

Public-Key Infrastrukturen für Finanzdienstleister

Detlef Hühnlein¹ · Andreas Jaletzke²

¹secunet AG, Sudetenstraße 16, D-96247 Michelau

²secunet AG, Mergenthalerallee 77-81, D-65760 Eschborn
{huehnlein, jaletzke}@secunet.de

Zusammenfassung

Diese Arbeit widmet sich dem Aufbau von Public-Key Infrastrukturen (PKI) für Unternehmen im Finanzdienstleistungssektor, wie z. B. Banken und Versicherungen. Insbesondere soll Finanzdienstleistern eine Entscheidungshilfe an die Hand gegeben werden, welche PKI-Art (unternehmenseigene PKI, signaturgesetzkonforme PKI, Identrus, ...) für den jeweiligen Bedarf gewählt werden sollte. Hierzu werden strategische Anforderungen und typische Anwendungen diskutiert und schließlich möglichen Realisierungsalternativen gegenübergestellt.

1 Einleitung

Neben der Notwendigkeit unternehmensweite Security-Policies – z. B. durch sichere E-Mail- oder Single-Sign-On-Lösungen – umzusetzen, besteht in vielen Unternehmen des Finanzdienstleistungssektors die strategische Management-Vorgabe, den entsprechenden Privat- und Geschäftskunden, Zulieferern und Partnern eine interaktive Schnittstelle, oder gar eine Plattform für nicht-bankspezifische Mehrwertdienste, zur sicheren Abwicklung elektronischer Geschäftsvorfälle zur Verfügung zu stellen. Während die internen Anforderungen oft durch gesetzliche, bank- und versicherungsfachliche Rahmenbedingungen, wie z. B. das Bankgeheimnis¹, motiviert sind, so zielen die letzteren Anforderungen auf die Reduktion von Transaktionskosten [Coa88] ab. Hierbei ist nicht nur eine Minimierung der unmittelbaren Kosten pro Transaktion angestrebt, sondern vielmehr ein ganzheitlicher Ansatz, der auch Aspekte der Kundenbindung umfasst und durch Anbieten von Mehrwertdiensten versucht, den Finanzdienstleister langfristig in das Zentrum der Wertschöpfungskette seiner Kunden zu rücken.

Ein essentieller, informationstechnologischer Baustein für die Umsetzung dieser Vorgaben ist eine umfassende Public-Key Infrastruktur, die sowohl internen als auch externen Anforderungen, heute und in Zukunft, genügen kann. Für die Umsetzung einer solchen PKI existieren verschiedene Realisierungsalternativen, wie z.B. unternehmensinterne PKI (ggf. in Verbindung mit herstellergetriebenen Strukturen oder einer Bridge-CA-Unterstützung), signaturgesetzkonforme PKI oder Identrus, die hierfür berücksichtigt werden sollten.

¹siehe z. B. [Gri00, „AGB Banken – Grundregeln für die Beziehung zwischen Kunde und Bank“, Seite 427]

Dieses Papier soll Finanzdienstleistern bei der Auswahl geeigneter Public-Key Infrastrukturen unterstützen und ist folgendermaßen gegliedert: Abschnitt 2 stellt verschiedene relevante PKI-Alternativen in kompakter Weise vor. Abschnitt 3 diskutiert strategische Anforderungen an eine PKI, sowie typische zertifikatsbasierte Anwendungen, im Finanzdienstleistungssektor. Abschnitt 4 bietet eine erste Entscheidungshilfe zur Auswahl geeigneter Strukturen, indem die möglichen Realisierungsalternativen den vorher diskutierten Anforderungen gegenüber gestellt werden.

2 PKI-Alternativen für Finanzdienstleister

In diesem Abschnitt werden grundsätzliche, für Finanzdienstleister relevante, PKI-Alternativen kurz vorgestellt. In Abschnitt 4 werden die hier skizzierten Ausprägungen den in Abschnitt 3 diskutierten Anforderungen gegenübergestellt.

2.1 Unternehmensinterne PKI

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

2.2 Unternehmensübergreifende PKI-Architekturen

Ein grundlegendes Problem der oben angedeuteten internen PKI ist, dass den durch den Finanzdienstleister ausgestellten Zertifikaten oft die externe Anerkennung fehlt. Deshalb müssen Finanzdienstleister insbesondere auch unternehmensübergreifende PKI-Architekturen berücksichtigen.

Im Folgenden werden verschiedene unternehmensübergreifende PKI-Alternativen kurz vorgestellt.

In den ersten beiden Abschnitten werden Möglichkeiten vorgestellt, wie ein Finanzdienstleister mit moderatem Aufwand den Vertrauensbereich seiner eigenen PKI vergrößern kann. Abschnitt 2.2.1 skizziert die Möglichkeit der Einbindung in entsprechende herstellergetriebene, unternehmensübergreifende PKIs. Abschnitt 2.2.2 stellt kurz die Bridge-CA-Initiative vor.

In den folgenden Abschnitten werden zwei Alternativen vorgestellt, die ein sehr hohes Sicherheitsniveau und einen deutlich größeren Akzeptanzbereich mit sich bringen. Zum Einen besteht die Möglichkeit und – wie aus der Diskussion in Abschnitt 3 ersichtlich wird – oft die Anforderung signaturgesetzkonforme Zertifikate zu verwenden. Abschnitt 2.2.3 erläutert kurz die Bedeutung von signaturgesetzkonformen PKIs für Finanzdienstleister. Abschnitt 2.2.4 geht kurz auf Identrus – eine globale Vertrauensinfrastruktur für den B2B E-Commerce – ein.

2.2.1 Herstellergetriebene PKI-Architekturen

Von verschiedenen PKI-Systemherstellern, wie z.B. Verisign, RSA und Entrust, wird die (unter Umständen kostenintensive) Möglichkeit geboten die unternehmensinterne PKI in "globale" herstellergetriebene Vertrauensinfrastrukturen einzubinden. Während der Akzeptanzbereich der eigenen Zertifikate offensichtlich vergrößert wird, so sind die verschiedenen herstellergetriebenen Infrastrukturen jedoch voneinander unabhängig und – insbesondere in Europa – weit von einer möglichen Flächendeckung entfernt.

2.2.2 Bridge-CA

Bei der Bridge-CA handelt es sich um eine gemeinnützige Initiative führender deutscher Industrieunternehmen und -verbände mit dem Ziel eine globale technisch/organisatorische Vertrauensinfrastruktur, z.B. für die sichere E-Mail-Kommunikation, zu schaffen. Die Bridge-CA, deren Management-Komitee aus Deutsche Bank AG, Deutsche Telekom AG, Daimler-Chrysler AG, SKO (Sparkassenorganisation), TeleTrusT e.V. und BSI besteht, überbrückt die Lücken in den Vertrauensbeziehungen zwischen isolierten PKIs, indem z.Zt. die Root-Zertifikate der teilnehmenden Organisationen sicher verteilt werden und zukünftig eine sternförmig cross-zertifizierte Infrastruktur – mit der Bridge-CA als zentraler Instanz – aufgesetzt wird. Für weitere Informationen zur Bridge-CA sei auf [EH01] verwiesen.

2.2.3 Signaturgesetz-konforme PKI

Die Bedeutung einer signaturgesetz-konformen PKI für Finanzdienstleister ist zweifach. Ist langfristig geplant *alle* Transaktionen papierlos durchzuführen, so ist – wegen des Schriftformerfordernisses, z. B. in §4 VerbrKG, oder der hohen Beweiskraft beim Abschluss von Verträgen – eine signaturgesetzkonforme PKI zwingend nötig. Auf der anderen Seite können beim Einsatz signaturgesetz-konformer Zertifikate auch Transaktionen mit Behörden und rechtlich abgesicherte Geschäfte zwischen Kunden und Partnern selbst durchgeführt werden.

2.2.4 Identrus

Identrus LLC wurde im April 1999 von den Banken ABN AMRO, Bank of America, Bankers Trust (inzwischen von der Deutschen Bank erworben), Barclays, Chase Manhattan, Citigroup, Deutsche Bank und Hypo Vereinsbank mit dem Ziel gegründet, eine weltweite Vertrauensinfrastruktur für B2B E-Commerce zu schaffen. Ausgenutzt wird im Identrus-System das Vertrauensverhältnis in der Geschäftsbeziehung zwischen Finanzinstitut und Geschäftskunde. Mittlerweile nehmen mehr als 40 internationale Großbanken an der Identrus-Initiative teil. Für weitere Informationen zu Identrus verweisen wir auf [Ide01, Ess00, Hüh01, HZ01].

3 Anforderungen an eine PKI für Finanzdienstleister

In diesem Abschnitt werden die wichtigsten Anforderungen an eine PKI für Finanzdienstleister zusammengetragen. Hierbei betrachten wir zunächst, in Abschnitt 3.1, grundsätzliche strategische Anforderungen an die IT-Infrastrukturen von Finanzdienstleistern und in Abschnitt 3.2 typische zertifikatsbasierte Anwendungen.

3.1 Strategische Anforderungen an eine PKI für Finanzdienstleister

Die strategischen Anforderungen an eine PKI für Finanzdienstleister erwachsen direkt aus entsprechenden Anforderungen an die gesamte IT-Infrastruktur.

Insbesondere sind die folgenden Aspekte zu berücksichtigen:

- **Rechtliche Aspekte**

Neben der Beachtung der bank- [Gri00] bzw. versicherungsrechtlichen [Büh00] Rahmenbedingungen, wie z. B. dem Schriftformerfordernis im Verbraucherkreditgesetz (§ 4, VerbrKrG, z. B. in [Gri00, Seite 207 ff.]) oder den Verschwiegenheitspflichten bei (der Kommunikation mit) dem Bundesaufsichtsamt für das Kreditwesen (siehe z. B. [Gri00, §9 KWG (Kreditwesengesetz), Seite 10 ff.] oder [Gri00, §8 WpHG (Wertpapierhandelsgesetz), Seite 280 ff.], sind hierbei insbesondere auch allgemeine rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr, wie z. B. [BGB01a], die EU-Direktive für elektronische Signaturen samt ihrer nationalen Umsetzungen (wie z. B. SigG in Deutschland [BGB01b] und Österreich [BGB00]), oder die Datenschutzgesetzgebung, z. B. im Bundesdatenschutzgesetz (BDSG), zu berücksichtigen.

- **Wirtschaftliche Aspekte**

- **Senkung der Transaktionskosten**

Um auch zukünftig im – durch technologische und rechtliche Entwicklungen – liberaleren Markt bestehen zu können, sind insbesondere auch Finanzdienstleister gezwungen, ihre Transaktionskosten zu senken. Hierbei ist es wichtig, dass ein ganzheitlicher Ansatz verfolgt wird, der unternehmensinterne und -externe Transaktionskosten senkt.

- **Erschließung neuer Geschäftsfelder**

Sind elektronische Schnittstellen für die Abwicklung von Transaktionen mit Kunden und Zulieferern vorhanden, so ist es ein konsequenter weiterer Schritt diese Plattformen zur Erschließung neuer Geschäftsfelder mit Mehrwertdiensten (z. B. in elektronischen Marktplätzen) zu nutzen.

- **Strategische Allianzen**

In kaum einem weiteren Segment sind Mergers & Acquisitions so häufig anzutreffen, wie im Finanzdienstleistungssektor. Außerdem gewinnen – insbesondere im Hinblick auf den prognostizierten Markt im mobilen Handel – strategische Partnerschaften zwischen Finanzdienstleistern und Telekommunikationsunternehmen zunehmend an Bedeutung. Dies impliziert, dass IT-Infrastrukturen und insbesondere PKIs entsprechend flexibel sein müssen, damit leicht auf sich verändernde strategische Allianzen eingegangen werden kann.

- **Technologische Aspekte**

Um die oben skizzierten Anforderungen in der Praxis umsetzen zu können, sind deshalb folgende technologische Aspekte zu berücksichtigen:

- **Elektronische Schnittstellen**

Um Transaktionskosten senken zu können, müssen elektronische Schnittstellen zwischen den Hintergrundsystemen des Finanzdienstleisters und Kun-

den, Lieferanten und Partner zur Abwicklung von Geschäftstransaktionen zur Verfügung gestellt werden. Im Hinblick auf die rasante technologische Entwicklung sollten die Front-Ends dieser Schnittstellen leicht austauschbar sein. Beispielsweise sollte bereits jetzt den erwarteten Entwicklungen im mobilen Handel Rechnung getragen werden.

– **Angemessene Sicherheitsmechanismen**

Diese Öffnung des Unternehmens gegenüber dem Markt setzt entsprechende Sicherheitsmechanismen, wie z. B. den Einsatz von Zertifikaten zur Verschlüsselung und elektronischen Signatur, zwingend voraus. Da die – oft vertrauliche – Geschäftskorrespondenz zukünftig verstärkt elektronisch, z. B. via E-Mail, abgewickelt wird, sind hier entsprechende E-Mail-Sicherheitsmechanismen vorzusehen. Werden Verträge ausschließlich elektronisch geschlossen, so ist die Signaturgesetzgebung samt damit verbundenen Haftungsregelungen zu beachten. Da nicht alle Anwendungen das gleiche Sicherheitsbedürfnis haben, bedeutet dies für die PKI, dass möglicherweise mehrere Vertrauensstufen zu berücksichtigen sind.

– **Skalierbarkeit und einfache Administration**

Durch die zunehmende elektronische Abwicklung der Geschäftsprozesse ist darauf zu achten, dass die gesamte IT-Infrastruktur, und dadurch auch die PKI, in der Lage ist, steigende Benutzerzahlen und eine Vielzahl neu geschaffener Anwendungen verwalten zu können. Deshalb ist in langfristiger Perspektive ein Single-Sign-On-artiger Mechanismus unumgänglich.

3.2 Zertifikatsbasierte Anwendungen für Finanzdienstleister

In diesem Abschnitt werden typische zertifikatsbasierte Anwendungen für Finanzdienstleister skizziert, die bei der Auswahl einer geeigneten PKI möglicherweise zu berücksichtigen sind.

Wir unterscheiden zwischen Basisanwendungen (Abschnitt 3.2.1), wie sie auch außerhalb des Finanzdienstleistungssektors anzutreffen sind, und finanzspezifische Anwendungen. Zu den letzteren gehören konventionelle bank- oder versicherungsspezifische Anwendungen (Abschnitt 3.2.2), wie sie heute bereits (oft noch papiergebunden) vorhanden sind und Mehrwertdienste (Abschnitt 3.2.3), die erst durch die elektronische Abwicklung möglich, bzw. für den Finanzdienstleister zugänglich, werden. Diese Mehrwertdienste sind für Finanzdienstleister von herausragender strategischer Bedeutung, da sie den Finanzdienstleister in das Zentrum der Wertschöpfungskette seiner Kunden rücken.

3.2.1 Basisanwendungen

In diesem Abschnitt werden zertifikatsbasierte Basisanwendungen angesprochen, wie sie auch außerhalb des Finanzdienstleistungssektors anzutreffen sind.

- **E-Mail-Sicherheit (B-1)**

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

wichtigsten Einsatzgebieten von PKIs. Das benötigte Sicherheitsniveau entspricht, wie auch bei den folgenden Anwendungsbeispielen, dem der kommunizierten Daten und kann damit u.U. sehr hoch sein.

- **Datei-Verschlüsselung (B-2)**

Neben dem Schutz der Daten während der Übertragung, kann es auch wichtig sein besonders sensible Daten lediglich verschlüsselt zu speichern. Hier kann man zwischen lokaler Dateiverschlüsselung und transparenter Dateiverschlüsselung gesamter Netzwerklaufwerke unterscheiden. Somit können leicht entsprechende Vertraulichkeitsanforderungen, z.B. aus dem Bankgeheimnis [Gri00, „AGB Banken – Grundregeln für die Beziehung zwischen Kunde und Bank“, Seite 427], auch für Aussen dienstmitarbeiter erfüllt werden.

- **Workflow-Signatures (B-3)**

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

- **Virtual Private Networks (B-4)**

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

- **Sichere Client-Server Kommunikation (B-5)**

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

- **Single Sign-On (B-6)**

Allgemeiner ist häufig – insbesondere bei heterogenen System- und Anwendungsstrukturen – eine einmalige Authentifizierung eines Benutzers angestrebt. Hier hilft eine PKI (in Verbindung mit entsprechenden Verzeichnis- und Rechteverwaltungsstrukturen) Zeit zu sparen. Dies gilt nicht nur für den Benutzer, sondern insbeson-

dere auch für die Administratoren. Ausserdem lassen sich somit unternehmensweite Security Policies leichter durchsetzen.

- **Zusatzanwendungen bei Chipkarten-Einsatz**

Verwendet man zum Speichern der privaten Schlüssel Hardware-Token (z. B. Smartcards), lassen sich damit weitere Systeme einführen oder migrieren, die diese nutzen. Während diese Systeme, z.B. zur **Bezahlung (B-7)** oder zur physikalischen **Zutrittskontrolle (B-8)** und **Zeiterfassung (B-9)**, nicht direkt die PKI verwenden, so verbessern sie die Akzeptanz und das Sicherheitsbewusstsein der Nutzer.

3.2.2 Konventionelle finanzspezifische Anwendungen

In diesem Abschnitt werden einige konventionelle bank- oder versicherungsspezifische Anwendungen aufgelistet, die beim Aufbau der PKI berücksichtigt werden sollten.

- **Kontoverwaltung (K-1)**

Bei der Kontoverwaltung können Zertifikate z.B. anstatt einer PIN zur Zugangsberechtigung eingesetzt werden. Da bei der Kontoverwaltung [AH99, VD00] u.U. sehr werthaltige Transaktionen möglich sind und eine Revisionsicherheit erwünscht ist, empfiehlt sich der Einsatz von nachrichtengebundenen Sicherheitsmechanismen, wie digitalen Signaturen.

- **Wertpapierhandel (K-2)**

Beim Wertpapierhandel spielt – aufgrund der Zeitkomponente und gesetzlichen Anforderungen – die Revisionsicherheit eine noch wichtigere Rolle. Hier können neben Zertifikaten z.B. auch Zeitstempeldienste zum Einsatz kommen.

- **Bereitstellung von Kursinformationen (K-3)**

Ein zusätzlicher, in der Regel nicht völlig kostenloser, Service für Wertpapierkunden ist die Bereitstellung von Kursinformation in Echtzeit. Während bei vielen Finanzportalen keine Gewähr für die Integrität der Daten übernommen wird und die Gebühren für diesen Dienst sehr moderat sind, könnte eine Zusatzleistung darin bestehen – gegen höhere Gebühren – Kursinformationen mit einer höheren Güte, signiert und zeitgestempelt anzubieten.

- **Elektronische Bankauskunft (K-4)**

Bei der Erstellung einer elektronischen Bankauskunft für einen Kunden können Zertifikate, und ggf. entsprechend zuverlässige Zeitstempel, zum Einsatz kommen.

- **Kreditgeschäft (K-5)**

Für den Abschluß von Verbraucherkrediten (siehe § 4, VerbrKrG, z. B. in [Gri00, Seite 207 ff.]) fordert der Gesetzgeber die Schriftform. Desweiteren ist in diesem Zusammenhang an das öffentliche Anbieten entsprechend sicherer Rating-Informationen zu denken, die flexiblere Kreditvergaben, z.B. im Zusammenhang mit dem elektronischen Handel, erlauben.

- **Versicherungsverträge (K-6)**

Während der Gesetzgeber beim Abschluß von Versicherungsverträgen nicht explizit die Schriftform erfordert, so sollten bei vollständig elektronischen Prozessen – der erhöhten Beweiskraft wegen – signaturgesetzkonforme Zertifikate, und ggf. Zeitstempel, zum Einsatz kommen. Ausserdem können durch den Einsatz von Zertifikaten auch im elektronischen Handel sehr dynamisch Zusatzversicherungen abgeschlossen werden.

- **Leasing (K-7)**

Neben dem zertifikatsbasierten Zugang zu Leasing-Portalen kann die PKI auch für den Vertragsabschluss (siehe Versicherungsverträge) eingesetzt werden.

- **Akkreditivgeschäft (K-8)**

Hier ist es denkbar, dass Akkreditive mit elektronischer Signatur eröffnet werden können. Das Akkreditiv ist hier wiederum wie ein (formfreier) Vertrag zu behandeln. Grosses Potential für diese Anwendung darf insbesondere in Verbindung mit offenen elektronischen Marktplätzen erwartet werden. Inwieweit das papiergebundene Akkreditiv mit den auf Marktplätzen verwendeten Zahlungsmechanismen und Zusatzleistungen (z.B. Versicherungen) vereint werden kann, bleibt abzuwarten.

- **Fremdwährungsverwaltung (K-9)**

Hier können Zertifikate zum Zugang zum Continuous Link Settlement (CLS-) System der Bank eingesetzt werden. Das typischerweise sehr hohe Transaktionsvolumen impliziert hohe Sicherheitsanforderungen.

- **Bankrechtlich vorgeschriebene Meldungen (K-10)**

Mit Zertifikaten können beispielsweise die Meldungen an die Aufsichtsbehörden für das Kreditwesen (z.B. in Deutschland das BAKred) gesichert werden. Der Vorteil hierfür liegt insbesondere in der Straffung der entsprechenden Prozesse, was Kosteneinsparungen nach sich zieht.

- **Inter-Bank-Clearing (K-11)**

Beim Zahlungsverkehrsclearing zwischen den Banken und entsprechenden (Landes-) Zentralbanken oder weiteren Dienstleistern, wie S.W.I.F.T. werden Zertifikate für die Absicherung der Verbindungen verwendet.

- **Treuhand-Dienstleistung (K-12)**

Treuhand-Konten kommen heute bei elektronischen Marktplätzen, im Wesentlichen aus Ermangelung maßgeschneiderter elektronischer Zahlungsmechanismen, zum Einsatz. Die Treuhand-Funktionalität ist häufig ein Teil der Kontoverwaltungssysteme.

3.2.3 Mehrwertdienste

In diesem Abschnitt werden Einsatzmöglichkeiten von Zertifikaten bei Mehrwertdiensten skizziert. Die eigentlichen Kerntransaktionen finden hier zwischen Kunden selbst statt. Ausnahmen ergeben sich, wenn die Bank, z.B. beim Betrieb einer eigenen Einkaufsplattformen, selbst in der Rolle des Nachfragers auftritt.

- **Einkaufsplattformen und Marktplätze (M-1)**

Hier kommen Zertifikate typischerweise zur System-Zugangskontrolle und für revisionssichere Transaktionen, z.B. bei Bestellvorgängen, zum Einsatz. Oft werden im Rahmen von Einkaufsplattformen und Marktplätzen auch weitere, z.B. Zahlungs- und Versicherungs-, Dienstleistungen angeboten. Ausserdem können Zertifikate bei komplexeren Supply-Chain-Management-Systemen zum Einsatz kommen.

- **Elektronische Rechnungsstellung, Bezahlung und Archivierung (M-2)**

Hier präsentiert der Finanzdienstleister seinen Kunden von anderen Unternehmen elektronisch erhaltene Rechnungen, die über integrierte Zahlungs- oder Kontoverwaltungssysteme beglichen werden können. Zertifikate kommen in der Regel bei der Systemzugangskontrolle und zur Absicherung der Dokumente und Transaktionen selbst zum Einsatz. Auf Kundenseite führt dies sowohl zu einer Kostenersparnis gegenüber dem Papierversand als auch zu einer Beschleunigung der betrieblichen Abläufe. Sich daran anschließende Vorgänge wie Zahlungsanweisungen und Protokollierung bzw. Archivierung des gesamten Vorgangs lassen sich in solche Systeme integrieren.

- **Elektronische Zahlung (M-3)**

In Einkaufsplattformen oder Marktplätzen können Zahlungen elektronisch erfolgen, wobei typischerweise die Zahlungsanweisungen signiert werden.

- **Versicherung finanzieller Risiken (M-4)**

Ausserdem kann die Zahlung mit zusätzlichen Leistungen, wie Zahlungsgarantien und der Versicherung von Währungsrisiken, verbunden werden.

- **Handels- und Transportversicherungen (M-5)**

Ausserdem können auch im Zusammenhang mit der logistischen Abwicklung einer Handelstransaktion auf elektronischen Marktplätzen entsprechende Zusatzversicherungen angeboten werden.

- **Trustcenter-Dienstleistung (M-6)**

Während in den vorhergegangenen Beispielen immer die Anwendungen im Vordergrund standen, ist auch die Trustcenter-Dienstleistung (rund um den „Verkauf von Zertifikaten“) selbst als Geschäftsfeld denkbar. Diese werden dann vom Kunden beispielsweise zur Sicherung seiner internen Prozesse (ähnlich der in Abschnitt 3.2.1 beschriebenen) eingesetzt, im einfachsten Fall zur E-Mail-Verschlüsselung.

- **Notariats- und Zeitstempeldienste (M-7)**

Neben der Ausstellung von Zertifikaten können zusätzliche Beglaubigungs- und Überprüfungsdienstleistungen angeboten werden.

- **Mitteilungs-Dienstleistung (M-8)**

Hier wäre z.B. die verbindliche Übermittlung amtlicher Nachrichten, wie Ad-Hoc-Meldungen oder Steuererklärungen denkbar. Zertifikate würden hier insbesondere für Signatur und Verschlüsselung der Nachrichten eingesetzt.

4 Entscheidungshilfe zur Auswahl geeigneter PKI-Alternativen

Nachdem in Abschnitt 2 verschiedene PKI-Alternativen und in Abschnitt 3 verschiedene – strategische und anwendungsgetriebene – Anforderungen an eine PKI für Finanzdienstleister erörtert wurden, bleibt es diese beiden Gedankengänge zusammenzuführen und eine Methodik zu entwickeln, die Finanzdienstleistern bei der Wahl einer geeigneten PKI-Architektur unterstützen kann.

Hierfür gehen wir folgendermaßen vor: In Abschnitt 4.1 wird eine einfache Metrik entwickelt, die weiteren Schritten zur Auswahl geeigneter PKI-Alternativen zugrundeliegt. In Abschnitt 4.2 werden die in Abschnitt 3.2 skizzierten Anwendungen (schwerpunktmäßig) in dieses „Koordinatensystem“ eingeordnet und den typischen Anwendungsfeldern der in Abschnitt 2 skizzierten PKI-Alternativen gegenübergestellt.

4.1 PKI-Anforderungs-Metrik für Finanzdienstleister

Betrachtet man die oben skizzierten strategischen Anforderungen an eine PKI für Finanzdienstleister und insbesondere die in Abschnitt 3.2 aufgelisteten potentiell relevanten Anwendungen, so unterscheiden sich die daraus erwachsenden Anforderungen im Wesentlichen in zwei Aspekten. Zum einen kann danach unterschieden werden, welche

- **Kommunikationspartner**

typischerweise an den Transaktionen beteiligt sind und welches

- **Sicherheitsniveau**

die jeweiligen Anwendungen benötigen.

Demnach können die Anforderungen an eine PKI für Finanzdienstleister bezüglich eines Koordinatensystemes – mit den Achsen „Kommunikationspartner“ und „Sicherheitsniveau“ betrachtet werden.

4.1.1 x-Achse – Kommunikationspartner

Bei den zertifikatsbasierten Anwendungen kann aus Sicht der Finanzdienstleister zwischen interner Kommunikation und Kommunikation mit Kunden unterschieden werden. Zunehmend werden auch Prozesse der Kunden untereinander interessant, an denen die Finanzdienstleister nur indirekt, beispielsweise als Trusted Third Party, beteiligt sind.

- **Finanzdienstleister-intern**

Hierunter fallen alle Prozesse und Transaktionen, bei denen ausschließlich interne Kommunikationspartner und Systeme eingebunden sind. Die Grenzen zwischen interner und externer Kommunikation sind dort fließend, wo die betreffenden Unternehmen in Konzernstrukturen eingebunden sind.

- **Finanzdienstleister–Kunde/Geschäftspartner**

Hier handelt es sich um das eigentliche Geschäftsgebiet des Finanzdienstleisters. Dazu zählt beispielsweise das Home-Banking für Privatkunden, z. B. mit HBCI [AH99], oder der elektronische Datenaustausch mit Geschäftskunden und Partnern, z. B. über EBCI oder andere Clearing-Schnittstellen [VD00].

- **Mehrwertdienste: Kunde – Kunde**

Bei den Mehrwertdiensten ist die Bank nicht mehr direkt an den Transaktionen beteiligt. Die Kunden nutzen jedoch das jeweils existierende Vertrauensverhältnis zur – idealerweise jeweils eigenen – Bank um sicher miteinander zu kommunizieren und Transaktionen abzuwickeln. Die Beteiligung des Finanzdienstleisters an dieser Stelle ist sinnvoll, da im Laufe der Geschäftsabwicklung der Kunden untereinander auch eine Kommunikation mit der Bank stattfindet, sei es zur Prüfung der Zahlungsfähigkeit oder bei der Zahlung selbst. In diesem Bereich existiert ein großes strategisches Potenzial für die Finanzdienstleister zur Erschließung neuer Geschäftsfelder. Beispielsweise scheint die Identrus-PKI, die neben Transaktionen zwischen Banken und Geschäftskunden oder Partnern auch eine Vertrauensinfrastruktur für B2B-Marktplätze bietet, von großer Bedeutung zu sein.

4.1.2 y-Achse – Sicherheitsniveau

Neben den beteiligten Partnern spielt auch die Klassifizierung der Informationen hinsichtlich ihres Schutzbedarfs eine wichtige Rolle. Üblicherweise definiert man die vier Sicherheitsniveaus „niedrig“, „mittel“, „hoch“ und „sehr hoch“, in die die einzelnen Transaktionen eingeteilt werden können.

Die Aufteilung erfolgt anhand der Auswirkungen im Falle einer Beeinträchtigung der Sicherheit. Hierbei können folgende Kriterien bewertet werden:

- Finanzielle Konsequenzen
- Verstoß gegen Gesetze, Vorschriften und Verträge
- Beeinträchtigung der Geschäftsprozesse
- Negative Innen- bzw. Außenwirkung
- Beeinträchtigung der informationellen Selbstbestimmung
- Beeinträchtigung der persönlichen Unversehrtheit

Die vier Sicherheitsniveaus können, z. B. in Bezug auf finanzielle und rechtliche Konsequenzen, folgendermaßen definiert werden:

- **niedrig**
Die Transaktionen sind nicht, oder kaum, werthaltig. Eine Veröffentlichung der mit der Transaktion verbundenen Informationen bedeutet keinen Verstoß gegen rechtliche Vorschriften.
- **mittel**
Die Transaktionen beinhalten einen relativ geringen Wert. Die zugehörigen Informationen sind aber bereits, z. B. aufgrund von AGBs, vertraulich zu behandeln.
- **hoch**
Der Wert der Transaktion ist relativ hoch, aber dennoch wertmäßig begrenzt. Ein Verstoß gegen rechtliche Vorschriften würde zu moderaten rechtlichen und damit auch finanziellen Konsequenzen führen.
- **sehr hoch**
Der Wert typischer Transaktionen ist sehr hoch und / oder nicht durch konventionelle Verträge zwischen den beteiligten Geschäftspartnern abgesichert. Somit könnten

Probleme bei diesen Transaktionen zu erheblichen rechtlichen und finanziellen – ggf. bis hin zu essentiell bedrohlichen – Konsequenzen führen.

4.2 Einordnung typischer Anwendungen in Metrik

In Abbildung 1 findet sich die Einordnung der in Abschnitt 3.2 gelisteten Anwendungen.

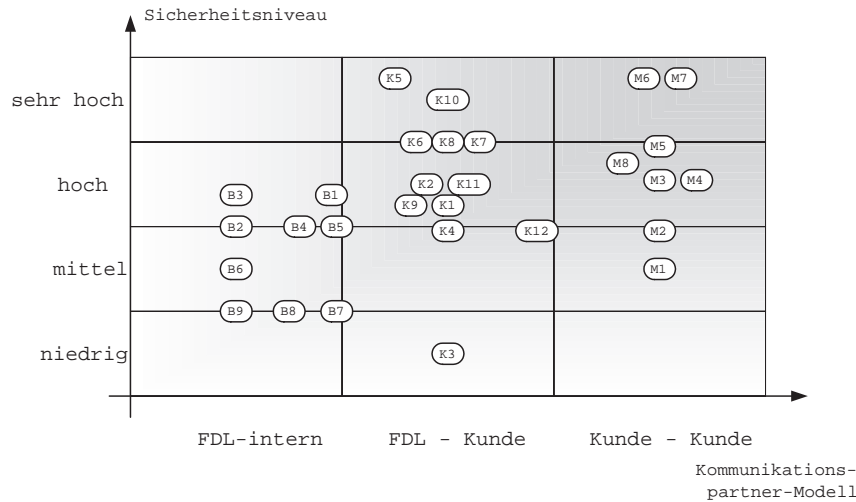


Abbildung 1: Einordnung typischer zertifikatsbasierter Anwendungen

Es sei angemerkt, dass diese Einordnung das „schwerpunktmäßige“ Anwendungsgebiet widerspiegelt. Im Einzelfall kann das Einsatzgebiet von diesem Schwerpunkt abweichen.

4.3 Welche PKI-Alternative sollte gewählt werden?

In diesem Abschnitt wird schließlich auf die zentrale Frage eingegangen, welche PKI-Alternative bei welchen Anforderungen gewählt werden sollte.

In Abbildung 2 ist das typische Anwendungsspektrum der verschiedenen PKI-Alternativen den vorher eingeordneten Anwendungen gegenübergestellt. Auch hier ist lediglich der „Anwendungsschwerpunkt“ der jeweiligen PKI-Ausprägung angegeben, der im Einzelfall von der hier gebrachten Darstellung abweichen kann. So *könnten* – aus technischer Perspektive – signaturgesetzkonforme Zertifikate selbstverständlich für die Implementierung einer internen Single-Sign-On-Plattform verwendet werden. Allerdings sprächen hier z.B. Kostenaspekte gegen eine solche Lösung.

Mit einer so erfolgten Zuordnung kann ein Finanzdienstleister erkennen, welche PKI-Alternative für ihn möglicherweise „die Richtige“ ist. Ausserdem sei angemerkt, dass der Begriff „Alternative“ hier keinen exklusiven Charakter hat. So ergänzt sich beispielsweise eine interne PKI ideal mit der Bridge-CA-Initiative.

Schliesslich werden führende Finanzdienstleister, aufgrund vielfältiger Anforderungen, nicht umhinkommen ein maßgeschneidertes System zu implementieren, dass mehrere der hier vorgestellten Varianten verbindet. Diese Aspekte müssen im Einzelfall – oft mit Unterstützung durch erfahrene Berater – untersucht werden.

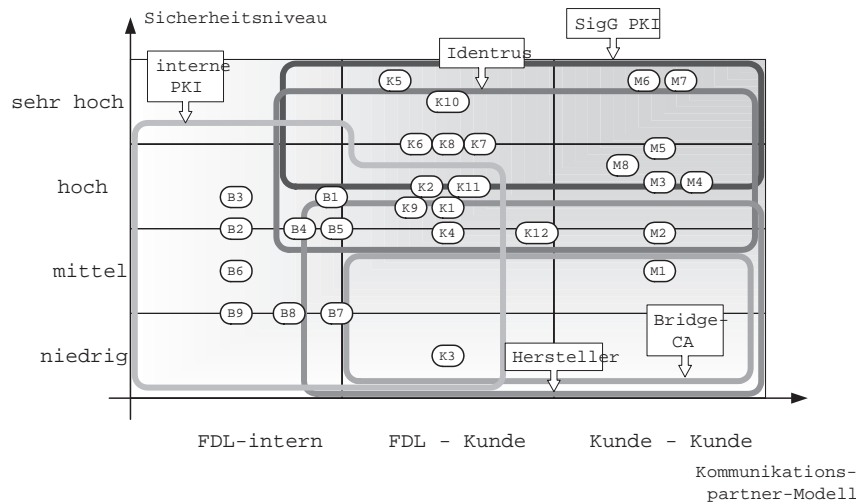


Abbildung 2: Welche PKI-Alternative für welche Anforderungen?

Literatur

- [AH99] ALGESHEIMER, René ; HÜHNLEIN, Detlef: HBCI - Eine sichere Plattform nicht nur für Homebanking. **In:** HORSTER, P. (Hrsg.): *Tagungsband Sicherheitsinfrastrukturen*, Vieweg, 1999
- [BGB00] BGBL.: Signaturgesetz (Österreich). BGBl. I (2000), Nr. Nr. 137/2000. – <http://www.signatur.tkc.at/de/legal/sigg.html>
- [BGB01a] BGBL.: Entwurf eines Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr (Elektronischer Geschäftsverkehr-Gesetz - EGG). (2001). – <http://www.dud.de/dud/documents/egg-e-0102.pdf>
- [BGB01b] BGBL.: Gesetz über elektronische Signaturen (Signaturgesetz - SigG). **In:** *Gesetz über elektronische Signaturen und zur Änderung weiterer Vorschriften* Bd. Artikel 1. Bd. Artikel 1, 2001. – <http://www.dud.de/dud/documents/sigg010215.pdf>
- [Büh00] BÜHREN, Hubert W.: *Anwaltspraxis, Handbuch Versicherungsrecht*. Bonn : Deutscher Anwaltsverlag, 2000. – ISBN: 3824003732
- [Coa88] COASE, Ronald H.: The Nature of the Firm: Origin. **In:** *Journal of Law, Economics, and Organization* 4 (1988), Nr. 3
- [EH01] ESSLINGER, Bernhard ; HÜHNLEIN, Detlef: Global Secure E-Mail Interoperability - The Europe-based Bridge-CA initiative. **In:** HORSTER, P. (Hrsg.): *Tagungsband „Elektronische Geschäftsprozesse“*, Vieweg Verlag, 2001
- [Ess00] ESSLINGER, Bernhard: IDENTRUS: a global digital identity verification network for business transactions building the basis for world-wide trust on the internet. **In:** *Tagungsband ISSE*. Barcelona, 2000

- [Gri00] GRILL, Hannelore: *Bankrecht für Auszubildende. Gesetze. Verordnungen. Abkommen. Geschäftsbedingungen. (Lernmaterialien)*. 18. Auflage. Regensburg : Walhalla, 2000. – ISBN: 3802951166
- [Hüh01] HÜHNLEIN, Detlef: Identrus-enabled applications. **In:** HORSTER, P. (Hrsg.): *Tagungsband „Elektronische Geschäftsprozesse“*, Vieweg Verlag, 2001
- [HZ01] HAAS, S. ; ZEINDL, S.: Identrus - eine globale Sicherheitsinfrastruktur auf der Basis von digitalen Zertifikaten. **In:** HORSTER, P. (Hrsg.): *Tagungsband „Elektronische Geschäftsprozesse“*, Vieweg Verlag, 2001
- [Ide01] IDENTRUS: Identrus-Homepage. (2001). – <http://www.identrus.com>
- [VD00] VELDE, Christian ; DRÄGER, Uwe: S-Clearing sorgt für einen Effizienzschub. **In:** *Sparkassenorganisation - Betriebswirtschaftliche Blätter* (2000), Februar