

Public Key Infrastrukturen

-

Über den Business Case zur Technologie

Thomas Hueske
thomas.hueske@src-gmbh.de

Dagmar Schoppe
dagmar.schoppe@src-gmbh.de

SRC Security Research & Consulting GmbH
Leipziger Straße 35
D-65191 Wiesbaden

Zusammenfassung

Die technikorienteerte Diskussion zum Thema PKI hat sich gewandelt, vielmehr steht der Anwendungsaspekt und der hiermit verbundene Nutzen einer PKI im Vordergrund. Es hat sich gezeigt, dass die Analyse und Betrachtung des Business Case an erster Stelle von zentraler Bedeutung ist. Die Diskussion der Technik steht demgegenüber erst an zweiter Stelle.

In dem vorliegenden Beitrag werden zunächst die Zielsetzung sowie die Rahmenbedingungen für den Einsatz einer PKI diskutiert. Anschließend folgt als zentraler Bestandteil die Darstellung der Geschäftsprozessanalyse sowie deren Umsetzung anhand von Beispielen aus der Praxis. Zur Analyse der Geschäftsprozesse sind sowohl funktionale als auch wirtschaftliche Betrachtungen zu führen. Mit konkreten Beispielen wird die Überführung herkömmlicher Verfahren in elektronisch gestützte PKI-Anwendungen illustriert (z. B. eKurier).

1 Einleitung

Die Etablierung von Public Key Infrastrukturen in Europa und besonders in Deutschland ist unübersehbar und inzwischen unabstreitbar. Indizien hierfür sind ebenso wie die große Anzahl von Trust Centern, die ihre Dienste anbieten, die Vielzahl von Herstellern von PKI-Produkten und nicht zuletzt auch das zunehmende Augenmerk der Öffentlichkeit für diese Technologie und den damit verbundenen und versprochenen Anwendungen.

So groß wie die Anzahl der Trust Center und Hersteller, so groß ist auch die Bandbreite des angebotenen Spektrums an Dienstleistungen und Produkten. Bei den Trust Centern trifft man auf Anbieter von Serverzertifikaten bis hin zu akkreditierten Zertifizierungsdiensteanbietern, die qualifizierte Zertifikate ausstellen. Das Spektrum der PKI-Produkte erstreckt sich von Kryptomodulen und CA-Management-Software für Trust Center bis hin zu Programmen zur

sicheren Signatur und Verschlüsselung, Absicherung von Internet Kommunikation (z. B. SSL) oder Virtual Private Networks (VPN) auf der Anwenderseite.

Rahmengebend für die Entwicklung der Public Key Technologie ist sicherlich auch der europaweite Gesetzgebungsprozess. Die Umsetzung der EU-Richtlinie in die nationale Gesetzgebung ist in Deutschland mit der Novellierung des Signaturgesetzes nun abgeschlossen.

Für Unternehmen und die öffentliche Verwaltung stellt sich damit die Frage, ob die neue Technologie geeignet ist, die eigenen Prozesse zu unterstützen oder direkten ökonomischen Nutzen zu stiften. Dabei hat eine Abkehr von der technischen Sicht der PKI hin zu einer Prozessorientierung stattgefunden. Zahlreiche Beispiele zeigen, dass ein erfolgreicher Einsatz von PKI stattgefunden hat, wenn der „Business Case“ im Vordergrund steht und die folgenden Fragen analysiert wurden:

- Welche neuen Geschäftsmöglichkeiten eröffnen sich durch den Einsatz von Public-Key-Technologie?
- Welche Arten von Signaturfunktionen sind zur Unterstützung spezifischer Geschäftsabläufe geeignet?
- Wie sind PKI-Funktionen effizient in neue oder bestehende Geschäftsprozesse und Anwendungen einzubinden?
- Welche Vorteile können hieraus gezogen werden und welche Kosten sind damit verbunden?

Kurz gesagt: „Welchen Business Case ermöglicht PKI, und wie viel PKI benötige ich dafür?“. Überlegungen, wie Signaturfunktionen technisch in IT-Anwendungen integriert werden können, kommen erst an zweiter Stelle.

2 Erschließung neuer Geschäftsfelder durch PKI

Der Einsatz der Public-Key-Technologie bietet auf einzigartige Weise die Möglichkeit, alle grundlegenden Merkmale sicherer Transaktionen, nämlich

- Authentizität,
- Integrität,
- Vertraulichkeit und
- Unbestreitbarkeit

miteinander zu kombinieren und hieraus Gewinn in Form von effizienteren Prozessen oder neuen bzw. verbesserten Dienstleistungen und Produkten zu schöpfen.

Unmittelbarer ökonomischer Nutzen kann sich zum Beispiel aus der Etablierung hochwertiger Vertriebswege über das Internet, aus der Vermarktung bisher wirtschaftlich ungenutzter Daten oder aus der Verbesserung von Service und Kundenbindung ergeben.

Auf Prozessebene eignet sich die Public Key Technologie u.a. zum Schutz wertvoller Daten, zur Unterstützung des Qualitätsmanagements oder zur Vereinfachung logistischer Prozesse und bietet dabei vom Einsatz einfacher SSL-Zertifikate bis zum Aufbau einer eigenen Public Key Infrastruktur auf der Basis von Chipkarten eine eindrucksvolle Bandbreite an Hilfsmitteln.

Die Nutzung dieser Werkzeuge erfordert jedoch den zumindest teilweisen Aufbau und Betrieb der grundlegenden PKI-Funktionen. Diese umfassen insbesondere Registrierungsprozesse, Zertifikatsmanagement sowie Sperrlistenmanagement.

Diese Prozesse müssen betriebsintern definiert und integriert werden.

Die Diskussion um die Integration von PKI-Funktionen in Anwendungen stand bisher allerdings im Schatten einer Technik-Debatte, die sich eher mit der internen Funktionsweise von Public Key Infrastrukturen auseinandergesetzt hat, als mit der Frage, in welche Anwendungen auf welche Weise PKI-Funktionen integriert werden können, und welcher Nutzen hieraus entsteht.

Lange Zeit versteifte man sich auf die Suche nach der sogenannten „Killer-Applikation“, die allerdings noch unentdeckt blieb. Heute ist man dazu übergegangen, einen Business Case zu suchen, der durch Public Key Technologie unterstützt oder erst möglich wird. Hinzu kommt eine differenzierte und auf den Business Case abgestimmte Nutzung der verschiedenen PKI-Funktionalitäten.

Zudem haben viele Unternehmen bereits die imagefördernde Wirkung des PKI-Einsatzes erkannt.

3 Rahmenbedingungen

3.1 Gesetzliche Rahmenbedingungen

Am 13.12.1999 haben das europäische Parlament und der Rat die gemeinschaftlichen Rahmenbedingungen für elektronische Signaturen in Form einer Richtlinie [1999/93/EG] erlassen, die am 19.01.2000 in Kraft getreten ist. Diese Richtlinie legt für die Mitgliedsstaaten der europäischen Union die vereinheitlichenden Rahmenbedingungen zur Signaturgesetzgebung fest und erfordert die Umsetzung bis spätestens 19.07.2001.

Die Richtlinie hat zum Ziel, die Verwendung elektronischer Signaturen zu erleichtern und zu ihrer rechtlichen Anerkennung beizutragen. Wichtige Regelungskomponenten zur Gewährleistung der tatsächlichen Sicherheit sind neben der Haftung für Zertifizierungsdiensteanbieter die Anforderungen an die technische Sicherheit der eingesetzten Komponenten, die Sicherheitsanforderungen an die Einrichtungen und Prozesse der Zertifizierungsdiensteanbieter sowie deren Überwachung.

Ein weiterer Aspekt der EU-Vorgabe liegt in der rechtlichen Gleichstellung qualifizierter elektronischer Signaturen mit der eigenhändigen Unterschrift. Ergänzend hierzu werden in der E-Commerce-Richtlinie [2000/31/EG] die Mitgliedstaaten aufgefordert zu gewährleisten, dass

ihre für den Vertragsabschluss geltenden Rechtsvorschriften die Verwendung elektronischer Verträge ermöglichen. Die E-Commerce-Richtlinie ist bis zum 17.01.2002 in nationales Recht umzusetzen.

Seit dem 22. Mai 2001 ist das neue Signaturgesetz in Kraft (Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften vom 16. Mai 2001, BGBl. I, S. 876, veröffentlicht am 21. Mai 2001, SigG 2001), in dem die Vorgaben der EU umgesetzt wurden. Die wesentliche Änderung gegenüber der alten Gesetzesfassung besteht in der Hinzunahme der „qualifizierten elektronischen Signaturen“, die nun als Ersatz der eigenhändigen Unterschrift und als Beweismittel vor Gericht zugelassen sind. Das SigG 2001 unterscheidet zwischen folgenden Typen elektronischer Signaturen:

- (Einfache) elektronische Signaturen, §2 (1) SigG 2001,
- Fortgeschrittene elektronische Signaturen, §2 (2) SigG 2001,
- Qualifizierte elektronische Signatur, §2 (3) SigG 2001 und
- Qualifizierte elektronische Signatur mit Anbieter-Akkreditierung, §2 (3) i. V. m. § 15 SigG 2001.

Das Signaturgesetz und die Signaturverordnung definieren die verschiedenen Zertifikats- und Signaturtypen und legen die damit verbundenen Anforderungen fest. Über die Rechtswirkung der einzelnen Signaturtypen werden in dem Signaturgesetz keine Aussagen gemacht.

Die Rechtswirkung der unterschiedlichen Signaturtypen wird in diversen Gesetzbüchern geregelt. U.a. finden sich Regelungen

- im Bürgerlichen Gesetzbuch (BGB),
- im Verbraucherkreditgesetz (VerbrKrG),
- in der Zivilprozessordnung (ZPO),
- in der Verwaltungsgerichtsordnung (VwGO) sowie
- im Handelsgesetzbuch (HGB).

Mit der Einführung des Signaturgesetzes hat sich an der grundlegenden Definition eines Rechtsgeschäftes nichts geändert. Soweit keine Form vorgeschrieben ist, genügen für Rechtsgeschäfte somit elektronische oder fortgeschrittene Signaturen. Qualifizierte Signaturen können, müssen aber nicht eingesetzt werden.

In §126 BGB ist die Schriftform definiert. Ergänzend ist in §126a BGB die Definition der elektronischen Form aufgenommen worden. Die elektronische Form liegt vor, wenn der Aussteller der (elektronischen) Erklärung seinen Namen hinzufügt und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versieht.

Wiederum nach §126 BGB (Absatz 3) kann die schriftliche Form durch die elektronische Form ersetzt werden, wenn sich aus dem Gesetz nicht ein anderes ergibt. Die auf der qualifizierten Signatur beruhende elektronische Form hat also dieselbe Rechtswirkung wie die schriftliche Form, sofern sich nicht aus dem Gesetz ein anderes ergibt. Die elektronische

Form ist in einigen Fällen explizit durch gesetzliche Regelungen ausgeschlossen (z. B. Bürgschaftserklärungen, Arbeitszeugnisse, Kreditverträge).

3.2 Standardisierung

Aufgrund der Komplexität einer Public Key Infrastruktur mit einer Vielzahl von Schnittstellen zwischen Komponenten verschiedener Dienste und Herstellern bedarf es übergreifender Vereinbarungen, um eine Kommunikation zwischen beliebigen Anwendern zu ermöglichen. Hierzu sind einerseits die Aktivitäten zur Standardisierung im Bereich PKI zu berücksichtigen, andererseits werden Dokumente mit Anforderungen zur Interoperabilität von Komponenten von verschiedenen Interessengruppen publiziert. Letztere sind i.d.R. anwendungsbezogen.

Einer der grundlegenden Standards im Bereich der PKI ist der X.509 Standard, in dem Formate für Zertifikate, Attributzertifikate und Sperrlisten definiert werden. Das aktuelle Format für Zertifikate ist zur Zeit das sogenannte X.509 v3 Zertifikat, und für Sperrlisten ist die Version v2 aktuell.

Im internationalen Kontext der PKI finden insbesondere Aktivitäten der Arbeitsgruppe "Internet X.509 Public-Key Infrastructure" der Internet Engineering Task Force (IETF-PKIX) eine breite Unterstützung. Diese Arbeitsgruppe publiziert Internet-Standards (Request for Comments, RFCs) und in Diskussion befindliche Arbeitspapiere (Internet-Drafts). Dort behandelte Themen sind beispielsweise Profile für Zertifikate und Sperrlisten, Abruf von Zertifikaten als Datenobjekte, Validierungsdienst sowie Zeitstempeldienst.

Einen vergleichbaren Stellenwert hat die Serie der Industriestandards "Public-Key Cryptography Standards (PKCS)", die von RSA Security Inc. herausgegeben werden. Wesentliche Beispiele sind Vorgaben zur Anwendung des RSA Algorithmus (PKCS #1), Format von kryptographisch behandelten Nachrichten (PKCS #7), Anfragen an den Zertifizierungsdiensteanbieter zur Zertifizierung von öffentlichen Schlüsseln (PKCS #10), eine Schnittstelle zwischen Anwendung und Sicherheitstoken (PKCS #11), Format eines Sicherheitstokens (PKCS #12) sowie die Formatierung von Datenobjekten in einem Sicherheitstoken (PKCS #15).

Standardisierungsaktivitäten zur technischen Umsetzung der EU-Direktive erfolgen zur Zeit im Rahmen von European Electronic Signature Standardization Initiative – EESSI. Die Arbeiten werden von den Standardisierungsgremien CEN und ETSI unterstützt. Jedes Gremium betreut diverse Aktivitäten zur Standardisierung. Diese haben einerseits technischen Charakter – wie beispielsweise die Definition von Zertifikatsprofilen oder Anforderungen an eine sichere Signaturerstellungseinheit -, andererseits werden auch organisatorische Rahmendokumente erstellt (z. B. Policy für Diensteanbieter von Zeitstempeln).

Beispielsweise wurde das Zertifikatsprofil für einen Einsatz nach der EU-Direktive definiert. Hierbei wurden die Vorgaben der IETF-PKIX übernommen und geeignet ergänzt.

3.3 Initiativen zur Vernetzung

Die Verbindung von Vertrauensketten zwischen verschiedenen Organisationen ist das Ziel der von der Deutschen Telekom AG und der Deutschen Bank AG ins Leben gerufenen Bridge-CA-Initiative (BCA), die mittlerweile als Dienstleistung der TeleTrust-Organisation betrieben wird. Vertrauenslücken bei organisationsübergreifenden Transaktionen, wie z.B. die gesicherte E-Mail-Kommunikation, sollen überbrückt werden, wodurch eine gemeinsame Vertrauensinfrastruktur geschaffen werden soll, die verschiedene – existierende und zukünftige – PKI-Inseln umschließt. Die Bridge-CA ermöglicht die gegenseitige Prüfung von Zertifikaten der teilnehmenden Unternehmen, Behörden und Institutionen und prüft als Brücke zwischen den Beteiligten die Root-Zertifikate der teilnehmenden Organisationen. Der Teilnehmer erkennt die Bridge-CA als vertrauenswürdige Instanz an.

Um das Ziel der Bridge-CA in der Praxis erreichen zu können, ist ein grundlegendes Maß an Interoperabilität der für den Einsatz vorgesehenen sicheren Email-Client-Komponenten erforderlich. Voraussetzung für die Teilnahme an der Bridge-CA-Initiative ist die Durchführung eines Bridge-CA-Konformitätstest. Um die gewünschte Kompatibilität der jeweiligen Public Key Infrastruktur (PKI) zu erreichen, sind die Teilnehmer gehalten, die aufgrund der Ergebnisse des Konformitätstestes erforderlichen technischen und organisatorischen Anpassungen vorzunehmen. Weiterhin muss die Bereitschaft zur Migration der Komponenten bestehen, falls dies für die Bridge-CA aus Gründen der Interoperabilität, der technischen Fortentwicklung oder anderer Anforderungen erforderlich wird. TeleTrust informiert den Teilnehmer über etwaige Veränderungen und räumt eine angemessene Frist für die Migration ein.

Teilnehmer müssen ihr Einverständnis erklären, ihre Sicherheits-Policy sowohl der Bridge-CA als auch den anderen Teilnehmern zugänglich zu machen. Die Mindestanforderungen der Bridge-CA müssen in der eigenen Sicherheits-Policy (Teilnehmer-CPS) berücksichtigt sein. Begründete Abweichungen sind möglich.

4 Geschäftsprozessanalyse

Das Konzept der Geschäftsprozessanalyse, das in diesem Vortrag vorgestellt wird, dient der Prüfung von Geschäftsprozessen hinsichtlich ihrer „PKI-Tauglichkeit“. Hierbei werden zunächst in Form einer funktionalen Betrachtung die Anforderungen an die Geschäftsprozesse betrachtet. Dies wird in Abschnitt 4.1 beschrieben. Diese funktionale Betrachtung endet mit einer fachlichen Bewertung und Empfehlung, i. d. Regel in Form eines Grobkonzepts, für einen neuen Business Case. Diese Empfehlung ist dann die Grundlage für die Wirtschaftlichkeitsbetrachtung, die in Abschnitt 4.2 diskutiert wird. Erst in diesem Stadium werden technische Realisierungsmöglichkeiten sowie Kostenaspekte für den neuen Business Case betrachtet.

Erst nach einer erfolgreichen wirtschaftlichen Prüfung kann über eine Realisierung des neuen Business Cases entschieden werden.

4.1 Funktionale Betrachtung

Die Geschäftsprozessanalyse gliedert sich in vier Stufen. Sie wird eingeleitet durch die **Identifizierung von Geschäftsprozessen**. Hierbei werden die Geschäftsprozesse des zu untersuchenden Unternehmens oder Unternehmensteils ermittelt und in Bezug zueinander gesetzt. In der Regel besteht ein Unternehmen aus einer komplexen Vernetzung von Geschäftsprozessen.

Geschäftsprozesse, die an dieser Stelle priorisiert betrachtet werden, sind zum einen formularbasierte Prozesse, z. B. interne Prozesse oder Bestell- bzw. Lieferprozesse, Prozesse, in denen interne oder sensitive Daten verarbeitet werden, Prozesse im Rahmen des Zahlungsverkehrs oder Qualitätsmanagements sowie online-Dienste.

Anhand eines **Kriterienkatalogs** werden anschließend ausgewählte Prozesse auf „PKI-Tauglichkeit“ untersucht. Der Kriterienkatalog ermittelt Anforderungen an die im Prozess verarbeiteten Daten oder Informationen hinsichtlich ihrer Authentizität, Integrität, Vertraulichkeit und Unbestreitbarkeit.

Zusätzlich werden weitere Prozesscharakteristika betrachtet, wie beispielsweise externe Anforderungen (z. B. des Gesetzgebers oder einer Aufsichtsbehörde), interne Anforderungen (z. B. Qualitätsmanagement, Revision), Automatisierbarkeit oder örtliche Verteilung.

Es hat sich bewährt, diesen Kriterienkatalog in Form eines Fragenkatalogs prozessorientiert darzustellen. Hilfestellung zur Ermittlung von Prozessanforderungen geben beispielsweise folgende Fragestellungen:

- „Gibt es Verzögerungen dieses Prozesses durch die Abwesenheit von Zeichnungsberechtigten?“
- „Ist in diesem Prozess ein Vier-Augen-Prinzip vorgesehen?“
- „Liegen Medienbrüche in diesem Prozess vor?“

Anschließend wird eine **Gewichtung der Kriterien je Prozess** vorgenommen. Diese ist in Abhängigkeit mit den Anforderungen vorzunehmen. Hierbei werden auch gesetzliche oder andere (z. B. verfahrenstechnische) Anforderungen miteinbezogen.

Zum Schluss erfolgt eine zusammenfassende **Bewertung jedes Geschäftsprozesses in Form eines Grobkonzepts** hinsichtlich einer PKI-Unterstützung und eine fachliche Empfehlung für eine Prozessumgestaltung. Hierzu gehört ebenfalls die Benennung des potenziellen Nutzens des neuen Business Cases. Der zu erzielende Nutzen muss nicht notwendigerweise direkter ökonomischer Art sein.

Die Nutzenanalyse kann beispielsweise ergeben:

- Steigerung des Umsatzes
- Nutzung bisher ungenutzter Daten und Informationen
- Entwicklung eines neuen Produkts oder Anbieten einer neuen Dienstleistung
- Einsparung von Kosten
- Kürzeres „time-to-market“ bei der Produktentwicklung
- Imagegewinn bzw. verstärkte Kundenbindung
- Verbesserter Schutz sensibler Daten
- Verbesserte Qualitätssicherung.

Anhand des nun folgenden Beispiels des internen Prozesses einer Reisekostenabrechnung wird die eingeführte Geschäftsprozessanalyse schrittweise verdeutlicht.

Schritt 1: Identifikation des Geschäftsprozesses

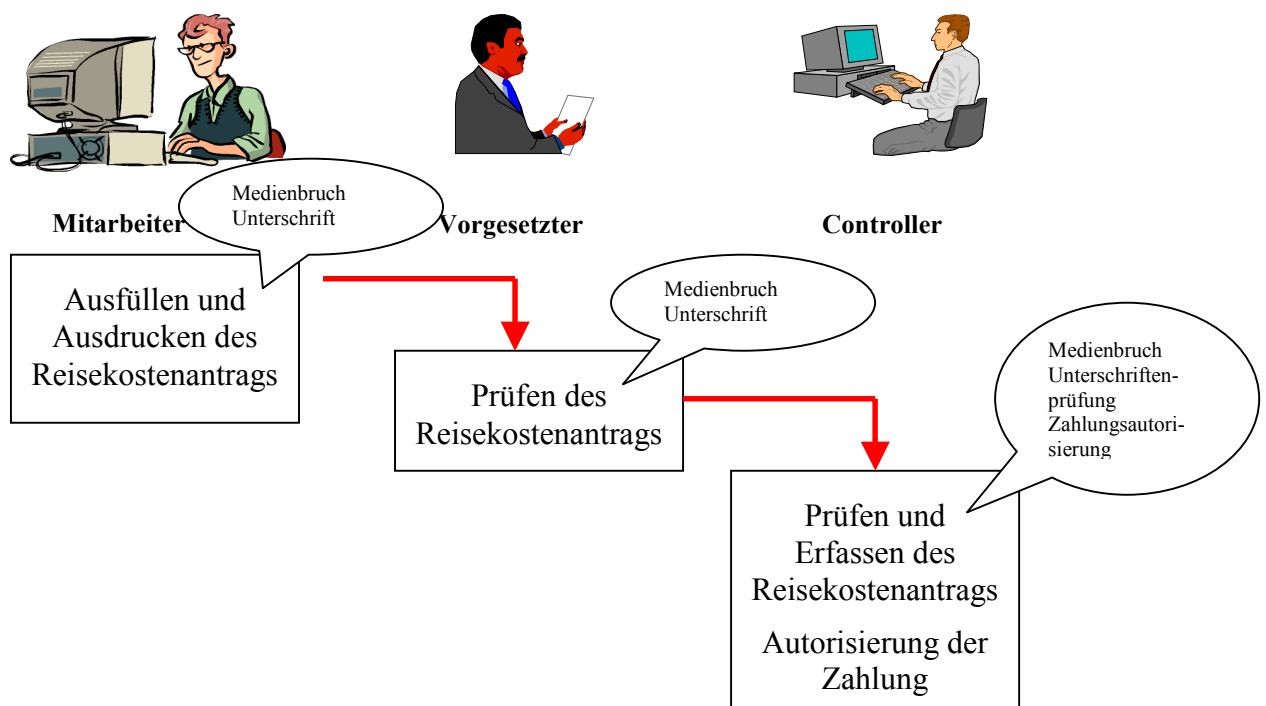


Abb. 1: Identifikation des Geschäftsprozesses

Schritt 2 und 3: Kriterienkatalog und Gewichtung der Kriterien

Kriterien	Gewichtung
Integrität der Daten im Reisekostenantrag	ⓂⓂⓂ
Vermeidung von Medienbrüchen	ⓂⓂⓂ
Prüfung der Unterschriften	ⓂⓂ
Autorisierung der Zahlung	ⓂⓂ
Vermeiden von Verzögerungen	Ⓜ
Automatisierbarkeit des Prozesses	Ⓜ
Workflow-Unterstützung	Ⓜ
Spezifische gesetzliche Anforderungen	Ⓜ

Schritt 4: Bewertung des Prozesses

Einführung einer Workflow-Unterstützung und Einsatz der digitalen Signatur

- Vermeidung der Medienbrüche durch Workflow-Unterstützung
- Einsatz der digitalen Signatur des Mitarbeiters zur Sicherung der Integrität der Daten im Reisekostenantrag
- Einsatz der digitalen Signatur des Controllers zur Zahlungsautorisierung

Nutzenanalyse

- Straffung des internen Prozesses durch zeitnahe Abrechnung der Reisekosten
- Elektronische Archivierung der Reisekostenabrechnungen
- Nachweisbare Prüfung der Unterschriften

4.2 Wirtschaftliche Betrachtung

Im vorherigen Abschnitt 4.1 wurden die funktionalen Betrachtungen zur Geschäftsprozessanalyse beschrieben, an deren Ende ein Vorschlag für einen neuen Business Case steht.

Zur Entscheidungsfindung wird neben der fachlichen Betrachtung auch eine wirtschaftliche Betrachtung („Businessplan“) durchgeführt. Diese besteht im wesentlichen aus einer **Machbarkeitsanalyse** und einer **Kostenanalyse**. Hierbei müssen noch für den Erfolg der

Geschäftsprozessanalyse relevanten technischen oder wirtschaftlichen Aspekte betrachtet werden.

Machbarkeitsanalyse	Kostenanalyse
<ul style="list-style-type: none"> • Technische Umsetzbarkeit • Technische Risiken • Zeitplan • Ressourcenplanung 	<ul style="list-style-type: none"> • Konzeption • Soft – und Hardware • Integration von Signatur- und/ oder Verschlüsselungssoftware • Zertifikats- und /oder Chipkartenmanagement • Anpassung und Anbindung an Hintergrundsysteme • Schulungsmaßnahmen • Dienstleister

Der abschließende **Entscheidungsprozess** ist in der folgenden Abbildung dargestellt:

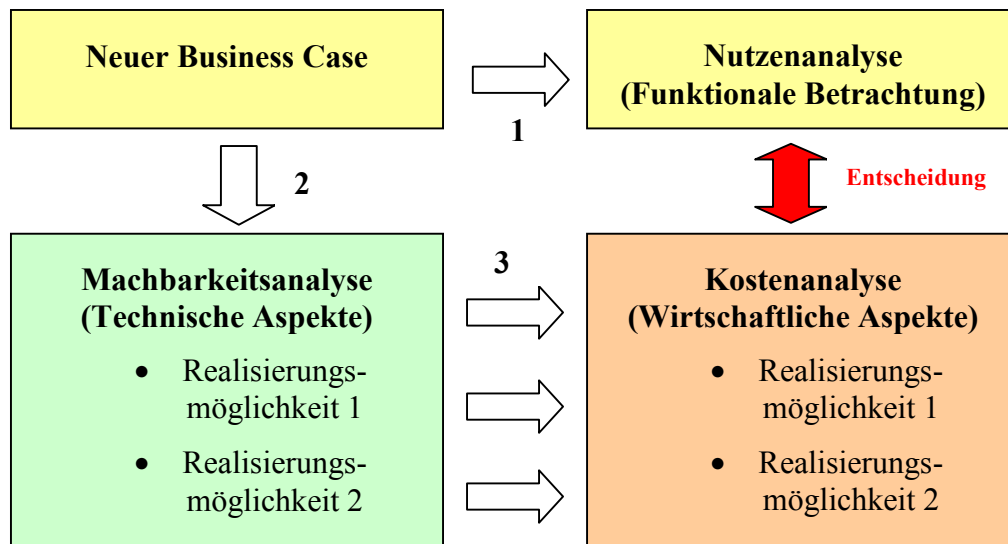


Abb. 2: Entscheidungsprozess

Für den neuen Business Case wird eine Nutzenanalyse erstellt, die den potenziell zu erwartenden Nutzen einer Prozessumstellung beschreibt (**Schritt 1**).

Ausschlaggebend für die Machbarkeitsanalyse ist das Grobkonzept für den neuen Business Case (**Schritt 2**). Erst in der Machbarkeitsanalyse werden technische Realisierungsmöglichkeiten betrachtet, die entscheidenden Einfluss auf die Kostenbetrachtung haben (**Schritt 3**). So variieren die Möglichkeiten im Beispiel des

Reisekostenantrags von Zertifikaten auf Software-Basis bis hin zur Einführung einer qualifizierten Signatur.

Der entscheidende Schritt („**Entscheidung**“) besteht dann in der Gegenüberstellung der Nutzenanalyse aus der funktionalen Betrachtung (siehe 4.1) sowie der Kostenanalyse der verschiedenen Realisierungsmöglichkeiten aus der wirtschaftlichen Betrachtung (siehe 4.2).

5 Beispiele für den realen Einsatz

In diesem Kapitel werden Beispiele für den realen Einsatz von Public Key Infrastrukturen dargestellt. Dabei werden unterschiedliche Anwendungsbereiche berücksichtigt, in denen bereits PKI-basierte Abläufe genutzt werden oder sich für den Einsatz von PKI-Lösungen eignen. Einige dieser Anwendungen können durch zusätzliche Nutzung einer elektronischen Zahlungsfunktion optimal ergänzt werden.

Beispielsweise existieren weltweit Projekte zum Auf- und Ausbau des sogenannten e-Government. Ziel dieser Projekte ist es, Verwaltungsabläufe effizienter zu gestalten und den Bürgern staatliche Leistungen auch über das Internet anzubieten.

Im Folgenden werden einige ausgewählte Beispiele vorgestellt:

- **Elektronische Steuererklärung**

Im Rahmen des Projekts „ELSTER“ (**E**lektronische **S**teuer**e**rklärung) können Steuererklärungen elektronisch bei der zuständigen Finanzbehörde eingereicht werden. Die elektronischen Steuererklärungen werden noch durch papierbezogene Erklärungen ergänzt. So werden beispielsweise Belege ebenfalls in Papierform eingereicht.

- **Online-Shop des Statistischen Bundesamtes**

Der Online-Shop „Destatis“ des Statistischen Bundesamtes (www.destatis.de) verkauft statistische Daten in Buch- oder Zeitschriftenform, auf CD-ROMs sowie als Dokumente im pdf-Format. Die Bestellung erfordert eine Online-Registrierung des Kunden, in der Name und Passwort des Benutzers vereinbart werden. Es werden personalisierte Web-Seiten angeboten, in denen der Kunde sich u.a. über seine bereits getätigten Bestellungen informieren kann.

- **Mitarbeiterausweis**

Eine weitere Anwendung stellt die Nutzung von Chipkarten als Mitarbeiterausweise dar, mit der Anwendungen zur Zugangskontrolle und für den internen Zahlungsverkehr, indem beispielsweise zur Zahlung in der Kantine die GeldKarte eingesetzt wird. Darüber hinaus dient der Mitarbeiterausweis für die Umsetzung einer PKI-basierten Lösung für den sicheren E-Mail Austausch sowie SSL-geschützten Zugriffe auf Servern des Intranets. Hierzu dient der Mitarbeiterausweis als Personal Security Environment mit den entsprechenden Schlüsseln und Zertifikaten.

6 Zusammenfassung

Die Gestaltung elektronischer Geschäftsprozesse bedarf zunächst einer grundlegenden Analyse. Für eine Umsetzung von Geschäftsprozessen in elektronisch gestützte Prozesse sind die funktionalen Aspekte zu betrachten sowie die Machbarkeit und die Kosten einer etwaigen Umsetzung zu bewerten. Die Betrachtung des Business Case steht also zunächst im Vordergrund. Die Umsetzung eines elektronischen Geschäftsprozesses ist durch eine Machbarkeitsanalyse zu untermauern und die letztendliche Entscheidung ist Ergebnis eines Abgleichs zwischen Nutzen- und Kostenanalyse.

Der Einsatz von Public Key Infrastrukturen ist erfolgreich, sofern eine entsprechende Betrachtung des Business Case geeignet und in positivem Sinne durchgeführt wurde. Eine rein technik-orientierte Betrachtung ist nicht zielführend und steht der sinnvollen Nutzung von Sicherheitslösungen eher im Wege.

7 Referenzen

- [1999/93/EG] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, veröffentlicht im Amtsblatt der Europäischen Gemeinschaften am 19.01.2000.
- [2000/31/EG] Richtlinie 2000/31/EG über die rechtlichen Aspekte des elektronischen Geschäftsverkehrs (E-Commerce-Richtlinie), veröffentlicht im Amtsblatt der Europäischen Gemeinschaften am 17.07.2000.
- [SigG2001] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, 16.05.2001, veröffentlicht im Bundesgesetzblatt Jahrgang 2001 Teil I Nr. 22, ausgegeben zu Bonn am 21. Mai 2001.
- [SigV2001] Verordnung zur elektronischen Signatur (Signaturverordnung, SigV), 16. November 2001.
- [BCA] Bridge CA Initiative
<http://www.bridge-ca.org>
- [PKCS] RSA Laboratories, Public Key Cryptography Standards
- [RFC3280] Internet X.509 Public Key Infrastructure, Certificate and CRL Profile, RFC 3280, April 2002
- [RFC2560] Internet X.509 Public Key Infrastructure, Online Certificate Status Protocol – OCSP, RFC 2560, June 1999.
- [X509] ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework, June 1997