

## PKI – Aktuelle Marktsituation

### Anwendungen

Eine PKI ist eine Infrastruktur, d.h. sie kann ohne Nutzenanwendungen nicht gerechtfertigt werden. Die Anwendungen sind die treibende Kraft für die Erstellung einer solchen Infrastruktur. Welche Anwendung dabei für ein Unternehmen der Motor ist, muss individuell festgestellt werden.

Die überwiegende Zahl von Anwendungen findet sich aber nicht im externen, sondern im internen Bereich eines Unternehmens. PKIs sind zu einem Begriff für Sicherheitsinfrastrukturen geworden. Sie ermöglichen es einem Unternehmen neue Anwendungen mit standardisierten und einheitlichen Sicherheitsverfahren auszurüsten und damit den Verwaltungsaufwand massiv zu reduzieren. PKIs sind eine umfassende Infrastruktur zur Abdeckung aller Sicherheitsbedürfnisse moderner, vor allem Web-basierender IT-Anwendungen.

Mit einem zertifikatsgestützten Sicherheitssystem ist es möglich, die Verwaltung der Berechtigungen wesentlich zu vereinfachen. Über die Einführung von PKI-Systemen gelangt man mehr oder minder automatisch zu einem "Single Sign on"-System oder einfacher gesagt, ein Benutzer muss sich nur noch einmal anmelden, um alle seine Anwendungen im Zugriff zu haben. In einem grösseren Betrieb bedeutet dies, dass Tausende von Objekten einfach verwaltet werden können. Man spricht hier bewusst von Objekten, da nebst den natürlichen Personen auch Prozesse, technische Objekte

(Server, Sicherheits-Gateway) oder juristische Personen identifizierbar gemacht werden können.

### Wer benötigt eine PKI ?

Jedes Unternehmen wird in Zukunft PKI-Technologie einsetzen. In welcher Ausprägung dies erfolgt, ist unterschiedlich. Mit Sicherheit werden neue Betriebssysteme wie Windows 2000 PKI-Technologie einsetzen und beinhalten. Die meisten Hersteller von Standardsoftware, welche Sicherheitsfunktionalitäten unterstützen, werden in Zukunft eine PKI voraussetzen.

PKIs sind wichtige Grundpfeiler für den Aufbau des E-Commerce. In allen Ländern der OECD sind Lösungen, welche digitale Signaturen als Hilfsmittel für die Beweisbarkeit elektronischer Transaktionen einsetzen, massiv im Vormarsch. In Zukunft ist zu erwarten, dass jeder Marktteilnehmer in der Lage sein muss, Meldungen (Bestellungen, Bestätigungen) digital zu signieren. Damit werden die heute gängigen Geschäftsprozesse massiv verändert, weil die traditionellen Verfahren zur Unterschriftenprüfung wegfallen. Die Prüfung erfolgt automatisch und die Verfahren können dadurch wesentlich vereinfacht sowie beschleunigt werden. Damit lassen sich Kosteneinsparungen, Kundenbindung und Wettbewerbsvorteile realisieren.

Digitale Signaturen können nicht zuletzt als Teil eines elektronischen Ausweises eine wesentliche Bedeutung

erlangen. Dies bedeutet, dass die öffentlichen Schlüssel der Teilnehmer bei der Zertifikatsausstellung beglaubigt werden müssen, d.h. die Qualität der getätigten digitalen Unterschrift ist im wesentlichen davon abhängig, wie gut die Identifikation des Teilnehmers und die spätere Verwaltung der Schlüssel erfolgt.

### Interne oder externe PKI?

Viele werden sich die Frage stellen, wie sie den Bedarf nach Zertifikaten abdecken sollen. Grundsätzlich ist die Zertifikaterstellung ein technisch einfacher Vorgang. Entsprechende Programme sind frei verfügbar oder können für wenig Geld erstanden werden. Der Aufwand liegt nicht in der technischen Zertifikaterstellung, sondern vor allem in der organisatorischen Bewältigung und der Unterstützung verschiedener Anwendungen. Eine PKI ist in die bankeninternen Abläufe zu integrieren und muss deshalb ein ausreichendes Mass an Prozessflexibilität besitzen. Die Aufwendungen entstehen somit bei der Verwaltung von Zertifikaten und bei der Anpassung der Anwendungen an eine PKI.

Man kann davon ausgehen, dass sowohl externe als auch interne Zertifikate genutzt werden müssen. Externe Zertifikate sind vor allem beim Einsatz als rechtsverbindliche Instrumente von Bedeutung. Wir gehen davon aus, dass jedes grössere Unternehmen in den nächsten zwei Jahren eine eigene PKI betreiben wird, d.h. es stellt sich nicht die Frage der Alternative sondern, wie man die interne PKI durch externe Nutzung ergänzen soll.

Die nachfolgenden Beispiele zeigen, in welchen Fällen zusätzlich externe Zertifikate (ausgestellt von einer firmenexternen Zertifikatsautorität) eingesetzt werden können:

- Zwingender Einsatz einer Vertrauensinstanz (z.B. im Signaturumfeld)
- Zertifikate im Einsatz mit "unbekannten Dritten" (Interbanking, Bank to Business, Bank to Consumer bzw. Zahlungspflichtiger)
- Unternehmen ohne eigene IT-Infrastruktur/Outsourcing
- Einsatz eines Zertifikates für bankenübergreifende Anwendungen (z.B. Homebanking).

Ein Outsourcing der PKI für interne Zwecke betrachten wir für grössere Unternehmen als nicht sinnvoll, für KMUs jedoch als angebracht. Für grössere Unternehmen ist ein Outsourcing wesentlich teurer, vor allem wenn man die Betriebskosten betrachtet (Total Cost of Ownership). Kostenmässig rechnet sich das Outsourcing bei hohen Zertifikatszahlen nicht, zumal grössere Banken in der Regel einen gut ausgebauten Dienst für die Verwaltung der Benutzerberechtigungen betreiben, der nach wie vor beibehalten werden muss. Wir gehen davon aus, dass pro Mitarbeiter und Jahr zwei Zertifikatsausstellungen sowie rund 30% an Mutationen (Zertifikatserneuerungen) erfolgen. Bei einem geschätzten Preis von Fr. 40.– pro Zertifikat ergibt das in einem Betrieb mit 1000 Mitarbeitern bereits den Betrag von rund Fr. 100 000.–. Hinzu kommt die Tatsache, dass man Sicherheit grundsätzlich nicht an Dritte outsourcen sollte, es sei denn, man bewegt sich in einem unkritischen Bereich bezüglich Haftung, was man im Finanzumfeld kaum behaupten kann. Will man die PKI trotzdem outsourcen, so muss

man sich im Minimum entsprechende Kontrollrechte vorbehalten und auf einer umfassenden Haftung der externen PKI beharren. Man muss sich bewusst sein, dass durch eine Kompromittierung des Systems ein sehr grosses Schadenspotential besteht. Ein weiterer Nachteil liegt in der beschränkten Flexibilität der externen PKI-Partner. Aus Sicherheitsgründen kann ein PKI-Outsourcer nicht verschiedenste Verfahren berücksichtigen, d.h. das Unternehmen muss sich dem Outsourcer anpassen.

Das Verhältnis von externer zu interner PKI lässt sich sehr gut mit dem aktuell gültigen System der Zeichnungsberechtigungen vergleichen. Grosse Unternehmen verzichten heute je länger je mehr darauf, jede Zeichnungsberechtigung eintragen zu lassen. Die Verwaltung dieser Befugnisse erfolgt rein intern. Gegen aussen werden nur die wichtigsten Unterschriften registriert. Ein Hauptgrund für dieses Vorgehen ist der hohe administrative Aufwand, der durch die dauernden Mutationen entstand. Die identische Ausgangslage präsentiert sich auch bei digitalen Zertifikaten. Hinzu kommt, dass derzeit kein externer Zertifikatsanbieter in der Lage ist, die Bedürfnisse, welche an eine interne PKI gestellt werden, zu erfüllen. So besteht für die firmeninterne Nutzung das zwingende Bedürfnis nach zwei verschiedenen Schlüsselpaaren, je einem Schlüsselpaar für die Verschlüsselung und die digitale Signatur. Der Grund liegt in der Tatsache, dass firmeninterne Daten auch entschlüsselbar sein müssen, wenn ein Mitarbeiter die Firma verlassen hat. Dies kann man nur mittels Hinterlegung des Schlüsselpaares für die Verschlüsselung lösen. Eine Hinterlegung des Schlüssel-

paares für die digitale Signatur gefährdet aber die Nicht-Abstreitbarkeit einer digitalen Unterschrift (da der Signaturschlüssel nicht nur dem ursprünglichen Eigentümer zugänglich ist). Diese widersprüchlichen Anforderungen lassen sich nur mit mehreren Schlüsselpaaren lösen.

## Rechtliches

Viel wird über die rechtliche Bedeutung von digitalen Signaturen geschrieben, vielfach ohne Kenntnisse des konkreten Einsatzes. Die rechtlichen Anforderungen an eine PKI können nicht allgemein formuliert werden. Ohne zusätzliche Regeln zum OR (CH) oder BGB (D) besteht eine grosse Rechtsunsicherheit bezüglich der Anwendung von digitalen Signaturen im Geschäftsleben. In Deutschland wurde per 1.8.97 das Gesetz zur digitalen Signatur als Teil des Informations- und Kommunikationsdienstegesetzes (Art. 3) in Kraft gesetzt. In der Schweiz wurde mit der Verabschiedung der OR Revision zu den Aufbewahrungsvorschriften (957, 962 OR) im Nationalrat Mitte Oktober 1999 ein wichtiger Schritt getan, dass auch Geschäftsunterlagen in Zukunft nur noch elektronisch gespeichert werden müssen. Die elektronische Speicherung dürfte aber nur dann anerkannt werden, wenn die Daten entsprechend gesichert wurden. Nicht unterstützt werden können Bestrebungen, die lediglich darauf abzielen, Sicherheitsstandards vorzuschreiben ohne einen rechtlichen Nutzen zu erzeugen, wie dies im Verordnungsvorschlag des BAKOM gemacht wird. Dies läuft auch entgegen einem aktuellen Parlamentsbeschluss der EU, wonach die Mitgliedsländer in der

kürzlich erlassenen Direktive zur digitalen Signatur aufgefordert werden, ihre Unterschriftendefinitionen im Privatrecht dem elektronischen Surrogat anzupassen. Unser Nachbarland Österreich wird per 1.1.2000 ein Signaturgesetz in Kraft setzen, welches die Gleichwertigkeit von Digitaler Signatur und eigenhändiger Unterschrift statuiert.

## Anbieter

In den letzten beiden Jahren haben sich sowohl auf Produkt- als auch Dienstleistungsseite verschiedene Anbieter im Markt positioniert. International gilt VeriSign als Marktleader im PKI-Segment, soweit dies die Ausstellung von Zertifikaten und das Outsourcing angeht. In der Schweiz hat sich Swisskey dies auf die Fahne geschrieben. Im Markt Europa haben sich die externen Anbieter bisher nicht wirklich positionieren können. Die Anläufe von VeriSign in Europa Fuss zu fassen sind bisher ohne nennenswerte Wirkung geblieben. Wir gehen davon aus, dass der europäische Kunde, vor allem im Finanzbereich, auf Fragen der Sicherheit sensibler reagiert und diese Funktionen deshalb nicht auslagern will. Zum Teil spielt auch das Element Wettbewerbsvorteil hier eine Rolle, kann doch eine attraktive Sicherheitslösung durchaus einen unmittelbaren Wettbewerbsvorteil erzeugen.

Im Corporate Markt hat nach wie vor Entrust Technologies einen Marktvorsprung, wird aber von Anbietern wie Baltimore Technologies, RSA und iD2 bedrängt. Es ist davon auszugehen, dass sich noch weitere Anbieter in diesem Markt positionieren wollen,

gilt der IT-Sicherheitsmarkt doch als einer der attraktivsten Wachstumsbereiche. Dies lässt sich unschwer feststellen, wenn man die Angebote diverser IT-Unternehmen betrachtet, die nach neuen Umsatzquellen suchend, nun plötzlich auf dieser Welle zu segeln beginnen. Erfahrungsgemäss ist der Faktor Vertrauen hier

entscheidend. Bei der Vergabe von Sicherheitsprojekten wird nach wie vor stark auf die Qualität des Anbieters und seine Vertrauenswürdigkeit geachtet.

*B. Wildhaber, iTrust, Zürich*

## Zum Status der PKI in Deutschland

In der Bundesrepublik Deutschland wurde 1997 das Informations- und Kommunikationsdienstegesetz (IuKDG -BT-Drs. 13/7934 vom 11.06.1997; BGBl I (1997), 1870) verabschiedet. Dieses ausserordentlich zügig konzipierte Artikelgesetz umfasste neben Änderungsvorschriften für andere Rechtsnormen in Art. 3 das Gesetz zur digitalen Signatur (Signaturgesetz-SigG). Zusammen mit der Signaturverordnung von 1997 (SigV; BGBl I (1997), 2498) bildet das SigG den Kern der bundesdeutschen PKI-Normierung.

Das SigG war das erste Gesetz zur Regelung digitaler Unterschriften in Europa. Es regelt die Grundzüge einer Infrastruktur (Zertifizierungsstellen, technische Komponenten) für digitale Signaturen auf einem hohen Sicherheitsniveau. Ziel des Gesetzes war auch, durch frühzeitige Vorgabe einer Rahmenordnung die Entwicklung inhomogener Standards und Produkte zu vermeiden. Die SigV dient der weiteren Ausgestaltung des SigG.

Die Zertifizierungsstellen unterliegen einem Zulassungsverfahren bei der Regulierungsbehörde für Telekom-

munikation und Post (RegTP). Die RegTP legt bei der Zulassung die im Gesetz vorgesehenen und 1998 vom BSI erstmals erarbeiteten, laufend zu aktualisierenden Massnahmenkataloge (Beil. BAnz 204a (1998)) für Zertifizierungsstellen und technische Komponenten zugrunde. Die zwei gegenüber den ursprünglichen Entwürfen stark gekürzten Massnahmenkataloge enthalten unverbindliche Empfehlungen, wie die Anforderungen aus SigG und SigV erfüllt werden können.

Die deutsche PKI-Rahmenordnung lässt aus Praktikabilitätsgründen gezielt sowohl private als auch staatlich sanktionierte, d.h. dem im Detail gesetzlich geregelten Verfahren unterliegende PKI-Verfahren zu. Den im gesetzlichen Rahmen zertifizierten Verfahren wird man bei der Beweiswürdigung bis zum Beweis des Gegenteils Rechtskraft unterstellen (Sicherheitsvermutung). Die Beweiskraft "privater" Verfahren wird – wenn angegriffen – in der Regel zu verteidigen sein; es gibt allerdings keinen Anlass zu der Vermutung, dass private Verfahren, die sich am Stand der Technik

orientieren, diesen Ansprüchen nicht genügen werden.

Mit dem Gesetz wurde eine Evaluierung nach zweijähriger Laufzeit der Rechtsnorm beschlossen. Das Ergebnis der im Sommer 1998 publizierten Evaluierung (BT-Drs. 14/1191 vom 16.06.1999) war, dass – trotz des sich konkretisierenden Normsetzungsverfahrens auf EU-Ebene – keine Veranlassungen zu grundlegenden Änderungen von SigG und SigV besteht. Hersteller, Anwender und Fachleute klagten allerdings über die hohen Anforderungen des Zertifizierungsverfahrens, zu teure Komponenten, fehlende Produkte und Unzulänglichkeiten des Normensets.

Neben der von der Deutschen Telekom AG betriebenen ersten deutschen Zertifizierungsstelle planen unter anderem der Bundesverband Deutscher Banken, der Deutsche Industrie- und Handelstag, die Deutsche Post AG, der Chipkarten-Produzent Giesecke & Devrient sowie weitere Unternehmen das Errichten einer Zertifizierungsstelle.

Es ist offensichtlich, dass in der Praxis vorrangig die nicht-regulierten, vom Gesetz ausdrücklich gebilligten Verfahren eingesetzt werden. Der rechtsverbindlichen elektronischen Unterschrift im Sinne des SigG kommt anscheinend bisher – konkrete Anwendungen befinden sich im Gesetzgebungsverfahren – nur in Ausnahmefällen Bedeutung zu. Zudem weichen die sich immer weiter verbreitenden, internationalen Standards wie PGP, SSL und S/MIME sowie grenzüberschreitende Zertifizierungsansätze (z.B. von Banken) zum Teil deutlich von den Anforderungen des SigG ab.

Vor diesem Hintergrund – und der Bedeutung grenzüberschreitender Transaktionen – gewinnen international-rechtliche Normen an Gewicht. So hat die EU-Kommission ausgehend von ihrem in 1997 kommunizierten Regelungsvorhaben im Juni 1998 einen ersten Regelungsentwurf (KOM (1998)297 endg., ABIEG C 325/5 vom 23.10.1998) vorgelegt. Eine mit handschriftlichen Unterschriften vergleichbare Beweiskraft elektronischer Signaturen wäre demnach an bestimmte Kriterien gebunden; für Zertifizierungsinstanzen war in bestimmten Situationen eine verschuldensunabhängige Haftung vorgesehen.

Dieser Entwurf wurde vom Rat als nicht weitreichend genug zurückgewiesen und ergänzt im April 1999 als gemeinsamer Standpunkt von Rat und Kommission verabschiedet (KOM (1999)195 endg. vom 29.04.1999). Nun sind zum Beispiel eine nationale Aufsicht und Kontrollen der Zertifizierungsinstanzen vorgesehen sowie – dies geht über das SigG hinaus – Rechtsfolgen (Beweiskraft der “fortschrittlichen” elektronischen Signatur) geregelt. Der Richtlinienentwurf wurde im Oktober 1999 vom EU-Parlament und am 30. November 1999 vom Rat der für Telekommunikation zuständigen Minister angenommen. Die Richtlinie ist in den 18 Monaten nach der Veröffentlichung im Amtsblatt in das nationale Recht umzusetzen. Erforderliche Änderungen des bundesdeutschen Rechts (z.B. der Schriftformerfordernisse des BGB) sind im Rahmen des Entwurfs für ein „Gesetz zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr“ bereits in Vorbereitung.

Weitere Rahmenbedingungen werden sich darüber hinaus aus der EU-Richtlinie zum elektronischen Geschäftsverkehr (Entwurf als KOM (1998)568 endg., ABIEG C 30/4 vom 05.02.1999) ableiten lassen. Ein überarbeiteter Richtlinienentwurf wurde dem Parlament am 01.09.1999 übermittelt.

Darüber hinaus hat der OECD-Rat am 27.03.1997 eine Kryptographierichtlinie (OECD-GI (97) 204) beschlossen. Das Technical Committee Security des European Standards Institute (ETSI) betreibt ein Vorhaben zur Standardisierung der elektronischen Signatur, um Minimalstandards zum Zusammenwirken der am elektronischen Geschäftsverkehr beteiligten festzulegen. Die Kommission für Handelsrecht der Vereinten Nationen (UNCITRAL) hat seit 1997 mehrere Entwürfe für einheitliche Regeln über elektronische Signaturen publiziert; sie enthalten Mindestanforderungen an die Sicherheit, Regeln zu Authentifizierung sowie Zertifizierung und Haftung von Signatordienstleistern.

Die weitere Entwicklung der europäischen PKI-Rahmenordnung wird vor dem Hintergrund des Gestalt annehmenden EU-Rechts sowie des darauf ausstrahlenden UNCITRAL-Normsetzungsprozesses stattfinden. Diese international-rechtlichen Vorgaben sehen wie das bundesdeutsche SigG eine PKI-Infrastruktur aus zertifizierten und freien Anbietern mit abgestuften Rechtswirkungen vor. Die konkrete Ausgestaltung einer sachgerechten PKI-Infrastruktur wird man von jeweils aktuellen, branchenbekannten Sicherheitsstandards (z.B. ITSEC) abhängig machen.

Über die unten aufgeführten Quellen hinausgehende Detailinformationen und Links sind auf der Webversion des Newsletters ([www.isaca.de/newsletter/newsletter.htm](http://www.isaca.de/newsletter/newsletter.htm)) hinterlegt.

## Ausgewählte Literatur

- André S., Glöckner, P.: TrustFactory, in: DuD 7/98, 373
- Baum, M.: Gültigkeitsmodell des SigG, in: DuD 4/99, 199
- Baum, M.: Die elektronische Identität, in: DuD 9/99, 511
- Bertsch, A., Pordesch, U.: Zur Problematik von Prozesslaufzeiten bei der Sperrung von Zertifikaten, in: DuD 9/99, 514
- Bieser W., Kersten H.: Elektronisch unterschreiben. Die digitale Signatur in der Praxis, Heidelberg (Hüthig) 1999
- Bitzer F., Brisch K. M.: Digitale Signatur. Grundlagen, Funktion und Einsatz, Berlin (Springer) 1999
- Boriths Müller, H., Roessler, T.: Zur rechtlichen Anerkennung elektronischer Signaturen in Europa, in DuD 9/99, 497
- Brisch, K.M.: EU-Richtlinienvorschlag zum elektronischen Geschäftsverkehr, in: CR 4/99, 235
- Emmert, U.: Haftung der Zertifizierungsstellen, in CR 4/99, 244
- Fox, D.: Zu einem prinzipiellen Problem digitaler Signaturen, in: DuD 7/98, 386
- Fox, D.: Die Regulierung der Nullmenge, in DuD 9/99, 494
- Fox, D.: Eine kritische Würdigung des SigG, in: DuD 9/99, 508
- Gramlich, L.: Die Regulierungsbehörde für Telekommunikation und Post im Jahre 1998, in: CR 8/99, 489
- Hoeren, T.: Internet und Recht – Neue Paradigmen des Informationsrechtes, in: NJW 39/99, 2854
- Jürgens, U.: Wachsende Bedeutung von Sicherheitszertifikaten, in: DSB 2/99, 6
- Kelm, S.: Signed in Germany?, in: DuD 9/99, 526
- Knupfer, J.: Europäische Kommission schlägt Richtlinie für elektronische Signaturen vor, in: DSB 8/99, 9
- Kuner, C.: Signaturgesetze und “Political Correctness”, in: DuD 4/99, 227
- Menzel, T., Schweighofer, E.: Das österreichische Signaturgesetz, in: DuD 9/99, 503
- Pordesch, U., Rossnagel, A.: Elektronische Signaturverfahren rechtsgemäss gestaltet, in: DuD 2/94, 82
- Rassmann, S.: Elektronische Unterschrift im Zahlungsverkehr, in: CR 1/98, 36
- Roessler, T.: PGP – “Kryptographie fürs Volk”, in: DuD 7/98, 377
- Rossnagel, A.: Digitale Signaturen im Rechtsverkehr, in: NJW-CoR 2/94, 96
- Rossnagel, A.: Das Gesetz und die Verordnung zu digitalen Signatur – Entstehung und Regelungsgehalt, in: RDV 1/98, 5
- Rossnagel, A.: Die Sicherheitsvermutung des Signaturgesetzes, in: NJW 45/98, 3312
- Rossnagel, A.: Das Signaturgesetz nach zwei Jahren, in: NJW 22/99, 1591
- Welsch, G.: Stufenweise skalierbare Sicherheit für digitale Signaturen, in: DuD 9/99, 520

## Rechtsnormen auf offiziellen Servern

- Deutsches Informations- und Kommunikationsdienstegesetz (IuKDG) mit Signaturgesetz (SigG) und Signaturverordnung (SigV): [www.iid.de](http://www.iid.de)
- OECD-Kryptographierichtlinie: [www.oecd.org](http://www.oecd.org)
- Richtlinienvorschlag der EU für digitale Signaturen: [www.ispo.cec.be](http://www.ispo.cec.be)
- UNCITRAL-Richtlinienvorschlag für elektronische Signaturen: [www.uncitral.org](http://www.uncitral.org)

## Zertifizierung

- [www.regtp.de](http://www.regtp.de): Deutsche Regulierungsbehörde für Telekommunikation und Post
- [www.admin.ch/bakom](http://www.admin.ch/bakom): Schweizerisches Bundesamt für Kommunikation
- [www.tkc.at](http://www.tkc.at): Österreichische Gesellschaft für Telekommunikationsregulierungen
- [www.bsi.de](http://www.bsi.de): Ausgestaltung der Zertifizierungsinstanzen und technischen Komponenten
- [www.teletrust.de](http://www.teletrust.de): Kompetenzverbund mit 70 Mitgliedern
- [www.dtag.de/zertifikate/index.htm](http://www.dtag.de/zertifikate/index.htm): Betreiber eines zugelassenen Servers

*Dr. U. Hahn/R. Muthmann, Eschborn/Frankfurt*

## PKI in der Schweiz

### Einleitung

Es wird heute viel über die Bedeutung der Information als vierten, Boden, Kapital und Arbeit ergänzenden Produktionsfaktor und die sich abzeichnende Informationsgesellschaft<sup>1</sup> gesprochen. Dabei sind der elektronische Handel und Geschäftsverkehr (engl. "Electronic Commerce" bzw. "E-Commerce"), sowie die damit realisierbaren Kosteneinsparungen die treibenden Kräfte für diese Entwicklung. Die Euphorie, mit der heute auf allen Fronten in Richtung Informationsgesellschaft hingearbeitet wird, wird allerdings auch etwas durch die Sicherheitsrisiken gebremst, die sich aus dem Einsatz der Informations- und Kommunikationstechnik (IT) bzw. der entsprechenden IT-Systeme ergeben. Man denke hier etwa an die verschiedenen Hackeran- und -übergriffe, über die in den Medien immer wieder berichtet wird, an die Wirtschaftsspionage, sowie an die Möglichkeiten zur informationstechnischen Kriegsführung (engl. "Information Warfare").

Damit die Attraktivität und Vorteile des elektronischen Handels und Geschäftsverkehrs voll ausgeschöpft werden können, müssen die entsprechenden Kommunikationsmedien (z.B. TCP/IP-basierte Intranets und

das Internet) sicher(er) gemacht werden. Kryptographische Verfahren spielen für diese Absicherung eine wesentliche Rolle<sup>2</sup>. Zwei wichtige Anwendungen der Kryptographie sind:

- die Verschlüsselung (Chiffrierung), um die Vertraulichkeit der übertragenen Daten zu sichern, sowie
- die digitale Signatur, um sowohl die Unverfälschtheit der Herkunft (Authentizität) als auch die Vollständigkeit und Unversehrtheit der Daten (Integrität) zu sichern.

Dabei wird als digitale Signatur ein mit Hilfe eines kryptographischen Verfahrens erzeugtes "digitales Siegel" für Daten verstanden, das von einem Aussenstehenden verifiziert werden kann. Die meisten digitalen Signaturverfahren basieren auf asymmetrischen Kryptosystemen. In einem solchen Kryptosystem verfügt jeder (jede) Benutzer (Benutzerin) über zwei Schlüssel:

- Ein öffentlicher Schlüssel, der öffentlich bekannt ist und z.B. über einen Verzeichnisdienst publiziert werden kann, sowie
- ein privater Schlüssel, der nur dem (der) betreffenden Benutzer (Benutzerin) bekannt sein darf.

Obwohl die beiden Schlüssel in einer mathematisch eindeutigen Beziehung

zueinander stehen (müssen), ist es mit vertretbarem Aufwand für einen Aussenstehenden nicht möglich, von einem öffentlichen Schlüssel auf den dazugehörigen privaten Schlüssel zu schliessen (wenigstens unter der Annahme, dass der Aussenstehende ein bestimmtes mathematisches Problem, wie z.B. das Faktorisierungsproblem<sup>3</sup> oder das diskrete Logarithmusproblem<sup>4</sup> für grosse Zahlen, nicht lösen kann).

Der sichere und effiziente Einsatz von asymmetrischen Kryptosystemen erfordert unter anderem auch den Einsatz von zertifizierten öffentlichen Schlüsseln (sogenannte "Zertifikate"), wie sie z.B. von einem Zertifizierungsdienstleister (engl. "Certification Authority" oder CA) bereitgestellt werden können. Ein zertifizierter öffentlicher Schlüssel ist ein öffentlicher Schlüssel (aus einem asymmetrischen Kryptosystem), der in bezug auf seine Authentizität und Integrität von einer vertrauenswürdigen Stelle (z.B. einer CA) beglaubigt (und digital signiert) worden ist. Dabei können sich CAs auch gegenseitig beglaubigen und zertifizieren. Man spricht in diesem Zusammenhang von sogenannten "Cross-Zertifizierungen".

Eine Public Key Infrastruktur (PKI) entsteht aus einer Menge von Zertifizierungsdienstleistern, die in einem bestimmten Geltungsbereich (z.B. einem Unternehmen oder Staat) formal anerkannt sind. Die formale Anerkennung kann dabei auf unterschiedliche Art und Weise erfolgen, wie z.B. durch die Publikation in einem Verzeichnis oder durch die Beglaubigung und Zertifizierung durch einen übergeordneten Zertifizierungsdienstleister (eine sogenannte "Root-CA"). In

1 Exemplarisch sei hier nur auf die am 18. Februar 1998 vom Bundesrat verabschiedete Strategie für eine Informationsgesellschaft in der Schweiz hingewiesen.

2 Die physikalische Absicherung der Kommunikationsmedien kommt aus wirtschaftlichen Gründen meist nicht in Frage.

3 Das Faktorisierungsproblem lässt sich folgendermassen beschreiben: Gegeben ist eine sehr grosse Zahl  $n$ . Gesucht ist die Primfaktorenzerlegung von  $n$ .

4 Das diskrete Logarithmusproblem lässt sich folgendermassen beschreiben: Gegeben sind eine grosse Primzahl  $p$ , ein  $y < p$  und ein Generator  $a$  der multiplikativen Gruppe  $Z_p^*$ . Gesucht ist ein  $x$ , das die Gleichung  $y = ax \pmod{p}$  erfüllt.

beiden Fällen müssen unabhängige Prüfstellen die Zertifizierungsdienst-erbringer anhand von bestimmten Kriterien prüfen und im positiven Fall auch zertifizieren (ähnlich wie bei ISO 9000). In Anlehnung an die Terminologie im Akkreditierungsbereich werden solche Prüfstellen als Zertifizierungsstellen (engl. "Certification Bodies" oder CBs) bezeichnet.

## Situation in der Schweiz

Am 16. Juni 1997 hat der Bundesrat das EFD beauftragt, eine Arbeitsgruppe zu bilden, welche die Grundlagen und Konzepte für eine Trusted Third Party (TTP) in der Bundesverwaltung zuhanden des Bundesrates ausarbeitet. Am 22. August 1997 hat das EFD die Einsetzung der interdepartementalen Arbeitsgruppe (AG BV-TTP) verfügt, um die Entwicklungen auf nationaler, europäischer und internationaler Ebene zu verfolgen, die technischen, juristischen und organisatorischen Grundlagen und Konzepte für eine TTP der Bundesverwaltung zu erarbeiten und dem Bundesrat zu berichten.

Aufgrund des von der AG BV-TTP vorgelegten Berichtes hat der Bundesrat am 29. Januar 1999 beschlossen,

- dass die Arbeiten im Rahmen der Massnahme 3 "elektronischer Geschäftsverkehr" der Strategie des Bundesrates für eine Informationsgesellschaft in der Schweiz vom 18. Februar 1998 und auf den heute vorhandenen Grundlagen und Konzepten der AG BV-TTP weiterzuführen sind,
- dass das UVEK für die Koordination der Arbeit (und für die Prüfung der Notwendigkeit der Erarbeitung von gesamtschweizerischen Regeln),

das EFD für die Erarbeitung von technischen Grundlagen und das EJPD für die Vorbereitung der Rechtsverbindlichkeit von digitalen Signaturen zuständig ist,

- dass das UVEK dem Bundesrat bis Mitte 1999 einen Schlussbericht mit entsprechender Umsetzungsplanung vorzulegen hat,
- und dass für die Übergangszeit das EFD in der Bundesverwaltung Zertifizierungsdienste anzubieten hat.

Eine wesentliche Erkenntnis der AG BV-TTP hat darin bestanden, dass es für die Bundesverwaltung a priori keine Rolle spielt, ob Zertifizierungsdienstleistungen selbst erbracht oder fremdbezogen werden, solange bestimmte Mindestanforderungen an die Qualität der resultierenden Zertifikate erfüllt sind. Was aber dringend benötigt wird, ist eine Art "Gütesiegel" für Zertifikate, die in der Bundesverwaltung eingesetzt werden und in dieser auch anerkannt werden und gültig sind. Damit decken sich die Anforderungen der Bundesverwaltung mit den Anforderungen der Wirtschaft und getrennte Wege sind in diesem Bereich wenig sinnvoll.

Vor diesem Hintergrund ist die vom UVEK geleitete Arbeitsgruppe "Digitale Signatur" (AG DigSig) ins Leben gerufen worden. Ziel der AG DigSig ist die Erarbeitung und Inkraftsetzung einer Verordnung für eine PKI (PKIV) in der Schweiz. Ein entsprechender Entwurf ist im Sommer 1999 interessierten Kreisen der Wirtschaft vorgelegt worden und befindet sich zur Zeit in der Ämterkonsultation. Flankiert wird die PKIV von Ausführungsbestimmungen, die vom Informatikstrategieorgan Bund (ISB) und der Schweizerischen Akkreditierungs-

stelle (SAS) erarbeitet werden. Die PKIV und die entsprechenden Ausführungsbestimmungen regeln, wie von der SAS akkreditierte Zertifizierungsstellen (CBs) Zertifizierungsdienst-erbringer (CAs) prüfen und formal anerkennen können, und wie die Liste der anerkannten Zertifizierungsdienst-erbringer publiziert wird. Die PKIV soll auf den 1. Januar 2000 in Kraft treten.

## Situation ausserhalb der Schweiz

Seit einigen Jahren versuchen verschiedene Staaten regulatorische und gesetzliche Vorgaben für den (rechtsverbindlichen) Einsatz von elektronischen bzw. digitalen Signaturen zu machen (in der Hoffnung, damit den elektronischen Handel zu fördern). In Europa hat Deutschland mit seinem Signaturgesetz (SigG) bzw. der entsprechenden Signaturverordnung (SigV) eine entsprechende Vorreiterrolle gespielt. Das SigG regelt zusammen mit der SigV den Aufbau und die formale Anerkennung von Zertifizierungsdienst-erbringern im Sinne einer PKI für Deutschland. Diese PKI ist streng hierarchisch aufgebaut und entspricht einem Baum der Tiefe 1, d.h. jeder Zertifizierungsdienst-erbringer muss hier zwingend von einer staatlichen Root-CA zertifiziert sein. Dabei bedeutet "zertifiziert", dass der Zertifizierungsdienst-erbringer formal anerkannt wird, und dass sein öffentlicher Schlüssel beglaubigt und von der Root-CA digital signiert wird.

Der im Rahmen der PKIV verfolgte Ansatz versucht die formale Anerkennung von der Zertifizierung im Sinne der Beglaubigung des öffentlichen

Schlüssels des Zertifizierungsdienst-erbringers logisch zu entkoppeln, und die anerkannten Zertifizierungsdienst-erbringer in Form einer (authentifizier-ten) Liste zu publizieren. Dieser An-satz zeichnet sich durch eine erhöhte Flexibilität aus und ist konform mit einer Richtlinie, die das Europäische Parlament und der Rat der Europä-ischen Union am 28. Juni 1999 über gemeinsame Rahmenbedingungen für elektronische Signaturen erlassen hat. Diese Richtlinie weicht vom streng hierarchischen Modell des SigG/SigV zugunsten eines allgemeineren Akkre-ditierungsmodells ab.

## Schlussfolgerungen und Ausblick

“PKI” ist eines der aktuellen Schlag- worte der Informatiksicherheitsin- dustrie. Die Versprechen, mit denen PKIs und PKI-basierte Sicherheits- lösungen auf den Markt gebracht werden, sind kritisch zu hinterfragen. Zunächst einmal muss festgehalten werden, dass digitale Signaturen zur Zeit nicht in dem Masse die treibende Kraft für den Aufbau und Betrieb von PKIs sind, wie es z.B. das SigG impli- ziert. Zertifikate werden heute meist für SSL- und TLS-basierte Sicher- heitslösungen, Single-Sign-On-Pro- dukte und S/MIME-basierte Lösungen für den sicheren Austausch von elekt- ronischen Nachrichten eingesetzt. Die Nutzung von digitalen Signaturen als Ersatz für handschriftliche Unter- schriften ist heute noch kaum verbreit- et. In diesem Sinn stellt der Einsatz einer PKI einfach eine (weitere) Mög- lichkeit dar, das Authentifikations- problem in vernetzten und verteilten Systemen anzugehen. Neben PKI- basierten Ansätzen gibt es hier auch

Alternativen, wie z.B. Authentifika- tionssysteme, die auf symmetrischen Kryptosystemen aufsetzen (z.B. Ker-beros), Challenge/Response-Systeme oder Hardware-Token, die einmalige Passworte erzeugen oder biometrische Authentifikationsverfahren nutzen.

Wie jede Technologie haben auch PKI-basierte Lösungsansätze spezi- fische Vor- und Nachteile.

*Vorteile:* Die Vorteile liegen in der Sicherheit dieser Systeme, im Grad der Standardisierung, sowie in der Möglichkeit, PKI-basierte Lösungen auch für die Umsetzung und Erbrin- gung von anderen Sicherheitsdiensten (neben Authentifikationsdiensten) zu nutzen.

*Nachteile:* Als nachteilig muss sicher- lich der Aufwand bezeichnet werden, mit dem PKIs aufgebaut werden (müs- sen). Aufwände liegen hier vor allem im Bereich der Benutzerschnittstelle (z.B. “Help Desk”-Funktionen). Zu- dem wird das Zertifikatsmanagement durch die Frage der Sperrung und Un- gültigkeitserklärung von Zertifikaten (engl. “Certificate Revocation”) er- schwert. Viele Erleichterungen, die man sich durch den Einsatz von asym- metrischen Kryptosystemen verspro- chen hat, verliert man wieder, wenn man die Sperrung und Ungültigkeits- erklärung von Zertifikaten mitberück- sichtigt. In der Tat stellt die Kompo- nente einer PKI-Lösung, die sich um diese Fragen kümmert, die einzige Komponente dar, die zwingend online verfügbar sein muss. Die Grenzen zu Authentifikationssystemen, die sich nicht asymmetrischer Kryptosysteme bedienen, sind dann fließend.

Aus sicherheitstechnischer und wirt- schaftlicher Sicht lässt sich der Aufbau

und Betrieb einer PKI eigentlich nur durch den Einsatz von digitalen Sig- naturen für die Umsetzung von Ver- bindlichkeitsdiensten begründen. Die Bedeutung von Verbindlichkeitsdien- sten wird in Zukunft (und vor allem auch vor dem Hintergrund des E- Commerce) noch stark zunehmen. Entsprechende rechtliche Rahmen- bedingungen sind wichtig und die Definition eines “Gütesiegels” für Zertifikate im Sinne der PKIV stellt für diese Rahmenbedingungen eine wichtige Voraussetzung dar.

*PD Dr. Rolf Oppliger,  
Informatikstrategieorgan Bund ISB,  
Fachbereich Informatiksicherheit,  
Bern*

## Business: Hindernis und Schlüssel zum Erfolg

Die geringen Kosten und die weltweite Verfügbarkeit des Internets – sowohl für privaten als auch geschäftlichen Gebrauch – münden derzeit in einer Revolution: Die Revolution des “Electronic Business” (E-Business). E-Business wird die Art und Weise Geschäfte zu machen radikal ändern, denn wir bewegen uns derzeit ins nächste Zeitalter: Vom Informations-Zeitalter in das Kommunikations-Zeitalter. Unternehmen, die sich diesem Trend anschliessen, erhoffen sich Chancen und Möglichkeiten für völlig neue Märkte, Geschäftsinitiativen und -aktivitäten, die erst durch den Gebrauch elektronischer Medien ermöglicht werden. Bestehende Geschäftspraktiken sollen aufgrund der geringen Bearbeitungskosten und der hohen Geschwindigkeit elektronischer Transaktionen wesentlich billiger und effektiver durchgeführt werden können.

Doch trotz einiger viel beachteter Erfolgsgeschichten (z.B. Amazon, IBM) sind viele Unternehmen und Privatkunden noch sehr vorsichtig und befassen sich nur zögerlich mit E-Business. Es herrscht zum einen Unsicherheit über das wahre Potential des elektronischen Marktes und dessen Reife. Ist der richtige Zeitpunkt gekommen, um die notwendigen Investitionen zu treffen? Ist die notwendige Technologie verfügbar, stabil und skalierbar? Noch öfter werden aber zweitens die scheinbar fehlende Sicherheit und mangelndes Vertrauen als die wesentlichen Barrieren genannt.

Die Hauptbedenken lassen sich wie folgt zusammenfassen:

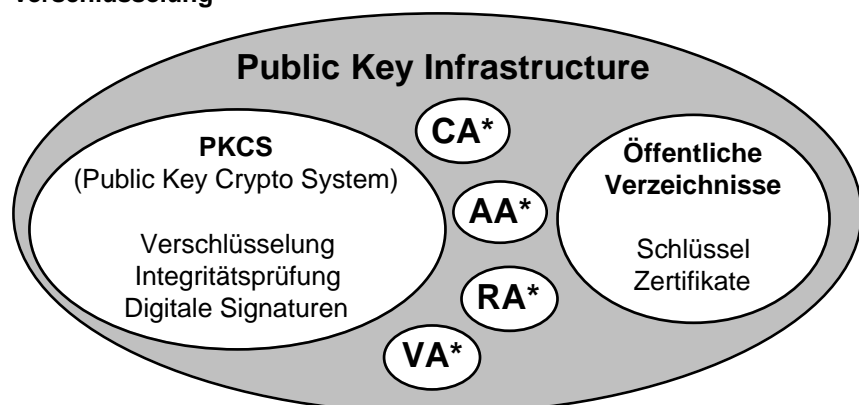
- Web-Server und interne Systeme, die die E-Business Applikationen unterstützen, sind aufgrund ihrer Verbindung zum Internet anfällig für Fehlfunktionen, Überlastung und gezielte Attacken (z.B. Hacker).
- Sowohl Kunden als auch Anbieter von E-Business Lösungen haben mangelndes Vertrauen in die Geheimhaltung und Authentizität von Transaktionen, die über das Internet durchgeführt werden (z.B. Kreditkartennummer).
- Private PCs und andere Endgeräte des Kunden stehen ausserhalb des Einfluss- und Kontrollbereichs eines Unternehmens und bieten meist nur unzureichende Sicherheit (z.B. Schutz gegen Computerviren).
- Der gesetzliche und regulative Rahmen bezüglich der Sicherheitsaspekte im E-Business ist immer noch nicht einheitlich und weit genug ausgebaut (z.B. US Exportrestriktionen).

Im Umfeld von E-Business spielen PKIs eine essentielle Rolle. Sie sind die Basis für das benötigte Vertrauen in die Technologie, Sicherheit, Vertraulichkeit und Authentizität der Transaktionen und Geschäftspartner. Ausserdem versprechen sich die Unternehmen von PKIs eine einheitliche und flexible Sicherheitsarchitektur bis hin zum Benutzer, die die Sicherheitsadministration (sowohl für Benutzer als auch für Anbieter und Administratoren) zentralisieren und damit erheblich vereinfachen soll.

Beispiele für erfolgreiche (d.h. gewinnbringende) Implementierungen von PKIs gibt es allerdings wenige. Dies liegt – wie bereits erwähnt – weniger an der technischen Machbarkeit, als vielmehr an der Komplexität der notwendigen organisatorischen Prozesse für Einführung und Betrieb einer PKI. Die Unternehmen sehen sich folgenden Fragen gegenübergestellt:

- Welche Applikationen sollen primär von der PKI unterstützt werden? Wie können diese integriert werden?
- Wie und wo werden die Schlüssel und Zertifikate veröffentlicht? Welche Informationen soll das Verzeichnis beinhalten? Wie können bestehende Verzeichnisse integriert werden?

### Eine PKI ist mehr als nur Verschlüsselung



\* C/A/R/VA: Certification/Administration/Registration/Validation Authority

- Wie können die Schlüssel und Zertifikate firmenfremder Mitarbeiter wie Geschäftspartner oder externer Berater sicher integriert werden? Unter welchen Voraussetzungen darf mit Partnern in fremden Ländern kommuniziert werden?
- Welche zusätzlichen Anforderungen stellt die Einführung einer PKI an den Benutzersupport respektive das Helpdesk (vergessene Passwörter, verlorene Smartcards, ungültige Zertifikate...)?
- Nach welchen Kriterien und von wem sollen verlorene Schlüssel zum Entschlüsseln und Prüfen digitaler Signaturen wiederhergestellt werden können?
- Welche Anforderungen stellt die Einführung einer PKI an die Benutzerregistrierung (Schlüsselgenerierung, Entzug von Zertifikaten, Initialisierung und Ausgabe von Smartcards, ...)?
- Wie und wo (intern oder durch externen Dienstleister) werden die Zertifikate ausgestellt und überprüft? Wie sehen die Zertifizierungs-Standards aus?
- Wie weit ist der Benutzer betroffen? Kann man die neuen Mechanismen und Prozeduren jedem Benutzer zumuten? Haben alle Benutzer die Kompetenz, das Konzept einer PKI zu verstehen und umzusetzen?

Da viele der Antworten zu den oben aufgeführten Fragen detaillierte (und damit teure) Untersuchungen und Abklärungen nach sich ziehen, scheuen sich die meisten Unternehmen noch, die Initiative zu ergreifen und beobachten weiterhin den Markt (Auffassung "leading edge = bleeding edge").

Unternehmen, die die vielversprechenden Möglichkeiten von E-Business nutzen wollen oder müssen, sollten ihre Strategien im Bereich PKI sorgfältig planen. Dazu gehört:

- Enge Einbindung und Verpflichtung des Top-Managements in die Projekte. Dazu gehören auch die Nicht-Informatikchefs.
- Grosszügiges Budgetieren der notwendigen Mittel wie interner und externer Mitarbeiter, Kosten für das Projekt, Soft- und Hardware. Dabei zeigt die Erfahrung, dass die vermeintlichen Standardaufgaben (Softwareverteilung, Dokumentation, Training, etc.) die meisten Ressourcen verschlingen, da sie oft nicht detailliert im Projektplan definiert sind.
- Abklären der rechtlichen Grundvoraussetzungen für den Einsatz und die Verteilung von Crypto-Systemen in multinationalen Unternehmen.
- Aneignen oder Einkaufen der notwendigen technischen und Management-Fähigkeiten.
- Definieren, Einführen und Betreiben der benötigten organisatorischen Prozesse (Benutzer-Registrierung, Helpdesk, CA, etc.)
- Prüfen, ob eine PKI intern entwickelt und betrieben oder ein Outsourcing Service herangezogen werden soll.
- Pilotieren von PKI-Technologien, Beratung und Dienstleistungen.

Die umfassende Einführung einer PKI stellt also immer noch eine grosse Herausforderung für die Unternehmen dar, besonders wenn es sich um grosse, internationale Konzerne handelt. Trotzdem ist dieser Schritt auf dem Weg zum erfolgreichen E-Business – zumindest nach heutigem Stand – ein Muss. Sicherheit und Vertrauen sind die wesentlichen Faktoren: Wenn sie

den Geschäftspartnern und Kunden nicht angeboten und transparent gemacht werden können, wird der Erfolg zwangsweise ausbleiben. In gleichem Masse sind sie aber auch der Schlüssel zum E-Business Erfolg, nämlich dann, wenn sie durch angemessene technische und organisatorische Vorkehrungen garantiert werden können.

*Frank Heinzmann,  
PricewaterhouseCoopers, Zürich*

## Infrastructure à clés publiques vers une nouvelle approche de la sécurité informatique: la confiance

L'engouement des entreprises pour les Intranets et les Extranets ne surprend plus personne: l'utilisation massive des technologies Internet par les entreprises s'explique par une grande facilité de mise en œuvre des applications, une économie considérable en comparaison aux autres techniques de communication (propriétaires de surcroît) et l'apport d'une réponse aux problèmes de l'hétérogénéité des systèmes.

Malheureusement, "sécurité du réseau" ne rime encore qu'avec "firewall", "anti-virus" et "mot de passe". Ces technologies de sécurité laissent pour compte certaines bases de la sécurité des systèmes d'information: *l'authentification* des correspondants, la *non répudiation* des transactions, *l'intégrité* et/ou la *confidentialité* des données échangées. En effet, sur un réseau Inter/Intra/ExtraNet la technologie TCP/IP s'appuie sur l'émission de trames en mode "non connecté" et "sans garantie", c'est à dire que, sans précaution de l'usager, les trames peuvent être altérées, perdues, interceptées ou modifiées.

Ces objectifs de sécurité peuvent pourtant être facilement atteints à l'aide des Infrastructures à clés publiques (PKI – Public Key Infrastructure). Concepts novateurs de ses quinze dernières années, les PKI ont pourtant longtemps semblé être

complexes à mettre en œuvre, en raison de l'absence de solutions facilement déployables et d'une législation sur le chiffrement très stricte en France. L'apparition d'offres "outsourcées" et "insourcées", la progressive libéralisation du chiffrement (loi sur les télécommunication de 1996, décrets de 1998 et 1999) font des PKI les solutions les plus attractives.

### Concepts

#### Confidentialité

Le concept des PKI se fonde sur les mécanismes de chiffrement à clés asymétriques. Sans rentrer dans les détails techniques, on peut définir, pour résumer, un protocole de chiffrement à clés asymétriques par l'utilisation de deux clés distinctes: pour chiffrer un message, on a besoin d'une clé P, pour déchiffrer un message, on a besoin d'une autre clé S. On obtient alors une *bi-clé*. Ce qui fait la force d'un tel mécanisme est le fait qu'on audez abersmatiquement choisi P et S de telle manière que:

- connaissant P, on ne puisse pas deviner S (et inversement)
- on puisse chiffrer de manière sûre en utilisant indifféremment P ou S.

Ainsi, si Bob veut envoyer à Alice un message *chiffré*, Alice devra *rendre publique* une de ses deux clés ( $P_A$  par exemple, qui devient la *clé publique*) tout en gardant confidentielle la clé associée ( $S_A$ , qui devient la *clé secrète*): Bob chiffrera alors le message à envoyer avec  $P_A$ . Le message ne pourra être déchiffrable qu'avec la clé  $S_A$  associée. La fonction de confidentialité est donc assurée.

#### Signature numérique

L'un des autres avantages des techniques de chiffrement à clés asymétriques est qu'il permet d'assurer des fonctions de signatures numériques. Comme pour la signature "physique" figurant au bas d'un chèque bancaire, la signature numérique apporte une preuve d'authentification et de non répudiation.

Ainsi, si Bob veut envoyer un message *signé* à Alice, il chiffrera son message à l'aide de sa *clé secrète*  $S_B$ . Puls enverra à Alice son message "en clair" accompagné du message chiffré<sup>1</sup>. Alice recevra donc deux messages: un clair et un chiffré. Pour vérifier que c'est bien Bob qui l'a envoyé, Alice déchiffrera le message chiffré à l'aide de la *clé publique* de Bob ( $P_B$ ): le message ainsi déchiffré devra être identique au message en clair.

Par rapport à la signature "physique", la signature numérique apporte un objectif de sécurité supplémentaire: l'intégrité des données. En effet, si le message clair est altéré ou modifié, il

<sup>1</sup> En pratique, pour des raisons d'efficacité, on calculera le condensat du message. Ce condensat sera chiffré, puis émis avec le message clair.

ne sera alors plus identique au message déchiffré.

### Certificats numériques et Autorités de Certification

On l'a vu, le chiffrement à clés asymétriques apporte dans l'échange de messages: authentification, non répudiation, confidentialité et intégrité. Ce principe s'applique très facilement lorsqu'il s'agit d'échanges entre deux personnes, mais lorsqu'on souhaite communiquer à plus grande échelle (au niveau d'une entreprise par exemple) survient le problème de la gestion des clés.

En effet, pour assurer ces objectifs de sécurité, les correspondants doivent publier leurs clés publiques (cf. plus haut). Dès lors, rien n'empêche un imposteur de se faire passer pour Bob et de publier sa clé publique: Alice croyant envoyer un message confidentiel à Bob, utilisera la clé publique de l'imposteur... C'est pour cette raison qu'interviennent les certificats numériques émis par des Autorités de Certification.

Lorsqu'un client paye avec un chèque bancaire chez un commerçant, ce dernier peut vérifier la signature sur le chèque en demandant une pièce d'identité, il s'assure ainsi que la personne qui est en face de lui est bien celle qui a signé le chèque. Il fait confiance à la pièce d'identité, car elle a été émise par une Autorité de Certification reconnue (l'Etat). Ainsi, de la même manière qu'une pièce d'identité associe un visage ou une signature physique à une personne, un certificat numérique associe une clé publique à une personne, un serveur,

une machine. On peut faire confiance au certificat numérique, s'il a été émis par une Autorité de Certification reconnue.

### Acteurs d'une PKI

Les certificats numériques sont émis de la même manière que les pièces d'identité: trois acteurs interviennent:

- l'Autorité Certifiante (AC) définit la politique de sécurité en énumérant les règles d'attribution et de gestion des certificats (pièces nécessaires à produire, conditions d'obtention etc.),
- l'Autorité d'Enregistrement (AE): se charge de vérifier que les conditions d'attribution du certificat sont remplies,
- l'Opérateur de Certification (OC): signe les demandes qui lui sont transmises par VAE.

Par exemple, dans le cas des cartes d'identité, l'Etat agit comme Autorité Certifiante, les mairies vérifient les pièces fournies en tant qu'Autorité d'Enregistrement, et enfin, les préfectures agissent en tant qu'Opérateur de Certification. Dans le contexte d'une entreprise, la Direction Générale peut être Autorité Certifiante, la Direction des Ressources Humaines peut tenir le rôle de l'Autorité d'Enregistrement, mais se pose le problème de l'Opérateur de Certification.

En effet, d'un point de vue technique, un certificat prend toute sa valeur dès qu'il a été signé par l'OC, c'est donc à cette étape que le niveau de sécurité doit être maximal. Dans l'entreprise, on peut imaginer l'OC comme étant un administrateur au sein de la

Direction Informatique, mais il faudra alors:

- que l'administrateur soit irréprochable (il est en effet en mesure de certifier la clé publique du PDG, donc rien ne l'empêche de créer lui-même une bi-clé et de certifier la clé publique créée comme étant celle du PDG),
- que l'ordinateur qui permet d'effectuer la certification soit dans un local extrêmement protégé,
- qu'il y ait des mécanismes et des procédures de sauvegarde, de secours etc.

Par ailleurs, les échanges électroniques étant de plus en plus ouverts, un certificat aura de la valeur s'il peut être reconnu en dehors de l'entreprise (cas typique de l'évolution d'un Intranet vers un Extranet).

Il s'agit là de la problématique d'une PKI "in-sourcée" où l'entreprise gère elle-même ses certificats, assumant elle-même la charge de la sécurité de son OC mais n'ayant pas de projet d'interopérabilité rapide avec des clients et/ou des partenaires par rapport à une PKI "out-sourcée". Dans ce cas, l'entreprise délègue la fonction d'OC à un tiers: ce dernier mutualise le coût lié à l'infrastructure nécessaire (locaux protégés, personnel habilité etc.), sert de *tiers de confiance* lors de transactions entre sociétés (comme lorsqu'on fait appel à un notaire quand on achète une maison), permet la reconnaissance mutuelle de certificats de plusieurs sociétés, et met à la disposition de ses clients son savoir faire et son expertise.

## Cycle de vie d'un certificat

Un certificat suit un "cycle de vie" défini en fonction de la politique de sécurité de l'entreprise, il peut se résumer en plusieurs étapes :

1. La *requête*: un utilisateur créé ou obtient une bi-clé et fait une demande de certificat pour sa clé publique.
2. La *validation*: en fonction des éléments fournis par l'utilisateur et conformément à la politique définie par l'AC, l'administrateur de l'AE valide ou rejette la requête de l'utilisateur.
3. La *certification*: l'OC reçoit la requête transmise et signée par l'AE et émet un certificat.
4. La *révocation*: si une clé privée associée à un certificat a été compromise ou si, par exemple, l'utilisateur a quitté ses fonctions, un certificat peut être révoqué par PAE.
5. L'*échéance*: pour des raisons de sécurité, les certificats ont une durée de vie limitée, généralement d'un an. Passé ce délai, le certificat est échu et ne peut plus être utilisé.
6. Le *renouvellement*: un certificat peut être ré-émis par un mécanisme de renouvellement avant ou après son échéance.

## Fonctionnalités

Une PKI est donc un ensemble de procédures, de technologies et d'expertise ayant pour but de gérer le cycle de vie des certificats. L'entreprise doit donc disposer de plusieurs fonctionnalités, quelques unes sont énumérées ci-après :

■ *Autorité de Certification*: l'entreprise doit paramétrer les champs que

l'utilisateur aura à saisir à des fins d'autentification (même si ces paramètres ne figurent pas dans le certificat). La fonctionnalité d'AC permet de définir la politique de sécurité (modalités de retrait des certificats, modalités des demandes).

■ *Autorité d'Enregistrement*: l'administrateur de l'AE a le pouvoir de consulter et traiter les requêtes de certificats, révoquer des certificats et ainsi gérer les listes de révocation (cf plus bas), mettre à jour l'annuaire d'entreprise.

■ *Gestion des listes de révocation*: lorsqu'un certificat a été révoqué par l'AE, il doit être ajouté à une liste de révocation de certificats, cette liste est téléchargée régulièrement où à la demande sur les serveurs de l'entreprise afin de se prémunir de toute utilisation de certificats révoqués.

■ *Annuaire*: pour plus de commodité d'utilisation, le répertoire des certificats des utilisateurs doit pouvoir être intégré à un annuaire d'entreprise.

■ *Recouvrement et gestion des clés*: permet de résoudre la problématique de la perte des clés. En effet, si un utilisateur perd sa clé privée (lui permettant de déchiffrer les messages qu'il a reçus, par exemple), il ne pourra plus accéder à ses messages. La fonctionnalité de gestion des clés, implémentée et gérée de manière très stricte permet de sauvegarder les clés privées.

## Conclusion

Avec les actuelles discussions au niveau de l'Union Européenne pour une reconnaissance juridique des signatures électroniques (voir aussi l'annexe 10 du dernier "Rapport Lorentz", recommandant la recon-

naissance de la valeur probante de la signature électronique et l'incitation à l'utilisation d'intermédiaires de confiance et d'autorités de certification), les PKI fondent sans conteste les bases des nouvelles architectures de sécurité que ce soit pour les besoins internes aux entreprises (Intranet et Extranet) mais aussi pour les applications plus ouvertes d'échange de données (commerce électronique, banque à domicile, téléprocédures, etc.).

Frédéric Huynh,  
 Certplus

# Freigabe- und Übergabeverfahren in heterogenen Umgebungen

## Einleitung

In diesem Artikel wird ein Überblick über Freigabe- und Übernahmeverfahren von Programmen, definierenden Daten sowie Berechtigungsdaten in unterschiedlichen Systemarchitekturen gegeben und einige Risiken angeführt. Ein Anspruch auf Vollständigkeit wird nicht erhoben; vielmehr kann nur ein kleiner Ausschnitt und einige Gedankenanstöße über Freigabe- und Übernahmeverfahren gegeben werden.

## Gesetzliche Anforderungen

In Österreichischen Gesetzen findet sich derzeit keine Passage, die ordnungsgemäße Freigabe- und Übergabeverfahren explizit fordert. Macht man sich jedoch Gedanken, welche Auswirkungen bestimmte Gesetze (z.B. das Handelsgesetzbuch oder die Abgabenordnung) auf die Informationstechnologie (IT) haben, stösst man relativ rasch auf das Thema der "Programmfreigaben" und "-übernahmen".

Spätestens wenn man die aktuellen – und immer wieder gerne angeführten – Sollvorschriften

- der "Grundsätze ordnungsmässiger DV-gestützter Buchführungssysteme (GoBS)",

- der definierten Anforderungen des "Fachausschusses für moderne Abrechnungssysteme" (FAMA) 1/87 in der Fassung von 1993 (Herausgegeben

von Institute für Wirtschaftsprüfer in Deutschland eV) oder

- der 1999 von der Kammer der Wirtschaftstreuhänder in Österreich herausgegebene "Kommentierten Fassung des Fachgutachten 'Die Ordnungsmässigkeit von EDV-Buchführungen'"

heranzieht, sind die Anforderungen ohne definierte, nachvollziehbare Verfahren nicht einzuhalten.

Rein theoretisch kann innerhalb der gesetzlichen Nachweispflicht von bestimmten Verarbeitungen (z.B. von der Buchhaltung und den Buchhaltungsanschlüssen) vom Gesetzgeber der komplette Verarbeitungsnachweis verlangt werden. 100%-ig kann dies natürlich nur dann erbracht werden, wenn die gesamte Hardware, Betriebssystemsoftware, betriebssystemnahe Software und die Anwendungssoftware lückenlos vorhanden sind. Dies stösst sicher an die Grenzen eines jeden Unternehmens. Z.B. ist es nahezu unmöglich ein SAP R/3-System, wie es vor ca. drei Jahren z.B. am 29. Oktober 1996 im Einsatz war, inklusive der damals geltenden Dokumentation, so zu rekonstruieren, dass alle damaligen Anwendungen mit dem gleichen Ergebnis wie einst durchgeführt werden können.

Weiter muss innerhalb der gesetzlichen Aufbewahrungsfrist (z.B. HGB 7 Jahre, AO 10 Jahre) jederzeit zu jedem Programm die zum entspre-

chendem Zeitpunkt gültige Dokumentation nachweisbar sein. Dies wiederum bedeutet, dass die Dokumentation mit dem Programm eine "untrennbare Einheit" bildet und sowohl das Programm als auch die Dokumentation den Aufbewahrungsfristen und somit einer Versionsführung unterliegen. Hinsichtlich der Aufbewahrungsfristen – zumindest ab wann diese zu laufen beginnen – gibt es in Österreich unterschiedliche Meinungen:

- Eine Meinung geht davon aus, dass die Aufbewahrungsfrist ab dem Einsatzzeitpunkt des Programmes beginnt. Dies würde jedoch bedeuten, dass wenn ein Programm 10 Jahre im Einsatz ist und die Aufbewahrungsfrist nur sieben Jahre beträgt, nach sieben Jahren keine Dokumentation sowie kein Nachweis des Einsatzzeitpunktes gegeben ist.

- Im Gegensatz dazu geht eine zweite Meinung davon aus, dass die Aufbewahrungsfrist erst ab dem Zeitpunkt des letzten Einsatzes eines Programmes (= letzte Durchführung) beginnt. Hier entsteht zwar ein grösserer organisatorischer und technischer Aufwand, dafür sind gesetzliche Anforderungen auf jeden Fall eingehalten.

## Allgemeine Dokumentationsanforderungen

Die GoB (Grundsätze ordnungsmässiger Buchführung) definieren zwar keine spezielle Dokumentation hinsichtlich Freigabe- und Übernahmeverfahren, jedoch verlangen sie eine "Verfahrensdokumentation". Zur Gewährleistung der Nachvollziehbarkeit muss diese Auskunft zu folgenden Bereichen geben:

- Art und Inhalt des Freigabeverfahrens für neue oder geänderte Programme
- die Aufgabenstellung (u.a. auch einen Antrag für Programmänderungen durch die Fachabteilung)
- den Datensatzaufbau
- Verarbeitungsregeln einschliesslich Kontrolle und Abstimmverfahren
- Fehlerbehandlung
- Datensicherung
- etc.

In der Praxis kristallisierten sich (im Grossrechnerbereich) einige grundlegende Dokumentationsanforderungen heraus:

- Schriftliche Freigabeunterlagen (schriftlich: mittels eigenhändiger bzw. digitaler fälschungssicherer Unterschrift)
- Vorhandensein einer System- und Programmdokumentation. Diese sollte für eine Anwendung zumindest
  - die Aufgabenstellung
  - Verarbeitungsregeln
  - Fehlerbehebung
  - Datensicherung (Aufbewahrungsdauer,...)
  - Sicherung/Nachweis der ordnungsgemässen Programmanwendung (z.B. Umwandlungslisten)
  - Testunterlagen
 enthalten.

Anzumerken ist jedoch, dass aufgrund des technologischen Fortschrittes sich auch die Art der Dokumentation ändern kann. Beispiele dafür sind der Einsatz von Case-Tools, Workflow-Definitions-Tools, etc. Es muss jedoch sichergestellt werden, dass auch in einigen Jahren, alte Dokumentationen in angemessener Zeit zur Verfügung stehen.

- Versionsführung der eingesetzten Software. Der Einsatzzeitraum jeder Programmversion ist nachzuweisen. Dies erfolgt am einfachsten durch
  - eine automatische Versionsführung
  - automatischer Vergabe und Hochzählen einer Versionsnummer mit jeder Änderung des Programms
  - Dokumentation der Versionsnummer im Vorblatt oder Kopfzeilen jeder vom Programm erzeugten Liste
  - Ausgabe einer Meldung im SYS-LOG mit Programmnamen und Versionsnummer

Weiter sollte bei der Übergabe darauf geachtet werden, dass

- laut Methodenhandbuch programmiert wurde
- die Namenskonvention eingehalten wurde
- die Dokumentation fertiggestellt ist (kein Einsatz ohne Dokumentation!)

Die Prüfung der Einhaltung dieser Forderungen sollte entweder durch die Qualitätssicherung oder durch ein Einsatz-/Freigabereview durch die betroffenen Bereiche erfolgen.

### Grossrechnerumgebungen/ Rückblick

In herkömmlichen Grossrechnersystemen (z.B. unter MVS) etablierten sich im Laufe der letzten 30 Jahre mehr oder weniger sichere und ordnungsgemässe Freigabe- und Übergabeverfahren. Eine Trennung von Entwicklung und Produktion ist bei diesen Systemen üblich und wird eigentlich nicht mehr in Frage gestellt. Weiter wurden diverse Verfahren und Methoden für die Entwicklung von Software unter Einbeziehung einer Qualitäts-

sicherung entworfen. Im Rahmen des Qualitätssicherungsprozesses wurde sichergestellt, dass die vom Unternehmen und externen Rahmenbedingungen definierten Vorgaben eingehalten wurden. Diese Vorgaben umfassen im Normalfall unter anderem:

- definierte Testverfahren (Modultests, Integrationstests, Anwendertests, ...)
- schriftliche Freigaben seitens der Anwender
- Prozeduren für die automatisierte Übernahme von einer Test- in die Produktionsumgebung inklusive neuerlicher Compilierung des Programms und Linken aller abhängigen Programme
- (automatische) Versionsführung (zum Beispiel mittels SCLM oder Panvalet)

### Beispiel eines Freigabeverfahrens

Jeder Freigabeantrag ist nachvollziehbar zu gestalten. D.h. Freigaben haben schriftlich oder elektronisch zu erfolgen. Es muss dabei ersichtlich sein, wann und wer die (elektronische) Freigabe erteilt. Freigabeanträge sind Teil der Dokumentation und aufbewahrungspflichtig.

Um jedoch tatsächlich neue/geänderte Programme in Produktion zu übernehmen, ist neben einem ordnungsgemässen Freigabeverfahren eine technisch bzw. organisatorisch gelöste Produktionsübernahme erforderlich.

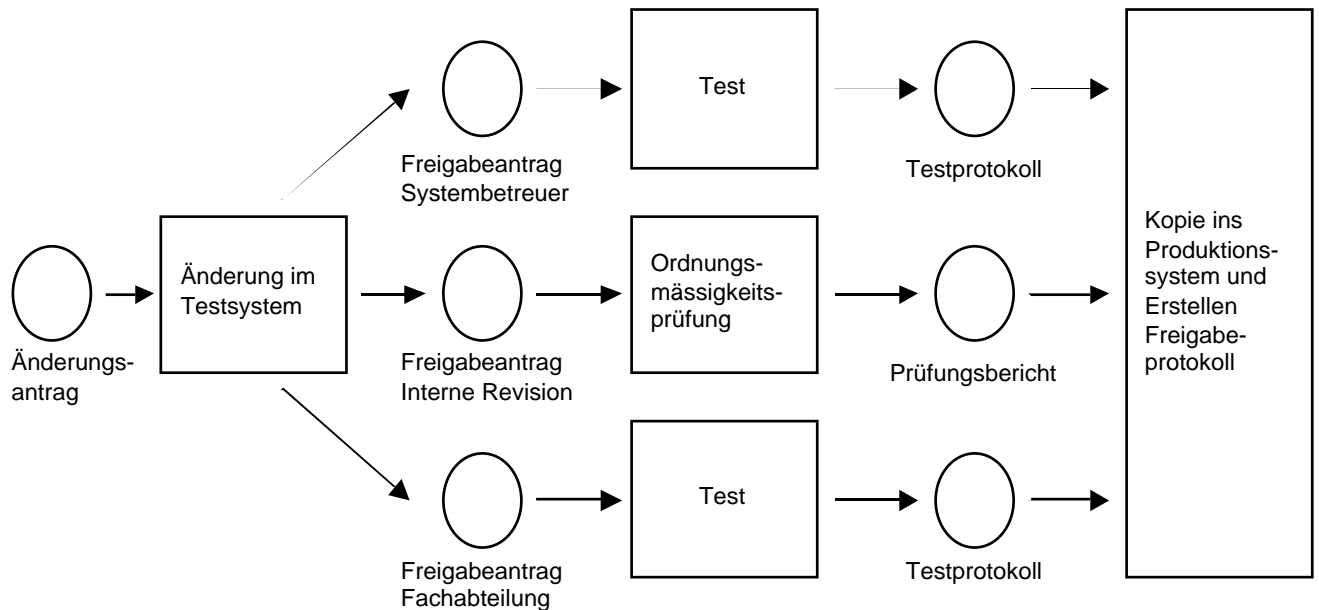


Abbildung 1: Beispiel eines Freigabeverfahrens, Quelle: interne Revision 1/97

### Beispiele und Theorie von Übernahmeverfahren bei Grossrechnersystemen

*Beispiel 1:* Ein einfaches jedoch relativ risikobehaftetes Übernahmeverfahren

Diese Art der Übernahme führt im Normalfall über kurz oder lang zu Inkonsistenzen zwischen Entwicklung und Produktion, da vor allen Dingen bei Modul- bzw. Includeänderungen häufig nicht alle in Produktion befindlichen und betroffenen Programme neu gelinkt werden. Die Folge davon ist, dass sich von einem Modul bzw. Include unterschiedliche Object- bzw. Phasencodes gleichzeitig in Produktion befinden, was wiederum spätestens mittelfristig zu Produktionsproblemen führt (z.B. Abstürze).

Es existieren Werkzeuge (z.B. Librarian), die eine Übereinstimmung Sourcecode und Objectcode sicherstellen. Die Nachvollziehbarkeit zwi-

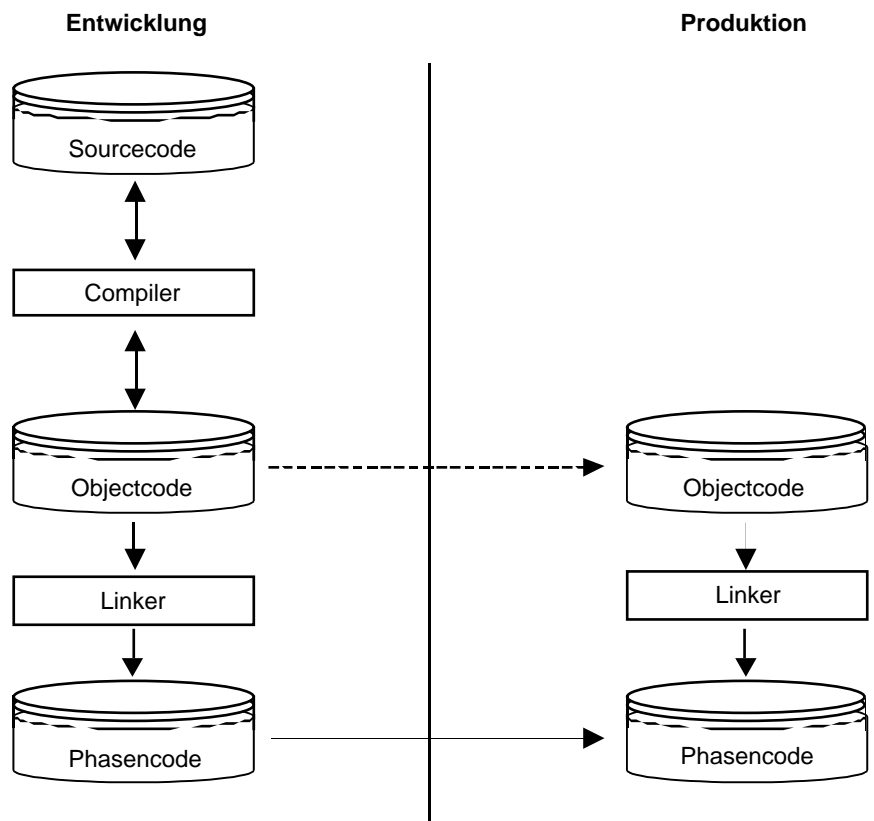


Abbildung 2: Beispiel 1: Ein Einfaches jedoch relativ risikobehaftetes Übernahmeverfahren

sehen Source- und Objectcodeversion kann dadurch gewährleistet werden.

Die Versionsverwaltung findet – wenn überhaupt – hauptsächlich auf der Entwicklungsseite statt.

Beispiel 2 eines Übernahmeverfahrens:

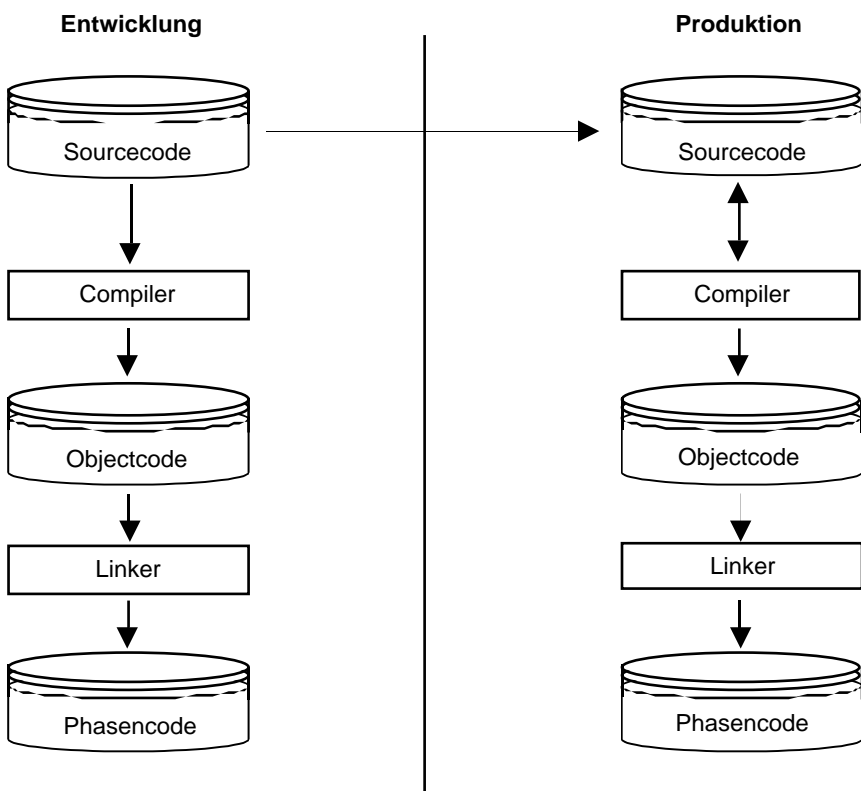


Abbildung 3: Beispiel 2 eines Übernahmeverfahrens

Bei dieser organisatorischen/technischen Lösung wird der Sourcecode (Hauptprogramm, Unterprogramm, Includes,...) in die Produktion kopiert, dort neuerlich compiliert und gelinked. Parallel dazu wird im Normalfall eine eigene Versionsverwaltung des Sourcecodes in der Produktion implementiert. Die Übergabe in die Produktion kann natürlich auch bei dieser Lösung auf unterschiedlichster Weise erfolgen. Im einfachsten Fall wird der Sourcecode manuell kopiert. In grös-

seren Organisationen ist es heutzutage durchaus üblich, dass Übergaben mittels technischer Prozeduren (z.B. mittels Rexx-Prozeduren) erfolgen. Diese Prozeduren ermöglichen automatische Protokolle, wie zum Beispiel Aufzeichnungen, welcher Entwickler wann welche (Programm-)Teile in Produktion übergeben hat oder Auf-

zeichnung der Änderungen zur "Vorversion".

Durch ausgeklügelte Linkmechanismen kann sichergestellt werden, dass alle betroffenen Programme neu gelinked werden und dieselbe Produktionsversion besitzen. Dies bringt u.a. Vorteile bei Änderungen von Unterprogrammen, die in mehreren Hauptprogrammen verwendet werden. Aufwendigere – und heutzutage durchaus übliche Verfahren – integrieren

in den technischen Übernahmeprozess bestimmte Teile des Freigabeverfahrens, das heisst ein Workflow für das Freigabeverfahren ist in den technischen Prozeduren implementiert. In diesen Fällen wird die Programmübernahme in die Produktion erst dann durchgeführt, wenn Mindestkriterien hinsichtlich der Freigabe (z.B. elektronische Freigabe der Fachabteilung, der Qualitätssicherung und des Rechenzentrums) erfüllt sind.

Um das System nicht unnötig zu belasten und zu destabilisieren, werden Übergaben nur zu bestimmten Zeitpunkten – im sogenannten Wartungsfenster – für die Produktion aktiviert; zum Beispiel täglich um 20.00 Uhr oder wöchentlich am Mittwoch um 21.00 Uhr. Andererseits muss es jedoch jederzeit möglich sein, sogenannte "Emergency Changes" über die definierten Prozeduren durchzuführen. Dies ist zum Beispiel dann der Fall, wenn es zu Programmabstürzen und Dumps kommt.

Beispiel 3 eines Übernahmeverfahrens:

Die Abbildung 4 verdeutlicht das Prinzip eines mehrstufigen Freigabe- und Übernahmeverfahrens. (Anmerkung: Aufgrund der Übersichtlichkeit wurde auf die Darstellung der Link-Phase verzichtet). Bei diesem Konzept werden "Programmänderungen" nur in der Entwicklung durchgeführt. Bereits in der Testumgebung greifen strengere Zugriffsmechanismen, das heisst, Entwickler besitzen z.B. keine Änderungsberechtigungen für Daten und Programme. Die Testumgebung dient vorrangig für Integrationstests und Tests durch die Fachabteilung. Bei diesem Konzept kommt es – wird es

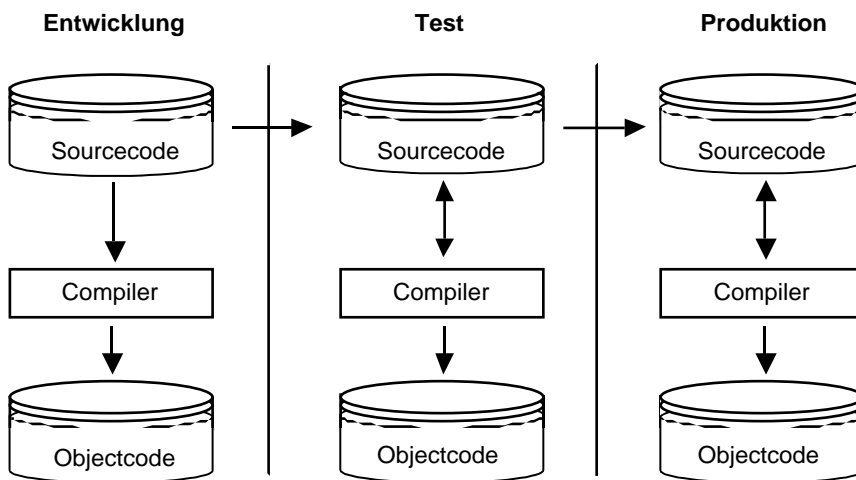


Abbildung 4: Beispiel 3 eines Übernahmeverfahrens, R. Bron

konsequent umgesetzt – bereits zwischen Entwicklung und Test zu einem ersten Übergabeverfahren wie bei der Abbildung 3 beschrieben wurde. Diese erste Übergabe unterliegt im Normalfall nicht so strengen Kriterien wie die zweite Übergabe vom Testsystem in die Produktion.

### “Neue” Anforderungen bei Nicht-Grossrechner-systemen?

Alle vorhin genannten Konzepte betreffen die bisherige sogenannte “Gross-EDV”. Es stellt sich natürlich die Frage, ob diese mehr oder weniger etablierten Konzepte auf heterogene Systeme übertragen werden können.

Betrachtet man heterogene Systeme, sieht man sich einer Vielzahl unterschiedlicher Anwendungssysteme, Entwicklungen, Methoden, Freigabe- und Übernahmeverfahren gegenüber. Unter anderem können folgende Systeme dabei betroffen sein:

- Standardsoftware (Host- und oder PC-seitig)

- eigenentwickelte “Host-Software” (z.B. für die Betriebssysteme MVS, BS2000, Unix)
- eigenentwickelte PC-Software inkl. Software-Verteilung (“Roll Out”)
- Client-/Server-Systeme (in den unterschiedlichsten Ausprägungen). Dies betrifft sowohl Standardsoftware, reine Informationssysteme als auch Anwendungen.
- Inter- und Intranet-Anwendungen

Sicherlich ist es wünschenswert, alle diese Systeme einem einheitlichen Abnahme- und Übernahmeverfahren zu unterziehen. Dies wird leider häufig aufgrund der unterschiedlichen technischen Anforderungen in den wenigsten Fällen gelingen. Es gibt jedoch Tools für das Change-Management (z.B. von TIVOLI), die – wenn sie entsprechend konfiguriert sind – die Ordnungsmässigkeit (Nachvollziehbarkeit) von Softwareinstallationen gewährleisten können.

Sieht man sich schon auf technischer Seite bei heterogenen Systemen möglicherweise einer Vielzahl von technischen Übernahmeverfahren gegenüber, sollten zumindest die organisa-

torischen Abnahmeverfahren (Freigeben) einheitlich gestaltet werden.

### PC-Anwendungen

Ohne weitere Sicherheitsmassnahmen ist ein PC ein offenes System. D.h. Änderungen können jederzeit nicht nachvollziehbar vorgenommen werden. Je nach Einsatzzweck sind daher geeignete Sicherheitsmechanismen (z.B. gesperrte Verzeichnisse) erforderlich. Möchte man den Benutzer nicht ganz vergrämen (schliesslich muss er mit dem PC noch arbeiten), sind organisatorische Massnahmen, um eine ordnungsgemässe DV zu gewährleisten notwendig. Ein Beispiel dafür sind Benutzerrichtlinien, die die eigenmächtige Installation von Software verbieten.

Ebenso hat die Art der Nutzung (Stand-alone, im Netzwerk,...) Einfluss auf das Übernahmeverfahren. Kann bei einem Stand-alone-Gerät eine Software nur manuell vor Ort installiert werden und das Übernahmeverfahren nur schriftlich festgehalten werden, gibt es in einer Lan-Umgebung durchaus andere Möglichkeiten.

In einer Lan-Umgebung ist es durchaus üblich, Softwareverteilungen mittels bestimmter Werkzeuge (z.B.: SMS bei Windows NT, Tivoli) durchzuführen (Stichwort: Change-Management). Durch mitloggen wird zumindest gewährleistet, dass festgestellt werden kann, auf welchem PC wann welche Software(-version) installiert wurde. Erfolgt das Deinstallieren nicht ebenfalls über Tools, die mitloggen bzw. werden Deinstallationen nicht schriftlich festgehalten, ist der Nachweis des Einsatzzeitraumes

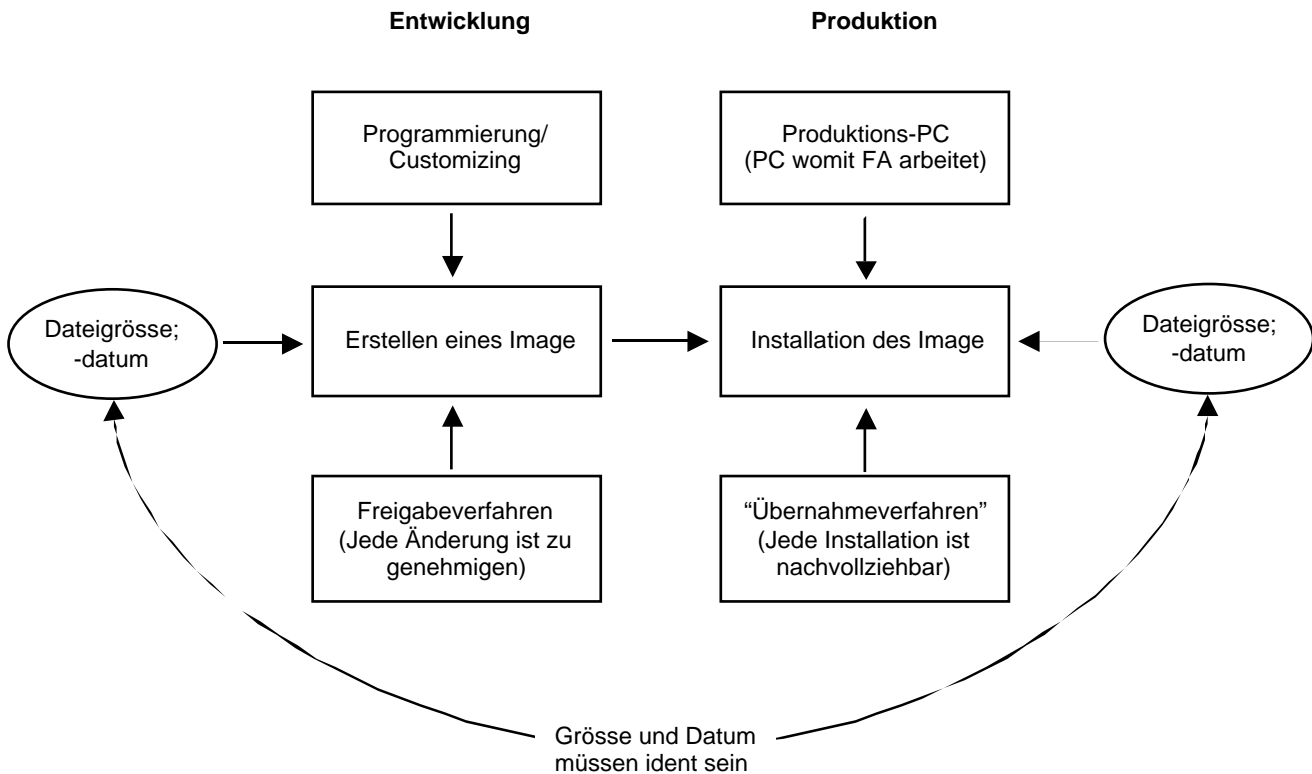


Abbildung 5: Schematische Darstellung eines Freigabe- und Übernahmeverfahrens im PC-Bereich

kaum möglich. Hierbei ist jedoch zu bedenken, dass sich der Nachweis des Einsatzzeitraumes auch alleine durch die einzelne Log-Einträge einer Installation ergeben kann, wenn z.B. neue Softwareversionen über die alte Version kopiert und dies mitgelogged wird. Festzuhalten ist, dass natürlich vor einer Softwareverteilung bereits ein Freigabe- und Übernahmeverfahren (für die Verteilung!) erfolgen muss. Häufig wird dabei auf Dokumentationsanfordernisse vergessen.

Einer der Schwachpunkte bei Change-Management-Systemen ist meistens die im Rahmen der Installation festgelegte Aufbewahrungsdauer der Log-Einträge, den diese beträgt häufig nur einigen Wochen bzw. Monate und werden danach gelöscht. Hierbei können eventuell notwendige gesetzliche Aufbewahrungsfristen z.B. zum Nachweis des "Einsatzzeitraumes" bzw.

vertraglich festgelegte Pflichten (Stichwort: Softwarelizenzen) verletzt werden bzw. vom Unternehmen nicht nachgewiesen werden.

Bei PC-Entwicklungen liegt meist die Führung einer Versionsverwaltung in Händen der Programmierer. Verglichen mit Grossrechnersystemen sieht man sich im Normalfall einem Übernahmeverfahren wie in Abbildung 1 dargestellt gegenüber. Weiter werden bei PC-Programmen in den seltensten Fällen alleine EXE-Files übergeben, sondern häufig sogenannte DLLs, Ini-Files etc. U.a. aus diesem Grunde etablierte sich das sogenannte "IMAGE-Verfahren" (Abbildung 5). Hierbei wird eine Anwendung inklusive aller DLLs, Steuerparameter, Ini-Dateien, etc. zu einem sogenannten Image zusammengefasst. Nach einer erfolgten Freigabe des neuen Image (wobei es sich empfiehlt, dieses auf einem nicht

manipulierbaren Datenträger z.B. CD-Rom zu speichern und zu archivieren), kann das Image manuell oder automatisiert durch Change-Management-Tools verteilt werden. Durch einen Vergleich der Dateigrößen und der Speicherdatei kann geprüft werden, ob sich auf den Produktionsmaschinen genau die genehmigten oder doch veränderte Dateien befinden. Es gibt jedoch auch Möglichkeiten, nach einer erfolgten Manipulation die Dateigröße und das Speicherdatum dem ursprünglichen anzupassen. Eine derartige Manipulation würde nur durch einen Vergleich der Dateinhalte auffallen.

## Client-/Server-Systeme

Client-/Server-Systeme stellen eine besondere Herausforderung hinsichtlich Change-Management dar. Der

Grund dafür ist, dass unterschiedliche Systeme bei einem Versionswechsel gleichzeitig betroffen sind. Dies können z.B. Lan-PCs und der Lan-Server sein, aber ebenso können gleichzeitig Lan-PCs, Lan-Server, ein Grossrechner (z.B. mit MVS als zentraler Datenbankserver) und eine Unix-Maschine mit SAP-R3 (für die Verbuchung) betroffen sein.

Hinsichtlich Übernahmen hat man von der technischen Seite betrachtet alle Vor- und Nachteile, die die jeweilige Plattform bietet, jedoch mit der Komplexität, dass ein System nur dann läuft, wenn alle Übernahmen zeitgleich aktiviert werden.

Dies hat zur Folge, dass Änderungen nur zu genau definierten Zeitpunkten (zu sogenannten Wartungsfenstern) durchgeführt werden sollten, um das System nicht unnötig der Gefahr von Inkonsistenzen und Betriebsunterbrechungen auszusetzen.

Ähnlich wie bei PC-basierten Anwendungen hat man auch hier im Normalfall mit Versionsführungen Probleme, da meist eine Anwendung nur funktioniert, wenn die entsprechende Kommunikationssoftware bzw. Middleware installiert ist. Dies würde wiederum zu der Forderung, diese Softwareteile inklusive der Einstellungsparameter ebenfalls zu versionieren, führen... Es stellt sich hier jedoch die Frage der Verhältnismässigkeit.

### **Inter- und Intranet-Anwendungen (WWW)**

In einer immer schneller sich verändernden Umwelt werden Internetan-

wendungen bei den meisten Firmen zum "Must". Andernfalls besteht bei vielen Unternehmen die Gefahr, dass sie sowohl technologisch als auch strategisch und dadurch mittelfristig auch wahrscheinlich umsatz- und gewinnmässig ins Hintertreffen gelangen.

Wenngleich heutzutage bei den wenigsten Internetanwendungen HGB oder AO-Vorschriften angewandt werden können, sollten auch für diese Anwendungen die GoDV gelten. Spätestens dann, wenn direkt über das Internet verkauft wird, oder wenn Internet-Technologie für Interne Front-End-Aufbereitung genutzt wird, sind Freigabe- und Übernahmeverfahren erforderlich. Auch in diesem Bereich müssen sich zumeist erst (firmeninterne) Standards, wie sie im Grossrechnerbereich üblich sind, etablieren. Es ergeben sich daher hinsichtlich Übernahmen ähnliche Problematiken wie bei PC-Anwendungen.

Häufig – z.B. bei E-Commerce-Anwendungen – entstehen idente Problematiken wie im Bereich Client/Server. Genau genommen sind dies Client-/Server-Anwendungen, wobei die Client- und Server-Seite durch das Internet getrennt sind. Im Normalfall übernimmt ein Browser auf der Client-Seite die Präsentation, d.h. zumeist wird der Internet-Dienst World Wide Web (WWW) für dies Art der Applikationen genutzt.

Auch "firmeninterne" Anwendungen nutzen häufig das Internet als Kommunikationsschiene. Ein Beispiel dafür wäre ein Aussendienstmitarbeiter, der Daten von seinem Notebook an seine Firma über das Internet in einer gesicherten Virtuell-Private-Network-Umgebung (VPN) übermittelt und

Programm- bzw. Datenupdates empfängt. In diesem Fall wird die Client-Seite durch ein Notebook, auf dem unterschiedlichste Technologien eingesetzt werden können, repräsentiert.

### **Definierende Daten/Berechtigungssysteme**

"Definierende Daten" sind Daten, die in Datenbanken oder Dateien hinterlegt sind und den Programmablauf, und/oder die Ergebnisse beeinflussen. Beispiele dafür wären Workflow-Daten, Steuerparameter, Daten für Prämienerrechnungen und Produktberechnungen,...

Heutzutage werden – um die Flexibilität zu gewähren – viele Anwendungssysteme mit definierenden Daten eingesetzt. Eines der bekanntesten Programmpakete, das mit definierenden Daten arbeitet, ist SAP R/3. "Definierende Daten" werden meist im Rahmen des sogenannten "Customizing" festgelegt. Jede Änderung dieser Daten sollte in einer Testumgebung erfolgen und einem ausführlichem Funktionstest unterzogen werden, um festzustellen, dass die gewünschten Ergebnisse – und nur diese – durch die Änderung eintreten.

Hinsichtlich Standardsoftware und definierender Daten ist anzumerken, dass sobald Standardpakete den eigenen Bedürfnissen angepasst werden (auch wenn dies "nur" durch "Definierende Daten" erfolgt), die Anforderungen an die traditionelle Entwicklung zu erfüllen sind, da durchgeführte Modifikationen und Erweiterungen als Softwareentwicklung anzusehen sind.

"Definierende Daten" haben massgeblichen Einfluss auf die ordnungsge-

müsse Programmanwendung. Es kann daher abgeleitet werden, dass sie denselben Ordnungsmässigkeitskriterien (Nachvollziehbarkeit, Dokumentation,...) wie Programme unterliegen. Dies bedeutet, dass auch für diese “Definierenden Daten” ordnungsgemässe Freigabe- und Übergabeverfahren zu entwickeln sind. Z.B. empfiehlt SAP bei R/3 ein zweistufiges Übergabeverfahren auch für definierende Daten (Übergabe von der Entwicklung in die sogenannte Integrationsumgebung und von dort in die Produktion).

Ein Beispiel für “Definierende Daten”, die einem Freigabe- und Übergabeverfahren unterliegen sollten, sind Produktdefinitionen. Werden neue Produkte definiert, indem “einfach” Werte in Datenbanktabellen hinzugefügt werden, ist dieses zuerst in einer Testumgebung zu testen und danach ordnungsgemäss in Produktion zu übergeben.

Ein weiteres Beispiel für “Definierende Daten”, das jedoch nicht mehr ganz so klar ist, ist z.B. die Änderung des Zinssatzes für Kreditberechnungen in einer Tabelle. Auch hier muss nachvollziehbar sein, wer dies wann durchführte und ab wann dieser Zinssatz gilt ebenso wie der Zeitraum, von wann bis wann der alte Zinssatz gültig war (u.a. zwecks Berechnung!). In diesem Fall kann die Ordnungsmässigkeit, wenn bestimmte Randbedingungen eingehalten werden, auch bei einer direkten Änderung in der Produktion gewährleistet werden. Dies ist auf jeden Fall dann gewährleistet, wenn die Änderung einem nachvollziehbaren Vier-Augen-Prinzip unterliegt und die oben geforderten Kriterien in der Tabelle oder in einem Log festgehalten werden.

Anzumerken ist, dass auf “Definierende Daten” Direktänderungszugriffe (z.B. mittels SQL), wenn diese nicht eindeutig nachvollziehbar sind, nicht erfolgen dürfen.

Ähnliches wie für “Definierende Daten” kann für Berechtigungen festgestellt werden. Immer mehr Anforderungen (Innerbetrieblich als auch extern – z.B. kann dies beim DSGVO2000 hinsichtlich personenbezogener Daten abgeleitet werden) verlangen eine Nachvollziehbarkeit wer wann welche Berechtigungen hatte. Hat man rollenbasierte Berechtigungssysteme im Einsatz, sind – um eine ordnungsgemässe DV zu gewährleisten – Rollendefinition in einem Testsystem zu erstellen und auszutesten. Um sicherzustellen, dass genau diese Definitionen in die Produktion übernommen werden und keine anderen, sind nach Ansicht des Autors ebenso Freigabe- und Übernahmeverfahren erforderlich.

## Schlussbemerkung

Bei heterogenen Systemen bestehen dieselben Anforderungen hinsichtlich Freigabe- und Übernahmeverfahren wie in Grossrechnersystemen, wenn gleich die organisatorisch/technische Umsetzung anders erfolgt. Da jede Systemplattform und jede eingesetzte betriebssystemnahe Software (z.B. Softwareverteilungstools) – ebenso wie die jeweilige Firmenkultur – das Verfahren beeinflussen, sind Freigabe- und Übernahmeverfahren in jedem Fall explizit zu bewerten. Insbesondere dann, wenn der Sicherheitsaspekt mitbetrachtet wird.

## Abkürzungen

AO	Abgabenordnung
DLL	Dynamic Link Library
DSG	Datenschutzgesetz
GoDV	Grundsätze ordnungsmässiger Datenverarbeitung
HGB	Handelsgesetzbuch
IT	Informationstechnologie
SQL	Structured Query Language
WWW	World Wide Web

## Literaturverzeichnis

- Grundsätze ordnungsgemässer Buchführung bei computergestützten Verfahren und deren Prüfung, Fachausschuss für moderne Abrechnungssysteme, Stellungnahme (FAMA 1/1987) in der Fassung von 1987, Institut der Wirtschaftsprüfer in Deutschland eV
- Kommentierten Fassung des Fachgutachten “Die Ordnungsmässigkeit von EDV-Buchführungen”, Kammer der Wirtschaftstreuhänder in Österreich (1999)
- Die Ordnungsmässigkeit der Buchführung beim Einsatz von mittelgrossen und grossen EDV-Systemen, Ing. Mag. Dr. Michael Schirmbrand (1997)

*Bernd Schütter, CISA,  
 Generali Holding Vienna AG,  
 IT-Audit*