukturelle und personelle Aspekte zu berücksichtigen.

Das beginnt bei den unternehmensinternen Abläufen, die eventuell stark angepasst werden müssen (zum Beispiel die Identifikation und Registrierung neuer Mitarbeiter durch die Personalabteilung und die Bereitstellung von entsprechenden Formularen), setzt sich fort mit der Schulung des einzelnen Mitarbeiters, der natürlich seine Schlüssel und Passworte sorgsam nutzen und verwahren muss, und erstreckt sich bis hin zur zentralen Beschaffung geeigneter Client-Produkte, die die Trustcenter-Dienste auch nutzen können (die beispielsweise das automatische Importieren der Zertifikate und Sperrlisten erlauben). Erst im abgestimmten Zu-

2 Das Konzept des „virtuellen Trustcenters“ erlaubt es einem Unternehmen, eine eigene PKI-Architektur zu entwerfen, welche dann aber nicht vom Unternehmen selbst, sondern vom Trustcenter-Dienstleister betrieben wird.

Trustcenter in Deutschland (Auswahl)

Name	Produkte/Services	Weitere Informationen
BSI PCA Verwaltung	Als Root-CA der Verwaltung stellt dieses Root-Trustcenter Zertifikate für Trustcenter aus (nur für Behörden)	www.bsi.bund.de/aufgaben/projekte/ sphinx/verwpki/erkl_pki.htm
Zertifizierungsstelle der Bundesnotarkammer (SigG)	Bietet SigG-spezifische Dienste (nur für Notare)	www.bnotk.de
CCI Trustcenter	Virtuelle CA Zertifikate für Personen und Services (z.B. Webserver)	www.cci.de/trustcenter.html
D-Trust GmbH	Virtuelle CA: D-Trust Corporate Zertifikate u.a. für Personen und Services (z.B. Webserver) Weitere Trustcenter-Dienste: OCSP, Zeitstempel, Verzeichnis	www.d-trust.net
DATEV Trustcenter	Bietet SigG-spezifische Dienste (nur für Steuerberater)	www.zs.datev.de
Deutsche Post Signtrust	Virtuelle CA (nach SigG) Zertifikate für Personen (nach SigG)	www.signtrust.de
DFN PCA	Zertifikate für Trustcenter von Institutionen im Hochschul- und Forschungsumfeld	www.cert.dfn.de/dfnpca/
FUN Keytrust Trustcenter	Virtuelle CA Zertifikate für Personen und Services (z.B. Webserver)	www.keytrust.de
IKS Jena	Zertifikate für Services (z.B. Webserver)	www.iks-jena.de /produkte/ca/
ITSG	Zertifikate für Institutionen im Gesundheitswesen	www.itsg.de
Medizon	Zertifikate für Personen im Gesundheitswesen (nach SigG): Produktlinie MediSign	www.medizon.de
mySAP-Trustcenter	mySAP-Kunden erhalten vom mySAP-Trustcenter Zertifikate („mySAP-passport“) für ihre mySAP-Anwendungen	www.sap.com/solutions/technology/ trust_center.htm
TC Trustcenter GmbH	Virtuelle CA: TC PKI Zertifikate für Personen und Services (z.B. Webserver) Spezielle Angebote: Identrus-Zertifikate	www.trustcenter.de (www.identrus.com)
Telekom Trustcenter SigG	Zertifikate für Personen (nach SigG)	www.telesec.de
Telekom Trustcenter	Virtuelle CA Zertifikate u.a. für Personen und Services (z.B. Webserver) Spezielle Angebote: ENX-Zertifikate	www.telesec.de (www.enxo.com)
Verisign	Virtuelle CA: Verisign Onsite Zertifikate u.a. für Personen und Services (z.B. Web- und WAP-Server, IPsec-Gateways)	www.d-trust.net
web.de-Trustcenter	Kostenlose Zertifikate für Personen (für E-Mail-Nutzung)	trust.web.de

Eine aktuelle Übersicht über Trustcenter in Europa und weltweit sowie viele weitere nützliche Links finden sich auf der „PKI Page“ von Stefan Kelm: www.pki-page.org

sammenspiel mit den unternehmensinternen Strukturen können die Trustcenter spezifischen Dienste tatsächlich zu einer hohen Gesamtsicherheit führen.

Wie viel Vertrauen verdient ein Trustcenter?

Wie kann ein Unternehmen Vertrauen in ein Trustcenter oder einen Trustcenter-Dienstleister gewinnen? Diese Frage ist nicht leicht zu beantworten, da „Vertrauen“ nur schwer zu operationalisieren ist. Ein Trustcenter sollte zunächst in der Lage sein, dem Unternehmen eine Einschätzung des mit ihm erreichbaren Sicherheitsniveaus zu erlauben. Dies kann zum Beispiel anhand der veröffentlichten „Policy“ des Trustcenters erfolgen (oft auch als Zertifizierungsrichtlinie oder „Certification Practice Statement“ – CPS – bezeichnet). Diese Policy sollte für das Unternehmen nachvollziehbar beschreiben, welche Dienstleistungen mit welchen konkreten Merkmalen angeboten werden und wie hoch die erreichbaren Sicherheitsniveaus sind. Ein Trustcenter, das keine schriftliche Policy vorweisen kann, sollte grundsätzlich als wenig vertrauenswürdig gelten. Letztlich sind aber natürlich auch die Policies reine Selbsterklärungen; erst wenn sie durch einen unabhängigen Gutachter in regelmäßigen Abständen bestätigt werden, zum Beispiel durch eine Sicherheitszertifizierung einer anerkannten oder akkreditierten Prüfstelle für IT-Sicherheit, kann das Unternehmen sicher sein, dass die vom Trustcenter versprochenen Dienste auch tatsächlich zuverlässig erbracht werden. Es gibt aktuell allerdings nur sehr wenige Trustcenter, die eine solche Sicherheitszertifizierung vorweisen können.

Das Vertrauen, welches ein Trustcenter

Trustcenter...

genießt, steht und fällt mit dem Vertrauen seiner (internen oder externen) Kunden. Jedes Unternehmen muss hierzu seine eigenen Kriterien aufstellen, um die Vertrauenswürdigkeit eines Trustcenters oder Trustcenter-Dienstleisters zu bewerten.

Wie viel kostet ein Trustcenter?
Bei der Abschätzung der Kosten eines Trustcenters oder Trustcenter-Dienstleisters sind nicht nur die effektiven Kosten für Aufbau und Betrieb beziehungsweise die Service-Dienstleistungen zu berücksichtigen. Daneben entstehen Kosten für die Beschaffung von Software-Lizenzen für die lokalen Anwendungen (zum Beispiel E-Mail-Sicherungskomponenten), und schließlich sind auch Aufwände für die Vorlaufphase (Konzeption, Umsetzung und Schulung) einzukalkulieren. Die Nutzung von Trustcenter-Diensten sollte sich für ein Unternehmen aber „rechnen":

- Durch die Einführung sicheren elektronischen Geschäftsverkehrs können kostenintensive Medienbrüche vermieden werden.
- E-Business kann den Zugang zu sonst nicht erschließbaren Märkten öffnen.

Können Geschäftsvorfälle durch den Wechsel auf elektronische Bearbeitung beschleunigt werden?
Zu den Vorteilen der Nutzung von Trustcenter-Diensten gibt es eine Reihe von Studien verschiedener PKI-Dienstleister und -Produktanbieter, die teilweise jedoch vor dem Hintergrund der Geschäftsinteressen der Herausgeber gelesen werden müssen. Denn jede Kosten-Nutzen-Analyse ist nur so gut wie die Annahmen, auf denen sie aufbaut – und die sind oft nur annäherungsweise zu bestimmen.

Wie findet man „seinen" Trustcenter-Dienstleister?
Die Kriterien für die Auswahl eines Trustcenter-Dienstleisters sind sehr vielfältig und hängen im Wesentlichen vom konkreten Anforderungsprofil des Unternehmens ab. Dieses sollte Antworten auf insbesondere die folgenden Fragen geben:

- Für welche Anwendungen des Unternehmens sollen Trustcenter-Dienste genutzt werden?
- Werden lediglich einfache Zertifikate für die Mitarbeiter oder den Webserver benötigt?
- Soll ein eigenes, „virtuelles" Trustcenter aufgebaut werden?
- Muss das Trustcenter die hohen gesetzlichen Anforderungen des Signaturgesetzes erfüllen?
- Stellt das Trustcenter die benötigten Schnittstellen bereit, damit seine Dienste auch in den eigenen organisatorisch-technischen „workflow" integriert werden können?
- Werden „Spezialdienste" wie Zeitstempeldienst oder „Key-Recovery" benötigt, oder reichen einfache „Basisdienste" aus?
- Werden nur wenige Zertifikate pro Jahr benötigt, oder wird ein hohes Volumen erwartet?
- Wie hoch sind die Sicherheitsanforderungen des Unternehmens?
- Sollen die Nutzer mit Smartcards ausgestattet werden, oder reicht es aus, die Schlüssel auf Diskette zu erhalten?

Zunächst sollte ein Unternehmen feststellen, welche Dienstleistungen tatsächlich benötigt werden („Anforderungskatalog" an die Trustcenter-Dienstleistung), bevor es mit einem Trustcenter-Dienstleister in konkrete Verhandlungen eintritt oder ein eigenes Trustcenter konzipiert. Die erforderlichen Dienstleistungen sollte sich ein Unternehmen schließlich vom Trustcenter-Dienstleister schriftlich zusichern lassen (zum Beispiel in Gestalt eines „Service Level Agreement" – SLA, in dem die vom Trustcenter-Dienstleister zu erbringenden Leistungen genau dokumentiert werden).

Darf es ein eigenes Trustcenter sein?
Ein Trustcenter unter „eigener Regie" aufzubauen und zu betreiben kann aus unterschiedlichen Gründen sinnvoll sein und sich im Vergleich auch rechnen. Viele Großunternehmen gehen diesen Weg, da oft nur über das eigene Trustcenter die benötigten spezifischen Dienste und Schnittstellen tatsächlich realisierbar und kontrollierbar sind. Insbesondere abhängig von der Anzahl der ausgestellten Zertifikate kann ein eigenes Trustcenter die kostengünstigere Realisierung sein.

Ein eigenes Trustcenter aufzubauen bedeutet aber auch, dass Personal für die Planung, den Aufbau und den Betrieb geschult und abgestellt werden muss. So sind Hard- und Software auszuwählen und zu beschaffen und geeignet abgesicherte Räumlichkeiten einzurichten. Um Fehlinvestitionen zu vermeiden, sollte dafür zu Beginn genügend Vorlaufzeit und Expertise investiert werden.

Das Trustcenter als Basisinvestition
Ab einer gewissen Größe und Komplexität des elektronischen Geschäftsverkehrs im Unternehmen können Trustcenter wesentliche Aufgaben der IT-Sicherheit übernehmen. Mehr noch: Die PKI kann die zentrale Sicherheitsinfrastruktur des Unternehmens darstellen, auf die sich alle Sicherheitsanwendungen und -dienste beziehen können.

Die Authentisierung von Benutzern und Servern bildet sehr oft die Basis für die unterschiedlichsten Sicherheitsdienste in einem Unternehmen – ein Sicherheitsdienst, der sich mit Hilfe einer PKI sehr gut realisieren läßt. Die Einbindung eines Trustcenters kann daher als Basisinvestition in die Sicherheitsinfrastruktur des Unternehmens begriffen werden.

Die Frage „Mehr Unternehmenssicherheit durch Trustcenter?" kann also mit einem eindeutigen „Ja, aber ..." beantwortet werden. Trustcenter können einen sehr guten Beitrag zur Gesamtsicherheit eines Unternehmens leisten. Allerdings ist der Aufbau einer PKI sehr komplex; es können Fehler auftreten, die die Sicherheit in Frage stellen. In [EF99], [FOX99] und [FOX00] finden sich viele praktische Hinweise für die Planung und den Aufbau einer unternehmensweiten PKI. Und: Unabhängige, auf IT-Sicherheit spezialisierte Beratungsfirmen können dabei helfen, schnell und verlässlich zu einer qualifizierten Entscheidung zu kommen, ob und wie eine PKI oder externe Trustcenter-Dienstleistungen in die eigene Sicherheitsinfrastruktur eingepasst werden können. ✓

Literatur und Verweise:

[BEU97] Beutelspacher, A. (1997): Geheimsprachen – Geschichte und Techniken.

[EF99] Esslinger, B.; Fox, D. (1999): Public Key Infrastructures in Banks - Enterprise-wide PKIs. In: Rannenberg, K.; Müller, G.; Pfitzmann, A. (Hrsg.): Multilateral Security in Communications (Volume III). (verfügbar im Internet unter: www.secorvo.de/publikat/bankpkis.htm)

[FOX99] Fox, D. (1999): Aufbau unternehmensweiter Public Key-Infrastrukturen. In: Proceedings zum 6. DFN-Workshop „Sicherheit in vernetzten Systemen", Hamburg 1999, S. G-1 bis G-12. (verfügbar im Internet unter: www.secorvo.de/publikat/aufbpki.htm)

[FOX00] Fox, D: (2000): E-Mail-Sicherheitslösungen. Secorvo White Paper. (verfügbar im Internet unter www.secorvo.de/whitepapers/wp01.pdf)

Weitere Internet-Ressourcen:

„The PKI-Page" von Stefan Kelm:
www.pki-page.org

Security-Server der Zeitschrift DuD:
www.datenschutz-und-datensicherheit.de/