

Zukünftige Verbreitung der Digitalen Signatur in Geschäftsprozessen - Ergebnisse einer Delphi-Studie

Michael Gaude

Daimler AG
71059 Sindelfingen
Michael.Gaude@Daimler.com

Abstract: Dieser Artikel liefert einen Beitrag für die Innovationsforschung bzgl. der Digitalen Signatur und deren Einsatz in Geschäftsprozessen. Die Digitale Signatur wird allgemein als die Grundlage für verbindliche Authentifizierung und sichere Transaktionen in der modernen Internetökonomie angesehen. Sie ermöglicht den beweiswürdigen Ersatz der eigenhändigen Unterschrift. Für den Einsatz einer beweiswürdigen Digitalen Signatur wird eine spezielle Infrastruktur, die Public Key Infrastructure (PKI) benötigt. Insbesondere Großunternehmen stehen heute vor einer Investitionsentscheidung in diese Technologie. Im Artikel wird der Nutzenbeitrag der PKI für Geschäftsprozesse modelliert. Anhand der Ergebnisse einer Experten-Delphi-Studie mit 69 Experten wird das Modell mit Realdaten befüllt und einer Kalibrierung unterworfen. Das Studienpanel besteht zu je einem Drittel aus Nutzern, Anbietern und Wissenschaftlern. Alle Teilnehmer sind ausgewiesene Experten in ihrem Gebiet und haben die Studienfragen zweimal bearbeitet, erweitert und kommentiert.

1 Einleitung und Motivation

Durch den globalisierten Wettbewerb entsteht für die Akteure der freien Wirtschaft ein starker Druck ihre Produkte und Dienstleistungen schnell den Anforderungen der unterschiedlichen Märkte anzupassen. In diesem Szenario kommt der sicheren Kommunikation und den agilen Transaktionen zwischen den Teilnehmern der Development- und Supply-Chains eine zentrale Bedeutung zu [Du01, CH+03, KK05, SW01].

Die grundlegende IT-Technologie für diese anspruchsvollen Netzwerktransaktionen ist die Public Key Infrastructure (PKI) [KLP05]. Mittels einer PKI werden die grundlegenden Anforderungen an nachvollziehbare und sichere Kommunikation sowie an sichere und authentische Transaktionen erfüllt. PKIs mit höchster Qualität erlauben die Erzeugung von qualifizierten Signaturen und damit die Erstellung von beweiswürdigen Verträgen und Dokumenten aller Art. Zudem ist eine PKI die Grundlage für die effiziente Authentifikation in offenen Netzwerken. Die qualifizierte elektronische Signatur ist in Deutschland und vielen anderen europäischen und außereuropäischen Ländern der eigenhändigen Unterschrift gleichgestellt [He04].

In deutschen Unternehmen ist die Nutzung von PKI-Technologien und -Diensten nicht weit verbreitet. Stand heute wird auch bei staatlichen Stellen und Bürgern ebenfalls nur eine sehr geringe Verbreitung der Nutzung von elektronischen Signaturen in Geschäftsprozessen beobachtet, wenngleich viele Einzelprojekte gestartet wurden [GS+04, LiMM06]. Weiterhin besteht Ungewissheit bzgl. der zukünftigen Verfügbarkeit und Verbreitung von PKI-Diensten in Deutschland, in Europa sowie im gesamten globalen ökonomischen System. Dies wäre aber gerade für international agierende Unternehmen, wie z.B. die Automobil-, Pharma- oder Luftfahrtindustrie, ein wichtiger Faktor bei der Ausgestaltung ihrer IT-Strategie [Ec05].

Ein offener Punkt der wissenschaftlichen Betrachtung der PKI-Technologie ist die innovationstheoretische Analyse der relevanten Einflussfaktoren auf die PKI-Diffusion. Dabei stellt insbesondere die Untersuchung der Potenziale der Digitalen Signatur in Geschäftsprozessen mittels wissenschaftlichen Methoden ein offenes Feld dar.

Dieser Beitrag stellt ein Modell für die Nutzung von PKI-Diensten in Geschäftsprozessen auf und zeigt wie eine Potenzialzuschreibung mittels einer Experten-Delphi-Studie geschehen kann. Als zentrales Forschungsergebnis werden die auf einer Delphi-Studie beruhenden Abschätzungen des Potenzials der PKI-Technologie in Prozessen dargestellt.

2 Ausgangssituation und Definitionen

Im Folgenden werden die zentralen Begriffe dieser Arbeit, die PKI-Technologie, die Innovationstheorie und die Geschäftsprozesspotenziale der PKI-Technologie, erläutert.

2.1 Elektronische Signatur und die Infrastruktur für öffentliche Schlüssel

Die PKI Technologie versetzt uns in die Lage, die eigenhändige Unterschrift durch eine gleichwertige, elektronische Signatur zu ersetzen. Damit besteht die Möglichkeit nahezu alle bekannten, papierbasierten und auch juristisch beweisrelevanten Vorgänge zu virtualisieren und damit alle bekannten Vorteile der Virtualisierung nutzbar zu machen [He04].

Die englischsprachige Abkürzung PKI bedeutet Public Key Infrastructure und bezeichnet generell die Infrastruktur, die nötig ist, um die Verteilung von öffentlichen Schlüsseln von Personen oder Organisationen zu gewährleisten. Die sichere Verteilung von öffentlichen Schlüsseln der Kommunikationspartner ist wiederum die Grundlage für eine flächendeckende Nutzung der elektronischen Signatur.

Die PKI-Dienste "Erstellen einer elektronischen Signatur", "Verschlüsseln" und "Zeitstempel" stellen die Basis für elektronische Verhandlungen und Vereinbarungen in virtualisierten, papierlosen und globalen Geschäftsprozessen dar [SR04, Sc05]. Davon betroffen sind einfache wie auch komplexe Geschäftstransaktionen bis hin zu Kooperationsverhandlungen und Rahmenverträgen. Um die oben genannten Dienste rechtsverbindlich und im technologischen Kontext korrekt durchzuführen, müssen vom Benutzer

weitere PKI-Dienste in Anspruch genommen werden. Dies sind die "Registrierung bei einem Zertifikatsdiensteanbieter" und die "Verzeichnisabfragen mit Zertifikatsprüfung", um Vertrags- und Kommunikationspartner verlässlich und beweismäßig zu identifizieren. Für die Erstellung einer qualifizierten Signatur wird eine spezielle Hardware benötigt, um die PKI-Dienste zu nutzen (SmartCard und Kartenleser, ggf. Biometrie). Weiterhin sind gesetzliche Regulierungen zur Ausführung und Konfiguration einer PKI für sogenannte qualifizierte Signaturen zu beachten. In Deutschland bildet diese gesetzliche Grundlage das Signaturgesetz (SigG). Die drei Elemente *Dienste*, *Technik* und *Regulierungen* werden im folgenden PKI-Technologie genannt.

Die Dienste einer PKI können auf allen Ebenen von Geschäftsprozessen zum Einsatz kommen. Dies beginnt bei der sicheren Kommunikation mittels SSL und wird fortgesetzt mit z.B. den Sicherheitsmechanismen von Modellierungsmethoden für Geschäftstransaktionen, wie ebXML oder Web Services [HH04]. Danach folgen personengebundene, einfache Signaturen auf elektronischen Dokumenten des gewöhnlichen Geschäftsverkehrs, bishin schließlich zu qualifizierten Signaturen auf beweismäßigen Vertragsdokumenten mit langjährigen Archivierungspflichten.

2.2 Die PKI Technologie als Gegenstand der Innovationsforschung

Bewährte Modelle des Innovationsmanagements beschreiben die Entstehung, den Einsatz und die Verbreitung von Neuerungen als Grundelemente des technischen Fortschritts. Die Grundbegriffe dieser Modelle sind: Invention, Innovation und Diffusion [Ro95]. Im Bereich der PKI-Technologie hat die Inventionsphase, also die Phase der Entwicklung neuer Ideen, einen sehr ausgereiften Entwicklungsstand erreicht. Die wichtigsten Inventionen hinter der PKI-Technologie sind die Entwicklung der asymmetrischen Kryptographie sowie die juristische Gleichstellung der eigenhändigen Unterschrift. Der Stand der Innovation weist allgemein einen ausbaufähigen Stand auf. Der Stand der Diffusion, also der Verbreitung der PKI in Märkte, wird allgemein als sehr gering angesehen [POL05].

Wenn sich eine Technologie wie die PKI in Märkten verbreiten soll, müssen viele Individuen eine Entscheidung für den Erwerb der nötigen Hard- und Software inkl. den Zertifikaten treffen. Der Vorgang wird Adoption genannt. Es schließt sich danach eine länger andauernde Phase der Nutzung der PKI-Technologie an. Während dieser Phase wird die PKI-Technologie für verschiedene Geschäftstransaktionen benutzt, sie wird im übertragenen Sinne von den Geschäftsprozessen adoptiert. Die PKI-Technologie kann daher als eine technologische Nutzungsinnovation bezeichnet werden [ABH01].

Die aggregierte Betrachtung vieler Adoptionsprozesse wird als Technologie-Diffusion bezeichnet und wird im Rahmen der Diffusionstheorie beschrieben. Das wichtigste dynamische Modell ist in diesem Gebiet die sog. Diffusionskurve, welche den Verbreitungsgrad einer Technologie über den Zeitablauf beschreibt [Ro95].

3. Ergebnisse: Nutzenpotenziale für Geschäftsprozesse

3.1 Konzeptioneller Rahmen der Studie

Die Diffusion der PKI-Technologie kann modellhaft als eine Nutzungsverbreitung der Digitalen Signatur über verschiedene Ebenen verstanden werden. Die PKI-Technologie wird in einem ersten Schritt von Sekundärtechnologien, wie Laptops und Handy, vereinnahmt (Ebene 1). Danach kommen die Sekundärtechnologien innerhalb von Geschäftsprozessen zum Einsatz (Ebene 2). Die Geschäftsprozesse wiederum werden von verschiedenen Nutzerpopulationen realisiert (Ebene 3). Verschiedene Populationen bilden schließlich Branchen und Märkte (Ebene 4). So kann von einer Diffusionsbewegung der PKI-Technologie in Branchen und Märkte gesprochen werden [Ga07].

3.2 Analysemethode Delphi-Studie: Ermittlung der PKI-Affinität zu Prozessen

Für die Prognose diffuser Sachverhalte im Bereich von PKI-Diensten lässt sich das Forschungsinstrument der Delphi-Studie anwenden. In einem mehrstufigen Befragungsprozess werden dabei Experten über ihre persönlichen Einschätzungen zu Entwicklungen in ihren jeweiligen Expertengebieten befragt. Die Total-Design-Methode und die Facetten-theorie beschreiben dabei, wie die einzelnen Themenkomplexe zu einem Fragebogen mit einfachen Multiple-Choice Fragen heruntergebrochen werden können [Hä02, Di78].

Eine Delphi-Studie verläuft in mehreren Runden. In der Initialrunde werden die ersten Einschätzungen sowie die Kommentare der Experten aufgenommen. In den folgenden Feedbackrunden bekommen die Experten die Gelegenheit, ihre Erstmeinung unter dem Eindruck der Kommentare und der Schätzungen der anderen Experten zu verändern. Ziel der Feedbackrunden ist eine Verbesserung der inhaltlichen Abdeckung und eine Konvergenz der Einschätzungen der Experten. Bereits eine Anzahl von 15-20 Experten wird dabei bereits als eine wissenschaftlich valide Grundlage angesehen [Hä02].

In der von mir durchgeführten Delphi-Studie wurden alle Ebenen mittels Facettenfragen modelliert und von 69 Experten mit Schätzwerten über Potenziale und zukünftige Entwicklungen befüllt.

Insgesamt sind in 7 großen Themenkomplexen 254 Fragestellungen beinhaltet. Darin finden sich zusammen 629 Facettenfragen mit insgesamt 2894 Antwortmöglichkeiten. Der Bereich der Prozessanalyse umfasst 42 Facettenfragen zu ebensovielen Prozessen. Die durchschnittliche Antwortquote über alle Fragestellungen lag bei 87% der Teilnehmer. D.h. dass nur 13% der Teilnehmer eine Fragestellung ungültig oder mit "Keine Angabe" beantwortet haben. Die Mortalitätsquote in der Feedbackrunde lag bei durchschnittlich 29%, d.h. alle Fragestellungen wurden von durchschnittlich 43 Teilnehmern (36 Teilnehmer der Vertiefungsstudie) zweimal bearbeitet. Die Facettenfragen, der in diesem Beitrag näher analysierten Prozessebene, wurden von 52 Teilnehmern zweimal bearbeitet.

Die Teilnehmer der PKI-Delphi-Studie rekrutieren sich zu je einem Drittel aus den Professionen: Wissenschaft, Nutzern und Anbietern und wurden selektiv mit der Maßgabe der besonderen Expertise im Gebiet der PKI-Technologie ausgewählt. Jeder Studienteilnehmer beantwortete in Kapitel 1 der Studie Fragen zu seiner konkreten theoretischen und praktischen Expertise im Bereich PKI. Anschließend gab er eine Selbsteinschätzung seines Theoriewissens und seines Praxiswissens ab. Die Ergebnisse dieser Fragen lassen darauf schließen, dass die Experten der Delphi-Studie hinreichend qualifiziert sind und dass die Ergebnisse der Studie einen belastbaren Stand erreichen können.

3.3 Ergebnisse im Detail

Die Teilnehmer der Studie wurden in Kapitel 3 der Gesamtstudie nach deren Einschätzung über 42 allgemeine Prozesse aus dem Bereich e-Commerce befragt. Die Zielsetzung hinter der Fragestellung ist die Abschätzung der Rentabilität der PKI-Technologie für heute existierende Geschäftsprozesse. Da "Rentabilität" für die Teilnehmer der Studie schwer zu schätzen wäre, wurde nach der Vorbedingung der Rentabilität, dem Nutzeneffekt allgemein, gefragt. Die Frage nach der Rentabilität wäre zwar diffusionstheoretisch interessanter, jedoch steht dem gegenüber die Erwägung, dass die nötige Erläuterung zum Konstrukt "Rentabilität" die Teilnehmer ggf. überfordert hätte oder zumindest deren Frustrationslevel während der Bearbeitung gesteigert hätte.

Abschluss von Kaufverträgen im Internet

3.1.1
 keine Angabe

Allgemein: (Formfreier) Abschluss von Kaufverträgen im Internet

PKI (Klasse 4) befreit den Prozess den Prozess
 (1)

kein Zusatznutzen
 (-) (2)

leichter Nutzeneffekt
 (+/-) (3)

klarer Vorteil mit PKI
 (++) (4)

ohne PKI (Klasse 4) geht hier gar nichts
 (+++) (5)

Kommentar: Ihr_neuer_Kommentar

(1) W Todd: Ein Vertrag entsteht bei 2 übereinstimmenden Willenserklärungen. Sichere Zertifikate haben nicht mit Formfreiheit zu tun.
 A Edwin: StG spielt hier keine Rolle, da keinerlei Unterschrift benötigt wird
 N Harry*: Bei qual. StG. Behinderung. Fortgeschrittene StG. gerügt oftmals

(2) W Eric: Funktioniert faktisch seit einem Jahrzehnt
 A Craig*: Was meint Klasse 4?
 N Tom*: Wer kauft schon online über E-Bay ein Haus?
 - Jeff*: Zusatznutzen primär für den Händler, für den Kunden nur beim Rechtsstreit

(3) W Evan*: für wen? Ein Prozess kann keinen Nutzen gewinnen!
 A Dick*: Nutzen steigt mit Höhe des Kaufwertes
 - Jose: Vorauskassa, Trendänder, Versicherungen helfen das Risiko auf beiden Seiten zu minimieren.
 - Jim: theoretischer Nutzen, Komplexität überfordert den Nutzer
 N Dustin: im B2C-Bereich keine Relevanz.
 - Russel: Wachsender Nutzen bei wachsender Nutzung und damit wachsendem Missbrauchspotential

(4) W Matt: Für alle nachfolgenden Gruppen gilt, dass der Anbieter nur dann mit Sicherheit seinen Vertragspartner identifizieren und die Gegenleistung erfordern kann, wenn Gewissheit über dessen Person und den Vertragsschluss besteht. Daher (++). Andernfalls wäre der Anbieter, der oft in Vorleistung tritt, im Zweifel beweispflichtig, was für ihn problematisch sein kann
 A Alan*: seit wann gibt es einen formfreien Kaufvertrag??? Es gibt die Formfreiheit von Verträgen/Vertragsfreiheit, wenn ich jedoch einen Kaufvertrag mache, muss ich mich für eine Form entscheiden: mündlich, elektronisch, Schriftlich etc. Sollte hier ein bestimmtes Ergebnis erwartet werden? - Ich gehe davon aus das hier die Textform gemeint ist, d.h. beispielsweise ein Webformular. Dies ist jedoch im Streitfall problematischer als die elektronische Form. So lange jedoch die Infrastruktur nicht vorhanden ist, wird es sinnvoller sein die Textform zu verwenden.
 N Al: durch Eindämmung von evtl. Betrugsfällen

Abbildung 2: Einschätzung der Wirkung einer PKI auf Abschluss von Verträgen

Daher wurden die Studienteilnehmer in genau einer Facettenfrage nach dem nutzenstiftenden Wert einer PKI in dem jeweiligen Prozess gefragt. Dabei war eine hypothetische Ausrüstung aller Prozessteilnehmer mit Hard- und Software für qualifizierte Signaturen anzunehmen. Zu einem gegebenen Prozess standen 5 Antwortfacetten bereit, aus der

eine zu wählen war. Zu jeder der 42 Fragen konnte zudem ein Kommentar abgegeben werden. In Abbildung 2 ist ein Auszug aus dem individualisierten MS-Word-Fragebogen eines Teilnehmers in der zweiten Runde zu sehen. Ziel der 2. Runde ist die Konvergenz der Expertenmeinungen. Dafür standen den Teilnehmern mehrere Hilfsmittel zur Verfügung.

1. Kennzeichnung der Stimmabgabe des jeweiligen Teilnehmers in Runde 1 durch Ausgrauung des Antwortfeldes.
2. Anschreibung der Absolutanzahl der gesetzten Kreuze je Antwortmöglichkeit und Visualisierung durch flächenäquivalente Kreisformen, um einen einfachen Vergleich der Absolutwerte zu ermöglichen.
3. Heraushebung der Stimmabgabe ausgewählter Teilnehmer durch "Sternchen". Durch Rangbildung nach den Kriterien Häufigkeit und Umfang von abgegebenen Kommentaren wurden die 10 rangbesten Teilnehmer als "Star" definiert. Es bestand die Annahme, dass die "Stars" die Studie mit besonderer Sorgfalt und Engagement bearbeitet haben und dass ggf. andere Experten sich für die Meinung dieser Personen interessieren würden.
4. Darstellung des gruppenspezifischen Antwortverhaltens. Für die Gruppe (W)issenschaftler (A)nbieder und (N)utzer wurden die jeweiligen Relativanteile an den Antworten durch höhenäquivalente Größendarstellung der Buchstaben W, A und N angezeigt. Es bestand die Annahme, dass die Meinungen der drei genannten Studiengruppen voneinander Abweichen und dass die Information über diese Abweichung meinungsbildend sei.
5. Möglichkeit zur Kommentierung der Antwort. In jeder Runde konnten die Teilnehmer einen freien Kommentar eingeben. Dieser Kommentar wurde häufig genutzt, um die eigene Stimmabgabe zu begründen. In der zusammenfassenden Darstellung der Kommentare wurden die Antworten daher mit einer Referenz zur gegebenen Antwort im Multiple-Choice-Bereich versehen. Die Kommentare wurden mit Pseudonymen versehen. Somit war die Verfolgung der Kommentierung eines Charakters möglich, ohne jedoch die Anonymität der Studie zu gefährden.

Unter dem Eindruck der 5 Hilfsmittel, hat der Teilnehmer, wie im Beispiel zu sehen ist, seine Meinung geändert und nun für "Klarer Vorteil mit PKI" votiert.

In den Schlussauswertungen können sowohl die Erstantwortbilder, als auch die Zweitantwortbilder, sowie auch ein Reihe von gruppenspezifischen Antwortbildern generiert werden. Dabei kommt eine Boxplotanzeige zum Einsatz, aus der der Mittelwert, die Standardabweichung (halbe Länge der Box), Median und Min-/Max-Werte zu erkennen sind. Abbildung 3 zeigt das Erstantwortbild zur Frage nach Kaufverträgen für das gesamte Teilnehmerfeld und stellt es dem Zweitantwortbild für die Gruppe der Wissenschaftler gegenüber. Durch grafische Korrelationsanalyse ist zu erkennen, dass drei Wissenschaftler ihre Meinungen geändert haben und die Ergebnisse für die Gruppe der Wissenschaftler damit tatsächlich konvergiert sind.

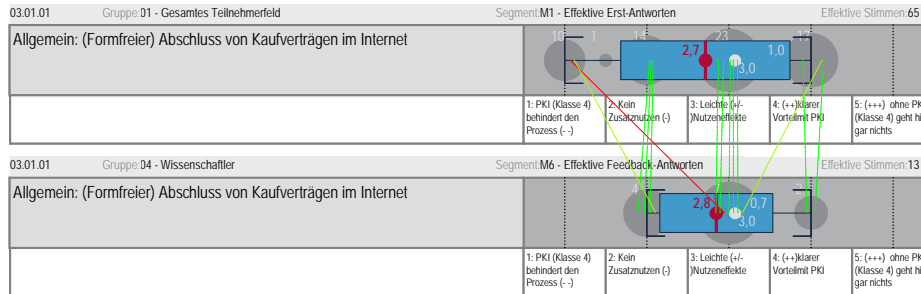


Abbildung 3: Boxplots, grafische Korrelationsanzeige und Gruppendifferenzanalyse

Eine weitere, graphische Clusteranalyse auf der Grundlage des Durchschnittswertes und der Standardabweichung der Facettenantworten unterteilt die 42 Prozesse in vier Bereiche mit einer klaren Aussage zum Nutzen einer PKI (A) und in zwei Bereiche mit indifferenten Antwortbildern (B) (vgl. Abb. 4). Im Folgenden werden die Bereiche und die dazugehörigen Kommentare der Teilnehmer vorgestellt und diskutiert.

A1 - PKI ohne Nutzen: Für den *Kauf von Medien* (P3), wie z.B. Bücher oder CDs, sowie den *Verkauf von reinen elektronischen Produkten* (P4), wie z.B. Software, Lieder und Videos, und sogar für den gesamten *Versandhandel* (P5) gilt: Diese Prozesse werden einhellig als nicht affin zu einer PKI gesehen. Als Gründe werden die starken und etablierten Bezahl- und Transaktionssysteme der Gegenwart angeführt. Auch die relativ geringen Kosten der gehandelten Produkte stünden in einem ungünstigen Verhältnis zu dem erwarteten PKI-Aufwand. Auch die heute schon weite Verbreitung der Prozesse ist als PKI-Hindernis zu sehen, da das Handling der PKI-Dienste nicht allen Internetbenutzern zugemutet werden könne. Positive Aspekte werden der PKI jedoch für diejenigen Teilprozesse ausgesprochen, welche einen Altersnachweis oder einen Nachweis der Geschäftsfähigkeit zwingend voraussetzen. Auch Copyright-Aspekte bei elektronischen Produkten wurden als positive Nutzeneffekte genannt. Vor dem Hintergrund von bereits etablierten Trustmodellen, die nicht auf PKIs basieren, werden die Geschäftsprozesse *Wareneingangsvereinnahmung* (P35), die *Bestands- und Kapazitätsabfragen beim Lieferanten* (P36) sowie die *Arbeitsplatzvermittlung* (P22) ebenfalls als nicht nutzenstiftend angesehen.

A2 - PKI stiftet Nutzen: Folgende Prozesse können durch den Einsatz einer PKI Nutzen erwarten: *E-Reisebuchung* (P2), *Mobile Transaktion* (P7), *Kommunikationsvorgänge innerhalb von Standesorganisationen (Ärzeschaft)* (P40). Zwar gibt es hier bestehende Konkurrenzmethoden, wie etw. das automatische Storno nach Auslaufen der Zahlungsfrist oder die klassische Einmalauthentisierung, dennoch ergäbe sich "ein hypothetischer Nutzen", der in der Einheitlichkeit der Authentisierung liegt. Insbesondere die heutige Einfachheit der Nutzung wird nach Einschätzung der Teilnehmer durch einen PKI-Einsatz nicht erreicht. Geschäftsprozesse im Unternehmen könnten im Bereich *Auftragsabwicklung* (P33) und *Lieferabruf* (P34) von einer PKI profitieren, insbesondere bei "Beweiswerterhaltung in sensiblen Fällen", wie zum Beispiel die "Zollabwicklung" oder chemische Güter oder Produkte, die einer staatlichen Kontrolle, wie z.T. Lebensmittel

oder Sondermüll, unterliegen. Dennoch würde heute vieles "zwischen Partnern einvernehmlich ohne PKI geregelt."

A1: PKI ohne Nutzen	A2: PKI stiftet Nutzen	A3: PKI bringt Vorteile	A4: PKI fast unentbehrlich
<p>P3: E-Medienkauf Bücher, DVDs, CDs etc. P4: Elektronische Produkte, Übertragung von Nutzungs-, Genuss- oder Kopierrechten an MP3s, Videos u. Bildern inkl. Digital Rights Management (DRM) P6: Versandhandel P22: Stellenvermittlung P35: Wareneingangser-einnahme P36: Bestands- und Kapazitätsabfragen beim Lieferanten</p>	<p>P2: E-Reisebuchung P7: Mobile Transaktion Kauf übers Handy etc. P33: Auftragsabwicklung P34: Lieferabrufe P40: Kommunikationsvorgänge von Standesorganisationen mit ihren Mitgliedern</p>	<p>P1: Allgemein: (Formfreier) Abschluss von Kaufverträgen im Internet P9: B2B - Auktionen Business to Business P11: Allg. Elektronische Rechnun, Beweiswürdige Präsentation von Rechnungen aller Art P12: Electronic Payment, Zahlen per digital signiertem Scheck P14: Aktienhandel P15: Versicherungsabschluss P16: Kreditverträge P17: Allg. Behördengänge und andere Vorgänge im "Virtuellen Rathaus", P19: Elektronische behördliche Benachrichtigung P23: E-Bafög P24: E-Steuererklärung P30: E-Fahrzeuganmeldung P37: Qualitätsdokumentation P39: Allg. Elektronischer Schriftverkehr E-Mail in denselben Prozessen und Kontext-situationen wie E-Mail heute P25: E-Veräußerungsmittelungen für Fahrzeuge oder Immobilien P26: E-Handelsregister-Eintragung P27: E-Meldewesen elektronische Melderegisterauskunft und -eintragung, An- und Ummelden</p>	<p>P20: E-Urkunden, z.B. E-Geburtsurkunde P21: E-Grundbuch P28: E-Personalausweis P41: Elektronische Patientenakte P42: Elektronischer Arztbrief</p>
<p>B1: PKI-Nutzen unklar</p>			<p>B2: Vorteile der PKI nicht klar ersichtlich</p>
<p>P5: E-Berechtigungshandel, z.B. Eintrittskarten, Tickets, Gutscheine P8: B2C - Auktionen, Business to Consumer P10: C2C - Auktionen, Consumer to Consumer P32: Allgemein: Geschäftsprozesse in Unternehmen P31: Vertraglicher Auftragsabschluss, elektronische Signatur und Timestamping P38: Online-Transport-Begleitschein</p>			<p>P13: Elektronisches Geld P18: E-Wahlen P29: E-Ausschreibung Auftragsvergabe der öffentlichen Hand</p>

Abbildung 4: Einschätzung der Wirkung einer PKI auf Geschäftsprozesse

A3 - PKI bringt Vorteile: Allgemein wird im Falle der Abgabe einer *gemeinsamen Willenserklärung von zwei oder mehr Personen* (P1) eine PKI als vorteilhaft angesehen. Dies betrifft *B2B-Auktionen* (P3), den *Aktienkauf* (P14), den *Abschluss von Versicherungen* (P15) und *Kreditverträgen* (P16). In den Kommentaren der Studienteilnehmer wird insbesondere auf bestehende flankierende Maßnahmen, wie "Vorkasse, Treuhänder, Versicherungen" und bestehende Widerrufsrechte hingewiesen. Auch der Hinweis auf die Wichtigkeit des Vertrauens in die Bezahlwilligkeit, noch vor der Bedeutung der Identifikation der Person dämpft hier jedoch den zu erwartenden Nutzenbeitrag einer PKI im Allgemeinen: "Business Trusts Requirements kann man nicht auf die qualifizierte Signatur reduzieren", jedoch "Bei Konkursfällen ist die Signatur für die Beweisführung sicherlich förderlich."

Auch den einfachen einseitigen Willenserklärungen werden mit PKI klare Vorteile bescheinigt. Dazu gehören *elektronische Rechnungen* (P11), *elektronische Zahlungsanweisungen* (P12), *Steuererklärungen* (P24) und *Veräußerungsmittelungen* (P25) und ganz *allgemein der elektronische Schriftverkehr* (P33). Kritisch wird vermerkt, dass eine elektronische Signatur sehr wohl das Fälschen von Rechnungen erschwere, dass aber gerade die "inhaltliche Überprüfung des Dokumentes" immer nötig sein wird. Wegen den vorherrschenden isolierten Lösungen im Bereich der Zahlungsverfahren stehen frei verfügbare Zertifikate kaum zur Verfügung. Dies schränke somit eine freie elektronische Zahlungsanweisung ein. Für den elektronischen Schriftverkehr wird die Möglichkeit zur

vertraulichen, verschlüsselten Kommunikation und der Schutz vor Spam-Mails in den Kommentaren der Studienteilnehmer hervorgehoben.

Klare PKI-induzierte Vorteile werden auch im Bereich der komplexen Prozesse gesehen: *Handelregisterprozesse* (P26), *Fahrzeuganmeldung* (P30), *Qualitätsdokumentation in Unternehmen* (P37), *Bafög-Prozesse* (P23) und *Prozesse des Meldewesens* (P27). Der Nutzen von virtualisierter, *behördlicher Kommunikation* (P17) steige mit der Häufigkeit. Vielfach kam jedoch der Hinweis auf, dass die geringe Häufigkeit von Behördenkontakten auf Seiten des Normalbürgers auch zu entsprechend geringen Nutzeneffekten auf der Seite des Bürgers käme. Der Nutzen läge sehr häufig auf Seiten der staatlichen Stellen bzw. der Unternehmen.

A4 - PKI fast unentbehrlich: Das Erstellen und Benutzen eines *elektronischen Personalausweises* (P28), das Führen eines *elektronischen Grundbuches* (P21) und das Ausstellen von *elektronischen behördlichen Urkunden* (P20) ist nach einhelliger Ansicht der Teilnehmer ohne eine PKI nahezu undenkbar. In den Kommentaren wird deutlich, dass es sich dabei immer um eine elektronische Kopie einer physikalisch vorhandenen Urkunde handelt. Dabei wird insbesondere die sichere Aufbewahrung (Langzeitarchivierung) für den Aussteller und das einfache Vorzeigen (Verfügbarkeit) und Kopieren für den Nutzer als Vorteil angesehen. Zumal die Verifikation für elektronische Urkunden für Laien wesentlich einfacher mit elektronischen Urkunden durchzuführen ist, als dies für papierbasierte Urkunden möglich wäre. Dem *Arztbrief* (P42) und der *Patientenakte* (P41) in elektronischer Form, die bereits im Rollout begriffen sind, werden wegen der "sehr hohen Anforderungen an Integrität und Authentizität" und insbesondere wegen des Geheimhaltungsbedarfs eine zwingende Affinität zur PKI nahe gelegt. Gegen den PKI-Einsatz in diesen Gebieten sprechen datenschutzrechtliche Bedenken und ein diffus vorhandenes "Missbrauchspotenzial".

B1 – PKI-Nutzen unklar: In dieser Kategorie liegen Antworten, die von einer Behinderung bis zu leichten Nutzeneffekten durch eine PKI für Prozesse ausgehen. *Geschäftsprozesse in Unternehmen allgemein* (P32) werden unklar bewertet. Contra PKI sprechen Kommentare wie "innerhalb einer Organisation kann alles ohne PKI geregelt werden", dafür brauche man also keine qualifizierte elektronische Signatur. Bei Großunternehmen spricht die Möglichkeit der Einschränkung von Missbrauch und Manipulation wiederum für den PKI-Einsatz. Ebenso wird die Situation bei unternehmensübergreifender Kooperation gesehen und überall dort, wo rechtsverbindliche Dokumentationspflichten bestehen, so auch beim *Online-Transport-Begleitschein* (P38) für z.B. Sondermüll. Für den *klassischen Einkaufsabschluss* (P31) wird insbesondere der Time-Stamping-Dienst einer PKI relevant. Besonders internationalen Großunternehmen wird zu einer "hausinternen Ausstattung mit Zertifikaten" geraten.

Bezüglich Auktionen unter Beteiligung von Endkonsumenten herrscht ebenso geteilte Meinung, dies betrifft *C2C-* (P10) und *B2C-Auktionen* (P8). Mit Hinblick auf den Erfolg von Ebay und Co. werden auf besondere Nachteile der Konsumenten hingewiesen. Dies wären die "Verfolgbarkeit des Kunden" und die Nichtabweisbarkeit einer Willenserklärung. Gerade die Nichtabweisbarkeit als ein Vorteil der elektronischen Signatur ist von Seiten des Gesetzgebers gar nicht gewünscht, da der Konsumkunde ja heute schon befä-

higt ist, den Kauf ohne Angaben von Gründen zu widerrufen, ungeachtet einer beweiswürdigen Nachweisbarkeit der Transaktion. Dies trifft auch auf den *Verkauf von Berechtigungen* (P5), wie Tickets und Gutscheine zu.

B2 – Überlegenheit der PKI nicht klar ersichtlich: In dieser Kategorie liegen Antworten, die zwar eine PKI-Beteiligung als positiv ansehen, die jedoch aufgrund der großen Streuung der Antworten keine eindeutige Kennzeichnung der Prozesse als "eindeutig überlegen mit PKI" erlauben. Neben den Prozessen *Auftragsausschreibung* (P29) *der öffentlichen Hand* und *Bezahlen mit elektronischem Geld* (P13) gehen insbesondere bei *elektronischen Wahlen* (P18) die Meinungen auseinander, ob für diese Prozesse die PKI unabdingbar wäre oder ob sogar ersichtliche Vorteile mit einer PKI zu verzeichnen wären. In allen Prozessen ist die Anonymität der Akteure und die Geheimhaltung eine wichtige Prozessvoraussetzung. Mit der Virtualisierung wird jedoch auch das Anfertigen von Kopien erleichtert, dies steht jedoch im Widerspruch zur Anonymität und Geheimhaltung. Die Nicht-Zurückweisbarkeit ist für den Ausschreibungsprozess "dringend erforderlich". Für den elektronischen Wahlprozess jedoch ist dies gerade nicht gewünscht.

Die Frage nach der Affinität der PKI zu Prozessen und nach dem Nutzen für Prozesse führt allgemein zu der Frage nach dem Nutzen der PKI für die Prozessbeteiligten. Nutzen ergibt sich meist aus der Interaktion von zwei Prozessbeteiligten. Es kommt bei Geschäftsprozessen vor, dass der Nutzen einer Digitalen Signatur ungleich zwischen den Prozesspartnern aufgeteilt ist. Diese Situation kann zu einer Blockierung führen. Eine Lösung wäre der Vorteilsausgleich zwischen den Beteiligten, diese Möglichkeit muss jedoch fallabhängig untersucht werden. Nur so jedoch können potenzielle Nutzeneffekte in eine Verbesserung der Rentabilität von Geschäftsprozessen münden.

3.4 Statistische Clusteranalysen der Antworten

Um die Gruppenbildung zu überprüfen und festzulegen sowie um Erkenntnisse über die unterschiedlichen Antwortverhalten der Studienteilnehmer zu erhalten, wurden die Stimmabgaben zu den 42 Prozessen mit statistischen Methoden untersucht. Dabei kam die agglomerativ hierarchische Clusterung (AHC) nach Ward für die Bildung der Cluster und die multidimensionale Skalierung (MDS) für die grafische Darstellung der statistischen Variablen zum Einsatz. Agglomerativ hierarchische Verfahren verbinden in mehreren Schritten die zunächst einzeln vorliegenden statistischen Variablen nach einem Ähnlichkeitsmaß, so dass agglomerativ immer größere Cluster entstehen. Das Ähnlichkeitsmaß nach Ward bezieht sich auf die Veränderung der Varianz nach einer möglichen Vereinigung zu einem größeren Cluster [BE+06]. Mit Bezug auf die PKI-Delphi-Studie werden also in jeder Iteration diejenigen Prozesse vereinigt, deren Zusammenlegung die geringste Varianzerhöhung der neu entstandenen statistischen Variable nach sich zieht. Die Gruppenbildung geschieht dann über einen Schwellwert der Varianzerhöhung.

Bei fünf vorgegebenen Clustern hat das AHC-Verfahren nach Ward für die 42 Prozesse folgende Gruppierung erzeugt (vgl. Abb. 5, links): 1. Prozesse ohne PKI, die bereits

heute schon etabliert sind, 2. Gruppe der Bezahlprozesse, 3. Gruppe der Prozesse im Unternehmen, 4. Gruppe der Prozesse mit klarer Affinität für die PKI und 5. Gruppe mit gesetzlich geforderter Beweiswürdigkeit.

Zum Teil wurde durch die Clustering die ursprüngliche Strukturierung der Prozesse beibehalten, teilweise aber auch umgestellt. Die Umstellung konnte jedoch inhaltlich nachvollzogen werden. Bei der multidimensionalen Skalierung, und damit der Reduzierung der euklidischen Distanzen der 42 Facettenfragen auf 2 Dimensionen, zeigte sich, dass auch hier die Facettenfragen derart positioniert wurden, dass eine Umrandung der AHC-Gruppen zu kompakten Formen führen.

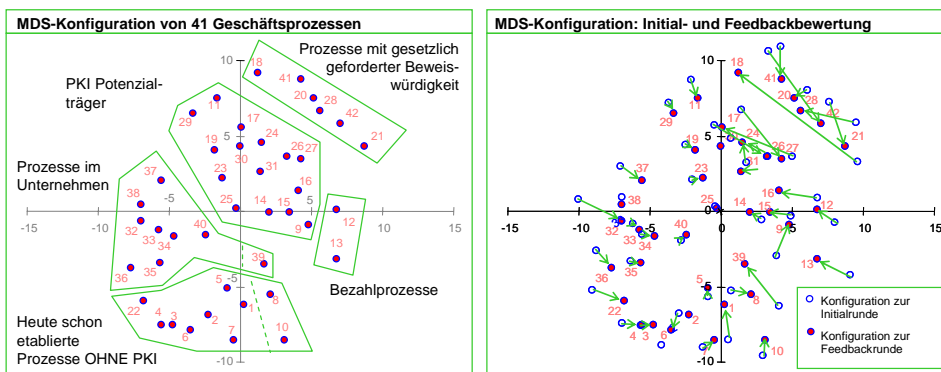


Abbildung 5: MDS-Konfiguration von 41 Prozessen – Ähnlichkeitsmaße für die Antworten

Ein Vergleich der MDS-Konfiguration in Runde 1 mit Runde 2 (vgl. Abb. 3, rechts) zeigt deutliche Änderungen bei den Prozessen: 18, 42, 27, 17, 32 und 39. Dies ist durch die Änderung der Meinungen in der Feedbackrunde und durch den Abgang von 17 Teilnehmern in Runde 2 zu erklären.

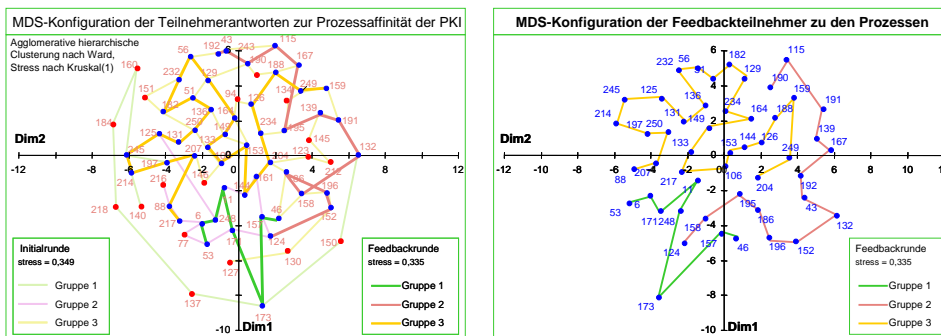


Abbildung 6: MDS-Konfiguration der Teilnehmerantworten – Ausscheiden der unkorrelierten Antwortbilder

Was bedeutet nun dieser Abgang von 17 Experten für die Validität der Ergebnisse? Auch hier kann eine Kombination aus AHC-Clustering und MDS-Analyse Erkenntnisse verschaffen. Diesmal werden jedoch alle Antworten eines Studienteilnehmers als eine

statistische Variable angesehen, d.h. die Clusteranalyse geschieht mit 69-Personen-Variablen statt wie zuvor mit 42-Prozess-Variablen. Eine AHC-Clusterung nach Studienteilnehmern ohne Vorgabe der Clusteranzahl hat zur Bildung von 3 Clustern geführt (vgl. Abb. 4). Links sind gepunktet die 3 Cluster der 69 Teilnehmer der ersten Runde und rechts die 3 Cluster der 52 Teilnehmer der 2. Runde zu sehen. Links sind zusätzlich die Clusterteilnehmer der 2. Runde in das MDS-Diagramm eingezeichnet. Bei Vergleich der Clusterung der Runde 1 mit Runde 2 fällt auf, dass insbesondere die Teilnehmer, die am äußeren Rand des MDS-Clusters lagen, die Studie verlassen haben. Diese Teilnehmer konnten nur sehr wenige signifikante Korrelationen zum Antwortverhalten von anderen Teilnehmern aufweisen. Ihr Abgang in Runde 2 bedeutet, dass die verbliebenen Antworten zu den Prozessfragen jetzt klarer und ohne das "Rauschen" von diesen ggf. unbedachten oder flüchtigen Antworten der Abgänge besser interpretierbar sind. Es kann angenommen werden, dass sich die Aussagekraft der Studie durch den Abgang sowie durch die Möglichkeit in der 2. Runde die Meinung nochmals zu überdenken und zu verändern, verbessert hat.

Eine weitere MDS-Analyse der 3 Teilnehmercluster zusammen mit anderen Gruppierungen der Studienteilnehmer hat ergeben, dass die Teilnehmercluster eine Ähnlichkeit mit der Einteilung der Gruppen in Wissenschaftler, Anbieter und Nutzer hat. Damit hat sich zumindest partiell die Eingangsthese bestätigt, nachdem mit unterschiedlichen Meinungen zwischen den drei Hauptgruppen der Studie zu rechnen wäre.

Unterstellt man der Entwicklung der Nutzung der elektronischen Signatur eine hohe Korrelation mit der Entwicklung der unternehmensübergreifenden elektronischen Kollaborationen, so lassen sich die Ergebnisse der Delphi-Studie hinsichtlich der Nutzung der PKI-Dienste auf die Entwicklung der elektronischen Kollaborationen übertragen.

4 Fazit, Ausblick und weiteres Vorgehen

Es wurde ein Modell vorgestellt, welches den potenziellen Nutzen der PKI-Technologie für Geschäftsprozesse verdeutlicht. Um das Modell zu stützen wurden 69 Experten aus den Bereichen Wissenschaft, Nutzer und Anbieter im Rahmen einer Delphi-Studie unter anderem zu deren Einschätzungen bezüglich aktueller Potenziale der qualifizierten Digitalen Signatur für 42 Geschäftsprozesse befragt. Die Ergebnisse haben als größten Potenzialträger die Bankenprozesse, die Prozesse der öffentlichen Verwaltung sowie Vertrags- und Transaktionsprozesse mit Anforderungen nach beweiswürdigen Nachweisen identifiziert.

Weitere Schritte im Rahmen dieses Forschungsvorhabens werden die Detailauswertung aller Befragungsebenen und Studienteile sein. Des Weiteren ist geplant, das Diffusionsmodell um weitere sozioökonomische Faktoren zu erweitern sowie die inneren Kausalitäten zwischen den Ebenen herauszuarbeiten. Unter Berücksichtigung der Prozesskonfiguration eines Unternehmens, kann anschließend eine Entscheidungshilfe für Unternehmen erstellt werden, wie eine optimale Adoptionsentscheidung für die PKI-Technologie aussehen kann.

Weitere Forschungsfelder liegen im Bereich der Marktforschung zur Erfassung von tatsächlichen Ist-Diffusionskurven aus dem Bereich PKI sowie in einer Ausweitung der Studie hinsichtlich des Studienpanels auf europäische Experten sowie eine Wiederholung der Befragung nach angemessener Zeitspanne zur Validierung der Studienergebnisse.

Literaturverzeichnis

- [ABH01] Albers, S.; Brockhoff, K.; Hauschildt, J. (Hrsg.): Technologie und Innovationsmanagement. Leistungsbilanz des Kieler Graduiertenkollegs, Deutscher Universitäts-Verlag, Wiesbaden 2001, S. 79-116.
- [BE+06] Backhaus, K.; Erichson, B.; Plinke, W.; Weiber, R.: Multivariate Analysemethoden - Eine anwendungsorientierte Einführung, 11 Auflage, 2006, Springer.
- [BPS05] Bichler, M.; Pikovskiy, A.; Setzer, T.: Kombinatorische Auktionen in der betrieblichen Beschaffung - Eine Analyse grundlegender Entwurfsprobleme, in: Wirtschaftsinformatik, Vol. 47 (2005) 2, S. 126–134.
- [CH+03] Childerhouse, P.; Hermiz, R.; Mason-Jones, R.; Popp, A.; Towill, D.-R.: Information flow in automotive supply chains-present industrial practice. In: Industrial Management + Data Systems, UK 2003.
- [Di78] Dillmann, D.: Mail and telephone surveys. The total design method. New York: Wiley, 1978.
- [Du01] Dudenhöffer, F.: Die Auto- und Zulieferindustrie im Informationszeitalter: Trends beim Blick in das Jahr 2010. In: GAK – Gummi, Fasern, Kunststoffe, Fachmagazin Polymerindustrie 54, 2001, S. 44- 47.
- [Ec05] Eckert, C.: IT-Sicherheit: Konzept, Verfahren, Protokolle. München , Oldenburg 2005.
- [Ga07] Gaude, M.: Future Diffusion of PKI Technology - A German Delphi Study, in: Pohlmann, N.; Reimer, H.; Schneider, W. (Hrsg.): ISSE/SECURE 2007 Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe/SECURE 2007 Conference, Vieweg, 2007, S. 386-395.
- [GS+04] Guida, R.; Stahl, R.; Bunt, T.; Secrest, G.; Moorcones, J.: Deploying and using public key technology: lessons learned in real life, in: Security & Privacy Magazine, IEEE, Vol. 2, Nr. 4, 2004, S. 67-71.
- [Hä02] Häder, M.: Delphi-Befragungen – Ein Arbeitsbuch. Westdeutscher Verlag, Wiesbaden, 2002.
- [He04] Heusch, C.-A.: Die elektronische Signatur - Änderung des Bürgerlichen Rechts aufgrund der Signatur-Richtlinie (1999/93/EG) durch das Gesetz zur Anpassung der Formvorschriften des Privatrechts an den modernen Rechtsgeschäftsverkehr vom 13. Juli 2001, Tenea Verlag, Berlin, 2004.
- [HH04] Hofreiter, B.; Huemer, C.: Transforming UMM Business Collaboration Models to BPEL; in Meersman, R.; Tari, Z.; Corsaro, A. (Hrsg.): On the Move to Meaningful Internet Systems 2004: OTM Workshops; Vol. 3292, Lecture Notes in Computer Science, Springer, 2004, S. 507–519.
- [HP99] Herrmann, G.; Pernul, G.: Viewing Business-Process Security from Different Perspectives, in: International Journal of Electronic Commerce , Spring 1999, Vol. 3, No. 3, S. 89-103.
- [KK05] Klein, A.; Krömer, H.: DCXNET: e-transformation at DaimlerChrysler, in: Journal of Information Technology, 2006, Vol. 21, Nr. 1, S. 52-65.
- [KLP05] Katsikas, S. K.; Lopez, J.; Pernul, G.: Security, Trust and Privacy in Digital Business. In: International Journal of Computer Systems, Science & Engineering, Vol 10 (2005) 6, CRL Publishing, 2005.

- [POL05] Pernul, G.; Opplinger, R.; Lopez, J.: Why have Public Key Infrastructures failed so far? In: Internet Research, Vol. 15 (2005) 5, S. 544-556.
- [Ro95] Rogers, E. M.: Diffusion of Innovations, 4. Aufl., The Free Press, New York 1995.
- [Sc05] Schoop, M.: A Language-Action Approach to Electronic Negotiations Systems Signs & Actions, Vol. 1 (2005), No. 1, S. 62-79.
- [SR04] Simon, C.; Rebstock, M.: Integration of Multi-attributed Negotiations within Business Processes, in: J. Desel, B. Pernici, M. Weske (Hrsg.): Business Process Management Proceedings, Second International Conference; Vol. 3080, Lecture Notes in Computer Science, Springer, 2004, S. 148-162.
- [SW01] Stevens, G.; Wulf, V.: Elektronische Archive in virtuellen Organisationen: Gestaltung im Spannungsfeld von Kooperation und Konkurrenz: in: Informatik-Spektrum, Vol. 24, Nr. 6, 2001, S. 369-377.

Danksagung

Für die inhaltliche Begleitung und die Unterstützung und Beratung während der Ausarbeitung und Durchführung der PKI-Delphi-Studie dankt der Autor Herrn Prof. Dr. Günther Pernul und seinen Mitarbeitern am Lehrstuhl für Wirtschaftsinformatik I, Informationssysteme, an der Universität Regensburg.