Entwicklungen in den Informations- und Kommunikationstechnologien

Herausgeber:
Friedrich-L. Holl

**Band 3**

# Studie zu Erfolgskriterien für Identifizierungs-, Authentifizierungs- und Signaturverfahren auf Basis asymmetrischer kryptographischer Verfahren (EKIAS)

**Im Auftrag des**

Bundesministriums für Bildung und Forschung

Bundesministerium für Bildung und Forschung

**Beauftragter:**

Fachhochschule Brandenburg
TeleTrusT e.V.


**Autoren:**

Anja Beyer
Sophie Hellmann
Malte Hesse
Friedrich-L. Holl
Peter Morcinek
Sachar Paulus
Helmut Reimer

**Unter Mitarbeit von :**

Markus Dahms
Karsten Kausmann
Simone Friedrich-Meier
Jens Ziegler

Entwicklungen in den
Informations- und
Kommunikationstechnologien

Herausgeber:
Friedrich-L. Holl

## Band 3

# Studie zu Erfolgskriterien für Identifizierungs-, Authentifizierungs- und Signaturverfahren auf Basis asymmetrischer kryptographischer Verfahren (EKIAS)

**Im Auftrag des**

Bundesministriums für
Bildung und Forschung

Bundesministerium
für Bildung
und Forschung

**Beauftragter:**

Fachhochschule Brandenburg
TeleTrusT e.V.

**Autoren:**

Anja Beyer
Sophie Hellmann
Malte Hesse
Friedrich-L. Holl
Peter Morcinek
Sachar Paulus
Helmut Reimer

**Unter Mitarbeit von :**

Markus Dahms
Karsten Kausmann
Simone Friedrich-Meier
Jens Ziegler

Herausgeber: Prof. Dr. Friedrich-L. Holl,
Fachhochschule Brandenburg


Redaktion: Friedrich-L. Holl
Gestaltung: Martin Schüngel
Druck: digital business and printing gmbh, Berlin

ISSN 1863-5016

# Inhaltsverzeichnis

# Einleitung

Die Bundesrepublik hat mit dem Signaturgesetz eine frühe Ausrichtung bei der Sicherstellung elektronisch gestützter Verfahren auf die Nutzung asymmetrischer Verschlüsselungsmechanismen geschaffen. Mit der dazugehörigen Einrichtung von Public-Key-Infrastrukturen, die als Grundlage für Authentifizierung, Identifizierung und Signatur dienen, können aus heutiger Sicht weitgehend organisationsübergreifende Geschäftsabläufe abgesichert werden.

Die Nutzung asymmetrischer kryptographischer Technologien unter Verwendung von Smart-Cards (oder anderer entsprechender Token) als Sicherheitsmedium hat jedoch bisher keine wirkliche Relevanz. Der Zugang zu Anwendungen wird vielmehr immer noch vorrangig über die wenig verlässliche Kombination von User-IDs und Passwörtern geregelt, selten werden Einmalpasswortverfahren oder andere, sicherere Verfahren verwendet. Auch neue Entwicklungen berücksichtigen anderweitige (stärkere) Identifizierungs- und Authentifizierungsverfahren selten beziehungsweise nur dann, wenn es sich um ausgewiesene Sicherheitsanwendungen handelt.

Aufbauend auf dieser Problematik  entstanden die im Projekt zu beantwortenden Fragen, die sich ganz besonders darauf beziehen, weshalb asymmetrische Verfahren nur in derart begrenztem Maße genutzt werden, beziehungsweise warum Unternehmen immer noch auf unsichere Zugangssysteme setzen, obwohl die Risiken weit gehend und allgemein bekannt sind. Diese Fragestellungen behandeln wir vorrangig im Kapitel Nutzungsbedingungen (vgl. Kapitel 3), wo wir die Kriterien

herausgearbeitet haben, die üblicherweise über eine erfolgreiche Umsetzung und vor allem Nutzung einer Public Key Infrastruktur entscheiden. Unser Ansatz zur Ermittlung dieser Kriterien bestand darin, diese über geeignete Literatur, wie z.B. Erfahrungsberichte herauszuarbeiten. Da jedoch praktisch keine verwertbaren Veröffentlichungen aus diesem Bereich (öffentlich) verfügbar sind, führten wir eine anonyme Befragung von Experten durch, die viel Erfahrung bei der Planung, Umsetzung und Betrieb von Public-Key-Infrastrukturen haben. Durch die Zusage der Anonymität der Befragten konnten wir aus unserer Sicht unverfälschte, nicht zensierte Ergebnisse erzielen.

Im Zusammenhang mit den durchgeführten Interviews wurden neben Fragen zur Planung Faktoren erhoben, die für und gegen die Nutzung von PKI sprechen, sowie Folgen für die Benutzer und Haftungsfragen erfasst. Bezüglich der Umsetzung wurden die eingesetzten Lösungen bzw. Produkte sowie die Entscheidung weshalb sie eingesetzt werden und der für die Einführung benötigte Zeitbedarf erhoben. Der Teil, in dem Fragen zum Betrieb von PKI gestellt wurden, bezog sich auf Hindernisse bzw. Herausforderungen beim Betrieb sowie die benötigte und wirklich verwendete Dokumentation. Bei der Problematik der organisationsübergreifenden Kommunikation wurde unter anderem auf technische Realisierungen und die damit gemachten Erfahrungen eingegangen. Insgesamt haben wir versucht, die möglichen Hürden für den Einsatz von PKI-Anwendungen und –Konzepten zu erfassen und bewerten zu lassen.

Im Weiteren haben wir überprüft, welche neuen technischen Entwicklungen derzeit im Zusammenhang mit der Entwicklung von Public-Key-Infrastrukturen zu finden sind, welche mittel- bis langfristigen Entwicklungslinien sich in diesem Bereich zeigen. Die hierbei im Kapitel „Technische Perspektiven" gewonnenen Informationen wurden über zwei unterschiedliche Ansätze erhoben:

Zum einen wurde eine international angelegte, an den Themenkomplexen Kryptographie, Token, PKI, alternative Konzepte ohne PKI, Biometrie und Sicherheitsevaluierungen sowie –zertifizierungen orientierte Literaturstudie durchgeführt. Zum Anderen interviewten wir 13 Experten aus den Bereichen Forschung, Industrie und Wirtschaft zu den oben genannten Themenbereichen.

Insgesamt bezieht sich dieses Kapitel insbesondere darauf, welche Sicherungsmöglichkeiten für Unternehmen bestehen, wenn Geschäfte sowohl im B2C- als auch im B2B-Bereich zunehmend online abgewickelt werden. Gesetze, wie der Sarbanes-Oxley-Act oder Basel II, erfordern für Unternehmen zudem einen organisierten, effizienten und proaktiven Ansatz der IT-Sicherheit. Die Bedeutung von IT-Sicherheitstechnologien wird dadurch erheblich verstärkt. Wir zeigen, dass gerade im Umfeld der PKI-Technologien hierfür nachhaltige Lösungsansätze zu finden sind.

Wesentliches Ziel des Kapitels „Betriebswirtschaftliche Betrachtungen" war zu

zeigen, welche Kosten/Nutzen-Relationen sich für die Anwendung von PKI-Systemen ergeben. Hierzu wurde zuerst geprüft, ob es Konzepte oder Anwendungen gibt, die eindeutig als PKI-Einsatzszenarien identifizierbar sind. Durch Literaturrecherchen und Erkenntnisse aus der Praxis konnten entsprechende Kriterien sowie eine Klassifikation entwickelt werden.

Daran anschließend wurde geprüft, inwieweit ein PKI-Einsatz vor allem auf Geschäftsprozessebene sinnvollerweise zu betrachten wäre und inwieweit PKI eine Enabler-Funktion zugesprochen werden kann. Dazu wurden u.a. Interviews mit Verantwortlichen durchgeführt, um sowohl die Erfolgskriterien als auch die betriebswirtschaftlichen Hintergründe zu erkennen. Insgesamt zeigte sich, dass der Ansatz der Geschäftsprozessorientierung zur Zeit wenig praxisrelevant ist, da der PKI-Einsatz immer noch vorrangig als Infrastrukturinvestition verstanden wird. Auf dieser Grundlage wurde untersucht, welche Kennzahlen(-Systeme) sich in welcher Art und Weise auf PKI-Investitionsentscheidungen auswirken. Dabei wurden Verfahren betrachtet, die zum einen vorrangig quantitativ zum anderen qualitativ ausgerichtet sind. Anhand realer, anonymisierter Unternehmensdaten wurde darauf aufbauend eine beispielhafte Kosten-Nutzen-Betrachtung durchgeführt. Als Ergebnis dieser Betrachtung zeigt sich unseres Erachtens, dass im Zusammenhang mit PKI-Investitionsentscheidungen nur eine Kombination verschiedener Kennzahlenverfahren ein ganzheitliches Bild liefern kann, mit Hilfe dessen eine umfassende und realitätsorientierte Entscheidung über das Umsetzen einer Investition zu begründen ist.

Auf der Basis der Ergebnisse der vorher beschriebenen Kapitel wurde ein ergänzender Workshop durchgeführt, der im Kapitel „Workshop-Ergebnisse“ beschrieben wird. Der Workshop sollte abschließend Erfolgskriterien identifizieren und Perspektiven aufzeigen. An diesen Zielen wurde sowohl die Organisation des Workshops als auch die Zusammensetzung der Teilnehmer ausgerichtet, die aus verschiedenen Kompetenzgruppen zusammengestellt wurden: Hersteller und Dienstleister aus dem PKI-Markt, Chief Information Security Officer, die erfolgreiche multinationale PKI-Projekte umgesetzt haben, Wissenschaftler, Unternehmensberater mit Sicherheits- und Betrugsbekämpfungsexpertise, IT-Manager. Dabei wurde besonders auf eine langjährige Erfahrung der Teilnehmer Wert gelegt.

Zur Vorbereitung der innerhalb des Workshops geplanten Arbeitsgruppen wurden die Teilnehmer über die bisherigen Ergebnisse informiert. Aufbauend auf diesen Informationen und ihren praktischen Erfahrungen sollten sie Problemfelder identifizieren und Wunsch-Zustände sowie Lösungen / Aktionsfelder erarbeiten.

Durch die breit differenzierte Kompetenz der Workshop-Teilnehmer, mit Beiträgen aus sehr unterschiedlichen Interessenlagen und einer entsprechenden Vertiefung in den Arbeitsgruppen wurde eine Fokussierung der Kernthematik erreicht. Insbesondere die interdisziplinäre Zusammensetzung von Technikern und Nicht-Technikern, von IT- und Sicherheitsverantwortlichen, PKI-Dienstleistern usw. war ein

wesentlicher Erfolgsfaktor für die Ausprägung von differenzierten und durchaus kontroversen Aspekten, mit einem dennoch klaren Fokus auf den Erfolg von Public-Key-Infrastrukturen, -Anwendungen und -Technologien. Zudem erhielten wir wichtige Detail- und Praxisinformationen sowie persönliche Einschätzungen, die in einer formellen Befragung nicht erfahrbar gewesen wären. Dies gilt in besonderem Maße für Meinungen oder Einschätzungen entgegen der „herrschenden" Expertenmeinung, die – vielleicht wegen politischer Motivationen – in dieser Form bisher nicht öffentlich diskutiert wurden. Diese Ergebnisse werden als Empfehlungen für das weitere Vorgehen bei der Gestaltung von PKI-Projekten in diesem Kapitel zusammengestellt.

Ein wesentliches Ziel des Projektes war, mögliche Weiterentwicklungen, Bedarf an Förderung oder einfach praktische Tipps zu identifizieren, die helfen, PKI noch mehr zu verbreiten bzw. umgekehrt, Stolpersteine der Erfolgs zu herauszufiltern und Empfehlungen zu formulieren, wie diese ausgeräumt werden können. Im Kapitel „Empfehlungen" werden daher die wichtigsten Erkenntnisse für die Bereiche Technik, Betriebswirtschaft und praktische Anwendung noch einmal zusammengestellt. Darauf aufbauend formulieren wir Empfehlungen für mögliche weitere Vertiefungen und Forschungsprojekte und geben konkrete Tipps für erfolgreiche PKI-Implementierungen.

Im Gesamtergebnis soll die hier vorgelegte Studie Hinweise darauf geben, wann und wo PKI erfolgreich eingesetzt werden kann, welche Massnahmen – unter Umständen auch von staatlicher Seite – dafür ergriffen werden können und auf welchen Gebieten weitere Forschung unseres Erachtens nach sinnvoll wäre.

# Executive Summary

Die EKIAS-Studie befasst sich mit Erfolgskriterien für Identifizierungs-, Authentifizierungs- und Signaturverfahren auf Basis asymmetrischer kryptographischer Verfahren und somit in erster Linie mit der Analyse positiv zu wertender sowie hemmender Faktoren beim Einsatz von Public-Key-Anwendungen. Die wichtigsten Ergebnisse der Studie sind, dass Nutzeraspekte einen höheren Stellenwert beim Einsatz von Public-Key-Infrastrukturen (PKI) besitzen als zuvor angenommen und betriebswirtschaftliche Argumente korrekterweise nur dann eine Rolle spielen können, wenn sie im Kontext eines konkreten Geschäftsprozesses betrachtet werden. Ferner ist es wichtig, die Anwender beim Einführungsprozess zu begleiten, damit diese die PKI-Anwendungen auch annehmen.

Ziel der Studie war es herauszufinden, wo Forschungs- und Förderungsbedarf für PKI-Technologien und -Anwendungen besteht und wo Innovationspotential zu finden ist.

Dabei wurden unter anderem folgende Ergebnisse erzielt:

## Technische Perspektiven

Eine lange Nutzungsdauer (Gewährleistung der Haltbarkeit von Algorithmen und Schlüssellängen) muss technisch realisierbar sein, damit sich insbesondere die Kosten amortisieren, da die Etablierung einer PKI vergleichsweise hohe anfängliche und über eine lange Zeit weiter zu tragende Investitionskosten erfordert. Die lange

Nutzungsdauer spielt vorrangig für staatliche Anwendungen (Ausweisdokumente, gesetzlich länger zu archivierende Dokumente) eine Rolle; bei Unternehmensanwendungen wird typischerweise marktorientiert und damit eher kurzfristig gedacht.

Ein wichtiger Punkt für die erfolgreiche Nutzung der PKI-Technologie ist die Interoperabilität. Diese muss bei multiprozessualen Anwendungen (Bsp.: E-Mailverschlüsselung) durch Standards gewährleistet werden.

Für eine erfolgreiche Anwendungsintegration muss das Schlüsselmanagement für mehrere Anwendungen gemeinsame Schlüssel bereitstellen oder alternativ die Verwaltung von parallel existierenden Schlüsseln ermöglichen. Als Ergänzung von softwarebasierten Zertifikaten ist die Verwendung von Tokens (z.B. Smart Cards, USB-Token) anzustreben, um ein verbessertes Sicherheitsnivau zu erreichen. Bei den Tokens muss auf deren Erweiterbarkeit (Austausch von Algorithmen etc.) geachtet werden – die Form der Token wird sich weiterentwickeln und an die Anwendungen anpassen. Zusätzlich zu Tokens werden in der Zukunft verstärkt biometrische Techniken eingesetzt, um Personen eindeutig zu identifizieren.

## Betriebswirtschaftliche Betrachtungen

Die PKI-Technologie kann ein Geschäftsprozess-Enabler sein. Die Aufwendungen dafür lassen sich jedoch nur im Kontext der konkreten Prozesse betriebswirtschaftlich begründen. Für den Einsatz von PKI gibt es zwei finanziell motivierte Argumente: Zum einen PKI als Kosteneinsparungsmaßnahme (PKI ermöglicht die Digitalisierung von Prozessen z.B. elektronische Rechnungen), zum anderen die Beschleunigung und Vereinheitlichung von Prozessen, damit diese „eleganter“ und mit weniger Aufwand elektronisch abgebildet werden können (z.B. bei Authentifizierung mit Zertifikaten bei Business Process Outsourcing). Problematisch ist, dass selbst die Prozessverantwortlichen oft keinen Überblick über die Kosten ihrer Prozesse haben, da diese an schwer zu durchschauenden und bewertenden Infrastruktur- und Systemkomponenten hängen. Auch der jeweilige Nutzen und das Risiko sind nur unter Schwierigkeiten quantifizierbar. Demzufolge können Einsparungen nur selten objektiv nachgewiesen werden. Um jedoch Geschäftsprozess-Enabler sein zu können, erfordert PKI Vorinvestitionen, weshalb Entscheider von deren Sinnhaftigkeit überzeugt werden müssen. Dabei können einzelne Kennzahlen wie ROI / ROSI oder NPV als Entscheidungshilfe dienen, doch liefern diese Kennzahlen häufig ein negatives Ergebnis. Diese Methodik würde oft gegen eine Investition in PKI sprechen, obwohl die Investitionen eigentlich sinnvoll wären. Deshalb sollte grundsätzlich ein Mix aus akzeptierten Methoden (z.B. ROSI inkl. TCO plus NPV und Balanced Scorecard) für eine detailliertere Kostenbetrachtung verwendet werden.

Ein weiteres Problem besteht darin, dass bei PKI die Träger der Kosten oft keinerlei Nutzen aus den Investitionen ziehen können. Auf Infrastrukturebene kann

üblicherweise auch kein Kosten-Nutzen-Transfer zustande kommen – dieser entsteht erst auf Prozessebene und auch hier nur bei organisationsinternen Prozessen. Deshalb haben auch organisationsübergreifende Bezahl- oder Kostenverlagerungsmodelle keine Akzeptanz im Markt gefunden.

Es ist festzuhalten, dass PKI ohne konkrete Anwendungen nur eine Infrastruktur ist, die keinem wirklich etwas bringt und die selbst aus Sicherheitssicht keinen Wert an sich darstellt. Ist eine PKI aber erst einmal etabliert, zeigen sich über die mit dem PKI-Einsatz verbundenen Unterstützungsmöglichkeiten von Geschäftsprozessen schnell die offensichtlichen Vorteile.

## Nutzungsbedingungen

Die PKI-Technologie ist noch nicht wirklich alltagstauglich und auch die Interoperabilität zwischen verschiedenen PKI-Anwendungen ist noch nicht in dem Maße gegeben, wie es von den Kunden gewünscht wird. Das gilt insbesondere für das beim Betrieb einer PKI notwendige Schlüsselmanagement.

PKI-Projekte sind als „empfindlich" einzustufen, deshalb kann der Erfolg eines solchen Projekts durch die sich innerhalb eines Projekts ändernden Anforderungen und Bedingungen gefährdet werden. Weiterhin zentralisiert PKI Vertrauensentscheidungen und sichert einen vorgesehenen Prozessablauf. Dies kann in der Praxis zu erheblichen Problemen führen, da derartige Entwicklungen den persönlichen Interessen der am Prozess Beteiligten entgegenstehen (können).

Die Akzeptanz von PKI-Anwendungen kann verbessert werden, wenn diese einfach und transparent, also im Kontext und in der Sprache des Geschäftsprozesses leicht nachvollziehbar sind. Aber, selbst wenn dies erreicht wurde, hat sich gezeigt, dass die Aufwände für den Support für PKI-Anwendungen dennoch höher sind als bei anderen Anwendungen. In diesem Zusammenhang muss zudem gewährleistet sein, dass im Support qualifizierte Mitarbeiter sitzen, damit die Sicherheitsvorgaben nicht durch falsche Handlungsempfehlungen kompromittiert werden können.

Das Akzeptanzproblem ist bei organisationsübergreifenden Prozessen noch wesentlich größer, weil hier heute in der Regel weder einfache noch nachvollziehbare Vertrauensentscheidungen zu treffen sind. Insofern sind bei derartigen Prozessen bestimmte Anforderungen an PKI-Anwendungen zu berücksichtigen. Dabei unterscheiden wir drei Szenarien, die alle eigenen Marktdynamiken gehorchen:

1. Für den Massenmarkt (z.B.: Home-Banking, Online-Shopping) stehen Einfachheit, Transparenz und minimalen Kosten im Vordergrund, was einen Einsatz einer komplexen Technologie wie PKI erschwert.

2. Im Unternehmensumfeld ist Flexibilität das wichtigste Kriterium, denn der Einsatz von PKI hängt beispielsweise von der Höhe der Sicherheitsanforderungen und der verwendeten Technologien ab. Erfolgreiche Insellösungen zeigen, dass Standardisierungen nicht die höchste Priorität besitzen und auch nur unter der Beachtung der jeweiligen Marktregeln etabliert werden können.
3. Beim Einsatz im staatlichen Interesse (z.B. elektronische Ausweisdokumente) ist dagegen eine Standardisierung in Verbindung mit hoher Sicherheit und Nachhaltigkeit (Austausch von Algorithmen, Biometrieeinsatz usw.) unabdingbar. Wichtigste Anforderungen bleiben jedoch einfache und nachvollziehbare Vertrauensentscheidungen für die Benutzer. Dabei ist allerdings zu berücksichtigen, dass sich Sicherheit aus Kontrolle und Vertrauen ergibt und eine Reduzierung von Kontrolle nur durch den Aufbau von Vertrauen möglich ist.

## Handlungsempfehlungen

Ziel des Projektes war es u.a., aufzuzeigen, wie Hindernisse im Zusammenhang mit den PKI-Technologien und ihren Einsatzbedingungen ausgeräumt werden können. Darauf aufbauend wurden Handlungsempfehlungen entwickelt, die die Weiterverbreitung von PKI fördern sollen.

Zu diesen Empfehlungen zählen auf technischer Seite unter anderem Hinweise auf die unseres Erachtens noch durchzuführenden Untersuchungen der Austauschbarkeit der kryptographischen Algorithmen, was insbesondere für den langfristigen PKI-Einsatz im staatlichen Umfeld von Interesse ist. Als weiterer Untersuchungsgegenstand wurde von uns die Integration von PKI in Anwendungen identifiziert, weil insbesondere durch die Förderung der Entwicklung von Frameworks standardisierte Verfahren ermöglicht werden. Ein wichtiger Aspekt ist zudem die Interoperabilität dieser Anwendungen und des Schlüsselmanagements, gerade im Behördenumfeld. Dabei sind sowohl weitere, über die Smart Card hinausgehende Formfaktoren wie auch ein standardiserter Zugriff auf kryptographische Schlüssel zu betrachten. Nicht zuletzt muss auf technischer Seite weitere Grundlagenforschung, im Bereich der Quantencomputer und deren Auswirkungen auf die bei PKI eingesetzten Krypto-Algorithmen, betrieben werden.

Aus betriebwirtschaftlicher Sicht müssen die Kosten für die Infrastrukturinvestitionen „PKI“ transparent gemacht werden und der Nutzen gegenüber gestellt werden. Aufgrund der Komplexität der den Geschäftsmodellen zugrunde liegenden Prozesse, sollte man sich auf die Kernprozesse konzentrieren bei denen PKI als „Enabler“ auftreten könnte. Sicherheit muss dabei zu einem impliziten Teil der Geschäftsprozessmodellierung/-entwicklung werden. Auf Managementebene ist das Verständnis für die Wichtigkeit von Sicherheit durch geeignete Maßnahmen weiter zu verbessern. Um die Kostenbetrachtung eines PKI-Projektes detaillierter durchführen zu können, empfehlen wir die Verwendung eines Methodenmixes aus verschiedenen Kennzahlensystemen.

Eine direkte und breit gefächerte Anwendungsunterstützung führt bei einer PKI-Realisierung häufig zu Problemen, weshalb unseres Erachtens PKI-Pilotprojekte schrittweise in die gesamte Umgebung integriert werden sollten. Um mögliche Probleme aufzufangen und anderen eine Entscheidungshilfe zu geben, empfehlen wir zudem, positive und negative Erfahrungsberichte über den PKI-Einsatz zu veröffentlichen.

Weiterhin sollten insbesondere die Abhängigkeiten von Technik, Wirtschaft und Nutzungsaspekten beim PKI-Einsatz untersucht werden, so dass Möglichkeiten gefunden werden, die Vertrauensbeziehungen im elektronischen Geschäftsverkehr zu verbessern. Die für die Nutzung von PKI-Anwendungen notwendigen Vertrauensentscheidungen sind für die Anwender einfach und nachvollziehbar zu gestalten. Dabei kann der direkte Kontakt mit Nutzern das Bewusstsein für Vertrauensbildung und -entscheidungen bei (Internet-) Anwendungen aufbauen beziehungsweise verbessern. Auch ist davon abzusehen, technische Anforderungen in Gesetze zu gießen; stattdessen empfehlen wir, dass diese in Verordnungen festgelegt werden, um Spielräume bei der Etablierung von PKI-Anwendungen ausnutzen zu können.

# 1.

# Technische Perspektiven

Die Bedeutung der IT-Sicherheitstechnologien steigt insbesondere für Unternehmen dadurch, dass Geschäfte sowohl im B2C als auch im B2B Bereich zunehmend online abgewickelt werden. Gesetze, wie der Sarbanes-Oxley-Act oder Basel II fordern für Unternehmen einen organisierten, effizienten und proaktiven Ansatz der IT-Sicherheit (Vgl. [Booker 2006]). Um Systeme, Daten und Kommunikationswege zu schützen, existieren Verfahren zur Verschlüsselung, Signatur, Identifikation und Authentifizierung.

## 1.1 Methodik

Für das hier vorliegende Kapitel „Technischen Perspektiven" wurden zwei verschiedene Ansätze zur Gewinnung der Informationen gewählt:

- → Zum einen wurden mit 13 Experten aus den Bereichen Forschung, Industrie und Wirtschaft leitfadengestützte Interviews über Telefon durchgeführt. Grundlage für diese Interviews war ein entsprechender Leitfaden, der zu den Themenbereichen Kryptographie, Token, PKI, alternative Konzepte ohne PKI, Biometrie und Sicherheitsevaluierungen sowie -zertifizierungen Fragen bereitstellte (Leitfaden und Liste der Interviewpartner siehe Anhang).
- → Parallel zu den Experteninterviews wurde eine international angelegte, an den oben genannten Themenkomplexen des Fragenkatalogs orientierte Literaturstudie durchgeführt.

Der vorliegende Bericht folgt dem thematischen Aufbau des Fragenkatalogs.

## 1.2 Kryptografie

Die Bundesnetzagentur veröffentlicht auf Grundlage des deutschen Signaturgesetzes jedes Jahr eine Empfehlung für die Verwendung kryptografischer Algorithmen für Qualifizierte Signaturen und Hashfunktionen sowie für die Verwendung von Zufallszahlengeneratoren (Vgl. [Bundesnetzagentur Algorithmenkatalog 2006]). Die im Katalog fixierten Empfehlungen für Qualifizierte Signaturen sollen laut Signaturverordnung ihre Sicherheit für „mindestens sechs Jahre nach dem Zeitpunkt der Bewertung und Veröffentlichung" [SigV 2001] gewährleisten. Der Zeithorizont ist für den praktischen Einsatz wenig sinnvoll, da Investitionen und die Amortisation der Investitionen in diesem Bereich einen längeren Zeithorizont haben. Der Algorithmenkatalog der Bundesnetzagentur aus dem Jahre 2006 empfiehlt für Hashfunktionen SHA[1]-1 (bis Ende 2009), RIPEMD[2]-160 (bis Ende 2010) und SHA-224, SHA-256, SHA-384, SHA-512 (bis Ende 2011).

**Für Signaturverfahren sind geeignet:**

1. RSA[3]-1024 (bis Ende 2007), RSA-1976 (bis Ende 2011), Empfehlung der Verwendung von RSA-2048
2. DSA[4]-1024 (bis Ende 2007), DSA-2048 (bis Ende 2011), Empfehlung der Verwendung von DSA-2048,
3. DSA-Varianten, basierend auf elliptischen Kurven (Bitlänge der verwendeten Primzahl q mind. 180 (Ende 2009) und 224 (bis Ende 2011)), insbesondere:
   a. EC[5]-DSA
   b. EC-KDSA,
   c. EC-GDSA[6],
   d. Nyberg-Rueppel-Signaturen

(Vgl. [Bundesnetzagentur Algorithmenkatalog 2006])

Es wird dringend empfohlen, zur Schlüsselerzeugung einen physikalischen Zufallszahlengenerator zu verwenden. Wenn für die Erzeugung von Schlüsseln oder Signaturen kein physikalischer Zufallszahlengenerator zur Verfügung steht, kommt als Alternative ein Pseudozufallszahlengenerator in Frage. „Der innere Zustand wird durch den [...] Seed initialisiert. In jedem Schritt muss der Zustand erneuert und daraus eine Zufallszahl abgeleitet werden. Der Seed muss gegen Auslesen und

1 Secure Hash Algorithm
2 RACE Integrity Primitives Evaluation Message Digest
3 Asymmetric cryptographic system named after Rivest, Shamir and Adleman
4 Digital Signature Algorithm
5 Elliptic Curves
6 KDSA and GDSA are DSA variants based on elliptic curves

Manipulation geschützt werden ...". Jeder Pseudozufallszahlengenerator muss ein Deterministic Random Number Generator der Klasse K3 (Evaluationsstufe 3, Stärke „hoch") im Sinne der AIS-20 (Vgl. [BSI 2006a]) sein. Die Entropie des Seed beträgt mindestens 80 Bit; empfohlen werden 100 Bit (bis Ende 2009), 100 Bit bzw. 120 Bit (ab 2010) (Vgl. [Bundesnetzagentur Algorithmenkatalog 2006]).

Ein Algorithmenkatalog, wie der der Bundesnetzagentur, kann als Grundvoraussetzung für die Verfügbarkeit verlässlicher Systeme über einen längeren Zeitraum angesehen werden und stellt ein gutes Mittel dar, um standardisierte Verfahren zu etablieren (Vgl. [Giessmann 2006]). Allerdings gibt es keine nationale Ausprägung der Algorithmen und Parameter für die Sicherheit von Signaturverfahren. Generell helfen die Empfehlungen der Kataloge im Hinblick auf Interoperabilität (Vgl. [Preneel 2006]).

Auf internationaler Ebene sind die Empfehlungen der „Suite B" der NSA ausschlaggebend und wertvoll (Vgl. [Temple 2006], [Preneel 2006]). Dieser Katalog empfiehlt für:

→ **Verschlüsselung**:
AES-128 bzw. AES-256 (Advanced Encryption Standard) (Vgl. [NSA A 2007])
→ **Digitale Signaturen:**
ECDSA-256 bzw. ECDSA-384 (Elliptic-Curve Digital Signature Algorithm)
(Vgl. [NSA B 2007])
→ **Key Agreement:**
EC DH (Elliptic Curve Diffie-Hellman) oder EC MQV (Menezes-Qu-Vanstone)
mit NIST P-256 bzw. NIST P-384 (Vgl.[NSA C 2007])
→ **Hash-Funktionen:**
SHA-256 and SHA-384 (Secure Hash Algorithm) (Vgl. [NSA D 2007])

Leider fehlt bei den von der NSA empfohlenen Funktionen oft die Nutzung in der Praxis (Vgl. [Temple 2006]).

> „Die Sicherheit der oben genannten Verfahren beruht dabei entsprechend auf:
> 1. dem Faktorisierungsproblem für ganze Zahlen,
> 2. dem Diskreten-Logarithmus-Problem in der multiplikativen Gruppe eines Primkörpers Fp,
> 3. dem Diskreten-Logarithmus-s-Problem in den Gruppen E(Fp) und E(F2m)."
> [Bundesnetzagentur Algorithmenkatalog 2006]

Ergänzend ist zu berücksichtigen, dass die Sicherheit der heute eingesetzten Verfahren durch die Kombination aus Leistungsfähigkeit der Rechner und der mathematischen Grundlagen der kryptoanalytischen Verfahren, wie im Folgenden auch dargestellt beeinflusst wird. Die Sicherheit beruht auch darauf, dass noch niemand bessere mathematische Verfahren gefunden hat. Fortschritte auf diesem Gebiet sind bei einer Bewertung als wichtiges Kriterium zu berücksichtigen, wenn auch sehr schwer abzuschätzen.

1978 haben Rivest, Shamir, Adleman den RSA-Algorithmus (Vgl. [RSA 1978]) vorgestellt, der nach wie vor den Anwendungsstandard der asymmetrischen Kryptographie darstellt. Er ist auch in die verbreiteten Chipkartenfamilien (Signaturkarten, Karten für Bankanwendungen – SECCOS, Gesundheitskarte) implementiert. Die Sicherheit dieses Algorithmus basiert auf einem hinreichend schweren mathematischen Problem: die Primfaktorenzerlegung, die mit heutigen Verfahren für große Zahlen nicht machbar ist (Vgl. [Buchmann 2006]). Bei ausreichender Schlüssellänge lässt sich deshalb ein z.B. RSA-verschlüsseltes Dokument nicht in annehmbarer Zeit entschlüsseln, wenn man den dazugehörigen privaten Schlüssel nicht besitzt.

Aktuelle Entwicklungen auf dem Gebiet der Quantenmechanik könnten diesen Schutz zerstören. Ein Quantencomputer kann aufgrund seiner Bauart Berechnungen sehr viel schneller ausführen, als herkömmliche Rechner. Aber nicht nur ein irgendwann evtl. möglicher Quantencomputer kann die Sicherheit der Algorithmen gefährden.

1996 hat Shor gezeigt, dass mit Quantencomputern das Faktorisieren von RSA Moduli machbar wird und somit RSA brechen würde (Vgl. [Shor 1996]), was dann aktuell verwendete Algorithmen, wie RSA unsicher macht (Vgl. [Schmidt 2006], [Brassard 1996]).

Um dieser Bedrohung zu begegnen, gibt es nach (Vgl. [Schmidt 2006]) zwei Möglichkeiten:

1. alternative Kryptosysteme entwickeln, z.B. Lattice Based Kryptosysteme
2. Schlüssellänge der aktuellen Algorithmen erhöhen

Inwieweit der erste Vorschlag wirklich eine Alternative darstellt, muss noch untersucht werden. Vermutlich lassen sich alle deterministisch eindeutigen mathematischen Probleme mit Einsatz von Quantencomputern in polynomieller Zeit lösen. Es ist jedoch zum heutigen Zeitpunkt nicht mit Sicherheit zu sagen, ob Quantencomputer in ausreichender Größe überhaupt jemals gebaut werden können (Vgl. [Buchmann 2006], [Schmidt 2006]). Schmidt geht davon aus, dass die Größe der Quantencomputer nur sehr langsam wächst (Vgl. [Schmidt 2006]). Solange keine großen Quantencomputer existieren, scheint die zweite Variante die bessere Wahl zu sein (Vgl. [Schmidt2006]). Der größte derzeit existierende Quantencomputer kann die Zahl 15 faktorisieren (Vgl. [Buchmann 2006]) weshalb Quantencomputer keine sofortige Bedrohung darstellen (Vgl. [Okamoto 2003]).Vor diesem Hintergrund lässt sich sagen, dass derzeit verwendete Verfahren, wie RSA und kryptografische Verfahren auf Basis elliptischer Kurven zumindest kurzfristig (short-term, bis 10 Jahre) sicher sind (Vgl. [Buchmann 2006B], [Preneel 2006]). Einige Anwendungen, zum Beispiel Code-Signing und SSL Authentication, benötigen nur short-term-security (Vgl. [Buchmann 2006a]).

Auch Entwicklungen auf dem Gebiet der DNA-Computer sind relevant für die Einschätzung der Sicherheit kryptografischer Verfahren. Boneh et al. haben gezeigt,

dass mit Molekular-Computern massive Parallelverarbeitung möglich ist (Vgl. [Boneh 1995], [Boneh 1996]), was potentiell dazu führt, dass Schlüssel gebrochen werden können?

Aktuell scheinen Hashfunktionen eine sehr viel kürzere Lebenszeit zu haben als Verschlüsselungsfunktionen. Bereits 6 Jahre nach dem Einführen des MD4 wurden Kollisionen entdeckt (Vgl. [Dobbertin 1996]). Da SHA-0 und SHA-1 auf einem ähnlichen Algorithmus basieren, wie MD4, wurde auch dieses Verfahren durch eine theoretische Attacke unsicher (Vgl. [Buchmann 2006a]). Insofern stellen Hashfunktionen eine wesentliche Problematik dar (Vgl. [Leitold 2006]). Die Kryptografie-Community muss deshalb große Anstrengungen unternehmen, um bessere Designkriterien für die Langzeitsicherheit von Hashfunktionen zu entwickeln (Vgl. [Weis 2005], [Buchmann 2006 a]).

Für Anwendungen wie die elektronische Patientenakte sind laut Gesetz allerdings sichere Verfahren für die nächsten 30 Jahre gefordert (Aufbewahrungspflicht ärztlicher Aufzeichnungen). Dafür reichen heutige Verfahren nicht aus (Vgl. [Buchmann 2006b]).

Schon die Frage, was wir in 20 Jahren machen (Vgl. [Buchmann 2006b]) kann nicht so ohne weiteres beantwortet werden. Um für die Zukunft und unerwartete Angriffe gerüstet zu sein sind zwei Dinge nötig:

- → ein Vorrat an sicheren Alternativen kryptografischen Algorithmen muss verfügbar gemacht werden
- → die Anwendungen, die kryptografische Algorithmen verwenden, müssen so modular entworfen werden, dass unsicher gewordene Algorithmen einfach durch sichere austauschbar sind (Vgl. [Buchmann 2006a])

Auch Giessmann hält dieses pragmatische Vorgehen für sinnvoll, eine sichere Lösung einzusetzen und nach und nach durch Alternativen zu ersetzen. Vor diesem Hintergrund haben auch die Algorithmenkataloge ihre Berechtigung (Vgl. [Giessmann 2006]). Das Hauptproblem der Austauschbarkeit der Algorithmen ist die Implementierung (Vgl. [Preneel 2006]). Die Software bzw. die Protokolle müssen so programmiert sein, dass eine einfache Austauschbarkeit der Algorithmen möglich ist. Derzeit ist das bei vielen Implementierungen noch nicht der Fall (z.B. Microsoft Windows Betriebssystem) (Vgl. [Buchmann 2006b]). Buchmann schlägt vor, dass alle Anwendungen ihre kryptografischen Algorithmen von einer zugehörigen Crypto API, wie dem Java Cryptographic Architecture (JCA) oder der Microsoft Crypto API, importieren. Genauso einfach müssen Schlüssel, Zertifikate usw. austauschbar sein (Vgl. [Buchmann 2006a]). Buchmann stellt die Crypto Library FlexiProvider vor, in dem auf Basis von JCA alle Mainstream und alternativen kryptografischen Verfahren implementiert sind. Die Trustcenter-Software Flexitrust basiert auf FlexiProvider und wird von der deutschen Root Certification Authority (CA) und der German Country Signing CA verwendet. Auch einige experimentelle Algorithmen, die eine gewisse Sicherheit gegenüber Quantencomputern bieten sollen, sind im

PostQuantumProvider implementiert, der im FlexiProvider integriert ist (Vgl. [Buchmann 2006a]). Der FlexiProvider unterliegt der GNU GPL (General Public License) und LGPL (Lesser General Public License) und wird im Internet frei zum Download zur Verfügung gestellt (Vgl. [Flexiprovider 2006]). Christoph Busch gab in einem Interview zur Thematik seine Überzeugung vom Flexi-PKI-Konzept bekannt (Vgl. [Busch 2006]).

Die IEEE (Institute of Electrical and Electronics Engineers) P1363 ist eine Projektgruppe, die an der Standardisierung von Spezifikationen der Public-Key Kryptografie arbeitet. Im Fokus der Standardisierung liegen sowohl traditionelle Verfahren (z.B. RSA, DSA, etc.) als auch neuere Verfahren, wie Lattice-Based Public-Key Kryptografie (z.B. NTRU), die auch bei Existenz von Quantencomputern sicher sein sollen (Vgl. [Buchmann 2006a]). NTRU ist ein Public-Key Kryptosystem, das sehr viel schneller ist als herkömmliche Verfahren (wie RSA) und von NTRU Cryptosystems Inc. entwickelt und vertrieben wird. Aufgrund der Schnelligkeit ist dieses System auf den Markt 'eingebetteter Systeme' fokussiert und kann u.a. für Telefone und RFID-Chips verwendet werden. Die dazugehörigen Verfahren für Verschlüsselung und Signatur heißen NTRUEncrypt und NTRUSign und finden bereits praktischen Einsatz. NTRU Cryptosystems Inc. vertreibt seine Security Suite für Drahtlos-Netzwerke 'Aerolink' mit dem NTRU-Kryptosystem (Vgl. [NTRU 2006]).

Eine weitere Möglichkeit langfristig Sicherheit herzustellen, sind quantenkryptografische Verfahren, welche die Möglichkeiten der Quantenmechanik nutzen. Die Basis dafür bereiteten Bennet and Brassard, die bereits 1989 die Demonstration einer experimentellen Verteilung der Quantenschlüssel (Quantum Key Distribution) veröffentlichten (Vgl. [Brassard 1996]). Die meisten der heute existierenden experimentellen Prototypen quantenkryptografischer Verfahren basieren auf dem 1984 veröffentlichten QKD Protokoll BB84. Die Frage, die in weiterer Forschung geklärt werden muss, ist, wie sicher QKD wirklich ist (Vgl. [Brassard 1996]). Außerdem wäre QKD keine Lösung für Internet-Anwendungen bzw. End-to-End-Kommunikation, da ein gewöhnlicher Kanal (elektromagnetische Wellen oder drahtgebundene Kanäle) gebraucht wird. Bei der konventionellen Quantenkryptografie wird ein Quantenkanal vorausgesetzt (Vgl. [Okamoto 2003]). Es gibt derzeit noch kein quantenkryptografisches Verfahren, das praktisch einsetzbar ist. Hier ist noch viel Forschungsarbeit zu leisten.

Zwar gibt es bereits erste Ansätze, mit ersten experimentellen Erfolgen einer quantenkryptografisch verschlüsselten Banküberweisung (Vgl. [Wissenschaft.de 2005]), doch können diese keinesfalls bereits praktisch genutzt werden. Auch bei Firmen, die bereits Produkte auf diesem Gebiet anbieten kann von einer praktischen Nutzbarkeit noch nicht wirklich geredet werden (Vgl. [ID Quantique 2007], [SmartQuantum 2007]). Erste Ansätze existieren bereits, zum Beispiel gab es erste experimentelle Erfolge einer quantenkryptografisch verschlüsselten Banküberweisung (Vgl. [Wissenschaft.de 2005]). Auch Firmen bieten schon Produkte auf diesem Gebiet an (Vgl. [id Quantique 2007], [SmartQuantum 2007]).

## 1.3 Der Mensch im Spannungsfeld zwischen Technik und Wirtschaft

Eine weitere Problematik, die in Zusammenhang mit IT-Sicherheit diskutiert wird, ist die „Schwachstelle" Mensch. Der Mensch, der ein System bzw. eine Software bedient, wird von Experten oftmals als die größte Schwachstelle bezeichnet (Vgl. [Preneel 2006], [Temple 2006]). Fakt ist, dass die Systeme zwar technologisch relativ sicher sind, sie aber nicht für die Benutzung durch einen Menschen gestaltet sind, da Menschen z.B. ihre Passwörter vergessen oder nicht geheim halten. Angreifer versuchen nicht die kryptografischen Verfahren zu brechen, sondern setzen dort an, wo sie schneller zum Ziel kommen: das ist zum einen die Implementierung und zum anderen der Mensch (Social Engineering) (Vgl. [Hilton 2007]). Eine Möglichkeit zur Lösung dieses Problems wären zusätzliche Awareness-Maßnahmen (Vgl. [Busch 2006]) oder andere Verfahren, z.B. Biometrie (Vgl. [Giessmann 2006]) oder Single-Sign-On (SSO) in Verbindung mit Smart Card und Biometrie. Durch höhere Benutzerfreundlichkeit der biometrischen Verfahren könnten diese schnell an Akzeptanz gewinnen (Vgl. [Kuppinger 2006a]).

Den Mensch als schwach zu deklarieren ist allerdings sehr kurzsichtig. Die Menschen bzw. die Gesamtheit der IT-Benutzer lassen sich, auch mit Awareness-Maßnahmen, nur sehr schwierig 'umgestalten'. Da Technik leichter gestaltbar ist, sollte sich nicht der Mensch an das System anpassen, sondern das System an den Mensch. Die IT muss so gestaltet werden, dass der Mensch nur sehr einfache Entscheidungen treffen muss und nicht mit der Komplexität des Systems überfordert ist (Vgl. [Kuppinger 2006a]). Eine detaillierte Diskussion der Thematik findet sich im Kapitel „Nutzungsbedingungen".

## 1.4 Token & Trusted Computing

Ein Token ist eine Art „Bitmuster", das zur Authentifizierung verwendet wird. Der Begriff stammt aus der Netzwerktechnik, wo es ein Token-Ring Verfahren gibt, dass für die Vernetzung von Computernetzwerken entwickelt wurde. Das Gerät, das den Token hat, darf Daten senden. Im Sicherheitsbereich stellt der Token letztlich nichts anderes dar. Ein Token wird entweder mittels Software (z.B. das AccessToken für Benutzer bei Anmeldung an MS Windows enthält auch die Benutzer-Privilegien) oder in Kombination mit Hardware (z.B. Chip auf Smart Card, USB-Stick) abgebildet und wird auch als Crypto-Token bezeichnet. Abhängig vom Token können Anwendungen mit definierten Berechtigungen genutzt werden. Beim Hardware-Token kommt noch der Aspekt des Besitzes hinzu. Nur wer ihn hat, kann sich gegenüber einem System bzw. einer Anwendung authentifizieren. Die auch als Token bezeichneten Systeme finden heutzutage breiten Einsatz in einer Vielzahl von Anwendungen (Gesundheitskarte, Ticketing, Finanzen, etc.) (Vgl. [Williamson 2006]).

Als Smart Cards werden Chipkarten bezeichnet, die einen eingebauten Chip, eine Hardware-Logik und Speicher enthalten. Der Beitrag von Shelfer gibt einen

Überblick über Arten von Smart Cards, Infrastrukturen und Standards (Vgl. [Shelfer 2002]). Auch RFID-Chips mit dem Leistungsumfang von Smart Cards sind verfügbar, basieren auf demselben Prinzip und erlauben die Realisierung von kontaktlosen Chipkarten. Die Freiheitsgrade für den ‚Formfaktor' haben sich auch dadurch vergrößert. Die Smart Card-Chips lassen sich leicht in portable (und personalisierbare) Komponenten (z.B. USB-Sticks, Mobile Phones usw.) integrieren.

Im Bereich der Identifikation haben in der Vergangenheit fehlende Standards die Durchsetzung der Smart Cards behindert. Die Situation hat sich mittlerweile verbessert. Derzeit sind noch keine Standards definiert, es wird aber daran gearbeitet. Der ISO-Standard 24727 ist hinsichtlich der Interoperabilität viel versprechend (Vgl. [Williamson 2006]). Der ISO-24727-Standard wird in (Vgl. [Spitz 2006]) genau beschrieben.

Bakdi stellt eine Methode vor, wie mehrere Smart Cards in einer vereint werden kann. Der Ansatz „virtual token" erlaubt es, mehrere Anwendungen mit einem Hardware Token zu bedienen (Vgl. [Bakdi 2006]). Die massenhaft eingesetzten RFID Systeme werden die Sicherheits-Thematik der Zukunft sein. Eine Herausforderung stellen immer noch die Gewährleistung des Datenschutzes und der Datenintegrität der Systeme dar (Vgl. [Calmels 2006]).

Ein Trusted Plattform Module (TPM) ist ein Smart Card Derivat verbunden mit einer API und Protokollen zur Erhöhung der Vertrauenswürdigkeit von Rechnerplattformen oder anderer Geräte (Trusted Plattform). Ziel ist es eine kryptografische Hash-Kette zu bilden, die den aktuellen Ausführungsstatus repräsentiert und diesen Wert sicher in einem Register des TPM zu speichern. Die Gegenstelle kann dann verifizieren, ob sich die Plattform in einem sicheren Modus befindet, indem sie das TPM beauftragt einen signierten Datenblock mit dem Wert der Hash-Kette zu erzeugen (Vgl. [Poritz 2006]). TPMs sind eine Entwicklung der Trusted Computing Group (Vgl. [TCG 2006]). Der wichtigste Unterschied zur Smart Card ist, dass sie an Systeme und nicht an Personen gebunden sind. Trusted Plattform Module wurden mit dem Ziel entwickelt, eine adäquatere Basis als Software für höchstvertrauenswürdige Plattformen zu bilden (Vgl. [Sandhu 2005]) und sollen ein „Root of Trust" herstellen (Vgl. [Sadeghi 2006]). Es werden bereits viele Plattformen mit TPM ausgeliefert (Vgl. [Sadeghi 2006]). Die Architektur erlaubt die spätere Integration von neueren Verfahren, wie lattice-based Access control (Vgl. [Sandhu 2005]).

Das BSI begrüßt die von Microsoft angestoßene Sicherheitsinitiative rund um Trusted Computing, da gegenwärtig PC's sehr anfällig für Schadprogramme sind, da „...die bisher eingesetzten Betriebssysteme – insbesondere der Microsoft Windows-Familie – diese Bedrohungen nur sehr unvollkommen abwehren". Das BSI erwartet eine Verbesserung der IT-Sicherheit, sagt aber auch, dass Befürchtungen „...zu große[r] Einschränkungen im freien Gebrauch von Rechnern" auch nicht von der Hand zu weisen sind. Offen sei auch noch „...welche genauen Auswirkungen sich für freie Software-Lösungen (Open Source) ergeben werden" (Vgl. [BSI 2006b]).

TPM haben bereits eine gute Verbreitung im PC-Breich und sind nützlich zur Geräteauthentifizierung (Vgl. [Giessmann 2006], [Preneel 2006]), während Chipkarten eher für Personen gut geeignet sind (Vgl. [Giessmann 2006]). Die Kombination aus TPM und Smart Card könnte nützlich sein (Vgl. [Preneel 2006]), da aus Datenschutzgründen eine Trennung der personenbezogenen Daten vom Gerät möglich sein sollte, z.B. im Bereich Mobile Computing (PDAs, Mobiltelefone etc.). Personenbezogene Daten werden auf der Smart Card gespeichert, die im Besitz des Nutzers ist. Die Smart Card wiederum wird benötigt, um sich gegenüber dem TPM zu autorisieren (Vgl. [Gawlas 2005]). Auch Temple hält den TPM-Standard für tragfähig (Vgl. [Temple 2006]).

Für eine weitgehende praktische Einsetzbarkeit von Trusted Computing sind jedoch noch einige Probleme zu lösen:

- → TPM Komplexität: Anzahl der Befehle und Parameter scheinen nicht handhabbar zu sein. Es fehlt eine Analyse, welche Funktionalität mindestens/essentiell enthalten sein muss
- → TPM Compliance: viele praktische Umsetzungen sind nicht mit der Spezifikation konform, Nutzer haben keine Möglichkeit die Vertrauenswürdigkeit oder Compliance ihrer TPMs zu testen
- → Maintenance: Methoden für Recovery versiegelter Informationen und Backups im Falle modifizierter Plattformkonfiguration nötig
- → Trust Infrastructure: Framework um Vertrauen praktisch zu handhaben wird benötigt, Plattform-Zertifikate, Trusted Channels, Attestation Kernel, etc
- → Attestation: existierende Verfahren zur Attestation sind nicht zufrieden stellend. Hier muss erneutes Nachdenken stattfinden: Derzeitige Verfahren legt die Systemkonfiguration offen. Der Datenschutz wird außer Acht gelassen. Es existiert ein „Property-Based Attestation“ Ansatz, der aber noch weiter spezifiziert werden muss

(Vgl. [Sadeghi 2006]).

Der Ansatz der „Property-Based Attestation“ klingt interessant erfordert aber noch weitere Forschung. Poritz kritisiert, dass das TPM nicht den Sicherheitsstatus der Plattform attestiert, sondern den Ausführungsstatus (Vgl. [Poritz 2006]).

## 1.5 PKI-Anwendungen

Die PKI-Technologie und die zu Grunde liegende asymmetrische Kryptographie stellen Sicherheitsfunktionen wie Benutzer-Authentifizierung, -Identifikation und elektronische Signaturen zur Verfügung.

### 1.5.1 Authentifizierung, Identifikation und Signaturen

Authentifizierung stellt den Prozess dar, anhand dessen die Identität eines Benutzers festgestellt wird. PKI kann als Teil des Authentifizierungsprozesses genutzt

werden. Außerdem ist die Authentifizierung von technischen Komponenten wie beispielsweise Routern möglich. Die Formen der Benutzerauthentifizierung sind vielfältig. Am stärksten verbreitet sind die Eingabe eines identifizierenden Namens oder einer Benutzererkennung sowie eines Passworts oder einer PIN. Die Sicherheit des Authentifizierungsprozesses hängt von der Anzahl der Beweise oder Faktoren ab, die während des Prozesses angesprochen werden (Vgl. [Nash 2001]).

Traditionelle Authentifikationstechniken wie Passwort- oder Smart Card-Verfahren beruhen darauf, dass der Teilnehmer über ein bestimmtes, nur ihm bekanntes Wissen verfügt (Verifikation der Identität durch Wissen) oder einen persönlichen Berechtigungsschlüssel besitzt (Verifikation der Identität durch Besitz). Biometrische Verfahren nutzen im Gegensatz dazu physiologische oder verhaltenstypische Merkmale des Teilnehmers zur Authentifikation (Vgl. [TeleTrusT 2006]).

PKI ist in der Lage, die Identität eines Clients zu garantieren, wenn ein Protokoll wie SSL verwendet wird. Die Verwendung von Public/Private Keys und Zertifikaten kann in diesem Zusammenhang als zweistufiges Authentifizierungsverfahren angesehen werden. Bei einer PKI Authentifizierung wird der zu authentifizierende Teilnehmer mit einer Challenge, konfrontiert die mit dem eigenen Public Key signiert oder verschlüsselt wird. Wenn der Urheber der Challenge die Gültigkeit der Signatur feststellt oder die Daten mit dem öffentlichen Schlüssel aus dem Zertifikat des Teilnehmers entschlüsseln kann, gilt der Teilnehmer als authentifiziert. In manchen Diensten überträgt der zu authentifizierende Teilnehmer sein Zertifikat in der Antwort auf die Challenge. In anderen Diensten holt der Authentifizierungsdienst das Zertifikat aus einem Zertifikatverzeichnis (Vgl. [Nash 2001]).

Ein Weg zur Bündelung von Authentifizierungsmechanismen ist Single Sign On (SSO). Zum einen soll es dem User damit ermöglicht werden, sich gegenüber unterschiedlichen Systemen mit der gleichen Methode, zum Beispiel dem gleichen Passwort, zu authentisieren. Zum anderen soll für den User zur Nutzung aller Systeme nur ein einziger Authentifizierungsvorgang notwendig sein. SSO-Systeme werden über einen SSO-Server realisiert, der zwischen die Arbeitsplatzrechner des Unternehmens und die jeweiligen Anwendungsserver geschaltet wird (Vgl. [Schmeh 2001]).

Identifikation bezeichnet die Überprüfung einer Person oder eines Objektes in Bezug auf vorgelegte, eindeutig kennzeichnende Merkmale. Für den Identifikationsprozess stehen verschiedene Verfahren zur Verfügung, beispielsweise Smart Cards oder biometrische Verfahren, auf die im Abschnitt „alternative Konzepte“ näher eingegangen wird.

Die Benutzer-Identifikation stellt allerdings keine PKI Anwendung im engeren Sinne dar. Aus den Aufgaben einer herkömmlichen Unterschrift ergeben sich für digitale Signaturen folgende Funktionen: Identifikation; Echtheit, Abschluss, Warnung. Das bedeutet für digitale Signaturen, dass sie zum einen die Identität des

Unterzeichners zweifelsfrei bestätigen müssen. Zum anderen dürfen sie nicht wieder verwendbar und nur in Verbindung mit dem Originaldokument gültig sein. Darüber hinaus darf eine nachträgliche Veränderung des signierten Dokumentes sowie die Zurückweisung der Signatur durch den Unterzeichner nicht möglich sein. Mithilfe asymmetrischer Verfahren können diese Anforderungen erfüllt werden. Die Erstellung digitaler Signaturen basiert auf dem Digital Signature Standard (DSS) sowie dem Digital Signature Algorithm (DSA) (Vgl. [Eckert 2006]).

### 1.5.2 PKI Standards und Protokolle

Die folgenden Protokolle und Standards stellen die Basis für Public Key Infrastrukturen dar.

#### 1.5.2.1 Protokolle

**Secure Sockets Layer**, SSL, ist das bekannteste PKI-basierte Protokoll, das eine breite Anwendung findet. SSL baut einen in der Transportschicht abgesicherten Kommunikationskanal zwischen zwei Teilnehmern auf. Durch die Bereitstellung einer symmetrischen Verschlüsselung und der Integrität durch Message Authentication Codes (MACs) gewährt es die Vertraulichkeit der Kommunikation. SSL nutzt PKI hauptsächlich für die Authentifizierung der Teilnehmer während des Verbindungsaufbaus (Vgl. Nash 2001]).

**IPSec** definiert einen sicheren Rahmen und eine Reihe von Sicherheitsdiensten für die (IP-) Kommunikation auf Netzwerkebene. Für IPSec sind zwei Betriebsmodi definiert, zum einen der Tunnelmodus und zum anderen der Transportmodus. In ersterem ist das komplette IP-Paket verschlüsselt und wird zum Datenabschnitt eines neuen, größeren Pakets, das mit einem neuen IP-Header und einem IPSec-Header ausgestattet wird. Im Transportmodus wird der IPSec Header direkt in das IP-Paket eingefügt. Der Tunnelmodus wird hauptsächlich von Gateways und Proxies benutzt. IPSec wird von den Komponenten des Leitwegs umgesetzt. Neben guten Sicherheitsmerkmalen bietet IPSec auch sehr viel Flexibilität (Vgl. [Nash 2001]).

**S/MIME**, die Secure/Multipurpose Internet Mail Extensions stellen Merkmale für die Authentifizierung, Integrität und Vertraulichkeit für Messaging-Applikationen bereit. S/MIME ist nicht auf E-Mail beschränkt und kann von anderen S/MIME konformen Transportmechanismen genutzt werden wie beispielsweise http. Mit diesem Protokoll können ein einzelner Nachrichtenabschnitt, mehrere Abschnitte oder eine komplette Nachricht abgesichert werden (Vgl. [Nash 2001]).

Das **Time Stamp Protokoll**, TSP, liefert durch die Dienste einer Time Stamp Authority (TSA) den Beweis dafür, dass Daten zu einem bestimmten Zeitpunkt existiert haben. Bei TSP handelt es sich um ein einfaches Anforderung/Antwort-Protokoll. Der Teilnehmer, der einen Zeitstempel benötigt, übermittelt eine Time StampReq-Nachricht

an die TSA, um den Zeitstempel anzufordern. Die TimeStampReq-Nachricht enthält einen Hash der Daten, die mit einem Zeitstempel zu versehen sind. Die TSA gibt den Zeitstempel in einer Time StampResp-Nachricht zurück. Die TimeStampResp-Nachricht enthält den Status der Anforderung und den Zeitstempel in einer signierten Datenübertragung, die gemäß CMS-Spezifikation formatiert ist (Vgl. [Nash 2001]).

**Wireless Transport Level Security**, WTLS, bietet eine ähnliche Funktionalität wie TLS, jedoch unter besonderer Berücksichtigung der drahtlosen Übertragung. WTLS verfügt beispielsweise über eine Handshake-Optimierung und ermöglicht die dynamische Auffrischung von Schlüsseln, um die Leistung in drahtlosen Netzwerken mit geringer Bandbreite und einer relativ hohen Latenz zu verbessern. Im Gegensatz zu TLS kann WTLS entweder in verbindungsorientierten oder verbindungslosen Netzwerken eingesetzt werden (Vgl. [Nash 2001]).

#### 1.5.2.2 Formatierungsstandards

Um die Interoperabilität zwischen PKI Applikationen zu gewährleisten, ist es erforderlich, durch entsprechende Standards die Datensyntax festzulegen.

**X.509** ist der wichtigste Formatierungsstandard für PKI und stellt somit das Standardformat für Zertifikate dar. Es ist der grundlegende Standard, mit dem die Struktur des Public Key Zertifikats definiert wird. Die aktuelle Version X.509 Version 3 unterstützt zusätzliche Erweiterungsfelder, welche die Flexibilität der Zertifikate erheblich verbessern. Die große Flexibilität des X.509 Standards führt allerdings auch zu Problemen der Interoperabilität (Vgl. [Nash 2001]).

**PKCS**, die Public Cryptography Standards, wurden mit dem Ziel entwickelt, die Interoperabilität der Public Key Kryptographie zu fördern. Die PKCS Standards bieten grundlegende Definitionen der Datenformate und Algorithmen, welche die Basis fast aller heutigen PKI Implementierungen bilden (Vgl. [Nash 2001]).

**XML**, die eXtensible Markup Language, bietet eine flexible Möglichkeit, digitale Datenformate zu definieren. Ein typisches Einsatzgebiet für XML ist die Definition von Formaten für signierte Datenblöcke. Die Signaturelemente dienen der Abgrenzung der signierten Daten und können außerdem weitere Informationen zur Signatur enthalten, wie beispielsweise einen Zeitstempel (Vgl. [Nash 2001]).

### 1.5.3 Ist die einfache PKI Vision der asymmetrischen Kryptographie gescheitert?

Die ursprüngliche Idee der PKI wurde unmittelbar im Zusammenhang mit den Key-Management Eigenschaften der asymmetrischen Kryptographie formuliert. Sie sah eine hierarchische Infrastruktur im Internet für die Verwaltung der Bindung öffentlicher Schlüssel an einen für jede Person einmaligen Namen vor und sollte –

so die Vision – auf diesem Wege allen eine eindeutige elektronische Identität vermitteln. Es konnte jedoch nie geklärt werden, wer den erheblichen Aufwand für die Infrastruktur tragen und wie ein geeignetes Geschäftsmodell zustande kommen könnte. Deshalb ist diese Idee nur partiell wirksam geworden. Sie lebt z.B. in den von Verisign angebotenen Personenzertifikaten. Im Zusammenhang mit der Entwicklung von Standards wurden auch die Instanzen Registration Authority (RA) und Certification Authority (CA) definiert, die seitdem feste Elemente der PK-Infrastrukturen sind. Beide Instanzen erhalten Art und Umfang ihrer öffentlichen Vertrauenswürdigkeit durch normative Regelwerke (Policies) für technische und organisatorische Abläufe. Die Transparenz dieser Vetrauensmodelle ist allerdings für den Nutzer nicht unmittelbar gegeben, so dass eine Risikoabschätzung häufig nicht sachgemäß erfolgen kann.

Die Eignung und Funktionalität der PKI-Technologie für IT-Sicherheitsanwendungen ist in Fachkreisen weltweit anerkannt. Trotzdem hat die ursprünglich erwartete PKI-Technologie im offenen Internet bis heute nicht die breite Anwendung gefunden. Dagegen sind die PKI-Konzepte verstärkt in geschlossenen Benutzergruppen und für spezielle Anwendungen wirksam geworden. In großen Unternehmen wird auf Ihrer Grundlage das IT-Security-Management erfolgreich realisiert, wobei zunehmend Chipkarten als Dienstausweis mit IT-Sicherheits-Funktionalität ausgerollt werden.

Ein anwendungsorientiertes Beispiel für eine öffentliche PKI ist die Unterstützung einer Handunterschriftsäquivalenz durch digitale Signaturen. Diese Entwicklungen haben dazu geführt, dass heute ein Spektrum von PKI-Domänen existiert, deren funktionelle und technische Interoperabilität und Vergleichbarkeit im Policy-Bereich einfache hierarchische Netzstrukturen ausschließt. Die Anforderungen an die Infrastruktur sind gegenüber dem Basis-Konzept noch wesentlich komplexer geworden: Neben der Verwaltung der Zuordnung öffentlicher kryptographischer Schlüssel zu Namen von Personen oder Instanzen ist auch die Chipkartenpersonalisierung und ihr Lebenszyklus zu managen.

Generell ist es bisher nicht gelungen, ein Spektrum von nützlichen Anwendungen zu etablieren, die für den ‚Normalverbraucher' ein Äquivalent für die anteiligen Infrastrukturkosten (Chipkarte, Zertifikate, technische Zusatzgeräte, Performanceeinbußen) und die Bereitschaft, der vertrauenden Partei einen Sicherheitsvorteil zu verschaffen, darstellen. Dieses Problem wird von vielen Autoren betrachtet und es wird immer wieder versucht, Wege aufzuzeigen, mit denen ein Durchbruch bei der Nutzung dieser Technologie potentiell möglich wäre.

Laut Eckert sei beispielsweise „[e]in wichtiger Hinderungsgrund [...] für das Fehlen von auf breiter Basis ausgerollten Signaturkarten [...] die damit verbundenen erheblichen Kosten [...], die auch die Banken (zum Beispiel EC-Karte als Signaturkarte) nicht bereit sind, zu übernehmen“ [Eckert 2006]. Neue Impulse erwartet Eckert durch die Einführung der elektronischen Gesundheitskarte sowie durch den Elektro-

nischen Einkommensnachweis „ELENA“, der es ab 2010 ca. 35 Mio. Arbeitnehmern in Deutschland ermöglichen soll, elektronische Verwaltungs- und Geschäftsvorgänge qualifiziert zu signieren. ELENA könnte damit laut Eckert zur „langersehnten Killeranwendung“ für elektronische Signaturen werden (Vgl. [Eckert 2006]).

Nach Wiegel ist eine ganze Reihe von Gründen für das Scheitern der PKI verantwortlich. Zum einen würde ein firmenweites Roll-out vor allem mit hohen organisatorischen Hürden konfrontiert werden. Zum anderen führt vor allem die umständliche Bedienung dazu, dass Endnutzer abgeschreckt werden. Darüber hinaus ist aus betriebswirtschaftlicher Sicht der Nachweis, dass sich Investitionen in eine PKI lohnen, sehr schwierig (Vgl. [Wiegel 2005]). Diese Problematik wird in den Kapiteln zu den wirtschaftlichen Betrachtungen der PKI und ihren Nutzungsbedingungen noch näher erläutert. Wiegel sieht vor allem im externen Key Management das anwenderseitige Problem, denn die „Anwendung von Sicherheitsfunktionen mit Benutzung des eigenen private keys – Authentifizierung, Signieren und Entschlüsseln – bereitet dem Endbenutzer in der Regel keine Probleme“ [Wiegel 2005]. Demgegenüber seien Sicherheitsfunktionen, die die Verwendung öffentlicher Zertifikate oder Public Keys benötigen, für den Endbenutzer in der Regel umständlich, da die Vertrauensregelung für eben diesen schwer nachzuvollziehen ist (Vgl. [Wiegel 2005]).

Das größte Problem nach Rossnagel ist bei der Anwendung elektronischer Signaturen die ungleiche Verteilung von Kosten und Nutzen. Der Endnutzer trage die Kosten, habe aber nichts davon. Demgegenüber trage die öffentliche Verwaltung keine Kosten, habe aber den größten Nutzen (Vgl. [Rossnagel 2006]). Versuche, ein Geschäftsmodell zur entwickeln, das diesem Befund entgegenwirkt, sind allerdings bisher gescheitert (Vgl. [SigBü 2005]). Um das Akzeptanzproblem der PKI zu lösen, müsse man nach Rossnagel vor allem die „early adopters fokussieren“ [Rossnagel 2006].

Drastischer formulieren Clarke und Nash die Probleme der PKI. Laut Clarke ist die „konventionelle PKI um den ISO Standard X.509 ein substanzieller Fehlschlag“ [Clarke 2001]. Als Gründe hierfür sieht Clarke die „enorme Komplexität und die hohen Kosten“ [Clarke 2001].

Nash führt als hauptsächlichen Hinderungsgrund die „bestenfalls mangelhafte“ Integration von PKI in Applikationen an. Infrastrukturen seien nutzlos, „bis sie Applikationen haben, die sich sinnvoll darin integrieren lassen und die in der Infrastruktur zur Verfügung stehenden Dienste effektiv nutzen“ [Nash 2001]. Grund für die mangelhafte Integration könnten die flexiblen Vertauensmodelle sein. Zu diesem Thema regen die Autoren weitere Untersuchungen an.

Schultz sieht dagegen in den Implementierungen das größte Problem, die „wie fast alles, das aus der Welt der Informationssicherheit kommt“, zu kompliziert seien. „Wenn PKI nicht einfacher nutzbar wird, wird es nicht ein Teil der Cyberwelt werden, in der wir leben“ [Schultz 2002].

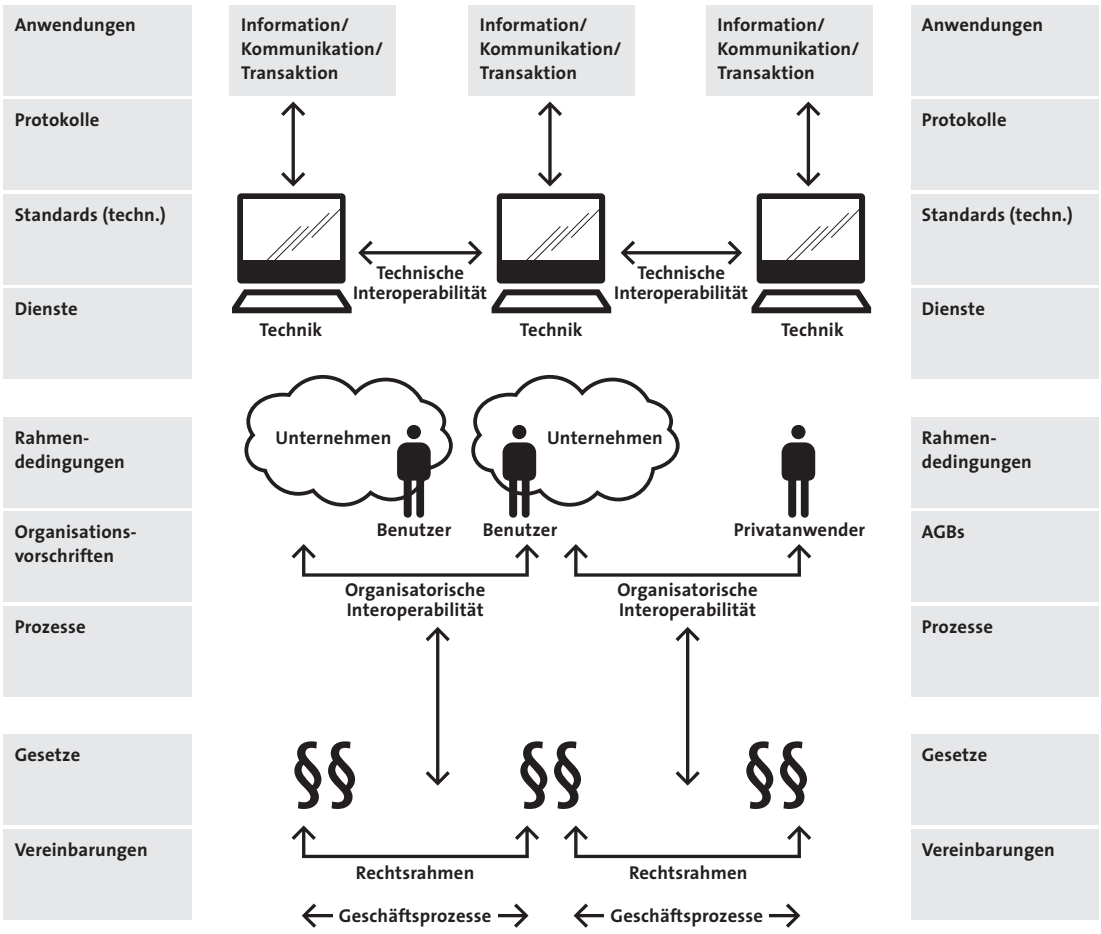


**Abbildung 1.1: Komplexer Hintergrund von PKI-gestützten Geschäftsprozessen**

Als mögliche Lösung für das Akzeptanzproblem der PKI wird häufig die Transparenz der verwendeten Verfahren genannt. „Um dauerhaft erfolgreich zu sein", so beispielsweise Nash, „muss sich PKI so gut in Geschäftssoftware integrieren lassen, dass die Anwesenheit von PKI transparent ist." Die wichtigsten Bereiche, die laut Nash angesprochen werden müssen, seien „Bedienerfreundlichkeit, Transparenz der zugrunde liegenden Infrastruktur für die Applikationen und Benutzer sowie weitgehende Interoperabilität." Denn wie bei jeder guten anderen Infrastruktur funktioniere PKI am besten, wenn man sie so gut wie gar nicht sieht (Vgl. [Nash 2001]).

Die im Rahmen dieser Studie geführten Experteninterviews spiegeln diese Aussagen wider. Die Daseinsberechtigung von Public Key Infrastrukturen wird nicht in

Frage gestellt. Allerdings betont die Mehrheit der Experten, dass es bisher an Killeranwendungen bzw. Enablern fehle (Vgl. [Buchmann 2006], [Busch 2006]).

Laut Pohlmann fehlen die großen Anwendungen und die Infrastrukturen. Die täglichen Hürden in der Umsetzung seien viel zu groß (Vgl. [Pohlmann 2007]). PKI könne sich nach Meinung von Busch sehr gut in Devices integrieren lassen, die bereits eine breite Anwendung finden wie beispielsweise Handys. Dies würde die Akzeptanz steigern.

In den geführten Interviews wird auch immer wieder betont, dass PKI Anwendungen für den Nutzer transparent sein müssen, um akzeptiert zu werden. „PKI funktioniert am besten, wenn der Nutzer vor ohnehin schwer bewertbaren Fragen bewahrt wird", so Temple (Vgl. [Temple 2006]). Weitgehende Transparenz in dem Sinne, dass die Vertrauensmodelle und -beziehungen klar nachvollziehbar sind, ist gerade förderlich für Awareness und Problembewusstsein. Transparenz bedeutet nicht, Komplexität zu verstecken, sondern letztendlich sie auszuräumen.

Generell, so Bart Preneel, sei die PKI „overhyped" worden. Sie sei schließlich keine universelle Lösung für alles. Ganz im Gegenteil hätte die PKI alle Grunderwartungen erfüllt (Vgl. [Preneel 2006]).

Auch Pohlmann sieht das eigentliche Problem darin, dass PKI überinterpretiert wird. Sie sei eine Infrastruktur, die man braucht, mehr aber auch nicht (Vgl. [Pohlmann 2007]). Für Beutelspacher stellt vor allem die extreme Komplexität der PKI den schwerwiegendsten Hinderungsgrund für ihren großflächigen Einsatz dar. So sollten das X. 509-Protokoll als PKI Grundlage sowie die erforderlichen Chipkarten-Infrastrukturen und -Hilfsprozesse vereinfacht werden. Darüberhinaus würden virtuelle Anwendungen mit scheinbar idealen Sicherheitseigenschaften nicht weiterhelfen. Stattdessen sollte vernünftiges Risk-Management betrieben werden (Vgl. [Beutelspacher 2007]), um anwendungsbezogene robuste und pragmatisch sichere PKI-Lösungen mit geringeren technischen und organisatorischen Aufwänden auszuwählen.

Weil PKI-Konzepte auf Grundlage der bestehenden Standards einen sehr komplexen Charakter haben, sind eine Reihe von einfacheren Lösungen verbreitet. Eine dieser Lösungen ist zum Beispiel PGP. Im klassischen Sinne nutzt dieses Verfahren das Web of Trust, einen „anarchischen Ansatz, der die Vertrauensstruktur der ungeordneten Internet-Gemeinde nachbildet" [Kirsch 2001] und „damit den Bedarf an professionellen CAs umgeht, da jeder selbst Zertifikate ausstellen kann" [Clarke 2001]. Während das Web of Trust für die private Nutzung viele Vorteile gegenüber einer X.509-Hierarchie bietet, ist es laut Kirsch allerdings für die Nutzung durch Unternehmen weniger geeignet (Vgl. [Kirsch 2001]).

Eine Vereinfachung gegenüber X.509 stellt die Simple Public Key Infrastructure (SPKI/SDSI) dar. Eine wesentliche Grundlage dieses Verfahrens bilden Zertifikate

mit lokalen Namen, da sich laut Schmeh global eindeutige Namen als Bestandteil eines digitalen Zertifikats als unpraktisch erwiesen haben. Nach diesem Konzept soll jeder Anwender den öffentlichen Schlüssel eines anderen Anwenders mit einem selbstgewählten Namen oder einer Eigenschaft in Verbindung bringen (Vgl. [Schmeh 2001]). SPKI/SDSI spielt in der Praxis bisher nur eine untergeordnete Rolle.

Eine weitere Möglichkeit der Vereinfachung bietet die Cross Zertifizierung. Cross-Zertifikate oder auch Mehrfachzertifikate liegen dann vor, wenn mehr als ein Nutzer ein Subject zertifiziert und dienen zum einen der Verknüpfung von Zertifizierungshierarchien sowie zum anderen der Verkürzung von Zertifikatketten (Vgl. [Hammer 2001]).

## 1.6 Alternative Konzepte

Als mögliche Alternativen zur PKI können zum einen symmetrische Verschlüsselungsverfahren, die im Gegensatz zur asymmetrischen Kryptographie nur mit einem Schlüssel arbeiten, zum anderen Hybridzertifikate oder auch alternative Infrastrukturen wie beispielsweise PGP angesehen werden. Als alternatives Authentifizierungsverfahren soll zudem die Biometrie diskutiert werden.

### 1.6.1 Symmetrische Verschlüsselungs- und Key Management-Verfahren

Asymmetrische Verfahren bieten zwar eine Vielzahl von Vorteilen, aus Performancegründen spielen heute aber immer noch die symmetrischen Verfahren eine große Rolle (Vgl. [Beutelspacher 2006]). Diese sind laut Eckert von einer großen praktischen Relevanz, da die verwendeten Ver- und Entschlüsselungsalgorithmen auf sehr einfachen Operationen basieren, die effizient in Hard- und Software implementierbar sind (Vgl. [Eckert 2006]).

Lange wurde der bereits 1976 vom NIST (USA) definierte Data Encryption Standard (DES) für die symmetrische Verschlüsselung genutzt. Der gesamte Schlüsselraum besitzt aber nur eine feste Größe von 56 Bit, was nach dem Stand der heutigen Technologie nicht mehr ausreichend ist. Die effektive Schlüssellänge von DES wurde übergangsweise aufgewertet (TripleDES), so dass auf dieser Grundlage noch ausreichende Sicherheit für ‚nichtklassifizierte' US-Verwaltungsdokumente und internationale Finanztransaktionen gewährleistet ist. Der Advanced Encryption Standard (AES), der mit Hilfe des Rijndael Algorithmus realisiert wird, wurde als Nachfolger von DES in einem internationalen Expertenverfahren ausgewählt. Sein einziger Nachteil sei laut Bruce Schneier, „die Schwierigkeit der korrekten Aussprache“ [Schneier zitiert nach Eckert 2006.] 1985 wurde X9.17 eingeführt. Ein Standard, der für das Key Management mit symmetrischen Schlüsseln im Bankenbereich gilt.

Ein wichtiges Protokoll, das breite Anwendung im Bereich der Nutzerauthentifizierung findet, ist das Kerberos Protokoll. Es stellt einen verteilten Authentifizierungsdienst auf Basis von symmetrischer Kryptographie zur Verfügung. Es erfolgt keine Übertragung von Passwörtern und erlaubt Single Sign On. Für Kerberos stand ein dreiköpfiger Hund aus der griechischen Mythologie (Cerberus) Pate, der den Eingang zur Unterwelt überwacht. Aufbauend auf diesem Bildnis stellt die Kerberos-Architektur eine Trusted Third Party zur Verfügung: den Kerberos-Server, der das Key Distribution Center (KDS) zur Schlüsselgenerierung und -verwaltung für eine Kerberos-Session, den Authentication Server (AS) und den Ticket Granting Server (TGS) enthält und als Vertrauensinstanz für Server und Clients fungiert. Der große Vorteil von Kerberos liegt in dem kompletten Verzicht auf asymmetrische Verschlüsselung. „Allerdings stellen die zentralen Server einen idealen Angriffspunkt dar" [Schmeh 2001].

Breite Anwendung finden symmetrische Key Management Systeme im Mobilfunkbereich sowie für die Verschlüsselung von Kabel- und Satelliten TV. Sie ermöglichen ebenfalls sehr effektive Authentisierungsverfahren.

### 1.6.2 Hybride Verfahren

Hybride Verschlüsselungsverfahren zielen darauf ab, den Verschlüsselungsaufwand und die langsame De- und Entchiffrierung der asymmetrischen Verschlüsselung zu kompensieren. Dabei werden die Vorteile der symmetrischen Verschlüsselung mit denen der asymmetrischen Verschlüsselung kombiniert. Dies entspricht also im metaphorischen Sinn einer Hochzeit zwischen der hohen Bearbeitungsgeschwindigkeit durch schnelle Algorithmen aus der Familie der symmetrischen Verschlüsselung mit dem öffentlichen Schlüsselaustausch der asymmetrischen Kryptographie. Hybride Verschlüsselungsverfahren betreiben den Nachrichtenaustausch mit symmetrischer und im Gegensatz dazu den Schlüsselaustausch mit asymmetrischer Verschlüsselung. Alle wichtigen Protokolle wie SSL oder S/MIME arbeiten mittlerweile mit hybriden Verfahren.

### 1.6.3 Biometrie

#### 1.6.3.1 Biometrische Authentifizierung

Authentifizierung im Zusammenhang mit Biometrie bedeutet „Bezeugung der Echtheit" [TeleTrusT 2006]. Biometrische Verfahren werden hauptsächlich zur Realisierung von Authentifikationsmethoden eingesetzt. Im Gegensatz zu traditionellen Authentifikationsverfahren benutzt die Biometrie physiologische oder verhaltenstypische Charakteristiken des Teilnehmers zur Authentifikation des Benutzers. Es werden somit personengebundene und nicht nur personenbezogene Merkmale erfasst (Vgl. [TeletrusT 2006]).

Nach Donnerhacke ist die Biometrie ein sicheres Mittel zur Authentifizierung. Schlüssel und Passworte dagegen dienen nur der Autorisierung. „Der Unterschied mag klein sein, aber er ist wesentlich: Authentifizierung ist personengebunden, Autorisierung hingegen kann übertragen werden" [Donnerhacke 1999].

Jueneman ist allerdings der Meinung, dass biometrische Techniken zwar eine exzellente Möglichkeit liefern, den physischen Zugang zu lokalen Netzwerken zu kontrollieren oder zu authentifizieren, aber biometrische Verfahren alleine reichen, beispielsweise nicht aus, so Jueneman, um den Verfasser oder den Inhalt eines elektronischen Dokuments sicher zu authentifizieren (Vgl. [Jueneman 1998]).

Biometrische Authentifizierung ist daher nur als sicher zu bewerten, wenn sie mit einer bestehenden Form der Authentifizierung wie beispielsweise PIN, Passwort, Smart Card kombiniert wird, und damit letztendlich eine mehrstufige Authentifizierung erzielt wird (Vgl. [Nash 2001]). Am sichersten ist dabei die dreistufige Authentifizierung, die biometrische Daten, eine Smart Card und den PIN Code zum Entsperren der Smart Card umfasst. Allerdings gibt Nash zu bedenken, dass ein solches Verfahren zwar die Sicherheit des Systems steigert, aber nicht die Benutzerfreundlichkeit (Vgl. [Nash 2001]).

#### 1.6.3.2 Biometrische Identifikation

Laut Kriterienkatalog zur Bewertung biometrischer Verfahren von TeleTrusT werden bei der Identifikation in der Biometrie die aktuellen biometrischen Daten einer Person erfasst und mit den im Vorfeld erfassten biometrischen Referenzdaten einer Vielzahl von Individuen verglichen (1:n-Vergleich). Diese Referenzdaten sind beispielsweise in einer Datenbank gespeichert. Es findet somit eine Vielzahl von Vergleichen statt. Die Person wird als dasjenige Individuum identifiziert, dessen biometrischer Referenzdatensatz mit dem aktuellen biometrischen Datensatz der Person innerhalb der gewählten Toleranzgrenzen übereinstimmt (Vgl. [TeleTrusT 2006]).

Nach Krause basieren alle Probleme heutiger biometrischer Identifikation und Authentifikation letztlich auf der Tatsache, dass die Datenverarbeitungsgeschwindigkeit gängiger (somit bezahlbarer) Computersysteme noch nicht genügt, um ausreichende Datenmengen in der gewünschten Geschwindigkeit zu verarbeiten. Krause bezeichnet diesen Umstand als das primäre Problem der Biometrie (Vgl. [Krause 2005]). Darüber hinaus kann die Biometrie trotz des hohen technischen Niveaus laut Krause mit den meisten herkömmlichen Verfahren derzeit noch nicht konkurrieren, und auch Feldversuche mit den unterschiedlichsten Biometrieverfahren führten noch nicht zu befriedigenden Ergebnissen (Vgl. [Krause

7 Die „Falschrückweisungsrate (false rejection rate) [...] [bezeichnet den] (meist prozentuale[n]) Anteil fälschlich zurückgewiesener Berechtigter" [TeleTrusT 2006].

2005]). Dies zeigt unter anderem auch die durch das BSI im Jahr 2004 mit 13 verschiedenen Fingerprintsensoren durchgeführte Studie BioFinger, bei der die Mehrheit der „Prüflinge" eine False Rejection Rate (FRR)[7] von über 3% aufwies (Vgl. [BioFinger 2004]).

#### 1.6.3.3 Bewertung biometrischer Verfahren

In der Literatur sowie in den im Rahmen dieser Studie geführten Interviews lassen sich verschiedene Trends zur Bewertung von Chancen und Risiken der Biometrie finden. Die Vorteile der Biometrie werden generell in der bequemen Nutzung gesehen sowie in der Tatsache, dass biometrische Merkmale wie etwa im Vergleich zu Passwörtern nicht vergessen oder gestohlen werden können (Vgl. [Sukhai 2004]).

Graevenitz sieht die Vorteile der Biometrie gegenüber herkömmlichen Authentifizierungsverfahren vor allem in der höheren Sicherheit, der Bequemlichkeit, der einfachen Bedienbarkeit, der Schnelligkeit und dem damit verbundenen höheren Komfort. Insbesondere entfalle die Notwendigkeit, sich Kennwörter oder PINs zu merken. Bei einer möglichen Substitution von wissensbasierten Authentifizierungssystemen durch biometrische Verfahren wird darüber hinaus der administrative Verwaltungsaufwand von PIN und passwortgestützten Verfahren eliminiert (Vgl. [Graevenitz 2006]).

Pohlmann stellt neben der erhöhten Sicherheit und der Vereinfachung für den Benutzer vor allem auch die Zukunftsausrichtung der Biometrie heraus, die dem Anwender eine hohe Investitionssicherheit biete (Vgl. [Pohlmann 2003]).

Demgegenüber sehen viele Experten vor allem in den hohen Kosten der biometrischen Authentifizierung einen großen Nachteil. Zudem wird häufig das Fehlen von Standards bemängelt, die die Interoperabilität der verschiedenen Devices ermöglichen würden (Vgl. [Albrecht 2001]).

Laut Chandra ist die Biometrie alleine als Informationssicherheitsmechanismus nicht ausreichend. Sie muss stattdessen mit anderen Komponenten verbunden bzw. in andere Mechanismen integriert werden (Vgl. [Chandra 2005]). Chandra sieht ebenfalls das Problem der hohen Kosten, die durch die Implementierung von biometrischen Verfahren verursacht werden. Außerdem weist er darauf hin, dass die bestehenden Standards im Matching Prozess äußerst unpräzise seien. Das größte Problem der Biometrie ist laut Chandra allerdings das fehlende Vertrauen der Endanwender in die Technologie. Die Lösung könnten hier Trusted Third Parties sein, die beispielsweise die Sicherheit und Integrität von biometrischen Datenbanken verifizieren (Vgl. [Chandra 2005]).

Graevenitz sieht vor allem in der Fälschungsanfälligkeit, der mangelnden Überwindungssicherheit und den hohen Fehlerraten wesentliche Schwächen von biometrischen Verfahren. Dies ist insbesondere zurückzuführen auf die mangelnde

Genauigkeit der Verfahren. Außerdem sei die Differenz zwischen Komfort und Sicherheit biometrischer Verfahren sehr hoch. Laut Graevenitz verhalten sich Komfort und Sicherheit sogar „umgekehrt proportional zueinander" [Graevenitz 2006].

Auch Bruce Schneier steht der Biometrie eher skeptisch gegenüber und formuliert das Kernproblem dieser Technologie: „Biometrische Merkmale sind keine Geheimnisse, sie werden überall hinterlassen. Sobald ein biometrisches Merkmal gestohlen wurde, bleibt es für den Rest des Lebens unbrauchbar" [Schneier 1999].

Laut Kriterienkatalog für biometrische Verfahren von TeleTrusT muss die Handhabung biometrischer Systeme durch ihre Nutzer geprägt sein von Einfachheit, Schnelligkeit, Bequemlichkeit, Ergonomie der Anwendergeräte und der Übertragbarkeit der Zugangsberechtigungen im Arbeitsalltag (Vgl. [TeleTrusT 2006]).

#### 1.6.3.4 Perspektiven

Grundlegende Aussagen zur Leistungsfähigkeit biometrischer Verfahren in IT-Anwendungen wurden bereits durch die Projekte BioTrusT (Vgl. [BioTrusT 2002]) und ROBIN (Vgl. [Bong 2005]) gewonnen. Demnach wird die Sicherheit bei der Authentifizierung von Mitarbeitern sowie beim Datentransfer durch den Einsatz von biometrischen Verfahren in Kombination mit Smart Cards deutlich erhöht. Allerdings hat sich die Integration in unterschiedliche Einsatzumgebungen wie Einzel-PCs oder Firmennetzwerke als sehr aufwendig sowohl für Hersteller als auch Betreiber erwiesen, was auf die hohe Komplexität des internationalen Industriestandards BioAPI zurückzuführen ist.

Die im Rahmen der vorliegenden Studie befragten Experten bemängelten die Tatsache, dass es momentan an einem Enabler oder einer Killeranwendung für biometrische Verfahren fehle. Wie bei der PKI könnte auch hier ein Device nutzbar gemacht werden, das im Alltag der Anwender breite Akzeptanz findet wie beispielsweise das Handy (Vgl. [Busch 2006]). Allerdings fehle es ebenfalls an Standards, die die Interoperabilität der verschiedenen Lösungen ermöglichen (Vgl. [Busch 2006]).

Pohlmann und Leitold stellen dagegen klar, dass die Sicherheit biometrischer Verfahren nicht zu 100% gegeben sei. Leitold ergänzt allerdings, dass dort, wo Biometrie mit Smart Cards kombiniert würde, ein sicherer Einsatz möglich sei (Vgl. [Leitold 2006], [Pohlmann 2007]).
Auch Paar relativiert die Sicherheitsproblematik biometrischer Verfahren, denn in der Theorie sei die Biometrie zwar überwindbar, aber in der Praxis biete ein mittelschwaches Biometriesystem zusammen mit einem mittelprächtigen Passwort bereits eine hohe Sicherheit (Vgl. [Paar 2007]).

Preneel erachtet den Einsatz von biometrischen Verfahren immer dort als sinnvoll, wo eine gewisse FAR[8] tolerabel ist, also bei rein lokalen Anwendungen (Vgl. [Preneel 2006]). Cardholm sieht die Zukunft der Biometrie langfristig im Ersatz für Pass-

wörter, als Ersatz für digitale Signaturen sei sie allerdings ungeeignet (Vgl. [Cardholm 2006]).

Um der Biometrie als Authentifizierungs- und Identifikationsverfahren zur breiten Anwendung zu verhelfen ist nach Ansicht von Graevenitz die Implementierung von biometrischen Technologien durch Regierungen unvermeidbar und notwendig. Die anfänglichen und initialen Anwendungen wie biometrische Grenzkontrolle anhand von biometrischen Pässen oder eGovernment Anwendungen werden zur Folge haben, dass sich Biometrie zukünftig auch bei kommerziellen und zivilen Anwendungen durchsetzt, wobei die biometrischen Verfahren immer nur ein Teil eines gesamten Sicherheitskonzeptes sein können. Insofern sei davon auszugehen, dass Biometrie sich zukünftig im alltäglichen Leben durchsetzen wird. (Vgl. [Graevenitz 2006]). Als mögliches Anwendungsszenario beschreibt Graevenitz den Einsatz von biometrischen Merkmalen bei Wahlen. Zum einen könne mit derartigen Systemen die wahre Identität des Wählers festgestellt werden, zum anderen sei es möglich, Wahlbetrug durch Mehrfachstimmen von Personen zu vermeiden (Vgl. [Graevenitz 2006]).

## 1.7 Evaluierung

Nach Schmeh ist Sicherheit ist „ein höchst abstraktes Gut und damit nicht messbar". Oftmals ist es aber wünschenswert die Sicherheit eines Systems zu messen bzw. zu beweisen. Obwohl sich Sicherheit nicht messen lässt, wurde nach Methoden gesucht Software und Systeme in Bezug auf Sicherheit, „anhand festgelegter Kriterien in eine bestimmte Sicherheitsstufe einzuordnen." Diese Einordnung wird von staatlichen Behörden, wie dem Bundesamt für Sicherheit in der Informationstechnik, durchgeführt. Die Überprüfung der Erfüllung der vorgegebenen Kriterien heißt Evaluierung. Erhält das evaluierte Produkt eine Urkunde, heißt dieser Vorgang Zertifizierung (Vgl. [Schmeh2001]).

Laut Savola ist die Evaluierung der Sicherheit von Systemen abhängig von den Erfahrungen von Sicherheitsexperten. Um die Evaluierung effizienter zu gestalten sei ein automatisierter Ansatz notwendig. Savola behauptet, es gäbe derzeit keinen praktischen Ansatz für eine Evaluierung auf systematische Art und Weise. Er stellt einen ganzheitlichen Ansatz (Framework) vor, welcher auf „security behavior modelling" und „security evidence collection" basiert. Das Prozessmodell zur Sicherheitsevaluierung enthält folgende Schritte:

1. Risiko- und Bedrohungsanalyse
2. Sicherheitsanforderungen definieren
3. Sicherheitsanforderungen priorisieren

8 Die „Falschakzeptanzrate ([FAR -] false acceptance rate) [...] [bezeichnet den] (meist prozentuale[n]) Anteil fälschlich zugelassener Unberechtigter" [TeleTrusT 2006].

4. Sicheres Verhalten modellieren
5. Beweise sammeln
6. Wahrscheinlichkeiten für Aktionen bestimmen
7. Ergebnisse zusammenfassen
(Vgl. [Savola 2006])

Nach Rottke existiert ein steigender Bedarf an Zertifizierung der Sicherheit von Systemen auf Basis der Common Criteria (CC). Die CC enthalten die Bedingungen, die sichere Systeme erfüllen müssen, helfen aber nicht bei deren Entwicklung sicherer Systeme. Rottke stellt eine Methode für Requirement Engineering und Modellierung von Systemen für die höhere Evaluierung nach CC vor (Vgl. [Rottke 2002]).

Die Evaluierungen nach CC sind sehr kosten- und zeitintensiv. Eine Evaluierung macht keinen Sinn, wenn sie länger dauert, als ein System am Markt ist (z.B. bei Mobiltelefonen) (Vgl. [Leitold 2006]). Die Kosten und die benötigte Zeit ist abhängig von der Verfügbarkeit korrekter Entwicklerdokumentationen, der Komplexität der Software und die Wiederverwendbarkeit früherer Evaluierungen. Das Ziel des von ihm vorgestellten CC-SEMS (CC Security Mangement System) ist ein praktischer Evaluierungs-Leitfaden, der einen Beitrag zur Automation der Evaluierung und für das Management des Evaluierungsprozesses leisten soll (Vgl. [Bang 2006]).

Cardholm hält die CC für zu komplex und hemmend. Für einen breiten Einsatz sollten sie eher in allgemeine Zertifizierung, wie ISO 27000 mit einbezogen werden (Vgl. [Cardholm 2006]). Für Preneel bieten CC dagegen klare Regeln und Protokolle, sind ein gutes Marketing-Tool, erzeugen aber viel Paperwork. Preneel nimmt, ähnlich wie Cardholm an, dass sich der Markt eher in Richtung einfacher Lösungen entwickelt (Vgl. [Preneel 2006]). Nach Temple können CC bei der Vertrauensbildung helfen, sind aber teuer und unflexibel. Als Alternative schlägt Temple Risikomanagement vor (Vgl. [Temple 2006]).

## 1.8 Zusammenfassung

Das Kapitel „Technische Perspektiven“ befasst sich im Schwerpunkt damit, wie kryptobasierte Anwendungen (PKI) für Identifikation, Authentifizierung und Signaturen hinsichtlich ihrer investitionssicheren Integrierbarkeit in elektronische Geschäftsprozesse zu bewerten sind. Hauptaugenmerk wurde darauf gelegt, die langjährigen Erfahrungen von IT-Sicherheitsexperten und die daraus resultierende Sicht auf permanent unsichere Kryptoverfahren und ihre schwachstellenbehaftete Implementierung an den praktisch vorliegenden Sicherheitserfahrungen zu spiegeln. Dabei hat sich ergeben, dass Erfolg und Wirksamkeit von PKI-Implementierungen nicht durch Lücken im Technologieangebot beeinflusst werden.

Die Ziele für die notwendige und praktisch erreichbare Sicherheit von Geschäftsprozessen sind jedoch nur durch ein fundiertes Risikomanagement unter beson-

derer Beachtung des Nutzers zu bestimmen. Wichtige Schlussfolgerungen bestehen darin, dass die Interoperabilität von Sicherheitslösungen in Anwendungsumgebungen unverzichtbar ist und dass ihre Implementierungen nicht durch starre Vorgaben oder technologienahe Regulierungen behindert werden dürfen.

Aspekte einer risikobewerteten Investitionssicherheit und der Nutzerakzeptanz haben Vorrang bei einer PKI-Einführung. Bewährte und neue Technologien sollen dabei flexibel verwendet werden. Wegen des hohen Innovationstempos bei den hier betrachteten Anwendungen für Identifikation, Authentifizierung und Signaturen können ihre quantitativen Sicherheitseigenschaften nicht generell vor ihrem Einsatz vollständig evaluiert werden. Eine fortlaufende Risikobewertung der Anwendungen wird empfohlen und dient auch der Ermittlung von praktisch relevanten Sicherheitslücken im Prozess und bei den verwendeten Technologien. Demzufolge sollte als ein grundlegendes Element für eine investitionssichere PKI-Einführung, eine auf Standardschnittstellen beruhende Migrationsstrategie für Sicherheitslösungen vorliegen.

# 2.

# Betriebswirtschaftliche Betrachtungen

## 2.1 Methodik

Dieses Kapitel befasst sich mit betriebswirtschaftlichen Aspekten des PKI-Einsatzes. Es wird untersucht, ob und wann ein erfolgreicher Einsatz aus dieser Sicht begründet werden kann.

Hierzu wurde zuerst geprüft, ob es Konzepte oder Anwendungen gibt, die eindeutig als PKI-Einsatzszenarien identifizierbar sind. Anhand verschiedener Kriterien, die durch Literaturrecherchen und Erkenntnisse aus der Praxis entwickelt werden konnten, wurde eine Klassifikation herausgearbeitet und in projektinternen Diskussionen überprüft.

Im Anschluss daran wurden am Beispiel der FH Brandenburg Server- und Benutzerzertifikate untersucht. Es sollte festgestellt werden, ob und inwieweit ein PKI-Einsatz vor allem auf Geschäftsprozessebene zu betrachten ist. Desweiteren galt es zu prüfen, ob PKI eine Enabler-Funktion zugesprochen werden kann. Dazu wurden Interviews mit Verantwortlichen durchgeführt, um sowohl die Erfolgskriterien als auch die betriebswirtschaftlichen Hintergründe zu erkennen.

Im Rahmen des von uns durchgeführten Workshop (siehe hierzu auch Kapitel Workshop-Ergebnisse) wurde klar, dass der Ansatz der Geschäftsprozessorientierung zur

Zeit wenig praxisrelevant ist. Der PKI-Einsatz wird als Infrastrukturinvestition verstanden. Auf dieser Grundlage wurde im Projekt weiter untersucht, mit welchen Kennzahlen sich eine Investitionsentscheidung begründen ließe. Aus der Vielzahl an betriebswirtschaftlichen Kennzahlenverfahren wurden jene näher betrachtet, die in der Praxis allgemein akzeptiert und angewendet werden. Dabei wurde Wert darauf gelegt, dass sowohl quantitative als auch qualitative Aspekte betrachtet werden. Anhand realer, anonymisierter Unternehmensdaten wurde darauf aufbauend eine beispielhafte Kosten-Nutzen-Betrachtung durchgeführt.

Dieser Schritt führte zu der Erkenntnis, dass nur eine Kombination verschiedener Kennzahlenverfahren ein ganzheitliches Bild liefert, mit denen dann eine Investitionsentscheidung umfassend und realitätsorientiert begründet werden kann.

## 2.2 Einsatzszenarien

### 2.2.1 Zielstellung

Als Grundlage für eine Untersuchung von Erfolgskriterien ist es erforderlich, geeignete PKI-Einsatzszenarien zu finden. Hiermit soll geklärt werden, ob es möglich ist, einen direkten Zusammenhang zwischen diesen PKI-Szenarien und erfolgreichen Anwendungen herzustellen. Zuvor muss allerdings untersucht werden, ob und inwieweit, sich PKI-Szenarien anhand geeigneter Kriterien klassifizieren lassen.

### 2.2.2 Klassifikationsansätze

Aufgrund der Vielzahl möglicher Szenarien für den Einsatz von Signatur-, Identifizierungs- und Authentisierungsverfahren muss eine Einschränkung getroffen werden. Deshalb werden im Folgenden die beteiligten Akteure, die zu sichernden Schutzziele und die Stakeholder betrachtet und untersucht, inwieweit sie einen eindeutig feststellbaren Einfluss auf Auswahl und den Erfolg beim Einsatz von PKI-Anwendungen haben.

#### 2.2.2.1 Klassifikation nach beteiligten Akteuren

Der erste Ansatz von PKI-Einsatzszenarien untersucht die beteiligten Akteure. Anlehnend an die Begriffe zur Speicherung und Verarbeitung von Informationen in IT-Systemen werden diese in Subjekte und Objekte unterteilt. Als Subjekte werden in diesem Zusammenhang natürliche und juristische Personen verstanden. Objekte sind Komponenten von IT-Systemen (Hardware, Software, Dateien, Prozesse).[1] Hieraus ergeben sich die folgenden drei unterschiedlichen Klassifizierungsansätze.

1 In der IT-Sicherheit unterscheidet man auch zwischen passiven und aktiven Objekten (vgl. [Eckert 2005], S. 2f.). Dieser Unterschied wird in der hier dargestellten Betrachtung nicht verwendet.

**Subjekt – Subjekt**
In einer Subjekt-Subjekt-Beziehung identifizieren und authentisieren sich (natürliche u/o juristische) Personen gegenseitig. Dies erfolgt über Eigenschaften des zu Identifizierenden oder den Besitz von im weitesten Sinne Gegenständen, die das Subjekt gegenüber anderen identifiziert. Natürliche Personen authentisieren sich gegenseitig durch biometrische Merkmale (Eigenschaft), juristische Personen durch Besitz, z.B. einen Handelsregisterauszug. Die Authentisierung von natürlichen zu juristischen Personen kann sowohl durch Eigenschaft, z.B. durch Augenschein, als auch Besitz, z.B. Ausweis, erfolgen. In elektronischen Prozessen werden digitale Unterschriften[2] verwendet.

Typische Anwendungsfälle für elektronische Subjekt-Subjekt-Beziehungen sind z.B. E-Mail, Instant-Messaging, Voice over IP (VoIP) oder der Austausch von Dokumenten und Verträgen. Der Einsatz von asymmetrischer Verschlüsselung kann hierbei mit verschiedenen Technologien umgesetzt werden. Dabei spielen unterschiedliche Vertrauensmodelle eine Rolle .[3]

**Subjekt – Objekt**
In dieser Beziehung agieren Personen mit Komponenten eines IT-Systems (Objekte). Die Identifizierung des Subjektes erfolgt durch eine eindeutige Benutzerkennung, die Authentisierung mittels Passwort/PIN oder sonstiger, beispielsweise auch biometrischer Merkmale. Objekte werden im einfachsten Fall über Adressen (bspw. MAC-Adresse) oder sonstige Gerätekennzeichnungen, bei der Verwendung höherer Sicherheitsniveaus mittels kryptografischer Verfahren authentisiert (z.B. Web-Server mittels SSL-Zertifikat). In den meisten Fällen identifizieren/authentisieren sich Personen gegenüber technischen Systemen, aber nicht umgekehrt!

Die Anwendungsfälle hierfür sind sehr vielfältig: Standardanwendungen im Client/Server-Betrieb in einem Unternehmen, z.B. (smartcardbasiertes) Login an Rechnersystemen, diverse Internetangebote, z.B. Kauf in Internet-Shops oder Online-Banking mittels TAN oder HBCI sowie Angebote der sog. Virtuellen Verwaltung (Bürgeramt, Finanzamt, Hochschule etc.) inkl. elektronischer Steuererklärung oder Online-Wahlen, viele eCommerce- oder eGovernment-Lösungen. Dabei kommen unterschiedliche technische Lösungen zum Einsatz.

**Objekt – Objekt**
In diesem Ansatz identifizieren und authentisieren sich technische Systeme gegenseitig. Die Identifizierung erfolgt über elektronische IDs, z.B. GUID oder IP-Adresse, die Authentisierung mittels kryptografischer Verfahren und Zertifikaten, z.B. für Server oder Router.[4] Hier spielt, im Gegensatz zu anderen Ansätzen, die Benutzerakzeptanz eine eher untergeordnete Rolle, weil diese Prozesse in der Regel von den Nutzern nicht bemerkt werden.

---

2 Auch als elektronische Signatur bezeichnet. vgl. [Signatur 2001], § 2.

3 Siehe Ausführungen zum Thema PKI in der Anlage.

Anwendungsfelder sind z.B. automatisierte Online-Bestellvorgänge, Kreditkarten-Clearance-Prozesse, das Signieren von Gerätetreibern und Betriebssystemdateien[5] sowie mobile Anwendungen (Softwareagenten) oder sog. Ad-hoc-Netzwerke. Es werden abhängig vom konkreten Einsatzfall verschiedene Techniken verwendet.

Mit dem Trend zu Serviceorientierten Architekturen (SOA) wird die direkte Subjekt-Subjekt-Beziehung zunehmend durch Ketten der Form Subjekt-Objekt-Objekt-...-Objekt-Subjekt abgelöst. Da die Objekte in der Mitte der Kette zu Beginn der Anfrage noch nicht feststehen müssen, werden Fragen bzgl. der Vertrauensbeziehungen aufgeworfen, die noch geklärt werden müssen (vgl. [Paulus 2006b], [Kuppinger 2006b]).

Die Betrachtung der beteiligten Akteure bietet einen ersten Ansatz zur Einordnung von PKI-Szenarien. Sie ist aber noch zu grob, um konkrete Techniken und Szenarien einzelnen Akteursbeziehungen zuordnen zu können. Zudem unterscheiden sich die verwendeten Authentisierungstechniken zu stark bzgl. des Sicherheitsniveaus, der Benutzerakzeptanz sowie der technischen Umsetzbarkeit (Vgl. [Braz 2006]). Die Unterteilung der Akteure, vor allem die Entkopplung von Subjekt und Objekt, ist aber eine hilfreiche Abstraktion, die in den folgenden Betrachtungen aufgegriffen wird.

#### 2.2.2.2 Klassifikation nach Schutzzielen

Beim Einsatz von Signatur-, Identifizierungs- und Authentisierungsverfahren steht, wie bei allen Verfahren der IT-Sicherheit, die Wahrung von Schutzzielen im Vordergrund. Neben der klassischen CIA-Triade Vertraulichkeit (**C**onfidentiality), Integrität (Integrity) und Verfügbarkeit (**A**vailability) sollen auch weitere Unterziele erreicht werden. (vgl. [Eckert 2006], S. 6ff.)

Der Informationsschutz wird vor allem durch die Anforderungen beschrieben, dass ein Subjekt oder Objekt keinen Zugriff auf Informationen haben darf, für die es keine Berechtigung/Autorisation besitzt (**Vertraulichkeit**, Confidentiality), diese nicht ohne Berechtigung ändern darf (**Integrität**, Integrity) und nicht in der Nutzung der hierfür benötigten Ressourcen (Hard- und Software) beeinträchtigt werden darf (**Verfügbarkeit**, Availability).

Die Festlegung von Zugriffsberechtigungen im Rahmen des Access-Managements und die Verschlüsselung von Daten und Kommunikation sind Maßnahmen zur Wahrung der Vertraulichkeit und Integrität. Hierzu gehören auch Datensicherungsmaßnahmen. Damit lassen sich auch Störungen des Betriebs eines IT-Systems weitgehend reduzieren (Prinzip der Verlässlichkeit).

---

4 Siehe auch Abschnitt Erfolgreiche Anwendungen auf Geschäftsprozessebene.

5 So werden bspw. Treiber und Dateien für MS Windows XP/2003 vom Hersteller digital signiert. vgl. [Microsoft 2005]

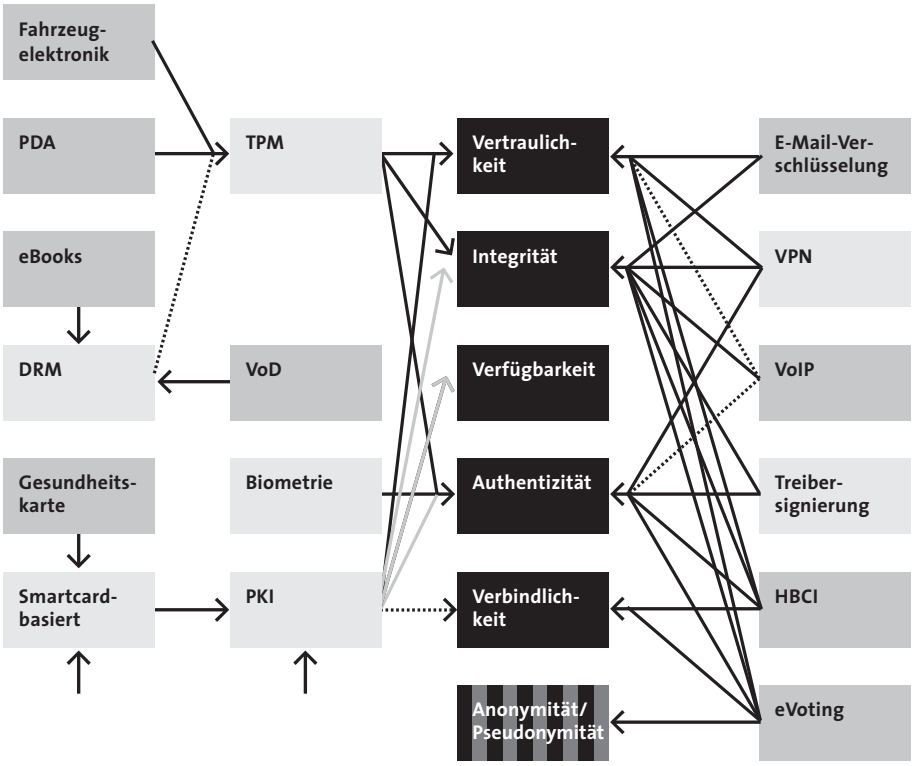


**Abbildung 2.1: Schutzziele und technische Verfahren**

Subjekte und Objekte müssen anhand einer eindeutigen Identität oder charakteristischer Eigenschaften überprüfbar sein (**Authentizität**, Authenticity). Nur so kann deren Authentizität und die Authentizität der von ihnen erzeugten Nachrichten geprüft werden. Dies wird durch Authentisierungskriterien wie Benutzerkennung/Passwort, biometrische Merkmale, Signaturen für Code oder Treiber sichergestellt.

**Anonymität** (Anonymity) und **Pseudonymität** (Pseudonymity) kann ebenfalls gefordert werden, wenn eine Identifizierung nicht gewünscht ist. Das steht zwar im Widerspruch zum Schutzziel der Authentizität, ist aber für bestimmte Anwendungen, z.B. elektronischen Wahlen, erforderlich und z.B. mittels sog. blinder Signaturen lösbar.

In besonderen Fällen ist es auch erwünscht, dass neben der Information auch das eigentliche Stattfinden einer Kommunikation vertraulich zu behandeln ist (sog. **Unbeobachtbarkeit**, Non-Observability), z.B. die Kommunikation mit Anwälten oder Ärzten.

Um die Rechtsverbindlichkeit von Verträgen im eBusiness sicherzustellen, besteht die Anforderung, dass getätigte Aktionen, z.B. der Versand einer E-Mail, im Nachhinein nicht abgestritten werden darf (**Verbindlichkeit/Nichtabstreitbarkeit**, Non-repudiation). Hierbei kommen elektronische Signaturen in Kombination mit der Protokollierung von Aktionen zur Sicherstellung der **Zurechenbarkeit** (Accountability) zum Einsatz.

Für unterschiedliche Anwendungen sind verschiedene Schutzziele von Interesse. Die Wahrung der Schutzziele kann mit unterschiedlichen (technischen) Verfahren erreicht werden, wie folgende Abbildung beispielhaft zeigt.

Die dargestellten Schutzziele lassen sich im Übrigen auch mit anderen Mechanismen als PKI erreichen. Dies kam in den im Rahmen der Studie durchgeführten Interviews zum Ausdruck (vgl. u.a. [Pohlmann 2007]). Im Umkehrschluss lässt sich sagen, dass die Auswahl von PKI-Verfahren offenbar nicht primär von der Möglichkeit der Wahrung konkreter Schutzziele bestimmt wird.

#### 2.2.2.3 Klassifikation nach Stakeholdern

Bei der Klassifikation nach Stakeholdern wird das Verhältnis von Subjekten im Kontext allgemeiner Geschäfts- und Verwaltungsprozesse betrachtet. Subjekte treten hier in unterschiedlichen Rollen als natürliche und juristische Personen auf. Bei der Betrachtung der Stakeholder stehen allerdings nicht das Subjekt-Subjekt-Verhältnis im Vordergrund sondern die aus diesen Beziehungen resultierenden Prozesse. Die folgende Abbildung stellt die Zusammenhänge dar.

Es lassen sich vielfältige Einsatzszenarien für PKI finden. Der Einsatz sicherer Transaktionen durch Verschlüsselung der Kommunikation ist für mehrere Stakeholder von Interesse (B2B, B2C, B2A, C2C). Rechtsgültige Dokumente durch elektronische Signaturen werden ebenfalls von mehreren Stakeholdern eingesetzt (B2B, B2A).

Ein Zusammenhang zwischen PKI-Szenarien und Stakeholdern ist zwar feststellbar, aber nicht ausreichend für eine systematische Klassifizierung. Eine von der konkreten Anwendung unabhängige Betrachtung des Einsatzes von PKI ist nicht sinnvoll. Aufgrund der Vielzahl an möglichen Geschäftsprozessen wird es aber schwierig, diese umfassende Betrachtung zu realisieren. Auch ist keine Aussage über zukünftige, noch nicht bekannte Geschäftsprozesse möglich.

Die Stakeholder-Sicht lässt sich zumindest in die Unterscheidung von Unternehmensprozessen (B2B, B2E, B2A, B2C), Verbraucherprozesse im Sinne des Massenmarktes (B2C, C2C) und staatlich-administrative Prozesse (A2A, B2A, C2A) verallgemeinern. Obwohl hier Überschneidungen bestehen, ermöglicht die gröbere Klassifikation, Merkmale bzgl. des Einsatzes von PKI-Lösungen zu erkennen, die zudem unterscheidbar sind.[6]

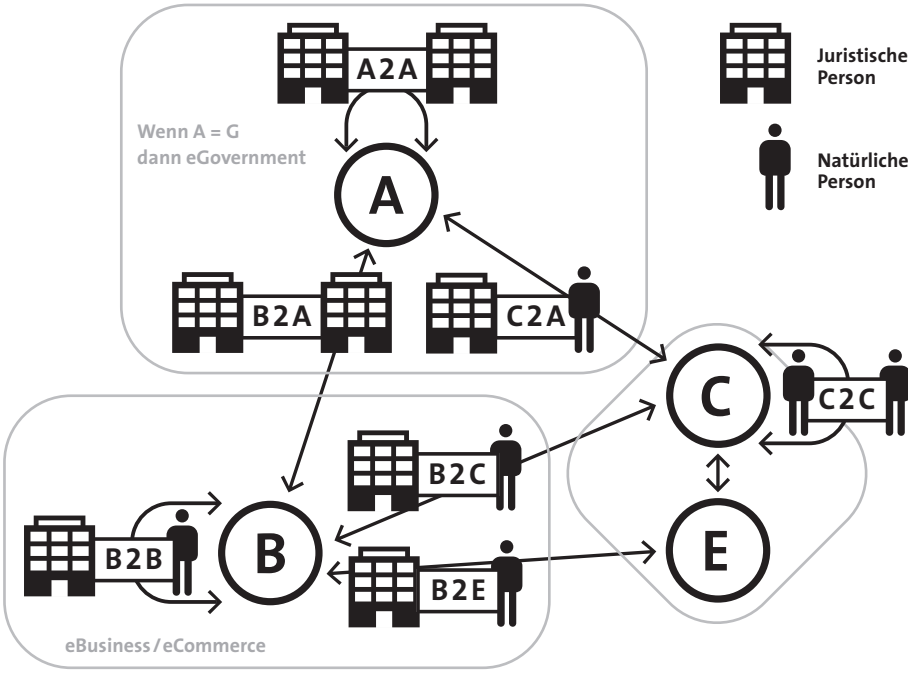


**Abbildung 2.2: A/B/C-Stakeholder**[7]

### 2.2.3 Schlussfolgerungen

Eine Betrachtung von PKI-Szenarien bzgl. einzelner Kriterien wie beteiligte Akteure, zu wahrende Schutzziele oder Stakeholder ist nicht zielführend. Die Kriterien gehen vielmehr ineinander über und gestalten gemeinsam einen konkreten Geschäfts- oder Verwaltungsprozess. Eine geschäftsprozessunabhängige Sicht, d.h. PKI als reine Sicherheitsinfrastruktur, scheint dagegen wenig sinnvoll zu sein. Im Fokus der PKI-Betrachtungen sollten deshalb die Anforderungen des Geschäftsprozesses stehen (vgl. [Brink 2002]).

Insofern bleibt zu klären, welche Rolle PKI-Lösungen bei der Unterstützung von Geschäftsprozessen haben können. Generell lassen sich drei Typen erkennen, auf die

6 vgl. Kapitel Nutzungsbedingungen.

7 A2A: Koordination des Verwaltungshandelns; B2A: Prozesse zwischen Industrie und Verwaltung; C2A: Abläufe zwischen Verwaltung und Bürgern; B2B: eBusiness zwischen Unternehmen, Lieferanten und Händlern; B2C: Internet-Handel zwischen Hersteller/Händler und Endverbraucher; B2E: Interne Geschäftsprozesse / Kommunikation zwischen Unternehmen und seinen Mitarbeitern; C2C: Internet-Handel zwischen Endkunden.
Eine natürliche Person kann als Kunde (Customer) und Mitarbeiter (Employee) in Personalunion auftreten.

PKI-Lösungen wirken können (vgl. [Gadatsch 2006], S.48f.). Diese unterscheiden sich auch dahingehend, inwieweit eine Wirtschaftlichkeitsbetrachtung möglich ist.

→ **Versicherung gegen Risiken:**
Mit dem Einsatz von PKI als IT-Sicherheitslösung sollen Risiken, die durch den Eintritt von sicherheitsrelevanten Vorfällen entstehen können, minimiert werden. Dies ist wohl der am häufigsten anzutreffende Anwendungsfall. Das Erzielen von Einsparungen steht hierbei nicht im Vordergrund. Eine Wirtschaftlichkeitsbetrachtung bezogen auf solch eine Sicherheitslösung ist meist nicht möglich.

→ **Ermöglichen von Geschäftsprozessen:**
Durch den Einsatz von PKI werden neue Geschäftsprozesse ermöglicht, die ohne diese Technologien, d.h. die Sicherheitskomponente, in dieser Form nicht möglich wären. Als Beispiele sind Homebanking mittels PIN/TAN-Verfahren, Online-Shopping über das SSL-Protokoll, Passwort-Authentifizierungsverfahren oder Firewallsysteme bekannt. Einsparungspotentiale erzielt hier aber die Anwendung, weniger die Sicherheitslösung.[8] Wirtschaftlichkeitsbetrachtungen sind in dem Fall nur indirekt möglich. Komplexe Lösungen wie PKI erscheinen aufgrund der in der Regel nur monokausal durchgeführten Wirtschaftlichkeitsberechnungen als unrentabel, was auch ein häufiger Grund für deren Nichteinsatz ist.

→ **Optimieren von Geschäftsprozessen:**
Der Einsatz von PKI-Lösungen kann betriebswirtschaftlich nachweisbare Einsparungen erzielen. Solche Effekte zeigen sich gegenwärtig aber nur selten.
Vielmehr finden sich negative Beispiele, wie der Versuch des Aufbaus einer signaturgesetzkonformen PKI. Diese ist bislang wirtschaftlich nicht erfolgreich insbesondere auch deshalb, weil der zentrale Punkt, eine „kritische Masse" von Anwendern/Anwendungen, noch nicht erreicht wurde. Deshalb konnten die eingesetzten Infrastrukturkosten bisher nicht erwirtschaftet werden.

Leider ist der Aufwand zur Betrachtung jedes einzelnen Geschäftsprozesses extrem hoch – sowohl bzgl. der Anzahl zu untersuchender Prozesse als auch bzgl. deren Kostenstruktur. Die Wirtschaftlichkeitsprüfung von PKI aus Geschäftsprozesssicht kann daher nur für ausgewählte Kernprozesse erfolgen. Hierfür müssen die jeweiligen Kernprozesseigner oder -verantwortlichen vorrangig die Anforderungen an die zu erfüllenden Sicherheitskriterien – insbesondere für die dann geänderten bzw. änderbaren Prozesse – formulieren und die Kostenstrukturen offen legen.

Die Entwicklungen im Bereich Serviceorientierter Architekturen (SOA) verschärfen die Problematik. Wenn Sicherheitsanforderungen eine implizite Eigenschaft jedes Geschäftsprozesses sein müssen, sind diese Eigenschaften auch in jede SOA-Komponente zu integrieren.

8 Zu diesem Ergebnis kommt auch [Gaude 2007]. In dieser Delphi-Studie konnten keine Geschäftsprozesse benannt werden, die ohne PKI nicht funktionieren würden.

Die Komplexität der Prozesse und ungenügende Information über die in den Prozessen benötigten und verwendeten (vor allem monetären) Ressourcen führen letztlich dazu, dass PKI vorrangig als Infrastrukturmaßnahme zum Einsatz kommt und nur in diesen Zusammenhängen betrachtet wird. Die Vorteile für die eine derartige Infrastruktur nutzenden Geschäftsprozesse zeigen sich deshalb erst nach einer gewissen Zeit.

### 2.2.4 Erfolgreiche Anwendungen auf Geschäftsprozessebene

Ein erfolgreicher Einsatz von PKI aus Geschäftsprozesssicht kann am Beispiel von Server- und Benutzerzertifikaten dargestellt werden. Serverzertifikate werden eingesetzt, um z.B. die Authentizität eines Web-Servers zu prüfen (vgl. [Losemann 2005], S.41ff.). Hier wird SSL als Verfahren eingesetzt. Eine weitere Anwendung stellen Virtual Private Networks (VPN) dar, welche Benutzerzertifikate verwenden. (vgl. [Nash 2001], S.430ff.) Die wesentlichen Bestandteile eines Zertifikates sind im Standard X.509 definiert. (vgl. [Brands 2005], S. 273) Die Fachhochschule Brandenburg (FHB) setzt Serverzertifikate für die o.g. Zwecke erfolgreich ein, was im Folgenden beschrieben wird.

Mit der Ablösung der ISDN-Anschlüsse durch DSL-Anschlüsse in den privaten Haushalten wurde insbesondere der Aufbau eines VPN zur sicheren Einwahl von Mitarbeitern und Studenten in das interne FHB-Netz nötig. Hierzu musste jedem Benutzer ein eigenes Zertifikat ausgestellt werden. Dieses konnte nur zu den universitätsüblichen Anforderungen an Kosten mit dem Aufbau einer eigenen Root-CA erfolgen.

Die Beantragung und Ausstellung der fortgeschrittenen elektronischen Zertifikate wird inzwischen als interne Lösung realisiert, wobei die Vergabe der Zertifikate online erfolgt. Durch diesen Schritt können zudem die Serverzertifikate durch die Root-CA der FHB zertifiziert werden. Allerdings ist die realisierte PKI nicht mit den rechtlichen Anforderungen an qualifizierte Signaturen konform. Dies ist aus Sicht der Fachhochschule auch nicht nötig, da das Risiko als nicht so hoch eingeschätzt wird und diese – auch im Handling – „einfache“ Lösung vollständig ausreicht.

Besonders vorteilhaft war die schnelle Umsetzbarkeit bei gleichzeitig günstigen Kosten, was vor allem darauf zurückzuführen ist, dass in einzelnen Bereichen Open Source-Tools eingesetzt werden. Diese genügen den Anforderungen und wurden von der Hochschulleitung genehmigt.

Zudem wird durch die Einführung einer PKI-Lösung in diesen Bereichen auch die Glaubwürdigkeit und Seriosität gegenüber Externen angehoben. Da auf dem Gebiet des Bildungswesens und speziell zwischen Hochschulen und Universitäten eine Konkurrenzsituation besteht, kann durch die Verstärkung der Sicherheit ein Image-

9 Wie bereits dargestellt, ergab sich dies auch als ein Ergebnis des durchgeführten Workshops.

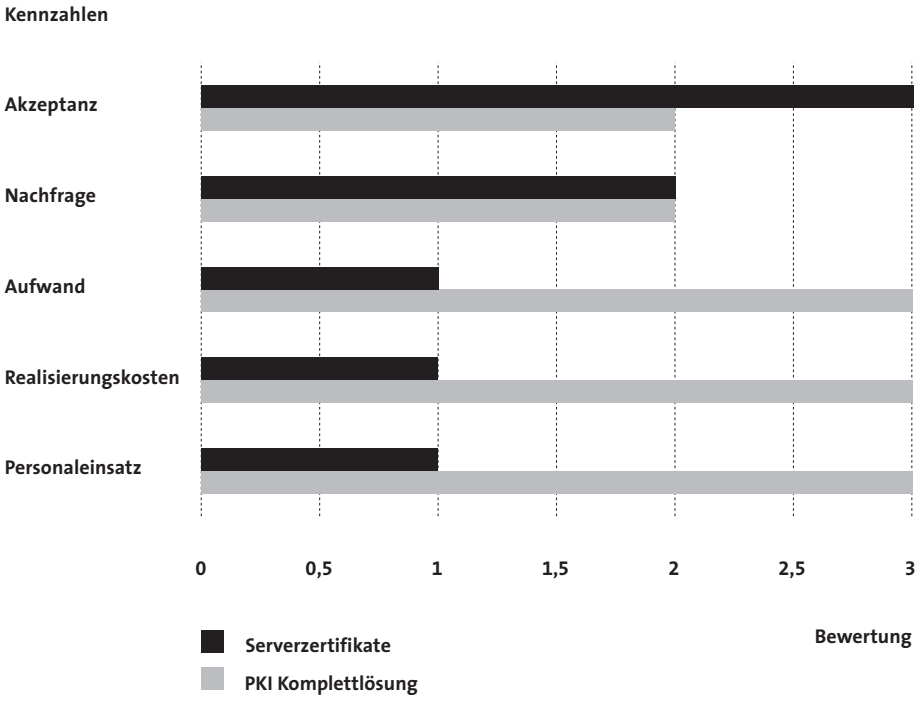


**Abbildung 2.3: Bewertung der Kennzahlen**

gewinn erzielt werden, der als Erfolgskriterium zu sehen ist und die Situation das Image der Hochschule im Konkurrenzkampf verbessert.

Die Einführung einer kompletten, fachhochschulübergreifenden PKI-Lösung scheitert bislang jedoch an fehlenden finanziellen und personellen Ressourcen. Das Bewusstsein, dass mit höherem Aufwand mehr Sicherheit erreichbar ist, ist zwar vorhanden, bisher ergibt sich aus einer Risikobewertung jedoch kein Handlungsbedarf der Hochschulleitung.

Im Rahmen einer Befragung wurde das Meinungsbild bzgl. der Kennzahlen Personaleinsatz, Realisierungskosten, Aufwand, Nachfrage und Akzeptanz analysiert. Die folgende Abbildung stellt die Ergebnisse dar. Für die Bewertung wurde eine Skala von 1 für niedrig bis 3 für hoch verwendet.

Bei der Befragung wurde festgestellt, dass für die Entscheidung über den Aufbau einer internen Root-CA und den Einsatz der Serverzertifikate keine betriebswirtschaftlichen Kennzahlen herangezogen wurden. Eine genaue Berechnung wäre auch nicht möglich gewesen, da hierfür kein auswertbares Datenmaterial an der FHB zur Verfügung stand. Das Heranziehen von Kennzahlen ist nach Auffassung der Befragten

erst bei der Planung und Umsetzung einer kompletten PKI-Technologie nötig.

Es gilt letztlich aber zu beachten, dass sich die Anforderungen, die seitens einer Hochschule an eine PKI-Lösung gestellt werden, von einem Einsatz in Unternehmen unterscheiden. Vor allem durch den Verzicht auf eine Bewertung der Kosten – sowohl im Vorfeld als auch im Nachhinein – ist dieses Beispiel untypisch und muss wohl als Sonderfall angesehen werden. Offen ist, ob dieser Ansatz auch auf andere öffentliche Einrichtungen zutreffen könnte.

## 2.3 Wirtschaftlichkeitsbetrachtungen

### 2.3.1 Messung von IT-Investitionen

Was ist der Nutzen meiner Investition in eine IT-Maßnahme? Diese Frage stellen sich viele Entscheidungsträger, speziell wenn es um das Budget für den Ausbau der IT-Sicherheit im Unternehmen geht. Unsicherheit und Zweifel reichen nicht als Gründe aus, um die permanent wachsenden Fixkosten der IT-Sicherheit zu legitimieren. Vielmehr sind quantitative und qualitative Ansätze zur Bestimmung einer wirtschaftlich sinnvollen Investition gefragt. Zur Beurteilung des Nutzens einer IT-Maßnahme werden Kriterien benötigt, anhand derer man Ergebnisse des Einsatzes messbar machen kann.

Die Abwehr von Gefahren muss in jedem Unternehmen unterschiedlich bewertet werden. So können gehäufte Angriffe aufgrund eines gestiegenen Medieninteresses am Unternehmen oder die Notwendigkeit des Schutzes von geistigem Eigentum verstärkte Schutzmaßnahmen erfordern. Imageverluste können für ein Unternehmen ebenfalls bedrohlich sein, falls z.B. vertrauliche Unternehmens- oder Personaldaten veröffentlicht werden, weshalb auch hier in Sicherheit investiert werden muss. Viele Unternehmen sind sich jedoch der Schäden durch Sicherheitsvorfälle und der daraus abzuleitenden Kosten nicht bewusst. Nur wenige Firmen sind überhaupt in der Lage, Angaben zur Schadenshöhe zu machen, wenn ein Angriff nicht abgewehrt werden konnte.

Eine exakte Bewertung von Risiken und Wirkungen ist äußerst schwierig. Das Problem liegt darin begründet, dass die Kosten für IT-Sicherheit als Querschnittsproblem und -aufgabe nicht eindeutig zuzuordnen sind. Es existieren vielfältige Wechselwirkungen zwischen den Prozessen im Unternehmen einserseits und den Sicherheitsmassnahmen andererseits, weshalb eine Wirtschaftlichkeitsanalyse und -optimierung eine betriebswirtschaftliche Kosten-Nutzen-Gesamtbetrachtung erfordert. (vgl. [Lubich 2006], S. 9)

Ein weiterer Ansatz, Sicherheit in einem Unternehmen zu bewerten, setzt bei den Versicherungen an. Ein in diesem Zusammenhang häufig genanntes Beispiel sind Sprinkleranlagen für Fabriken. Zu Beginn ihres Einsatzes Ende des 19. Jahrhunderts

wurde ihr Nutzen als ebenso zweifelhaft angesehen, wie der einiger Sicherheitsinvestitionen heutzutage. Erst als die Versicherungen günstigere Angebote für Fabriken mit Sprinkleranlagen anboten, konnte der Ertrag der Investition in solche Anlagen nachgewiesen werden. Das Problem besteht in der Verlässlichkeit und konsistenten Erhebung der zugrunde liegenden Daten. Hier ist eine gemeinsame Basis zur Berechnung zu finden. (vgl. [Berinato 2002])

Ob der Einsatz von PKI in einem Unternehmen sinnvoll ist, hängt davon ab, ob der Erfolg dieser Investition für ein Unternehmen festgestellt werden kann. Dabei werden letztlich die anfallenden Kosten einer Investitionsmaßnahme dem zu erwartenden Nutzen über einen bestimmten Zeitraum gegenübergestellt. Der Nutzen ist in Abhängigkeit vom jeweiligen Einzelfall zu quantifizieren, was nicht immer einfach zu realisieren ist.

Für die Betrachtung der Kosten unterscheidet man folgende Ebenen/Wirkungen (vgl. z.B. [Hanusch 1995], S. 557f.):

→ **Direkte** (=interne) und **indirekte** (=externe) **Wirkungen**:
Direkte Wirkungen stehen in unmittelbarem Zusammenhang mit der geplanten Investition (z.B. Kosten für Hardware, Software, Administration, Support etc). Die indirekten Wirkungen beziehen sich meist auf Dritte (z.B. Kosten für Einarbeitung, Effizienzverluste wie Wartezeiten o.ä.). Indirekte Kosten sind schwer zu kalkulieren.

→ **Tangible** (direkt meßbare) und **intangible** (nicht direkt meßbare) **Wirkungen**:
Tangible Wirkungen sind monetär ausdrückbar, intangible Wirkungen, z. B. Zeitersparnis, sind es nicht direkt. Hier müssen Schätzungen in die Rechnungen einbezogen werden.

→ **Primäre** und **sekundäre Wirkungen**:
Primär sind die unmittelbaren Folgen einer Investition. Als sekundäre Wirkungen sind Folgewirkungen zu sehen.

### 2.3.2 Häufig angewandte Kennzahlenverfahren

Zur Ermittlung betriebswirtschaftlicher Kennzahlen existiert eine Vielzahl an Methoden. Für IT-Investitionen und insbesondere Investitionen in IT-Sicherheit bestehen besondere Anforderungen, die z.T. mittels spezieller Verfahrensmodifikationen berechnet werden.

Die folgende Übersicht stellt verschiedene Bewertungsmethoden für IT-Wirtschaftlichkeitsanalysen gegenüber. (vgl. [Hirschmeier 2005], S.190ff.)

10 Grau hinterlegte Bereiche kennzeichnen, ob die jeweilige Methode prinzipiell für die entspr. qualitative, quantitative u/o periphere Analyse geeignet ist.

| | Qualitative Analyse | | | | Quantitative Analyse | | | Periphere Analyse | |
|---|---|---|---|---|---|---|---|---|---|
| | LME | PrE | KuE | KoE | TeE | IdE | VoE | Ak | Dq |
| **Statische Methoden** | | | | | | | | | |
| Return on Investment (ROI) | | | | | | | | ■ | |
| Rentabilität | | | | | | | | ■ | |
| Amortisation (Payback Period, PBP) | | | | | | | | ■ | |
| **Dynamische Methoden** | | | | | | | | | |
| Kapitalwert (Net Present Value, NPV) | | | | | ■ | | | ■ | |
| Interner Zinssatz (Internal Rate of Return, IRR) | | | | | ■ | | | ■ | |
| Nutzen-Kosten-Analyse (Cost Benefit Analysis, CBA) | | | | | ■ | | | ■ | |
| **Qualitative Methoden** | | | | | | | | | |
| Nutzwertanalyse (Scoring Models) | ■ | ■ | ■ | ■ | | | | ■ | |
| Balanced Scorecards (BSC) | ■ | ■ | ■ | ■ | | ■ | | ■ | |
| EFQM-Modell | ■ | ■ | ■ | ■ | | | | ■ | |
| Key Performance Indicators (KPI) und DART | ■ | ■ | ■ | ■ | | ■ | | ■ | |
| **Kostenorientierte Methoden** | | | | | | | | | |
| Prozesskostenrechnung (Activity Based Costing, ABC) | | ■ | | ■ | | | | ■ | ■ |
| Function Point Methode (FPM) | ■ | | | ■ | | | | ■ | |
| Constructive Cost Model (CoCoMo) | ■ | | | ■ | | | | ■ | |
| Total Cost of Ownership (TCO) | ■ | ■ | | ■ | | | | ■ | ■ |
| **Realoptionsmodelle** | | | | | | | | | |
| Analytische Lösungen (Black-Scholes) | | | | | ■ | | ■ | | |
| Binomiale Bäume (Cox-Rubinstein-Ross) | | | | | ■ | | ■ | ■ | |
| **Simulation** | | | | | | | | | |
| System Dynamics | | | | | ■ | ■ | ■ | ■ | |
| Sensitivitätsanalyse | | | | | | | | ■ | |
| Monte Carlo Simulation (MCS) | | | | | ■ | ■ | ■ | ■ | |
| **Makroskopische Modelle** | | | | | | | | | |
| Lern- und Erfahrungskurven | ■ | ■ | | ■ | | | | | |
| Diffusionskurven | | | ■ | ■ | ■ | | | | |
| Customer Lifetime Value (CLV) | | | ■ | | ■ | | | | |

Die Qualitative Analyse unterscheidet Lern- und Mitarbeitereffekte (LME), Prozesseffekte (PrE), Kundeneffekte (KuE) und Kosteneffekte (KoE). Die Quantitative Analyse beschreibt Temporale Effekte (TeE), Interdependenzeffekte (IdE) und Volatilitätseffekte (VoE). Zur Peripheren Analyse werden Akzeptanz (Ak) und Datenqualität (Dq) gezählt.

Zur Präzisierung der zu betrachtenden Methoden muss zuerst geklärt werden, welche Methoden im Rahmen von IT-Investitionen überhaupt von Relevanz sind.

Mit **statischen und dynamischen Methoden** lassen sich Kosten und Nutzen in eine Beziehung setzen. Die Wirtschaftlichkeit kann hierbei dimensionslos (ROI, Rentabilität, IRR), monetär (NPV, CBA) oder über die Zeit (PBP) betrachtet werden. Kosten und Nutzen müssen als monetäre Werte vorliegen. Insbesondere für den Nutzen liegen jedoch selten ausreichende Werte vor. Trotzdem werden diese Methoden aufgrund ihrer einfachen Handhabbarkeit häufig angewendet. Dynamische Methoden werden auch zur Risikobetrachtung angewendet, z.B. mittels Capital Asset Pricing Model (CAPM) oder Risikoprämien.

Mit **qualitativen Methoden** können die qualitativen Einflüsse auf die Kosten-/Nutzen-Betrachtung untersucht werden. Zeitliche Aspekte fließen hierbei ebenfalls nur qualitativ ein. Zusätzlich können Interdependenzeffekte in die Berechnung einfließen (BSC, KPI, DART). Das größte Problem bei der Anwendung dieser Methoden besteht in der subjektiven Bewertung. Nichtsdestotrotz werden sie ebenfalls häufig angewendet.

Die **kostenorientierten Methoden** betrachten ausschließlich die Kostenseite von IT-Investitionen. Der entstehende Nutzen wird nicht betrachtet. Auch quantitative Analysen können hiermit nicht durchgeführt werden. Allerdings stehen in der Regel ausreichend Daten für Auswertungen zur Verfügung. Ein wesentliches Problem dieser Methoden ist, dass Kosteneinsparungen durch zeitlich bedingte Effizienzsteigerungen nicht betrachtet werden. Bezogen auf die klassische Kostenrechnung ist dieser Ansatz sinnvoll, da Effizienzsteigerungen keine Kosteneinsparungen sind die in der Bilanz wirksam werden.

Vergleichbar mit den statischen und dynamischen Modellen sind die **Realoptions-preismodelle**. Methodisch kann hier zusätzlich der Effekt von Folgeinvestitionen un-tersucht werden. Das ist für Infrastrukturinvestitionen wie PKI von Interesse. Der Berechnungsaufwand ist aber aufgrund der Komplexität der Verfahren sehr hoch. Einige Größen sind nur über Simulationen ermittelbar. Das führt zu einem begrenzten Vertrauen in die Ergebnisse und eine geringe Akzeptanz in die Modelle.

Mit **Simulationen** können Zusatzinformationen z.B. zur Prognose gewonnen werden. Ein bekanntes Verfahren ist die Monte-Carlo-Simulation. Für die reine Investitionsbetrachtung sind sie nicht gedacht. Simulationsmethoden betrachten auch

keine IT-spezifischen Aspekte. Daher fällt das Ergebnis oft negativ aus. Auch ist die Akzeptanz aufgrund der Modellkomplexität eher gering.

Erfahrungswerte konnen mit sog. **makroskopischen Modellen** abgebildet werden. Auch hier liegt die Hauptanwendung in der Prognose und Trendabschätzung. Der Einsatz dieser Modelle ist aber stark an den Nutzen gekoppelt (Lern-, Kosten-, Kunden-, Prozesseffekte).

Die Nutzung einzelner Methoden ist für komplexe IT-Investitionen wie PKI als Infrastrukturlösung nicht ausreichend. Es gibt keine Methode zur vollständigen Wirtschaftlichkeitsbetrachtung. Eine Berücksichtigung aller Investitionsmerkmale kann unseres Erachtens nur über eine Methodenkombination erfolgen.

Dies kann aber zu einer Komplexität führen, die in der Praxis nicht beherrrschbar ist bzw. abgelehnt wird. Wir empfehlen deshalb, anerkannte und häufig verwendete Verfahren zu kombinieren. Basierend auf der oben dargestellten Entscheidungsmatrix sieht unser Vorschlag wie folgt aus:

| | Qualitative Analyse | | | | Quantitative Analyse | | | Periphere Analyse | |
|---|---|---|---|---|---|---|---|---|---|
| | LME | PrE | KuE | KoE | TeE | IdE | VoE | AK | Dq |
| **Statisch:** Return on Investment (ROI) | | | | | | | | ■ | |
| **Dynamisch:** Net Present Value (NPV) | | | | | ■ | | | | |
| **Qualitativ:** Balanced Scorecards (BSC) | ■ | ■ | ■ | ■ | | ■ | | | |
| **Kostenorientiert:** Total Cost of Ownership (TCO) | | | | ■ | | | | ■ | ■ |

**Tabelle 2.1: Auswahl geeigneter Kennzahlenverfahren**

Mit diesem Methodenmix können sowohl quantitative als auch qualitative und periphere Aspekte betrachtet werden. Die Methoden ROI, NPV, BSC und TCO werden im Folgenden dargestellt.

### 2.3.2.1 Return On Investment

Mittels Return on Investment (ROI) wird der prozentuale Anteil des Gewinns an einer Investition ermittelt. Eine Nutzungsdauer fließt nicht in die Berechnung ein. Der (einfache) ROI berechnet sich folgendermaßen:

11 Die Hervorhebungen sollen verdeutlichen, für welche Analyse welches Verfahren am sinnvollsten einsetzbar ist. In ihrer Kombination decken sie die wichtigen benötigten Analysen ab.

$$ROI = \frac{Gewinn - Investitionskosten}{Investitionskosten}$$

Diese Berechnung ist anwendbar, wenn die Kosten und der Nutzen einer Investition sich einander direkt zuordnen lassen. Bei gleichen Randbedingungen spricht ein höherer ROI für eine Investitionsentscheidung. Über den Rückfluss oder die Investitionsrisiken liefert der ROI keine Aussage. Je komplexer die Investitionsentscheidungen sind, je mehr indirekte Kosten einfließen, desto weniger ist ein ROI aussagekräftig, insbesondere bzgl. des Kosten-Nutzen-Verhältnisses.

Die Betrachtung des Investitionszeitraumes wird ebenfalls nicht in der ROI-Berechnung berücksichtigt. Deshalb sollte für die Betrachtung finanzieller Folgen einer Investition über mehrere Jahre ein weiteres Verfahren, z.B. Net-Present-Value (NPV) einbezogen werden.

Im Rahmen der Betrachtung von Investitionen in IT-Sicherheit kommt üblicherweise ein modifizierter ROI-Ansatz, Return On Security Investment (ROSI), zum Tragen.

#### 2.3.2.2 Return On Security Investment

Auf Grundlage des ROI wurde das Return On Security Investment-Verfahren (ROSI) entwickelt. Er bietet ein nutzen- und bilanzorientiertes Modell als Grundlage für die verbesserte Schätzung der Investitionen in IT-Sicherheit. Es gibt verschiedene nicht standardisierte Methoden, den ROSI zu ermitteln, die aber auf ähnlichen Annahmen beruhen. Die folgenden Berechnungsverfahren werden gewöhnlich angewandt. (vgl. [Schadt 2006], S. 21)

**Formel 1:**
Jährliche Verlusterwartung = Recovery-Kosten – Ersparnis + Investition
ROSI = Recovery-Kosten – Jährliche Verlusterwartung

**Formel 2:**[12]

$$ROSI = \frac{(SLE \times ARO \times RM) - Investion}{Investion}$$

Das zweite Verfahren lehnt sich mehr an der ursprünglichen Berechnung des ROI an. Im Vergleich berücksichtigt dieser Ansatz in höherem Maße die Eintrittswahrscheinlichkeit. Die jährliche Verlusterwartung wird nicht rein monetär berechnet. Es wird auch der Umstand berücksichtigt, dass bei einer Gefahrenbetrachtung wahrscheinlich nicht jedes Auftreten (Angriff) abgewehrt oder verhindert werden kann.

12 SLE = Single Loss Exposure = projizierte Kosten eines Schadensfalls;
ARO = Annual Rate of Occurence = erwartete jährliche Eintrittshäufigkeit eines Schadens;
RM = Risk Mitigated = prozentuale Wahrscheinlichkeit der Risikominderung

Da es keine standardisierten Methoden gibt, den SLE oder ARO zu berechnen, kann man nur auf Erfahrungswerte zurückgreifen oder in versicherungsmathematischen Tabellen nachschlagen, die auf echten Schadensfällen beruhen. Allerdings ist es sehr schwierig, Daten von Schadensfällen zu gewinnen. Nur wenige Firmen verfolgen nach einem Angriff die insgesamt tatsächlich aufgetretenen Schäden und Kosten. (vgl. [Sonnenreich 2006])

Aufgrund der Notwendigkeit, Risiken in Hinsicht auf Eintrittswahrscheinlichkeit und Schadenshöhe einschätzen und auf diesen Schätzungen aufbauend berechnen zu müsssen sowie der Missachtung des Faktors Zeit, kann ein ROSI nur als Näherungs- oder Richtwert angesehen werden. Dies ist die größte Schwäche des ROSI-Ansatzes. Bei gleich bleibender Berechnungsweise ist aber die Möglichkeit des Vergleichs gegeben. (vgl. [Schadt 2006], S. 21)

#### 2.3.2.3 Net Present Value

Für die Berücksichtigung des Zeitpunktes, an dem Kosten- und Nutzeneffekte einer Investition auftreten, werden dynamische Methoden, wie die Ermittlung des Kapitalwertes oder Net Present Values (NPV) herangezogen.

Der NPV „bildet die Summe aus diskontierten Einzahlungen und Auszahlungen einer IT-Investition über den Nutzungszeitraum“. ([Hirschmeier 2005], S. 44) Der (einfache) NPV wird wie folgt berechnet:

$$NPV = \sum_{Zeit=o}^{N} Nettozahlungen_{Zeit} (1+Zins)^{-1}$$

Die Zeit fließt bei dieser Berechnung über einen diskontierten Zinswert ein. Folgeinvestitionen werden allerdings nicht mit berücksichtigt.

Für die für IT-Investitionen wichtige qualitative Analyse ist der NPV nicht geeignet. Die Daten basieren zudem häufig auf mehr oder weniger intuitiven Schätzungen des Zinssatzes. Außerdem werden gleiche Soll- und Habenzinssätze angenommen. Die Höhe zukünftiger Zahlungsströme ist ebenfalls eine Schätzung.

Nichtsdestotrotz ist der NPV eine stark akzeptierte Methode und aufgrund der Berücksichtigung des Zeitaspektes eine häufig angewandte Methode.

#### 2.3.2.4 Balanced Scorecards

Die in der Regel hohe Komplexität einer Investition und die möglicherweise problematischen finanziellen Auswirkungen auf ein Unternehmen erfordern neben einer kennzahlbasierten Betrachtung auch den qualitativen Erfolg/Misserfolg der Investition zu beschreiben. Als Hilfsmittel für diese Betrachtung kann das Verfahren der Balanced Scorecard (BSC) verwendet werden.

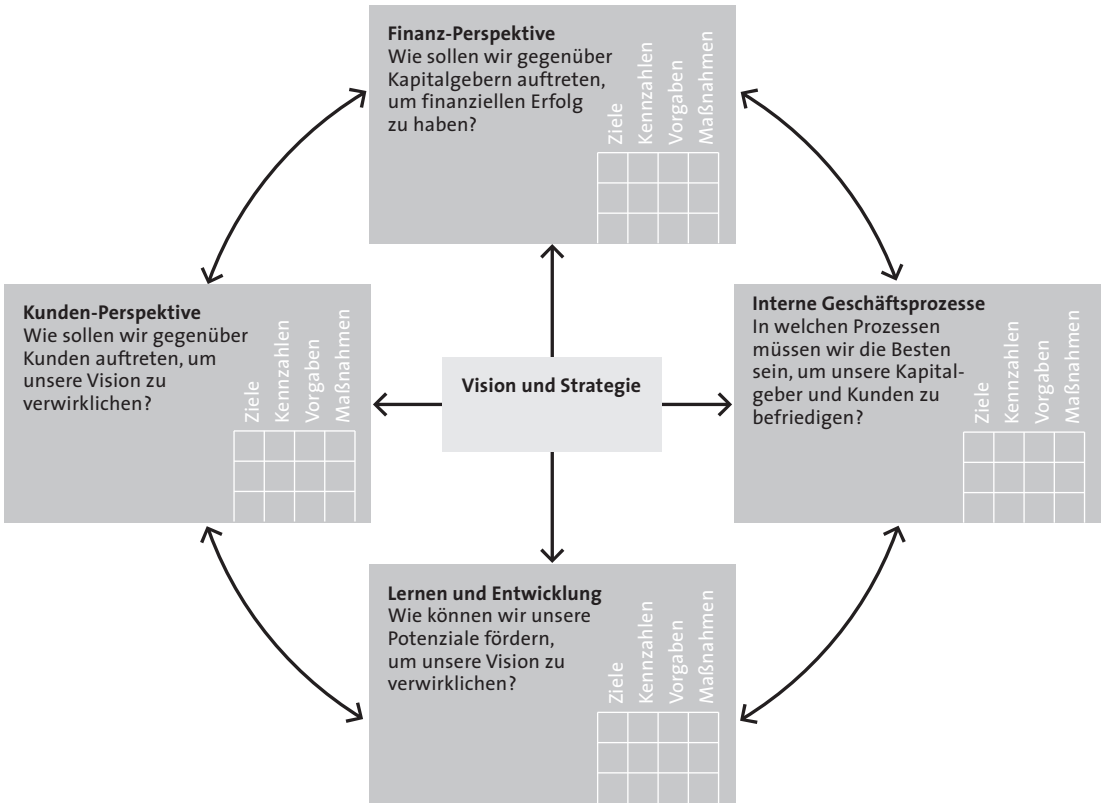


**Abbildung 2.4: Balanced Scorecard (vgl. [Kaplan 1997], S. 9)**

Mit einer BSC kann die einseitige Fokussierung auf finanzielle Ziele durch eine ausgeglichene Sichtweise aus drei weiteren Blickwinkeln (Prozess-, Kunden- und Lern-/Entwicklungsperspektive) vermieden werden. Grundlage bildet eine ausformulierte Unternehmensvision oder -strategie. Aus dieser werden Kennzahlen abgeleitet, anhand derer man die Umsetzung der strategischen Maßnahmen in den zu betrachtenden Bereichen messen kann.

Aufgrund der darin enthaltenen nicht-finanziellen Kennzahlen kann die oft einseitig geführte Diskussion um Finanzierbarkeit und Budget auf qualitative Aspekte gelenkt werden. Beispielsweise kann gefragt werden, welchen Nutzen die Investition bringt? Was leistet die Investition intern und extern? Wie innovativ ist die Investition? Wo liegt der Vorsprung durch die Investition gegenüber Wettbewerbern?

Da eine Investition immer durch eine unternehmerische Positionierung determiniert ist, gilt es die Auswirkungen und Potentiale der Investition aus mehreren Per-

spektiven zu zeigen. Der Nutzen, den eine BSC hier bringen kann, ist:
(vgl. [Bernhard 2000])

→ Verdeutlichung der Verbindung der Investition zur Unternehmensstrategie
→ Verlagerung der Diskussion von Budget- und Finanzierungsfragen zu qualitativen und strategischen Fragestellungen
→ Detaillierte Formulierung der Ausrichtung einer Investition
→ Systematisches Herangehensweise bei der Beurteilung von Investitionen
→ Möglichkeit zur Nutzung der BSC als Managementsystem für Prozesse die mit der Investition zusammenhängen oder durch sie angestoßen werden
→ Kritische Überprüfung der Investitionsstrategie und Anfang eines kontinuierlichen strategischen Lernprozesses
→ Hilfsmittel zur Bewertung des Lebenszyklus von Investitionen

### 2.3.2.5 Total Cost of Ownership

Für technische Geräte fallen nicht nur hohe Anschaffungskosten an. Sie verursachen auch hohe Kosten während des Betriebes und für die Wartung. Diese Folgekosten sollten bei der Investitionsplanung mit betrachtet werden. Eine geeignete Methode ist die Ermittlung der Kosten mittels Total Cost of Ownership (TCO).

Mittels TCO können die Lebenszykluskosten ermittelt werden. Dieser Ansatz wird häufig angewandt, da z.B. die Betriebskosten eines IT-Sytems ein Mehrfaches der Anschaffungskosten betragen können.[13] In eine TCO-Betrachtung fließen folgende Kosten ein. (vgl. [Elsener 2005], S. 208)

| | | |
|---|---|---|
| **Indirekte Kosten** | **(Eigene) Anwendungsentwicklung** | **Schulung** |
| | **Ausfallzeit** | **Selbststudium** |
| | **Datei-/Datenverwaltung** | **Support/Help-Desk** |
| **Direkte Kosten** | **Hardware** | **Betrieb** |
| | **Software** | **Administration** |

**Abbildung 2.5: Direkte und indirekte Kosten einer TCO**

Die indirekten Kosten werden als Bestandteil der Personalkosten betrachtet. Gerade diese Kosten sind aber schwer quantifizierbar. Laut Gartner Group sind 76% der TCO mit den Personalkosten verknüpft. Hierunter fallen auch Kosten wie die Auswirkungen einer Investition auf die Mitarbeitermotivation und daraus folgende mögliche Krankheiten oder Fluktuationen. Zur Feststellung von indirekten Kosten bieten sich standardisierte Fragebögen u.ä. Massnahmen an.

13 Es gibt auch eine Reihe von Tools zur TCO-Ermittlung basierend auf definierten Kostenmodellen, z.B. www.tcotool.de

Abgesehen von der Möglichkeit, Kosteneinsparungen darstellen zu können, zeigt TCO keine weiteren betriebswirtschaftlichen Effekte auf. Bei einer TCO-basierten Entscheidungsfindung wird daher zudem angenommen, dass der Nutzen verschiedener Alternativen gleichwertig ist und sich nur die Kostenseite unterscheidet.

### 2.3.3 Beispielhafte Kosten-Nutzen-Betrachtung

#### 2.3.3.1 ROSI-Berechnung für einen Sicherheitsprozess[14]

Ein typisches Beispiel für die transparente Darstellung des ROSI für eine IT-Sicherheitsinvestition in einer PKI-Umgebung stellt ein Single Sign On (SSO)-System dar. Mit dieser Investition soll ein Sicherheits-Geschäftsprozess optimiert werden.

Im Unternehmensumfeld wird häufig eine Vielzahl unterschiedlicher Systeme parallel betrieben. Die Nutzer erhalten in der Regel unterschiedliche Benutzernamen/Kennwörter, mit denen sie sich beim jeweiligen System authentifizieren müssen. Im Falle von vergessenen Passwörtern benötigen sie schnelle Unterstützung, damit ihre Produktivität gewährleistet ist. Hierfür dient in der Regel ein Help-Desk System, welches die Störungen schnellstmöglich bearbeitet.

Mit einem SSO-System kann diese Problematik entschärft werden. Der Nutzer benötigt nur noch eine Anmeldekennung, mit dem er sich gegenüber dem SSO-System ausweist, z.B. mittels Passwort oder Chipkarte. Die Anmeldungen für die anderen Systeme übernimmt das SSO-System unter Verwendung von Benutzerzertifikaten automatisch.[15]

An den Beispielen soll die Einführung und das erwartete Einsparpotential durch die Nutzung eines SSO stellvertretend für ein Mittelstands- und ein Großunternehmen verdeutlicht werden. Die hierfür verwendeten Daten orientieren sich an [Gadatsch 2006], S. 46 und wurden angepaßt.

Ein Schaden entsteht neben dem möglichen Missbrauch der User-Accounts aufgrund des unsicheren Authentifizierungs-Verfahrens[16] insbesondere durch den Produktivitätsverlust der Mitarbeiter, während sie auf das Rücksetzen eines Passworts oder eine erneute Vergabe warten. Die Zeit und Häufigkeit kann mit einem quantifizierenden Fragebogen ermittelt werden. Die Zeit, die durchschnittlich zur Bearbeitung einer Passwortanfrage am Help Desk benötigt, lässt sich durch eine gleichwertige Evaluierung ermitteln. Zusammen mit dem durchschnittlichen internen Stun-

14 Das folgende Beispiel wird ausführlich im Anhang dargestellt.

15 Es gibt mehrere Single Sign On Ansätze (vgl. [Kuppinger 2007]). Im Beispiel kommen Zertifikate, z. B. nach X.509, im Rahmen einer PKI zum Einsatz.

16 Der hierbei entstehende potentielle Schaden, beispielsweise durch Industriespionage, ist nur schwer allgemein zu quantifizieren, weshalb diese Problematik im Berechnungsbeispiel auch nicht weiter verfolgt wird.

densatz der Mitarbeiter, lässt sich somit die jährliche Verlusterwartung berechnen. Zur Ermittlung der Investitionskosten hat sich der TCO-Ansatz bewährt. Für die Beispiele wurde auf Grundlage der in [Gadatsch 2006] genannten Werte die Anzahl passwort-bezogener Anfragen jeweils heruntergerechnet.

Die erwarteten Einsparungen und die Risikominderung werden auf gleiche Weise gegengerechnet wie die jährliche Verlusterwartung. Zuvor muss prognostiziert werden, in welcher Höhe die Investition die Anfragen senken kann. Diese Angaben kann man von Erfahrungswerten anderer Unternehmen ableiten, Studien oder Schadensberichten von Versicherungen entnehmen, sofern entsprechende Daten verfügbar sind.

**Beispiel 1 – Mittelstand – 100 Mitarbeiter:**

| | |
|---|---|
| Passwortbezogene Anfragen pro Monat: | 100 |
| Produktivitätsverlust pro Anfrage: | 20 Minuten |
| Interner Stundensatz der Mitarbeiter: | 33 Euro[17] |
| Veranschlagte Reduzierung der Anfragen durch SSO: | 40% |
| Anschaffungs- und Installationskosten von SSO: | 10.000 Euro |
| Betriebskosten der SSO-Lösung pro Monat: | 400 Euro |
| Wahrscheinliche Risikominderung: | 40% (lt. Gartner Group) |

Recovery-Kosten: Anfragen * Produktivitätsverlust * Stundensatz * Monate
Investitionen: Anschaffungs- und Installationskosten + Betriebskosten
Einsparungen: Verringerte Anzahl von Anfragen: 40 * Stundensatz * Monate
Jährliche Verlusterwartung: Anfragen * Produktivitätsverlust * Stundensatz * Monate

**Nach ROSI-Formel 1:**

| | 1. Jahr | 2. Jahr | 3. Jahr | 4. Jahr | 5. Jahr |
|---|---|---|---|---|---|
| Recovery Kosten | 13.200 | 13.200 | 13.200 | 13.200 | 13.200 |
| Einsparungen | 5.280 | 5.280 | 5.280 | 5.280 | 5.280 |
| Investitionskosten | 10.000 | | | | |
| Betriebskosten | 4.800 | 4.800 | 4.800 | 4.800 | 4.800 |
| Jährliche Verlusterwartung | 22.720 | 12.720 | 12.720 | 12.720 | 12.720 |
| Recovery Kosten | 13.200 | 13.200 | 13.200 | 13.200 | 13.200 |
| Jährliche Verlusterwartung | 22.720 | 12.720 | 12.720 | 12.720 | 12.720 |
| **ROSI** | **–9.520** | **–9.040** | **–8.560** | **–8.080** | **–7.600** |

17 In [Gadatsch 2006] wird ein interner Stundensatz von 60 Euro angenommen. Für ein mittelständisches Unternehmen scheint uns der Wert zu hoch angesetzt. Ein interner Stundensatz zwischen 30 und 35 Euro dürfte realistischer sein.

**Nach ROSI-Formel 2:**

| | 1. Jahr | 2. Jahr | 3. Jahr | 4. Jahr | 5. Jahr |
|---|---|---|---|---|---|
| SLE | 11 | 11 | 11 | 11 | 11 |
| ARO | 1.200 | 1.200 | 1.200 | 1.200 | 1.200 |
| Wahrsch. Risikominderung | 40% | 40% | 40% | 40% | 40% |
| Investitions-/Betriebskosten | 14.800 | 4.800 | 4.800 | 4.800 | 4.800 |
| **ROSI** | **–64,32%** | **–54,32%** | **–44,32%** | **–34,32%** | **–24,32%** |

**Beispiel 2 – Großunternehmen – 1000 Mitarbeiter:**

| | |
|---|---|
| Passwortbezogene Anfragen pro Monat: | 1000 |
| Produktivitätsverlust pro Anfrage: | 20 Minuten |
| Interner Stundensatz der Mitarbeiter: | 60 Euro |
| Veranschlagte Reduzierung der Anfragen durch SSO: | 40% |
| Anschaffungs- und Installationskosten von SSO: | 60.000 Euro |
| Betriebskosten der SSO-Lösung pro Monat: | 1.200 Euro |
| Wahrscheinliche Risikominderung: | 40% (lt. Gartner Group) |

**Nach ROSI-Formel 1:**

| | 1. Jahr | 2. Jahr | 3. Jahr | 4. Jahr | 5. Jahr |
|---|---|---|---|---|---|
| Recovery Kosten | 240.000 | 240.000 | 240.000 | 240.000 | 240.000 |
| Einsparungen | 96.000 | 96.000 | 96.000 | 96.000 | 96.000 |
| Investitionskosten | 60.000 | | | | |
| Betriebskosten | 14.400 | 14.400 | 14.400 | 14.400 | 14.400 |
| Jährliche Verlusterwartung | 218.400 | 158.400 | 158.400 | 158.400 | 158.400 |
| Recovery Kosten | 240.000 | 240.000 | 240.000 | 240.000 | 240.000 |
| Jährliche Verlusterwartung | 218.400 | 158.400 | 158.400 | 158.400 | 158.400 |
| **ROSI** | **21.600** | **103.200** | **184.800** | **266.400** | **348.000** |

**Nach ROSI-Formel 2:**

| | 1. Jahr | 2. Jahr | 3. Jahr | 4. Jahr | 5. Jahr |
|---|---|---|---|---|---|
| SLE | 20 | 20 | 20 | 20 | 20 |
| ARO | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 |
| Wahrsch. Risikominderung | 40% | 40% | 40% | 40% | 40% |
| Investitions-/Betriebskosten | 74.400 | 14.400 | 14.400 | 14.400 | 14.400 |
| **ROSI** | **29,03%** | **595,70%** | **1162,37%** | **1729,03%** | **2295,70%** |

Die Berechnung des ROSI ist in den Beispielen sehr einfach gehalten. Bei differen-zierter Betrachtung fallen einige Faktoren auf, die nicht in die ROSI-Berechnung ein-bezogen wurden. Zum Beispiel ist die Reduzierung der Nutzeranfragen kein stati-scher Wert. Erfahrungen zeigen, dass bei steigender Akzeptanz und Erfahrung mit SSO-Systemen noch höhere Einsparquoten erreicht werden. Weiterhin wird die Häufigkeit der Anmeldungen mit und ohne SSO nicht berücksichtigt, ebenso wie die freigewordenen Kapazitäten beim Help-Desk. Ein Beispiel für einen sehr schwer zu messenden Faktor ist der Einfluss der verringerten Anmeldungen auf die Produktivität der Mitarbeiter. Es wird z.B. das erneute Eindenken in eine Aufgabe vermieden. Um diese Werte sichtbar zu machen, bietet sich der qualitative Ansatz einer Balan-ced Scorecard an. Damit können die Werte auch in die betriebswirtschaftliche Be-trachtung einfliessen.

**Fazit**
Die Einführung eines SSO-Systems als Sicherheitslösung auf Geschäftsprozess-Ebene führt, zumindest für kleine Unternehmen, zu einem negativen ROSI auch über einen längeren Zeitraum. Das kann zur Folge haben, dass gegen die Einführung solch einer Lösung entschieden wird.

Hinsichtlich des Einsatzes solch einer PKI-Lösung ist eine reine ROSI-Betrachtung noch zu einseitig. In die Betrachtung müssen die Menschen, Prozesse und Technologien im Unternehmen einfließen und wie diese miteinander interagieren, um die Geschäftstätigkeit zu ermöglichen. Solch ein ganzheitliches Bild läßt sich nicht mit einer einzigen Kennzahl ermitteln. Nur die Kombination verschiedener Verfahren ergeben ein umfassendes und realitätsnahes Bild.

#### 2.3.3.2 Balanced Scorecard-basierte Betrachtung

Der Einsatz eines SSO-Systems kann nicht nur den Sicherheitsprozess der Authentifizierung optimieren. Mit dem Aufbau einer PKI können Geschäftsprozesse optimiert oder gar ermöglicht werden, die vorher zu risikobehaftet waren. (vgl. [Lareau 2002], S. 2) Die vorhandene Infrastruktur kann somit auch von anderen Geschäftsprozessen genutzt werden. Die Investitionen in eine Infrastruktur können sich dadurch wieder rechnen.

So bietet es sich an, die PKI auch für elektronsiche Rechnungen oder den elektronischen Dokumentenversand zu verwenden. Das Beispiel soll auch zeigen, wie mittels eines Methodenmixes eine umfassendere Betrachtung der Einflussfaktoren möglich ist.

**Berechnung am Beispiel des elektronischen Dokumentenversands**[18]
Im Laufe der täglichen Geschäftstätigkeit entsteht in einem Unternehmen eine Vielzahl von Dokumenten, die der Aussenkommunikation, z. B. mit Partnern oder

18 Die Daten des Beispiels stammen aus [Beilschmidt 2007]. Da das SSO-Beispiel aus [Gadatsch 2006] Referenzcharakter hat, ist eine Verknüpfung leicht herstellbar.

Kunden, dienen. Heute wird noch in vielen Bereichen mit Post auf herkömmlichen Wegen operiert. Häufig werden diese Dokumente jedoch von den Empfängern digitalisiert, um sie elektronisch verarbeiten oder archivieren zu können. Um diese Medienbrüche und den zusätzlichen Arbeitsaufwand zu verringern und somit Kosten zu sparen, lassen sich Dokumente auch vollständig auf dem elektronischen Weg erstellen und versenden. Dieser Prozess kann durch eine PKI unterstützt und optimiert werden. Entscheidend ist dabei, dass die Authentizität der Dokumente ebenso gesichert ist, wie z.B. bei handschriftlich unterzeichneter Korrespondenz.

**Gesamtbetrachtung mittels Balanced Scorecard**
Um eine ganzheitliche Sicht auf die mit dem Dokumentenversand verbundenen Prozesse zu erhalten, bietet sich der Einsatz einer Balanced Scorecard (BSC) an. Der folgende Ansatz stellt eine Grundlage zur Bewertung dar.

Die Balanced Scorecard erscheint zur Messung von Investitionsprojekten insofern als geeignetes Instrument, als dass Ursache-Wirkungszusammenhänge aus unter-schiedlichen Perspektiven betrachtet und Zusammenhänge und Abhängigkeiten transparent aufgezeigt werden. Um jedoch die vollständigen Erfolgskriterien herauszufinden, müsste eine umfassende Unternehmensanalyse durchgeführt werden.

Basierend auf dem betrachteten Beispiel zeigt die folgende Übersicht einige relevante Kriterien und Fragestellungen aus Sicht der einzelnen Perspektiven, die ggf. zu präszieren sind, um ein Gesamtbild zu erhalten. (vgl. [Beilschmidt 2007])

**Finanzperspektive:**

→ **Investitions- und Betriebskosten:**
Hierzu zählen die Zertifikatskosten (Anzahl der Mitarbeiter, die Zertifikate benötigen). Möglicherweise braucht ein Mitarbeiter für bestimmte Zwecke, z.B. Rech-nungsversand, qualifizierte (teurere) Zertifikate als für den normalen Geschäftsverkehr (E-Mail Kommunikation mit Kunden, Partner, Lieferanten usw.). Andere Mitarbeiter benötigen evtl. keine Zertifikate und nur die SSO-Funktionalität für ihre Anmeldung. Desweiteren sind die Kosten für Service-Level-Agreements zur Nut-zung von Verzeichnis- und Validierungsdiensten zu betrachten.
Hardwarekosten für SSO und elektronischen Dokumentenversand müssen in verschiedenen Ausführungen getestet werden, z.B. Softwaresignatur von E-Mails an jedem Arbeitsplatz. Das würde aber mehr Schulungsaufwand und Einarbeitungsaufwand für die Mitarbeiter bedeuten.
Letztlich stellt sich auch die Frage, ob die Kosten für den Ausbau einer eigenen PKI sind eventuell günstiger sind. [Beilschmidt 2007] nennt einen Betrag im 6–8stelligen Bereich und Wartungskosten bis 100.000 Euro/Jahr für ein KMU.

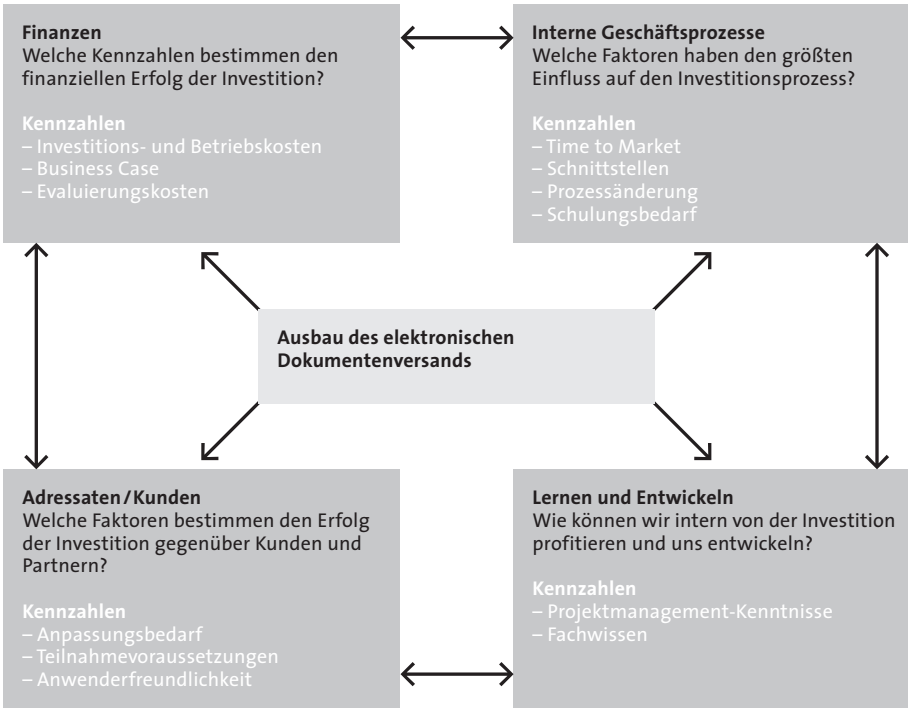


**Abbildung 2.6: Balanced Scorecard für die Bewertung des elektronischen Dokumentenversands**

→ **Business Case:**
Es entstehen Mitarbeiter- und Projektkosten, wenn die Geschäftsfälle und Einsatzziele erstellt werden, z.B. die Erstellung des Anforderungskatalogs oder Pflichtenheftes. Falls dafür neue Software angeschafft wird, sind entspr. Werkzeugkosten zu beachten. Es können auch Lizenzkosten für die teilnehmenden Projektmitarbeiter fällig werden.
Auf Grundlage der Einsatzmöglichkeiten muss geprüft werden, ob eine Hardwarelösung einer Softwarelösung vorzuziehen ist. Des Weiteren stellt sich die Frage, wieviele mögliche neue Partner sich finden und ob gemeinsame Projekte möglich sind. Es ist zu klären, wie viele der Partner überhaupt bereit sind, die neue sichere Kommunikation zu nutzen.

→ **Anbietervergleich:**
Dieser Aspekt entspricht im Wesentlichen den Evaluierungskosten. Es entstehen ebenfalls Mitarbeiter- und Projektkosten, während die Mitarbeiter statt produktiv zu arbeiten, Anbietervergleichsangebote einholen. Eventuelle Fahrtkosten für Vor-Ort-Präsentationen, Messebesuche, Geschäftsessen sind auch einzurechnen. Im Einzelfall gehören auch Prototypinstallationen dazu und Kosten der Mitarbeiter, die dies überwachen, die Anbieter betreuen, Hardware bereitstellen etc.

**Interne Geschäftsprozesse**

→ **Time to Market:**
Wie lange wird für Einführungs- und Testzeiten veranschlagt? Sind die verfügbaren Produkte marktreif und können produktiv eingesetzt werden oder ist erheblicher Customizing-Aufwand nötig?

→ **Schnittstellen:**
Wie kompatibel ist die Software zu weiteren Systemen? Wie hoch sind die Kosten für mögliche Anpassungen an Legacy-Systeme?
Zeigt der Business Case für die gefundenen Lösungen noch weitere Einsatzgebiete, z.B. VPN-Verbindungen für Heimarbeit der Mitarbeiter oder Zertifikatsbereitstellung für Außenstehende?

→ **Prozessänderung:**
Wie hoch ist die Zeitersparnis durch den Wegfall von Ausdrucken, Verpacken und Zur-Post-Bringen der Dokumente? Wie hoch sind die Anmeldezeiten? Wie viele Anfragen pro Monat gehen beim Help-Desk ein? Wie ist der Produktivitätsverlust zu bewerten?

→ **Schulungsbedarf:**
Mitarbeiter benötigen je nach Umsetzung Schulungen und Einweisungen in die neuen Systeme. Administratoren müssen gesondert geschult werden, um einen möglichst herstellerunabhängigen Betrieb zu gewährleisten.

**Adressaten / Kunden**

→ **Anpassungsbedarf:**
Kunden, Partner und Lieferanten müssen über die neuen technischen Möglichkeiten informiert werden. Das Marketing muss auf den Unternehmensseiten mit sicherer Kommunikation werben und Neukunden anregen, davon Gebrauch zu machen.

→ **Teilnahmevoraussetzungen:**
Welche Voraussetzungen müssen meine Kontaktpartner erfüllen? Funktioniert die Kommunikation auch reibungslos, wenn Partner die Technik nicht unterstützen?
Bei Teilnahme verkürzt sich die Zeit, bis man eine elektronische Geschäftbeziehung eingehen kann. Vertragliche Angelegenheiten und Prüfungen können übersprungen werden.

→ **Anwenderfreundlichkeit:**
Da Softwarelösungen zur Verschlüsselung einen starken Eingriff in die Arbeitsweise bestimmter Mitarbeiter bedeuten, muss abgeschätzt werden, inwieweit

sich Einsparungen am Help-Desk durch SSO durch erhöhte Anfragen wegen Dokumentensignaturen (E-Mail-Versand) mehren und Einspareffekte aufheben.

**Lernen und Entwickeln**

→ **Projektmanagement-Kenntnisse:**
Zeiten, Kosten und Mitarbeiteraufwand für die Planung, Umsetzung und den Betrieb der neuen Systeme sind zu kalkulieren. Hierbei sollten etablierte Vorgehensmodelle und Erfahrungswerte genutzt werden.
Wichtig sind Auswertungen zur Mitarbeiter- und Kundenzufriedenheit mit den neuen Systemen. Wo liegen Verbesserungsmöglichkeiten, Entwicklungs- und Ausbaupotentiale? Welche Prozesse verursachen nach der Umstellung die meisten Kosten?

→ **Fachwissen:**
Es sollte ebenfalls der Ausbau des internen Wissenmanagements vorangetrieben werden. Publikationen und PR-Arbeit können als Aushängeschild genutzt werden.

Es gilt auch zu beachten, dass für die Akzeptanz und Praktikabilität des Verfahrens die entscheidenden 20% der Kennzahlen betrachtet werden, die lt. Pareto den Investitionserfolg zu 80% tragen.

**Kostenbetrachtung**
Im vorliegenden Fall wird die Optimierung des Prozesses des Dokumentenversands betrachtet. Die Dokumente werden elektronisch erzeugt, über ein Zertifikat signiert[19], um die Identität des Absenders zu gewährleisten und anschließend elektronisch versandt.

Es werden die Kosten der herkömmlichen Variante benötigt, die durch die Umstellung auf den elektronischen Versand eingespart werden können. Das Problem zur Bestimmung konkreter Zahlen zeigt sich hier in der Bestimmung der Kosten eines zu versendenden Dokuments. Aufwendungen für Papier, Tonerverbrauch und der Arbeitseinsatz der Poststelle für Verpackung, Frankierung und Versand werden in jedem Unternehmen anders eingeschätzt. Hier zeigt sich deshalb auch der Charakter des ROSI als Näherungswert zur Abschätzung der Wirtschaftlichkeit einer Investition.

Im Beispiel wird von folgenden Kosten ausgegangen:
→ 2,00 Euro Aufwendungen für Papier, Toner usw. je Dokument, von denen 1,40 Euro durch den elektronischen Versand eingespart werden können
→ 0,55 Euro Portokosten je verschicktem Dokument
→ 19,75 Euro Zertifikatskosten pro Mitarbeiter im Jahr für eine qualifizierte Signatur

19 Es werden X.509-Zertifikate verwendet, die meist von öffentlichen Trustcentern ausgestellt werden. (vgl. [Beilschmidt 2007])

→ Kosten für eine Hardwarelösung, die ausgehende Dokumente automatisch signiert. Die Kosten unterscheiden sich je nach Unternehmensgröße und beinhalten Anschaffung, Betrieb, Administration und Wartung.
→ Kosten für die Poststelle, vor und nach der Installation, da die Poststelle in der Regel in kleinerer Form erhalten bleibt

Die Beispielunternehmen haben eine Größe von 100 und 3000 Mitarbeitern, da hierfür konkrete Angaben zu Lizenzkosten für das zentrale Gateway vorlagen.

| **Unternehmen A** | |
|---|---|
| Mitarbeiterzahl | 100 |
| Dokumentenaufkommen / Monat | 130 |
| Kosten / Document | 2,00 Euro |
| Zertifikatskosten / Mitarbeiter | 19,75 Euro |

| **Papierbasierter Dokumentenversand** | |
|---|---|
| **Einmalige Kosten** | |
| keine | |
| **Monatliche Kosten** | |
| Documentenkosten | 260,00 Euro |
| Porto (0,55 Euro / Dokument) | 71,50 Euro |
| Poststelle (1–2 Mitarbeiter) | 1.000,00 Euro |
| **Summe / Monat** | **1.331,50 Euro** |

| **Elektronischer Dokumentenversand** | |
|---|---|
| **Einmalige Kosten** | |
| zentrales Gateway | 6.000 Euro |
| **Monatliche Kosten** | |
| Dokumentenkosten (0,60 Euro / Dokument) | 78,00 Euro |
| Zertifikate | 164,58 Euro |
| Poststelle | 500,00 Euro |
| Wartungskosten Gateway | 90,00 Euro |
| **Summe / Monat** | **832,58 Euro** |

**ROSI nach Formel 1**

| Monat | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Investitionskosten | 6.000,00 | | | | | |
| Betriebskosten PKI | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 |
| Einsparungen | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 |
| **ROSI** | **–5.501,08** | **–5.002,16** | **–4.503,24** | **–4.004,32** | **–3.505,40** | **–3.006,48** |
| Monat | 7 | 8 | 9 | 10 | 11 | 12 |
| Investitionskosten | | | | | | |
| Betriebskosten PKI | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 |
| Einsparungen | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 |
| **ROSI** | **–2.507,56** | **–2.008,64** | **–1.509,72** | **–1.010,80** | **–511,88** | **–12,96** |

**ROSI nach Formel 2**

| Monat | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Investitionskosten | 6.000,00 | | | | | |
| Betriebskosten PKI | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 |
| Kosten kumuliert | 6.832,58 | 7.665,16 | 8.497,74 | 9.330,32 | 10.162,90 | 10.995,48 |
| Schaden | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 |
| Schaden gesamt | 1.331,50 | 2.663,00 | 3.994,50 | 5.326,00 | 6.657,50 | 7.989,00 |
| **ROSI** | **–80,51%** | **–65,26%** | **–52,99%** | **–42,92%** | **–34,49%** | **–27,34%** |
| Month | 7 | 8 | 9 | 10 | 11 | 12 |
| Investitionskosten | | | | | | |
| Betriebskosten PKI | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 |
| Kosten kumuliert | 11.828,06 | 12.660,64 | 13.493,22 | 14.325,80 | 15.158,38 | 15.990,96 |
| Schaden | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 |
| Schaden gesamt | 9.320,50 | 10.652,00 | 11.983,50 | 13.315,00 | 14.646,50 | 15.978,00 |
| **ROSI** | **–21,20%** | **–15,87%** | **–11,19%** | **–7,06%** | **–3,38%** | **–0,08%** |

Mit beiden Verfahren lässt sich hier zeigen, dass sich die Investitionen nach rund 12 Monaten weitgehend „gerechnet“ haben, ein positiver Return on Invest jedoch noch nicht vollständig erreicht ist.

| Unternehmen B | |
|---|---|
| Mitarbeiterzahl | 3000 |
| Dokumentenaufkommen / Monat | 2800 |
| Kosten / Document | 2,00 Euro |
| Zertifikatskosten / Mitarbeiter | 19,75 Euro |

| Papierbasierter Dokumentenversand | |
|---|---|
| **Einmalige Kosten** | |
| keine | |
| **Monatliche Kosten** | |
| Documentenkosten | 5.600,00 Euro |
| Porto (0,55 Euro / Dokument) | 1.540,00 Euro |
| Poststelle (1–2 Mitarbeiter) | 3.000,00 Euro |
| **Summe / Monat** | **10.140,00 Euro** |

| Elektronischer Dokumentenversand | |
|---|---|
| **Einmalige Kosten** | |
| zentrales Gateway | 25.000,00 Euro |
| **Monatliche Kosten** | |
| Dokumentenkosten (0,60 Euro / Dokument) | 1.680,00 Euro |
| Zertifikate | 4.937,50 Euro |
| Poststelle | 1.000,00 Euro |
| Wartungskosten Gateway | 375,00 Euro |
| **Summe / Monat** | **7.992,50 Euro** |

**ROSI 1**

| Monat | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Investitionskosten | 25.000,00 | | | | | |
| Betriebskosten PKI | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 |
| Einsparungen | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 |
| **ROSI** | **–22.852,50** | **–20.705,00** | **–18.557,50** | **–16.410,00** | **–14.262,50** | **–12.115,00** |

| Monat | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|
| Investitionskosten | | | | | | |
| Betriebskosten PKI | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 |
| Einsparungen | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 |
| **ROSI** | **–9.967,50** | **–7.820,00** | **–5.672,50** | **–3.525,00** | **–1.377,50** | **770,00** |

**ROSI 2**

| Monat | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Investitionskosten | 25.000,00 | | | | | |
| Betriebskosten PKI | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 |
| Kosten kumuliert | 32.992,50 | 40.985,00 | 48.977,50 | 56.970,00 | 64.962,50 | 72.955,00 |
| Schaden | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 |
| Schaden gesamt | 10.140,00 | 20.280,00 | 30.420,00 | 40.560,00 | 50.700,00 | 60.840,00 |
| **ROSI** | **–69,27%** | **–50,52%** | **–37,89%** | **–28,80%** | **–21,95%** | **–16,61%** |

| Monat | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|
| Investitionskosten | | | | | | |
| Betriebskosten PKI | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 |
| Kosten kumuliert | 80.947,50 | 88.940,00 | 96.932,50 | 104.925,00 | 112.917,50 | 120.910,00 |
| Schaden | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 |
| Schaden gesamt | 70.980,00 | 81.120,00 | 91.260,00 | 101.400,00 | 111.540,00 | 121.680,00 |
| **ROSI** | –12,31% | –8,79% | –5,85% | –3,36% | –1,22% | 0,64% |

Im zweiten Beispiel zeigt sich, dass sich die Investitionen nach dem Ablauf von 11 Monaten zu rechnen beginnen.

**Ergebnis**
Die Berechnung zeigt, dass durch die Kenntnis der grundlegenden Kostentreiber, d.h. der Faktoren, die den größten Anteil an den Gesamtkosten haben, bereits eine vergleichende Berechnung möglich ist. Im Beispiel wurden qualifizierte Zertifikate als Berechnungsgrundlage gewählt. Ebenso wurde für jeden Mitarbeiter ein Zertifikat beantragt. In diesem Beispiel ließen sich Kosten u.a. durch eine Bestimmung der Mitarbeiter sparen, die unbedingt teure qualifizierte Zertifikate benötigen. Für die restlichen Mitarbeiter reichen möglicherweise fortgeschrittene Zertifikate, vielleicht kann aber auch auf qualifizierte Zertifikate grundsätzlich verzichtet werden. Weiterhin kann man Softwarelösungen evaluieren, mit denen sich die Anschaffungs- und Betriebskosten des Gateway verringern oder sogar einsparen lassen. Das würde jedoch von den dann erhöhten Administrationskosten und dem zusätzlichen Schulungsaufwand für die Mitarbeiter zumindest in Teilen kompensiert. Was in den Beispielen ebenso nicht berücksichtigt wurde, ist der verringerte Arbeitsaufwand der Mitarbeiter, z.B. durch das sonst notwendige Ausdrucken und zur Poststelle bringen. Die Untersuchung solcher Prozesse würde jedoch zu unternehmensspezifisch werden sowie der schnellen und einfachen Berechnung entgegenstehen. Die Konzentration auf wesentliche Faktoren zum schnellen aber dennoch aussagekräftigen Vergleich von Alternativen steht hier im Vordergrund.

**Die Quantifizierung von Risiken**
Es stellt sich noch die Frage, inwieweit es sinnvoll ist, Risiken auf Grundlage von unvollständigen Daten abzuschätzen. Wir gehen davon aus, dass es auf jeden Fall sinnvoll ist, wenn die verwendeten Methoden reproduzierbare und einheitliche Ergebnisse liefern.

Da für diesen Zweck die Genauigkeit der zugrunde liegenden Kosten eine untergeordnete Rolle spielt, gilt es, die Methodik der Kostenberechnung und -beschreibung konsistent zu gestalten. In die Ermittlung der Faktoren zur Bemessung des wirtschaftlichen Nutzens der Investition wird häufig die Produktivität höher bewertet als der eigentliche Sicherheitsaspekt. Unternehmen müssen also nach Einflussgrößen Ausschau halten, die eine Produktivitätssteigerung oder neue Prozesse ermöglichen. Bei der Ermittlung sind es in der Regel auch keine Detailfragen, die den Gesamtnutzen entscheidend beeinflussen. Nach dem Pareto-Ansatz gilt es, wie schon weiter oben erwähnt, die treibenden 20% der Faktoren zu ermitteln, die 80% des wirtschaftlichen Nutzens ausmachen. Da sich Unternehmen, besonders aus unterschiedlichen Branchen, jedoch schwerlich auf einen Standard festlegen lassen, muss die Berechnung auf Faktoren beruhen, die unabhängig messbar sind und direkt mit dem Schweregrad z.B. eines Sicherheitsvorfalls korrelieren. Auch ermöglicht die Konzentration auf wenige entscheidende Größen eine leichtere Vergleichbarkeit über Produkte, Projekte, Unternehmen und ganze Branchen hinweg. (vgl. [Sonnenreich 2006])

20 Der Zertifikatstyp ist vom zu signierenden Dokumententyp abhängig. So verlangt das Umsatz-steuergesetz (§ 14) für die Unterzeichnung einer elektronischen Rechnung eine qualifizierte Signatur.

## 2.4 Zusammenfassung

Der konkrete Einsatz von PKI sollte aus Geschäftsprozesssicht betrachtet werden kann. Die PKI kann hierbei häufig neue Geschäftsprozesse ermöglichen oder bestehende Prozesse optimieren. Aufgrund der Komplexität von und der Interdependenzen zwischen Geschäftsprozessen wird in der Praxis der Top-Down-Ansatz, d.h. PKI als Infrastrukturinvestition, favorisiert.

Die Investitionen in PKI-Lösungen sind mit anderen Infrastrukturinvestitionen vergleichbar. Insofern müssen bekannte betriebswirtschaftliche Kennzahlenverfahren angewendet werden, um Investitionsentscheidungen zu begründen. Dabei ist zu beachten, dass nur ein Methodenmix ein vollständiges Bild liefern kann. Ein solcher Ansatz sollte immer unter gleichen Bedingungen durchgeführt und wiederholt werden, um Vergleichswerte zu erhalten, um den Erfolg einer Investition messbar zu machen.

Der Sicherheitsaspekt bei PKI-Investitionsentscheidungen ist eher ein sekundäres Argument. Er erfüllt aber eine wichtige Funktion in der Ermöglichung von Geschäftsprozessen. Er sollte bei geschäftsprozessbasierten Untersuchungen mit einfließen. Gerade die Entwicklungen im Bereich SOA werden diese Orientierung wohl weiter in den Vordergrund rücken.

# 3.

# Nutzungsbedingungen

## 3.1 Methodik

Dieses Kapitel befasst sich mit den Kriterien, die i.d.R. über eine erfolgreiche oder weniger erfolgreiche Implementierung und Nutzung einer Public Key Infrastruktur entscheiden. Der erste Ansatz zur Ermittlung dieser Kriterien bestand zunächst in der Recherche nach geeigneter Literatur, wie z.B. nach Erfahrungsberichten. Dabei hat sich schnell herausgestellt, dass Unternehmen mit Problemen bei der Realisierung von Projekten nicht „hausieren gehen" wollen und somit kaum verwertbare Literatur aus diesem Bereich öffentlich verfügbar ist. Daher wurden im Rahmen dieser Studie einige Experten, die viel Erfahrung mit der Planung, Umsetzung und Betrieb von Public Key Infrastrukturen haben, anonym befragt. Die Anonymität der Befragten zu gewährleisten war notwendig, um diese von möglichen bürokratischen Hürden in ihren Unternehmen bezüglich „offizieller" Stellungnahmen zu entlasten und unverfälschte, nicht zensierte Ergebnisse erzielen zu können.

Die Befragung erfolgte telefonisch anhand eines zuvor bereitgestellten Fragebogens. Dieser Fragebogen war gegliedert in allgemeine Fragen zur Planung, Umsetzung und Betrieb sowie zur organisationsübergreifender Kommunikation.

Im Zusammenhang mit den Fragen zur Planung wurden neben den Faktoren, die für und gegen die Nutzung von PKI sprechen, auch Folgen für die Benutzer und Haftungsfragen erfasst. Im Frageteil zur Umsetzung wurden die eingesetzten Lösungen bzw. Produkte sowie die Entscheidung weshalb sie eingesetzt werden und der für

die Einführung benötigte Zeitbedarf erfasst. Die Hindernisse bzw. Herausforderungen beim Betrieb sowie die benötigte und wirklich verwendete Dokumentation waren Thema innerhalb des Fragenteils zum Betrieb der PKI. Bei den Fragen zur organisationsübergreifenden Kommunikation wurde unter anderem auf technische Realisierungen sowie die damit gemachten Erfahrungen eingegangen. Insgesamt wurde versucht, die möglichen Hürden für den Einsatz von PKI-Anwendungen und -Konzepten zu erfassen und bewerten zu lassen. Nachfolgend werden die Aussagen der Befragten nach inhaltlichen Aspekten gegliedert wiedergegeben.

## 3.2 Produkte

Technische Realisierungen basieren teils auf Open Source Technologien in Verbindung mit eigenen Implementierungen sowie auf am Markt erhältlichen Produkten, die zum Teil auch nichtstandardisierte, proprietäre Technologien einsetzen. Gerade in der Anfangszeit von PKI hatten Unternehmen wegen der mangelnden Verfügbarkeit von marktreifen Lösungen keine große Wahl und waren praktisch gezwungen, eigene Lösungen zu schaffen. Inzwischen werden von manchen Unternehmen benötigte Entwicklungen über die gezielte Förderung der jeweiligen Open Source Community finanziell unterstützt. Open Source Projekte bieten insofern auch eine starke, marktreife Konkurrenz zu Standard-Produkten. Dieser Aspekt in Verbindung zu der ausbleibenden erwarteten großen Nachfrage führt sogar zur Einstellung von Produkten durch die Hersteller, was wiederum das Angebot einschränkt.

Heute werden Produkte, wie Festplattenverschlüsselung, VPN-Lösungen und virtuelle Poststellen, häufig jeweils als eigenständiges Nischenprodukt mit einer eigenen, komplett integrierten PKI ausgeliefert und bieten eine per Definition integrierte Administration innerhalb der Infrastrukturkomponente (eine Prozessorientierung ist bei den Produkten mit großer Marktverbreitung nicht zu erkennen). Konsequenz ist eine heterogene PKI-Landschaft. Die Befragten versuchen zwar eine zu große interne Heterogenität und den daraus resultierenden erhöhten Verwaltungsaufwand zu vermeiden, doch bleibt gerade kleinen- und mittelständischen Unternehmen (KMU) oft keine andere Wahl, als unterschiedliche, nicht zusammenarbeitende Produkte zu kaufen. Diesen Unternehmen fehlen die Ressourcen und der Einfluss bei den Herstellern, um Problemen, die sich z.B. durch die unterschiedlichen zusätzlichen Zertifikatsattribute der jeweiligen Hersteller ergeben, entgegenzuwirken. Es fehlt also an Interoperabilität der Anwendungen der unterschiedlichen Hersteller, insbesondere beim Schlüsselmanagement und der Zertifikatsverwaltung. In bestimmten Bereichen sind allerdings durch Profilierungsansätze schon erste Erfolge erzielt worden, etwa im S/MIME-Umfeld. Eine grundsätzliche Stärkung von Interoperabilität ist jedoch immer noch intensiver anzustreben.

Da mit fortlaufender Weiterentwicklung der Zertifikatsformate insbesondere die Einheit zur Erstellung der Zertifikate permanent angepasst werden muss, sollte dies als externe Lösung eingekauft werden. Dies kann für reine PKI-Komponenten pro-

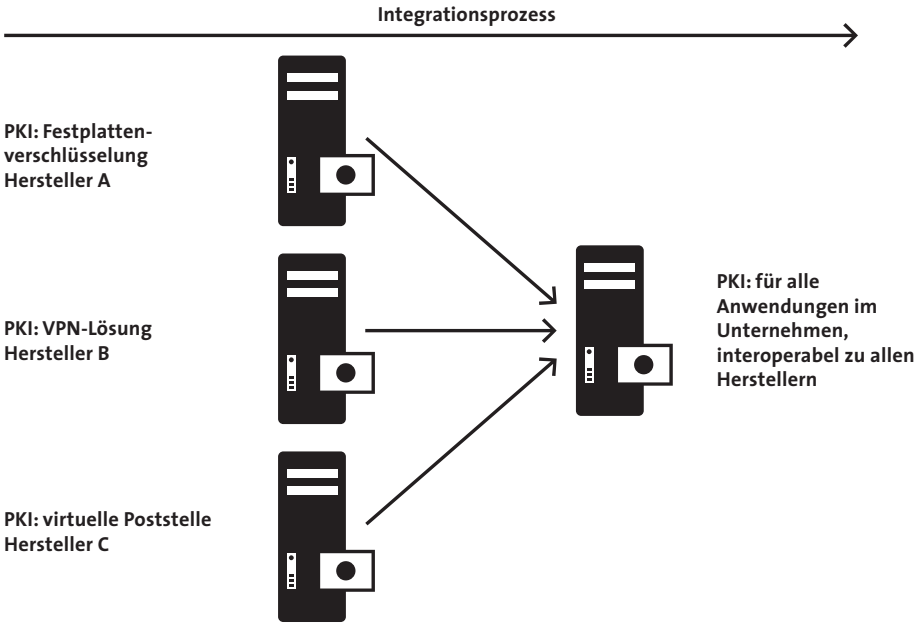


**Abbildung 3.1: Integrationsprozess von mehreren PKIs**

blemlos umgesetzt werden, nicht jedoch für integrierte Anwendungen. Denn mit den verfügbaren Lösungen lassen sich die vorhandenen Geschäftsprozesse nicht immer optimal abbilden. Die Befragten weisen darauf hin, dass insbesondere zur Verbesserung der Akzeptanz der Anwender jedoch die PKI an die Geschäftsprozesse angepasst werden muss und nicht umgekehrt. Um die optimale Abbildung der eigenen Geschäftsprozesse zu erreichen, raten die Befragten deshalb dazu, die notwendigen Komponenten selbst zu entwickeln. Dies wird jedoch für KMU mit den üblicherweise vorhandenen Ressourcen schwer umzusetzen zu sein. Eine deutlich stärkere Orientierung an Geschäftsprozessen und eine dementsprechende Kompetenz bei den Lösungsherstellern ist also essentiell notwendig, um den Einsatz von PKI zu stärken.

Da PKI auch immer mit kryptographischer Technologie in Verbindung steht, ergibt sich bei globalen bzw. global operierenden Unternehmen die Notwendigkeit mit Im- und Exportbeschränkungen umzugehen. Die Verwendung von Kryptographie ist in einigen Ländern, wie z.B. China oder Russland, stark reguliert. Das Einholen von Genehmigungen für die Einfuhr beziehungsweise Ausfuhr kryptographischer Verfahren ist nach den Erfahrungen der Befragten teilweise sehr langwierig und kompliziert und kann zu Verzögerungen im Projektverlauf führen. Es stellt sich die Frage, ob Kryptographie immer noch als „Dual-Use-Item" angesehen werden muss. Es ist jedoch anzumerken, dass die Import- und Exportregulierungen für Kryptogra-

phie einen nicht erheblichen Einfluss auf die Produktauswahl haben. Im Interesse der Deutschen Kryptowirtschaft ist anzuraten, die Regulierungen aus deutscher Sicht zu vereinfachen. Auf die Problematik der Wirtschaftsspionage wird in diesem Zusammenhang nicht weiter eingegangen.

## 3.3 Projektvorgehen

Als Infrastruktur-Technologie benötigt PKI Anwendungen, die ihren Einsatz begründen. Dabei sind die möglichen Anwendungen von PKI durchaus sehr unterschiedlich. In der Praxis können sich insofern widersprechende Anforderungen ergeben, die durchaus den Erfolg eines Projekts erheblich bedrohen können. Man sollte bei der Realisierung deshalb grundsätzlich nicht versuchen, gleich so viele Anwendungen wie möglich zu unterstützen. Ein guter Ansatz scheint eine schrittweise Integration von Anwendungen bei der Pilotprojekte in Kooperation mit den Benutzern umgesetzt werden.

Zudem ist insbesondere auf frühe PKI-Projekte hinzuweisen, die nur für einen Zweck, z.B. der Authentifizierung der Mitarbeiter, aufgesetzt wurden und sich sowohl in finanzieller als auch organisatorischer Hinsicht bewährt haben. Diese Projekte bieten aufgrund der damals so gewollten technischen Konzeption möglicherweise wenig Raum für eine weitere Entwicklung, ihre eindeutige Zweckbestimmung hat jedoch zu ihrem Erfolg beigetragen.

Es lässt sich allgemein feststellen, dass PKI-Projekte in der Regel immer „lebendige" Projekte sind, die mit neuen Anwendungen, Zertifikaten und Algorithmen klarkommen müssen. Andererseits kann eine PKI-Umsetzung wechselnde Anforderungen in der technischen Realisierung aufgrund der inhärenten Komplexität nicht so gut verkraften. Deshalb ist abzuwägen, ob und wie Stakeholder schon zu Beginn des Projekts involviert werden oder bewusst herausgehalten werden, um den Projekterfolg nicht zu gefährden. Andererseits ist anzuraten, weiter zu untersuchen, was der Grund für die mangelnde Flexibilität von PKI ist und wie diese verbessert werden kann.

Die Tragweite unternehmenspolitischer und politischer Einflussnahme sowie rechtlicher Aspekte werden zu Projektbeginn häufig unterschätzt. Auch wenn die allerwenigsten Lösungen Rechtskonformität anstreben, so gibt es doch eine ganze Reihe unternehmensinterner nicht technischer Einflüsse, die berücksichtigt werden müssen. Ein grundlegendes Problem ergibt sich bereits mit der hierarchischen Struktur von PKI, da besonders bei organisationsübergreifenden Projekten oder großen Unternehmen mit eigenverantwortlichen Abteilungen schnell der Eindruck entsteht, die betroffenen Teile hätten sich einer „zentralen Macht" unterzuordnen.. Somit haben technische Diskussionen oft einen eher (organisations-)politischen Hintergrund. Diese Hürden sind problematisch und. müssen durch politische Arbeit in Gremien und Initiativen entsprechend überwunden werden, was allerdings nicht

immer so einfach möglich ist. Im Vergleich zu den technischen Problemen benötigt die Bearbeitung der politischen bzw. organisatorischen Hürden nach Aussage der Befragten den weitaus größeren Zeitbedarf bei der Umsetzung von PKI-Projekten. Die technischen Probleme sind notfalls mit Workarounds zu lösen.

Darüber hinaus entwickelt sich gerade bei der Durchführung von PKI-Projekten häufig eine Faszination für die Technologie bei den Projektbeteiligten. Dies führt dann dazu, dass im Verlauf von PKI-Projekten immer mehr Personen mitreden wollen und sich so auch aus persönlichen Gründen Entscheidungen und Anforderungen stetig ändern. Eine weitere Herausforderung ist das mangelnde langfristige Vertrauen in die Kryptographie-Algorithmen (hauptsächlich derjenigen, die wenig substantielle Kenntnisse über PKI und Kryptographie haben).

Ein Grund für die Komplexität von PKI-Projekten könnte die Vermischung der beiden Ebenen sein, die für eine PKI-Implementierung besonders relevant sind: die technische und die Ebene der Vertrauensbeziehungen. Dabei ist die Ebene der Vertrauensbeziehungen oft unklar und nicht eindeutig definiert, weshalb sich hier besondere Probleme und Komplexitätsbedingungen ergeben. Die Trennung dieser Ebenen in allen Phasen (z.B. auch bei der Produktentwicklung) könnte zu einer Lösung beitragen.

## 3.4 Einsatz

Entscheidungen im PKI-Umfeld, wie Beurteilung der Gültigkeit von Zertifikaten oder Signaturen, überfordern oft den Benutzer. Zudem erkennen Benutzer keinen direkten Vorteil, in der Nutzung von PKI, weshalb ihr Einsatz einen zusätzlichen Aufwand bedeutet. Wie bei vielen anderen Sicherheitskonzepten fehlt auch häufig das Verständnis, warum Sicherheit überhaupt notwendig ist. Schulungen, mit denen dieses Problem beseitigt werden könnte, werden häufig nicht durchgeführt, da hierfür die Ressourcen nicht zur Verfügung gestellt werden (können) und die Benutzer sie auch aus eigener Bequemlichkeit nicht konsequent einfordern. Andererseits ist der Aufwand für den aus dieser Tatsache resultierenden Support nicht zu unterschätzen.

Einen direkten Nutzen für den Benutzer versprechen dagegen Single-Sign-On (SSO) Konzepte, bei denen sich der Benutzer weniger Passwörter merken muss - dort sind Akzeptanz und Verständnis der Benutzer deutlich höher.

PKI-Anwendungen sollten den Anwender nicht vor komplexe, nicht durchschaubare Vertrauensentscheidungen stellen. Vielmehr ist anzustreben, Entscheidungen nur dort einzufordern, wo sie durch den Anwender auf der Basis der durch ihn umzusetzenden Prozesse sowieso getroffen werden müssen. Insgesamt sind Anwendungen, die so transparent wie möglich für den Benutzer arbeiten, leichter einzuführen und umzusetzen.

Sollten Entscheidungen durch den Mitarbeiter getroffen werden müssen, so ist die Durchsetzung organisatorischer Vorgaben essentiell für den Erfolg - sonst ist das gesamte PKI-Konzept in seinem Sinn bedroht. Dabei müssen diese Vorgaben unbedingt von allen Mitarbeitern ernst genommen und eingehalten werden. Nehmen wir als allgegenwärtiges Beispiel die Vorgabe Betriebs- und Besucherausweise sichtbar zu tragen. Ohne die konsequente Durchsetzung der Vorgabe, durch alle Mitarbeiter sowie durch entsprechende Kontrolle und eventuelle Disziplinierung durch den Werkschutz, verliert diese schnell an Glaubwürdigkeit und führt zu Gleichgültigkeit.

Im PKI-Umfeld können Situationen entstehen, in denen Signaturen von Daten, die z.B. von einem Server neu codiert wurden, nicht zu verifizieren sind, was üblicherweise den Benutzer angezeigt wird. Ist diese Situation für den Benutzer neu, besteht die Gefahr, dass er die für diesen Fall vorgesehene Vorgabe nicht kennt / sich nicht mehr daran erinnern kann und im Sinne einer effizienten Arbeit die Warnung nicht beachtet. Im besten Fall wendet er sich an den Support. Die richtige Reaktion des Supportmitarbeiters ist in dieser Situation essentiell für die Problemlösung und die weitere Akzeptanz durch den Benutzer.

Grundsätzlich muss jedoch überlegt werden, inwieweit Lösungen anzustreben sind, die es ermöglichen, nicht auf die oft schwer durchsetzbaren organisatorischen Regeln zurückgreifen zu müssen, um das Vertrauensmodell einer PKI-Implementierung einzuhalten.

Als Beispiel für eine für den Benutzer transparente Realisierung, die es zudem vermeidet auf zu komplexe organisatorische Regeln zurückzugreifen, könnte man ein zentrales E-Mail-Sicherheits-Gateway anführen. E-Mails werden von dem Gateway ver- und entschlüsselt sowie verifiziert. Lediglich der Status dieser Überprüfung wird dem Benutzer möglichst intuitiv, z.B. per Rot-Grün-Ampel, direkt im E-Mail-Programm angezeigt. Damit geht auf der einen Seite zwar der Vorteil der Ende-zu-Ende Verschlüsselung zwischen den Kommunikationspartnern verloren, auf der anderen Seite lassen sich jedoch die Zertifikats- und Signaturprüfung vereinfachen, verschlüsselte E-Mails auf Viren prüfen und technische Möglichkeiten für Urlaubsvertretungen und E-Mail-Verteiler realisieren.

In der Praxis wird die aus Sicht der Befragten überbewertete, formale Dokumentation nicht entsprechend genutzt. Zwar verfügen die meisten, auch unternehmensinterne Lösungen über ein Certificate Practice Statement (CPS), welches die Anforderungen der PKI beschreibt. Dieses wird meist nach RFC 3647 oder ETSI TS 101 456 standardkonform erstellt. Dennoch deuten die Erfahrungen mit diesen Dokumenten darauf hin, dass sie von Theoretikern mit sehr viel Aufwand erstellt werden, bei der Implementierung möglicherweise als eine Art Pflichtenheft helfen, dann aber im Betrieb aufgrund des Umfangs wenig hilfreich sind. Für den Betrieb werden jedoch für relevante Prozesse Handbücher erstellt, auch weil dies besonders für risikobehaftete Prozesse im Rahmen eines Risikomanagements und auch für Qualitäts-

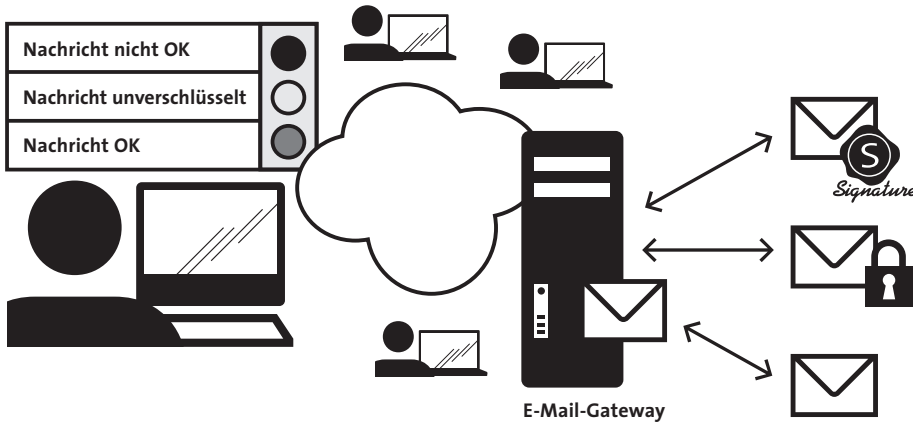


**Abbildung 3.2: Zentrales E-Mail-Sicherheitsgateway**

management gefordert wird. Nutzungsbedingungen, die durch ein zusätzliches Zertifikatattribut referenziert werden, werden dagegen äußerst selten abgerufen. Dieser Abrufungsprozess allein, der aktiv durch den Benutzer durchgeführt werden muss, überfordert bereits die meisten Benutzer. Eine tatsächliche Auswertung dieser Nutzungsbedingungen dürfte aufgrund der enthaltenen juristischen Belange und der Verweise auf andere Dokumente, wie CPS, AGBs usw., zudem schwierig und sehr zeitaufwändig sein. Statt des Modellierens der Vertrauensanforderungen in einem Certificate Practice Statement ist daher eine Dokumentation wie der Ziel-Prozess durch den Einsatz von PKI abgesichert werden kann, deutlich wichtiger.

Bei der organisationsübergreifenden Kommunikation ergeben sich darüber hinaus technische Probleme, da die Verteilung der Zertifikate meist nur mit einer Standardgerätekonfiguration gut funktioniert. Benutzer, die davon abweichen, sorgen für einen höheren Supportaufwand. Daneben kann auf Sperrlisten anderer Organisationen und damit die Information über die Gültigkeit von Zertifikaten, teilweise nicht adäquat zugegriffen werden. Da diese Einträge von einem nicht im eigenen Bereich verfügbaren LDAP-Server abgefragt werden müssen, ergibt sich u.a. das Problem, dass es für einige Firewalls noch keinen LDAP-Proxy gibt, über den ein derartiger Zugriff realisiert werden kann. Die Interoperabilität unternehmensübergreifender Kommunikation ist zwar inzwischen bei E-Mail weitestgehend umgesetzt, für den praktischen Einsatz im Zusammenhang mit zu schützenden Geschäftsprozessen dagegen nach wie vor nicht spezifisch genug geklärt.

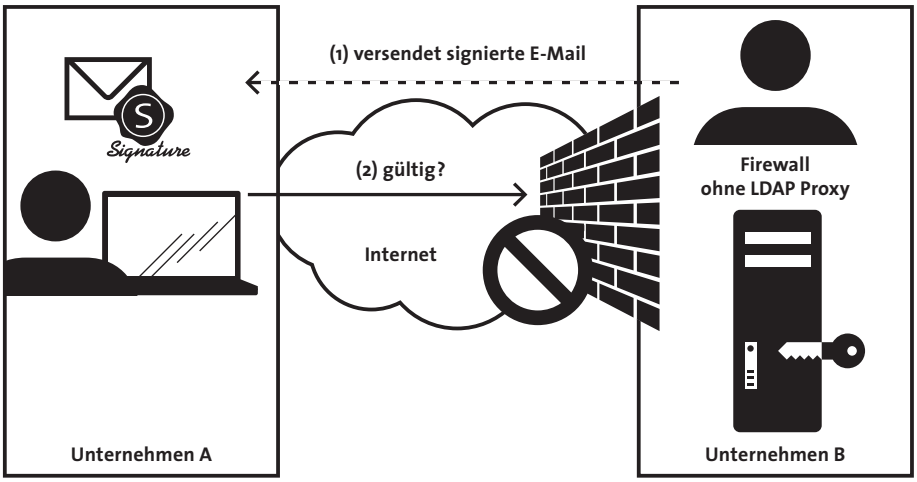


**Abbildung 3.3: Mangelnde Interoperabilität bei E-Mail-Kommunikation**

## 3.5 Haftung

Bei Haftungsfragen gibt es sehr kontroverse Meinungen, die vom jeweiligen Einsatzszenario des Befragten geprägt sind. Unterscheiden muss man zwischen unternehmensinternen und organisationsübergreifenden Lösungen sowie Lösungen mit qualifizierten Zertifikaten.

Unternehmen, die eine pragmatische, unternehmensinterne Realisierung gewählt haben, dennoch qualifizierte Zertifikate für Signaturen verwenden, tun dies nur für eine höhere Verlässlichkeit, jedoch nicht für eine zusätzliche rechtliche Verbindlichkeit. So war den Befragten kein Fall bekannt, wo beispielsweise ein Mitarbeiter aufgrund der fehlerhaften Verwendung einer elektronischen Signatur zur Verantwortung gezogen wurde.

Signaturen werden insbesondere in E-Mails an Vertreter anderer Unternehmen verwendet, also bei organisationsübergreifender Kommunikation. Hierbei wurde die Meinung vertreten, dass diese Prozesse bisher üblicherweise über Faxgeräte abgewickelt wurden, die Relevanz der Übermittlung und damit auch die daraus resultierende Haftung gleich geblieben sind. Nur wegen der Nutzung eines neuen Übermittlungsdienstes auf Basis elektronischer Signaturen sollten hier jedoch die Haftungsfragen nicht neu gestellt werden, da die abgewickelten Prozesse dieselben bleiben und die Verlässlichkeit eher gestiegen ist.

Sind Haftungsfragen jedoch  besonders relevant, z.B. aufgrund der Verbindlichkeit von qualifizierten Zertifikaten, neigen die meisten Unternehmen dazu die Haftung

im möglichen Rahmen sowieso stark zu beschränken. In letzter Konsequenz kann dies zur Ablehnung qualifizierter Signaturen und zur Beschränkung der Nutzung von PKI bei Vorgängen mit höherem Schadenspotential führen - also genau zum Gegenteil dessen, was sich Protagonisten von PKI bezüglich der elektronisch gestützten Prozesse im Zusammenhang mit der Abwicklung von Verträgen usw. vorgestellt haben. Andererseits kann die Umsetzung einer angemessenen Haftung nach Ansicht einiger Befragter auch für mehr Vertrauen sorgen, was insbesondere beim Umgang mit Verbrauchern relevant scheint.

Bei ganz pragmatischen, rein unternehmensinternen Lösungen wurde üblicherweise gezielt auf fortgeschrittene Zertifikate gesetzt, was im Gegensatz zu qualifizierten Zertifikaten die Anforderungen an die IT-Sicherheit mindert, keine Smard-Cards oder Token als sicheren Zertifikatsspeicher voraussetzt und vor allem die meisten rechtlichen Vorgaben aus dem Weg räumt. Somit war das unmittelbare Ziel der meisten Unternehmen nicht die Verbesserung der Verbindlichkeit, sondern eher die Möglichkeit der starken zertifikatsbasierten Authentifizierung und der Sicherung elektronisch basierter Prozesse über die Nutzung von Verschlüsselungen. Außerdem wollen Unternehmen durch geprüfte, nicht verfälschbare elektronische Prozesse eine höhere Vertrauenswürdigkeit bei Wirtschaftsprüfern erreichen.

Von einigen Befragten, die sich mit rechtskonformen Lösungen auseinander setzten, wurde die Diskussion um qualifizierte Zertifikate in Deutschland als „eine ganze Weile fehlgeleitet" bezeichnet. So werden von den meisten Befragten fortgeschrittene Zertifikate als „vollkommen ausreichend" für die meisten Anwendungen angesehen, wohingegen nach die Anwendungsfälle für qualifizierte Zertifikate „gegen Null" gingen. Besteht dagegen ein echter Bedarf an qualifizierten Zertifikaten für bestimmte Anwendungen (z.B. E-Vergabe) wird dies i.d.R von einem externen Dienstleister eingekauft.

Baut jedoch eine PKI-Lösung auf qualifizierten Zertifikaten auf, klagen die Befragten über die realitätsfernen Anforderungen und Überregulierungen durch die Politik bzw. die Regulierungsbehörden in vielen Bereichen. So wurde explizit auf die Beispiele „signaturauslösendes Ereignis" bei elektronischen Rezepten oder Massensignaturen sowie auf die revisionssichere Langzeitarchivierung hingewiesen. Mit der Einführung der Gesundheitskarte und der damit verbundenen Verwendung elektronischer Rezepte, muss der Arzt die elektronische Signatur für das Rezept durch eine PIN-Eingabe am Arbeitsplatz einzeln auslösen bzw. frei schalten. Dies wird nach Ansicht der Experten in jedem Fall einen deutlichen Mehraufwand verursachen, da Rezepte für eine händische Unterschrift bisher zwischen zwei Patienten ins Behandlungszimmer gereicht werden konnten. Die Möglichkeit der Massensignatur, also die automatische Ausführung mehrerer Signaturen, wurde nach Meinung einiger Befragter bisher nur in einzelnen Bereichen, wie der elektronischen Rechnungsstellung, reguliert. Bei der revisionssicheren Langezeitarchivierung, z.B. bei der Patientendokumentation, müssen Aufbewahrungsfristen von bis zu 30 Jahren eingehalten werden. Neben Problemen die sich aus alternden Schlüssellängen

sowie der Aufbewahrung von Zertifikaten zur Verifikation von Signaturen ergeben, müssen auch allgemeine Fragen zur Haltbarkeit von Dokumentenformaten und Datenträgern gelöst bzw. gewährleistet werden.

Außerdem finden sich z.B. im Umfeld des Sozialgesetzbuches, bereits sehr detaillierte technische Anforderungen im Gesetz und werden dort unabhängig und ohne entsprechende Bezüge zu anderen Einsatzbereichen von Signaturen reguliert. Die Befragten drücken aus, dass verfehlt wurde, durch die Gesetze ein sicheres aber dennoch praktikables Sicherheitsniveau zu schaffen. Die Anforderungen werden als zu hoch beschrieben, was zur Zurückhaltung bei der Umsetzung gesetzeskonformer Lösungen führt.

Als weiteres grundsätzliches Problem wurde erkannt, dass in Deutschland noch kein „gelebtes Recht beim Einsatz von elektronischen Signaturen" vorhanden ist. So bedarf es üblicherweise einer ganzen Reihe von Einzelfallentscheidungen vor unterschiedlichen Instanzen, bis sich das Recht und das Verständnis für eine Technologie bei den beteiligten Vertretern gesetzt haben. Rechtssicherheit im Zusammenhang mit der Nutzung von PKI ist derzeit daher sehr schwer zu erzielen. Allerdings könnte dieser Problematik über Rechtsgutachten anerkannter Persönlichkeiten zumindest in Teilen entgegengewirkt werden. Für die Unternehmen stellt das Fehlen dieser Rechtssicherheit jedoch kein grundsätzliches Problem dar, weshalb auch nicht versucht wird Sicherheit durch entsprechende Maßnahmen zu erreichen.

Die heterogene Infrastrukturlandschaft bei der Verwendung von Signaturen auf Seiten der Behörden und Gerichte ist außerdem durch das föderale System in Deutschland geprägt. Dieser „Flickenteppich" und der unterschiedliche Grad der Akzeptanz sorgt für eine schleppende Verbreitung von Zertifikaten bei den Anwendern. Andere, insbesondere zentral regierte Länder und solche die einen pragmatischen Ansatz für die Integration gewählt haben, besitzen nach Aussage einiger Befragter inzwischen einen deutlichen Vorsprung in Bezug auf die Nutzungsmöglichkeiten.

Die Umsetzung der EU-Signaturrichtlinie in den einzelnen EU-Staaten weist teilweise dramatische Unterschiede auf. So werden in den einzelstaatlichen Gesetzen insbesondere in einigen Ländern mit Open Source PKI-Projekten die Anforderungen an qualifizierte Signaturen umgesetzt, wohingegen in Deutschland diese Open Source Projekte gerade einmal für fortgeschrittene Signaturen geeignet sind. Aus Sicht der Experten sollten deshalb die Hürden in Politik bzw. Behörden aufgebaut werden, durch pragmatische Ansätze entschärft werden, zumindest in einer Übergangszeit.

## 3.6 Zusammenfassung

PKI-Lösungen dienen vorrangig dem unternehmensinternen Einsatz von elektronischen Zertifikaten für eine starke Authentifizierung und Verschlüsselung. Das Erfüllen gesetzlicher Anforderungen steht dabei üblicherweise nicht im Vordergrund,

Gerade in diesem Umfeld ergeben sich jedoch nicht-technische Probleme durch unternehmenspolitische und organisatorische Einflüsse, die oft nur schwer lösbar sind. Die Befragten der wenigen PKI-Anwendungen, die den Anforderungen von qualifizierten Zertifikaten genügen wollen, klagen über die hohe Regulierungsdichte durch Politik und Aufsichtsbehörden, realitätsferne Anforderungen sowie schlechte Akzeptanz gegenüber Behörden und Gerichten. Als Konsequenz sollten mehr pragmatische Ansätze zumindest für eine längerfristige Übergangszeit angestrebt werden und die Verbreitung des PKI-Einsatzes bei Behörden und Gerichten aktiv gefördert werden.

Nach Aussage der Befragten lassen sich technische Probleme, und sei es durch Workarounds, eigentlich immer lösen. Um gerade KMU den Umgang mit PKI zu erleichtern, sollten jedoch Unternehmen mit Marktmacht gewonnen werden, die insbesondere über die Veröffentlichung prozessorientierter Dokumentationen ihrer PKI-Lösungen und anderer Maßnahmen zu einer besseren Interoperabilität beitragen . Außerdem könnten, durch die Förderung gezielter Forschungsvorhaben in diesem Bereich, KMU indirekt gefördert und so langfristig Arbeitsplätze gesichert werden. Auch sollte durch die Förderung wissenschaftlicher Forschung im Bereich von Algorithmen, das Vertrauen in derzeitige und zukünftige Algorithmen verstärkt werden.

Für die Zukunft ist eine Förderung der organisationsübergreifenden Verwendung von PKI sinnvoll, um den Standort Deutschland zu stärken. Dabei sollten konkrete Lösungsansätze geschaffen werden, die zeigen, wie derzeitige Probleme beim Einsatz von PKI in den Unternehmen gelöst werden können.

# 4.

# Workshop-Ergebnisse

Dieses Kapitel beschreibt die Ergebnisse des High-Level-Workshops im Rahmen des Projekts „Erfolgskriterien für Signatur-, Identifizierungs- und Authentifizierungsverfahren auf Basis asymmetrischer kryptographischer Verfahren“. Das Kapitel ist wie folgt gegliedert: im ersten Abschnitt wird der Ablauf und die Methodik des Workshops vorgestellt. Dabei wird auch auf die Zusammensetzung der Teilnehmer des Workshops eingegangen. Im zweiten Abschnitt werden die Kommentare der Teilnehmer zu den bisherigen Ergebnissen der Studie vorgestellt. Im dritten Abschnitt werden die in den Break-Out-Sessions des Workshops erarbeiteten Ergebnisse vorgestellt. Im Anschluss daran werden die Erkenntnisse des Projektteams aufgrund der Erfahrungen des Workshops zusammengestellt. Schließlich stellen wir einige Empfehlungen für das weitere Vorgehen zusammen.

## 4.1 Methodik und Ablauf des Workshops

Der Workshop ist der vierte wesentliche Teil des Projekts „Erfolgskriterien für Signatur-, Identifizierungs- und Authentifizierungsverfahren auf Basis asymmetrischer kryptographischer Verfahren“. Auf Grundlage der Abschnitte, die sich mit den technischen Perspektiven, den wirtschaftlichen Betrachtungen und den Nutzungsbedingungen beschäftigen, sollte der Workshop abschließend Erfolgskriterien identifizieren und Perspektiven aufzeigen. An diesen Zielen wurde sowohl die Organisation des Workshops als auch die Zusammensetzung der Teilnehmer ausgerichtet.

Die Teilnehmer wurden aus verschiedenen Kompetenzgruppen zusammengestellt: Hersteller und Dienstleister aus dem PKI-Markt, Chief Information Security Officers, die erfolgreiche multinationale PKI-Projekte umgesetzt haben, Wissenschaftler, Unternehmensberater mit Sicherheits- und Betrugsbekämpfungsexpertise, IT-Manager. Dabei wurde besonders auf eine langjährige Erfahrung der Teilnehmer Wert gelegt. Neben der grundlegenden Bereitschaft aller, ihr Wissen für die Fragestellungen des Projekts zur Verfügung zu stellen, war die weitere Motivation zur Teilnahme sehr unterschiedlich. Einige sehen das Engagement in PKI als wichtigen Teil ihrer persönlichen Expertise, die sich durch die Teilnahme und die Diskussion mit den anderen Experten erweitern und ausbauen ließ, andere wollten zudem neue Kontakte knüpfen. Dabei war die vielfältige Zusammensetzung der Teilnehmer sicherlich ein motivierender Grund. Insgesamt ist festzustellen, dass trotz oder vielleicht auch gerade aufgrund der Seniorität der Experten eine außergewöhnliche Bereitschaft zur konstruktiven Mitarbeit zu finden war. Wichtig für den Erfolg erwies sich auch, neben der durch das Projektteam getragenen Expertendiskussion, genug Raum und Zeit für bilaterale Gespräche vorzusehen, welche sich im Nachgang zum moderierten Teil der Veranstaltung für die Erkenntnisse des Projektteams als besonders gewinnbringend erwies.

Um die Teilnehmer auf die zu einem späteren Zeitpunkt geplanten Arbeitsgruppen vorzubereiten wurden sie in einem ersten Schritt über die bisherigen Ergebnisse der Arbeiten des Projektteams informiert. In den darauf folgenden „Break-Out-Sessions" sollten die Teilnehmer auf der Basis ihres Wissens und ihrer Erfahrung und der von uns dargestellten Ergebnisse jeweils 3-5 Problemfelder identifizieren, daraufhin passende Wunsch-Zustände sowie Lösungen / Aktionsfelder erarbeiten, die den Wunsch-Zustand zum Ziel hatten. Die Problemfelder wurden dann unter Erklärungen und Feedback durch die Sitzungsteilnehmer weiter bearbeitet. Ein Rapporteur jeder Arbeitsgruppe berichtete eine Zusammenfassung der Diskussion im darauf folgenden Plenum.

Die Diskussionen waren von Anfang an sehr intensiv durch die breit differenzierte Kompetenz der Workshop-Teilnehmer, mit Beiträgen aus sehr unterschiedlicher Interessenlage. Durch die Vertiefung in den Arbeitsgruppen wurde eine Fokussierung der Kernthematik erreicht, die durch die abschließende Feedback-Runde noch einmal zusammengefasst wurde. Insbesondere die interdisziplinäre Zusammensetzung von Technikern und Nicht-Technikern, von IT- und Sicherheitsverantwortlichen über PKI-Dienstleister bis hin zu Professoren der Betriebswirtschaft war ein wesentlicher Erfolgsfaktor für die Ausprägung von differenzierten und durchaus kontroversen Aspekten.

Besonderer Wert wurde darauf gelegt, die Zusammensetzung der Break-Out-Sessions so zu gestalten, dass möglichst Personen zusammen gearbeitet haben, die sich vorher nicht kannten. Durch diese Maßnahme wurde eine offene, vorurteilsfreie Diskussion unterstützt. Dieses Vorgehen hat sich unserer Meinung nach als erfolgreich erwiesen, obwohl das Bestreben in den Diskussionen, ein gemeinsames Ver-

ständnis zu Sachthemen zu erreichen, natürlich Zeit kostete.

Auch wenn die Diskussionen insgesamt sehr breit verteilte Aspekte berührten, war doch der Verlauf geprägt von optimistischen, aber dennoch kritischen Auseinandersetzungen mit klarem Fokus: dem Erfolg von Public-Key-Infrastrukturen, -Anwendungen und -Technologien. Im weiteren Verlauf dieses Kapitels werden die Ergebnisse der Diskussionen aufgezeigt. Sehr wertvoll waren die Empfehlungen zur weiteren Vorgehensweise, die uns von den Teilnehmern ohne Aufforderung mitgegeben wurden.

Schließlich enthielten die eher informellen Kommentare im nicht moderierten Teil des Workshops wichtige Detail- und Praxisinformationen sowie persönliche Einschätzungen, die das Projektteam in einer formellen Befragung nicht erfahren hätte. Dies gilt in besonderem Maße für Meinungen oder Einschätzungen entgegen der „herrschenden" Expertenmeinung, die – vielleicht wegen politischer Motivationen – in dieser Form bisher nicht öffentlich diskutiert wurden.

Zusammenfassend kann man zur Methodik des Workshops sagen, dass die beiden Aspekte „Interdisziplinarität der Teilnehmer" und „Mischung aus moderierter Diskussion und informellen Gesprächen" Garanten für den Erfolg des Workshops waren und damit ein wesentliches Element in der Erkenntnisbildung des Projekts darstellen. Darüber hinaus ist zu betonen, dass vermutlich eine in dieser Form selten erreichte Zusammensetzung von anerkannten Experten gelang. So konnten wir ein facettenreiches, durchaus mit Spannungen und Widersprüchen versehenes Bild über Nutzungsbedingungen von PKI in der Praxis gewinnen, was ohne eine solche Veranstaltung, etwa nur durch Interviews, mit hoher Sicherheit nicht erreicht worden wäre. Wir können daher das von uns gewählte Vorgehen für weitere Themen mit interdisziplinärem Charakter grundsätzlich empfehlen.

## 4.2 Kommentare zu den bisherigen Ergebnissen

Im ersten Teil des Workshops wurden die bisherigen Untersuchungsergebnisse vorgestellt. Dabei wurden die drei Bereiche „Technische Perspektiven", „Betriebswirtschaftliche Aspekte" und „Nutzungskriterien" vorgestellt und jeweils von den Teilnehmern diskutiert.

### 4.2.1 Anmerkungen zu den „Technischen Perspektiven"

Grundsätzlich wurde von den Teilnehmern mehrfach betont, dass es sich bei PKI und den darauf basierenden anwendungsspezifischen Kombinationen von Komponenten um weitestgehend ausgereifte Technologien handelt. Die Diskussionen seien zum Teil sehr esoterisch, und man solle einfach anfangen: „Alles was wir damit machen ist besser als das was wir heute haben, nämlich nichts".

In Punkto Investitionssicherheit wurden drei Aspekte zur Diskussion gestellt: zum ersten die Beobachtung, dass PKI für eine Infrastrukturtechnologie vergleichsweise sehr lange Implementierungsphasen (Planung, technische Realisierung, Definition der Policy, Bestimmung der Token, Benutzerintegration, Implementierung in Anwendungen) und hohe Anfangsinvestitionskosten hat. Das wurde von den Teilnehmern deutlich bestätigt, insbesondere von denjenigen, die schon erfolgreich große PKI-Projekte umgesetzt haben. Als Voraussetzung für den Erfolg wurde angeführt, dass zumindest lange Nutzungsdauern technisch vorgesehen sein müssen, damit sich die Kosten amortisieren. Dazu gehört auch die Forderung, dass die Anwendungsumgebungen über den gleichen Zeitraum stabil bleiben müssen. Als Beispiel wurden für den Bereich Finanztransaktionen und Bankdienstleistungen die Kryptoparameter für eine ausreichende Anwendungssicherheit genannt. Ebenfalls wesentlich sei die Beachtung des Zeitraumes, der für die Gewöhnung der Benutzer an die Identifikations-, Authentifizierungs- oder Signaturanwendungen in Verbindung mit dem vorgeschriebenen Handling der Zertifikate und Token (häufig der Mitarbeiterausweis) notwendig ist.

Unter anderem Blickwinkel widersprachen allerdings die Nicht-Techniker unter den Teilnehmern deutlich den genannten Erfahrungen: ob eine Technologie sich durchsetzt, reguliere der Markt, und der Technologie-Markt denke immer kurzfristiger. Gerade unter diesen Gesichtspunkten sei eine technologische Ausrichtung an langfristiger Verwendung nicht sinnvoll. Unter diesem Gesichtspunkt der Praktiker wurde auch die Fokussierung auf die Stabilität der kryptographischen Basis – zumindest in dem Maße, in dem dies in Deutschland in den letzten Jahren diskutiert wurde – in Frage gestellt. Konkret: die Austauschbarkeit der Algorithmen und die langfristig gewählte Schlüssellänge als Konsequenz einer langen Nutzungsdauer wurden im Hinblick auf Unternehmensanwendungen als nicht adäquat angesehen. Für staatliche Anwendungen hingegen, die langfristige Sicherheit brauchen (dazu zählen nicht nur Ausweisdokumente, sondern z.B. auch gesetzlich längerfristig zu archivierende Dokumente) kann dies durchaus ein sinnvoller und notwendiger Entscheidungsparameter sein, bei dem allerdings die Durchsetzbarkeit mit bedacht werden müsste. Die Planungs- und Realisierungsphasen sind im öffentlichen Bereich eher länger als in Unternehmen. Deshalb sind dort Anforderungen an standardisierte stabile Parameter der Technologie höher. Während Unternehmensanwendungen es sich leisten können, „kurzfristig" zu denken und nur kurze Amortisationszeiten in Betracht zu ziehen, ist das bei staatlichen Anwendungen anders. Konflikte in diesem Bereich treten demnach logischerweise genau dort zu Tage, wo beide Einsatzgebiete sich berühren, etwa beim Steuerrecht. Der Consumer-Markt ist in diesem Kontext eher dem Unternehmensumfeld zuzurechen, da die Dienstleistung, die PKI verwendet, von einem wirtschaftlich agierenden Unternehmen erbracht wird.

Das Thema Interoperabilität, welche als wesentliche Voraussetzung für erfolgreiche PKI-Anwendung vorgestellt wurde, ist ebenfalls durchaus kontrovers diskutiert worden. Es konnte festgestellt werden, dass diese bei „monoprozessualen" Anwendungen von PKI-Technologie (also Einsatzgebieten, wo die eingesetzte PKI genau

einem an einen Prozess gebundenen Zweck dient, wie etwa einem VPN („Virtual Private Network“) oder einer Software-Update-Infrastruktur) so gut wie keine Rolle spielt, da sie komplett transparent integriert werden kann. Bei „multiprozessualer“ Anwendung (also Einsatzgebieten, wo mehrere Prozesse auf die Komponenten und Sicherheitseigenschaften zugreifen, wie z.B. E-Mail-Sicherheit oder Authentifizierung) hingegen ist Interoperabilität Programm und unabdingbar, und wird weitestgehend durch den Markt getrieben. Dies hat sich beispielsweise bei den Industriestandards S/MIME oder SSL gezeigt. Dennoch ist eine Anschubunterstützung wichtig, um eine mögliche Standardisierung in Aussicht zu stellen. Bestes Beispiel: die beiden etablierten E-Mail-Verschlüsselungsstandards PGP und S/MIME sind bis heute inkompatibel. Bei staatlichen Anwendungen ist hingegen auch der internationale Aspekt von Standardisierungen zu beachten. Fazit bleibt: Standards und Interoperabilität kann man nicht verordnen, der Markt muss sie fordern.

Die Anwendungsintegration ist ebenfalls vorrangig marktgetrieben. In diesem Bereich gibt es auch bisher nicht viele standardisierte Vorgehensweisen. Es zeigt sich aber, dass nicht nur die Algorithmen, sondern auch die Implementierungen (bei multiprozessualen Anwendungen) interoperabel sein müssen. Die Digitale Signatur ist ein Sonderfall: dort ist die Interoperabilität nicht nur auf Implementierungs- sondern sogar auf Dokumentenebene notwendig. Dies zeigt sich bei der qualifizierten Signatur, wo durch national unterschiedliche Regulierungen Interoperabilitätsprobleme auf internationaler Ebene entstanden sind. Ob das Ziel der Dokumenteninteroperabilität mit proprietären gesetzlich vorgeschriebenen Signaturverfahren erreicht werden kann, ist fraglich.

Der größte Bedarf im Bereich der Anwendungsintegration wurde im Bereich des Schlüsselmanagements identifiziert: Oft wird das Key Management noch als „proprietäre“ Eigenschaft der Anwendungsintegration gesehen, obwohl – insbesondere im Unternehmensumfeld – die Verwaltung der Schlüssel sich zunehmend als das Hauptproblem herauskristallisiert, sogar für monoprozessuale Anwendungen. Die Entwicklung gemeinsam verwendbarer Schlüssel oder alternativ die Verwaltung parallel existierender Schlüssel ist deshalb nach Meinung der Teilnehmer anzustreben.

Bei der Betrachtung „Sicherheit als Prozess“ wurde herausgestellt, dass es technische Anforderungen an Umsetzbarkeit und Akzeptanz gibt, die wiederholt über die Lebensdauer der Anwendung nachgehalten werden müssen. Dies bezieht sich insbesondere auf zwei Aspekte (auf die bei den Nutzungsbedingungen genauer eingegangen werden wird): die transparente Realisierung von Technik für den Benutzer (also dass er technische Zwänge nicht nachvollziehen können und sich nicht darauf einstellen muss), und wenige Entscheidungen für den Benutzer bzw. die weitestgehende Übernahme von Vertrauensentscheidungen durch die Technologie („Policy-based decision making“).

Es wurde auch die Notwendigkeit der Einführung von Tokens auf breiter Basis diskutiert. Dabei waren sich die Teilnehmer einig, dass eine Ergänzung der rein softwareba-

sierten Verwendung von Zertifikaten – auch wenn diese besser sind als die Verwendung von Passwörtern – mittelfristig notwendig ist. Die physische Gestaltung der Token wurde offen gelassen: ob Smart-Card im klassischen Chipkartenformat, als USB-Token, oder in Gestalt bestehender Devices wie etwa Handys, MP3-Player, Kameras oder PC-Platinen (als ‚Hardware-Module', Trusted Computing wurde von den Teilnehmern nicht genannt), oder im staatlichen Umfeld Ausweise – die Form wird nicht als relevant angesehen, weder für den prinzipiellen Erfolg von PKI noch für eine bestimmte Ausprägung. Hingegen wurde einhellig die Meinung vertreten, dass eine Kombination mit biometrischen Techniken nicht mehr zu vermeiden ist. Im Consumer- und Unternehmenskontext zwar vorrangig aus Usability- und Bequemlichkeitsgesichtspunkten, im staatlichen Bereich auch aus Sicherheitserwägungen heraus eingesetzt, dienen sie der eindeutigen Identifikation von Personen. Zur Interoperabilität wurde – konsequent zur Debatte bei der Anwendungsintegration – gesagt, dass es keinen Zwang, keine Regulierung dafür brauche, denn das werde „der Markt schon richten". Hingegen ist eine Förderung von bestimmten Token gebunden an die Akzeptanz der Verbraucher sinnvoll, weil diese nur in einem langwierigen Prozess durch eine kritische Masse erzeugt werden kann. Gerade die Smart-Card wird immer wieder in Frage gestellt, im staatlichen Umfeld ist sie aber – ergänzt durch die neuen Konzepte einer kontaktlosen Schnittstelle – noch immer favorisiert. Wichtig ist aber im Hinblick auf die Diskussion bezüglich der Austauschbarkeit der Algorithmen, dass auch die Smart-Cards bzw. allgemeiner die Tokens die Austauschbarkeit unterstützen.

Abschließend wurde die Sicherheit der technologischen Komponenten besprochen. Es wurde allgemein anerkannt, dass es einen Bedarf für die Transparenz der Sicherheit von Systemen und Komponenten gibt. Allerdings wurde die Produktzertifizierung, sowie sie bei Common Criteria praktiziert wird, nur für „langfristig stabile Prozesse" als sinnvoll erachtet. Für allgemein verwendete Software-Komponenten wie etwa einen Browser wird dagegen eine Prozess-Zertifizierung des produzierenden Unternehmens als deutlich sinnvoller gesehen, insbesondere aufgrund des damit verbundenen hohen zeitlichen und monetären Aufwands. Dabei wird eine Prozess-Zertifizierung keineswegs als Ersatz, sondern vielmehr als Ergänzung gesehen.

Am Rande wurde erwähnt, dass die neuen, aufkommenden IT-Technologien wie Service-Orientierte Architekturen, Smart Items und der ubiquitäre Gebrauch von intelligenten Geräten neue Vertrauensmodelle benötigen und damit Herausforderungen an die PKI-Implementierungen stellen werden.

Zusammengefasst ist festzustellen, dass die Teilnehmer folgende Auffassungen im Zusammenhang mit den technischen Perspektiven vertreten haben:

- → Die Austauschbarkeit von Algorithmen ist bei staatlichen Anwendungen sinnvoll, beim Unternehmenseinsatz eher nicht,
- → Interoperabilität und Anwendungsintegration sind vorrangig marktgetrieben,
- → Tokens werden kommen, aber der Formfaktor für Tokens ist nicht wesentlich,
- → Biometrie wird zunehmend eine wichtige Rolle spielen,
- → die isolierte Betrachtung von Mensch und Technik ist nicht sinnvoll.

### 4.2.2 Anmerkungen zu den „Betriebswirtschaftlichen Aspekten“

Von den Projektteilnehmern wurden Aspekte zur Strukturierung der beteiligten Akteure, der verschiedenen Stakeholder, und von Wirtschaftlichkeitsbetrachtungen vorgestellt.

Die Akteure sind nach folgenden Szenarien zu trennen: Subjekt-Subjekt, Subjekt-Objekt und Objekt-Objekt (wobei Subjekte natürliche oder juristische Personen sein können). In die Kategorie Subjekt-Subjekt fallen z.B. E-Mail-Kommunikation oder Instant Messaging, aber auch Online-Steuererklärungen. In die Kategorie Subjekt-Objekt fallen Web-Seiten oder „normale“ Anwendungen im Internet oder innerhalb einer Organisation und in die Kategorie Objekt-Objekt fallen die meisten System-Kommunikationen, so z.B. Zahlungsläufe oder Kreditkarten-Clearance-Prozesse oder auch automatisierte Online-Bestellprozesse. Diese Charakterisierung wurde so von den Teilnehmern als sinnvoll erachtet. Angemerkt wurde, dass mit dem Trend zu Service-Orientierten Architekturen die direkten Subjekt-Subjekt-Aktivitäten zunehmend durch Ketten der Form Subjekt-Objekt-Objekt-...-Objekt-Subjekt abgelöst werden, wobei die Objekte in der Mitte der Kette zu Beginn der Anfrage noch nicht feststehen müssen. Das wirft bzgl. Vertrauensbeziehungen und deren Verwaltung natürlich einen erheblichen Bedarf an Klärung, evtl. sogar Forschung auf.

Bezüglich der verschiedenen Stakeholder (B2B, B2C, G2C etc.) wurde vorgestellt, dass die Natur des Stakeholders für die PKI losgelöst von der Anwendung keinen Sinn macht, und erst durch die Betrachtung des von der PKI unterstützten Prozesses eine Unterscheidung sinnvoll wird. Das Problem dabei ist, dass eine Betrachtung jedes einzelnen Geschäftsprozesses enorm aufwendig ist. Grundsätzlich ist an diesem Punkt die Diskussion Infrastruktur vs. Prozess entbrannt. Dabei ist das gemeinsam identifizierte Problem, dass PKI als Infrastruktur aus Sicht des Einsparpotenzials nicht direkt prozessrelevant ist (wie unter anderem auch E-Mail oder Netzwerktechnologie). Dies gilt in gleicher Weise allerdings für jede Technologie. Die Investitionen in technologische Grundlagen, die neuartige Prozesse ermöglichen, sind immer kritisch betrachtet worden und hatten es schwer bei der Durchsetzung. Identitätsmanagement als größerer Rahmen von PKI ist dem gleichen Effekt unterworfen: ohne Grundlagentechnologie gibt es keine neuen, schlanken Prozesse mit Einsparpotenzial, wobei sich das Einsparpotenzial aber nicht für die Technologie-Treiber ergibt. Ergo ist PKI ein Geschäftsprozess-Enabler (wie Service-Orientierte Architekturen), der sich nur im Kontext von konkreten Prozessen betriebswirtschaftlich begründen lässt. Wenn das nicht geht, kann nur der „Glaube“ in Vorteile durch innovative Infrastrukturen zur Einführung einer PKI führen. Dieses Prinzip findet in Unternehmen aufgrund der immer stärkeren Kostenorientierung aber immer weniger „Anhänger“.

Somit ergeben sich zwei mögliche, finanziell motivierte, in der Natur ähnliche Argumentationen für PKI: PKI als Kosteneinsparungsmaßnahme, da damit Prozesse erstmalig digitalisiert werden können (z.B. elektronische Rechnungen) oder PKI als

Maßnahme zur Steigerung der Geschäftsprozesseffizienz, da damit bestehende Prozesse beschleunigt oder vereinheitlicht, also eleganter und mit weniger Aufwand elektronisch abgebildet werden können (z.B. Authentifizierung mit Zertifikaten bei Business Process Outsourcing).

Das generelle Problem ist, dass der Prozess-Verantwortliche in der Regel keinen Überblick über die Kosten eines Prozesses hat, weil die Kostenstrukturen in Unternehmen meistens an Infrastruktur- und Systemkomponenten hängen. Auch kann er oft den Nutzen wie auch das Risiko nicht quantifizieren. In der Summe ergibt sich, dass Prozess-Kosten sehr schwer zu berechnen sind, demzufolge Einsparungen eher selten objektiv nachgewiesen werden können und wenig vergleichbar sind, da sie direkt an die Komplexität des Geschäftsmodells des Unternehmens gekoppelt sind. Es bleibt somit festzuhalten, dass PKI als Enabler für Geschäftsprozesse Vorinvestitionen erfordert und damit die Entscheider von der Sinnhaftigkeit von PKI überzeugt sein müssen, weil eine rein betriebswirtschaftliche Betrachtung aufgrund von Prozess-Kosten-Einsparungen in der überwiegenden Anzahl der Fälle nicht sinnvoll möglich ist.

Unabhängig davon ist festzustellen, dass eine nicht unbeträchtliche Anzahl von PKIs schon in der Praxis ausgerollt wurden; gerade multinationale Unternehmen haben in der einen oder anderen Form schon PKI-Projekte realisiert. Oft wird aber die PKI nicht so flächendeckend genutzt, wie sie genutzt werden könnte. Ein positives Beispiel ist Siemens, wo die PKI mit Anwendungsservices wie Authentifizierung verknüpft ist und damit eine Motivation für Fachabteilungen besteht, sich dieser Services zu bedienen. Bei aller Diskussion wurde daher auch von den Teilnehmern bestätigt, dass es durchaus eine Reihe von erfolgreichen Implementierungen gibt.

Ein wesentlicher Teil der Diskussion drehte sich um das Thema „Return on Security Investment“ (ROSI). Auch wenn das Thema nicht direkt PKI-relevant ist, spielt es doch bei den Diskussionen um betriebswirtschaftliche Betrachtungen von Sicherheits-Maßnahmen immer eine zentrale Rolle. Grundsätzlich geht es dabei um die Frage: will man Schaden eindämmen, also Maßnahmen gezielt einsetzen, um bestimmte Ereignisse in ihrer Wirkung zu schwächen, oder will man – analog einer Versicherung – Vorsorge treffen, damit generell der Status Quo besser geschützt bleibt. Damit ist ROSI nicht auf Sicherheit beschränkt, die Frage stellt sich für alle möglichen Risiken, die ein Unternehmen bedrohen. Das wesentliche Problem dabei ist – in beiden Alternativen -, dass ROSI wie „Kaffeesatzleserei“ ist, denn die Kalkulationen gehen immer vom „verhindertem angenommenen Schaden“ aus. Das impliziert aber die Annahme, dass ein Schadensfall nicht nur mit einer gewissen Wahrscheinlichkeit eintritt, sondern sogar (im Verhältnis der Wahrscheinlichkeit) tatsächlich irgendwann aufträte, wenn die schützende Maßnahme nicht umgesetzt würde – eine Annahme, die jeder empirischen Grundlage entbehrt.

Wenn aber der Nutzen nicht direkt monetär ausgedrückt werden kann, so kann man dennoch versuchen, den Nutzen zumindest qualitativ zu erfassen. Nun ist bei PKI

ein wesentlicher Faktor, dass „in der Natur der Dinge von PKI das Asymmetrische“ liegt. Das heißt, aus Nutzengesichtspunkten ist es sehr wahrscheinlich – und das zeigt auch die Praxis -, dass der, der den Aufwand zu tragen hat, oft keinen direkten Nutzen daraus ziehen kann. Nun haben die Betrachtungen zu PKI als Infrastruktur gezeigt, dass ein gewünschter Kosten-Nutzen-Transfer auf der Infrastrukturebene gar nicht stattfinden kann, sondern erst auf der Ebene der Geschäftsprozesse. Das geht innerhalb eines Unternehmens oder einer Organisation auch relativ gut – im Rahmen der Möglichkeiten, in denen eine Infrastruktur-Investition überhaupt auf Prozess-Ebene als Nutzen erkenntlich gemacht werden kann. Bei organisationsübergreifenden Prozessen ist dagegen klar, dass ein Kosten-Nutzen-Transfer nur schwer zu realisieren ist. Das ist auch der Grund dafür, dass Bezahlmodelle bzw. Ansätze zur Verlagerung der Kosten keine Akzeptanz im Markt finden – ein Grund für den Niedergang der Trust Center. Es muss daher andere Motivatoren für die Kostenübernahme geben – und zu den „Kosten“ zählen nicht nur Produkt- und Projektkosten, sondern auch weiche Faktoren wie Gewohnheitsänderungen, Schulungsbedarf oder Abgabe von Kontrolle. Eine mögliche Motivation – die aber erfahrungsgemäß nicht lange anhält – ist die der Compliance, also dass das Risiko für Geschäftsführer verringert wird. Entsprechend könnte es motivierend sein, PKI als Enabling-Technologie einzusetzen, wenn die Haftung auf der Seite des Dienste-Anbieters verstärkt wird. Ein Gegenargument könnte sein, dass dadurch die Innovationsgeschwindigkeit verringert wird.

Daneben bleibt auch die Möglichkeit, nachzuweisen, dass die Sicherheit von Informationen verbessert worden ist. Das ist ein wichtiges Feld, und bisher gibt es dort keine nennenswerten Ergebnisse. Das liegt hauptsächlich daran, dass der Wert von Informationen so schwer zu bestimmen ist (genau genommen kann nicht der Wert von Informationen bestimmt, sondern nur jeweils der Wert von Verfügbarkeit, Integrität und Vertraulichkeit von Information zu schätzen versucht werden), und daran, dass Vorfälle so schwer quantifiziert und nachvollziehbar erfassbar sind. Letztendlich brauchen wir hier die Kompetenzen und Erfahrungen der Versicherungsbranche. Es stellt sich die Frage, wann die Versicherungsbranche in der Lage ist, IT-Sicherheit zu berechnen, wenngleich ein Vertreter der Versicherungswirtschaft im Laufe der Veranstaltung argumentierte, die Versicherungsbranche habe kein Interesse, Anstrengungen in diese Richtung zu unternehmen.

Zusammengefasst kann man feststellen, dass PKI ohne Anwendung nur eine Infrastruktur ohne Wert ist. Der Wert entsteht aus den unterstützten, nun neu möglichen Prozessen. Gibt es keine neuen Prozesse, die damit unterstützt oder verschlankt werden können, braucht man auch keine PKI. Konsequenterweise kann – auf die Spitze getrieben – PKI zu einer ROSI-Berechnung nichts beitragen. PKI ist in erster Linie „Business Enabler“, und nur nachrangig Sicherheitstechnologie.

PKI muss den Beweis antreten, dass ein Prozess ohne PKI teurer wird als mit ihm. Ist PKI aber einmal etabliert, so zeigen die positiven Beispiele, sind die Vorteile für die Unterstützung weiterer Geschäftsprozesse offensichtlich.

### 4.2.3 Nutzungsbedingungen

Der dritte Vortrag zu Beginn der Veranstaltung bezog sich auf die „alltäglichen Wahrheiten“ von PKI im Einsatz. Die Erkenntnisse aus anonymisierten Interviews mit Praktikern wurden zu 4 Themenblöcken vorgestellt: Produkte, Projektvorgehen, Einsatz und Haftung. Einer der Teilnehmer machte am Anfang des Vortrags eine Bemerkung, dass Sicherheit aus Vertrauen und Kontrolle bestehe; diese Einschätzung ist hilfreich, um einige der Kommentare entsprechend bewerten zu können.

Bei Produkten machen inzwischen Open Source Lösungen einen großen Anteil aus, oft finden sich aber auch Eigenentwicklungen und individuell in die Geschäftsprozessanwendungen integrierte Projektlösungen. Erste Produkte im PKI-Bereich sind inzwischen wieder vom Markt genommen worden, dabei handelt es sich aber nicht um Prozessintegrations-Komponenten sondern um Infrastrukturprodukte. Lösungen von der Stange sind in der Praxis eher selten, der Markt ist demnach noch nicht „commoditized“, also noch kein Massenmarkt. Dazu passt, dass die Interoperabilität zwischen Lösungen oft noch nicht so weit ist wie es für die Kunden wünschenswert wäre. Das betrifft insbesondere das Schlüsselmanagement. Kunden wünschen sich eine zentrale Verwaltung von allen Schlüsseln in ihrer Organisation statt der heute üblichen anwendungsspezifischen Verwaltung. Dafür ist aber die Interoperabilität bei der Schlüsselverwaltung unbedingte Voraussetzung. In der Praxis haben sich die unterschiedlichen Regulierungen von Krypto-Einsatz und -Import – obgleich für Verschlüsselung und nicht für Authentifizierung und digitale Signatur gedacht – als größte Hürden in diesem Zusammenhang erwiesen. Dies trifft naturgemäß nur für internationale Unternehmen zu.

Zum Projektvorgehen wurde mehrfach angemerkt, das PKI kein Selbstzweck ist und damit anderen Projektzielen untergeordnet sein muss. Hier ist ein Verweis auf den vorigen Abschnitt (Kapitel 4.3.2) zur prozessorientierten Betrachtung angebracht. Ein unseres Erachtens noch wichtigerer Punkt ist die Beobachtung, dass PKI-Projekte „empfindlich“ sind. Darunter verstehen wir, dass sich die Anforderungen und Bedingungen, die sich im Laufe des Projektes oft ändern, den Erfolg des PKI-Projektes in Frage stellen können. Die größten Schwierigkeiten sind aber meist politischer Natur. Das wurde von vielen Workshop-Teilnehmern bestätigt. Hauptgrund ist paradoxerweise die Vertrauenswürdigkeit der Prozesse, die mit PKI eingeführt werden, denn die neue Vertrauenswürdigkeit bedeutet gleichzeitig eine Einschränkung der Freiheit von Prozessbeteiligten, also einen individuell empfundenen Kontrollverlust: die Beteiligten können die Prozesse somit nicht mehr nach eigener Einschätzung (möglicherweise durchaus im Sinne des Unternehmens) manipulieren. Abstrakter formuliert: PKI zentralisiert Vertrauensentscheidungen und sichert einen vorgesehenen Prozessablauf – gewolltes Ziel der Unternehmensleitung. In der Praxis ist dies aber schwer durchsetzbar, weil es den individuellen Interessen der Mitarbeiter entgegenläuft bzw. entgegenlaufen kann. Entsprechend stark sind die individuell empfundenen Veränderungen durch die Realisierung eines PKI-Projektes.

Am Anfang der Diskussion um das von uns intendierte Hauptdiskussionsthema der Einsatzbedingungen stand die Feststellung, dass der Nutzen von IT-Sicherheit im Allgemeinen für den Anwender nicht fassbar ist. Dementsprechend bringt er kein Verständnis auf für zusätzliche Handlungen oder Entscheidungen, die im Umfeld von IT-Sicherheit erforderlich werden. Die Erwartung (und diese ist sowohl für Verbraucher als auch für Anwender im Unternehmensumfeld gleich) ist, dass die Geschäftsprozesse, in die sie eingebunden sind, sicher sind, und dass kein eigener Beitrag zur Sicherheit des Prozesses notwendig sein darf.

Um eine Akzeptanz für PKI-Anwendungen zu schaffen, müssen deshalb Vertrauensentscheidungen (die heute bei PKI-Anwendungen in den gängigen Produkten durch den Anwender zu treffen sind, so z.B. „möchten Sie diesem Zertifikat vertrauen?") einfach und transparent, also im Kontext und in der Sprache des Geschäftsprozesses leicht nachvollziehbar sein. Es darf keine vom Geschäftsprozess losgelöste Entscheidung getroffen werden müssen. Was wäre auch deren Wert? Ich vertraue ja auch keiner Person in vollem Umfang zu jedem Thema, Vertrauen ist immer auf eine Transaktion bezogen. Aus Akzeptanzgründen sind deshalb idealerweise keine Entscheidungen durch den Anwender zu treffen und die entsprechenden Alternativen durch die Vertrauensparameter des Geschäftsprozesses vorweggenommen.

Erfahrene PKI-Projektleiter berichteten, dass der Aufwand für den Support, also Help-Desk, Onsite-Schulungen bei PKI ungleich höher sei als durchschnittlich bei IT-Projekten beobachtet. Einerseits warnten sie davor diesen Teil des Projektes zu unterschätzen, andererseits wurde mehrfach darauf hingewiesen, dass es für den Gesamtprojekterfolg unbedingt notwendig sei, im Help-Desk geschulte Mitarbeiter zu haben, die die Sicherheitsvorgaben nicht durch falsche Hinweise korrumpieren. Die Teilnehmer bestätigten, dass die formalen Handbücher wie das „Certificate Practice Statement", in der Praxis nicht benutzt würden, „diese seien etwas für Juristen".

Die Akzeptanzproblematik wurde unter der Berücksichtigung weiterer Punkte diskutiert. Einige behaupteten, das sei ein „technisches" Problem, sprich: die fehlende Akzeptanz komme von mangelnder Reife der technischen Komponenten. Andere behaupteten, dass die Menschen den Umgang mit der Technologie und neuen Vertrauensmodellen erst lernen müssten: „Akzeptanz braucht Zeit, Vertrauensbildung im Internet ist eine Generationensache".

Letztendlich ist für den Anwender zentral, ein subjektives Gefühl der Sicherheit zu haben, um den Geschäftsprozess annehmen zu können. Das tatsächliche Sicherheitsniveau kann dabei durchaus gering sein. Dieses subjektive Gefühl ist sehr individuell: ein sehr erfahrene PC-Anwender mit ausgeprägtem Sicherheitsbewusstsein fühlt sich deutlich sicherer, wenn er Vertrauensentscheidungen selbst treffen kann, während ein Durchschnittsanwender dadurch eher (v)erschreckt wird.

Weiterhin wurde bestätigt, dass die wirklich schweren Probleme bezüglich der Akzeptanz erst bei organisationsübergreifenden Prozessen auftreten, weil gerade

dort die Vertrauensentscheidungen nicht einfach und/oder nachvollziehbar sind. Es wurde mehrfach erwähnt, dass aus IT-Leiter-Sicht häufig nicht klar ist, wer in einem solchen Szenario für die IT-Komponenten verantwortlich zeichnet. Letztendlich, so die Workshop-Teilnehmer, müsse man zwischen drei verschiedenen Szenarien unterscheiden:

- → Massenmarkt (Online Shopping, Homebanking, etc.): dort muss die Benutzung für den Anwender so leicht und so billig wie möglich sein. Dies kann durchaus bedeuten, dass PKI-Lösungen aufgrund ihrer Komplexität keine Anwendung finden. Zumindest sind in diesem Kontext die Anforderungen an Einfachheit, Transparenz und minimale Kosten für PKI-Lösungen besonders hoch.
- → Unternehmenseinsatz: in diesem Umfeld ist eine größtmögliche Flexibilität erforderlich, d.h. je nach Höhe der Sicherheitsanforderungen müssen unterschiedliche Modelle, von der Technologie bis zur Stringenz der Mitarbeiterhandlungen, um- und durchgesetzt werden. In diesem Umfeld besitzen Standardisierungen nicht die höchste Priorität, Insellösungen sind hier durchaus sehr erfolgreich. Standardisierung wird sich nach Marktregeln etablieren.
- → Einsatz mit staatlichem Interesse (Ausweise, aber auch steuerrelevante Prozesse der Finanzverwaltung): dort ist Standardisierung, in Verbindung mit hoher Sicherheit und Nachhaltigkeit erforderlich. Entsprechend sind Austauschbarkeit der Algorithmen, Einsatz von Biometrie und vorkonfigurierte Vertrauensentscheidungen als grundsätzlich nutzbare Standards gesetzt.

Alle drei Szenarien funktionieren nach eigenen Marktdynamiken. Somit ist eine Vergleichbarkeit der PKI-Anwendungen nur schwer möglich, insbesondere bezüglich ihrer Einsatzbedingungen.

Bei der Diskussion um Haftungsfragen wurde einmütig festgestellt, dass qualifizierte Zertifikate mit heutigem Stand kaum verwendet werden. Die „A-Priori"-Regulierung der Haftungsfrage sei weltfremd; es wird stattdessen empfohlen, mit PKI-Anwendungen unterschiedlicher Sicherheitsstufen in die Anwendung zu gehen und auf das „gelebte Recht" zu warten. Die Sinnhaftigkeit des Sicherheitsniveaus von qualifizierten Zertifikaten wurde nicht in Frage gestellt, alleine die „staatliche Verordnung" dieses hohen Sicherheitsniveaus, verbunden mit den Kosten für alle Beteiligten, wurde kritisiert. Darüber hinaus sollte die Haftungsfrage wegen des Einsatzes von PKI nicht neu gestellt werden, da sie schon für den Geschäftsprozess beantwortet werden muss.

Als Fazit ergibt sich: wir brauchen einfache und nachvollziehbare Vertrauensentscheidungen für den Benutzer. Viele Tools machen es sich zu leicht und dem Benutzer zu schwer. Darüber hinaus müssen die unternehmenspolitischen Probleme vorher gelöst werden, um den Einsatz einer PKI erfolgreich machen zu können. Dabei ist zu beachten, dass diese Probleme nicht mit technischen „Kniffen" erledigt werden können, auch wenn die Technologie damit unter Umständen vor neue Anforderungen gestellt wird – das Problem ist menschlich / soziologisch und muss dementsprechend ange-

gangen werden. Es empfiehlt sich somit, bei PKI-Projekten Change-Management-Experten hinzuzuziehen. Qualifizierte Zertifikate „sind die Mühe nicht wert" – zumindest für den Unternehmenseinsatz ist das Kosten-Nutzen-Verhältnis nicht akzeptabel. Wir brauchen stattdessen mehr Interoperabilität, und zwar an zwei wesentlichen Stellen: bei der Integration der PKI in Geschäftsprozesse und bei der Verwaltung der Schlüssel. Wir müssen darüber hinaus weiter Konzepte entwickeln, um einfache(re) organisationsübergreifende Vertrauensbeziehungen zu modellieren, wie z.B. „Instant workgroups". Wesentlich zu beachten dabei ist, dass Vertrauen prozessbezogen ist und einem Kommunikations- oder Geschäftspartner nicht grundsätzlich entgegengebracht werden kann. Die Tools müssen diese Orientierung widerspiegeln.

Unseres Erachtens ist die wichtigste Erkenntnis aus diesem Abschnitt folgende: Sicherheit ergibt sich aus Vertrauen und Kontrolle und Reduzierung von Kontrolle kann nur durch Aufbau von Vertrauen kompensiert werden.

### 4.3 Ergebnisse der Break-out-Sessions

Die Break-Out-Sessions hatten zum Ziel, die Teilnehmer in strukturierter Diskussion identifizieren zu lassen, was aus ihrer Sicht
→ Problemfelder darstellt,
→ welche Situation erstrebenswert wäre und
→ welche notwendigen Maßnahmen dafür zu ergreifen wären.

Im Folgenden wird das Ergebnis der Gruppen sowie das Feedback der Teilnehmer im Plenum kurz skizziert.

#### 4.3.1 Gruppe „Grün"

**Als Problemfelder wurden identifiziert:**
→ Es besteht eine Vorfinanzierungsnotwendigkeit durch die Infrastruktur-Kosten,
→ PKI ist zu teuer und
→ im Roll-Out zu komplex,
→ es fehlen Killer-Applikationen /-Prozesse,
→ der Zugang zu PKI ist zu kompliziert,
→ der Nutzen wird nicht gut verkauft,
→ der Einsatz von PKI wird nicht gefordert und gefördert,
→ es existiert keine (Standard-) PKI für verbreitete Komponenten.

**Wunschzustände waren:**
→ Einheitliche Standards werden benötigt,
→ Vertrauen muss geschaffen und Kontrolle ermöglicht werden,
→ Unternehmensentscheidungen für PKI müssen auf der Basis eines unternehmensweiten Konzepts getroffen werden,
→ PKI ist bei neuen Projekten ein „Muss",

→ bei einer Migration zu PKI gibt es für bestehende Anwendungen finanzielle Anreize,
→ „jeder hat ein Zertifikat dem man vertrauen kann“,
→ Vertrauliche Information ist verschlüsselt und nur Berechtigten zugänglich,
→ kostengünstiger Zugang und honorierter Einsatz,
→ einfache, transparente Technologie,
→ weltweite Umsetzung mit z.B. Bridge-CAs und ID-Karten,
→ PKI für Trusted Computing.

**Als mögliche Maßnahmen wurden identifiziert:**
→ Kompatibilität fördern,
→ interdisziplinären Austausch voranbringen,
→ Lösung der organisatorischen Zuständigkeit in Unternehmen,
→ Budgetneutralität für PKI entwickeln,
→ Globale Bürgercard oder Bankcard etablieren,
→ (Federated) Identity Management weiterentwickeln,
→ universelle Nutzbarkeit und Verfügbarkeit sicherstellen,
→ globale ID fordern,
→ in Trusted Computing investieren.

**Als gemeinsames Statement im Plenum wurden von der Gruppe „Grün“ folgende Forderungen gestellt:**

1. Derjenige der die Kosten für eine PKI-Infrastruktur trägt muss am Benefit teilhaben. Um das zu erreichen, müssen einerseits Best Practices zusammengestellt und andererseits mit Betriebswirten Modelle entwickelt werden, die eine „Benefit-Umkehr“ realisieren.
2. Die Anwendung von PKI muss reguliert werden, sprich: dort wo es volkswirtschaftlich sinnvoll ist, muss die Verwendung von PKI gesetzlich verpflichtend gemacht werden.
3. Es muss eine globale Infrastruktur mit einer Karte geben. Auch wird eine staatliche Verantwortung gesehen, diese Infrastruktur interoperabel bereitzustellen.

### 4.3.2 Gruppe „Rot“

**Als Problemfelder wurden identifiziert:**
→ momentane Lösungen werden von Nutzern als ausreichend angesehen,
→ weltweite Interoperabilität fehlt,
→ fehlendes Vertrauen potentieller Anwender,
→ Mehrwert von PKI ist nicht messbar (es gibt kein Mess- bzw. Bewertungsverfahren, auf dessen Grundlage mit Entscheidern diskutiert werden kann, dass sich PKI lohnt),
→ dort wo PKI funktioniert, sind es nur Insellösungen, die eine flächendeckende Durchsetzung nicht vorantreiben,
→ bereits existierende Systeme verhindern die Verbreitung von PKI,

→ starke Politisierung des Themas, dadurch Mitbestimmungsrechte unterschiedlichster Gruppen,
→ zu wenig normativer Zwang (Gesetze),
→ mehr Sicherheit kostet, hat aber keinen erkennbaren monetären Nutzen, Sicherheit ist nicht fassbar,
→ ROI als Bewertungsverfahren schwierig bzw. sogar unpassend.

**Wunschzustände waren:**
→ PKI als Versicherungsleistung,
→ PKI mit Service – und Wartungsleistungen,
→ klare, vergleichbare Bewertungsverfahren,
→ übergreifendes Framework (PKI, die sich bei einem Unternehmen bewährt hat, sollte auch anderen zur Verfügung gestellt werden, dadurch Herstellung einer funktionierenden Infrastruktur),
→ PKI muss technisches Hilfsmittel sein (nicht mehr und nicht weniger),
→ interdisziplinäre Diskussion, um ein vernünftiges Businessmodell aufzustellen (Einbeziehung von Technikern, Betriebswirten und Sozialwissenschaftlern),
→ Bridge Szenarien fördern (übergreifendes Vertrauen schaffen),
→ Service-Orientierte Architekturen etablieren,
→ PKI als automatische und unsichtbare Technologie gestalten,
→ keine Veränderung der Entscheidungsprozesse vornehmen.

**Als Lösungen wurden diskutiert:**
→ Bei PKI muss der Fokus nicht auf Infrastruktur, sondern auf Integration und Interoperabilität liegen,
→ bestehende Lösungen schrittweise ablösen bzw. in PKI integrieren,
→ globale Identitätskarte (Ausgabe nicht durch Unternehmen, sondern durch Autoritäten),
→ Regulierung der Anwendungen (Gesetze),
→ Nachfrage schaffen, erhöhen,
→ Standards und Gesetzgebungen zur Vereinheitlichung schaffen,
→ Bewusstsein der Anwender erhöhen (bspw. Best Practice Forum, Schulungsmaßnahmen).

**Im Plenum wurden die folgenden drei Forderungen / Vorschläge vorgestellt:**
1) Vertrauen und Sicherheit immer in den Kontext stellen. Dies impliziert eine Prozess-Sichtweise bei PKI einzunehmen.
2) Interne und externe Sicht unterscheiden. Dies passt zu der Anmerkung, dass PKI in verschiedenen Szenarien nicht direkt vergleichbar ist.
3) Den Schwerpunkt auf Integration in Anwendungen legen

### 4.3.3 Gruppe „Blau“

**Die folgenden Probleme wurden identifiziert:**
→ mangelnde einfache Bedienbarkeit,

→ fehlende einfache, integrierte Verwaltungsfunktionalität, insbesondere im Unternehmensumfeld,
→ mangelnde Flexibilität im Einsatz,
→ im Verbraucherumfeld zu viele Insellösungen,
→ die Einstiegsschwelle zu PKI ist zu teuer,
→ die Akzeptanz bei Benutzern ist zu gering,
→ falsche Erwartungen im Markt durch das Signaturgesetz,
→ zu wenig Wissen über Kostenstrukturen im PKI-Umfeld.

**Diskutierte Wunschzustände:**
→ einheitliche Standards,
→ Transparenz über Kosten und Nutzen von PKI,
→ PKI ist eine etablierte „Enabler-Technologie",
→ PKI wird in der öffentlichen Wahrnehmung positiv empfunden,
→ die wesentlichen Geldgeber sind über PKI gut informiert,
→ bei Ausschreibungen ist PKI Teil der Anforderung,
→ die, die mehr investieren in PKI werden belohnt,
→ es gibt einen erkennbaren Nutzen von PKI, und zwar sowohl im Unternehmens- als auch im Consumer-Umfeld.

**Als mögliche Lösungen wurden vorgestellt:**
→ weitere Standards entwickeln,
→ Best Practice Sharing zwischen Unternehmen, um die „Angst vor PKI" zu nehmen,
→ der Preis für Kosten und Nutzen von PKI muss bestimmt werden,
→ durch technologische Innovationen die Bedienerfreundlichkeit verbessern,
→ grenzüberschreitend Standards vereinheitlichen,
→ der Gesetzgeber muss die Standardisierung einfordern um die Interoperabilität zu fördern, aber ohne zu überregulieren.

**Die im Plenum vorgestellten Thesen waren wie folgt:**
1) Nachfrage schaffen: durch anwendungsorientierte Forschung und staatliche Förderung und Incentives, wie etwa Vorteile für den Kunden die sicheres online Banking machen, Fördern der Leute die PKI verwenden (ähnlich Steuererleichterungen bei Autos mit weniger Abgasen).
2) Standards schaffen: Gütesiegel einführen, evtl. mit Gesetzgebung Standardisierung einfordern.
3) Bewusstsein stärken: Bewusstsein aller Anwender branchenübergreifend erhöhen (Ausbildung, Best Practice)

### 4.3.4 Fazit

Die Gruppen haben sehr unterschiedliche Empfehlungen ausgesprochen: von sehr drastischen, wie der gesetzlichen Forderung von PKI bis zu den üblichen, weichen Maßnahmen wie Bewusstsein erhöhen und Ausbildung verbessern. Allen gemein

waren aber eine optimistische Grundstimmung und die Grundannahme, dass der Wert von PKI erst gehoben werden kann, wenn Starthilfe zur Verfügung steht.

Bei der Vorstellung der Gruppenergebnisse und der abschließenden Diskussion wurde noch einmal betont, dass im Unternehmensumfeld die Anwendung, der Prozess im Zentrum steht, und dass PKI eine Möglichkeit ist, Sicherheit zu schaffen. Weiterhin gelte: PKI hat erst mit Sicherheit zu tun, wenn Funktionen im Business Case genutzt werden. Zuvor ist es reine Infrastruktur.

PKI-Technologie muss sich gegen die anderen möglichen Verfahren beweisen. Anders sieht es im staatlichen Kontext aus: dort müsse gefordert werden, dass es keine Identitätskarten ohne Integration einer PKI geben dürfe. Bei unternehmensübergreifenden Prozessen wurde festgestellt, dass die Integration durchaus problematisch sein kann, wenn Unternehmen im Wettbewerb stehen. Die Teilnehmer stellten aber gemeinsam fest, dass Sicherheit kein wettbewerbsfördernder Faktor für Unternehmen untereinander sein sollte, sondern für Lösungen und elektronische Geschäftsprozesse. Die Unternehmen sollten also bei der Auswahl von sicheren Prozessen mit einem PKI-Angebot unterstützt werden.

## 4.4 Ergebnisse des Workshops

Der Workshop war sicherlich ein Erfolg. Er hat einerseits viele Annahmen bestätigt und andererseits einige interessante Aspekte in neues Licht gestellt. Interessant war, dass es zu vielen Themen durchaus widersprüchliche Aussagen im Verlauf des Workshops gab, insbesondere zum Frage „wie viel Förderung braucht PKI / soll PKI erfahren“. Der Beitrag der Nicht-PKI-Experten war in diesem Kreis besonders anregend, weil sie die PKI-Diskussion immer wieder in einem größeren Kontext betrachtet haben. Daraus resultiert für uns die wesentliche Erkenntnis, dass PKI aus dem Kreis der Experten herausgezogen und in einem breiteren Zusammenhang betrachtet werden sollte.

Wir fassen unsere Erkenntnisse nochmals zusammen:

### 4.4.1 Technologie

Eine der Haupterkenntnisse aus technologischer Sicht ist, dass PKI-Technologie keinen Selbst-Zweck hat, sondern nur im Kontext sinnvoll eingesetzt werden kann. PKI ist Prozess-Enabler, erlaubt neue Prozesse oder bestehende Prozesse jetzt rein elektronisch abzubilden. Die Interoperabilität innerhalb der PK-Infrastrukturen wurde überbewertet, viel wichtiger ist es, die Integrationsfähigkeit in Anwendungen und Prozesse zu verbessern und zu standardisieren. Zwar gibt es Schnittstellen für die Verwendung von PKI-Funktionen aus Anwendungen heraus (beispielsweise PKCS [Public Key Cryptography Standards]), aber die Abbildung auf Vertrauensbeziehungen innerhalb der jeweiligen Anwendung hat in weiten Teilen nicht

geklappt. Erst jetzt, mehr als 10 Jahre nach der flächendeckenden Einführung von SSL für Web-Server und Browser, ist es zum Beispiel möglich, direkt im Browser zu erkennen, ob eine Web-Seite wirklich vertrauenswürdig ist (Stichwort: „Extended Validation Certificates"). Interessant und „merk-würdig" ist die Aussage eines Teilnehmers: „wir sollten PKI als Public-Key-Integration verstehen, nicht als Public-Key-Infrastruktur, das ist die eigentliche Herausforderung".

Die Verwendung von Token, in verschiedenster Art und Form, wird sich mittelfristig durchsetzten. Der Markt wird den Formfaktor und auch die Anbieterstruktur selbst regulieren. Insbesondere gehen wir davon aus, dass eine flächendeckende PKI-Integration in Anwendungen die Frage nach den Token über deren praktische Nutzung entscheidet.

Auch die Beurteilung von Bedienerfreundlichkeit und Benutzungsschnittstelle geht in die gleiche Richtung: es wurde festgestellt, dass zu viele Vertrauensentscheidungen vom Benutzer getroffen werden müssen, heute oft noch außerhalb des Prozess- / Anwendungskontextes . Das überfordert den Benutzer und gibt ihm darüber hinaus das Gefühl, die Technik nicht zu beherrschen. Der Grund dafür ist, dass das Prozessverständnis und die Integrationsbereitschaft in Anwendungen bei den meisten PKI-Entwicklern nicht ausreichend ausgebildet sind. Bei den Benutzungsschnittstellen wird davon ausgegangen, dass eine Vertrauensentscheidung grundsätzlich getroffen werden muss und nicht, wie im „nicht-technischen" Leben, bezogen auf eine bestimmte Aktivität und/oder einen Prozess. Wir sehen deshalb den deutlichen Bedarf, die PKI-Technologen mit den Prozess-Designern zusammen in einen Dialog zu bringen. Davon würden unseres Erachtens nach beide Parteien deutlich profitieren: die Prozesse würden sicherer und nachvollziehbarer, und die PKI würde in die Anwendung integriert.

Für die IT-Verantwortlichen (und letztlich auch den Verbraucher zu Hause) wird mittelfristig die Verwaltung vieler Schlüssel und Zertifikate zur Herausforderung – ähnlich wie bei der Verwaltung von Passworten. Daher brauchen wir einen Ansatz zur Interoperabilität der Schlüsselverwaltung, damit zentrale Verwaltungstools, aber auch Verbraucher-orientierte Anwendungen (siehe z. B. Projekt Higgins, „InfoCard") Schlüssel und Zertifikate von beliebigen Anwendungen verwalten können. Damit ist nicht gemeint, dass das Vertrauensmanagement mit diesen Tools abgedeckt werden sollte. Im Gegenteil: die Verwendung und den Zweck des Schlüssels / der Zertifikate sollte frei vergebbar sein und durch die Anwendung bestimmt werden.

### 4.4.2 Betriebswirtschaftliche Aspekte

PKI basiert auf asymmetrischer Kryptographie – es liegt in der Natur dieser Technologie, dass auch Kosten und Nutzen asymmetrisch verteilt sind. Ein Ausgleich ist schwierig (wenn es einfach wäre, hätte es schon entsprechende Geschäftsmodelle gegeben), dennoch ist es für den Erfolg von PKI unabdingbar, dass auch derjenige,

der die Kosten zu übernehmen hat einen Benefit erhalten muss, genauso wie umgekehrt, dass derjenige, der den Nutzen hat, auch die Kosten tragen oder sich zumindest daran beteiligen sollte.

Wie im Laufe des Workshops festgestellt wurde, ist eine Kosten-Nutzen-Betrachtung von PKI Technologien nur sinnvoll im Kontext der jeweiligen Geschäftsprozesse. Derartige Kosten sind aber mit den heutigen Mitteln nur schwer zu berechnen, insofern ist eine enge ROI-Betrachtung im Umfeld von PKI im Prinzip „Kaffeesatzleserei". Um den Nutzen von PKI besser erfassen zu können, müssen wir Kosten und Nutzen von Geschäftsprozessen besser erfassbar machen, und zwar insbesondere bezüglich der Vertrauenselemente dieser Prozesse. Dabei gibt es zwei sehr unterschiedliche Sichten: die unternehmensinterne Sicht (Optimierung von Abläufen) und die externe Sicht (Kundenanforderungen, Gesetze etc.). Bei der unternehmensinternen Sicht muss PKI die Investitionen wie jede andere Infrastruktur-Technologie durch Einsparungen, etwa den Wegfall zusätzlicher Kontrollen rechtfertigen. Bei der externen Sicht kann unter Umständen eine Rationalisierung durch Selbstbedienung, etwa für Authentisierung, PKI interessant machen. Dort stellt sich dann aber wieder die Frage, wer Kosten und wer Nutzen hat.

Eine weitere wesentliche Erkenntnis ist, dass die Bedingungen und Erfolgskriterien für PKI in den drei Szenarien Unternehmensprozesse, Verbraucher und Staatliches Interesse sehr unterschiedlich sind, und sich damit die Rahmenbedingungen des Einsatzes nur bedingt vergleichen lassen. Insbesondere scheint es sehr schwer zu sein, Transfer-Möglichkeiten zu erreichen, um neue Geschäftsmodelle durch Anwendung von Technologien / Prozessen in dem jeweils anderen Szenario erfolgreich zu realisieren. Zum Beispiel stellen qualifizierte Zertifikate im Verbraucher- und Unternehmensmarkt keine sinnvolle Einsatzalternative dar, im Gegensatz zu staatlichen Prozessen (etwa: Gerichtsverfahren und elektronische Akten). Ein weiteres Beispiel in diesem Zusammenhang bezieht sich auf die Austauschbarkeit von Kryptoalgorithmen: diese lohnt sich bei Personalausweisen (wenn die kryptographische Hardware das unterstützen würde), nicht aber bei Standard-Unternehmensanwendungen (wie etwa VPN-Technologie, auch wenn durch Industriestandards bei den Algorithmen zunehmend Invesitionssicherheit greifbarer wird).

### 4.4.3 Sozialwissenschaftliche Aspekte

Sicherheit besteht aus Vertrauen und Kontrolle – das ist eine der wesentlichen Erkenntnisse dieses Workshops. Vertrauen, weiter gedacht, ergibt sich aus Erfahrung und der Bereitschaft, positive Erfahrungen zu einem gewissen Grad zu projizieren. Menschen fühlen sich sicher, wenn sie noch keine schlechte Erfahrung gemacht haben, also noch keine Angst in einem bestimmten Kontext verspürt haben. Haben sie Angst, tendieren sie zur Kontrolle, um die Ursachen für diese Angst auszuschließen. Aus dieser Position heraus ist es sehr schwierig, erneut Vertrauen zu gewinnen beziehungsweise zu verlangen.

Genau das wird aber bei PKI-Projekten vorausgesetzt. Der durchschnittliche Anwender hat vermutlich bis heute keine wirklich negative Erfahrung mit dem Internet gemacht, für viele sind Spam, Viren und Dialer zwar lästig, aber kein Grund, in Sicherheit zu investieren. Der Anwender vertraut der Technik und darauf, „dass schon alles gut gehen wird". Sobald er aber bei E-Bay betrogen wurde oder sein Bankkonto leergeräumt wurde, wird er versuchen, die Kontrolle zu erlangen. Gelingt ihm das nicht, wird er die Technik eventuell gar nicht mehr einsetzen. Nun kommen die PKI-Experten und sagen: „verwende die digitale Signatur, dann kannst Du wieder vertrauen".

Das ist zwar ein überzeichnetes Bild, macht aber die Problematik deutlich. Insbesondere zeigt es, warum PKI jetzt noch so wenig verbreitet ist (wie viele andere präventive Sicherheitsmassnahmen): die handelnden Personen sind noch in der „angstfreien" Phase und haben keinen Bedarf nach Absicherung!

Wir müssen uns unserer Meinung nach dem Thema in deutlich strukturierterer Form widmen. Dafür ist eine interdisziplinäre Herangehensweise erforderlich. Die Mechanismen von Vertrauensbildung, im Kontext von Interaktionen, also Prozessen, müssen besser verstanden werden, bevor wir erwarten können, dass die handelnden Personen der Technik ausreichendes Vertrauen gegenüberbringen können. Als erster Ansatz wäre die Trennung der drei Ebenen Technologie, Prozess und Vertrauen ein wichtiger Schritt. Alleine die Loslösung und Separierung dieser drei, heute oft vermischten und stark verwobenen Bereiche, würde nicht nur auf der Seite der PKI-Implementierer viel Einsicht bringen.

### 4.4.4 Die Rolle des Staates

Die Rolle des Staates wurde sehr kontrovers diskutiert und auch in den Empfehlungen wurden sehr unterschiedliche Ansätze gewählt: von der staatlichen Verordnung der Verwendung von qualifizierten Zertifikaten bis zur Förderung von Best Practices. Auch bei der Problematisierung der Frage, wie Nachfrage geschaffen werden kann, wurde ein Einbezug des Staates als primäres Kriterium genannt.

Unsere Position dazu ist nach unseren eigenen Erfahrungen und den Ergebnissen des Workshops wie folgt: der Staat hat einerseits Eigeninteressen im Umfeld – diese sollten vom Staat umgesetzt und finanziert werden. Eine Bürgerkarte, wenn sie denn staatliche Anwendungen unterstützen soll, kann nur vom Staat kommen, da hier nicht auf die Industrie zurückgegriffen werden kann, weil dort andere (eben industrielle) Anforderungen (wie oben beschrieben) bestehen. Um die Verwendung darüber hinaus zu unterstützen, hat der Staat die Rolle im Rahmen der Industriepolitik, Standardisierung und Interoperabilität zu fördern, damit die Märkte durchlässig werden und um den Export zu stärken. Aber er kann und darf, außer für den staatlichen Einsatz, nicht regulativ eingreifen und bestimmte Technologien favorisieren. Wir plädieren daher für die weitere Unterstützung von Standardisierung und Interoperabilität, etwa im Rahmen der Einführung einer BürgerCard (mit dem

elektronischen Personalausweis), die weltweit möglichst interoperabel ist, andererseits aber auch die Persönlichkeitsrechte umfassend berücksichtigt (bspw. kein Einführen einer PKZ über die „Hintertür"). Wir warnen aber davor, die Regulierung der Technologie auf die Privatwirtschaft oder gar den Verbraucher abzudrängen. Dies würde das Innovationspotenzial des Technologiemarkts deutlich verringern und künstliche Barrieren schaffen. Ein Gütesiegel und ähnliche Auszeichnungen zur Förderung einer positiven Wahrnehmung begrüßen wir ausdrücklich.

# 5.

# Empfehlungen

Eine PKI stellt wichtige Infrastrukturelemente für Anwendungen zur Verfügung, die kryptographische Protokolle verwenden. Diese sind bei Verwendung der asymmetrischen Kryptographie für die Authentifizierung, für die Integritätssicherung von Informationen, für Signaturen und Transaktionsverschlüsselung unverzichtbar. Demzufolge liefern die Verfügbarkeit, Nutzungsgrad und die Nutzerakzeptanz von PKI belastbare Aussagen über die Verbreitung von Kryptographie in Anwendungen und damit auch über die Sicherheit von Informationen in offenen Netzen. Ein wesentliches Ziel des Projektes ist, mögliche Weiterentwicklungen, Bedarf an Förderung oder einfach praktische Tipps zu identifizieren, die helfen, PKI noch mehr zu verbreiten bzw. umgekehrt, Stolpersteine der Erfolgs zu herauszufiltern und Empfehlungen zu formulieren, wie diese ausgeräumt werden können.

In diesem Abschnitt stellen wir daher die wichtigsten Erkenntnisse für die Bereiche Technik, Betriebswirtschaft und praktische Anwendung noch einmal zusammen. Darauf aufbauend formulieren wir Empfehlungen für mögliche weitere Vertiefungen und Forschungsprojekte auf der einen Seite, geben aber auch konkrete Tipps für erfolgreiche PKI-Implementierungen.

## 5.1 Technik

Die wichtigsten Erkenntnisse aus dem Bereich Technik sind folgende:

→ Technische Lösungen für PKI sind ausreichend am Markt verfügbar. Ihre Bewer-

tung im Hinblick auf Anwendungen lässt sich nur vornehmen, wenn auch sozialwissenschaftliche und ökonomische Aspekte berücksichtigt werden.

→ Interoperabilität und Anwendungsintegration sind vorrangig marktgetrieben; die Probleme, die in diesen Zusammenhängen auftreten werden vorrangig für geschlossene Benutzergruppen (in Unternehmen oder Behörden) gelöst.

→ Die Tendenz, PKI durch personalisierte Hardwaretoken zu ergänzen, setzt sich weiter fort. Dabei werden Chipkarten zukünftig durch andere Token ergänzt. Der Formfaktor spielt dabei keine wesentliche Rolle; Biometrie wird zunehmend eingesetzt werden.

Der Wechsel von Kryptoalgorithmen und -Parametern ist extrem aufwendig. Deshalb ist die Austauschbarkeit von Algorithmen bei staatlichen Anwendungen sinnvoll, beim Unternehmenseinsatz eher nicht.

→ Die Ausrichtung von PKI auf eine verordnete Sicherheitsstufe (wie qualifizierte Signatur) erschwert selbst im hoheitlichen Umfeld die Verbreitung von Kryptoanwendungen, obwohl davon ausgegangen werden kann, dass ihr Einsatz in diesem Umfeld sinnvoll ist.

Aus unserer Sicht ergeben sich folgende Empfehlungen für den technischen Bereich.

**Austauschbarkeit kryptographischer Algorithmen**
Für den dauerhaften Erfolg von PKI im staatlichen Umfeld mit den dort gültigen langfristigen Investitionszyklen sind Konzepte zu entwickeln, die eine Austauschbarkeit von Algorithmen in Kryptobibliotheken und Standardprotokollen ermöglichen. Auf Grundlage einer Analyse der derzeitigen Gegebenheiten könnten die notwendigen Schritte abgeleitet werden, beispielsweise weshalb Anwendungen und Protokolle die notwendige Modularität nicht unterstützen. Insbesondere ist aber auch die Austauschbarkeit von Algorithmen in Hardware, also Tokens, Smart Cards usw. erforderlich, und für diese Zwecke sind erhebliche Anschubinvestitionen insbesondere in Forschung und Entwicklung notwendig.

**Trusted Plattform Modul (TPM) mit Smart Card-Erweiterung**
Die Kombination aus TPM zur Identifikation und zur Prüfung der Konfigurationsintegrität von Geräten und Systemkomponenten und personalisierten Token (z.B. Smart Cards) wird nützlich sein, da u.a. aus Datenschutzgründen eine Trennung der personenbezogenen Daten vom datenverarbeitenden Gerät möglich sein sollte, z.B. im Bereich Mobile Computing (PDAs, Mobiltelefone etc.). Personenbezogene Daten werden beispielsweise auf dem Speicherbereich der Smart Card gespeichert, auf den nur der Besitzer Zugriff hat. Die dazu laufenden Arbeiten sollten weiter unterstützend begleitet werden.

**Untersuchung weiterer Formfaktoren**
Neben Smart Card und TPM sollte die Praxistauglichkeit weiterer Form-Alternativen für Tokens (Mobiltelefone, PDAs, MP3-Player, Digitalkameras, RFID-unterstützte Ausweisdokumente,...) untersucht werden.

**Langzeitsicherheit von Hashalgorithmen**
Derzeitige Hashalgorithmen bieten nur für kurze Zeiträume Sicherheit, langfristige Sicherheit wird aber – zumindest im hoheitlichen Einsatzumfeld – benötigt. Dieses Problem kann nur im internationalen Kontext durch den Entwurf und die Prüfung neuer Hashalgorithmen durch die globale „Kryptoexpertengemeinde“ gelöst werden. Unter der Federführung des NIST (USA) ist ein entsprechender Wettbewerb eingeleitet worden. Die deutschen Kryptoexpertenteams sollten hinsichtlich ihrer Kooperation mit der NIST unterstützt werden.

**Verfahren zum Zugriff auf die kryptographischen Schlüssel**
Die Gegenüberstellung der praktischen Sicherheit von biometrischen und passwortbasierten Verfahren zum Schutz der kryptographischen Schlüssel ist bisher nicht abschließend erfolgt. Wir schlagen daher vor, vergleichende interdisziplinäre Untersuchungen mit ausführlicher Bewertung durchzuführen, bei denen nicht nur die technischen, sondern insbesondere auch sozialwissenschaftliche Einflussfaktoren (Wahrnehmung und Nutzerverhalten und -akzeptanz) berücksichtigt werden.

**Integration der PKI in Anwendungen / Service-Orientierte Architekturen**
Die Anwendungsintegration wird in weiten Teilen projektbezogen gelöst und ist nicht ausreichend standardisiert. Die Frage bleibt, wie dies besser als derzeit üblich umgesetzt werden kann. Wie können bspw. die Erfahrungen mit flexiblen Vertrauensmodellen weiter ausgebaut werden? Ein aus unserer Sicht wichtiger Ansatz ist die Förderung der Entwicklung von Frameworks, um praxisbezogene standardisierte Verfahren zu ermöglichen. Dies könnte z.B. anhand eines Forschungsprojekts "PKI für Service-Orientierte Architekturen" konkretisiert werden.

**Interoperabiltiät von PKI-Anwendungen**
Wir empfehlen grundsätzlich, besonders die Hersteller zu fördern, die auf Interoperabilität achten. In diesem Zusammenhang ist auch darauf hinzuweisen, dass im Behördenumfeld keinesfalls proprietäre Insellösungen eingesetzt werden sollten.

**Interoperabilität des Schlüsselmanagements**
Anwendungen tendieren heute weitestgehend dazu, Schlüssel und Vertrauensbeziehungen intern zu verwalten. Dies ist im privaten und Unternehmensumfeld für den Anwender bzw. den Administrator mit zunehmend hohem Aufwand verbunden. Deshalb ist aus unserer Sicht eine Standardisierung der Verwaltungsfunktionen für kryptographische Schlüssel dringend nötig. Um PKI weiter zu unterstützen sollte besonderes Augenmerk auf die derzeit stark geförderten alternativen Initiativen zur Standardisierung von "Credentials" gelegt werden (z.B. Projekte Higgins – IBM, CardSpace – Microsoft).

**Krypto-Exportvorschriften vereinfachen**
Im Interesse der Deutschen Kryptowirtschaft ist anzuraten, die Regulierungen beim Im- und Export von Kryptographie im Rahmen der internationalen Vereinbarungen zu vereinfachen.

**Flexiblere Sicherheitslevel für Anwendungen**
Alle Anwendungen sollten robuste und performante, aber vor allem angemessene Sicherheitskonzepte vorweisen können. Welche Verantwortung dabei den jeweiligen Anbietern der Anwendungen zuzuordnen ist, kann derzeit im Markt nicht klar erkannt werden. Dieser Prozess könnte unterstützt werden durch eine Bewertung von einzelnen Sicherheitsmaßnahmen, entweder durch Selbsterklärungen der Hersteller oder durch Prüfinstitute. Entsprechende Kriterien und Evaluierungsprozeduren wären hierfür allerdings zu entwickeln. Weitergehend wäre die Wirkung von Haftungsregelungen, technischen Regulierungen, Standards und Gütesiegeln auf den Markt zu untersuchen.

**Weiterentwicklung der Common Criteria**
Die Common Criteria sind sehr statisch, d.h. sie erlauben eine Prüfung der Sicherheit in einem definierten Umfeld. Veränderungen des Umfeldes sind – ohne die Zertifizierung infrage zu stellen – nach heutigem Stand nicht "erlaubt". Dennoch wäre genau dies sinnvoll, da sich das Umfeld in Abhängigkeit vom jeweiligen Geschäftsprozess verändern und damit andere Anforderungen stellen kann.

**Zu beantwortende Fragen durch die Grundlagenforschung**
Als langfristig einflussreichster Faktor für eine eingeschränkte Praxisrelevanz von PKI wird zurzeit die Quantenkryptographie gesehen. In diesem Zusammenhang gibt es jedoch noch eine Reihe offener Fragen:

- → Es gibt noch keine Aussage, ob Quantencomputer überhaupt in "ausreichender" Menge hergestellt werden können, inwieweit sie in der bisher geplanten Weise funktionieren und wann mit ihnen überhaupt zu rechnen ist. Erst wenn diese Fragen einigermaßen schlüssig beantwortet werden können, ist eine sinnvolle Beurteilung der "Gefahr" von Quantencomputern für kryptografische Verfahren und PKI möglich.
- → Wie sicher sind andererseits die dann umsetzbaren quantenkryptographischen Verfahren wirklich, die als potentielle Alternativen zu PKI gezählt werden könnten? Es gibt bisher nur wenige Information über ihre tatsächliche praktische Sicherheit.
- → Für Quantencomputer und Quantenalgorithmen ist ein flächendeckender Einsatz von Quantenkanälen notwendig. Unsere derzeitigen Kanäle, wie drahtgebundene Kanäle und elektromagnetische Wellen können dafür nicht genutzt werden. Wie realistisch – gerade unter Investitionsgesichtspunkten – ist der Aufbau einer derartigen Infrastruktur?
- → Bisher besteht die Annahme, dass nur die klassischen Krypto-Algorithmen von der "Gefahr Quantencomputing" betroffen sind. Es muss untersucht werden inwieweit Lattice-Based oder ähnliche Kryptosysteme durch die Existenz von Quantencomputern unsicher werden.

Neben der Quantenkryptographie empfehlen wir, die Möglichkeiten und Grenzen von DNA Computern ebenfalls zu untersuchen.

## 5.2 Betriebswirtschaft

Die wichtigsten Erkenntnisse aus dem betriebswirtschaftlichen Teil sind folgende:

- → PKI-Lösungen lassen sich aus Kostensicht nur sinnvoll auf Geschäftsprozessebene betrachten, was deren detaillierte Kenntnis erfordert. Die Entwicklungen im Bereich SOA verstärken diese Notwendigkeit.
- → ROSI-Berechnungen im PKI-Umfeld sind nicht hilfreich: einerseits ist die Bestimmung möglicher Schäden nicht ausreichend realitätsbezogen, andererseits sind die Berechnungsmodelle für ROSI noch nicht ausgereift.
- → PKI-Anwendungen haben in Abhängigkeit vom Szenario (staatlich, unternehmerisch, verbraucherzentriert) unterschiedliche Kriterien und Einsatzbedingungen. Daraus folgt, dass keine echte Vergleichbarkeit gegeben ist und Lösungen für ein Szenario nicht als Referenzen für andere Szenarien gelten können.
- → Bei organisationsübergreifenden Prozessen ist die Kosten-Nutzen-Verteilung nicht ohne zusätzliche Anreize und festzulegende Verteilungsmechanismen auszugleichen.

Folgende Empfehlungen gelten für diesen Bereich:

**Anwendernutzen in Geschäftsmodelle umwandeln**
Geschäftsmodelle für die PKI-Nutzung im Privatbereich sind aufgrund der Kostenasymmetrie schwierig zu gestalten. Klar ist, dass der potentielle Nutzen für den Anwender so hoch sein muss, dass eventuelle Kosten akzeptiert werden können. Es ist genauer zu untersuchen, welche Anwendungen bzw. Anwendungskombinationen möglich sind, damit Kosten überhaupt in Anrechnung gebracht werden können.

**Sicherheit als impliziter Teil der Geschäftsprozessmodellierung**
Ein Verständnis sicherheitsbasierter Prozesse ist auch auf Managementebene erforderlich; dafür muss Sicherheit zu einem impliziten Teil der Geschäftsprozessmodellierung/-entwicklung werden. Um dies zu erreichen, ist z.B. in Pilotprojekten zu untersuchen, welche methodischen Ansätze verfügbar sind beziehungsweise entwickelt werden müssten, damit Sicherheitsanforderungen während der Geschäftsprozessmodellierung einbezogen werden können.

**Ausgewählte Kernprozesse als Enabler**
Eine Betrachtung aller beteiligten Prozesse und Kosten für die Betrachtung in Kennzahlenmodellen ist zu komplex und zu teuer. Es müssen ausgewählte Kernprozesse benannt werden, bei denen PKI als „Enabler“ dienen könnte. Hierfür müssen die jeweiligen Prozessverantwortlichen die Anforderungen an die zu erfüllenden Sicherheitskriterien kennen und formulieren. Um dies zu erreichen, bietet es sich an, Kernprozesse auszuwählen, dafür die Kriterien in Form von "Best Practices" zu formulieren und zur Verfügung zu stellen.

**Transparenz für Infrastrukturinvestitionen**
Fehlende Informationen über die jeweiligen Prozesskosten lassen ggw. nur Infrastrukturinvestitionen zu. Dadurch wird es schwierig, die „Enabler"-Funktion von PKI zu erkennen. Man muss sich bewusst sein, dass es grundsätzlich Vorteile für die Geschäftsprozesse gibt, die allerdings verzögert wirksam werden.

Da Kosten gerade bei Infrastrukturinvestitionen i.d.R. an anderer Stelle anfallen als der zu realisierende Nutzen, muss das Kosten-Nutzen-Verhältnis transparant gemacht werden. Der Träger der Kosten muss in irgendeiner Form am Nutzen beteiligt werden, schon allein um die Investition zu rechtfertigen. Dementsprechend ist zu untersuchen, welche Anreize und Verteilungsmechanismen geschaffen werden können, die zu einem Ausgleich in der Kosten-Nutzen-Struktur führen.

**Methodenmix für Kostenbetrachtungen erforderlich**
Die heute i.d.R. für eine Investitionsentscheidung verwendeten Kennzahlensysteme wie ROI / ROSI oder NPV liefern kein vollständiges Bild. Sie führen häufig zu einem negativen Ergebnis, was gegen eine Investition spräche. Mit der Anwendung eines Methodenmixes kann eine detailliertere Kostenbetrachtung vorgenommen werden, was zu valideren Ergebnissen führt. Hier sollten vor allem akzeptierte Methoden zum Einsatz kommen, z.B. ROSI inkl. TCO plus NPV plus Balanced Scorecards. Allerdings sind die Kosten auf Geschäftsprozessebene schwer berechenbar, wenn bspw. die Prozesskomponenten nicht bekannt sind. Sinnvoll wäre daher ein Projekt zur Untersuchung von Umsetzbarkeit und Wirksamkeit verschiedener Methodenmixe auf Sicherheitsinvestitionen.

**Anwendung des Pareto-Prinzips**
Die Ermittlung eines ROI ist grundsätzlich eine Schätzung. Es werden i.d.R. nie alle Daten berücksichtigt werden können, die eigentlich in die Rechnung einbezogen werden müssten. Daher empfehlen wir, bei der Sammlung der Daten das Pareto-Prinzip anzuwenden. Danach erbringen üblicherweise 20% der Kosten, die den Hauptkomponenten zugeordnet werden können, 80% des Nutzens. Das Erkennen dieser 20% ist im Einzelfall schwierig und sollte aufgrund von Erfahrungswerten verallgemeinert werden. Wir schlagen deshalb vor, entsprechende Werte für Sicherheitsprojekte in einer Studie zusammen zu tragen.

**Elektronische Gesundheitskarte als Killeranwendung**
Es existiert die Meinung, dass mit der Verbreitung der elektronischen Gesundheitskarte der PKI-Einsatz auf breite Akzeptanz stoßen wird. Wir empfehlen eine begleitende (Langzeit-)Studie, die genau diese Behauptung untersucht.

## 5.3 Nutzungsbedingungen

Die Hauptergebnisse in Bezug auf eine PKI-Nutzung sind folgende:

- → Eine sozialwissenschaftliche Betrachtung von PKI wurde bisher stark vernachlässigt.
- → Die Automatisierung von Geschäftsprozessen führt oft zum individuell empfundenen Kontrollverlust, welcher nur durch mehr Vertrauen in den betroffenen Mitarbeiter ausgeglichen werden kann.
- → Vertrauensentscheidungen sollten in den Geschäftsprozess integriert sein. Wenn der Nutzer Entscheidungen im Prozess treffen muss, dann sollten diese möglichst nachvollziehbar und transparent sein.
- → Bei der Einführung von PKI-Projekten sollte man Change Management-Experten hinzuziehen.

Für die weitere Vorgehensweise sind unseres Erachtens folgende Empfehlungen relevant:

**Abhängigkeiten zwischen Technik, Wirtschaft und Nutzungsaspekten**
Im PKI-Umfeld sollten die Abhängigkeiten von Technik, Wirtschaft und sozialwissenschaftlichen Aspekten systematisch untersucht werden, mit dem Ziel, Faktoren und Möglichkeiten zu entwickeln, mit deren Hilfe die Vertrauensbildung im elektronischen Geschäftsverkehr verbessert werden kann.

**Best Practices bei Einführungen**
Man sollte bei einer PKI-Realisierung grundsätzlich nicht versuchen, gleich so viele Anwendungen wie möglich zu unterstützen, sondern eine schrittweise Integration über Pilotanwendungen anstreben. Es sollten auch Hilfestellungen für den Umgang mit unternehmensinternen politischen Konflikten erarbeitet werden, die insbesondere die hierarchische Struktur von PKI berücksichtigen.

Um dies zu erreichen ist die Veröffentlichung von Best- aber auch von Worst-Practice-Beispielen ein unseres Erachtens besonders gut geeignetes Mittel. Insbesondere Behörden und andere öffentliche Einrichtungen könnten aufgrund der nicht beziehungsweise nicht so stark vorhandenen Konkurrenzsituation detaillierte Erfahrungsberichte von erfolgreichen und nicht erfolgreichen PKI-Projekten veröffentlichen. Es sollte allerdings auch versucht werden, eine Motivation zu schaffen, damit auch Unternehmen derartige Berichte öffentlich machen.

**Awareness**
Im Kontext dieses Projektes stellt sich die Frage, wie es um das Bewusstsein der Menschen zu Vertrauensbildung und Vertrauensentscheidungen insbesondere bei Internet-Anwendungen steht. Ein entsprechende Untersuchung könnte auch gleichzeitig darauf ausgerichtet sein, zu zeigen, wie sich Vertrauen bildet und wie Maßnahmen zum Erzeugen von Awareness gestaltet sein sollten, damit sie von den Nutzern akzeptiert und umgesetzt werden. Unseres Erachtens sind traditionelle Schulungen hierfür beispielsweise nicht unbedingt der beste Weg, da sie nach kurzer Zeit vergessen sind. Wir stellen uns eher Maßnahmen vor, die über einen ständigen Kontakt Awareness schaffen oder zumindest verbessern.

**Mangelnde Flexibilität**

Es sollte untersucht werden, welche Gründe für die mangelnde Flexibilität von PKI, gerade in der Realisierungsphase, zu finden sind und wie diese verbessert werden kann.

**Einfache Vertrauensentscheidungen**
PKI-Anwendungen sollten Anwender nicht vor zu komplexe und insbesondere nicht vor intransparente oder nicht nachvollziehbare Vertrauensentscheidungen stellen. Entscheidungen sollten dort zu treffen sein, wo der Anwender sie im Prozesszusammenhang erwartet. Insofern sind Lösungen gefordert, die nicht auf am grünen Tisch erarbeitete und damit oft nicht erfolgreich durchsetzbare organisatorische Regeln zurückgreifen müssen, um das Vertrauensmodell der PKI-Implementierung einzuhalten. Entsprechende Erfolgskriterien beim Design von PKI-Anwendungsintegration sollten aus unserer Sicht Ziel einer Studie werden.

**Experimentieren, um den Nutzen von PKI stärker herauszustellen**
Es sollten Formen einfacherer organisationsübergreifender Vertrauensmodelle ("instant workgroups") untersucht werden.

**Keine Certificate Practice Statements**
Statt dem Modellieren von Vertrauensanforderungen in einem Certificate Practice Statement ist eine Dokumentation, wie der Ziel-Prozess durch den Einsatz von PKI abgesichert werden kann, deutlich wichtiger. Für die Erstellung solcher Dokumentationen sollten sinnvolle Rahmenbedingungen (Vorschläge) erarbeitet werden.

**Technische Anforderungen nicht in Gesetzen formulieren**
Wie die Erfahrung mit der digitalen Signatur gezeigt hat, sollten technische Anforderungen an Verfahren nicht in Gesetzen, sondern vorrangig in Verordnungen geregelt werden. Um Erfahrungen sammeln und mögliche Spielräume ausnutzen zu können ist es aus unserer Sicht besonders wichtig, pragmatische Ansätze zu ermöglichen, wenn nicht sogar zu unterstützen – zumindest in einer Übergangszeit. Hierdurch ließen sich voraussichtlich viele Probleme in der Abstimmung und Durchsetzung im politischen Umfeld bzw. den Verwaltungsbehörden vermeiden.

## 5.4 Weitere Projektideen

PKI muss zukünftig stärker im Spannungsfeld von Technik, Betriebswirtschaft und Sozialwissenschaft betrachtet werden – erst dann wird sich der Erfolg als Enabling-Technologie für Geschäftsprozesse erweisen. Hier einige Ideen (zum Teil auch von den Teilnehmern des Workshops) für die nächsten Schritte:

Man sollte einen Vergleich mit anderen Industrien, die eine hohe Standardisierung erfahren haben, heranziehen und die Frage beantworten, warum dort mehr Stan-

dards umgesetzt werden konnten und wie dies potentiell auf das PKI-Umfeld zu übertragen wäre.

Mit Simulation- bzw. Szenariotechnik sollten unterschiedliche Geschäftsfälle durchgearbeitet und die Aufteilung in die Szenarien weiter verfeinert werden, um für Industrie und Verwaltung zu besseren und nachvollziehbaren Entscheidungskriterien für oder gegebenenfalls auch gegen einen PKI-Einsatz zu gelangen. Aspekte, die es dabei zu berücksichtigen gilt, sind: Anforderungen von Anwenderseite, Anwendungsfälle und unterschiedliche Branchenspezifika.

Insgesamt entwickelte sich in der internen und externen Diskussion die Frage, inwieweit die von uns herausgearbeiteten Ergebnisse nur für PKI im Speziellen, oder ob sie auch allgemein für IT-Sicherheit Anwendung finden könnten. Unseres Erachtens sind viele der Fragestellungen (beispielsweise die "ROSI"-Diskussion) auch für eine breitere Diskussion im gesamten IT-Sicherheitsumfeld relevant. Die Ergebnisse des Projekts könnten zudem als ein Input für den nächsten IT-Gipfel dienen.

# 6.

# Quellenverzeichnis

Alle Hyperlinks wurden am 06.08.2007 erfolgreich auf ihre Verfügbarkeit geprüft.


[Albrecht 2001] Albrecht, A.; Probst, T.: Bedeutung der politischen und rechtlichen Rahmenbedingungen für biometrische Identifikationssysteme. Behrens, M.; Roth, R. (Hrsg.): *Biometrische Identifikation : Grundlagen, Verfahren, Perspektiven*, Vieweg Verlag Wiesbaden, 2001, S. 27–54.

[Bang 2006] Bang, Y.; Kang, Y.; Lee, G.: CC-SEMS: A CC Based Information System Security Evaluation Mangagement System. Dongarra, J.; Madsen, K.;Wasniewski, J. (Ed.): *Applied Parallel Computing, 7th International Conference* (PARA 2004), Lyngby, Denmark, June 20-23, 2004. Revised Selected Papers; Springer-Verlag Berlin Heidelberg, 2006, S. 964–973.

[Bakdi 2006] Bakdi, I.: Towards a Secure and Practical Multifunctional Smart Card. *[Domingo 2006]*, S. 16–31.

[Beilschmidt 2007] Beilschmidt, A.: Geschäftsmodelle für die European Bridge-CA; TeleTrusT Deutschland e.V.; 2007.

[Berinato 2002] Berinato, S.: Finally, a Return on Security Spending. CIO Australia; 08.04.2002; http://www.cio.com.au/index.php?id=557330171

[Bernhard 2000] Bernhard, M.: Balanced Scorecard in der IT – Den Nutzen für das Unternehmen darstellen. Bernhard, M.; Hoffschröer, S.: *Report Balanced Scorecard – Strategien umsetzen, Prozesse steuern, Kennzahlensysteme entwickeln*; 3. überarbeitete Auflage; Symposion Publishing; 2003.

[Beutelspacher 2006] Beutelspacher, A.; Schwenk, J.; Wolfenstetter, K.: Moderne Verfahren der Kryptographie: Von RSA zu Zero-Knowledge; Vieweg Verlag Wiesbaden; 2006

[Beutelspacher 2007] Telefon-Interview mit Prof. Dr. Albrecht Beutelspacher, Professor für Geometrie und Diskrete Mathematik am Mathematischen Institut der Universität Gießen; am 22.01.2007

[BioFinger 2004] BSI Studie: Evaluierung biometrischer Systeme Fingerabdrucktechnologien - BioFinger, Technical Report; BSI; 2004.

[BioTrusT 2002] BioTrusT, Ein interdisziplinäres Projekt zur Förderung biometrischer Identifizierungsverfahren; CD Abschlussbericht; September 2002.

[Boneh 1995] Boneh, D.; Dunworth, C.; Lipton, R. J.: Breaking DES Using a Molecular Computer, Technical Report CS-TR-489-95, Princeton University, 1995.

[Boneh 1996] Boneh, D.; Dunworth, C.; Lipton, R. J.; Sgall, J.: On the Computational Power of DNA; *Journal DAMTH: Discrete Applied Mathematics and Combinatorial Operations Research and Computer Science*, Volume 71, 1996.

[Bong 2005] Bong, D.; De Swaart, J.: ROBIN, a Biometrics-based Security Environment at the Dutch Court Organization. Paulus,S.; Pohlmann, N.; Reimer, H. (Hrsg.): *ISSE 2005 - Securing Electronic Business Processes : Highlights of the Information Security Solutions Europe 2005 Conference*, Budapest, Hungary, September 27 – 29, Vieweg Verlag Wiesbaden, 2005, S. 201–209

[Booker 2006] Booker, R.: Re-engineering enterprise security. *Computers & Security* 25; 2006, S.13–17.

[Brands 2005] Brands, G.: IT-Sicherheitsmanagement; Springer; 2005.

[Brassard 1996] Brassard, G.; Crepeau, C.: 25 years of quantum cryptography. *SIGACT News* 27 (3); 1996, S. 13–24.

[Braz 2006] Braz, C.; Robert, J.-M.: Security and Usability: The Case of the User Authentication Methods; *18th Francophone Conference on Human Computer Interaction* (IHM '06); Montreal; 18.–21.4.2006.

[Brink 2002] Brink, D.: PKI and Financial Return on Investment; Whitepaper; PKI Forum; August 2002.

[BSI 2006a] AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 1, 2.12.99, samt mathematisch-technischem Anhang (Version 2.0, 2.12.99).
http://www.bsi.bund.de/zertifiz/zert/interpr/aisitsec.htm

[BSI 2006b] Stellungnahme des BSI zur TC-Initiative.
http://www.bsi.de/sichere_plattformen/trustcomp/stellung/palladium.htm

[Buchmann 2006a] Buchmann, J.; May, A.; Vollmer, U.: Privacy and security in highly dynamic systems: Perspectives for cryptographic long-term security. *Communications of the ACM* 49 (9); 2006, S. 50–55.

[Buchmann 2006b] Telefon-Interview mit Prof. Dr. Johannes Buchmann, Professor für Computer Science und Mathematik, Technische Universität Darmstadt; am 5.12.2006.

[Bundesnetzagentur Algorithmenkatalog 2006] Bundesnetzagentur (für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen). Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 02. Januar 2006, Bundesanzeiger Nr. 58 vom 23.03.2006, S. 1913–1915.
http://www.t-systems-zert.com/pdf/bas_03_kri/alg2006.pdf

[Busch 2006] Telefon-Interview mit Prof. Dr. Christoph Busch; Professor an der Hochschule Darmstadt, am 6.12.2006.

[Calmels 2006] Calmels, B.; Canard, S.; Girault, M. & Silbert, H.: Low-Cost Cryptography for Privacy in RFID Systems. *[Domingo 2006]*, S. 237–251.

[Cardholm 2006] Telefon-Interview mit LL.M. Lucas Cardholm, Direktor Ernst & Young Schweden; am 15.12.2006.

[Chandra 2005] Chandra, A.; Calderon, T.: Challenges and constraints to the diffusion of biometrics in information systems. Communications of the ACM 48 (12), 2005, S. 101–106.

[Clarke 2001] Clarke, R.: The Fundamental Inadequacies of Conventional Public Key Infrastructure. Proceedings of the 9th European Conference on Information Systems (ECIS 2001), Bled, Slovenia, June 27–29 2001. http://www.anu.edu.au/people/Roger.Clarke/II/ECIS2001.html

[Dobbertin 1996] Dobbertin, H.: Cryptoanalysis of MD4. Proceedings of the 3rd Workshop on Fast Software Encryption; Cambridge, UK; February 21–23 1996; Lecture Notes in Computer Science; Bd. 1039; S. 53–70, Berlin, Springer, 1996.

[Domingo 2006] Domingo-Ferrer, J.; Posegga, J.; Schreckling, D. (Ed.): Smart Card Research and Advanced Applications; 7th IFIP WG 8.8/11.2 International Conference (CARDIS 2006), Tarragona, Spain, April 19–21, 2006. Proceedings (Lecture Notes in Computer Science); 2006.

[Donnerhacke 1999] Donnerhacke, L.: Anonyme Biometrie. Datenschutz und Datensicherheit 23 (3) 1999, S. 151–154.

[Eckert 2006] Eckert, C.: IT-Sicherheit : Konzepte, Verfahren, Protokolle; 4. Auflage, Oldenbourg, 2006.

[Elsener 2005] Elsener, M.: Kostenmanagement in der IT: Leistungssteigerung und Kostenoptimierung; Bonn: mitp Verlag; 2005.

[Flexiprovider 2006] Technische Beschreibung des Flexiprovider toolkit for the Java Cryptography Architecture (JCA/JCE). http://www.flexiprovider.de

[Gadatsch 2006] Gadatsch, A.; Uebelacker, H.: Wirtschaftlichkeitsbetrachtungen für IT-Security-Projekte. [Mörike 2006]; S. 44–50.

[Gaude 2007] Gaude, M.; Pernul, G.: Die Rolle der Public Key Infrastruktur und der elektronischen Signatur in Geschäftsprozessen. Nutzenpotenzial – Schwächen – Zukünftige Entwicklung und Verbreitung; Delphi-Studie; Sindelfingen; 2007.

[Gawlas 2005] Gawlas, F.; Meister, G.: Interaktionen TPM und Smart Card. Datenschutz und Datensicherheit 29 (9) 2005; S. 517ff.

[Graevenitz 2006] von Graevenitz, G.: Erfolgskriterien und Absatzchancen biometrischer Identifikationsverfahren; Lit Verlag; 2006.

[Giessmann 2006] Telefon-Interview mit Prof. Dr. Ernst-Günter Giessmann, Professor für Algorithmen und Komplexität an der Humboldt-Universität Berlin; am 11.12.2006.

[Hammer 2001] Hammer, V.; Petersen, H.: Aspekte der Cross-Zertifizierung; SecuMedia Verlags GmbH; 2001. http://www.kes.info/archiv/material/bsikongress2001/01-05-52.htm

[Hanusch 1995] Hanusch, H.; Kuhn, T. (Hrsg.): Kosten-Nutzen-Untersuchungen. Akademie für Raumforschung und Landeplanung. *Handwörterbuch der Raumordnung*; S. 555-559; Hannover; 1995.

[Hilton 2007] Telefon-Interview mit Jeremy Hilton, Lecturer an der Cardiff University UK; am 11.01.2007.

[Hirschmeier 2005] Hirschmeier, M.: Wirtschaftlichkeitsanalysen für IT-Investitionen; WiKu-Verlag; Berlin; 2005.

[ID Quantique 2007] Firmenwebseite. http://www.idquantique.com/

[Jueneman 1998] Jueneman, R.; Robertson, R.: Biometrics and digital signatures in electronic commerce. *Jurimetrics Journal of Law, Science and Technology* 38 (3), 1998, S. 427–458.

[Kaplan 1997] Kaplan, R.; Norton, D.: Balanced Scorecard. Strategien erfolgreich umsetzen; Schäffer-Poeschel Verlag; Stuttgart; 1997.

[Kirsch 2001] Kirsch, C.: S/MIME vs. OpenPGP: Eine Entscheidungshilfe. In: KES 1, SecuMedia Verlags GmbH, 2001, S.60 ff. http//www.kes.info/_archiv/_onlinearch/01-01-60-SMIMEvsOpenPGP.htm

[Krause 2005] Krause, R.: Bewertungskriterien für biometrische Identifikationssysteme im Vergleich zu bisherigen Identifikationsverfahren, Hochschulschrift, Freiburg (Breisgau), 2005.

[Kuppinger 2006a] Telefon-Interview mit Martin Kuppinger, Senior Partner Kuppinger Cole + Partner; am 28.12.2006.

[Kuppinger 2006b] Kuppinger, M.: SOA ohne IAM: geht nicht! In: *InfoWeek* 19/2006; http://www.infoweek.ch/archive/ar_single.cfm?ar_id=18007&ar_subid=2

[Kuppinger 2007] Kuppinger, M.; Cole, T.: Nur noch ein Passwort – Die richtige Single sign-on-Strategie. *SearchSecurity.de* vom 05.04.2007. http://www.searchsecurity.de/themenkanaele/applikationssicherheit/websicherheit/webservicessoa/articles/62644/

[Lareau 2002] Lareau, P.: PKI Basics – A Business Perspective; PKI Forum Business Working Group; April 2002.

[Leitold 2006] Telefon-Interview mit Herbert Leitold, A-SIT Zentrum für sichere Informationstechnologie Graz; am 28.12.2006.

[Losemann 2005] Losemann, F.: Zertifikatsmanagement für große Organisationen; Books on Demand GmbH; April 2005.

[Lubich 2006] Lubich, H. P.: IT-Sicherheit: Systematik, aktuelle Probleme und Kosten-Nutzen-Betrachtungen. *[Mörike 2006]*; S. 6–15.

[Microsoft 2005] Signieren von Treibern für Windows; Microsoft Corp.; 21.01.2005. http://www.microsoft.com/technet/prodtechnol/windowsserver2003/de/ library/ServerHelp/f211560e-ed86-4821-97ba-fcfdd525a842.mspx

[Mörike 2006] Mörike, M.; Teufel, S. (Hrsg.): Kosten & Nutzen von IT-Sicherheit; HMD – Praxis der Wirtschaftsinformatik; Heft 248; April 2006.

[Nash 2001] Nash, A.; Duane, W.; Joseph, C.: PKI, e-security implementieren; mitp; 2001.

[NSA A 2007] Federal Information Processing Standards Publication 197, November 26, 2001; Announcing the Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[NSA B 2007] Federal Information Processing Standards Publication 186-2; Digital Signature Standard; Januar 2000. http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf

[NSA C 2007] NIST Special Publication 800-56, Recommendation on key establishment schemes; Januar 2003. http://csrc.nist.gov/CryptoToolkit/kms/keyschemes-Jan03.pdf

[NSA D 2007] Federal Information Processing Standards Publication 180-2, Announcing the secure hash standard; August 2002. http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf

[NTRU 2006] Produktbeschreibung der Security Suite für Drahtlos-Netzwerke 'Aerolink' mit dem NTRU-Kryptosystem. http://www.ntru.com/products/AL15_4.pdf

[Okamoto 2003] Okamoto, Tatsuaki: Trends in Cryptography: Technologies and their Future, Special Feature: Information Security Technologies Supporting Safe and Secure Information Sharing; NTT Review Vol.15 No.1; 2003, S 234–247.

[Paar 2007] Telefon-Interview mit Prof. Dr.-Ing. Christof Paar, Professor für Kommunikationssicherheit an der Ruhr-Universität Bochum; am 26.01.2007.

[Paulus 2006a] Paulus, S.; Pohlmann, N.; Reimer, H. (Hrsg.): ISSE 2006 - Securing Electronic Business Processes: Highlights of the Information Security Solutions Europe 2006 Conference, Rome, Italy, October 10–12, Vieweg Verlag Wiesbaden; 2006.

[Paulus 2006b] Paulus, S.: Sicherheit für Service-Orientierte Architekturen. Franz, R.U.; Heinrich, H. (Hrsg.): *Moderne IT-Architekturen – eine Herausforderung für die Sicherheit? Tagungsband zum 5. Berlin-Brandenburger SAP-Forum der FH Brandenburg*; Shaker Verlag; Aachen 2006; S.21–44.

[Pohlmann 2003] Pohlmann, N.: Integration biometrischer Verfahren in Sicherheitsinfrastrukturen. Horster, P. (Hrsg.): *D-A-CH Security* 2003, Syssec, 2003, S. 322–331.

[Pohlmann 2007] Telefon-Interview mit Prof. Dr. Norbert Pohlmann, Geschäftsführender Direktor des Institutes für Internet-Sicherheit an der Fachhochschule Gelsenkirchen; am 12.1.2007.

[Poritz 2006] Poritz, J. A.: Trust[ed | in] computing, signed code and the heat death of the internet. *Proceedings of the 2006 ACM*

*Symposium on Applied Computing* (SAC '06); ACM Press; New York; 2006, S. 1855–1859.

[Preneel 2006] Telefon-Interview mit Prof. Dr. Bart Preneel; Professor an der K.U. Leuven; am 12.12.2006.

[Rossnagel 2006] Rossnagel, H.: On Diffusion and Confusion – Why Electronic Signatures Have Failed. Fischer-Hübner, S.; Furnell, S.; Lambrinoudakis, C. (Ed.): *Trust and Privacy in Digital Business, Third International Conference* (TrustBus 2006); Krakow; Proceedings TrustBus; Springer; 2006, S. 71–80.

[Rottke 2002] Rottke, T.; Hatebur, D.; Heisel, M.; Heiner, M.: A Problem-Oriented Approach to Common Criteria Certification. Anderson, S. et al., (Ed.): *Computer Safety, Reliability and Security: 21st International Conference* (SAFECOMP 2002), Catania, Italy, September 10-13, 2002. Proceedings; Springer-Verlag Berlin Heidelberg; 2002, S. 334–346.

[RSA 1978] R. L. Rivest, A. Shamir, L. Adleman – A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* 21 (2); 1978, S. 120–126.

[Sadeghi 2006] Sadeghi, A.: Challenges for Trusted Computing. Goubin, L.; Matsui, M. (Ed.): '*CHES 2006*'; International Association for Cryptologic Research; 2006, S. 414.

[Sandhu 2005] Sandhu, R.; Zhang, X.: Peer-to-peer access control architecture using trusted computing technology. *Proceedings of the 10th ACM symposium on Access control models and technologies* (SACMAT '05); ACM Press; New York; 2005, S. 147–158.

[Savola 2006] Savola, R: Towards Security Evaluation based on Evidence Collection. Wang, L. et al. (Ed.): *Fuzzy Systems and Knowledge Discovery, Third International Conference* (FSKD 2006), Xi'an, China, September 24-28, 2006. Proceedings; Springer-Verlag Berlin Heidelberg; 2007, S. 1178–1181.

[Schadt 2006] Schadt, D.: Über die Ökonomie der IT-Sicherheit – Betrachtungen zum Thema „Return on Security Investment". *[Mörike 2006]*, S. 16–25.

[Schmeh 2001] Schmeh, K.: Kryptografie und Public-Key-Infrastrukturen im Internet; dpunkt-Verlag; 2001.

[Schmidt 2006] Schmidt, A.: Quantum Algorithm for Solving the Discrete Logarithm Problem in the Class Group of an Imaginary Quadartic Field and Security Comparison of Current Cryptosystems at the Beginning of Quantum Computer Age. G. Müller, G. (Ed.): *Emerging Trends in Information and Communication Security, International Conference* (ETRICS 2006), Freiburg, Germany, June 6–9, 2006. Proceedings Springer-Verlag Berlin Heidelberg; 2006, S. 481–493.

[Schneier 1999] Schneier, B.: Inside risks: the uses and abuses of biometrics, *Communications of the ACM* 42 (8); 1999, S. 136.

[Schultz 2002] Schultz, E.: The gap between cryptography and information security. *Computers & Security* 21(8), 2002, S. 274–276

[Shelfer 2002] Shelfer, K. M.; Procaccino, J. D.: Smart card evolution. *Communications of the ACM* 45 (7); 2001; S. 83–88.

[Shor 1996] Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. Goldwasser, S. (Ed.): *Proceedings of the 35th Annual Symposium on foundation of Computer Science* (FOCS 1994); 1996, S. 56–65.

[SigBü 2005] Signaturbündnis Bericht der Arbeitsgruppe „Geschäftsmodelle“, Deutscher Sparkassenverlag GmbH; 2005.

[Signatur 2001] Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876); zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179); http://bundesrecht.juris.de/sigg_2001/

[SigV 2001] Signaturverordnung (SigV) 2001, 16. November 2001, BGBl. I S. 3074, Anlage 1 Abschnitt I Nr. 2

[SmartQuantum 2007] Datasheet SQKey Generator that uses the QKD (Quantum Key Distribution). http://www.smartquantum.com/IMG/pdf/SQKeyGenerator_Datasheet.pdf

[Sonnenreich 2006] Sonnenreich, W.: Return On Security Investment (ROSI): A Practical Quantitative Model. Journal of Research and Practice in Information Technology; Vol. 38, No. 1; February 2006.

[Spitz 2006] Spitz, S.; Urmann, J.; Meister, G.: ISO/IEC 24727 – A Future Standard for Smart Card Middleware. *[Paulus 2006a]*, S. 102–107.

[Sukhai 2004] Sukhai, N.B.: Access control & biometrics. *Proceedings of the 1st annual conference on Information security curriculum development* (InfoSecurity 2004), ACM Press, New York, NY, USA, 2004, S. 124–127.

[TCG 2006] Webseite der Trusted Computing Group. https://www.trustedcomputinggroup.org/home

[TeleTrusT 2006] TeleTrusT Deutschland e.V.: Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren – Kriterienkatalog Version 3.0. http://www.teletrust.de/fileadmin/files/publikationen/KritKat-3_final.pdf

[Temple 2006] Telefon-Interview mit Robert Temple, Chief Security Architect, British Telecom UK; am 8.12.2006.

[Weis 2005] Weis, R., Lucks, S.: Hashfunktionen gebrochen. Datenschutz und *Datensicherheit* 29 (4) 2005, S. 219ff.

[Wiegel 2005] Wiegel, B.: Public Key Infrastrukturen – höhere Akzeptanz durch Anwenderfreundlichkeit – Vorteile eines zentralen Zertifikatsmanagements; PKI Forum Zertifikon Solutions White Paper. http://www.zertificon.com/resourcen.php?k=3&t=9&detail

[Williamson 2006] Williamson, G.: e-ID and Smartcards – Current Status, Hopeful Developements and Best Practices. [Paulus 2006a], S. 17–24.

[Wissenschaft.de 2005] Weltweit erste quantenkryptografisch verschlüsselte Banküberweisung. http://www.wissenschaft.de/wissenschaft/news/240269.html

# Anhang

**Anhang A** Fragebogen Technische Perspektiven

**Anhang B** Interviewpartner zu Technischen Perspektiven

**Anhang C** Public-Key-Infrastruktur (PKI)

**Anhang D** Return on Security Investment (ROSI)

**Anhang E** Fragebogen zur Erfassung von Kriterien für die Nutzung von PKI

**Anhang F** Details zum Workshop

# Anhang A: Fragebogen Technische Perspektiven

| **Experte:** | **Interviewer:** |
|---|---|
| | |

| **Firma/Positionsbezeichnung des Experten:** | **Datum** |
|---|---|
| | |

| **Wissenschaftlicher Background des Experten:** |
|---|
| |

| **I Bewertung der Grundlagen von IT-Sicherheitstechnologien:** |
|---|
| **1 Kryptographie:** |
| 1.1 Bitte bewerten Sie die kryptographische Sicherheit von Algorithmen für Verschlüsselung, Key-Management, Nicht-Abstreitbarkeit und die Kollisionsfestigkeit von Einwegfunktionen. |
| 1.2 Investitionen in IT-Sicherheitsinfrastrukturen brauchen Investitionssicherheit (= 10+ Jahre). Welche Algorithmenkombinationen und –parameter können dafür zugrunde gelegt werden? Sind Kryptosuiten á la NSA/NIST ein denkbares Konzept? |
| 1.3 Welches Gewicht haben Kriterien für die Bewertung kryptographischer Sicherheit? Gibt es eine Strategie zum Umgang mit Expertenanalysen und praktische Erfahrungen? |
| 1.4 Wie bewerten Sie den Stand der Standardisierung bei Kryptoalgorithmen und ihren Stellenwert im Hinblick auf Interoperabilität in Anwendungen? Welche Rolle können ‚Algorithmenkataloge' (z.B. der Bundesnetzagentur) spielen? |
| 1.5 Welche Schlussfolgerungen ergeben sich für die Weiterentwicklung von Standard-Protokollen für Anwendungen aus der permanenten Algorithmendebatte? Wo sehen Sie Ziele und Grenzen bei ihrer Anwendungsflexibilität? |
| 1.6 Welches Gewicht haben Implementierungs- und Anwendungssicherheit im Vergleich zur kryptographischen Sicherheit? Lässt sich Anwendungssicherheit mit differenzierten Policies für Identifikation, Authentifizierung, Signaturen (IAS) und Verschlüsselung pragmatisch definieren? |
| 1.7 Welche Anforderungen an und Policies für den Schutz kryptographischer Schlüssel sind unter Beachtung von Privacy, informationeller Selbstbestimmung und Informationsmanagement sinnvoll? |
| 1.8 Bitte bewerten Sie die ‚Schwachstelle Mensch' (z.B. Umgang mit ‚Wissen'; Passwortdilemma) im Kontext der technischen Möglichkeiten? Gibt es ein ‚vernünftiges' Maß an Anforderungen (und für die Komplexität) von Kryptoverfahren und deren Implementierungen? |
| 1.9 Welche Rolle spielen System- und Komponentensicherheit? Welche Zukunft und welche Grenzen hat möglicherweise das Konzept von ‚Besitz (Token) und Wissen' für IAS? |

| | |
|---|---|
| **2** | **Token:** |
| 2.1 | Wie wird zukünftig die Entwicklung von Tokenfunktionalität und ihrer Integration in Anwendungen verlaufen? Kann die Mobilität von Nutzern und Anwendungen praktikabel und interoperabel abgebildet und flexibel sichergestellt werden? |
| 2.2 | Welche Zukunft haben Trusted Hardware Module (Chipkartenderivate), Trusted Computing und TPM-Anwendungen in Systemarchitekturen? Sind eindeutige Identitäten für Organisationen, Systemkomponenten **und** natürliche Personen praktisch relevant und machbar? |
| 2.3 | Wie werden sich aus Ihrer Sicht die Anforderungen an Gerätekonfigurationen, Betriebssysteme, Middleware und Schnittstellen entwickeln? |
| 2.4 | Welche Kompromisse zwischen ‚theoretischer Sicherheit', Anwenderakzeptanz, Performance, Flexibilität und Migrationsfähigkeit haben Zukunftschancen? |
| 2.5 | Wie sollte sich das Verhältnis zwischen Regulierung und Technologie weiterentwickeln, um ausreichend Spielraum für die dynamische Anwendung von technischen Innovationen und für eine begleitende Rechtsentwicklung zu schaffen? |
| **II** | **Bewertung der Grundlagen von IT-Sicherheitsinfrastrukturen:** |
| 1 | Warum ist die ‚einfache' PKI-Vision der asymmetrischen Kryptographie gescheitert? |
| 2 | Wie bewerten Sie den Stand der Standardisierung für komplexe Trusted Services (Zertifizierungsdienste, Personalisierung von Token)? |
| 3 | Wie können sich technische Standards gegen nationale Policies und Regulierungen behaupten? Können die Folgen (nationaler) gesetzlicher Vorgaben durch robuste Implementierungen auf Basis von Anwendungserfordernissen überwunden werden? |
| 4 | Wie bewerten Sie die Zukunft von IT-Sichheitsinfrastrukturen hinsichtlich des Dienstespektrums, der Interoperabilität und Kooperation sowie der Architektur (hierarchische Lösung versus Bridge- Netzwerkansatz)? |
| 5 | Wie sind Komplexität und Flexibilität von Unternehmens-PKI und öffentlichen Infrastrukturen (Zertifizierungsdiensteanbieter) zu bewerten? Welche Aspekte sind beim Vergleich im Hinblick auf Sicherheit theoretisch und praktisch relevant? |
| 6 | Welche wesentlichen technischen und organisatorischen Aspekte sollten einer wirksamen Umsetzung von Sicherheitspolicies zu Grunde liegen? Welche Services sind unter der Beachtung der ‚Schwachstelle Mensch' von besonderer Bedeutung? |
| 7 | Wie sehen zukünftige Lösungen für die technische Gestaltung von Wirkungs- und Haftungsketten aus? |

| | |
|---|---|
| **III Alternative Konzepte** | |
| **1 Ohne PKI** | |
| 1.1 | Wie bewerten Sie die Chancen von kryptobasierten Identifikations- / Authentifizierungsverfahren ohne PKI? |
| **2 Biometrie** | |
| 2.1 | Welchen Entwicklungsstand haben biometrische Verfahren erreicht? Wie sind sicherheitsrelevante Fragen (z.B. der Überwindungssicherheit) zukünftig eindeutig zu beantworten? |
| 2.2 | Wie bewerten Sie grundsätzlich die Entwicklungstendenzen hinsichtlich Verfahrensbreite, Standardisierung und Konvergenz zu Kryptoverfahren? |
| 2.3 | Welche Ziele sind für die Reichweite der biometrischen Identifikation (eigene Benutzerumgebung, geschlossene Benutzergruppe, offene Systemumgebung) realistisch? |
| 2.4 | Welche Vertrauensinstanzen sind für die biometrische Identifikation in offenen Netzen geeignet (technische – z.B. PKI oder regulatorische - z.B. Policies)? |
| 2.5 | Welche erfolgsversprechende Implementierungsziele für biometrische Verfahren sehen Sie? |
| 2.6 | Unter welchen Voraussetzungen bietet die Biometrie einen Ausweg aus dem Passwortdilemma? Wie kann sie die Anwendungssicherheit in IT-Systemen erhöhen? |
| **IV Sicherheitsevaluierungen, -zertifizierungen** | |
| 1 | Wie bewerten Sie die standardisierten Konzepte (Common Criteria, Protection Profiles usw.) und die heutige Praxis ihrer Anwendung unter den Aspekten Machbarkeit und Wirksamkeit sowie Flexibilität? |
| 2 | Sehen Sie erfolgsversprechende technische Konzepte, die von der Komponenten- oder Systemsicherheit zu einer bewertbaren Anwendungssicherheit führen? |

## Anhang B: Interviewpartner zu Technischen Perspektiven

| | |
|---|---|
| **Prof. Dr. Albrecht Beutelspacher** | Justus-Liebig-Universität Gießen<br>Mathematisches Institut |
| **J. Buchmann** | Forum für Sicherheitstechnologie beim Zentrum<br>für graphische Datenverarbeitung<br>Technische Hochschule Darmstadt |
| **Christoph Busch** | Hochschule Darmstadt<br>CAST e.V., Darmstadt |
| **Lucas Cardholm** | ERNST & YOUNG AB<br>Stockholm, Sweden |
| **Prof. Ernst-Günter Gießmann** | T-Systems<br>Berlin |
| **Jeremy Hilton** | Viviale Ltd<br>Cardiff, UK |
| **Martin Kuppinger** | KUPPINGER COLE + PARTNER<br>Digital ID Analysis & Evaluation<br>München – Stuttgart – Düsseldorf |
| **Herbert Leitold** | A-SIT Zentrum für sichere Informations-<br>technologie Graz |
| **Prof. Christof Paar** | Chair for Communication Security<br>Dept. of Electr. Eng. & Information Sciences<br>Ruhr-University Bochum |
| **Prof. Dr. Norbert Pohlmann** | Fachhochschule Gelsenkirchen<br>Institut für Internet-Sicherheit |
| **Prof. Dr. Bart Preneel** | Katholieke Universiteit Leuven<br>Dept. Electrical Engineering-ESAT/COSIC |
| **Robert Temple** | IT Security Architect<br>BT exact Technologies, Ipswich, UK |

# Anhang C

# Public-Key-Infrastruktur (PKI)

## 1. Einleitung

1978 wurde mit dem RSA-Algorithmus der auch heute noch am häufigsten verwendete Public-Key-Algorithmus entwickelt. Dieses Verfahren ist, wie auch alle anderen asymmetrischen Verschlüsselungsverfahren, dadurch gekennzeichnet, dass für die Verschlüsselung ein anderer Schlüssel als für die Entschlüsselung verwendet wird. Die Sicherheit des Algorithmus beruht auf der Komplexität der Primfaktorzerlegung (vgl. [Ferguson 2002]).

Diese beiden Schlüssel (public key und private key) werden im Prozess der Schlüsselgenerierung erzeugt. Der private Schlüssel muss vom Schlüsselerzeuger und auch später vom Nutzer geheim gehalten werden, währenddessen der öffentliche Schlüssel jedermann zugänglich gemacht wird.

Möchte jemand mithilfe eines asymmetrischen Verschlüsselungsverfahrens eine verschlüsselte Nachricht schicken, so verschlüsselt er diese Nachricht mit dem öffentlichen Schlüssel dessen, an den die Nachricht geschickt wird.
Die Entschlüsselung der Nachricht ist dann nur noch mit dem zum öffentlichen Schlüssel zugehörigen privaten Schlüssel möglich.

Asymmetrische Verschlüsselungsverfahren kann man zusätzlich zur digitalen Signierung einsetzen. Dazu wird von der gegebenenfalls auch selbst zu verschlüsselnden Nachricht ein Hashwert (eindeutiger Fingerprint der Nachricht) erzeugt. Das verwendete Hash-Verfahren muss dabei die Forderung erfüllen, dass zwei unterschiedliche Nachrichten niemals denselben Hashwert besitzen dürfen. Diese Eigen-

schaft wird als Kollisionsresistenz bezeichnet (vgl. [Selke 2000]). Der errechnete Hashwert wird mit dem privaten Schlüssel des Absenders der Nachricht verschlüsselt und kann seitens des Empfängers ausschließlich mit dem öffentlichen Schlüssel des Absenders entschlüsselt werden.

Auf Empfängerseite wird nach dem eventuellen Entschlüsseln der Nachricht ebenfalls der Hashwert der übertragenen Daten gebildet und mit dem eben entschlüsselten Hashwert verglichen. Sind beide identisch, so kann garantiert werden, dass die Nachricht auch wirklich von dem Absender kommt, der im Besitz des privaten Schlüssels ist. Außerdem kann garantiert werden, dass die Nachricht auf dem Übertragungsweg nicht verändert wurde. Die digitale Signatur garantiert somit die Nicht-Abstreitbarkeit seitens des Absenders und die Integrität der Daten.

Aus der asymmetrischen Verschlüsselung ergeben sich klare Vorteile. Diese kommen jedoch nur zum Tragen, wenn sichergestellt werden kann, dass der öffentliche Schlüssel (als Bestandteil eines digitalen Zertifikates) auch wirklich von einer entsprechenden Person stammt und deren digitale Identität somit als vertrauenswürdig angesehen werden kann. Auf dieser Basis lassen sich zudem entsprechende Authentifizierungs- und Identifizierungsmechanismen entwickeln, mithilfe derer sichergestellt werden kann, dass Identitäten (Personen, Unternehmen, Organisationen usw.) eindeutig zugeordnet werden können.

Ein Ansatz zur Lösung all der oben dargestellten Aufgaben ist der Aufbau einer so genannte Public Key Infrastructure (PKI). Diese muss folgende Rahmenbedingungen erfüllen (vgl. [Nash 2002]):
Die PKI muss die sichere Erstellung von gültigen Schlüsseln ermöglichen. Dazu muss sie die Gültigkeitsprüfung der ursprünglichen Identität vornehmen.
Außerdem ermöglicht sie die Ausgabe, Erneuerung und Beendigung von Zertifikaten (vgl. [Oppliger 2005]). Diese Zertifikate und die darin enthaltenen Informationen werden durch die PKI verteilt.

Sowohl der öffentliche als auch der private Schlüssel können in einer PKI archiviert und somit sicher wieder gefunden werden, wobei die Archivierung der privaten Schlüssel nur unter bestimmten Bedingungen notwendig und sinnvoll ist.
Eine PKI ermöglicht auch die Generierung von Signaturen und Zeitstempeln. Eine weitere Aufgabe einer PKI ist der Aufbau und die Verwaltung von Vertrauensstellun-gen. Somit kann eine PKI als Rahmen für den Einsatz von Public-Key-Technologien gesehen werden.

Zwingende Anforderungen an die Technologien stellt die PKI nicht, sodass z.B. der Verschlüsselungsalgorithmus ausgetauscht werden kann. Voraussetzung dafür ist, dass alle an der PKI beteiligten Instanzen in der Lage sind, den Algorithmus benutzen zu können.

Im nächsten Abschnitt werden die einzelnen Komponenten einer PKI vorgestellt.

## 2. Komponenten einer PKI

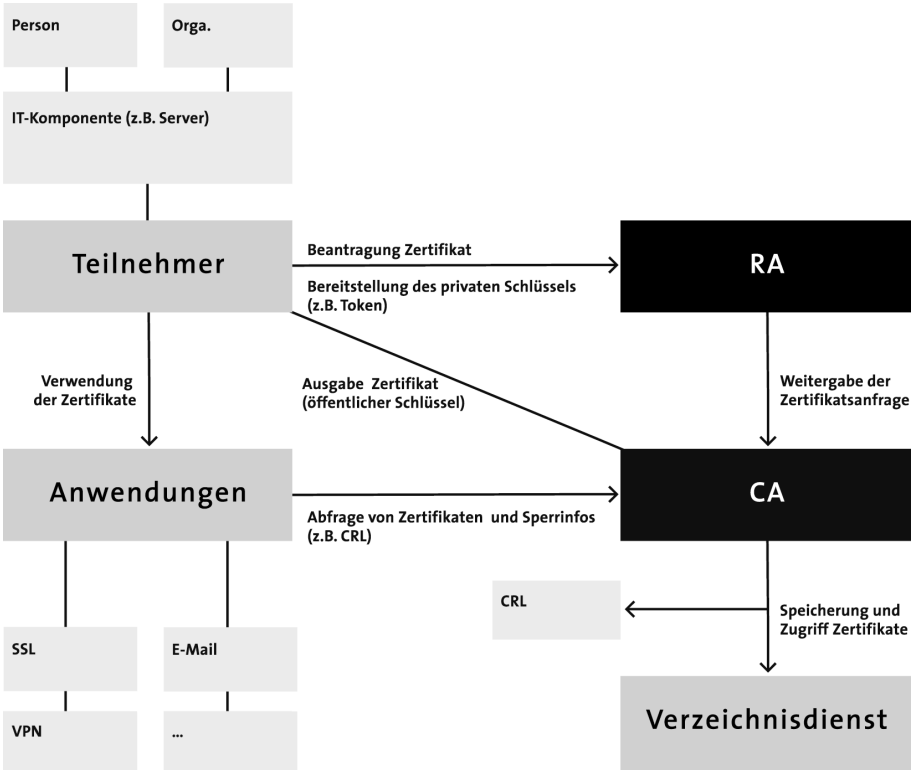


**Abbildung 1: Schema einer PKI**

### 2.1 Registrierungsstelle (Registration Authority – RA)

Eine Registrierungsstelle ist entweder Bestandteil einer Zertifizierungsstelle (CA) (siehe Abschnitt 2.2) oder kann als eigene Komponente betrieben werden. Die Aufgabe der RA besteht (vgl. [Cobb 2004]) darin, die Identität des Antragstellers festzustellen oder zu bestätigen. Der Identitätsnachweis kann z. B. über Geburtsurkunden oder (Lichtbild-) Ausweise erbracht werden. Dabei wird auch die Gültigkeit der Nachweise geprüft. Es wird festgestellt, ob der Antragsteller die Berechtigung für bestimmte Zertifikatsattribute (z.B. für ein CA-Zertifikat) besitzt. Wichtig ist die Feststellung, ob der Antragsteller auch im Besitz des Private-Keys (auch Proof of Possession genannt) ist. Eine RA kann unter Umständen auch die Schlüssel initial erzeugen.

Wenn eine Kompromittierung oder eine zeitliche Ungültigkeit des Schlüsselmaterials vorliegt, gibt die RA diese Informationen an die CA weiter, damit die entsprechenden Zertifikate gesperrt werden, z. B. durch Eintragung in die Certificate Revocation List (CRL).

Die RA leitet den Registrierungsprozess zusammen mit der CA ein, indem die RA einen Antrag auf die Erstellung eines Zertifikates über eine gesicherte Verbindung an die CA weiterleitet.

Außerdem werden private Schlüssel unter bestimmten Umständen (sofern dies rechtlich zulässig ist und/oder von den Teilnehmern gewünscht ist) archiviert, und gegebenenfalls kann durch eine RA eine Schlüsselwiederherstellung veranlasst werden.

Die RA sorgt auch für die Ausgabe von physischen Tokens (z.B. Smartcards) auf denen der private Schlüssel gespeichert ist.
Während des Lebenszyklus der Schlüssel und der Zertifikate ist die RA die Vermittlungsstelle zwischen dem Teilnehmer und der PKI. Die RA macht – bis auf die Bestätigung gegenüber der CA – keine Angaben über die Vertrauenswürdigkeit der Teilnehmer einer PKI.

### 2.2 Zertifizierungsstelle (Certificate Authority – CA)

Vorrangige Aufgabe einer CA ist die Übernahme des Managements aller Lebenszyklen eines Zertifikates. So wird ein gesperrtes Zertifikat in die Certificate Revocation List (CRL) eingetragen und gleichzeitig für den Fall einer späteren Überprüfung archiviert.

Eine weitere Aufgabe der Zertifizierungsstelle besteht darin, Zertifikate zu erstellen und diese auszugeben, nachdem es den Antrag auf Erstellung des Zertifikats von RA überprüft hat.

Für die Verwendung einer qualifizierten Signatur mit Anbieterakkreditierung dürfen die qualifizierte Zertifikate nur von in Deutschland durch die Bundesnetzagentur akkreditierten CA (hier auch TrustCenter genannt) ausgestellt werden. Mit dieser Akkreditierung ist verbunden, dass das TrustCenter ein Gütesiegel für garantierte organisatorische und technische Sicherheit besitzt und die Zertifikate 30 Jahre nach Ablauf ihres Gültigkeitszeitraums in einem Verzeichnis speichert, damit dessen Gültigkeit überprüft werden kann (vgl. [IHK 2005]).

Die von der CA ausgegebenen Zertifikate werden mit dem privaten Schlüssel des CA signiert. Somit ist die Integrität und Authentizität eines Zertifikats durch die Entschlüsslung der Signatur mit dem im CA-Zertifikat enthaltenen öffentlichen Schlüssel überprüfbar, indem der durch die Entschlüsselung erhaltene Hashwert (Fingerprint) des Zertifikats mit dem generierten Hash verglichen wird.

Das Zertifikat einer CA ist entweder selbst-signiert, wenn es sich um ein Root-CA-Zertifikat handelt (es gibt keine weiteren CA-Instanzen in der Hierarchie oberhalb dieser CA) oder es wird mit dem privaten Schlüssel der jeweils nächst höher gelegenen CA signiert.

Durch die Möglichkeit, die CA-Zertifikate durch höhere CA-Instanzen signieren zu lassen, entsteht ein so genannter Validierungspfad, an deren Ende eine Root-CA steht. Ein Teilnehmer, welcher dieser Root-CA vertraut (z.B. durch das Abspeichern des entsprechenden Root-CA-Zertifikats im Zertifikatsspeicher eines IT-Systems), vertraut automatisch auch allen anderen CA-Zertifikaten dieses Pfades.

Eine CA ist somit ein elementarer Bestandteil einer PKI, deren Grundbedeutung unabhängig vom verwendeten Vertrauensmodell (vgl. Kapitel 3) ist. Da CAs für die unterschiedlichsten Einsatzgebiete etabliert werden, sind die Rahmenbedingen und die Vorgaben (z.B. Speicherung der Zertifikate auch nach Ablauf ihrer Gültigkeit, um den Nachweis der Gültigkeit von digitalen Signaturen sicherstellen zu können) für jede CA individuell. So gilt für eine Root-CA das Höchstmaß an Sicherheit, um die Notwendigkeit einer Neuzertifizierung aller untergeordneten Instanzen so gering wie möglich zu halten.

### 2.2.1 Certificate Revocation List (CRL)

In der CRL werden die gesperrten Zertifikate gespeichert. Die CRL hat eine be-stimmte Laufzeit, nach deren Ablauf sie erneuert werden muss. Die CRL wird von der CA signiert, sodass die Vertrauenswürdigkeit der Liste sichergestellt werden kann. Eine CRL lässt sich zur Offline-Überprüfung von Zertifikaten nutzen.

### 2.2.2 Validierungsdienst

Neben der Offline-Validierung von Zertifikaten durch die Verwendung von CRL kann die Validierung auch online über die Protokolle „Online Certificate Status Protocol“ (OCSP) und „Server-based Certificate Validation Protocol“ (SCVP) erfolgen.

Das OCSP dient dazu, Zertifikate zu identifizieren, die vor dem Ablauf ihres Gültigkeitszeitraums ungültig geworden sind. Ungültige Zertifikate dürfen bei sicherheitskritischen Anwendungen keine Verwendung finden. Der Status eines Zertifikats kann durch die Anfrage an den so genannten OCSP-Responder, welcher meist vom Zertifikatsherausgeber betrieben wird, abgefragt werden. Folgende Stati sind möglich (vgl. [RFC 2560]):

→ „good“ (Zertifikat ist gültig)
→ „revoked“ (Zertifikat gesperrt)
→ „unknown“ (Zertifikat unbekannt)

Wenn ein Zertifikat gesperrt ist, dann wird auch der Zeitpunkt der Sperrung angegeben. Als Transportprotokoll für die Übertragung der Daten zwischen Client und Server werden meist die Protokolle http oder https verwendet. Es ist möglich, den Status von mehreren Zertifikaten abzufragen. OCSP wird jedoch nicht so häufig zur Validierung von Zertifikaten eingesetzt, dennoch betreiben alle CAs in Deutschland, die qualifizierte Zertifikate ausgeben, einen solchen Responder, um dem Signaturgesetz (vgl. [SigG 2001]) zu entsprechen.

Ein großer Vorteil des OCSP gegenüber einer CRL besteht darin, dass die Sperrinformationen in Echtzeit vorhanden sind, sofern der OCSP-Server direkten Zugriff auf die Datenbank der CA hat (vgl. [Holenstein 2004]), währenddessen CRL nur periodisch erneuert werden.

Nachteil von OCSP ist, dass der Client (für den Fall, dass er nur der Root-CA vertraut) selbst einen Validierungspfad aufbauen muss, um an die notwendigen Informationen zur Überprüfung eines Zertifikates zu gelangen, denn der OCSP-Responder liefert die Struktur des Validierungspfades nicht mit (vgl. [Nash 2002]).
Wenn eine CA vorübergehende Sperrungen zulässt (dies ist nach dem deutschen Signaturgesetz unzulässig), dann lässt sich nicht nachvollziehen, ob ein Zertifikat zu einem bestimmten Zeitpunkt ungültig war.

Das SCVP, welches bisher nur als Entwurf existiert (vgl. [IETF 2007]), wurde entwickelt, um die Schwächen des OCSP zu beheben (vgl. [Nash 2002]). Der grundlegende Unterschied zu OCSP besteht darin, dass der SCVP-Client an den Server kom-plette Zertifikate zur Überprüfung z.B. mittels http an den SCVP-Server überträgt. Der Client kann auch weitere übergeordnete Zertifikaten übertragen, welche bei der Echtheitsüberprüfung der zu prüfenden Zertifikate mit berücksichtigt werden müssen.

Der Client kann außerdem angeben, wie der Server die Anfragen zu bearbeiten hat: z.B. durch die Angabe der anzuwendenden Zertifikatsrichtlinien und welche CRL- und OCSP-Dienste zum Abfragen der Zertifikatssperrstati genutzt werden sollen. Der Client muss sich dabei nicht um die Überprüfung der Validierungspfade kümmern, somit ermöglicht das SCVP das teilweise bis vollständige Auslagern der Zertifikats-Validierung (vgl. [Holenstein 2004]). Die Antworten des Servers werden ebenso wie im OCSP digital signiert um die Integrität und Authentizität der Nachricht zu gewährleisten.

### 2.2.3 Gültigkeit von Zertifikaten

Um die Gültigkeit eines Zertifikates zu überprüfen gibt es drei verschiedene Gültigkeitsmodelle (vgl. [Wolf 1998]). Das Schalenmodell wird im PEM[1]-Standard, siehe

[1] Privacy Enhancement for Internet Electronic Mail

RFC 1421 – 1424, beschrieben. Das Schalenmodell trifft die Aussage über die Gültigkeit eines Zertifikates anhand des Verifikationszeitpunktes. Die Gültigkeit eines Zertifikates zu einem bestimmten Zeitpunkt ist genau dann gegeben, wenn die Signatur des Zertifikates gültig ist, der Zeitpunkt innerhalb des Gültigkeitszeitraums des Zertifikates liegt und das Zertifikat zum fraglichen Zeitpunkt nicht gesperrt ist. Außerdem müssen zum prüfenden Zeitpunkt alle Zertifikate der zum Validierungspfad des Zertifikats gehörenden CAs gültig sein. Beim Schalenmodell wird nicht überprüft, ob das Zertifikat zu dem Zeitpunkt gültig war, an dem mit dem zum Zertifikat entsprechenden privaten Schlüssel eine Signatur erzeugt wurde. Um dies zu prüfen verwendet man das so genannte modifizierte Schalenmodell.

Im Gegensatz zum Schalenmodell wird hier die Gültigkeit des Zertifikats und des Validierungspfades zum Zeitpunkt der Signierung eines Dokumentes geprüft. Dies hat zur Folge, dass Signaturen auch dann als gültig angesehen werden, obwohl das Zertifikat zum Verifikationszeitpunkt bereits abgelaufen ist.

Das Kettenmodell verfolgt einen anderen Ansatz. Die Gültigkeit einer Signatur ist gegeben, wenn das Teilnehmer-Zertifikat zum Signierzeitpunkt gültig war. Ferner wird geprüft, ob Zertifikate des Validierungspfades zum Zeitpunkt ihrer Anwendung gültig waren. Das bedeutet, das Zertifikat der CA die das Signierzertifikat ausgegeben hat, muss zum Ausgabezeitpunkt gültig gewesen sein. Auf dieselbe Art und Weise wird die Gültigkeitsprüfung an den Zertifikaten der hierarchisch darüberliegenden CAs vorgenommen. Es wird bei diesem Modell nicht überprüft, ob das Zertifikat seit der Signatur gesperrt wurde.

Damit die Signatur eines Dokumentes nach allen drei Modellen gültig ist, muss es kurz vor Ablauf des Gültigkeitszeitraums des Zertifikates, welches zum entsprechen-den Signaturschlüssel gehört, neu signiert werden.

### 2.3 Digitale Zertifikate

Ein digitales Zertifikat ist eine Datenstruktur, die eine bestimmte Identität (Person, Organisation oder IT-System) und dessen Public-Key miteinander verknüpft. Der derzeit wichtigste Standard für digitale Zertifikate für die Benutzung in einer PKI heißt X.509. Derzeit aktuell ist X.509v3 und wurde von der ITU-T[2] als Standard festgeschrieben.

In einem Zertifikat sind unter anderem folgende Daten enthalten:

1. Versionsnummer (z. B.: 3)
2. Seriennummer (z. B.: 42)

---

[2] Sektor der internationalen Fernmeldeunion (International Telecommunications Union – ITU), welcher für Empfehlungen und Standardisierungen im Fernmeldewesen zuständig ist.

3. Herausgeber des Zertifikates (Angabe von Land, Bundesstaat, Ort, Organisation, Abteilung, Name, E-Mail-Adresse)
4. Gültigkeitszeitraum
   a. nicht vor einem Zeitpunkt
   b. nicht nach einem Zeitpunkt
5. Inhaber des Zertifikates (Angabe von Land, Bundesstaat, Ort, Organisation, Abteilung, Name [Person, Organisation, IT-System], E-Mail-Adresse)
6. Public-Key-Algorithmus (z.B. rsaEncryption)
7. Public-Key
8. Signaturalgorithmus (z.B.: md5WithRSAEncryption)
9. Signatur des Zertifikats
10. Erweiterungen

Zu den Erweiterungen zählt z.B. die Angabe einer URL, unter welcher die Policy der Zertifizierungsstelle (CA), welche die Arbeitsweise der CA beschreibt, eingesehen werden kann. Eine weitere beschreibt den Einsatz des Zertifikates (z.B. für die Daten-Verschlüsselung). Ein Zertifikat sollte ausschließlich für diese aufgeführten Zwecke eingesetzt werden.

Es gibt folgende zwei wichtige Zertifikatstypen:
→ Teilnehmerzertifikate und
→ CA-Zertifikate (erkennbar in der Erweiterung „Basic Contraints“, in dessen Feld „CA“ den Wert TRUE besitzt), die dem Inhaber erlauben, selbst Zertifikate auszustellen.

### 2.3.1 Arten von Zertifikaten

Neben selbst-signierten Zertifikaten (aus denen einer Root-CA), bei denen keine sichere Identifizierung des Inhabers sichergestellt werden kann, gibt es die so genannten fortgeschrittenen Zertifikate. Bei diesen kann die Identität des Inhabers ein-deutig sichergestellt werden, jedoch sind die mit diesen Zertifikaten erzeugten fortgeschrittenen Signaturen einer Unterschrift von Hand rechtlich nicht gleich gestellt (vgl. [D-Trust 2007]). „Der entscheidende Unterschied zur gewöhnlichen Unterschrift besteht darin, dass die digitale Signatur [...] untrennbar mit der Nachricht [...] verbunden ist.“ [Beutelspacher 2002]

Qualifizierte Zertifikate hingegen ermöglichen qualifizierte digitale Signaturen, die einer händischen Unterschrift rechtlich gleichgestellt sind. Solche Zertifikate dürfen nur von offiziellen Zertifizierungsstellen ausgegeben werden, die sich an die Bestimmungen des in Deutschland gültigen Signaturgesetzes halten. Die höchste Stufe sind qualifizierte Zertifikate mit Anbieterakkreditierung, bei denen die ausstellungsberechtige Zertifizierungsstelle durch den TÜV-IT geprüft und von der Bundesnetzagentur bestätigt ist.

### 2.3.2 Beispiele der Verwendung von Zertifikaten

Zertifikate kommen z.B. beim Secure-Sockets-Layer(SSL)-Protokoll zum Einsatz, welches im OSI-Modell oberhalb der Transportschicht angesiedelt ist. Protokolle in der Anwendungsschicht des OSI-Modells können um die SSL-Protokoll-Funktionalität (und somit um die Möglichkeit der Verschlüsselung und Gewährleistung der Authentizität und Integrität von Daten) erweitert werden.

Ein Beispiel dafür ist das Hypertext Transfer Protocol Secure (https)-Protokoll. Über dieses Protokoll kann eine verschlüsselte Verbindung zwischen Browser und Webserver hergestellt werden.

Obwohl eine gegenseitige Authentifizierung beider beteiligen Parteien möglich ist, wird meist nur der Server durch die Überprüfung des Server-Zertifikates, welches als Namen des Inhabers die Domain des Webservers enthält, authentifiziert. Hierbei wird das Zertifikat vom Server zum Browser übertragen.

Dieser überprüft das Zertifikat nach bestimmten Kriterien:

1. Stimmt die Domain mit der im Zertifikat angegebenen Domain überein?
2. Ist das Zertifikat abgelaufen oder steht es auf einer Zertifikatsperrliste (Certificate Revocation List – CRL)?
3. Ist das Zertifikat von einer dem Browser als vertrauenswürdig eingestuften CA signiert?

Sollten einige Kriterien nicht zutreffen, so gilt das Zertifikat als nicht-vertrauenswürdig und der Benutzer wird gefragt, ob er diesem Zertifikat trotzdem vertrauen möchte. Wenn dem Zertifikat vertraut wurde, wird browser- und serverseitig der Sitzungsschlüssel erzeugt. Dieser dient anschließend auf beiden Seiten zur symmetrischen Verschlüsselung der zu übertragenden Daten, was einen Geschwindigkeitsgewinn gegenüber der asymmetrischen Verschlüsselung bietet, der übertragenen Daten erzeugt.

Ein weiteres Anwendungsgebiet ist E-Mail. Hierbei werden Zertifikate für zwei verschiedene Zwecke eingesetzt.
Zum einen kann mit dem öffentlichen Schlüssel des Empfängers, welcher in seinem Zertifikat oder einer entsprechenden CA hinterlegt ist, eine Nachricht verschlüsselt werden. Zum anderen ist es möglich, die Identität des Absenders und die Integrität des Mailinhalts zu gewährleisten, indem der Absender mithilfe seines privaten Schlüssels den Hashwert der Nachricht verschlüsselt. Dieser verschlüsselte Hashwert wird an die verschlüsselte Nachricht angehängt und ermöglicht dem Empfänger, mit dem öffentlichen Schlüssel des Absenders den Hashwert und mit seinem eigenen privaten Schlüssel die Nachricht selbst zu entschlüsseln. Anschließend kann er für die entschlüsselte Nachricht den Hashwert erzeugen, mit dem entschlüsselten Hashwert vergleichen und somit die Identität feststellen.

Auch bei der Verwendung von Virtual-Private-Networks (VPN), welche durch den Aufbau von Tunneln verschlüsselte Verbindungen zwischen Kommunikationsteilnehmern innerhalb eines öffentlichen ungesicherten Netzes ermöglichen, werden Zertifikate zur Feststellung der Identität eines an einem VPN beteiligten Endpunktes verwendet. Dabei wird im Zertifikat für einen am VPN beteiligten Endpunkt die Netzwerkadresse des Netzwerkknotens vermerkt (vgl. [Nash 2002]). Die Endpunkte identifizieren sich gegenüber den anderen Teilnehmern, indem sie ihr Zertifikat zeigen und auch sicherstellen, dass der entsprechende private Schlüssel vorliegt.

### 2.4 Verzeichnisdienst

Ein Verzeichnisdienst bietet als Bestandteil einer PKI die Möglichkeit der zentralen Speicherung von Zertifikaten. Durch die Nutzung dieses Dienstes können benötigte Zertifikate geholt werden. Ein Zertifikatsinhaber muss somit sein Zertifikat seinen Kommunkationspartnern nicht bilateral zur Verfügung stellen (vgl. [Hammer 1999]).

Die Zertifikate werden in einem Verzeichnisdienst technisch gesehen in einer hierarchischen Datenbank abgelegt. Über das Client/Server-Prinzip können die darin enthaltenen Daten manipuliert werden. Früher verwendete man als Verzeichnisdienst den X.500-Verzeichnisdienst. Gegenwärtig werden häufig LDAP-basierte Verzeichnisdienstlösungen zur Speicherung der Zertifikate eingesetzt (vgl. [Schmeh 2001]), welche u.a. bei der Verwaltung der verfügbaren Ressourcen (z.B. Speicherplatz) effizienter sind.

### 2.5 Dokumente

Zu den Dokumenten, welche innerhalb einer PKI gepflegt werden müssen, gehört das Certificate Practice Statement (CPS), welches die Umsetzung der Richtlinien für die Ausstellung von Zertifikaten festschreibt. Das CPS wird in den RFC 3647 und RFC 2527 beschrieben. Falls das CPS nicht veröffentlicht werden soll, wird ein Policy Disclosure Statement (PDS) mit einem für die Öffentlichkeit relevanten Auszug aus dem CPS veröffentlicht. Daneben gibt es das Dokument „Certificate Policy“ (CP), welches das Anforderungsprofil einer PKI an ihre Arbeitsweise und die Zertifizierungsrichtlinien beschreibt.

Auf diese Dokumente kann im Zertifikat über ein Erweiterungsfeld, welches eine URL zu den Dokumenten enthält, verwiesen werden, sodass derjenige, der einem Zertifikat vertrauen will, genau mit der Arbeitsweise der PKI hinsichtlich der Zertifikatserstellung und –verwaltung vertraut gemacht werden kann. Auf dieser Basis wird er u.U. auch Zertifikaten vertrauen, die zunächst nicht als vertrauenswürdig eingestuft wurden.

Außerdem gibt es Dokumente, auf die nicht über das Erweiterungsfeld (vgl. Abschnitt 2.3) zugegriffen werden kann. Diese beschreiben, wie Abläufe, Schnittstellen und Rollen innerhalb einer PKI definiert sind. Weitere Dokumente beschreiben das Verhalten im laufenden Betrieb der PKI. Auch ein Sicherheits- und ein Notfallkonzept gehört zu den PKI-Dokumentationen.

## 3. Vertrauensmodell

Ein Vertrauensmodell bildet die Grundlage für die Erstellung und das Management von Vertrauensstellungen, die für den Betrieb einer PKI mit mehreren CA notwendig sind. Solche Vertrauensstellungen werden z.B. durch das Ausstellen von einem CA-Zertifikat für eine CA durch eine andere CA erreicht. Wenn man einer CA vertraut, welche das Zertifikat einer anderen signiert hat, dann kann man folglicherweise auch dieser vertrauen. Es gibt verschiedene Vertrauensmodelle. Auf einige von ihnen wird in den nächsten Abschnitten eingegangen.

### 3.1 Hierarchisches Modell

Im Vertrauensmodell der allgemeinen Hierarchie sind bidirektionale Vertrauensstellungen zulässig und der Zertifikatsbenutzer kann eine beliebige CA als vertrauenswürdige Stelle definieren.

Im Modell der untergeordneten Hierarchie gibt es genau eine Vetrauensbasis: die Root-CA. Alle Vertrauensstellungen basieren darauf, dass die Root-CA, für die CAs der nächsten Ebene, die ihrerseits ebenfalls Zertifikate ausstellen können, Zertifikate ausstellt.

Das Zertifikat der Root-CA kann von keiner anderen CA als der Root-CA selbst ausgestellt werden. Man spricht von der Selbst-Signierung des Root-CA-Zertifikates, bei welcher der Aussteller des Zertifikates mit dem CA-Betreiber identisch ist, die Wertigkeit und Vertrauenswürdigkeit der Root-CA jedoch beispielsweise über staatliche Mechanismen oder Öffentlichkeit und Bekanntheitsgrad abgesichert ist.

Die Verkettung von Zertifikaten zur Überprüfung eines Zertifikats nennt man Zertifi-zierungspfad. In diesem Vertrauensmodell ist das Root-CA-Zertifikat immer Basis dieses Pfades.

Bei diesem Modell entsteht ein Problem, wenn das Root-CA-Zertifikat kompromittiert werden würde. Dann müsste dieses – und somit auch alle untergeordneten Zertifikate – ausgetauscht werden. Da die Root-CA jedoch selten in Anspruch genommen wird (nur bei Zertifizierung von untergeordneten CAs und evtl. Sperrung von CAs) ist die Wahrscheinlichkeit einer Kompromittierung eher als gering einzustufen.

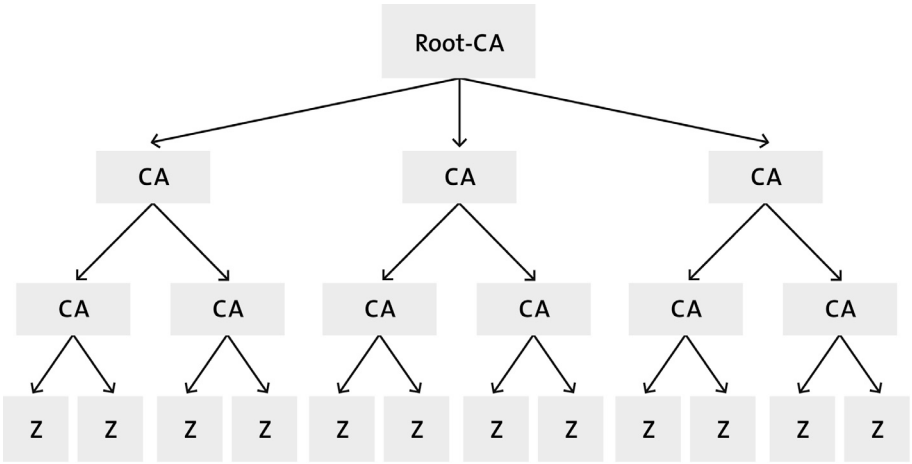


**Abbildung 2: Vertrauensmodell „untergeordnete Hierarchie“**

Dieses Vertrauensmodell ist das verbreitetste, was u.a. dadurch begründet ist, dass für eine erfolgreiche Zertifikatsüberprüfung nur der Zertifizierungspfad bis zur Wurzelinstanz durchlaufen werden muss.

## 3.2 Peer-To-Peer-Modell

Im Peer-To-Peer-Modell wird der Aufbau einer Vertrauensbeziehung von zwei gleich gestellten Zertifizierungsinstanzen beschrieben. Dazu stellt jede CA der jeweils anderen CA ein Zertifikat aus (auch gegenseitige Zertifizierung genannt).
Nachteil dieses Modell ist, dass es nicht skalierbar ist. Denn wenn zum Beispiel vier CAs sich gegenseitig zertifizieren und jede mit jeder anderen in einer bidirektionalen Vertrauensstellung steht, dann sind 12 Zertifikate notwendig. Die allgemeine Formel lautet für die Anzahl der benötigten Zertifikate:

Anzahl der Zertifikate = CA-Anzahl * (CA-Anzahl – 1).

Dieses Modell ist meist erst nutzbar, wenn von PKI-Herstellern angebotene Plug-Ins genutzt werden, die den Aufbau und die Überprüfung von Zertifizierungspfaden mit gegenseitigen Zertifizierungen unterstützen.

## 3.3 Maschenmodelle

Bei einem Maschenmodell gibt es nicht zwischen allen CAs eine bidirektionale Vertrauensstellung, sondern nur zwischen einigen dieser CAs. Zur Überprüfung eines

Zertifikats muss deshalb erst der Zertifizierungspfad gefunden werden.
Durch das Anfragen an verschiedene CAs, welche Vertrauensstellung diese mit anderen CAs besitzt, gelangt man schließlich von der eigenen vertrauenswürdigen CA zu der CA, welche das zu untersuchende Zertifikat signiert hat.
Dabei ist es jedoch nicht möglich vorherzusagen, welcher Zertifizierungspfad genommen werden muss, da man zunächst nicht weiß, welche CAs untereinander durch eine Vertrauensstellung verknüpft sind. Deshalb kann im Gegensatz zu der in Abschnitt 3.1 beschriebenen untergeordneten Hierarchie der Zertifizierungsweg nicht mit dem Teilnehmerzertifikat übermittelt werden.

Ein Problem dieses Maschenmodells ist, dass man keine Aussage darüber treffen kann, welche Aktivitäten ein zertifizierter Partner plant. So kann es passieren, dass die CA eines Konkurrenten durch den Aufbau einer Vertrauensstellung mit dem Partner Teil der Masche wird. Um dies zu verhindern, ist eine Richtlinienstelle (Policy Authority) zu etablieren, die sich um das Management der Richtlinien (damit eben keine Konkurrenten Teil der Masche werden können) kümmert.

### 3.4 Hybride Vertrauensmodelle

Zu den hybriden Vertrauensmodellen gehört das Verbinden von untergeordneten Hierarchien. Dieses Modell besteht aus mehreren Root-CAs, welche jeweils die Vertrauensbasis für die darunterliegenden Ebenen bilden. Merkmal dieses Vertrauensmodell ist es, dass sich die Root-CAs untereinander zertifizieren, also eine Vertrauensstellung zwischen ihnen besteht. Als Alternative zur Zertifizierung der Root-CAs untereinander besteht die Möglichkeit des Einsatzes einer so genannten Bridge-CA. Dabei zertifizieren sich jeweils die Bridge-CA und jede einzelne Root-CA gegenseitig. Die Bridge-CA ist dabei jedoch weder Vertrauensbasis noch Wurzelinstanz (vgl. [Nash 2002]).

Es gibt ferner innerhalb einer Hierarchie die Möglichkeit, dass sich untergeordnete CAs gegenseitig zertifizieren. Dies führt u.U. zur Optimierung der Zertifikatsgültigkeitsfeststellung, da der Zertifizierungspfad kleiner ist, als der im Falle einer untergeordneten Hierarchie.

### 3.5 Web of Trust

Dieses dezentrale Vertrauensmodell basiert darauf, dass man (A) einer Zertifizierungsinstanz (C-H) vertraut werden kann, sofern eine andere Instanz (B-G), welcher man selbst (auch indirekt ) traut, dieser Instanz vertraut. Dies geschieht durch das gegenseitige Signieren der öffentlichen Schlüssel (vgl. [Schwenk 2002]). Je kürzer der Pfad von der eigenen Zertifizierungsinstanz zur Zielzertifizierungsinstanz ist, desto vertrauenswürdiger kann dieser Weg angesehen werden (vgl. [Vaudenay 2006]).

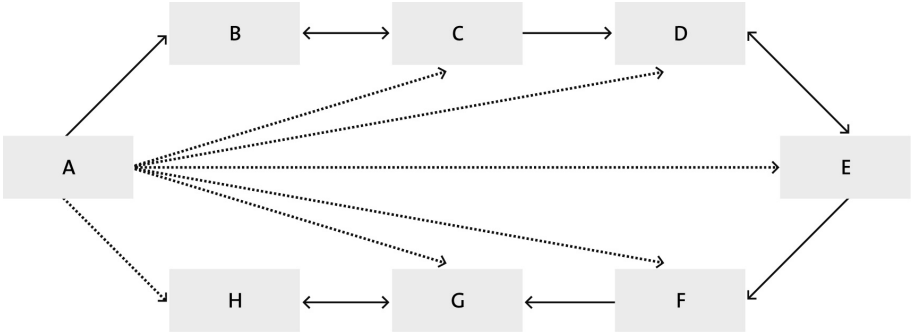


**Abbildung 3: Vertrauensmodell „Web of Trust“**

Das Problem bei diesem Modell besteht darin, dass jede Instanz sehr sorgfältig mit den Vertrauensbeziehungen umgehen muss damit das Vertrauensmodell seinen Zweck erfüllen kann und keine „boshaften“ Instanzen Teil des Web of Trust werden.

## 4. Fazit

Eine PKI ermöglicht durch ihre Komponenten die vertrauenswürdige Nutzung von Zertifikaten, welche die öffentlichen Schlüssel von Teilnehmern enthalten und zur Authentifizierung und Identifizierung von Benutzern sowie zur Verschlüsselung von Daten und zur Überprüfung von digitalen Signaturen verwendbar sind.
Eine PKI beschreibt dabei den Rahmen, in dem verschiedenste Public-Key-Technologien zum Einsatz kommen können. Diese Technologien sind hierbei austauschbar.

## 5. Quellen


[Beutelspacher 2002] Beutelspacher, A.: Kryptologie; 6. Auflage; Vieweg; 2002.

[Cobb 2004] Cobb, C.: Cryptography for Dummies; Wiley Publishing Inc.; 2004.

[D-Trust 2007] Kommunikationssicherheit à la carte; D-Trust; 2007. https://www.d-trust.net/internet/content/kommunikationssicherheit.html

[Faber 2007] von Faber, E.: PKI-Vorlesungsmaterialien; FH Brandenburg; 2007.

[Ferguson 2002] Ferguson, N.; Schneier, B.: Practical Cryptography; Wiley Publishing Inc.;2002.

[Hammer 1999] Hammer, V.: Die 2. Dimension der IT-Sicherheit; Vieweg; 1999.

[Holenstein 2004] Holenstein, N.; Pfister, C.: Statusprüfung von Zertifikaten mit CRL und OCSP, bewertet auf Basis des aktuellen Umfelds von UBS; Zürcher Fachhochschule Winterthur; 25.10.2004. http://security.hsr.ch/theses/DA_2004_CertificateRevocationStudy.pdf

[IETF 2007] Public-Key Infrastructure (X.509) (pkix) Charter; IETF Secretariat ; 02.04.2007. http://www.ietf.org/html.charters/pkix-charter.html

[IHK 2005] Digitale Signatur Überblick; IHK für Oberfranken Bayreuth; 2005. http://www.bayreuth.ihk.de/xist4c/download/web/5710488422_3576_uplId_92712__coId_1057_.pdf;jsessionid=0538F61B107B706A15DC682534FE8AA6

[Nash 2002] Nash, A.: PKI – e-security implementieren; RSA Press; 2002.

[Oppliger 2005] Oppliger, R.: Contemporary Cryptography; Artech House; 2005.

[RFC 2560] Request for Comments 2560: X.509 Internet Public Key Infrastructure – Online Certificate Status Protocol – OCSP; Juni 1999. http://tools.ietf.org/html/rfc2560

[Schmeh 2001] Schmeh, K.: Kryptografie und Public-key-Infrastrukturen im Internet; 2. Auflage; dpunkt-Verlag; 2001.

[Schwenk 2002] Schwenk, J.: Sicherheit und Kryptographie im Internet; Vieweg; 2002.

[Selke 2000] Selke, G.W.: Kryptographie – Verfahren, Ziele, Einsatzmöglichkei-ten; O'Reilly; 2000.

[SigG 2001] Gesetz über Rahmenbedingungen für elektronische Signaturen (Signaturgesetz); Bundesministerium der Justiz; 16.05.2001. http://www.gesetze-im-internet.de/sigg_2001/index.html

[Vaudenay 2006] Vaudenay, S.: A Classical Introduction to Cryptography; Springer; 2006.

[Wolf 1998] Wolf, R.: Verifikation digitaler Signaturen; TU Darmstadt; 1998. http://www.informatik.tu-darmstadt.de/BS/Lehre/Sem98_99/T11/index.html

# Anhang D

# Return on Security Investment (ROSI)

## 1. Einleitung: Messung von IT-Sicherheitsinvestitionen

Was ist der Nutzen meiner Investition in eine IT-Sicherheitsmaßnahme? Diese Frage stellen sich viele Entscheidungsträger, wenn es um das Budget für den Ausbau der IT-Sicherheit im Unternehmen geht. Unsicherheit, Angst und Zweifel reichen nicht mehr als Argument für die permanent wachsenden Fixkosten der IT-Sicherheit. Quantitative und qualitative Ansätze zur Bestimmung einer wirtschaftlich sinnvollen Investion sind gefragt. Zur Beurteilung des Nutzens einer IT-Sicherheitsmaßnahme werden Kriterien benötigt, anhand derer man das Ergebnis messen kann. Eventuell ist es sogar sinnvoller, einen möglichen Schaden hinzunehmen als Unsummen für seine Abwehr auszugeben.

Die Abwehr von Gefahren muss in jedem Unternehmen unterschiedlich bewertet werden. So kann ein Unternehmen durch starkes Wachstum oder gestiegenes Medieninteresse viel häufiger Opfer von Angriffen sein als ein bedeutungsloser Konkurrent. Ein Anderes begründet seinen Erfolg durch wertvolles geistiges Eigentum, welches verstärkt geschützt werden muss. Eine weitere Bedrohung liegt im Imageverlust, den ein Unternehmen erleidet, falls ein erfolgreicher Angriff bekannt wird oder geheime Unternehmens- oder Personaldaten im Internet veröffentlicht werden. Jedoch sind sich viele Unternehmen der Schäden durch Sicherheitsvorfälle und auch der daraus abzuleitenden Kosten nicht bewusst. Nur wenige Firmen sind überhaupt in der Lage, Angaben zur Schadenshöhe eines erfolgreichen Angriffes zu machen.

An den oben genannten Beispielen kann man erkennen, dass eine exakte Bewertung von Risiken äußerst schwierig ist. Das Problem liegt in der IT-Sicherheit als Querschnittsthema begründet. Es existieren vielfältige Wechselwirkungen mit den Prozessen im Unternehmen, weswegen eine Kosten-Nutzen-Betrachtung und -Optimierung eine betriebswirtschaftliche Gesamtbetrachtung erfordert. (vgl. [Lubich 2006], S. 9)

Ein weiterer Ansatz, Sicherheit in einem Unternehmen zu bewerten, setzt bei den Versicherungen an. Ein in diesem Zusammenhang häufig genanntes Beispiel sind Sprinkler-Anlagen für Fabriken. DIese kamen Ende des 19. Jahrhunderts erstmals zum Einsatz. Ihr Nutzen wurde damals als ebenso zweifelhaft angesehen, wie der einiger Sicherheitsinvestitionen heutzutage. Erst als die Versicherungen günstigere Angebote für Fabriken mit Sprinkler-Anlagen anboten, konnte der Ertrag der Investition in solche Anlagen glaubhaft nachgewiesen werden. Das Problem besteht in der Verlässlichkeit und konsistenten Erhebung der zugrunde liegenden Daten. Hier ist eine gemeinsame Basis zur Berechnung zu finden. (vgl. [Berinato 2002])

## 2. Berechungsarten des ROSI

Für die Gesamtheit aller Kosten einer Investition werden häufig die Berechungsmethoden Total Cost of Ownership (TCO) und Return on Investment (ROI) verwendet. Bei der TCO-Berechnung werden alle Kosten über den gesamten Lebenszyklus der Investition berücksichtigt. Dazu gehören Anschaffung, Installation und dauerhafte Betriebs- und Wartungskosten. Es wird jedoch kein Nutzen oder Ertrag ermittelt. Der ROI geht einen Schritt weiter, indem man von der Annahme ausgeht, dass eine Investition im Laufe der Jahre einen positiven Nutzen generiert. (vgl. [Müßig 2006], S. 39) In einer Amortisationsrechnung wird die Investition dem Nutzen gegenübergestellt. Es wird also ermittelt, ab wann die Investition einen Ertrag erwirtschaftet. (vgl. [Schmeh 2004])

Auf Grundlage des ROI wurde an der Universität Idaho der Return On Security Investment (ROSI) entwickelt. Er bietet ein nutzen- und bilanzorientiertes Modell als Grundlage für die verbesserte Schätzung der Investitionen in IT-Sicherheit. Es wird versucht, unter Betrachtung aller Kosten aufzuzeigen, ob und wann ein Investment in IT-Sicherheitsmaßnahmen zu einem Return On Invest führt oder nicht. Es gibt verschiedene nicht standardisierte Methoden, den ROSI zu ermitteln, die aber auf den gleichen Annahmen beruhen und sich ähnlich berechnen. Dies ist auch als die größte Schwäche des ROSI hervorzuheben. Aufgrund unterschiedlicher Berechnungsmethoden und Einschätzungen von Risiken in Hinsicht auf Eintrittswahrscheinlichkeit und Schadenshöhe sowie der Missachtung des Faktors Zeit kann ein ROSI nur als Näherungs- oder Richtwert angesehen werden. Bei gleich bleibender Berechnungsweise ist aber die Möglichkeit des Vergleichs gegeben. (vgl. [Schadt 2006], S. 21)

Die erste Berechnungsmöglichkeit ist definiert als Differenz aus den Kosten, die zur Behebung des angefallenen Schadens nötig sind (Recovery Costs – R), sowie der jährlichen Verlusterwartung (Annual Loss Expenditure – ALE). Die ALE ist definiert als die Summe der wahrscheinlichen Schäden und Investition (Tool Costs – T) minus der Ersparnis (Savings – S). (vgl. [Schadt 2006], S. 21)

Formel 1: ALE = R-S+T
R-ALE = S-T = ROSI

Die **Recovery Costs – R** (Kosten der wahrscheinlichen Schäden) beschreiben alle Aufwendungen zur Behebung eines Schadens und der Rückkehr zum Ursprungszustand. „Sie werden in die Gesamtkosten der geschäftlichen Tätigkeit mit einbezogen. Die Wiederherstellungskosten hängen vom tatsächlichen Eintritt von Schäden ab, müssen aber aus Erfahrungswerten für die Zukunft abgeschätzt werden." ([Pohlmann 2006], S. 29) Hierbei sind auch aktuelle Entwicklungen auf gesetzlicher Ebene wie Basel II und der Sarbanes Oxley Act zu berücksichtigen. Diese verursachen Kosten bei Nichteinhaltung, die in eine Kostenbetrachtung einbezogen werden müssen. (vgl. [Pohlmann 2006], S. 29)

**Savings – S** (Reduzierung der Kosten der wahrscheinlichen Schäden) umfasst alle Kosten, die durch die Einführung der neuen IT-Sicherheitsmaßnahme eingespart werden können. Es wird davon ausgegangen, dass die IT-Sicherheitsmaßnahme eine sehr hohe Anzahl von Angriffen abwehren kann. (vgl. [Pohlmann 2006], S. 29f.) Eine Reduzierung des Prämienaufwands für die IT-Versicherung bei Einsatz von IT-Sicherheitsmaßnahmen ist ein Beispiel für indirekte Ersparnisse.

Die **Tool Costs – T** (Kosten für IT-Sicherheitsmaßnahmen) beinhalten alle mit der neuen Investition verbunden Kosten. In der Regel werden die Total Cost of Ownership berechnet. (vgl. [Pohlmann 2006], S. 30) Dabei sind direkte und indirekte Kosten möglichst genau zu quantifizieren, was die Berechnung, wie oben genannt, problematisch und umstritten macht.

Die **Annual Loss Expenditure – ALE** (verbleibende jährlich erwartete Kosten) sind die Kosten, die verbleiben, nachdem die IT-Sicherheitmaßnahme installiert worden ist. (vgl. [Pohlmann 2006], S. 30)

Der **Return On Security Investment – ROSI** (gesparte Kosten, erzielter Profit) sind „die Einsparungen der Recovery Costs (Schäden), die durch das Investment in IT-Sicherheitsmaßnahmen erzielt wurden." (vgl. [Pohlmann 2006], S. 30) Für einen positiven ROSI müssen die Tool Costs immer kleiner sein als die Einsparungen durch die Investition.

Die zweite Möglichkeit den ROSI zu berechnen, ist mehr an der ursprünglichen Berechnung des ROI angelehnt. Die erwartete Einsparung berechnet sich aus der jährlichen Gefährdung (Risk Exposure – RE) multipliziert mit der prozentualen

Wahrscheinlichkeit der Risikominderung (Risk Mitigated – RM). Die jährliche Verlusterwartung wird also nicht rein monetär berechnet. Es wird der Umstand berücksichtigt, dass bei einer Gefahrenbetrachtung wahrscheinlich nicht jedes Auftreten (Angriff) abgewehrt oder verhindert werden kann. Die jährliche Gefährdung errechnet sich aus den projizierten Kosten eines Schadensfalls (Single Loss Exposure – SLE) multipliziert mit seiner erwarteten jährlichen Eintrittshäufigkeit (Annual Rate of Occurence – ARO).

Anschließend subtrahiert man noch die Investitionskosten (Tool Costs – T) und dividiert nochmals durch diese. Somit erhält man eine Kennziffer, die als Schätzwert die prozentuale Rendite widerspiegelt.

Im Vergleich berücksichtig der zweite Ansatz in höherem Maße die Eintrittswahrscheinlichkeit.

Formel 2: ROSI= ((RE * %RM) – T) / T
RE = SLE * ARO

Da es keine standardisierten Methoden gibt, den SLE oder ARO zu berechnen, kann man nur auf Erfahrungswerte zurückgreifen oder in versicherungsmathematischen Tabellen nachschlagen, die auf echten Schadensfällen beruhen. Erstellt werden diese aufgrund von Versicherungsfällen, Forschungsdaten oder unabhängigen Studien. Allerdings ist es sehr schwierig, Daten von Schadensfällen zu gewinnen. Nur wenige Firmen verfolgen nach einem Angriff die insgesamt tatsächlich aufgetretenen Schäden. (vgl. [Sonnenreich 2006])

## 3. ROSI und PKI

Der ROSI wird meist mit der Bewertung einer Sicherheitsmaßnahme in Verbindung gebracht, die eventuelle Angriffe und somit Schäden vom Unternehmen abwehren soll. Hinsichtlich des Einsatzes einer PKI ist diese Betrachtung jedoch zu einseitig und erfasst nicht den angestrebten systematischen und geschlossenen Ansatz zur Informationssicherheit im Unternehmen. PKI erfordert, dass eine vollständige Security Policy etabliert und mit einer Infrastruktur umgesetzt wird. Diese Planung muss die Menschen, Prozesse und Technologien im Unternehmen berücksichtigen und festlegen, wie diese miteinander interagieren, um die Geschäftstätigkeit in einem sicheren und vertrauenswürdigen Umfeld zu ermöglichen. Diese Infrastruktur muss Dienste anbieten wie Vertraulichkeit und Integrität von Daten, Benutzerauthentifizierung, Belegbarkeit der Datenherkunft gegenüber Dritten und die Sicherstellung der Erreichbarkeit und Verfügbarkeit von Informationen. Ein weiterer Faktor ist die Freischaltung neuer Tätigkeitsfelder. Erst durch den Aufbau einer PKI werden Geschäftsprozesse möglich, die vorher zu risikobehaftet waren. (vgl. [Lareau 2002], S. 2)

## 4. Berechnung des ROSI am Beispiel von Single Sign On (SSO)

Ein typisches Beispiel für die transparente Darstellung des ROSI für eine IT-Sicherheitsinvestition in einer PKI-Umgebung stellt ein Single Sign On-System dar. Im Unternehmensumfeld werden häufig eine Vielzahl unterschiedlicher Systeme parallel betrieben. Die Nutzer dieser Systeme erhalten in der Regel unterschiedliche Anmeldekennungen, mit denen sie sich beim jeweiligen System authentisieren müssen. Die Nutzer müssen dementsprechend viele Passwörter und Benutzernamen verwalten. Im Falle von vergessenen Passwörtern benötigen sie schnelle Unterstützung, damit ihre Produktivität gewährleistet ist. Hierfür dient in der Regel ein Help-Desk System, welches die Störungen schnellstmöglich bearbeitet.

Bei einem SSO wird diese Problematik entschärft. Der Nutzer benötigt nur noch eine Anmeldekennung und muss sich nur gegenüber dem SSO z.B. durch Passwort oder Chipkarte ausweisen. Die Anmeldedaten für die anderen Systeme sind hinterlegt und das SSO übernimmt die Anmeldung an diese Systeme automatisch mittels Benutzerzertifikaten. An den Beispielen soll die Einführung und das erwartete Einsparpotential durch die Nutzung eines SSO stellvertretend für ein Mittelstands- und ein Großunternehmen verdeutlicht werden. Die verwendeten Daten orientieren sich an [Gadatsch 2006], S. 46 und wurden angepaßt.

**Beschreibung der Faktoren:**
Bei dem Beispielprojekt handelt es sich um eine Investition in ein Sicherheitsprojekt, bei dem ein Prozess mit sicherheitstechnischem Hintergrund optimiert werden soll. Vorweg soll beschrieben werden, wie man die benötigten Daten zum Vergleich des Nutzens der Investition ermitteln kann. Im Beispiel entsteht der Schaden durch den Produktivitätsverlust der Mitarbeiter, während sie auf das Rücksetzen eines Passworts oder eine erneute Vergabe warten. Die Zeit und Häufigkeit kann mit einem quantifizierenden Fragebogen ermittelt werden. Bei der Ausarbeitung des Fragebogens muss darauf geachtet werden, dass keine offenen Fragen gestellt werden. Stattdessen sollten Wahlmöglichkeiten vorgegeben werden, die eine gleich bleibende Auswertung ermöglichen, z.B. Wie häufig vergessen sie ein Passwort? x mal pro Tag, x mal pro Woche, x mal pro Monat.

Die Zeit, die durchschnittlich zur Bearbeitung einer Passwortanfrage am Help Desk benötigt wird, lässt sich durch eine gleichwertige Evaluierung ermitteln. Zusammen mit dem durchschnittlichen internen Stundensatz der Mitarbeiter lässt sich somit die jährliche Verlusterwartung (Recovery Costs, Risk Exposure) berechnen.

Zur Ermittlung der Investitionskosten (Tools Costs) hat sich der TCO-Ansatz der Gartner Group bewährt. Dieser Ansatz berücksichtigt alle direkten und indirekten Kosten, die zur Beschaffung, Nutzbarmachung und zur Sicherstellung des Betriebs nötig sind. Die direkten Kosten setzen sich zusammen aus der Untersuchung potentieller Produkte (auch die Kosten für Berichte, Tests und Berater), dem Design der Abhängigkeiten und benötigten Komponenten, der Beschaffung (Ausschreibungen, Anbie-

terauswahl und Marktforschung), dem Kauf (Hardware, Software, Steuern, Zölle, Änderungen an bestehenden Systemen z.B. Upgrades), der Lieferung-/ des Transports, der Installation (Umgebungsanpassung, Downtime anderer Systeme, Endnutzerproduktivität während der Installation), der Entwicklung/Anpassung, der Schulungen und dem Ausfahren in den Betrieb (Anpassung der Prozesse, vollständige Integration in die Systemlandschaft, Bekanntmachung unter den Mitarbeitern).

Indirekte Kosten zur Wahrung der Erreichbarkeit des Systems beinhalten Operationsmanagement (alle Aufgaben des normalen Betriebs, Hoch- und Runterfahren, Auftragssteuerung, Ausgabesteuerung, Backup, Wiederherstellung), Systemmanagement (Problembearbeitung, Veränderungsmanagement, Performancekontrolle), Instandhaltung der Hardware-/ Softwarekomponenten (Updates, Fehlerbehebung, generelle Pflege), Lizenzkosten, Benutzersupport (Schulungen, Helpdesk-Einrichtung, jede Art von Service) und Umgebungsfaktoren (Klimaanlage, Stromversorgung, Unterbringung, Flächenbedarf).

Die erwarteten Einsparungen (Savings, Risk Mitigated) werden auf gleiche Weise gegengerechnet wie die jährliche Verlusterwartung. Diesmal natürlich, nachdem prognostiziert wurde, in welcher Höhe die Investition die Anfragen senken kann. Diese Angaben kann man von Erfahrungswerten anderer Unternehmen ableiten (falls man die Daten bekommt), Studien wissenschaftlicher Insitute entnehmen, im jährlichen Bericht des Computer Security Institut und des FBI nachlesen oder aus Schadensberichten von Versicherungen ableiten.

**Beispiel 1 – Mittelstand – 100 Mitarbeiter:**

| | |
|---|---|
| Passwortbezogene Anfragen pro Monat: | 100 |
| Produktivitätsverlust durch Anfrage: | 20 Minuten |
| Interner Stundensatz der Mitarbeiter: | 33 Euro[1] |
| Veranschlagte Reduzierung der Anfragen durch SSO: | 40% |

| Formel 1: | Formel 2: |
|---|---|
| **Recovery Costs:**<br>Schaden durch passwortbezogene Anfragen: 100 Anfragen * 11 Euro anteil. Stundensatz * 12 Monate = 13.200 Euro/Jahr | **Risk Exposure:**<br>Schaden durch passwortbezogene Anfragen: 100 Anfragen * 11 Euro anteil. Stundensatz * 12 Monate = 13.200 Euro/Jahr |
| **Tool Costs:**<br>Einmalige Anschaffungs- und Installationskosten des SSO: 10.000 Euro<br>Betriebskosten des SSO: 4.800 Euro/Jahr | **Tool Costs:**<br>Einmalige Anschaffungs- und Installationskosten des SSO: 10.000 Euro<br>Betriebskosten des SSO: 4.800 Euro/Jahr |

| **Savings:** | **Tool Costs:** |
|---|---|
| Verringerte Anzahl von Anfragen: 40 Anfragen * 11 Euro anteil. Stundensatz * 12 Monate = 5.280 Euro/Jahr | 40% |

**Nach Formel 1:**

| | 1. Jahr | 2. Jahr | 3. Jahr | 4. Jahr | 5. Jahr |
|---|---|---|---|---|---|
| Recovery Costs | 13.200 | 13.200 | 13.200 | 13.200 | 13.200 |
| Savings | 5.280 | 5.280 | 5.280 | 5.280 | 5.280 |
| Tool Costs (Installation) | 10.000 | | | | |
| Tool Costs (Betrieb) | 4.800 | 4.800 | 4.800 | 4.800 | 4.800 |
| Annual Loss Expenditure | 22.720 | 12.720 | 12.720 | 12.720 | 12.720 |
| Recovery Costs | 13.200 | 13.200 | 13.200 | 13.200 | 13.200 |
| Annual Loss Expenditure | 22.720 | 12.720 | 12.720 | 12.720 | 12.720 |
| **ROSI** | **–9.520** | **–9.040** | **–8.560** | **–8.080** | **–7.600** |

**Nach Formel 2:**

| | 1. Jahr | 2. Jahr | 3. Jahr | 4. Jahr | 5. Jahr |
|---|---|---|---|---|---|
| Single Loss Exposure | 11 | 11 | 11 | 11 | 11 |
| Annual Rate of Occurence | 1.200 | 1.200 | 1.200 | 1.200 | 1.200 |
| Risk Mitigated | 40% | 40% | 40% | 40% | 40% |
| Tool Costs | 14.800 | 4.800 | 4.800 | 4.800 | 4.800 |
| **ROSI** | **–64,32%** | **–54,32%** | **–44,32%** | **–34,32%** | **–24,32%** |

**Beispiel 2 – Großunternehmen – 1.000 Mitarbeiter:**

| | |
|---|---|
| Passwortbezogene Anfragen pro Monat: | 1.000 |
| Produktivitätsverlust durch Anfrage: | 20 Minuten |
| Interner Stundensatz der Mitarbeiter: | 60 Euro |
| Veranschlagte Reduzierung der Anfragen durch SSO: | 40% |

[1] In [Gadatsch 2006] wird ein interner Stundensatz von 60 Euro angenommen. Für ein mittelständisches Unternehmen scheint uns der Wert zu hoch angesetzt. Ein interner Stundensatz zwischen 30 und 35 Euro dürfte realistischer sein.

| Formel 1: | Formel 2: |
|---|---|
| **Recovery Costs:**<br>Schaden durch passwortbezogene Anfragen: 1000 Anfragen * 20 Euro anteil. Stundensatz * 12 Monate = 240.000 Euro/Jahr | **Risk Exposure:**<br>Schaden durch passwortbezogene Anfragen: 1000 Anfragen * 20 Euro anteil. Stundensatz * 12 Monate = 240.000 Euro/Jahr |
| **Tool Costs:**<br>Einmalige Anschaffungs- und Installationskosten des SSO: 60.000 Euro<br>Betriebskosten des SSO: 14.400 Euro/Jahr | **Tool Costs:**<br>Einmalige Anschaffungs- und Installationskosten des SSO: 60.000 Euro<br>Betriebskosten des SSO: 14.400 Euro/Jahr |
| **Savings:**<br>Verringerte Anzahl von Anfragen: 400 Anfragen * 20 Euro anteil. Stundensatz * 12 Monate = 96000 Euro/Jahr | **Tool Costs:**<br>40% |

**Nach Formel 1:**

| | 1. Jahr | 2. Jahr | 3. Jahr | 4. Jahr | 5. Jahr |
|---|---|---|---|---|---|
| Recovery Costs | 240.000 | 240.000 | 240.000 | 240.000 | 240.000 |
| Savings | 96.000 | 96.000 | 96.000 | 96.000 | 96.000 |
| Tool Costs (Installation) | 60.000 | | | | |
| Tool Costs (Betrieb) | 14.400 | 14.400 | 14.400 | 14.400 | 14.400 |
| Annual Loss Expenditure | 218.400 | 158.400 | 158.400 | 158.400 | 158.400 |
| Recovery Costs | 240.000 | 240.000 | 240.000 | 240.000 | 240.000 |
| Annual Loss Expenditure | 218.400 | 158.400 | 158.400 | 158.400 | 158.400 |
| **ROSI** | **21.600** | **103.200** | **184.800** | **266.400** | **348.000** |

**Nach Formel 2:**

| | 1. Jahr | 2. Jahr | 3. Jahr | 4. Jahr | 5. Jahr |
|---|---|---|---|---|---|
| Single Loss Exposure | 20 | 20 | 20 | 20 | 20 |
| Annual Rate of Occurence | 12.000 | 12.000 | 12.000 | 12.000 | 12.000 |
| Risk Mitigated | 40% | 40% | 40% | 40% | 40% |
| Tool Costs | 74.400 | 14.400 | 14.400 | 14.400 | 14.400 |
| **ROSI** | **29,03%** | **595,70%** | **1.162,37%** | **1.729,03%** | **2.295,70%** |

In den Beispielen ist die Berechnung des ROSI sehr einfach gehalten. Bei differenzierter Betrachtung fallen einige Faktoren auf, die nicht in die Berechnung einbezogen wurden. Zum Beispiel ist die Reduzierung der Nutzeranfragen kein statischer Wert. Erfahrungen zeigen, dass bei steigender Akzeptanz und Erfahrung mit SSO-Systemen noch höhere Einsparquoten erreicht werden. Weiterhin wird die Häufigkeit der Anmeldungen mit und ohne SSO nicht berücksichtigt, ebenso wie die freigewordenen Kapazitäten beim Help-Desk. Ein Beispiel für einen sehr schwer zu messenden Faktor ist der Einfluss der verringerten Anmeldungen auf die Produktivität der Mitarbeiter. Es wird z.B. das erneute Eindenken in eine Aufgabe vermieden.

Das Problem äußert sich also bei der Bestimmung der relevanten Faktoren zur Messung des ROSI. Es gibt kein standardisiertes Modell, welches festlegt, wie hoch man das finanzielle Risiko einer Schwachstelle oder die Effektivität von Schutzmaßnahmen bewertet.

### 4.1 ROSI-Berechnung am Beispiel des elektronischen Dokumentenversands

Im Laufe der täglichen Geschäftstätigkeit enstehen in einem Unternehmen eine Vielzahl von Dokumenten, die der Kommunikation nach Außen dienen, z.B. mit Partnern oder Kunden. Auch heutzutage wird noch in vielen Bereichen mit Post auf herkömmlichen Wegen operiert. Häufig werden diese Dokumente jedoch von den Empfängern digitalisiert, um sie elektronisch verarbeiten oder archivieren zu können. Um diese Medienbrüche und den zusätzlichen Arbeitsaufwand zu verringern und somit Kosten einzusparen, lassen sich mit Hilfe von PKI Dokumente auch vollständig auf dem elektronischen Weg erstellen und versenden. Entscheidend ist dabei, dass die Authentizität der Dokumente ebenso gesichert ist, wie z.B. bei einer handschriftlich unterzeichneten Korrespondenz.

Die Möglichkeiten, den Prozess auf elektronischem Wege ablaufen zu lassen, bedingen entweder den Aufbau einer eigenen PKI oder die Beantragung der Zertifikate bei einem Trust-Center. Da die Schaffung einer eigenen Infrastruktur in der Regel nur für große Unternehmen mit mehr als 1000 Mitarbeitern in Betracht kommt, beschränkt sich das Beispiel auf die Erstellung der Zertifikate durch einen externen Anbieter. Die Daten des Beispiels stammen aus [Beilschmidt 2007].

Zur Berechnung eines ROSI wird die Erweiterung des Prozesses des Dokumentenversands auf die elektronische Variante betrachtet, d.h. die Dokumente werden elektronisch erzeugt, über ein Zertifikat signiert, um die Identität des Absenders zu gewährleisten und anschließend elektronisch versendet. Weiterhin müssen die dazu nötigen Investitionen zur Schaffung einer eventuell nicht vorhandenen Hardwaregrundlage und der Beantragung der Zertifikate betrachtet werden. Die Kosten, die zum Aufbau einer solchen Infrastruktur nötig sind, werden den Kosten des Ver-

sands auf herkömmlichem Wege über die Poststelle gegenübergestellt. Dabei soll sich nach dem Pareto Ansatz auf die Kostentreiber beschränkt werden, die den größten Einfluss auf die Kostenentwicklung haben und möglichst branchenübergreifend zutreffen.

### 4.2 Kostenbetrachtung

Zur Berechnung des ROSI sind als Erstes die Kosten der herkömmlichen Variante zu betrachten, die durch die Umstellung auf den elektronischen Versand eingespart werden können. Das Problem zur Bestimmung konkreter Zahlen zeigt sich hier in der Bestimmung der Kosten eines zu versendeten Dokuments. Aufwendungen für Papier, Tonerverbrauch und der Arbeitseinsatz der Poststelle für Verpackung, Frankierung und Versand werden in jedem Unternehmen anders eingeschätzt. Hier zeigt sich der Charakter des ROSI als Näherungswert zur Abschätzung der Wirtschaftlichkeit einer Investition.

**Im Beispiel wird von folgenden Kosten ausgegangen:**

- → 2,00 Euro Aufwendungen für Papier, Toner usw. je Dokument, von denen 1,40 Euro durch den elektronischen Versand eingespart werden können
- → 0,55 Euro Portokosten je verschicktem Dokument
- → 19,75 Euro Zertifikatskosten pro Mitarbeiter im Jahr für eine qualifizierte Signatur
- → Kosten für eine Hardwarelösung, die ausgehende Dokumente automatisch signiert. Die Kosten unterscheiden sich je nach Unternehmensgröße und beinhalten Anschaffung, Betrieb, Administration und Wartung.
- → Kosten für die Poststelle, vor und nach der Installation, da die Stelle in der Regel in kleinerer Form erhalten bleibt

Die Beispielunternehmen haben eine Größe von 100 und 3.000 Mitarbeitern, da hierfür konkrete Angaben zu Lizenzkosten für das zentrale Gateway vorlagen.

**Beispiel 1 – Mittelstand – 100 Mitarbeiter:**

| **Unternehmen A** | |
|---|---|
| Mitarbeiteranzahl | 100 |
| Dokumentenaufkommen/Monat | 130 |
| Kosten/Dokument | 2,00 Euro |
| Zertifikatskosten/Mitarbeiter | 19,75 Euro |

| **Papierbasierter Dokumentenversand** | |
|---|---|
| **Einmalige Kosten** | |
| keine | |
| **Monatliche Kosten** | |
| Dokumentenkosten | 260,00 Euro |
| Porto (0,55 Euro / Dokument) | 71,50 Euro |
| Poststelle (1–2 Mitarbeiter) | 1.000,00 Euro |
| **Summe/Monat** | **1.331,50 Euro** |

| **Elektronischer Dokumentenversand** | |
|---|---|
| **Einmalige Kosten** | |
| Zentrales Gateway | 6.000 Euro |
| **Monatliche Kosten** | |
| Dokumentenkosten (0,60 Euro/Dokument) | 78,00 Euro |
| Zertifikate | 164,58 Euro |
| Poststelle | 500,00 Euro |
| Wartungskosten Gateway | 90,00 Euro |
| **Summe/Monat** | **832,58 Euro** |

**ROSI nach Formel 1**

| Monat | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Investitionskosten | 6.000,00 | | | | | |
| Betriebskosten PKI | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 |
| Einsparungen | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 |
| **ROSI** | **–5.501,08** | **–5.002,16** | **–4.503,24** | **–4.004,32** | **–3.505,40** | **–3.006,48** |

| Monat | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|
| Investitionskosten | | | | | | |
| Betriebskosten PKI | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 |
| Einsparungen | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 |
| **ROSI** | **–2.507,56** | **–2.008,64** | **–1.509,72** | **–1.010,80** | **–511,88** | **–12,96** |

**ROSI nach Formel 2**

| Monat | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Investitionskosten | 6.000,00 | | | | | |
| Betriebskosten PKI | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 |
| Kosten kumuliert | 6.832,58 | 7.665,16 | 8.497,74 | 9.330,32 | 10.162,90 | 10.995,48 |
| Schaden | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 |
| Schaden gesamt | 1.331,50 | 2.663,00 | 3.994,50 | 5.326,00 | 6.657,50 | 7.989,00 |
| **ROSI** | **–80,51%** | **–65,26%** | **–52,99%** | **–42,92%** | **–34,49%** | **–27,34%** |

| Monat | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|
| Investitionskosten | | | | | | |
| Betriebskosten PKI | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 | 832,58 |
| Kosten kumuliert | 11.828,06 | 12.660,64 | 13.493,22 | 14.325,80 | 15.158,38 | 15.990,96 |
| Schaden | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 | 1.331,50 |
| Schaden gesamt | 9.320,50 | 10.652,00 | 11.983,50 | 13.315,00 | 14.646,50 | 15.978,00 |
| **ROSI** | **–21,20%** | **–15,87%** | **–11,19%** | **–7,06%** | **–3,38%** | **–0,08%** |

**Beispiel 2 – Großunternehmen – 3.000 Mitarbeiter:**

| Unternehmen B | |
|---|---|
| Mitarbeiteranzahl | 3.000 |
| Dokumentenaufkommen/Monat | 2.800 |
| Kosten/Dokument | 2,00 Euro |
| Zertifikatskosten/Mitarbeiter | 19,75 Euro |

| Papierbasierter Dokumentenversand | |
|---|---|
| **Einmalige Kosten** | |
| keine | |
| **Monatliche Kosten** | |
| Dokumentenkosten | 5.600,00 Euro |
| Porto (0,55 Euro/Dokument) | 1.540,00 Euro |
| Poststelle (1–2 Mitarbeiter) | 3.000,00 Euro |
| **Summe/Monat** | **10.140,00 Euro** |

| Elektronischer Dokumentenversand | |
|---|---|
| **Einmalige Kosten** | |
| Zentrales Gateway | 25.000 Euro |
| **Monatliche Kosten** | |
| Dokumentenkosten (0,60 Euro/Dokument) | 1.680,00 Euro |
| Zertifikate | 4.937,50 Euro |
| Poststelle | 1.000,00 Euro |
| Wartungskosten Gateway | 375,00 Euro |
| **Summe/Monat** | **7.992,50 Euro** |

**ROSI nach Formel 1**

| Monat | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Investitionskosten | 25.000,00 | | | | | |
| Betriebskosten PKI | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 |
| Einsparungen | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 |
| **ROSI** | **–22.852,50** | **–20.705,00** | **–18.557,50** | **–16.410,00** | **–14.262,50** | **–12.115,00** |

| Monat | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|
| Investitionskosten | | | | | | |
| Betriebskosten PKI | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 |
| Einsparungen | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 |
| **ROSI** | **–9.967,50** | **–7.820,00** | **–5.672,50** | **–3.525,00** | **–1.377,50** | **770,00** |

**ROSI nach Formel 2**

| Monat | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| Investitionskosten | 25.000,00 | | | | | |
| Betriebskosten PKI | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 |
| Kosten kumuliert | 32.992,50 | 40.985,00 | 48.977,50 | 56.970,00 | 64.962,50 | 72.955,00 |
| Schaden | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 |
| Schaden gesamt | 10.140,00 | 20.280,00 | 30.420,00 | 40.560,00 | 50.700,00 | 60.840,00 |
| **ROSI** | **–69,27%** | **–50,52%** | **–37,89%** | **–28,80%** | **–21,95%** | **–16,61%** |

| Monat | 7 | 8 | 9 | 10 | 11 | 12 |
|---|---|---|---|---|---|---|
| Investitionskosten | | | | | | |
| Betriebskosten PKI | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 | 7.992,50 |
| Kosten kumuliert | 80.947,50 | 88.940,00 | 96.932,50 | 104.925,00 | 112.917,50 | 120.910,00 |
| Schaden | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 | 10.140,00 |
| Schaden gesamt | 70.980,00 | 81.120,00 | 91.260,00 | 101.400,00 | 111.540,00 | 121.680,00 |
| **ROSI** | **–12,31%** | **–8,79%** | **–5,85%** | **–3,36%** | **–1,22%** | **0,64%** |

Die Berechnung zeigt, dass durch die Kenntnis der grundlegenden Kostentreibern, d.h. der Faktoren, die den größten Anteil an den Gesamtkosten haben, schon eine vergleichende ROSI-Berechnung möglich ist. Im Beispiel wurden qualifizierte Zertifikate als Berechnungsgrundlage gewählt. Ebenso wurde für jeden Mitarbeiter ein Zertifikat beantragt. In diesem Beispiel ließen sich Kosten u.a. durch eine Bestimmung der Mitarbeiter sparen, die unbedingt teure qualifizierte Zertifikate benöti-

gen. Für die restlichen Mitarbeiter reichen möglicherweise fortgeschrittene Zertifikate, vielleicht kann aber auch auf qualifizierte Zertifikate grundsätzlich verzichtet werden. Weiterhin kann man Softwarelösungen evaluieren, mit denen sich die Anschaffungs- und Betriebskosten des Gateway verringern oder einsparen lassen. Das würde jedoch von den dann erhöhten Administrationskosten und dem zusätzlichen Schulungsaufwand für die Mitarbeiter zumindest in Teilen kompensiert. Was in den Beispielen ebenso nicht einkalkuliert wurde, ist der verringerte Arbeitsaufwand der Mitarbeiter, z.B. durch das sonst notwendige Ausdrucken und zur Poststelle bringen. Die Untersuchung solcher Prozesse würde jedoch zu unternehmensspezifisch werden sowie der schnellen und einfachen ROSI-Berechnung entgegensprechen. Die Konzentration auf wesentliche Faktoren zum schnellen aber dennoch aussagekräftigen Vergleich von Alternativen steht bei der ROSI-Ermittlung im Vordergrund.

## 5. Die Quantifizierung von Risiken

Es stellt sich noch die Frage, inwieweit es sinnvoll ist, Risiken auf Grundlage von unvollständigen Daten abzuschätzen. Die Anwort ist: Ja! Wenn die Methoden zur Bestimmung des ROSI reproduzierbare und einheitliche Ergebnisse liefern, kann der ROSI als hilfreiches Mittel zum Vergleich von Sicherheitslösungen auf einer relativen Basis dienen.

Da für diesen Zweck die Genauigkeit der zugrunde liegenden Kosten eine untergeordnete Rolle spielt, gilt es, die Methodik der Kostenberechnung und –beschreibung konsistent zu gestalten. In die Ermittlung der Faktoren zur Bemessung des wirtschaftlichen Nutzens der Investition wird häufig die Produktivität höher bewertet als der eigentliche Sicherheitsaspekt. Unternehmen müssen also nach Einflussgrößen Ausschau halten, die eine Produktivitätssteigerung oder neue Prozesse ermöglichen. Bei der Ermittlung sind es in der Regel auch keine Detailfragen die den Gesamtnutzen entscheidend beeinflussen. Nach dem Pareto-Ansatz gilt es, die treibenden 20% Faktoren zu ermitteln, die 80% des wirtschaftlichen Nutzens ausmachen. Da sich Unternehmen, besonders aus unterschiedlichen Branchen, jedoch schwerlich auf einen Standard festlegen würden, muss die Berechnung auf Faktoren beruhen, die unabhängig messbar sind und direkt mit dem Schweregrad z.B. eines Sicherheitsvorfalls korrelieren. Auch ermöglicht die Konzentration auf wenige entscheidende Größen eine leichtere Vergleichbarkeit über Produkte, Projekte, Unternehmen und ganze Branchen hinweg. (vgl. [Sonnenreich 2006])

### 5.1 Problematik bei der Anwendung des ROSI

Die Problematik bei der Berechung des ROSI hängt mit der Abschätzung des direkten und indirekten Schadens zusammen, der durch einen Mangel an Sicherheit eintritt. Hierdurch wird die Berechnung eines aussagekräftigen Wertes zu einem sehr

komplexen Vorgang. Ebenso muss die Abschätzung des Erfolgs der Sicherheitsmaßnahme gegenübergestellt werden. Die Zusammenhänge zwischen einem konkreten Angriff und einem speziellen Schaden sind schwer herzustellen. Ebenso zwischen einem Angriff und der unmittelbaren Wirkung der Sicherheitsmaßnahme. Insbesondere wenn weitere Sicherheitsmaßnahmen getroffen wurden, kann der Erfolg nur schwer anteilig aufgegliedert werden. Bei mehreren Angriffen stellt die verursachergerechte Abrechnung das gleiche Problem dar. Ebenso basieren die Rechnungen auf groben Schätzungen. Die Varianz der Ergebnisse kann dementsprechend hoch sein. Wird z.B. eine ALE berechnet, dann wird davon ausgegangen, dass bei mehrmaligem Eintreten eines Angriffes potentiell immer der gleiche Schaden zu erwarten ist. In der Praxis jedoch unterscheiden sich die Angriffziele und -methoden und möglicherweise verursacht nur ein erfolgreicher Angriff den gleichen Schaden, wie für alle potentiellen Gefahren des ganzen Jahres veranschlagt wurden.

## 6. Schlussfolgerungen

Der Return on Security Investment ist im Allgemeinen sehr schwer zu messen und auszuweisen. Die Grundlage auf ungenauen Messwerten und schwierig zu beziffernden Eintrittswahrscheinlichkeiten hinterlässt den Eindruck eines bloßen Näherungswertes der mitunter bezweifelt wird.

Den Mehrwert von Sicherheitsinvestitionen mit dem ROSI zu beurteilen, beruht auf der Annahme, dass eine Investitionen im Laufe der Jahre positiven Nutzen generiert. In einfachen Szenarien werden dazu Anschaffungs-, Implementierungs- und Betriebskosten eines Sicherheitssystems mit den möglichen Schäden verglichen, die der Missbrauch einer Sicherheitslücke ohne Sicherheitssystem verursachen könnte. Um die Vergleichbarkeit von Sicherheitsinvestitionen zu gewährleisten, ist jedoch die Methode zur Ermittlung des ROSI entscheidend. Nach dem Pareto-Prinzip ist nur eine geringe Anzahl von Faktoren zur Kostenbeurteilung entscheidend. Diese müssen allerdings mit reproduzierbaren und konsistenten Verfahren ermittelt werden, auch wenn sie inakkurat sind. Zur Ermittlung der grundlegenden Kosten einer Investition eignet sich beispielsweise der TCO-Ansatz. Will man den Produktivitätsverlust eines Mitarbeiters bewerten, eignen sich Umfragen, die den direkten Zusammenhang zwischen Ausfall und der Einschränkung des Mitarbeiters widerspiegeln. Stellt man sicher, dass die Fragen schnell bewertbar (z.B. Skalen), eindeutig und leicht zu beantworten sind, kann man einen starken Zusammenhang zwischen den Umfragewerten und den finanziellen Auswirkungen herstellen. (vgl. [Sonnenreich 2006])

Diese statische Berechnung lässt allerdings den Faktor Zeit außer Acht. Ansätze, welche die Diskontierung des Kapitals berücksichtigen, sind z.B. die Kapitalwertmethode (Net Present Value) oder der interne Zinsfuß (Internal Rate of Return).

## 7. Quellen


[Beilschmidt 2007] Beilschmidt, A.: Geschäftsmodelle für die European Bridge-CA; 2007.

[Berinato 2002] Berinato, S.: Finally, a Return on Security Spending. In: CIO Australia; 08.04.2002.
Onine: http://www.cio.com.au/index.php?id=557330171

[Gadatsch 2006] Gadatsch, A.; Uebelacker, H.: Wirtschaftlichkeitsbetrachtungen für IT-Security-Projekte. In: [Mörike 2006]; S. 44–50.

[Lareau 2002] Lareau, P.: PKI Basics – A Business Perspective; PKI Forum Business Working Group; April 2002.

[Lubich 2006] Lubich, H. P.: IT-Sicherheit: Systematik, aktuelle Probleme und Kosten-Nutzen-Betrachtungen. In: [Mörike 2006]; S. 6–15.

[Mörike 2006] Möricke, M.; Teufel, S. (Hrsg.): Kosten & Nutzen von IT-Sicherheit; HMD – Praxis der Wirtschaftsinformatik; Heft 248 April 2006.

[Müßig 2006] Müßig, S.: Haben Sicherheitsinvestitionen eine Rendite? In: [Mörike 2006]; S. 35–43.

[Pohlmann 2006] Pohlmann, N.: Wie wirtschaftlich sind IT-Sicherheitsmaßnahmen? In: [Mörike 2006], S. 26–34.

[Schadt 2006] Schadt, D.: Über die Ökonomie der IT-Sicherheit – Betrachtungen zum Thema „Return on Security Investment“. In: [Mörike 2006], S. 16–25.

[Schmeh 2004] Schmeh, K.; Uebelacker, H.: Sicherheit, die sich rechnet. In: Telepolis; 06.12.2004.
Online: http://www.heise.de/tp/r4/artikel/18/18954/1.html

[Sonnenreich 2006] Sonnenreich, W.: Return On Security Investment (ROSI): A Practical Quantitative Model. In: Journal of Research and Practice in Information Technology; Vol. 38; No. 1; February 2006.

# Anhang E: Fragebogen Technische Perspektiven

| Fragebogen zur Erfassung von Kriterien für die Nutzung von PKI | |
|---|---|
| **Name:** | |
| **Unternehmen:** | |

**Geben Sie bitte eine kurze Beschreibung des/der von Ihnen betreuten PKI-Projektes/Projekte. Welche Ziele verfolgte das Projekt?**

**Wann und wie lang waren die Zeiträume für die Planung und die Umsetzung?**

## 1. Fragen zur PKI Planungsphase

**1.1 Welches waren seitens der Entscheider die ausschlaggebenden Faktoren für den Einsatz von PKI?**

**1.2 Welche Faktoren sprachen gegen die Nutzung von PKI?**

**1.3 Welche alternativen Konzepte waren im Gespräch?**

**1.4 Welche Anwendungen bzw. Prozesse sollten durch die PKI Unterstützung finden?**

**1.4a Wie wurde die Einbindung dieser Anwendungen bzw. Prozesse umgesetzt?**

**1.5 Die Nutzung von PKI hat meist auch Folgen für die Benutzer. Wurden diese Veränderungen in der Planungsphase erfasst? Wenn ja, was wurde vorgesehen, um diesen zu begegnen?**

**1.6 Waren rechtliche Überlegungen und Richtlinien in der Planungsphase von Bedeutung? Wenn ja, welche?**

**1.6a Wie wurden Haftungsfragen behandelt?**

**1.7 Wurden in der Planungsphase bereits Szenarien für eine Kooperation mit anderen Organisationen erwogen? Wenn ja, welche?**

## 2. Fragen zur Umsetzung

**2.1 Wurde für die Umsetzung auf eine Eigenimplementierung gesetzt oder eine fertige Lösung eingekauft?**

**2.2 Anhand welcher Kriterien wurde die Entscheidung getroffen eine eigene PKI oder eine Dienstleistung einzukaufen?**

| 2.3 Welche nicht vorhersehbaren Hindernisse/Herausforderungen haben sich bei der Umsetzung ergeben? Konnte diese gelöst werden? Wenn ja, wie? |
| --- |
| |
| **2.3 Wurde der gesetzte Zeitplan für die Umsetzung eingehalten? Wenn nein, warum nicht?** |
| |
| **3. Fragen zum Betrieb** |
| **3.1 Muss die PKI-Lösung fortlaufenden technischen Herausforderungen und Änderungsanforderungen standhalten? Wenn ja, wie wird dies realisiert?** |
| |

| 3.2 Planen Sie Dienste anderer Organisationen in Ihren Anwendungen einzubinden? Z.B. sichere E-Mail, Webservices, gemeinsame Einkaufsplattformen, etc. Wenn ja, welche? Sind diese PKI-gestützt? |
| --- |
| |
| 3.3 Haben sich nicht vorhersehbaren Hindernisse/Herausforderungen beim Betrieb ergeben? Wenn ja, welche? |
| |
| 3.3a Konnten diese gelöst werden? Wenn ja, wie? |
| |

**3.4 Welche Dokumentation sind für Ihre PKI relevant (CP, CPS, etc.) und welchen Stellenwert nehmen diese beim Betrieb ein?**

## 4. Fragen zur organisationsübergreifenden Kommunikation

**4.1 Wird die PKI organisationsübergreifend verwendet? Wenn ja, wie sieht diese Verwendung aus? Was wird als organisationsübergreifend verstanden? (Abteilungen, Mutterkonzerne, Kooperationen usw.)**

**4.2 Welche Rahmenbedingungen sind für Sie bei Beziehungen zwischen Unternehmen wichtig? (z.B. : Verträge, ISO-900x, ....)**

**4.3 Welche organisatorischen Abläufe sind bei organisationsübergreifenden Geschäftsprozessen notwendig, um bilaterale Vertrauensbeziehungen zu schaffen?**

**4.4 Wie wurde die organisationsübergreifende Kommunikation technisch realisiert? Wie sind die PKIs miteinander verbunden? (Root, Bridge, Cross)**

**4.4a Welche Erfahrungen haben Sie mit dieser technischen Realisierung gemacht?**

## 5. Allgemeine Fragen

**5.1 Welche Hürden sind bei Ihren PKI Anwendungen kennzeichnend?**

**5.1a Wie haben Sie es geschafft diesen Hürden zu begegnen?**

**5.1b Welche dieser Hürden sind auch mit Ihrem heutigen Wissen sehr schlecht einzuplanen?**

**5.2 Welche Hürden sind bei Ihren PKI Konzepten kennzeichnend?**

**5.2a Wie haben Sie es geschafft diesen Hürden der PKI Konzepte zu begegnen?**

**5.2b Welche dieser Hürden sind auch mit Ihrem heutigen Wissen sehr schlecht einzuplanen?**

**5.3 Welche noch offenen Probleme sehen Sie bei der Nutzung von PKI?**

**5.4 Wurden Ihre eigenen PKI Erfahrungen gesammelt und ausgewertet? Sind diese Informationen (anonymisiert) verwertbar?**

**5.5 Gibt es Literatur, Erfahrungsberichte oder andere Dokumente, welche Sie in diesem Umfeld als besonders hilfreich erachtet haben? Wenn ja, wo können wir diese finden?**

**Bemerkungen:**

# Anhang F

# Details zum Workshop

Der Veranstaltung „Workshop mit Kaminfachgespräch“, im Folgenden kurz „Workshop“ genannt, ist der vierte wesentliche Teil des Projekts „Erfolgskriterien für Signatur-, Identifizierungs- und Authentifizierungsverfahren auf Basis asymmetrischer kryptographischer Verfahren“. Auf Grundlage der Abschnitte, die sich mit den technischen Perspektiven, den wirtschaftlichen Betrachtungen und den Nutzungsbedingungen beschäftigen, soll der Workshop abschließend Erfolgskriterien identifizieren und Perspektiven aufzeigen. An diesen Zielen wurde sowohl die Organisation des Workshops als auch die Zusammensetzung der Teilnehmer ausgerichtet.

## 1. Teilnehmer

Die Teilnehmer wurden aus verschiedenen Kompetenzgruppen zusammengestellt: Hersteller und Dienstleister aus dem PKI-Markt, Chief Information Security Officers, die erfolgreiche multinationale PKI-Projekte umgesetzt haben, Wissenschaftler, Unternehmensberater mit Sicherheits- und Betrugsbekämpfungsexpertise, IT-Manager. Dabei wurde besonders auf eine langjährige Erfahrung der Teilnehmer wert gelegt. Neben der grundlegenden Bereitschaft aller, ihr Wissen für die Fragestellungen des Projekts zur Verfügung zu stellen, war die weitere Motivation zur Teilnahme sehr unterschiedlich. Einige sehen das Engagement in PKI als wichtigen Teil ihrer persönlichen Expertise, die sich durch die Teilnahme und die Diskussion mit den anderen Experten erweitern und ausbauen ließ, andere wollten zudem neue Kontakte in entspanntem Rahmen knüpfen. Demnach war es wichtig, einen

geeigneten Rahmen mit „Beiprogramm“ zu finden, der die angesprochenen Experten aus der Industrie zur Teilnahme motiviert. Zum einen war die vielfältige Zusammensetzung der Teilnehmer sicherlich ein motivierender Grund, zum anderen musste aufgrund der Seniorität der Experten ein gewisser gesellschaftlicher Mindeststandard geboten werden. Es ist im Gegenzug dazu ausdrücklich festzuhalten, dass kein Honorar gezahlt wurde, selbst Reisekosten wurden nur von den wenigsten dem Projektteam in Rechnung gestellt, was – nach der initialen Entscheidung zur Teilnahme – die außergewöhnliche Bereitschaft zur konstruktiven Mitarbeit der Teilnehmer belegt. Wichtig für den Erfolg erwies sich auch, neben der durch das Projektteam getragenen Expertendiskussion, im Rahmen des gemeinsamen Abendessens und dem anschließenden Kaminfachgespräch genug Raum und Zeit für bilaterale Gespräche vorzusehen, welche sich im Nachgang zum moderierten Teil der Veranstaltung auch und gerade für die Erkenntnisse des Projektteams als sehr gewinnbringend erwies. Folgende Teilnehmer konnten wir für die Mitarbeit an dem Workshop gewinnen:

| | | |
|---|---|---|
| **Dr. Anders Bally** | **Business Development Manager, VP** | **SECUDE** |
| **Prof. Hans-Ottomar Beckmann** | **Chief Information Security Officer** | **Volkswagen** |
| **Dr. Gunter Frank** | **Ex-Chief Information Officer** | **Dresdner Bank / DREGIS** |
| **Birgit Galley** | **Geschäftsführerin** | **Steinbeis-Institut Risk-and-Fraud** |
| **Dr. Saskia Günther** | **Security Officer, PKI Service-Owner** | **Allianz** |
| **Wolfgang Hawreluk** | **Geschäftsführer** | **Business Integrity Management** |
| **Dr. Franz-Peter Heider** | **Manager Security Consulting** | **T-Systems** |
| **Dr. Henning Herzog** | **Geschäftsführer** | **Steinbeis-Institut Risk-and-Fraud** |
| **Dr. Rüdiger Mock-Hecker** | **Geschäftsbereichsleiter Kartensysteme** | **Sparkassenverlag** |
| **Prof. Norbert Pohlmann** | **Vorstandsvorsitzender TeleTrusT e.V.** | **FH Gelsenkirchen** |
| **Dr. Achim Schmidt** | **Chief Information Officer** | **Beta Systems** |
| **Wolfgang Schneider** | **Stellvertretender Institutsleiter** | **Fraunhofer SIT** |
| **Reinhard Schöpf** | **Ex-Chief Information Security Officer** | **Siemens** |

Trotz einiger Absagen hat das volle Engagement und die Kompetenz der Teilnehmer in den intensiven Diskussionen den Erfolg des Workshops gewährleistet.

## 2. Methodik und Ablauf des Workshops

Der Ablauf des Workshops war wie folgt geplant:

| | |
|---|---|
| **13:00–14:00** | **Ankunft der Teilnehmer, Snacks & leichter Imbiss** |
| **14:00–14:10** | **Begrüßung und Einführung in den Tag, Vorstellung Projekt, unsere Erwartungen** |
| **14:10–14:30** | **Vorstellung der Teilnehmer (Position zur PKI, Erwartungen an die Veranstaltung)** |
| **14:30–14:45** | **Vorstellung bisherige Literaturrecherche und Ergebnisse der Interviews zur Technik** |
| **14:45–15:00** | **Vorstellung wirtschaftliche Betrachtungen und erste Ergebnisse** |
| **15:00–15:15** | **Vorstellung Nutzungsbedingungen und Ergebnisse der anonymen Telefoninterviews** |
| **15:15–15:20** | **Kurze Erklärung der Workshop-Technik (Paulus)** |

| | |
|---|---|
| 15:20–15:40 | Kaffeepause |
| 15:40–17:00 | Break-Out in 3 parallelen Sitzungen |
| 17:00–18:00 | Vorstellung der in den Sitzungen erarbeiteten Ergebnisse |
| 18:00–18:30 | Feedback-Runde |
| 18:30–19:00 | Pause |
| 19:00–21:00 | Gemeinsames Abendessen mit Platzierung der Teilnehmer zur Fortführung der Diskussion |
| 21:00–22:30 | Kaminfachgespräch: bilaterale Diskussionen zur Ergänzung und Abrundung |

Die Gesamt-Moderation des Workshops bis zum Abendessen wurde von H. Paulus durchgeführt. Um die Teilnehmer auf die zu einem späteren Zeitpunkt geplanten Arbeitsgruppen vorzubereiten wurden sie in einem ersten Schritt über die bisherigen Ergebnisse der Arbeiten des Projektteams informiert. In den darauf folgenden „Break-Out-Sessions" sollten die Teilnehmer auf der Basis ihres Wissens und ihrer Erfahrung und der von uns dargestellten Ergebnisse mit Hilfe von Moderationskarten jeweils 3–5 Problemfelder identifizieren, daraufhin passende Wunsch-Zustände sowie Lösungen/Aktionsfelder erarbeiten, die den Wunsch-Zustand zum Ziel haben. Die Moderationskarten wurden dann unter Erklärungen und Feedback durch die Sitzungsteilnehmer weiter bearbeitet. Ein Rapporteur jeder Arbeitsgruppe berichtete eine Zusammenfassung der Diskussion im darauf folgenden Plenum.

Die Diskussionen waren von Anfang an sehr intensiv durch die breit differenzierte Kompetenz der Workshop-Teilnehmer, mit Beiträgen aus sehr unterschiedlicher Interessenlage. Durch die Vertiefung in den Arbeitsgruppen wurde eine Fokussierung der Kernthematik erreicht, die durch die abschließende Feedback-Runde noch einmal zusammengefasst wurde. Insbesondere die interdisziplinäre Zusammensetzung von Technikern und Nicht-Technikern, von IT- und Sicherheitsverantwortlichen über PKI-Dienstleister bis hin zu Professoren der Betriebswirtschaft war ein wesentlicher Erfolgsfaktor für die Ausprägung von differenzierten und durchaus kontroversen Aspekten.

Besonderer Wert wurde darauf gelegt, die Zusammensetzung der Break-Out-Sessions so gestalten, dass möglichst Personen zusammen gearbeitet haben, die sich nicht vorher kannten. Durch diese Maßnahme wurde eine offene, vorurteilsfreie Diskussion unterstützt. Dieses Vorgehen hat sich unserer Meinung nach als erfolgreich erwiesen, obwohl das Bestreben in den Diskussionen, ein gemeinsames Verständnis zu Sachthemen zu erreichen, natürlich Zeit kostete.

Auch wenn die Diskussionen über die Zeit sehr breit verteilte Aspekte berührten, war doch der Verlauf geprägt von optimistischen, aber dennoch kritischen Auseinandersetzungen mit klarem Fokus: dem Erfolg von Public-Key-Infrastrukturen, -Anwendungen und -Technologien. Im weiteren Verlauf dieses Kapitels werden die Ergebnisse der Diskussionen aufgezeigt. Sehr wertvoll waren die Empfehlungen zur weiteren Vorgehensweise, die uns von den Teilnehmern ohne Aufforderung mitgegeben wurden.

Schließlich enthielten die eher informellen Kommentare während des gemeinsamen Abendessens und des anschließenden Kamingesprächs wichtige Detail- und Praxisinformationen sowie persönliche Einschätzungen, die das Projektteam in einer formellen Befragung wie in dem moderierten Teil des Workshops nicht erfahren hätte. Dies gilt in besonderem Maße für Meinungen oder Einschätzungen entgegen der „herrschenden" Expertenmeinung, die – vielleicht wegen politischer Motivationen – in dieser Form bisher nicht öffentlich diskutiert wurden.

Zusammenfassend kann man zur Methodik des Workshops sagen, dass die beiden Aspekte „Interdisziplinarität der Teilnehmer" und „Mischung aus moderierter Diskussion und informellen Gesprächen" Garanten für den Erfolg des Workshops waren und damit ein wesentliches Element in der Erkenntnisbildung des Projekts darstellen. Darüber hinaus ist betonen, dass es vermutlich nur durch den gesellschaftlichen Rahmen überhaupt möglich war, die in dieser Form selten erreichte Zusammensetzung von anerkannten Experten zu erreichen. So konnten wir ein facettenreiches, durchaus mit Spannungen und Widersprüchen versehenes Bild über Nutzungsbedingungen von PKI in der Praxis gewinnen, was ohne eine solche Veranstaltung, etwa nur durch Interviews, mit hoher Sicherheit nicht erreicht worden wäre. Wir können daher dieses Vorgehen für weitere Themen mit interdisziplinärem Charakter grundsätzlich empfehlen.

## 3. Aufteilung in Gruppen

**Gruppe „Blau":** Moderation: Reimer
Protokoll: Hesse
→ Schöpf
→ Hawreluk
→ Mock-Hecker
→ Bally

**Gruppe „Grün":** Moderation: Morcinek
Protokoll: Beyer
→ Beckmann
→ Galley
→ Heider
→ Frank
→ Pohlmann

**Gruppe „Rot":** Moderation: Holl
Protokoll: Hellmann
→ Günther
→ Herzog
→ Schneider
→ Schmidt

## 4. Einladungstext

*Sehr geehrte Damen und Herren,*

*im Auftrag des BMBF führen wir ein Forschungsprojekt zur Untersuchung der Erfolgskriterien von Public-Key-basierten Anwendungen durch. Dabei steht nicht die Technik im Vordergrund, sondern Nutzungsbedingungen und betriebswirtschaftliche Aspekte.*

*Insbesondere wollen wir erarbeiten, warum die sicherheitstechnisch überlegene Technologie (noch) nicht flächendeckend eingesetzt wird, was Hinderungsgründe sind, warum IT-Verantwortliche oft andere Lösungen bevorzugen und welche Parameter zur erfolgreichen Umsetzung notwendig sind.*

*Um von Erfahrungen von Entscheidern und deren Umfeld profitieren zu können, führen wir einen High-Level Workshop durch, bei dem wir IT-Entscheider (und nicht unbedingt Sicherheitsverantwortliche) zu Wort kommen lassen wollen. In dem seminarähnlichen Umfeld, ansprechend moderiert, soll der lockere Austausch nicht zu kurz kommen, um auch Networking und Diskussionen zu anderen Themen Raum zu lassen.*

*Die Gestaltung der Veranstaltung ist entsprechend folgendermaßen aufgebaut:*
*→ Anreise am Vormittag, leichter Lunch ab 13h*
*→ Seminararbeit 14h bis 18h*
*→ Gemeinsames Abendessen 19h*
*→ Übernachtung im Schlosshotel Grunewald, Berlin*

*Als mögliche Termine haben wir den 22. Februar oder alternativ den 27. Februar vorgesehen. Die aktuelle Präferenz liegt auf Donnerstag, dem 22. Februar.*

*Wir würden uns sehr geehrt fühlen, wenn Sie uns mit Ihrer Expertise zur Verfügung stehen könnten. Um eine kurze Rückmeldung per E-Mail in den nächsten Tagen würden wir uns sehr freuen. Bei einer positiven Rückmeldung wird Ihnen eine offizielle Einladung zugesendet. Natürlich übernehmen wir die Reisekosten für die Veranstaltung.*

*Herzliche Grüße*

*Friedrich Holl*
*Sachar Paulus*
*Helmut Reimer*

Ebenfalls erhältlich:

Band 1: Metastudie Open-Source-Software und ihre Bedeutung für Innovatives Handeln
Band 2: Studie zum Innovationsverhalten deutscher Software-Entwicklungsunternehmen


Redaktion: Friedrich-L. Holl
Gestaltung: Martin Schüngel
Druck: digital business and printing gmbh, Berlin

ISSN 1863-5016