k p m g

Bundesministerium für Wirtschaft und Technologie

Bundesministerium für Wirtschaft und Technologie

Einsatzmöglichkeiten der elektronischen Signatur in öffentlicher Verwaltung und Wirtschaft

Abschlussbericht

8. November 2001

Inhalt

Anlagen

Abbildungs- und Tabellenverzeichnis

Abkürzungsverzeichnis

ADV	Automatisierte Datenverarbeitung
BAFl	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAföG	Bundesausbildungsförderungsgesetz
BÄK	Bundesärztekammer
B2B	Business toBusiness
B2C	Business to Consumer
BfA	Bundesversicherungsanstalt für Angestellte
BGB	Bürgerliches Gesetzbuch
BISA	Betriebsinformationssystem Sachsen-Anhalt
BLK	Bund-Länder-Kommission
BMAS	Bundesministerium für Arbeit, Gesundheit und Soziales
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMWi	Bundesministerium für Wirtschaft und Technologie
bos	bremen online services
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStbK	Bundessteuerberaterkammer
BVerwAmt	Bundesverwaltungsamt
CA	Certification Authority
DES	Data Encryption Standard
Difu	Deutsches Institut für Urbanistik
DIHT	Deutscher Industrie- und Handelstag
DIN	Deutsche Industrienorm
DIZ	Daten- und Informationszentrum
DMS	Dokumenten-Management-System
EESSI	European Signature Standardization Initiative

EG	Europäische Gemeinschaften
Elster	Elektronische Steuererklärung
eSig	Elektronische Signatur
EU	Europäische Union
FINREAD	Financial Transactional IC Card Reader Project
FTP	File Transfer Protocol
G2B	Government to Business
G2C	Government to Citizen
G2G	Government to Government
GMD	Gesellschaft für Mathematik und Datenverarbeitung
HBCI	Homebanking Computer Interface
HCP	Healthcare Professionals
HRK	Hochschulrektorenkonferenz
HWK	Handwerkskammer
IETF	Internet Engineering Task Force
IHK	Industrie- und Handelskammer
IP	Internet Protocol
IPSEC	IP Security Protocol
ISDN	Integrated Services Digital Network
ISIS	Industrial Signature Interoperability Specification
ITSEC	Information Technology Security Evaluation Criteria
ITU	International Telecommunication Union
IuKDG	Informations- und Kommunikationsdienste-Gesetz
IuK	Informations- und Kommunikationstechnologien
IVBB	Informationsverbund Berlin-Bonn
KBSt	Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung
KBV	Kassenärztliche Bundesvereinigung

KoopA ADV	Kooperationsausschusses ADV Bund/Länder/Kommunaler Bereich
LDAP	Lightweight Directory Access Protocol
LSA	Land Sachsen-Anhalt
LVA	Landesversicherungsanstalt
ÖPNV	Öffentlicher Personennahverkehr
OSCI	Online Services Computer Interface
OSCP	Online Status Certificate Protocol
OSI	Open Systems Interconnection
PCA	Policy Certification Authority
PDA	Personal Digital Assistant
PEM	Privacy Enhanced Mail
PGP	Pretty Good Privacy
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RA	Registration Authority
RegTP	Regulierungsbehörde für Telekommunikation und Post
S/MIME	Secure/Multipurpose Internet Mail Extensions
SGB	Sozialgesetzbuch
SigG	Signaturgesetz
SignaturG	Signaturgesetz
SignaturVO	Signaturverordnung
SKOUT	Sichere Kommunale Unternehmen im Internet
SMTP	Simple Mail Transport Protocol
SSL	Secure Socket Layer
StBerG	Steuerberatungsgesetz
TC	Trust Center
TCP	Transmission Control Protocol

TDDSG	Teledienstedatenschutzgesetz
TSP	Time Stamp Protocol
TU	Technische Universität
TÜV	Technischer Überwachungsverein
VOB	Verdingungsordnung für Bauleistungen
VOF	Verdingungsordnung für freiberufliche Leistungen
VOL	Verdingungsordnung für Leistungen
VwVfG	Verwaltungsverfahrensgesetz
WPK	Wirtschaftsprüferkammer
WWW	World Wide Web
ZKA	Zentraler Kreditausschuss
ZPO	Zivilprozessordnung

1 Auftrag und Zielsetzung

Hintergrund

Die Transformation von der Industriegesellschaft zur Wissenschaftsgesellschaft nimmt in den letzten Jahre deutliche Formen an. Eine wichtige Rolle spielt hierbei das Internet, das sich international als zentrales elektronisches Medium herausgebildet hat. Über die Zukunft dieses Mediums bestehen seitens der Wissenschaft und Verwaltung weitgehend übereinstimmende Auffassungen. Bereits jetzt haben sich in den Bereichen eBusiness und eGovernment in einem historisch sehr kurzem Zeitraum zahlreiche unterschiedliche Anwendungen entwickelt, die auf der Internettechnologie aufsetzen, z. B.

- Internet-Banking,
- eCommerce mit Zahlungstransaktionen,
- Virtuelle Rathäuser,
- Online-Wahlen,
- Online-Auktionen,
- Dateiaustausch per FTP oder eMail.

Neben den damit verbundenen Verbesserungen (u. a. leichterer Zugang zu Informationen, erhöhte Schnelligkeit, verbesserte Markttransparenz) sind mit den neuen Technologien und Anwendungsmöglichkeiten jedoch auch zahlreiche neue Risiken verbunden. Eine aktuelle Studie von KPMG zeigt z. B., dass 11% aller Unternehmen in den letzten 12 Monaten Sicherheitsverletzungen ihres eCommerce-Systems festgestellt haben; vermutlich ist ein größerer Teil der Angriffe nicht entdeckt worden[1]. Im Einzelnen gibt es u.a. folgende Schwachstellen:

- Anwenderprogramme – Verbreitete Anwenderprogramme (z. B. Outlook) weisen zahlreiche Schwachstellen auf, die Netzattacken durch „bösartige Software“ (malicious programs wie der „I love you“-Virus) ermöglichen.
- Daten – Das Potenzial des Datenmissbrauchs persönlicher und anderer schutzrelevanter Daten steigt mit der Verbreitung der Technologie.
- Datentransfer – Der Informations- und Datenaustausch mittels eMails wird sowohl innerhalb der Bevölkerung als auch in der Wirtschaft kritisch betrachtet, da weder Integrität der Daten noch Authentizität der Adressaten gewährleistet sind. Jeder Internetnutzer kann leicht unter falschem Namen eMails verschicken[2].

Der Bundesgesetzgeber hat mit der Verabschiedung des Informations- und Kommunikationsdienste-Gesetzes (IuKDG) am 1. August 1997 auf Sicherheitsbedürfnisse reagiert, die sich aus den skizzierten Defiziten ergeben. Auftragsrelevant ist hierbei die elektronische Signatur und in Teilen die Verschlüsselung (inkl. Public Key Infrastrukturen), die im Signaturgesetz von 1997 (Artikel 3 des IuKDG) behandelt wurden. Ihnen kommt beim Aufbau einer „Vertrauensinfrastruktur“ eine besondere strategische Bedeutung zu.

---

[1] Vgl. KPMG: efraud@vd.servey, Umfrage zur Wirtschaftskriminalität im eCommerce, Februar 2001

[2] Das für den Transport von elektronischen Nachrichten zuständige SMTP (simple mail transfer protocol) besitzt in seiner ursprünglichen Form keine Mechanismen zur Überprüfung, ob der Absender zum Versand einer eMail berechtigt ist. Das heißt, jeder Anwender kann über einen öffentlich zugänglichen SMTP-Server unter beliebigen e-Mail-Adressen Nachrichten verschicken; man muss lediglich die Konfiguration des eMail-Programms geringfügig ändern, indem man eine andere Absenderadresse und einen anderen Server eingibt.

Mit der Verabschiedung des Programms „BundOnline2005“, bei dem bis zum Jahr 2005 alle internetfähigen Dienstleistungen der 350 Bundesbehörden online angeboten werden sollen, hat die Bundesregierung ein wichtiges politisches Signal gesetzt und sich ein ehrgeiziges Ziel gesteckt. Für die Umsetzung dieses Zieles ist es erforderlich, dass Transaktionen ohne Medienbrüche rechtsgültig über das Internet abgewickelt werden können. Die elektronische Signatur stellt hierfür die Voraussetzung dar.

Das Signaturgesetz von 1997 hat bis zum jetzigen Zeitpunkt bereits zum Aufbau von Trustcentern sowie zur Entwicklung von Pilotprojekten und einzelnen Anwendungen geführt; eine Massenanwendung ist allerdings bis dato ausgeblieben. Mit der Verabschiedung der EG-Richtlinie über elektronische Signaturen ist ein einheitlicher Rechtsrahmen für Europa geschaffen worden. Das Deutsche Signaturgesetz wurde angepasst, so dass die Anwendung von Signaturen in Wirtschaft und Verwaltung beschleunigt werden kann. Damit könnte auch der technische Vorsprung der deutschen Industrie bei der Signatur-Infrastruktur zum Zuge kommen.

Auftrag und Zielsetzung

Mit dem Vertrag vom Oktober 2000 hat KPMG den Auftrag erhalten, Einsatzmöglichkeiten elektronischer Signaturen (eSig) in der öffentlichen Verwaltung zu erheben bzw. aufzuzeigen. Zielsetzung ist es, Transparenz über den Stand der Aktivitäten zu schaffen und Empfehlungen für die breite Einführung der eSig zu geben. Hierfür sollten sowohl bereits realisierte als auch in Planung befindliche eSig-Projekte auf den Verwaltungsebenen ermittelt und dargestellt werden. Mit der Beauftragung wurde der Projektumfang gegenüber der ursprünglichen Aufgabenstellung konkretisiert. Das Projekt umfasst demnach drei Aufgabenpakete:

- Bestandsaufnahme der bisher bereits realisierten und in Planung befindlichen Vorhaben auf der Ebene von Bund, Ländern und Kommunen unter besonderer Berücksichtigung der Pilotprojekte
  - DOMEA (Bund)
  - MEDIA@Komm (Kommunen)
- Berücksichtigung der Wirtschaft, vornehmlich Banken, Sozialversicherungen und Internetprovider
- Ausarbeitung von Empfehlungen mit den Gesichtspunkten
  - schnelle Umsetzung,
  - Breitenwirkung und Signalgebung,
  - Aufnahmefähigkeit von Verwaltungen für neue Technologien,
  - Einbindung in bestehende und neue Workflow-Prozesse,
  - Verbindungen zur mittelständischen Wirtschaft.

Vorgehensweise

Das Projekt wurde im November 2000 begonnen und Ende März 2001 abgeschlossen. In der ersten Projektphase lag der Schwerpunkt auf der Bestandsaufnahme von Vorhaben, in denen elektronische Signaturen verwendet werden bzw. verwendet werden sollen. Die Ergebnisse wurden in einer Zwischenpräsentation am 26.1.2001 vor Vertretern des BMWI, des BMI, der KBSt und der Begleitforschung zum Projekt MEDIA@Komm vorgestellt.

Für die Bestandsaufnahme hat KPMG ca. 65 strukturierte Telefoninterviews und 15 persönliche Gespräche geführt. Ergänzend wurden Ergebnisse anderer Projekte (z. B. Studie über Sachstand eGovernment in der öffentlichen Verwaltung) oder Aktivitäten (z. B. KPMG- eGovernment-Wettbewerb 2001) sowie weitere Unterlagen ausgewertet und ggf. durch Internetrecherchen detailliert. Darüber hinaus hat das Projektteam die Messen „Interaktive Televerwaltung“ und die Messe „Moderner Staat“, beide in Berlin, im November 2000 besucht, auf denen elektronische Signaturen thematisiert wurden.

Im Rahmen der Befragung auf *Bundesebene* wurden die einzelnen Ressorts direkt angesprochen. Bei der Recherche zum Dokumentenmanagementprodukt „DOMEA“ wurden zunächst Telefoninterviews mit den sechs Herstellern geführt, mit denen die Bundesregierung im Juni 2000 Rahmenverträge für die Lieferung DOMEA-konformer Systeme bzw. Produkte abgeschlossen hat. Erschien die Informationsgrundlage bzgl. relevanter Projekte nach dem Gespräch mit dem Hersteller als noch nicht ausreichend, wurden die Behörden direkt kontaktiert.

Auf der *Länderebene* wurden über die Innenministerien die jeweils für die einzelnen Projekte zuständigen Referenten befragt. Die Ergebnisse wurden dem länderübergreifenden Ausschuss in IT-Fragen, dem KoopA ADV, übermittelt.

Bei der *kommunalen Ebene* wurde auf Sekundärquellen aufgesetzt, da eine eigene empirische Untersuchung im Rahmen der Studie nicht möglich und – angesichts zahlreicher vergleichbarer aktueller Erhebungen im kommunalen Sektor[3] – auch nicht sinnvoll war. Bezüglich der im Wettbewerb MEDIA@Komm geförderten Projekte wurden Gespräche mit Verantwortlichen geführt und die Ergebnisse der Begleitforschung einbezogen.

Der Ergebnissdarstellung der Bestandsaufnahme sind eine kurze Begriffsbestimmung sowie Ausführungen zu zentralen technischen, rechtlichen und sozioökonomischen Aspekten im Zusammenhang mit der elektronischen Signatur vorangestellt. In der Bestandsaufnahme wird sich zeigen, dass Anwendungen der eSig sich weiterhin auf Insellösungen im Rahmen von Pilotprojekten beschränken. In den sich anschließenden Empfehlungen werden daher Maßnahmen für eine breite Anwendung der eSig vorgeschlagen und die hierfür erforderlichen nächsten Schritte skizziert.

[3] Vgl. Difu-Umfrage bei allen deutschen Kommunen > 50.000 Einwohner; Befragung der Kommunen im Land Sachsen durch die TU Chemnitz, 2000, unveröffentlicht; Bertelsmann-Studie, 2000; KPMG-Studie, 2000.

2 Einsatzmöglichkeiten der elektronischen Signatur

2.1 Begriff elektronische Signatur

Die Terminologie in der EU-Signaturrichtlinie ersetzt den durch das Deutsche Signaturgesetz von 1997 eingeführten Begriff der digitalen Signatur durch „elektronische Signatur“. Die allgemeinere, weniger technische Begrifflichkeit „elektronische Signatur“ soll dazu dienen, die einzelnen Bestimmungen von der schnellen technologischen Entwicklung unabhängig zu machen. Im Folgenden wird durchgängig von elektronischer Signatur (eSig) gesprochen.

Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und zur Authentifizierung dienen. Diese Definition schließt eine Vielzahl elektronischer Signaturen mit sehr unterschiedlichen Sicherheitsniveaus ein. So kann beispielsweise auch der Namenszug unter einer eMail als elektronische Signatur aufgefasst werden.

Für sichere, sogenannte fortgeschrittene bzw. qualifizierte elektronische Signaturen sind daher konkrete Anforderungen formuliert worden:

- Die Signatur ist ausschließlich dem Unterzeichner zugewiesen.
- Die Signatur kann den Unterzeichner identifizieren.
- Die Signatur wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann.
- Die Signatur ist so mit den Daten verknüpft, dass eine nachträgliche Veränderung der Daten offenkundig wird.

Sowohl einfache als auch fortgeschrittene und qualifizierte Signaturen dürfen nach der EG-Richtlinie von einem Richter nicht mehr deshalb abgewiesen werden, weil sie elektronisch sind. Zur Erfüllung von Formvorschriften (Schriftlichkeit) können aber nur die qualifizierten Signaturen nutzt werden. In der deutschen Gesetzgebung war im Signaturgesetz von 1997 die zusätzliche Vorgabe enthalten, dass die Anbieter einer eSig bestimmte Anforderungen erfüllen müssen. Diese von der Regulierungsinstanz akkreditierten Anbieter zeichnen sich insbesondere durch eine dauerhafte Überprüfbarkeit der Signaturgültigkeit (30 statt 2 Jahre) sowie eine nachgewiesene Sicherheit (u.a. vor Ort Prüfung durch die RegTP) aus.

Die unterschiedlichen Stufen der Signatur sind an sicherheitstechnische Voraussetzungen geknüpft. Die nachfolgende Abbildung soll dies und den Zusammenhang zu den Formerfordernissen verdeutlichen.

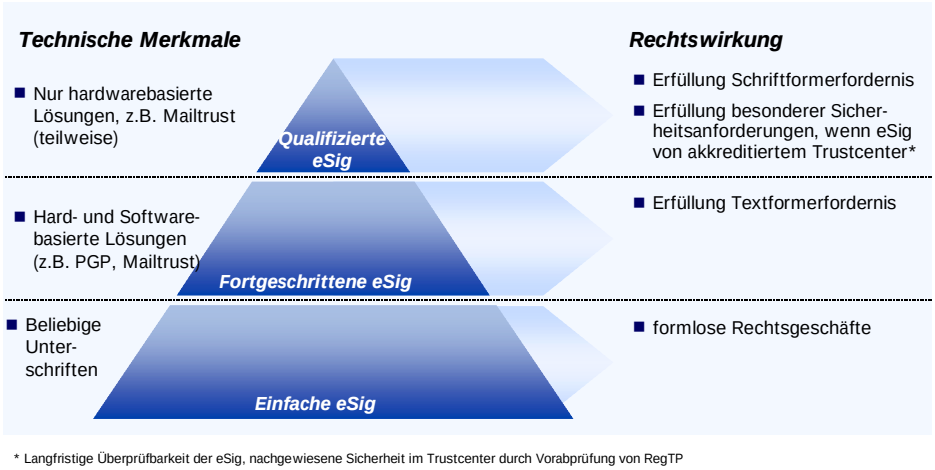


Abbildung 2-1: Stufen elektronischer Signaturen

Verschlüsselung

In Verbindung mit der eSig wird häufig auch die Verschlüsselung genannt. Die Verschlüsselung einer elektronischen Nachricht ist sowohl technisch als auch rechtlich zunächst völlig unabhängig von der elektronischen Signatur zu beurteilen. Auch eine unsignierte Nachricht kann verschlüsselt, auch eine qualifiziert signierte Nachricht kann unverschlüsselt übermittelt werden. Gleichwohl sind Signatur und Verschlüsselung im Kontext von eGovernment eng miteinander verbunden, da bestimmte Daten (z. B. Steuererklärung) vertraulich auszutauschen sind.

Die folgenden Ausführungen beziehen sich auftragsgemäß auf die eSig, sofern nicht ausdrücklich vermerkt.

2.2 eSig als Substitut der eigenhändigen Unterschrift

Elektronische Signatur- und Verschlüsselungsverfahren sind im Prinzip funktionale Äquivalente zu althergebrachten Methoden zum sicheren Nachrichtenaustausch. Hinsichtlich ihrer Praktikabilität und Alltagstauglichkeit müssen sie sich mit der handschriftlichen Unterschrift messen lassen.

Jeder Bürger muss Unterschriften leisten. Dies ergibt sich daraus, dass die institutionelle Ordnung in Deutschland traditionell weitestgehend auf Papier beruht. Die Schriftform wird in ca. 3.000-4.000 Regelungen in über 900 Vorschriften gefordert, in denen explizit auf Papierdokumente (Ausweise, Schecks, Verträge, Rechnungen, Diplome etc.) Bezug genommen wird. Praktisch jede rechtsverbindliche Willenserklärung wird erst durch eine handschriftliche Signatur auf Papier wirksam. Das Unterschreiben kann in jeder Lebenssituation mit überall verfügbaren In-

strumenten geschehen (z. B. Kugelschreiber). Die Instrumente kann man sich ggf. auch leihen. Der Akt des Unterschreibens ist unmittelbar wahrnehmbar kontrollierbar.

Bei der Abgabe von Willenserklärungen in Schriftform werden üblicherweise drei Funktionen unterschieden [4]:

- Dauerhafte Dokumentation des Erklärungsinhalts, des Absenders und ggf. auch des Empfängers der Erklärung (Klarstellungsfunktion)
- Jederzeitige Überprüfbarkeit und Beweisbarkeit der dokumentierten Erklärung (Beweisfunktion)
- Dem Schutz des Absenders der Erklärung vor Übereilung, (letzte) Warnung vor der Abgabe einer ggf. in ihren folgenden gravierenden verpflichtenden Erklärung (z. B. Immobilienkauf, eidesstattliche Erklärung, Testament)

Außerdem lässt sich auch der Vorgang des Unterschreibens als symbolische Geste des Bekennens zu einem bestimmten Vertragsinhalt (z. B. bei Staatsakten, Zielvereinbarungen) als Funktion auffassen.

Die handschriftliche Signatur ist dabei stets gleichartig, egal welcher Art und wie risikoreich die jeweilige Willenserklärung ist. Sie kann nicht verlorengehen oder ihre Gültigkeit verlieren. Gleichwohl kann sie kopiert bzw. gefälscht werden. Von jeher existiert daher das Problem, wie sichergestellt werden kann, dass eine bestimmte Willenserklärung tatsächlich von dem bezeichneten Absender stammt (Authentizität), der Inhalt nicht verfälscht wurde (Integrität) und dieser ggf. keinem Unbefugten bekannt ist (Vertraulichkeit).

Diese Sicherheit wurde herkömmlich durch die handschriftliche Unterschrift unter einem Originaldokument als gewährleistet angesehen, dass in einem verschlossenen Umschlag einem Empfänger zugeleitet wird. Durch digitale Kopier- und Druckverfahren ist Manipulation von Papierdokumenten jedoch nur mit hohem Aufwand nachweis- bzw. vermeidbar. Da in der Praxis häufig lediglich Kopien versandt/verteilt werden, ist ein Abgleich mit dem Original kaum möglich. Unterschriften sind häufig unlesbar und daher nicht zuzuordnen; allein das Briefpapier weist Personen als Zugehörige einer Organisation aus. In den meisten Fällen lässt sich erst aufgrund von graphologischen Gutachten nachweisen, ob eine Unterschrift wirklich authentisch ist.

Grundsätzlich ist festzustellen, dass eigenhändige Unterschriften keineswegs sicher sind. Dennoch beschränkt sich in der Praxis die Unterschriftenprüfung auf Störungen (Missbrauch, Diebstahl, einer der Beteiligten bestreitet, seine Unterschrift geleistet zu haben). Graphologische Gutachten werden nur in gravierenden Fällen (z. B. in Gerichtsverfahren) angefordert.

Die eSig führt daher zu einer maßgeblichen Anhebung des Sicherheitsniveaus.

2.3 Der Nutzen von eSig Anwendungen

Jeder Einsatzbereich von eigenhändigen Unterschriften stellt zugleich einen potenziellen Anwendungsbereich der elektronischen Signatur dar. Die eSig ist allerdings insbesondere dafür gedacht, die Sicherheit in offenen Netzen zu verbessern. Gleichwohl lässt sie sich auch in geschlossenen Netzen anwenden, wenn eine besonders sichere Kommunikation erforderlich bzw. die Authentifizierung der Bearbeiter maßgeblich ist (z. B. wegen Unterschriftskompetenzen).

[4] Vgl. M. Eifert, Online-Verwaltung und Schriftform im Verwaltungsrecht, K&R 2000 (Beilage 2, S. 11 ff.).

Angesichts der Verknüpfung offener und geschlossener Netze in der Praxis lässt sich sowieso kaum eine klare Abgrenzung vornehmen.

Für die Zwecke der Systematisierung der Bestandsaufnahme über Signaturprojekte lassen sich grob drei Akteursgruppen unterscheiden:

- „Government", hier verstanden als Sammelbegriff für Gremien und Einrichtungen der öffentlichen Verwaltung
- „Business", wobei hier sowohl staatliche als auch öffentliche Unternehmen (z. B. Rechenzentren, Krankenhäuser) einbezogen werden
- „Citizen/Consumer": Privatpersonen in ihren verschiedenen Rollen als Bürger, Konsument, Patient u.ä.

Daraus ergeben sich, berücksichtigt man den Initiator der Kommunikation, neun mögliche Beziehungskombinationen, die in der nachstehenden Tabelle mit Beispielen versehen wurden. Dabei ist allerdings die Richtung der Kommunikationsbeziehung nicht überall eindeutig zuzuordnen.

Akteure[5]	**Government**	**Business**	**Citizen/Consumer**
Government	Austausch von eMails und Dateien Austausch und Bearbeitung von elektronischen Akten Dokumenten-Archivierung	Versand von Ausschreibungsunterlagen Dokumenten-Archivierung	Bürgerdienste (Virtuelles Rathaus etc.) Aus-, Fort- und Weiterbildung
Business	Abgabe eines Angebotes nach Ausschreibungen Elektronische Steuererklärung Elektronischer Schriftverkehr mit Gerichten Zugriff auf amtliche Verzeichnisse (Grundbücher etc.) Abwicklung von Zollverfahren	Elektronische Marktplätze Automatisierte Bestellung eines Herstellers bei einem Zulieferer Electronic Publishing (Absicherung von Schutzrechten in Wort, Bild, Musik, Absicherung der Urheberschaft, z. B. von wiss. Publikationen) Autorisierter Zugang zu vertraulichen Dokumenten (z. B. Patientenakten) Elektronische Mahnverfahren	Angebot von Waren und Dienstleistungen im Internet
Citizen/ Consumer	Elektronische Wahlen Elektronische Steuererklärung Anmeldung nach Wohnungswechsel Beantragung von Pass, Personalausweis, Führerschein	Kauf bei Online-Versandhändlern Internet-Buchungen von Flugtickets Veranlassen elektronischer Zahlungsvorgänge (Online-Banking)	Tauschbörsen (z. B. Napster) Austausch von eMails Diskussionsforen

Tabelle 2-1: Beispiele für Einsatzmöglichkeiten der elektronischen Signatur

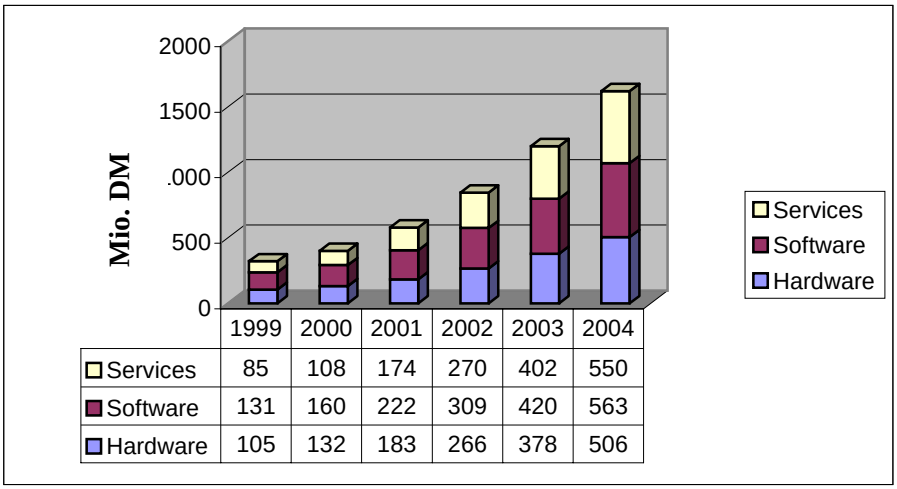
[5] Die Verwendung englischer Bezeichnungen trägt der Tatsache Rechnung, dass praktisch die gesamte Diskussion über das Internet auf Englisch verläuft und sich daher bestimmte Begriffe (z. B. „B-C" als Kurzform für Beziehungen zwischen Unternehmen und Konsumenten) als Fachtermini etabliert haben.

Die genannten Beispiele unterscheiden sich jedoch stark hinsichtlich der üblichen Form. So ist der Erwerb eines Buches über das Internet genauso wie der Einkauf im Supermarkt formfrei, ohne Signatur durchführbar. Beim Ausstellen eines medizinischen Rezeptes dagegen ist die Unterschrift des Arztes erforderlich. Beim Geschäftsverkehr mit dem Staat gibt es auch zahlreiche Leistungen, die ohne eigenhändige Unterschrift empfangen werden können (z. B. Bestellung von Abfallbehältern, Adressenänderung). Insofern stellt sich die Frage, für welche Arten von Transaktionsbeziehungen tatsächlich qualifizierte eSig erforderlich bzw. nützlich sind.

Nutzen der eSig im eCommerce: Prozesskostensenkungen, Umsatzausweitung

Kunden- und Lieferantenbeziehungen im eCommerce/Online-Banking kommen zwar derzeit auch mit einem geringeren Sicherheitsniveau aus (Kreditkarten, Kundennr., PIN-Codes), bei einem durchschnittlichen Warenwert von derzeit 108 DM pro Kauf ist jedoch auch das Risiko sehr eingeschränkt. Sobald es um den Kauf komplexerer, teurerer Produkte geht (Autos, Investmentfonds, Häuser u.ä.) wird derzeit unter Hinweis auf die unzureichende Sicherheit im Internet der Papierweg gesucht[6]. Insbesondere Anbieter solcher Produkte dürften ein Interesse daran besitzen, beweissicherere Online-Transaktionen anzubieten.

In einer aktuellen Studie der Meta Group wird der Markt für Sicherheitsleistungen im Internet-Umfeld (eSecurity) von einem Marktvolumen von 400 Mio. DM mit einer durchschnittlichen Wachstumsrate von 42% auf 1,6 Mrd. DM ansteigen (siehe Abb. 2-2)[7]:



	1999	2000	2001	2002	2003	2004
Services	85	108	174	270	402	550
Software	131	160	222	309	420	563
Hardware	105	132	183	266	378	506

Abbildung 2-2: eSecurity-Marktentwicklung 1999-2004

Aus einer eher kleinen (116 Unternehmen) und durch im eBusiness-erfahrene Unternehmen geprägten Stichprobe der genannten Studie haben 84% der Befragten angegeben, dass sie beabsichtigen, eine qualifizierte eSig einzusetzen. Dabei wird es in der Praxis stark darauf ankommen, wie aufwendig und kostenintensiv die Implementierung und Nutzung qualifizierter Signaturen im Vergleich zu anderen Möglichkeiten sein wird, Sicherheit herzustellen (z. B. Nichtverfolgung von Ausfällen, Adressenüberprüfung, schwarze Listen).

[6] Vgl. z. B. „Virtuell und schnell“, Handelsblatt vom 15.12.2000.
[7] Quelle: Meta Group Deutschland GmbH: Security im E-Business-Zeitalter. Status, Lösungen, Trends in Deutschland – 2001, S. 128 unveröffentlichte Vorabversion.

Nutzen der eSig im eGovernment: Voraussetzung für die Umsetzung von eGovernment

Bürger haben offenbar ein großes Interesse an Online-Kontakten mit der Verwaltung. Auf die Frage, für welche Zwecke das Internet genutzt werden sollte, setzten die Befragten in verschiedenen Studien die öffentliche Verwaltung/Behördenkontakte an erste Stelle; vor Arbeitsplatzangeboten Reisen und Fortbildung u.ä.[8]. Insofern scheint auf Kundenseite ein hoher Nutzen damit verbunden zu sein, Behördengänge schneller abwickeln zu können.

Inwiefern nützt die eSig der Verwaltung selbst? Grundsätzlich gilt zwar auch im öffentlichen Recht der Grundsatz der Formfreiheit; im Rahmen der zahlreichen Fachgesetze wird jedoch häufig das Schriftlichkeitsgebot, notarielle Beurkundung, Aufbewahrungsfristen u.ä. gefordert. Die Rechts- und Regelbindung des Verwaltungshandelns prägt die Organisationskultur in der Verwaltung. Veränderungen wie z. B. eGovernment haben es schwer, sich durchzusetzen, so lange sie nicht mit der Tradition und „Sprache“ der Verwaltung kompatibel sind. Dadurch dass die eSig rechtsgültiges Handeln über Netze ermöglicht, wird eGovernment für die Verwaltung nicht nur in Randbereichen (Bürgerinformation, Tourismus), sondern auch für den Kernbereich hoheitlicher Entscheidungen relevant. Vor diesem Hintergrund stiftet die eSig nicht nur wegen ihres funktionalen Wertes (Sicherheit) einen besonderen Nutzen, sondern – und dieser Nutzen dürfte möglicherweise sogar höher zu bewerten sein - sie schafft kulturelle Voraussetzungen für die Akzeptanz von eGovernment innerhalb der Verwaltung.

Das erforderliche technische Niveau einer Signatur lässt sich daran bemessen, welche der drei Grundfunktionen der Schriftform im Einzelfall im Vordergrund steht: Wenn die Schriftform vor allem der Klarstellung oder dem Übereilungsschutz dient, dann kann - bei entsprechender technischer Gestaltung[9] - auch eine unsignierte bzw. einfach signierte Nachricht als funktionales Äquivalent angesehen werden. Geht es primär um die Beweisbarkeit im Streitfall, dann ist für die Herstellung funktionaler Äquivalenz der Einsatz qualifizierter elektronischer Signaturen erforderlich.

Welche Bedeutung der Beweisfunktion gegenüber den beiden anderen Grundfunktionen im konkreten Fall zukommt, hängt wesentlich vom Missbrauchsrisiko und von der Höhe des potenziellen Schadens ab. Je geringer das Missbrauchsrisiko und je geringer der potenzielle Schaden, umso geringer ist die Bedeutung der Beweisfunktion und umso eher ist es gerechtfertigt, auch ein Handeln per einfacher eMail zu ermöglichen.

Wie groß der Anteil der Tranksaktionsbeziehungen mit bzw. innerhalb der Verwaltung tatsächlich ist, die eine (qualifizierte) elektronische Signatur erfordern, kann nicht genau benannt werden, da hierzu die einzelnen Verfahren im Detail untersucht werden müssten.

[8] Vgl. z. B. BAT Freizeitforschungsinstitut, 3.000 Personen ab 14 Jahre, 1998 und INRA Eurobarometer, 16.245 Personen in 15 Ländern.

[9] Um die Warnfunktion der Schriftform auch bei elektronischer Kommunikation hervorzuheben, kann die Benutzerführung zum Beispiel so gestaltet werden, dass das Absenden Nachrichten mehrfach bestätigt werden muss.

3 Rahmenbedingungen für den Einsatz elektronischer Signaturen

Seit mehreren Jahren gibt es elektronische Signaturen im Rahmen von Standardsoftwarepaketen. Mit dem Signaturgesetz von 1997 war Deutschland Vorreiter in der Regulierung elektronischer Signaturen. Gleichwohl ist die Anwendung bisher kaum verbreitet. Dies begründet sich insbesondere darin, dass bestimmte Voraussetzungen (noch) nicht gegeben waren oder bestimmte Kontextfaktoren möglicherweise nicht in ausreichendem Maße berücksichtigt wurden. Im Folgenden werden die rechtlichen, technischen, sozioökonomischen Rahmenbedingungen für den Einsatz der elektronischen Signatur kurz umrissen.

3.1 Rechtliche Rahmenbedingungen

Die Einführung der rechtsgültigen elektronischen Signatur tangiert zwei klassische Rechtsgebiete:

- Das *öffentliche Recht* in den unmittelbar oder mittelbar mit dem Signaturgesetz verbundenen öffentlich-rechtlichen Themenstellungen (Signaturgesetzgebung) sowie weiteren daran anknüpfenden, öffentlich-rechtlichen Rechtsfragen (z. B. das Verwaltungsverfahrengesetz).
- Das *Privatrecht* in den Bereichen, in denen es um die Gleichstellung der elektronischen Signatur mit der persönlichen Handschrift geht. Darüber hinaus sind weitere mit eBusiness und eCommerce verbundene Rechtsfragen innerhalb unterschiedlicher Rechtsgebiete (u. a. Haftungsrecht, Schuldrecht, Vergaberecht) von Relevanz.

Wie das nachfolgende Schaubild verdeutlicht, sollen bei der Rechtsentwicklung für ein einfacheres Verständnis zwei Phasen unterschieden werden. Zum einen die „reine“ öffentlich-rechtliche Phase I mit der Signaturgesetzgebung im engeren Sinne sowie Phase II mit sowohl öffentlich-rechtlichen als auch privatrechtlichen Komponenten:

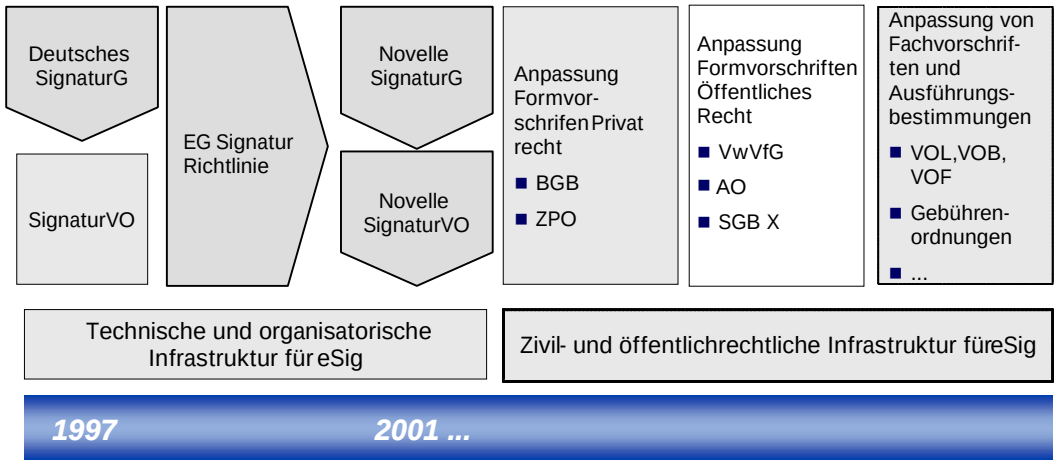


Abbildung 3-1: Überblick Rechtsentwicklung

Phase I mit der Schaffung eines allgemeinen rechtlichen Rahmens für eine technische und organisatorische Infrastruktur steht gegenwärtig vor dem Abschluss.

In Phase II befinden sich sowohl die öffentlich-rechtlichen als auch die privatrechtlichen Aspekte in einem unterschiedlichem Entwicklungsstand.

Nachfolgend wird zunächst auf beide Phasen gesondert eingegangen. Abschließend erfolgt dann eine übergreifende Gesamtbewertung der rechtlichen Rahmenbedingungen.

3.1.1 Phase I: Technische und organisatorische Infrastruktur für eSig

Phase I umfasst nach der in der Abbildung getätigten Aufteilung das Signaturgesetz im engeren Sinne als die zentrale Rahmenbedingung für den Einsatz elektronischer Signaturen. Nachfolgend werden zunächst dessen Chronologie kurz dargestellt sowie die wesentlichen Inhalte der jeweiligen Gesetze:

Deutsches Signaturgesetz

Schon früh hat sich der Bundesgesetzgeber dem Thema elektronische Signaturen angenommen. Die wesentlichen Inhalte des Signaturgesetzes vom 1. August 1997 und der Signaturverordnung vom 22. Oktober 1997 lassen sich wie folgt zusammenfassen:

- Fokus auf Sicherheitsanforderungen in Hinblick auf Infrastruktur für Schlüssel
  - -erzeugung,
  - -zertifizierung,
  - -verteilung und
  - -anwendung.
- Anerkannte Zertifizierungsstellen, d. h. Stellen, die ein Sicherheitskonzept besitzen und sich regelmäßigen Prüfungen unterziehen.
- Einsatz technischer Komponenten mit hohem Sicherheitsstandard (ITSEC E2/E4 hoch)

Das Signaturgesetz von 1997 selbst regelte nicht die rechtliche Gleichstellung von elektronischer Signatur und handschriftlicher Unterschrift, da dies nachgeschalteten Gesetzesänderungen überlassen werden sollte.

Das Signaturgesetz enthielt auch keine expliziten Aussagen zur Rechtswirksamkeit digitaler Signaturen. Stattdessen bestand ex ante eine widerlegbare Sicherheitsvermutung für SigG-konforme Signaturen, die darin bestand, dass „gesetzeskonformen“ elektronischen Signaturen innerhalb der freien richterlichen Beweisführung eine angemessene Bedeutung zukommen dürfte. Hierbei wurde von der (hohen) Wahrscheinlichkeit ausgegangen, dass einer „gesetzeskonformen digitalen Signatur“ im Rechtsstreit ein hoher Stellenwert eingeräumt wird, wenn

- die Erstellung des Schlüsselpaars privat/öffentlich von einer autorisierten Zertifizierungsstelle (CA) erfolgt,
- die Zuordnung öffentlicher Schlüssel durch Zertifikat der CA bescheinigt und
- evaluierte Hard- und Software eingesetzt wird.

EG-Richtlinie als Basis einer Neuausrichtung

Mit der Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13.12.1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen wurde von europäischer Seite das Thema elektronische Signatur aufgegriffen. Kennzeichen dieser Richtlinie sind:

- Verwendung aller elektronischen Signaturen ist freigestellt (wenn nicht Rechtsvorschriften anderes vorschreiben); d. h. keine grundsätzliche „Diskriminierung" aller elektronischer Signaturen im Gerichtsverfahren (z. B. Anspruch rechtlicher Wirksamkeit; Zulässigkeit als Beweismittel)
- Fortgeschrittene Signatur + qualifiziertes Zertifikat + erstellt mit sicherer Signaturerstellungseinrichtung = handschriftliche Unterschrift
- Keine Übernahme der im Deutschen Signaturgesetz enthaltenen strengen CA-Regeln (stattdessen: „geeignetes System zur Überwachung")
- Freiwilliges Akkreditierungsverfahren statt Genehmigungsverfahren als zulässige Anforderung; ansonsten zusätzliche Anforderungen möglich
- Keine Aussage, welche Funktionalität mit welcher Klasse von Signatur erbracht werden soll; die Richtlinie ist insofern technologie-offen
- Einführung der Haftung durch die CA, deren Mindestsumme von den einzelnen Nationalstaaten festzulegen ist

Novellierung des Deutschen Signaturgesetzes

Die europäische Entwicklung machte eine Modifizierung der deutschen Gesetzgebung notwendig. Zielsetzung einer Novellierung des Deutschen Signaturgesetzes war vor diesem Hintergrund eine vollständige Umsetzung der EG-Richtlinie in nationales Recht und die Schaffung eines rechtlichen Rahmens, der es erlaubt, für verschiedene Anwendungsgebiete rechtlich anerkannte elektronische Signaturen unterschiedlicher Qualität einzusetzen.

Hierbei sollte auch die Evaluierung des IuKDG von 1999 berücksichtigt werden, die u. a. folgende Forderungen beinhaltete:

- Klarstellung, dass Übertragung von CA-Überwachungsaufgaben an Dritte (z. B. RegTP) möglich ist
- Klare Grundlage für Anerkennung von Prüf- und Bestätigungsstellen (Anregung der Berufskammern)

Die Bundesregierung legte auf Basis dieser Überlegungen im April 2000 die Eckpunkte für einen Gesetzesentwurf vor und beschloss am 31. Mai 2000 die Änderung der Signaturverordnung. Der Beschluss des Bundeskabinetts vom 16. August 2000 leitete die Novellierung des Deutschen Signaturgesetzes endgültig ein. Der Gesetzesentwurf wurde am 16. November 2000 dem Bundestag zugeleitet und von diesem am 7. Dezember 2000 an den Wirtschaftsausschuss zur Beratung überwiesen.

Am 15. Februar 2001 stimmte der Deutsche Bundestag in zweiter und dritter Lesung einer Novellierung des Signaturgesetzes zu. Das „neue" bzw. novellierte SigG ist nach erfolgter Zustimmung des Bundesrates im Mai 2001 in Kraft getreten. Zu den Eckpunkten des novellierten Gesetzes zählen:

- Rechtliche Angleichung der allgemeinen Sicherheitsanforderungen an Zertifizierungsstellen und an technische Komponenten entsprechend der EG-Signaturrichtlinie
- Wegfall der Genehmigungspflicht für Zertifizierungsstellen
- Beibehaltung des hohen Sicherheitsniveaus nach geltendem Signaturgesetz durch Einräumung einer Prüfung von Zertifizierungsstellen und technischen Komponenten mittels einer freiwilligen Akkreditierung. Damit verbunden ist die Berechtigung, im Rechts- und Geschäftsverkehr mit der hiermit verbundenen „geprüften" Sicherheit zu werben.
- „Bestandsschutzregelungen" für die Betreiber von CA-Stellen nach dem „alten" (geltenden) Signaturgesetz
- Aufnahme einer Regelung zur Haftung von Zertifizierungsstellen einschließlich einer Deckungsvorsorge (Sanktionsmittel)
- Ausweitung der spezifischen Datenschutzregelungen entsprechend der EG-Signaturrichtlinie
- Technische Detaillierung über Rechtsverordnung in §24 (5)
- Regelungen im Zusammenhang mit europäischen und außereuropäischen Signaturen
- Schaffung eines §1(3), der es dem Gesetzgeber ermöglicht, über Rechtsvorschriften zu bestimmen, „dass für die öffentlich-rechtliche Verwaltungstätigkeit der Einsatz qualifizierter elektronischer Signaturen zusätzlichen Anforderungen unterworfen werden kann". Allerdings wird einschränkend angeführt, „dass die Anforderungen ... objektiv, verhältnismäßig und nicht diskriminierend sein dürfen." Sie dürfen sich überdies „nur auf die spezifischen Merkmale der betreffenden Anwendung beziehen."

Der Gesetzgeber hat somit zum einen zahlreiche Forderungen von Experten (z. B. Deckungsvorsorge) aufgegriffen und zugleich für bestehende Einrichtungen (zertifizierte CA) die erforderliche Rechtssicherheit gewährleistet.

Die Signatur-Verordnung, in der vor allem technische Aspekte der elektronischen Signatur geregelt werden, befindet sich gegenwärtig noch in der Abstimmung.

3.1.2 Phase II: Zivil- und öffentlich-rechtliche Infrastruktur für eSig

Die rasche Verbreitung der elektronischen Signatur hängt nicht nur von der Signaturgesetzgebung und einer darauf aufbauenden Signatur-Verordnung ab, sondern auch von anderen kontextbezogenen rechtlichen Regelungen, von denen einige an dieser Stelle kurz angerissen werden sollen: das Verwaltungsverfahrensrecht, die elektronische Aktenführung und Archivierung, der Datenschutz.

Rechtliche Regelungen im Verwaltungsverfahren

Für den Einsatz elektronischer Signaturen im öffentlichen Sektor spielt vor allem das Verwaltungsverfahrensrecht eine zentrale Rolle, da hierin die generellen Grundtypen und Grundbausteine von Verfahrensweisen der Verwaltung einheitlich geregelt sind.

Wenngleich im öffentlichen Recht prinzipiell Formfreiheit besteht, ist die Schriftform in vielen Bereichen zwingend vorgeschrieben. Schätzungen kommen in diesem Zusammenhang auf bis zu 3.000 bis 4.000 Vorschriften.

Gegenwärtig liegt ein Musterentwurf des BMI vor, der eine Anpassung des Verwaltungsverfahrensrechts an den modernen elektronischen Datenaustausch im Sinne einer Simultangesetzgebung bei Bund und Ländern beabsichtigt. Ziel ist hierbei eine Gleichstellung elektronischer Signaturen im Verwaltungsverfahrensrecht mit der Schriftform. Vor dem Hintergrund der vorhandenen zahlreichen Spezialgesetze (z. B. Abgabenordnung - Federführung BMF - oder Sozialgesetzbuch Band 10 (SGB X) - Federführung BMA) kann dies ggf. über Artikelgesetzgebung beschleunigt werden. Da die Redaktion des Musterentwurfs nach gegenwärtigem Kenntnisstand weniger den Textinhalt als die Begründung betrifft, könnte bereits im Herbst 2001 mit einem Referentenentwurf gerechnet werden – vorausgesetzt Bund und Länder finden eine Übereinstimmung. Daneben sind eine Reihe anderer Änderungen zum Teil schon in Kraft getreten (Vergaberecht).

Die Möglichkeit der EG-Richtlinie für bestimmte Vorgänge der öffentlichen Verwaltung qualifizierte Zertifikate von akkreditierten CAs zu verlangen, wird voraussichtlich nicht ausgeschöpft.

Unabhängig davon ist zu beachten, dass es in der Praxis – anders als gegenwärtig festgelegt – bei vielen Prozessschritten gar keiner Schriftform bedarf.[10] Wenn der Gesetzgeber die Chance wahrnimmt, Überregulierungen im Rahmen des aktuellen Gesetzgebungsprozesses abzubauen, würde dies eine Änderung des Verwaltungsverfahrensgesetzes verlangsamen.

Eine derartige Verlangsamung träte auch ein, wenn eine parallele Anpassung von VwVfG und einzelnen Fachgesetzen durchgeführt werden sollte.

Elektronische Aktenführung

Die elektronische Aktenführung muss den Anforderungen der Gesetzmäßigkeit des Verwaltungshandels gerecht werden, d. h.

- Rechts- und Fachaufsicht,
- parlamentarische Kontrolle,
- Akteneinsichtsrecht der Beteiligten,
- Vorlage vor Gericht sowie
- vollständige und wahrheitsgetreue Aktenführung

müssen gewährleistet sein und rechtmäßig erfolgen können. Gegenwärtig ist die Aktenführung am Informationsträger Papier orientiert. In der elektronischen Aktenführung stellt sich z. B. das Problem der Mehrfachunterschriften. Diese können seriell erfolgen („Zwiebelschalenprinzip“), wobei der Nachfolgende ein elektronisches Dokument einschließlich aller nachher erzeugten Unterschriften signiert; hier stellt sich jedoch die Frage, ob nicht jeweils unterschiedliche Dokumente signiert werden.

Elektronische Archivierung

Durch Aufbewahrungspflichten der Behörde ist die Sicherung elektronischer Daten über teilweise lange Zeiträume sicherzustellen. Ein Zertifikat zur Erzeugung einer eSig hat eine Gültigkeit von zwei Jahren (qualifizierte eSig). Ein Dokument, das Gebäude oder Bauwerke bezeichnet,

[10] So hat etwa die Arbeitsgruppe „Bau eines Hauses“ beim MEDIA@Komm-Projekt der Freien Hansestadt Bremen herausgearbeitet, dass beim Bauordnungsverfahren unter Beachtung der Funktionserfordernisse (vgl. Abschnitt 2.2), nur bei 17 von 44 Prozesschritten die Schriftform geboten ist, und dass demnach die pauschale Anwendung der qualifizierten elektronischen Signatur eine Anhebung des Formerfordernisses darstellen würde.

muss jedoch durch eine Kommune bis fünf Jahre nach Abriss aufbewahrt werden. Auch muss die Rechtsverbindlichkeit von Kaufurkunden elektronisch nachweisbar sein (z. B. Grundstücke). Ein wiederholtes Signieren dieser Dokumente durch Archivare löst aber nur einen Teil des Problems. Denn bisher ungeklärt ist die Frage, wie man eine Abwärtskompatibilität über mehrere Dekaden hinweg sicherstellen kann (Wer wird im Jahr 2020 noch Speicherformate von Windows 95 lesen können?).

Hier sind Verfahrensvorschriften sowie gesetzliche Bestimmungen und Rechtsgrundsätze zur Archivierung anzupassen oder ggf. neu zu regeln.

Datenschutz und organisationsrechtliche Aspekte

Die Einführung elektronischer Verfahren begünstigt Zentralisierungstendenzen; so z. B. Bestrebungen, Dienstleistungen an einer „virtuellen" Stelle zusammenzulegen (z. B. auf Basis eines Lebenslagenkonzepts). Diese Entwicklung muss bei ihren Auswirkungen die organisationsrechtlich gewünschte informationelle Gewaltenteilung (z. B. Abgleich von Bürgerdaten nur im gesetzlich definierten Bedarfszwang) berücksichtigen. Um dies auch in Zukunft zu gewährleisten, sind gegebenenfalls organisationsrechtliche Regelungen neu zu definieren.

Privatrechtliche Aspekte

Auch für das Privatrecht sind zahlreiche Erleichterungen auf den Weg gebracht worden.

Für den Einsatz von elektronischen Signaturen im privatrechtlichen Bereich ist vor allem das Außenverhältnis, und hierbei vor allem die gerichtsfeste Identitätsfeststellung des Vertragspartners, von Interesse.

Die Bundesregierung hat am 14.3.2001 den zweiten Entwurf des federführend vom BMJ erarbeiteten „Gesetzentwurf zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr" vorgelegt (Änderungsgesetz). Wichtig ist hier die Einfügung eines Absatz 2 in §126 BGB, der den Ersatz der Schriftform durch eine elektronische Form ermöglicht: „Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt."

Der neu geschaffene §126a legt darüber hinaus die qualifizierte elektronische Signatur als erforderlich fest, wenn die gesetzlich vorgeschriebene schriftliche Form ersetzt werden soll.

Mit der Neufassung des §127 wird der Einsatz qualifizierter elektronischer Signaturen auch ermöglicht, wenn die Schriftform nicht durch Gesetz, sondern durch Rechtsgeschäft bestimmt worden ist. Darüber hinaus können auch andere Formen elektronischer Art vereinbart werden.

Wichtig für die Praxis ist neben den Änderungen im BGB auch die Frage, ob und wieweit die höhere Beweiskraft von Urkunden (§§416, 440 ZPO) auch für qualifizierte elektronische Signaturen gilt, oder ob ihnen nur im Sinne eins Augenscheinbeweises der freien richterlichen Beweiswürdigung (§286 ZPO) keine in besonderem Maße erhöhte Beweiskraft zukommt. Der Gesetzgeber beabsichtigt vor diesem Hintergrund im Rahmen des „Änderungsgesetzes" die Schaffung eines §292a, der eine wesentliche Gleichstellung der qualifizierten elektronischen Signatur in der Zivilprozessordnung herbeiführt.

Abschließend lässt sich feststellen, dass es weiterhin eine große Zahl von Detailfragen zu klären gibt, die für den praktischen Nutzen der eSig höchst relevant sind (z. B. die Erzeugung, Nutzung und Rechtsverbindlichkeit von Attributzertifikaten, Nutzung von Pseudonymen). Weitere offene

Fragen bestehen in Bereichen, die in keinem unmittelbaren Zusammenhang mit der elektronischen Signatur stehen, wohl aber im generellen Zusammenhang mit der Internettechnologie. Hierzu zählen ungelöste oder unbefriedigend gelöste Aspekte des Wettbewerbsrechts, des Schuldrechts, des Urhebervertragsrechts und anderer Rechtszweige.

Werden die geplanten Änderungen im öffentlich-rechtlichen Bereich zügig durchgeführt, so ist – ungeachtet einzelner offener Fragen – noch in 2001 mit einer tragfähigen rechtlichen Basis für den Einsatz von elektronischen Signaturen zu rechnen.

3.2 Technische Rahmenbedingungen

Die technischen Rahmenbedingungen für eine tragfähige Signierumgebung sind sehr komplex. Die Komponenten der Basisinfrastruktur sowie Standards befinden sich noch in der Entwicklungsphase.

In diesem Abschnitt wird daher zunächst kurz auf die Entstehungsgeschichte eingegangen, bevor nationale und europäische Standards, Komponenten der Signierumgebung sowie spezielle Anwendungsaspekte behandelt werden.

3.2.1 Historische Entwicklung der technischen Rahmenbedingungen

Anfang der 90er Jahre setzte sich das Internet breitflächig durch, nachdem es durch das Aufkommen des WorldWideWeb (WWW) einer großen Benutzerschaft zugänglich gemacht wurde. Kurz darauf entwickelten sich auch Sicherheitsstandards zur Signierung und Verschlüsselung von Daten im Internet, die von der IETF (Internet Engineering Task Force) als bindender Internetstandard Stück für Stück festgelegt wurden, z. B.:

- IPsec: Signierung und Verschlüsselung von einzelnen Datenpakten (Layer 3 im OSI-Referenzmodell)
- SSL (Secure Socket Layer): verschlüsselte Verbindungen, z. B. beim WWW (Layer 4 im OSI-Referenzmodell)
- S/MIME (Signierte und verschlüsselte Mail) (Layer 7 im OSI-Referenz-Modell)

Bei allen Standards kam Public-Private-Key Technologie (Asymmetrische Verfahren) zur Anwendung, wobei ein Public Key (Öffentlicher Schlüssel) jedem in der Welt bekannt sein darf und ein Private Key existiert, der vom Benutzer streng geheim gehalten werden muss.

Alle Verfahren benutzten dabei Zertifikate nach X.509, einer ITU-Vorschrift. Zum Signieren und Verschlüsseln wurde dasselbe Public/Private-Paar benutzt. Zur Handhabung der Schlüssel und der Zertifikate, die von CAs (Certification Authorities) ausgegeben wurden, definierte die US-Firma RSA die Reihe der PKCS-Standards, die sich weit durchsetzten (Public Key Cryptography Standard).

Nachteil der Methode war, dass die Zertifikate und der Private Key in Software vorlagen, also vom Sicherheitsstandpunkt aus nur auf Wissen nicht aber auf Besitz gründeten, da Dateien leicht kopierbar sind und somit eine eindeutige Zuordnung zu einem bestimmten Benutzer nicht immer möglich ist.

3.2.2 Nationale und europäische Standards

Mit Einführung des Deutschen Signaturgesetzes wurde der Mangel behoben, indem die Zertifkate und der Private Key in eine Chipkarte gegeben werden, so dass neben Wissen auch immer Besitz gegeben sein muss. Ursprünglich war vorgesehen, die Schlüssel in Trustcentern (CAs) zu generieren und zu hinterlegen, so dass bei Verlust der Karte eine Ersatzkarte ausgestellt werden konnte, aber auch den Sicherheitsdiensten Zugang zu den Private Keys gegeben werden konnte (Key-Escrow-Diskussion). Diese Entwicklung ist aber vom Tisch. Es besteht breiter Konsens, dass aus Sicherheitsgründen für eine Signatur der Private Key nur dem Benutzer zugänglich sein soll, nicht aber Dritten über das Trustcenter. Seitdem werden die Private Keys in einer Chipkarte erzeugt und verlassen diese nicht.

Zu beachten ist aber auch, dass neuere Entwicklungen dazu geführt haben, dass für Signierung und Verschlüsselung unterschiedliche Public-/Private-Schlüsselpaare verwendet werden. Sicherheitstechnisch ist das von Standards abgedeckt und begrüßenswert. Der Anwendungskomfort sinkt dagegen.

Aus dem SigG-1997 und der SigVO-1997 wurden dann weitere Standards abgeleitet, um eine voll funktionsfähige Signatur-Anwendungsumgebung zu schaffen.

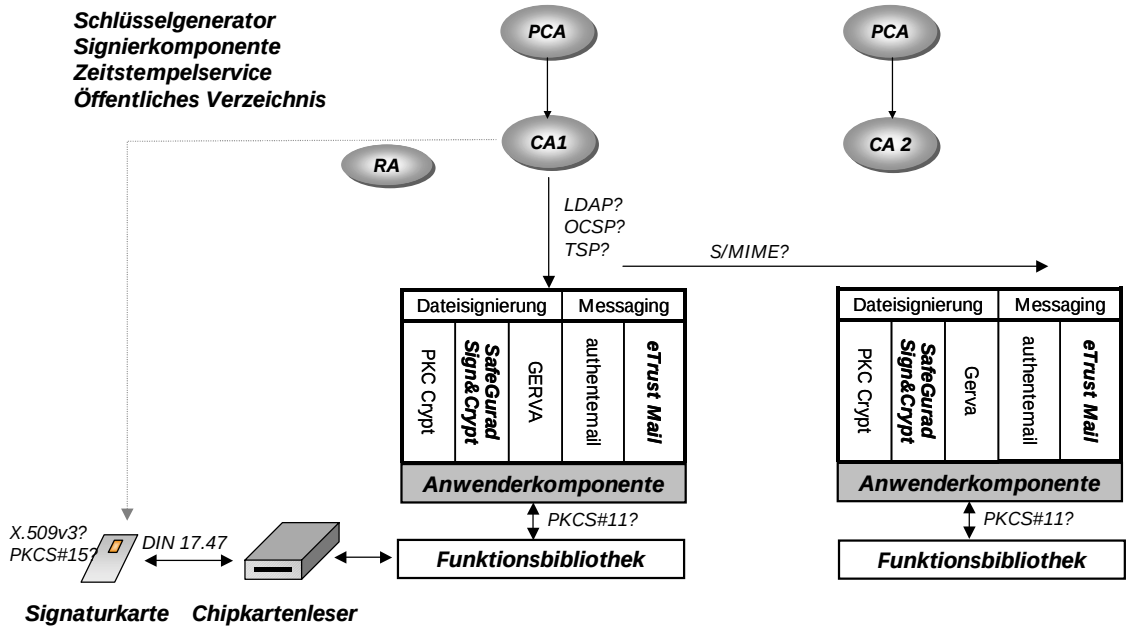


Abbildung 3-2: Zusammenspiel der Komponenten der Basisinfrastruktur für das Signieren

Nach §17.3 SigV-1997 wurden technische Komponenten festgelegt, die für eine sichere Signierumgebung gebraucht und zertifiziert werden müssen:

- Signaturkarten
- Chipkartenlesegeräte
- Funktionsbibliotheken
- Anwendungskomponenten (z. B. für Dateisignierung oder Messaging)

- Für Trustcenter (Certification Authorities [CA]): Schlüsselgenerator, Signierkomponenten, Zeitstempelservice, öffentliche Verzeichnisse für gültige und zurückgezogene Zertifkate.

Das Zusammenspiel der einzelnen Komponenten ist in Abbildung 3-2 dargestellt (s.o.). Voraussetzung für eine funktionsfähige Anwendungsumgebung ist, dass die Komponenten untereinander kompatibel bzw. interoperabel sind. Hierfür sind eine Reihe von Schnittstellen exakt zu spezifizieren (z. B. PKCS#11, PKCS#15, S/MIME Version 2 oder 3, zulässige private Ergänzungen der X.509v3-Zertifikate).

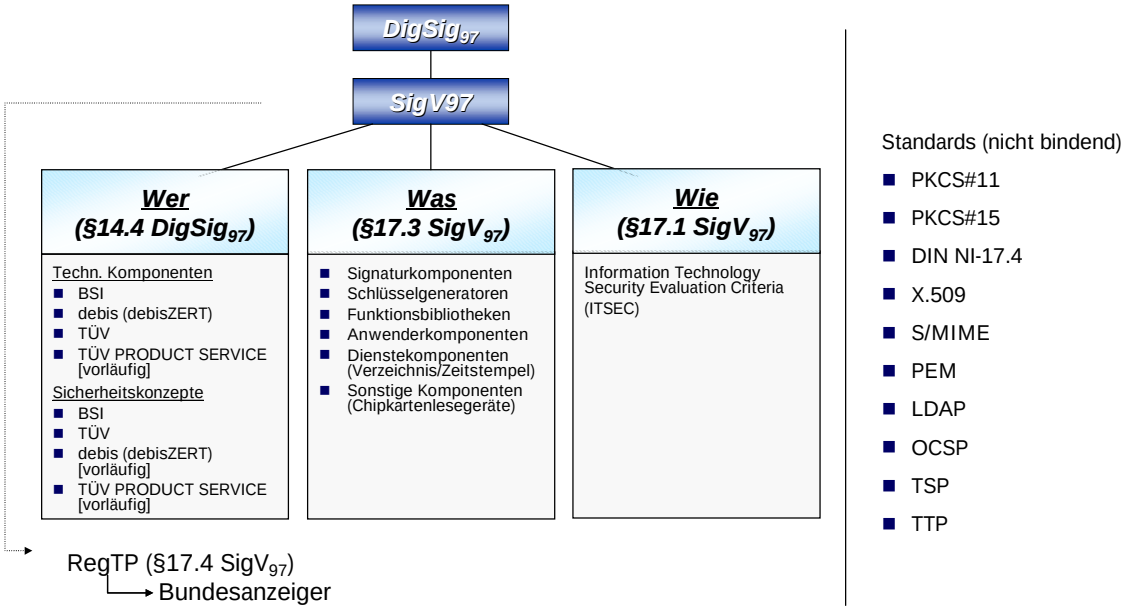


Abbildung 3-3: Regulierte und nicht regulierte Aspekte der Basisinfrastruktur eSig

Bei der Formulierung der technischen Anforderungen an die Signaturumgebung hat sich der Gesetzgeber im Lichte der sonst hörbaren öffentlichen Kritik der Überregulierung und der Kritik an der Staatsquote von folgenden Grundsätzen leiten lassen:

- Minimale Regulierung
- Einbeziehung privater Organisationen bei der Erarbeitung und Abstimmung der technischen Standards

Im Ergebnis gibt es heute einige Organisationen, die bei der Zertifizierung erforderlicher Produkte tätig werden. Es sind auch einige Produkte zertifiziert, die von der RegTP bekannt gegeben werden und mit denen qualifizierte Signaturen erstellt und verifiziert werden können.

Allerdings sind auch viele notwendige Standards nicht festgelegt worden, die für eine Interoperabilität der Produkte notwendig wären. Abbildung 3-3 soll dies verdeutlichen. Es werden zwar Zuständigkeiten, Produkte und Prozesse vorgegeben; hinsichtlich der Interoperabilitäten gibt es jedoch keine bindenden Standards.

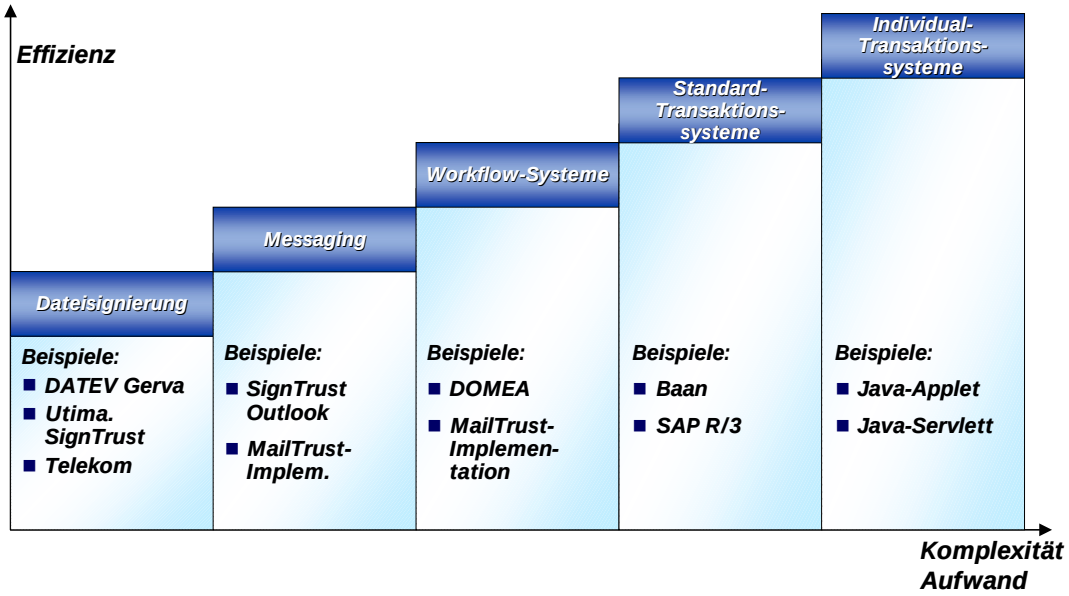


Abbildung 3-4: Anwendungsformen eSig nach Zweck und technischer Komplexität

Über die sich historisch herausgebildeten Komponentenklassen hinaus hat KPMG eine Klassifizierung von technischen Anwendungen vorgenommen, für die es zertifizierte und nicht zertifizierte Produkte gibt:

- Dateisignierung
  (z. B. DATEV Gerva, Utimaco SignTrust, Telekom)
- Messaging (elektronische Post)
  (z. B. Outlook-Plugins, Lotus-Notes-Plugins, Standalone-Messaging-Systeme)
- Workflowsysteme
  (z. B. DOMEA)
- Standard Transaktionssysteme
  (z. B. SAP R/3 oder Baan)
- Individuelle Transaktionssysteme
  (z. B. auf Java basierende Systeme wie bei Bremen Online Services)

Die organisatorische Effizienz, aber gleichzeitig auch die technische Komplexität nimmt auf den einzelnen Stufen sukzessive zu.

In der Regel funktionieren diese Systeme in ihren insularen Umgebungen. Aber es gibt eine große Anzahl von Problemen, die eine Interoperabilität und damit eine große Ausbreitung der Lösungen verhindern, beispielsweise:

- Bei der Dateisignierung gibt es keine Standardformate. Jedes Produkt hat sein eigenes Format, so dass Sender und Empfänger das gleiche Produkt vom gleichen Hersteller benutzen müssen.
- Die Chipkarten sind nicht standardisiert. Ein Benutzer kann seine Karte nicht allumfassend als Substitut für die eigene Unterschrift benutzen (ein Student aus Berlin kann mit seiner Karte nicht nach Bremen umziehen, ein Telekom-Kunde kann kein Messaging-Produkt der Post AG benutzen usw.).

- Karten, die im Büro für Lesegeräte funktionieren, können in Lesegräten zu Hause nicht verwendet werden.
- Bei den Zertifikaten nach X.509 wurde nicht die Einheit von Signatur-Schlüssel und Verschlüsselungsschlüssel beibehalten. Stattdessen wurden private, nicht standardisierte aber technisch durchaus zulässige Erweiterungen vorgenommen, die in ihrer Vielfalt zu fehlender Interoperabilität führen (z. B. Attributszertifikate).

An einzelnen Standards wurden beispielhaft vorgefunden:

- DIN V 66291-1 „Chipkarten mit Digitaler Signatur-Anwendung/Funktion nach SigG und SigV“
- SigI Signatur-Interoperabilitätsspezifikation
  BSI – März 2000
- ISIS – Industrial Signature Interoperability Specification
  Arbeitsgemeinschaft Trust-Center für digitale Signaturen
  Version 1.2, 3.12.1999; http://www.t7-isis.de/ISIS/isis.html
- MailTrust
  Version 2, 16.3.1999
- OSCI – Online Services Computer Interface
- Health Care Professionals’ Protocol
  Kassenärztliche Vereinigung Bayern – Bayerische Landesärztekammer – GMD
  Version 0.52, 26.7.2000; http://www.hcp-protokoll.de/
- FINREAD- Konsortium - Standardisierung von Chipkarten-Lesegeräten

Im Vorfeld der EG-Richtlinie haben die europäische Industrie und europäische Standardisierungskörper eine Arbeitsgruppe damit beauftragt, Anforderungen an Standards zu identifizieren, um die Richtlinie umsetzen zu können:

- EESSI European Signature Standardization Initiative
  Final Report of the EESSI Expert Team
  20th July 1999

Mit ihrem Bericht hat die EESSI einige Handlungsfelder identifiziert, in denen für eine Interoperabilität von Produkten weitere Standards verbindlich gemacht werden müssen.

3.2.3 Komponenten und Anwendungsaspekte der eSig

Zertifikate

Zertifikate als Kern der PKI-Infrastrukturen werden heute üblicherweise nach dem X.509-Standard aus der X-Reihe der ITU (übernommen von vielen anderen Standardkörpern) dargestellt. Ursprünglich wurden in Internetanwendungen X.509-Zertifikate verwendet, die Signierfunktion und Verschlüsselungsfunktion mit demselben Public-Private-Key-Paar erbringen.

Es ist standardkonform, die Zertifkate nach Signier- und Verschlüsselungsfunktion zu trennen und gesonderte Public-Private-Key-Paare zu verwenden. Allerdings ist diese Trennung nicht bei allen Massenprodukten implementiert.

Darüber hinaus ist vom Standard vorgesehen, den Pflichtkern der Zertifikate, der für alle gleich ist, um private Erweiterungen zu ergänzen. Anwendungsdesigner können bestimmte Felder ihrer Erweiterungen als zwingend notwendig (critical) markieren. Vorschrift für andere Anwendungen ist dann, die Felder stillschweigend zu ignorieren, wenn sie diese nicht interpretieren können und im Falle einer Signatur diese als ungültig (weil nicht interpretierbar) auszuweisen. Dies wird aber in manchen Anwendungen nicht befolgt, so dass es bis zu Programmabstürzen kommt.

Auch ist zu beobachten, dass bei den vorgefundenen nationalen Standards eine durchgängige, stimmige Wichtung von critical-non/critical nicht gegeben ist, so dass mehrere Anwendungskreise unterschiedliche Zertifikatstrukturen erfordern. Damit werden die Anwendungen inkompatibel.

Entgegen dem Modell der eigenhändigen Unterschrift, die nur an eine natürliche Person gebunden ist, wurde durch die Einführung von Attributzertifikaten zusätzlich die Bindung an eine Rolle (öffentlich-rechtliche Funktion wie Wirtschaftsprüfer, Arzt, Notar usw. oder Rolle als Arbeitnehmer) eingeführt. Was früher im Schriftbereich strikt getrennt war (z. B. Unterschrift und Siegel/Stempel), wurde durch die Einführung der Attributszertifikate zusammengeführt. Es bleibt spannend zu beobachten, ob sich mit diesem komplexitätssteigernden Ansatz ein äquivalenter Nutzen herbeiführen lässt.

Chipkartenlesegeräte

Es sind hinreichend Typen von Lesegeräten zertifiziert, um mit einem akzeptablen Sicherheitsniveau elektronische Signaturen zu erstellen. Chipkarten haben Schnittstellen zu ihrer Umwelt, die bei zu geringer Standardisierung dazu führen, dass eine geschlossene, proprietäre Lösung vorliegt. Dies betrifft:

- Funktionsbibliotheken (Treiber, Libraries)
  Von der Firma RSA wurde vor einigen Jahren der Standard PKCS#11 vorgeschlagen, der auf einem Rechner einer Anwendung erlaubt, abstrakt auf einen beliebigen Chipkartenleser zuzugreifen. Bisher ist dieser in den zertifizierten Produkten nicht realisiert. Das führt dazu, dass jeder Anwendungssoftwarehersteller seine Programme für jedes Lesegeräte anpassen muss.
- den elektrischen Chipkartenzugang
  Der elektrische Chipkartenzugang ist standardisiert.

- den logischen Chipkartenzugang
  Beim logischen Chipkartenzugang muss das Lesegerät verschiedene Funktionen erfüllen; z. B. Auslesen eines Zertifikates (z. B. nach Format PKCS#15), Verschlüsseln eines Komprimats, Verschlüsseln eines Nutztextes, PIN-Abfrage

Wenn der Zugang zu den Funktionsbibliotheken und der logische Chipkartenzugang nicht standardisiert werden, dann besteht hier ein wesentliches Verbreitungshemmnis. Ein Nutzer wird schon technisch nicht in der Lage sein, die Vielfalt der Einsatzmöglichkeiten elektronischer Signaturen zu nutzen, da sich eine Vielzahl von unterschiedlichen Lesegeräten mit unterschiedlichen Funktionsbibliotheken nicht in einem einzigen Endgerät integrieren lassen. Die vorgefundenen Lösungen beschränken sich zudem auf den Microsoft Windows-Bereich. Dies ist bei dem Marktanteil von Microsoft aus Sicht der Anbieter nachvollziehbar, aber den Nutzern von Apple-, Sun- oder Linuxrechnern ist eine Anwendung versperrt.

Biometrische Verfahren

Die bisher verwendeten Verfahren mit Wissen (PIN) und Besitz (Chipkarte) schützen nur bedingt vor Missbrauch (wer die Chipkarte eines anderen besitzt und die zugehörige PIN weiß, kann im Namen eines anderen elektronisch signieren). Eine denkbare Abhilfe sind biometrische Verfahren, bei denen biologische Merkmale einer natürlichen Person zur Identifikation hinzugezogen werden (Fingerabdrücke, Augeniris, Stimme). Dabei werden aktuelle Stichproben mit einer hinterlegten Stichprobe verglichen. Es sind grob zwei Szenarien zu unterscheiden:

- Substitutiv zu gängigen Verfahren
  Hierbei wäre die komplette Infrastruktur auf das jeweilige biometrische Verfahren umzustellen (Hinterlegung der Stichprobe in einem Trustcenter, gegen die dann Online verglichen wird).
- Ergänzend zu gängigen Verfahren
  Hierbei wird der Zugang zum klassischen Verfahren durch biometrische Verfahren überwacht (statt PIN) und das Vergleichsmuster lokal hinterlegt.

Bei beiden Varianten existieren (noch?) keine Standardisierungen. Darüber hinaus ist derzeit nicht zu erwarten, dass ein oder mehrere Verfahren eine gleichartige Vielfachheit der Einsatzmöglichkeiten erlaubt, wie die eigenhändige Unterschrift oder auch das World Wide Web, die völlig kontextfrei global einsetzbar sind. Ein Szenario, in dem gleichzeitig Chipkarten mit PINs, Fingerabdrücken und Stimmproben an allen Arbeitsplätzen, Heimrechnern und öffentlichen Kiosken mit hinterlegten Proben einsetzbar sind, ist nur mit enormen finanziellen Aufwand denkbar, bei geringem inkrementellen Nutzen einer weiteren Technologievariante.

Signatur und Verschlüsselung

In den ersten kommerziellen Softwarevarianten zum Messaging waren Signatur und Verschlüsselung durch das S/MIME-Format der Nachrichten gleichzeitig implementiert (z. B. Microsoft Outlook, Lotus Notes 5 und Netscape Messenger). Allerdings waren diese Produkte wegen der Zertifikate in Software (statt in Chipkarten) unsicherer und nach Deutschem Signaturgesetz nicht zertifizierungsfähig. Das SigG behandelte ausschließlich die Signaturverfahren als Ersatz für die eigenhändige Unterschrift. Zudem wurde damals von den Strafverfolgungsbehörden gefordert, dass eine effektive Verschlüsselung verboten würde zum Zwecke der Strafverfolgung und des nachrichtendienstlichen Erkenntnisgewinns.

Mitte bis Ende der neunziger Jahre gab es auch bei US-amerikanischen Produkten nur schwache Verschlüsselungen. Diese Lage hat sich heute geändert. Einerseits besteht bei den amerikanischen Produkten kein Exportverbot mehr bei starker Verschlüsselung, andererseits hat in Deutschland auch das Sicherheitsbedürfnis gegenüber den Nachrichtendiensten zugenommen, so dass heute auch nicht mehr gefordert wird, dass eine Kopie des privaten Schlüssels im Trustcenter hinterlegt ist. Statt dessen wird der private Schlüssel nunmehr in der Chipkarte erzeugt und verlässt diese nicht. Im finnischen Bürgerausweis wird die Verschlüsselung von eMail mit S/MIME direkt neben anderen Verfahren unterstützt.

In Deutschland zeichnet sich ab, dass auch in Verfahren, die von der öffentlichen Hand initiiert werden, auf eine Verschlüsselung im Umfeld von elektronisch signierten Dokumenten nicht verzichtet werden kann. So wurden im Rahmen der Studie folgende Bereiche identifiziert, die eine Verschlüsselung der Nachrichten (nicht nur der Signierungskomprimate) erfordern. Beispiele:

- eVergabe
  Angebote nach den entsprechenden Vergabeordnungen sind in verschlossenem Umschlag einzureichen. Das entsprechende elektronische Äquivalent ist ein verschlüsseltes Dokument.
- Elster
  Um das Steuergeheimnis zu wahren, müssen die eingereichten Erklärungen verschlüsselt. werden.
- eVoting
  Um geheime Wahlen ermöglichen zu können, werden die abgegeben Stimmen verschlüsselt
- HCP – Healthcare Professionals
  Im HCP-Standard werden zur Wahrung des Patientengeheimnisses personenbezogene Daten vor der elektronischen Übermittlung verschlüsselt und in ein S/MIME-Format gebettet.

Der ursprüngliche Verzicht auf Standardisierung der Verschlüsselung und die gesetzgeberische Fokussierung auf die Signierfunktion erweist sich in praktischen Anwendungen als Verbreitungshemmnis, da alle beteiligten Anwenderkreise eigene (und damit dann häufig proprietäre) Standards setzen müssen.

Zeitstempelservice

Ein Zeitstempelservice ist notwendig zum Nachweis eingehaltener Fristen („Eingangsstempel Poststelle“). Anwendungen sind nicht beobachtet worden.

Archivierung

Bei der Archivierung elektronischer Dokumente tritt das Problem auf, dass gesetzliche Aufbewahrungsfristen länger sind als die Gültigkeitsdauern von Zertifikaten, die zur Signierung verwendet werden. Ein Vorschlag in der Gesetz- und Verordnungsgebung war, dass Dokumente, die ordnungsgemäß signiert sind, dann zusätzlich signiert werden dürfen, um durch diesen „Refresh“ immer über eine gültige Signatur unter dem Dokument zu verfügen. Hierzu existiert noch Forschungsbedarf, zumal keine Produkte für eine technische Realisierung vorliegen.

Schlüsselmanagement

Bei der verwendeten Public-Private-Key-Technolgie kommen zwei Schlüssel zum Einsatz:

- ein Public Key, den jeder kennen darf und soll
- ein Private Key, der unter allen Umständen geheim zu halten ist

Die Tatsache, dass ein Private Key in einer sicheren Umgebung (z. B. auf einer Chipkarte) erzeugt wird und diese nicht verlässt und nicht ausgelesen werden kann, führt zu unterschiedlichen operativen Problemen bei der Signierfunktion und bei der Verschlüsselungsfunktion im Falle des Verlustes der Chipkarte.

Bei der Signierfunktion wird dem Benutzer eine neue Karte ausgestellt, das alte Zertifikat wird beim Trustcenter als zurückgezogen gemeldet. Werden mit dem alten Zertifikat von einem neuen Benutzer Signierungen erstellt, können diese als ungültig erkannt werden. Der rechtmäßige Benutzer trägt lediglich das Risiko, dass er für die Zeit der Wiederbeschaffung nicht signieren kann.

Bei der Verschlüsselung verhält es sich anders. Verliert der Benutzer seinen Private Key, dann hat er systemimmanent keine Sicherungskopie. Das bedeutet für ihn, dass er alle für ihn verschlüsselten Dokumente nicht mehr lesen kann. Dieses Problem ist noch unzureichend erforscht und pragmatisch noch nicht geklärt. Angedachte Lösungsvorschläge gehen in die Richtung, gelesene Mail und eigene unverschlüsselt zu speichern, so dass durch die Verschlüsselung hauptsächlich der Transport gesichert wird.

HBCI und OSCI

Im Jahre 1998 führte der ZKA (Zentraler Kreditausschuss) der Deutschen Bankenwirtschaft (Geschäftsbanken, Sparkassen und Genossenschaftsbanken) für alle Banken verbindlich den Standard HBCI (Homebanking Computer Interface) ein. Ziel war es, das Home Banking mit einem einheitlichen Standard auf Internettechnologiebasis zu ermöglichen, wobei der private Benutzer zu Hause alle Geschäftsvorfälle mit einer beliebigen deutschen Bank mit nur einer Anwendungsumgebung erledigen können sollte. Zahlreiche Transaktionen wurden in einem umfangreichen Werk definiert. Als Sicherheitsfunktion wurden zunächst softwarebasierte Benutzerzertifikate unterstützt, später auch chipkartenbasierte. Allerdings wurden die Spezifikationen so festgelegt, dass die Anwendungen technisch nur von einem ungesicherten Heimarbeitsplatz aus durchgeführt werden konnten. In Firmennetzen mit nach BSI-Empfehlungen gesicherten Intranets (screened subnetworks mit Application-Level Gateway) ist ein Zugriff auf HBCI-Anwendungen nicht möglich. Wird nicht am Endgerät ein eigenständiger HBCI-Client verwendet, sondern ein Java-Applett, das mit einem externen HBCI-Client kommuniziert, lässt sich die Protokolleinschränkung umgehen.

Bankenspezifische Transaktionen sind in den Banken meist mit selbstentwickelten Programmen auf Großrechnern implementiert. Die Idee, Kunden von extern mit einem einheitlichen Interface Zugang zu den Transaktionen bei allen Banken zu geben, ist von der OSCI-Initiative für behördenspezifische Transaktionen übernommen worden. Auch hier ist es denkbar, dass Benutzer mit einem einheitlichen Werkzeug (Java-fähiger Browser) spezifische Transaktionen vornehmen, unabhängig davon, wie die dahinterliegenden Plattformen aussehen.

Interoperabilitätstest

Um eine Interoperabilität der auf dem Markt verfügbaren Signaturprodukte zu untersuchen, wurden durch KPMG-Mitarbeiter folgende Komponenten von der Deutschen Telekom AG und der Deutschen Post AG beschafft und in Betrieb genommen:

- Chipkarte mit Zertifikat
- Chipkartenlesegerät
- Funktionsbibliothek
- Messaging-Produkte
- Dateisignierungsprodukte

Im Einzelnen waren folgende Beobachtungen zu verzeichnen:

- Lieferzeit 2-3 Wochen
- Die Funktionsbibliotheken der Produkte sehen keine Softwareschnittstelle nach PKCS#11 vor, d.h. jeder Anwendungssoftwarehersteller muss in seine Produkte die spezifische Ansprache der Lesegeräte selbst hineinprogrammieren.
- Die Telekom vertreibt kein eigenes Messaging Produkt. Der auf der Website angegebene Vertreiber (secude) sieht keinen Vertrieb für Privatkunden vor. Ausnahmsweise wurde auch eine Losgröße von 1 zur Verfügung gestellt.
- Obwohl die Chipkarten baugleich und vom gleichen Hersteller stammten, waren sie nicht gegenseitig substituierbar.
- Messaging-Signierung: ausgehende Nachrichten konnten signiert werden. Das Telekom-Produkt erkannte die Signatur des Post-Produktes nicht an und umgekehrt. Das Versenden an Empfänger mit S/MIME-Produkten von Microsoft und Netscape führte bei den Empfängern zum Crash (Absturz) dieser Produkte. Wenn die Produkte nicht abstürzten, war die Signatur als ungültig markiert.
- Datei-Signierung: Die Deutsche Telekom stellt ein Dateisignierungsprogramm zur Verfügung. Eine Vielzahl von Variationsmöglichkeiten (Rohdatei und externe Signatur, Rohdatei ergänzt um Signatur usw.) sind möglich. Es gab keinen Hinweis darauf, dass die Dateiformate standardisiert seien, dass ggf. die Signatur mit einem Fremdprodukt (zum Beispiel Gerva von der datev) geprüft werden könnte.
- Verschlüsselung: Beim Telekom-Trustcenter können die Zertifikate mit einem TTP-Viewer (TTP-Protokoll der Telekom) heruntergeladen und zur Verwendung in Standard-Produkte exportiert werden. Beim Post-Trustcenter kann das Verschlüsselungszertifikat mit einem WWW-Browser verfügbar gemacht werden. Bei beiden Messaging-Produkten konnten verschlüsselte Nachrichten erstellt, aber mit dem jeweils anderen Produkt nicht entschlüsselt werden.

Nach mehr als drei Jahren bei geltendem Signaturgesetz ist es erstaunlich, dass die beteiligten Anbieter offenbar Produkte in den Markt gebracht haben, die keinen Interoperabilitätstests ausgesetzt waren.

Deutschland ist mit seinem Signaturgesetz von 1997 in eine weltweit führende Position gekommen, was die Anwendung qualifizierter elektronischer Signaturen anbelangt. Andere Staaten und auch die Europäische Union orientieren ihre eigenen Maßnahmen an den deutschen Erfahrun-

gen. Die Grundbaupläne für die technischen Infrastrukturen sind vorhanden, ein Markt von Anbietern beginnt sich zu entfalten. Einige technische Themen sind noch zu elaborieren (z. B. Verschlüsselung, Zeitstempeldienste und Archivierung). Wenn es gelänge, die Interoperabilität der vorhandenen Produkte herbeizuführen, wäre auch ein Fundament für eine weltweite wirtschaftliche Nutzung der gewonnenen Erkenntnisse gelegt. Womöglich müssen einige Standards nochmals überarbeitet werden, um durch die Interoperabilität den beteiligten Unternehmen auch einen breiten Markt für ihre bisherigen Nischenprodukte zu öffnen.

Einen ersten Schritt in diese Richtung ist die zunächst privatwirtschaftliche Initiative „Bridge-CA“ der Deutschen Telekom AG und der Deutschen Bank AG gegangen, der sich mittlerweile einige wichtige Großunternehmen (Siemens, BMW, DaimlerChrylser und andere), diverse Trustcenter und auch die öffentliche Verwaltung (BSI) angeschlossen haben und die mittlerweile unter der Schirmherrschaft des Bundesinnenministeriums steht.

Technisch geht es zunächst darum, unterschiedliche Vertrauenspfade disjunkter Root-CAs nicht an der eigenen Root-CA terminieren zu lassen, sondern über die Bridge auch Teilnehmern anderer wohldefinierter Root-CAs zu vertrauen (Zertifikate als ‚valid’ in einer Anwendung anzeigen lassen zu können).

Als erste Anwendung für die diese Zusammenarbeit der Infrastrukturen erfolgreich verprobt wurde, ist Messaging nach dem S/MIME-Standard für Signierung und Verschlüsselung ausgewählt worden. Bisher wurde mit fortgeschrittenen Signaturen gearbeitet, eine Erweiterung auf qualifizierten Signaturen wurde angekündigt.

Ebenfalls in diesem Interoperabilitätsumfeld bewegen sich die Bemühungen den MailTrust-Standard kompatibel zum ISIS-Standard zu machen. Dafür soll ein erster Draft für einen gemeinsamen ISIS-MTT-Standard im Sommer 2001 erarbeitet werden, der möglicherweise schon im Herbst 2001 in Kraft tritt.

3.3 Sozioökonomische Rahmenbedingungen

Einsatz und die Verbreitung der elektronischen Signatur sind vor dem Hintergrund der Entwicklungsprinzipien des Internets zu bewerten. Neben rein ökonomischen sind dabei auch soziokulturelle Rahmenbedingungen, insbesondere der Aspekt des Vertrauens zu berücksichtigen.

Regeln in der Netzwerkökonomie

Folgende „neue“ ökonomische Gesetzmäßigkeiten werden üblicherweise in Zusammenhang mit der Net-Economy genannt:

- ***Kritische Masse als Erfolgsfaktor*:** In Marktmodellen der traditionellen Ökonomie ist der Preis für ein Gut üblicherweise umso höher, je knapper es ist. In der Netzwerkökonomie wird dieser Grundsatz umgekehrt, denn der Nutzen eines Netzwerkes ist umso höher, je mehr Teilnehmer es hat. Diese Netzwerkeffekte verlaufen nicht linear, sondern der Nutzen eines Netzwerkes steigt exponentiell mit Zahl der Teilnehmer. Das bedeutet, es gibt stark wachsende statt sinkende Skalenerträge. Wie groß die kritische Masse sein muss, damit sich Netzwerkeffekte sich maßgeblich auswirken, ist abhängig vom jeweiligen Gut.
- ***Emergenz von Standards*:** In der marktgetriebenen Entwicklung des Internet hat sich gezeigt, dass Standards immer weniger von Regulierungsinstanzen geschaffen werden, sondern durch Marktentwicklungen entstehen. Wer eine große Anzahl von Teilnehmern „besitzt“, hat die

Möglichkeit, (seine) Standards zu setzen. Proprietäre Systeme, d.h. Anwendungen, die keine Kompatibilität besitzen, sind zum Scheitern verurteilt. Im Internetgeschäft geht es also darum, möglichst schnell möglichst viele Teilnehmer/Nutzer anzuziehen, um eine kritische Masse zu erreichen, die Basis für die Bildung eines Standards sein kann.

- ***Gratisstrategien*:** Um diesen Effekt zu nutzen und zu beschleunigen, bieten viele Unternehmen/Organisationen ihre Informationen und Leistungen gratis an. Erst in einem zweiten Schritt, wenn genügend Teilnehmer vorhanden sind, werden kostenpflichtige komplementäre Produkte oder Updates veräußert. Nicht bilanzierbare Assets wie Kundenbesitz und Know-how werden so zu wertbestimmenden Treibern von Größen- und Verbundvorteilen.
- ***Zentralisierungstendenz:*** Da die Grenzkosten der Datenhaltung und -übertragung gering sind, ergeben sich in diesem Bereich erhebliche Kostenvorteile durch Größe. Die Konsequenz ist eine Zentralisierung auf Seiten der technischen und organisatorischen Infrastruktur, die für den Betrieb von IT-Systemen erforderlich ist.

eSig im Kontext der Internetentwicklung[11]

Diese Regeln gelten auch für die elektronische Signatur, sofern man sie in der gesetzlich regulierten Form als (deutsches/europäisches) „Produkt" begreifen will, das aus Sicht des Gesetzgebers zu einem Standard werden soll.

Betrachtet man die aktuelle Situation im Bereich eSig so zeigt sich aber, dass die o.g. Regeln nicht durchgängig beachtet werden oder möglicherweise noch keine Anwendung finden, weil die Märkte noch nicht ausreichend entwickelt bzw. anders strukturiert sind.

Der Erwerb einer Signaturkarte einschließlich Nutzungsgebühr für ein Jahr kostet derzeit ca. 150 DM einschließlich Kartenlesegerät und ggf. einer eMail-Anwendung. Die für Privatpersonen beziehbaren Produkte sind noch verbesserungsfähig; die Abläufe sind deutlich nicht routiniert (vgl. Bestandsaufnahme).

Das Dilemma, in dem sich Institutionen befinden, die eine qualifizierte elektronische Signatur einsetzen wollen, besteht darin, dass die Anfangsinvestitionen der Pioniere für die Überwindung technischer und anderer Hindernisse groß sind und gleichzeitig aber noch keine Einsparungen durch Größenvorteile realisiert werden können.

Die zentrale Herausforderung im Rahmen der Einführung von eSig besteht deshalb darin, möglichst schnell möglichst viele Transaktionen mit der Signatur abzuwickeln. Da dies derzeit mangels verbreiteter Anwendungen noch nicht der Fall ist, muss derjenige, der seine Kommunikations- und Transaktionspartner dazu bringen will, die hohe (teure) Sicherheitsstufe der Signatur zu verwenden, zusätzliche Anreize geben, so z. B.:

- Kostenlose Verteilung oder Subvention von Hard- und Softwarekomponenten
- Zusatzangebote, Bonussysteme
- Bereitstellung von günstigen Softwareanwendungen, bei denen die Signaturfunktion genutzt werden kann

[11] Vgl. auch Grabow, U.: Ökonomische Voraussetzungen und Fragen, in: Deutsches Institut für Urbanistik (Hrsg.): Berichte aus der Begleitforschung MEDIA@Komm, Ausgangssituation, Rahmenbedingungen und Hintergründe für die Umsetzung der MEDIA@Komm-Projekte, 2/2000, S. 48ff und ders.: Ökonomische Aspekte, in: Die Startphase der Preisträgerkonzepte. Erste Einschätzungen und Handlungsbedarfe, in: Berichte aus der Begleitforschung MEDIA@Komm, 3/2000, S. 35ff.

- Zwang durch Regulierung (z. B. Nutzung der qualifizierten Signatur im öffentlichen Vergaberecht vorschreiben)

Eine weitere Herausforderung besteht darin, die richtige Balance zwischen Regulierung und Marktentwicklung zur erarbeiten. Nationale Alleingänge im Bereich der Sicherheit entsprechen nicht dem Charakter globaler Standards im globalen Internetgeschäft. Insofern wird sich zeigen, inwieweit die qualifizierte eSig sich als Standard im außereuropäischen B-B-Geschäft entwickeln kann. Besonders interessant wird sich dies bei Transaktionen mit dem amerikanischen Markt darstellen, denn das dortige Signaturgesetz überlässt dem Markt vollständig die Ausgestaltung und das Sicherheitsniveau der Signatur.

Die oben genannten Regeln lassen sich an einem einfachen Beispiel verdeutlichen: Wenn ein Mitarbeiter des Landes Niedersachsen für die Tätigkeit bei seinem Arbeitgeber eine Chipkarte bekommt, die aufgrund der gesetzlichen Bestimmungen des SigG an ihn als natürliche Person gebunden ist, dann muss er mit dieser Karte auch

- seine persönliche Steuererklärung (Elster) abgeben können,
- an der Landtagswahl (eVoting) teilnehmen können,
- seiner Hausratversicherung eine Schadensmeldung per eMail zukommen lassen können (rechtsgeschäftliches Schriftformerfordernis, §127 BGB),
- gegen die Gebührenfestsetzung des Jugendamtes für den Kindergartenplatz seiner Tochter Widerspruch per eMail einlegen können (VwVfG, Schriftform oder zu Niederschrift bringen).

Hier zeigt sich, dass das häufig zu hörende Argument, dass ein Bürger sich wegen einer einzelnen Anwendung nicht die Infrastruktur für qualifizierte Signaturen zulegen würde, obsolet ist. In Hinblick auf die Chipkarte hat der Landesmitarbeiter für seine privaten Rollen kostenlosen Zugang zur Infrastruktur. Der Wert der Infrastruktur steigt, je mehr Anwendungen damit erreichbar sind, der Preis dagegen sinkt wegen der Massenskaleneffekte.

Dieses Phänomen zeigte sich auch in der Anfangszeit des WorldWideWeb im Internet. Zunächst kosteten die notwendigen Browser knapp 100 DM, was für einzelne Anwendungen eine Kosten-Nutzen-Rechnung notwendig machte. Heute gibt es keine Betriebssysteme im PC-Bereich mehr ohne kostenlosen Browser.

Vertrauensinfrastruktur

Neben des reinen Kostenargumentes ist auch das Problem der fehlenden Vertrauensinfrastruktur im Internet und den diesbezüglichen Leistungen relevant. Dies gilt auch für die eSig, weil mit ihr erhebliche persönliche Verpflichtungen eingegangen werden können; das Erfahrungswissen aber noch sehr gering ist. In der klassischen Ökonomie wird Vertrauen insbesondere durch Markennamen geschaffen. Diese besitzen einen schwer quantifizierbaren Wert, der auf der Tradition der Zuverlässigkeit aufbaut. Bei Neustarts von Internetunternehmen gilt es daher insbesondere, schnell ein Markenzeichen einzuführen und Allianzen aus Reputationsspendern und -empfängern zu schaffen.

Im Hinblick auf die elektronische Signatur liegt es auf der Hand, ein bestehendes Trägermedium zu nutzen und so das Kostenproblem zu reduzieren, Transaktionen zu bündeln und vorhandenes Vertrauen zu nutzen.

Prinzipiell kommen hier sowohl amtliche als auch nichtamtliche Chipkarten oder Ausweise in Frage, die eine hohe Verbreitung innerhalb der Bevölkerung besitzen. Etwa 96% aller Haushalte in Deutschland besitzen einen Telefonanschluss; etwa die Hälfte verfügt über einen PC und ca. 35% haben einen Internetanschluss (Daten aus 2000). Für den Einsatz der eSig ist jedoch nicht zwingend ein (eigener) PC erforderlich. Zugangsmöglichkeiten könnten auch über Kiosksysteme geschaffen werden. Die wichtigsten sind in der folgenden Tabelle aufgelistet und wurden in Bezug auf 5 Kriterien bewertet. Eine Erläuterung zur Bewertung ist als Anlage 2 beigefügt.

Potenzielle Trägermedien für eine eSig	**Verbreitungs-grad (in % deut. Bürger > 16 Jahre)**	**Vertrauen**	**Gewohnheit**	**Kurzfr. Umsetz-barkeit**	**Interesse Eigentü-mer an eSig**
Personalausweis	99%	hoch	hoch	gering (R)	hoch
Krankenversichertenkarte	97,5%	hoch	mittel	gering (R)	hoch
Sozialversicherungsausweis	90%	hoch	gering	gering (R)	hoch
EC-Karte	70%	hoch	hoch	hoch	mittel
Mobiltelefonkarte	35%	mittel	hoch	gering (T)	hoch
Beliebige pers Gegenstände	100%	?	hoch	gering (T)	k.A.

Tabelle 3-1: Vergleich der Eignung verschiedener potenzieller eSig-Trägermedien

R = rechtliche Gründe, T = technische Gründe, O = organisatorische Gründe

Der Vergleich zeigt, dass aus Gründen der Verbreitung und des Eignerinteresses die amtlichen Trägermedien grundsätzlich zu bevorzugen wären. Aufgrund der rechtlichen Komplexität sind sie jedoch nicht kurzfristig hierfür nutzbar. Insbesondere sind Personalausweis und Sozialversicherungsausweis nach Rasterfahndung, Datenschutzdebatte und Verwerfen des maschinenlesbaren Ausweis belastet und können nicht wie in Finnland für eine schnelle Umsetzung herangezogen werden. Insofern kommen insbesondere die Chipkarten der Banken und – sofern die technische Entwicklungen entsprechend verläuft – (Mobil-) Telefonanbieter als Träger für eSig in Frage.

Fazit Rahmenbedingungen

Die Ausführungen zu den Rahmenbedingungen zeigen, dass der Anspruch, mit der eSig ein elektronisches Substitut zur eigenhändigen Unterschrift zu schaffen, nicht gelingen kann, da beide Formen der Unterschrift sich zu sehr unterscheiden (vgl. nachfolgende Tabelle).

Merkmale	händische Unterschrift	eSig
Begriffliche Klarheit	eindeutig definiert	nicht eindeutig definiert, erklärungsbedürftig
Vertrautheit	hoch	gering
Bezug	natürliche Person	natürliche Person
Nachprüfbarkeit	unbegrenzt	i.d.R. 2 Jahre, bei akkedit. Trustcentern 30 Jahre?
Fälschungssicherheit	eher niedrig	hoch
Fehleranfälligkeit	keine	(noch) sehr hoch
Verfügbarkeit	überall	nur in spezifischem technischem Umfeld
Individualisierbarkeit	persönliche Formgebung möglich	Spezifikation über Attributierung bzw. Pseudonyme
Kosten	keine	derzeit ca. 150 DM

Tabelle 3-2: Vergleich eigenhändige Unterschrift – eSig

Diese Feststellung ist zwar offensichtlich; gleichwohl müssen diese Unterschiede bewusst gemacht werden, um zu verdeutlichen, welchen Probleme sich die Durchsetzung der eSig gegenübersieht und dass nicht versucht werden sollte, eine zu starke Assoziation mit der händischen Signatur aufzubauen.

Insbesondere für die Warnfunktion, bei der die kulturelle Verankerung der eSig wohl am deutlichsten hervortritt, gibt es in gravierenden Fällen (noch) kein äquivalentes elektronisches Abbild. Daher sollte bei der Information über die eSig deutlich werden, dass es nicht darum geht, jegliche Art der händischen Unterschrift zu ersetzen, sondern mit der eSig ein Angebot zu schaffen, das für bestimmte abstrakt-standardisierte Prozesse eine Vereinfachung darstellt.

Die Debatte über elektronische Signaturen wurde lange Zeit weitestgehend durch einen technisch-juristischen Expertendiskurs geprägt. Dabei wurde häufig unzureichend berücksichtigt, dass die objektive Risikobeurteilung durch Fachleute häufig ganz anders ausfällt als die subjektive Wahrnehmung von potenziellen Anwendern. Dementsprechend wird auch der Nutzen von sicherheitsinduzierenden Produkten wie der eSig möglicherweise abweichend beurteilt. (Dies zeigt sich deutlich an der enormen Akzeptanz von Elster, der elektronischen Steuererklärung).

Daher sind die vorgenannten Vorteile einer eSig so lange rein theoretisch, bis sie sich nicht in der praktischen Anwendung tatsächlich beweisen. Hier kann die Analyse der Erfahrungen mit dem tatsächlichen Einsatz von eSig, wie sie die nachfolgende Bestandsaufnahme zeigt, wichtige Erkenntnisse und Anregungen geben.

Die folgenden zusammenfassenden Ausführungen zu den Ergebnissen der Bestandsaufnahme von laufenden Projekten und geplanten Vorhaben zur eSig geben einen Überblick über die auf den Verwaltungsebenen existierenden Projekte. Dabei liegt der Schwerpunkt auf den für die jeweilige Verwaltungsebene spezifischen Problemen. Eine ausführliche Beschreibung der einzelnen Projekte ist den Projektprofilen in Anlage 1 zu entnehmen.

4 Ergebnisse der Bestandsaufnahme von eSig-Vorhaben

4.1 Überblick

Pilotprojekte und Anwendungen mit Einsatz der elektronischen Signatur sehen sich einer Reihe von Problemen gegenübergestellt:

- nicht vollständig geklärte Rechtslage
- unzureichende Standardisierungen
- geringes Erfahrungswissen
- komplexe Gemengelage zwischen organisatorischen und technischen Aspekten

Legt man diese schwierigen Ausgangsvoraussetzungen zu Grunde, so ist der gegenwärtige Stand durchaus positiv zu beurteilen. Electronic Government in Deutschland entwickelt sich kontinuierlich, wie folgende Schlagzeilen illustrieren:

- 2000 Studierende wählen per Chipkarte – Beamte unterschreiben digital; Niedersachsen macht Ernst mit dem Einsatz elektronischer Signaturen“ – Computerwoche, 11. Februar 2000
- „eCommerce wird Maßstab für den Staat – Verwaltung muss sich auf kundenfreundliche elektronische Dienstleistungen einstellen“ – Süddeutsche Zeitung, 3. Juli 2000
- „Pilotprojekt in Baden-Württemberg hat sich bewährt; Digitale Grundbucheinträge sparen Kosten und sorgen für mehr Bürgernähe“ – Computerwoche, 24. November 2000
- „Das modernste Dorf Deutschlands. Oberhambach ist (dr)in – Ein verschlafenes Nest aus dem Hunsrück ist seit Freitag offiziell Deutschlands erste Online-Gemeinde mit virtueller Einkaufsstadt“ – Die Welt, 5. März 2001

Wenngleich Zeitungsmeldungen oft den faktischen Sachverhalten vorauseilen, so können doch im Untersuchungsfeld „elektronische Signaturen“ bereits innovative Anwendungen und verschiedene erfolgreiche Piloten ausgemacht werden. Neben „echten“ eSig-Projekten, d.h. Vorhaben, in denen eine (qualifizierte) eSig eingesetzt wird, hat KPMG im Rahmen der Bestandsaufnahme auch solche Vorhaben berücksichtigt, die aktuell teilweise noch keine eSig einsetzen, bei denen dies nach Einschätzung von KPMG jedoch mit einer gewissen Sicherheit und Konkretheit geplant ist.

Orientiert man sich zunächst an den **Anwendungsbereichen**, so wird erwartungsgemäß ein leichter Trend erkennbar, der darin besteht, dass auf der kommunalen Seite eher G-C und G-B-Lösungen verfolgt werden, also Projekte im Bereich Verwaltung zu Bürger (Government to Citizen) und Verwaltung zu Unternehmen (Government to Business), während auf der Seite der Länder und des Bundes tendenziell eher G-B und G-G-Lösungen angestrebt werden, also Projekte innerhalb der Verwaltung oder zu Organisationen (Wirtschaft, professionelle Benutzergruppen).

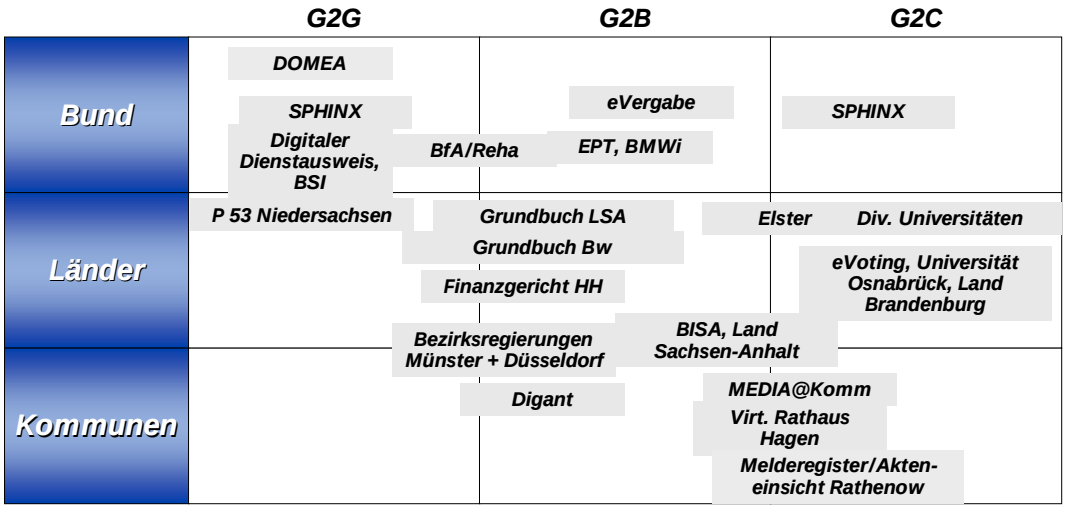


Abbildung 4-1: Identifizierte eSig-Projekte nach Anwendungsbeziehungen

Einige Projekte auf Landesebene (einschließlich der Bezirksebene) finden in den Fachanwendungen statt. Auf Ebene des Bundes liegt der Fokus eher auf ressortübergreifenden Infrastrukturthemen (Workflow, eMail-Austausch) – eine Linie, zu der jedoch auch viele der Länder neigen.

Der **Projektfortschritt** der vorliegenden Projekte ist auch vor dem Hintergrund der genannten Definitionsprobleme unterschiedlich zu bewerten. Ein Großteil der Projekte lässt sich den Stufen I (Ideen) oder II (Konzept) zuordnen; weitere Projekte haben bereits den Experiment-Status (Stufe III) erreicht. Nur wenige Projekte können als Stufe IV (bewährte Anwendung) betrachtet werden. Es gibt praktisch nur eine echte Großanwendung (Haushaltswirtschaftsystem Niedersachsen). Die nachfolgende Grafik stellt die Projekte in der gegenwärtigen Zuordnung dar.

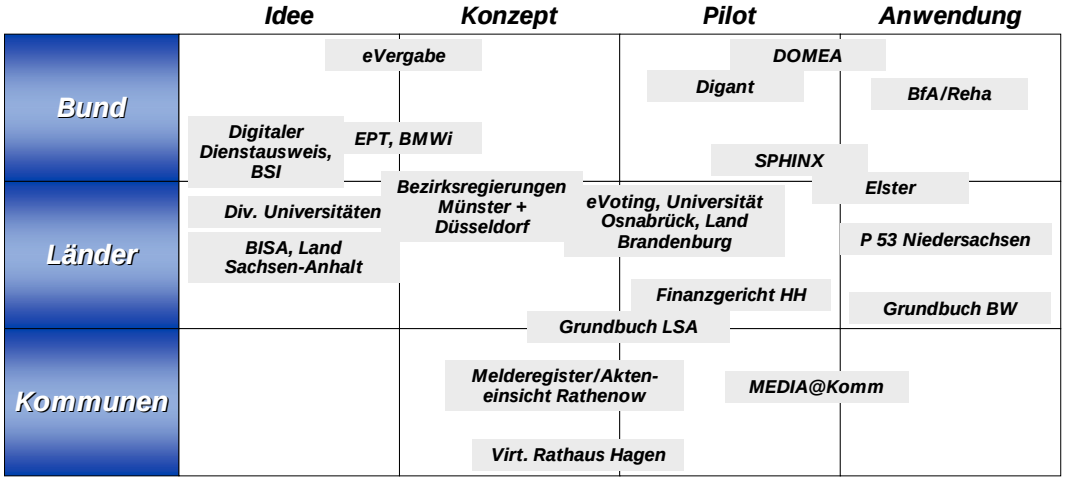


Abbildung 4-2: Identifizierte Projekte nach Umsetzungsstand

Aus den bisherigen Darstellungen lassen sich keine Aussagen über den Erfolg einzelner Projekte ableiten. Auf eine derartige Zuordnung soll auch bewusst verzichtet werden, da das Ziel der Untersuchung nicht in der detaillierten Prüfung einzelner Projekte, sondern in einer Darstellung und kritischen Generalisierung vorliegender Einzelfallergebnisse liegt, soweit sie sich im Rah-

men der Projektlaufzeit erschließen. Diesem Auftragsziel soll in den nachfolgenden Kapiteln nachgegangen werden.

Dabei werden zunächst Projekte auf Ebene des Bundes, der Länder und schließlich der Kommunen synthesenartig dargestellt, bevor auf Akteure an der Schnittstelle zur Wirtschaft eingegangen wird.

4.2 Vorhaben des Bundes

Im Rahmen der Initiative BundOnline2005 werden derzeit 14 Modellverfahren durchgeführt. Darunter gibt es mehrere Projekte, in denen elektronische Signaturen eingesetzt werden bzw. eingesetzt werden sollen. Zu nennen sind:

- Elektronische Vorgangsbearbeitung von Akten (DOMEA)
- eMail-Sicherheit (SPHINX)
- Elektronische Beschaffung und Vergabe
- Sozialversicherung
- MEDIA@Komm - Leitprojekt des BMWi, BMI und BMVBW (Vorstellung unter P. 4.4.2)

Im Folgenden werden die einzelnen Projekte kurz vorgestellt. Weitere Informationen sind den Projektprofilen in Anlage 1 zu entnehmen.

4.2.1 DOMEA

Das Projekt DOMEA wurde 1996 bei der Koordinierungs- und Beratungsstelle der Bundesregierung für Informationstechnik in der Bundesverwaltung im Bundesministerium des Innern (KBSt) initiiert.

Ziel des Projekts ist der „Aufbau eines Pilotsystems für Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang“, m. a. W. der Aufbau eines Dokumentenmanagementsystems in der Ministerialverwaltung.

DOMEA beinhaltet ein Konzept, das die organisatorischen und technischen Anforderungen dieses Pilotsystems spezifiziert. Insbesondere sieht DOMEA eine stufenweise Nutzung des Systems vor; ausgehend von einem Schriftgutverwaltungssystem über die elektronische Aktenablage bis zur elektronischen Vorgangsbearbeitung.

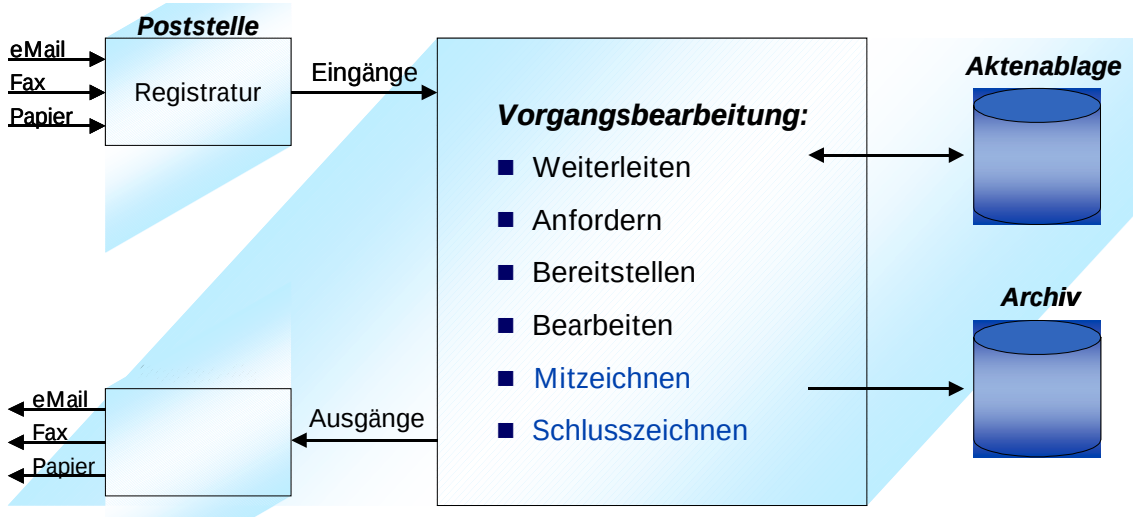


Abbildung 4-3: Vorgangsbearbeitung mit DOMEA

Wie bei der konventionellen Bearbeitung von Akten gibt es auch bei der elektronischen Bearbeitung die Notwendigkeit der Mitzeichnung bzw. Schlusszeichnung. Die Unterschrift kann dabei durch die elektronische Signatur realisiert werden.

Gegenwärtig gibt es zahlreiche Behörden, in denen das DOMEA-Konzept umgesetzt wird. Dabei handelt es sich aber zum Großteil um Implementierungen in einzelnen Referaten bzw. um nachgeordnete Behörden mit wenigen Nutzern, wie nachfolgende Tabelle zeigt. Das größte DOMEA-Projekt wird zur Zeit im Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) realisiert, in dem ab März 2001 1.500 Anwender geplant sind.

Anwender	Nutzer IST	Nutzer Plan	Hersteller	Lieferant	Produkt[12]
Bundesverwaltungsamt	380	2000 (2002)	Debis GEI	Debis GEI	Favorit
Bundespräsidialamt	180		Compaq	Compaq	VIS kompakt
BAFl	100	1.500 (03/2001)	SER	SBS	DOMEA
KBSt	25 (alle Mitarbeiter)		SER	SER	DOMEA
BSI	15 (ein Referat)		SER	SER	DOMEA
BMJ	55 (Registratur)		SER	SER	DOMEA
RegTP		ca. 30 (2001)	Debis GEI	Debis GEI	Favorit
BStMLU (Bayern)	500 (alle Mitarbeiter)		Compaq	Compaq	VIS kompakt
Land NRW	10	40 (2002)	Debis GEI	Debis GEI	Favorit

Tabelle 4-1: Überblick über ausgewählte DOMEA-Projekte

Abgesehen von der relativ niedrigen Anwenderzahl wurden die bisherigen Erfahrungen von fast allen befragten bzw. untersuchten Behörden als gut bezeichnet. Als Hindernisse wurden Akzep-

[12] Zu beachten ist, dass es das DOMEA-Konzept der KBSt gibt und ein gleichnamiges Softwareprodukt der Firma SER.

tanzprobleme beim Anwender und Schwierigkeiten bei der Anpassung von organisatorischen Abläufen an DOMEA genannt.

Im Rahmen der Recherche hat sich allerdings gezeigt, dass es derzeit keinen Einsatz von elektronischen Signaturen im Rahmen von DOMEA gibt. Die Zeichnung von Dokumenten wird stattdessen mit der Eingabe des Benutzernamens und einem persönlichen Passwortes realisiert. In zahlreichen Behörden besteht jedoch ein Interesse an dem Einsatz elektronischer Signaturen, wobei zunächst die für 2001 geplanten Gesetzesänderungen abgewartet werden.

4.2.2 SPHINX (eMail-Sicherheit)

Das Pilotprojekt SPHINX wurde unter Federführung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) 1998 initiiert, um den Austausch von signierten und verschlüsselten eMails in der öffentlichen Verwaltung zu realisieren.

Mit dem Pilotprojekt werden folgende Ziele verfolgt:

- Test der Interoperabilität von Produkten verschiedener Hersteller
- Gewinn von Erkenntnissen über die Akzeptanz bei den Anwendern
- Ermittlung der Aufwände, die mit der Einführung der eingesetzten Produkte in der öffentlichen Verwaltung verbunden sind

Ferner soll eine Basis zur breiten Einführung von Produkten, die konform zum Signaturgesetz sind, geschaffen werden.

An SPHINX beteiligt sind über 50 Organisationen, darunter der Deutsche Bundestag, Bundesministerien und -behörden, Einrichtungen der Bundesländer aber auch verschiedene Unternehmen aus dem privaten Sektor. Die Anzahl der Endanwender (siehe Tabelle 4-2) wurde dabei absichtlich gering gehalten, weil der Fokus auf der Einbindung einer Vielzahl von unterschiedlichen Organisationen aus der öffentlichen Verwaltung (Bund, Länder, Kommunen) und der Wirtschaft lag und nicht auf einer großen Teilnehmeranzahl innerhalb einer Organisation.

Phase	Zeitraum	Anzahl der Endanwender
1	April 1998 – September 1998	180
2	Oktober 1998 – März 1999	350
3	Dezember 1999 – Dezember 2000	600

Tabelle 4-2: Anzahl der SPHINX-Endanwender je Phase

Im Pilotprojekt werden Software-Produkte verschiedener Hersteller eingesetzt. Die Produkte umfassen sowohl Anwendungen, die für den Betrieb einer PKI notwendig sind, als auch Anwendungen, die den Austausch von signierten und verschlüsselten eMails ermöglichen. Um die Interoperabilität zwischen den Produkten der unterschiedlichen Hersteller zu gewährleisten, hat man sich auf den herstellerübergreifenden Standard MailTrusT des TeleTrust e.V.[13] geeinigt. MailTrusT umfasst eine Vielzahl international anerkannter Standards (z. B. X.509, PKIX, PEM,

[13] Verein zur Förderung der Vertrauenswürdigkeit von Informations- und Kommunikationstechnik“ mit 110 Mitgliedern aus Forschung, Entwicklung und Politik.

S/MIME). Innerhalb dieser Standards sind allerdings viele Parameter frei wählbar, die im Rahmen von MailTrusT aus Interoperabilitätsgründen fest definiert werden (sogenannte Profile). Das führt allerdings u.a. dazu, dass die Interoperabilität zu weitverbreiteten eMail-Anwendungen (Microsoft Outlook, Netscape Messenger) nicht mehr gewährleistet ist.

Bei der Entwicklung der eingesetzten Produkte bestand der Fokus auf der Gewährleistung der Interoperabilität. Auf eine Prüfung der Produkte nach SigG 1997 wurde verzichtet, weil das die geforderte Fortentwicklung der Produkte nicht zuließ oder die Erstellung von Produkten sehr aufwendig machte.

Das Pilotprojekt wurde in drei Phasen durchgeführt. Die ersten beiden Phasen wurden durch das Bundesministerium des Inneren finanziert, die dritte Phase durch das BSI.

In der Phase 1 wurden ein Gesamtkonzept für den sicheren Austausch von eMails auf Basis der MailTrusT-Spezifikation entwickelt und piloteigene Zertifizierungsstellen aufgebaut. In den Phasen 2 und 3 wurde das Gesamtkonzept um zusätzliche Anforderungen erweitert bzw. an die gewonnenen Erkenntnisse aus den vorangegangen Phasen angepasst. Insbesondere wurde in der Phase 2 ein Verzeichnisdienst aufgebaut und in Phase 3 das bisherige Austauschformat für e-Mails PEM durch S/MIME ersetzt.

Das Pilotprojekt wurde Ende 2000 beendet und in den Wirkbetrieb überführt. Im Rahmen des Wirkbetriebs wird eine neue PKI aufgebaut, deren Wurzelzertifizierungsstelle (Root-PCA) durch das BSI betrieben wird. Die Root-PCA legt Sicherheitsrichtlinien (Certificate Policy) fest, durch die ein bestimmtes minimales Sicherheitsniveau definiert wird. Insgesamt sind aber verschiedene Sicherheitsniveaus vorgesehen. Unter anderem wird ein Sicherheitsniveau angestrebt, das den Anforderungen an qualifizierte Signaturen nach dem neuen Signaturgesetz entspricht.

Zertifizierungsstellen, die die Interoperabilitäts- und Sicherheitsrichtlinien der Root-PCA erfüllen, können von der Root-PCA zertifiziert werden und werden dadurch Teil der PKI. Zertifizierungsstellen aus folgenden Bereichen sind zertifiziert bzw. haben die Zertifizierung beantragt:

- Bundesverwaltung (IVBB, Bundeswehr)
- Landes- und Kommunalverwaltung
- private Zertifizierungsstellen (z. B. Telesec und TC Trustcenter)

Ferner ist geplant, dass sich die Root PCA des BSI an einem Zusammenschluss mehrerer Root-PCAs (u.a. von der Dt. Bank und Dt. Telekom) beteiligt, die durch den Mechanismus einer Bridge-CA miteinander verbunden werden sollen. Derzeit stehen fortgeschrittene Signaturen und die Interoperabilität von S/MIME-Produkten im Vordergrund. Eine Ergänzung um qualifizierte Signaturen ist geplant.

Insgesamt hat SPHINX dazu beigetragen, Erkenntnisse und Erfahrungen zu gewinnen, die mit dem Einsatz von elektronischen Signaturen verbunden sind (Aufbau/Betrieb einer PKI, Akzeptanz beim Anwender etc.). Allerdings hat SPHINX bisher keinen maßgeblichen Effekt auf die Verbreitung von elektronischen Signaturen gehabt. Die Verbreitung ist u. a. von der Steigerung der Nutzerzahlen im Wirkbetrieb abhängig und von der Lösung der Interoperabilitätsprobleme zu den weitverbreiteten eMail-Anwendungen, um den Austausch von signierten und verschlüsselten Emails mit Anwendern zu gewährleisten, die nicht an SPHINX teilnehmen.

4.2.3 eMail-Sicherheit in der RegTP

In der Regulierungsbehörde für Telekommunikation und Post (RegTP) wird gegenwärtig die Anwendung qualifizierter digitaler Signaturen, die auf dem Signaturgesetz von 1997 basieren, im Rahmen eines Pilotprojekts, an dem ca. 100 Personen beteiligt sind, erprobt. Hauptanwendungsgebiet ist der Austausch sicherer eMails. Gegenstand der Erprobung sind auch Produkte zur Verschlüsselung von Nachrichten.

4.2.4 „eVergabe“ - Elektronische Vergabe von öffentlichen Aufträgen

Das Pilotprojekt „eVergabe“ beinhaltet die elektronische Vergabe von öffentlichen Aufträgen des Bundes. Es ist Bestandteil der Initiative „BundOnline2005“ und wurde vom Bundesministerium für Wirtschaft und Technologie, vom Bundesinnenministerium und vom Bundesministerium für Verkehr, Bau und Wohnungswesen initiiert. Gegenstand der elektronischen Vergabe werden Dienstleistungen, Waren und Bauleistungen sein. Eine Einschränkung auf bestimmte Produkte findet nicht statt.

Die für die eVergabe notwendige Änderung der Vergabeordnung wurde am 13.12.2000 vom Bundeskabinett beschlossen. Die Neuregelung ist zum 1.2.2001 in Kraft getreten. Damit wird das Einreichen von Angeboten in elektronischer Form möglich, soweit diese mit einer elektronischen Signatur versehen sind.

Beteiligt am Pilotprojekt sind

- das Bundesamt für Bauwesen und Raumordnung BBR und
- das Beschaffungsamt des Bundesinnenministerium.

Für den Einsatz der elektronischen Signatur soll jeder Mitarbeiter (ca. 1.000) der teilnehmenden Behörden mit einer Signaturkarte ausgestattet werden. Das Pilotprojekt wird wissenschaftlich begleitet.

Das Ziel der eVergabe ist es, den ganzen Vorgang der Auftragsvergabe abzubilden. Folgende Teilschritte bei der Vergabe von öffentlichen Aufträgen sollen dabei berücksichtigt werden:

- Bekanntmachung der Ausschreibung
- Anforderung der Verdingungsunterlagen durch die Bieter
- Angebotsaufforderung
- Angebotsabgabe des Bieters / Eingang des Angebots in der Behörde
- Sammeln und Öffnen gem. §22 VOL/A
- Prüfung und Bewertung der Angebote
- Mitteilung an die Bieter
- Zuschlag/Vertragsabschluss

Im gesamten Vorgang soll es zu keinem Medienbruch kommen.

Die folgende Tabelle gibt einen Überblick über den Zeitplan des Pilotprojektes.

Zeitplan	Inhalt
Dezember 2000 bis Januar 2001	Abschluss des Feinkonzepts
Anfang 2001	Ausschreibung für die Implementierung des Feinkonzepts
Frühjahr 2001	geplante Auftragsvergabe
Sommer oder Herbst 2001	Erster Testbetrieb
Anfang 2002	Aufnahme Pilotbetrieb

Tabelle 4-3: Zeitplan für das Projekt „eVergabe“

Der Nutzen der elektronischen Vergabe von öffentlichen Aufträgen wird vor allem in Kosteneinsparungen beim Bieter und Auftraggeber und in der Steigerung der Effizienz des Verfahrens gesehen.

Der primäre Erfolgsfaktor für das Gelingen des Pilotprojekts wird in der Akzeptanz der Bieter gesehen. Innerhalb der Behörden werden keine größeren Hemmnisse erwartet.

4.2.5 Sozialversicherungsträger

Bei den öffentlichen Sozialversicherungsträgern (Renten- und Unfallversicherer) sind fast alle Erwerbstätigen versichert. Daher ist es nicht verwunderlich, dass nach Angaben des Bundesministeriums für Arbeit und Sozialordnung durch die Rechtsänderung im Bereich der Sozialversicherung zehn Prozent der Verwaltungskosten gespart werden könnten. Das ist bei zehn Milliarden Mark im Jahr ein Einsparpotenzial von rund einer Milliarde Mark pro Jahr [14].

Obwohl bereits 1999 wurde die „Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung“ umgesetzt wurde, die eine Gleichstellung gesetzeskonforme elektronischer Signaturen mit handschriftlichen Unterschriften vorsieht, ist eine Verbreitung der eSig im Bereich der Sozialversicherung bisher nicht erkennbar. Hierzu im Einzelnen:

Die *Rentenversicherungsträger* beabsichtigen, die qualifizierte elektronische Signatur in der Archivierung einzusetzen, und zwar in den folgenden Prozessschritten:

- Kontenzustand vor der Leistungsberechnung
- Druckergebnisse aus der Leistungsberechnung
- Digitale Aufnahme des Aktengutes (Scannen der Unterlagen)

Das Vorhaben befindet sich in der Detaillierungsphase. Ein Pilotprojekt läuft bei der LVA Baden. Beim Verband der Rentenversicherer gibt es eine Projektgruppe „Einführung von Chipkarten in der Rentenversicherung“, die das Ziel hat, qualifizierte eSig in der Kommunikation zwischen den RV-Trägern zu implementieren.

Die *Bundesversicherungsanstalt für Angestellte* (BfA) betreibt ein nicht zertifiziertes Trust-Center für die Absicherung des Datenaustausches mit medizinischen Leistungserbringern, das

[14] Wendelin Bieser : http://www.heise.de/ct/99/01/058/, Interview in der Zeitschrift C’t , 3.11.99.

nach § 301 SGB V Zertifikate für die eigenen Kliniken und die Reha-Vertragskliniken der BfA ausstellt. Das Trustcenter wurde auskunftsgemäß bisher nicht ausgebaut, weil zum einen die rechtlichen Anpassungen noch ausstanden und da technische Voraussetzungen bisher eine Ausstellung von Karten vor Ort erschwerten und die Karten interoperabel sein sollen, damit sie auch im Geschäftsverkehr mit Dritten angewendet werden können.

Im *Verband Deutscher Rentenversicherungsträger* (VDR) beschäftigen sich der Fachausschuss für Organisation (FAO), die Datenkommission (DAKO) und die ADV-Arbeitsgruppe (ADVAG) mit dem Einsatz von Chipkarten in der Rentenversicherung. Letztere hat eine Projektgruppe „Chipkarte in der Rentenversicherung“ (PGCKRV) beauftragt,

- Einsatzmöglichkeiten von Chipkarten in Geschäftsprozessen der Rentenversicherungsträger zu evaluieren,
- Standardisierungsbedarf innerhalb der RV zu identifizieren,
- Pilotprojekte zu benennen,
- die Chipkarten-Infrastruktur zu identifizieren und
- Kosten-Nutzen-Aspekte zu beleuchten.

Bei den *Unfallversicherern* finden derzeit vorbereitende Maßnahmen statt (u.a. Informationsveranstaltungen, Marktanalysen, Identifikation von Pilotanwendungen).

Die *Bundesanstalt für Arbeit* beabsichtigt, die Möglichkeiten der eSig zu nutzen und auf die sich aus dem Projekt SPHINX ergebenden Empfehlungen des BSI für die Bundesverwaltung aufzusetzen.

4.2.6 Sonstige Projekte auf Bundesebene

Aufgrund ihrer Größe und Relevanz sollen hier noch zwei weitere Projekte auf der Ebene des Bundes genannt werden, die grundsätzlich auch Anknüpfungspunkte für den Einsatz der eSig bilden. Dabei handelt es sich um die elektronische Steuererklärung (Elster) und ein im weiteren Sinne zum Bund gehöriges Projekt zur Online-Bestellung von Personalausweisen durch die Kommunen (Digant).

Elster

Steuerpflichtige können mit Elster, das mittlerweile in allen Bundesländern läuft, ihre Erklärungen oder Bilanzen auf den entsprechenden Formblättern an das zuständige Finanzamt per Internet übermitteln.

Zum Schutz des Steuergeheimnisses verschlüsselt das Programm die Daten mit einem 112-Bit-Triple-DES-Schlüssel und einem 1024 RSA-Schlüssel, also auf hybride Weise. Der Output aus Standard-Paketen (Taxman usw.) wird per Internet oder ISDN die an Finanzbehörde übermittelt. Das erspart der Behörde die eigenhändige Eingabe der Daten. Parallel dazu wird der Output ausgedruckt, unterzeichnet und der Behörde zugesendet. Alle Bundesländer nehmen die Erklärungen an. Das Land Bayern entwickelt und pflegt die Software für die anderen Länder mit. Wahlweise kann auch der Steuerbescheid „rückübermittelt“ werden. Da die Belege sowieso per Post nachgeschickt werden müssen, stellt das Fehlen einer elektronischen Signatur keinen Medienbruch dar. Bis zum Januar 2001 waren 150.000 Steuererklärungen und

dienbruch dar. Bis zum Januar 2001 waren 150.000 Steuererklärungen und Steueranmeldungen eingegangen, Zielgröße sind 220.000.

Neben der Einkommensteuer können mit Elster auch die Umsatzsteuervoranmeldung, der Antrag auf Dauerfristverlängerung, die Anmeldung von Sondervorauszahlungen und die Lohnsteueranmeldung Online erledigt werden.

Zynischerweise führte das Aufdecken der Tatsache, dass die zu übermittelnden Daten nicht signiert waren und somit hypothetisch das Verfahren einer „Man-in-the-middle-attack" schutzlos ausgeliefert war, zu einer kurzzeitigen Aussetzung bis zur Nachbesserung des Verfahrens.

Bemerkenswert bleibt aber, dass die hohe Elastizität der Steuerbürger (mehrere hunderttausend Nutzer haben das Verfahren trotz eines eher geringen Vorteils genutzt) ein deutlicher Indikator für die hohe Nachfrage elektronischer Dienstleistungen des Staates durch den Bürger ist, die deutlich manche zögerlichen Haltungen übertrifft. Zudem hat Elster für 2002 den Einsatz elektronischer Signaturen angekündigt.

Digant in der Bundesdruckerei

Digant ist ein digitales Antragsverfahren zur Herstellung von Ausweisdokumenten durch die Bundesdruckerei. Dabei werden die bisher 50.000 –70.000 Vorgänge pro Tag durch einen digitalen Datenaustauschvorgang ersetzt. Die für den Ausweis erforderlichen Daten – einschließlich Unterschriften und Fotos des Antragstellers – werden in den Kommunen digitalisiert, drucktechnisch vorbereitet und Online an die Bundesdruckerei unter Verwendung starken Verschlüsselung übermittelt.

Das Verfahren wir derzeit in Modellversuchen in Siegburg und Bad Aibling erprobt.

Es ist insoweit besonders interessant, da es sich bei der Ausstellung von Personalausweisen um eine den Kommunen vom Bund übertragene Aufgabe handelt, die bundesweit einheitlichen Regelungen/Verfahren unterliegt.

Elektronischer Projektträger (EPT)

Im Mittelpunkt des seit 1997 laufenden Projekts des BMWi steht die Fortentwicklung des bestehenden Kommunikationsnetzwerks zwischen BMWi-Referat, Projektträger, Gutachtern und Antragsstellern/Zuwendungsempfängern. Der EPT soll zu einem elektronischen Kommunikations- und Informations-Managementsystem zwischen den Beteiligten mit den Eigenschaften eines Dokumentenmanagement- und Workflowmanagementsystems entwickelt werden. Der Einsatz der elektronischen Signatur soll eine rechtsverbindliche und sichere Information gewährleisten. Das Projekt ist Teil der Initiative „Förderung von Forschung, Entwicklung und Innovation in kleinen und mittleren Unternehmen und externen Industrieforschungseinrichtungen in den neuen Bundesländern" des BMWi sowie der Initiative „Moderner Staat – moderne Verwaltung" von Seiten des Bundes.

Digitaler Dienstausweis

Der bisherige Dienstausweis im Bereich der Bundesbehörden soll durch einen Dienstausweis in Form einer multifunktionalen Chipkarte ersetzt werden. Hierbei sollen zahlreiche Funktionen möglich sein: Optische Ausweisfunktion, Zutrittskontrolle/Zeiterfassung, Zugangskontrolle zu Rechner und Server, digital signierte Speicherung von Ausweisdaten, digitale Signatur, Verschlüsselung, Authentisierung.

Das Bundesamt für Sicherheit in der Informationstechnik schreibt gegenwärtig eine Generalunternehmerschaft aus. Vorgesehen ist eine Pilotphase mit 100 Beschäftigten, die bis Ende des Jahres abgeschlossen werden soll. Nach Abschluss der Pilotphase ist eine Einführung des digitalen Dienstausweises in der Bundesverwaltung geplant.

4.3 Vorhaben bei den Ländern

4.3.1 Überblick

In der nachfolgenden Tabelle findet sich ein Überblick über bestehende Projekte in den einzelnen Bundesländern, in denen die elektronische Signatur eine Rolle spielt. Einzelheiten zu den Projekten können den als Anlage 1 beigefügten Projektprofilen entnommen werden, sofern KPMG hierzu nähere Informationen von Seiten der Projektbeteiligten erhalten hat.

Bundesland	**Identifizierte Projekte auf Landesebene**
Bayern	Außer MEDIA@Komm im Städteverbund Nürnberg keine lfd. Projekte bekannt, Verfolgung SPHINX
Schleswig-Holstein	Keine lfd. Projekte bekannt, Verfolgung SPHINX
Baden-Württemberg	elektronisches Grundbuch [A] Mahnverfahren beim Finanzgericht Karlsruhe Verwaltungsgericht Sigmaringen
Brandenburg	eVoting (Forschungsvorhaben); nach Abschluss Entscheidung, ob andere Einsatzmöglichkeiten (Brandenburg-Card) [A]
Sachsen	Überlegungen, ob Aufbau PKI-Struktur im Rahmen von SPHINX
Sachsen-Anhalt	BISA: Eingliederung eSig in Betriebsinformationssystem beabsichtigt Überlegungen zum eSig-Einsatz im Rahmen des Projekts „Zukunftsregion Wernigerode“
Berlin	Entwicklung eines Konzepts für die PKI-Infrastruktur des Landes
Hamburg	Finanzgericht Hamburg [A]
Mecklenburg-Vorpommern	Digitale Signatur und Verschlüsselung
Niedersachsen	P 53 (Haushaltswirtschaftssystem) [A] eVoting Universität Osnabrück
Rheinland-Pfalz	Ausschreibung DIZ zum Thema einheitliches landesweites Signatursystem

Bundesland	Identifizierte Projekte auf Landesebene
Nordrhein-Westfalen	Vernetzung von 6.500 Schulen für den Austausch von Statistiken Austausch von signierten und verschlüsselten eMails Elektronische Bewerbung (Pilot) Zugriff auf verschiedene Register: Schuldenverzeichnis (für dedizierte Anwender), Handelsregister (geplant), Grundbuch (geplant) Verschiedene Pilotprojekte für die elektronische Antragsstellung Kommunale Kooperation (Bezirksregierung Münster) [A] Virtuelle Bezirksregierung (Bezirksregierung Düsseldorf) [A]
Hessen	Aufbau Projektgruppe für ministeriumsübergreifende eSig-Lösung für eMail + Dokumentenaustausch
Thüringen	Konzeption für Sicherungsverbund für das Land auf Basis der Ergebnisse von SPHINX; freiwilliger Anschluss der Kommunen
Saarland	Vereinheitlichung der eMail-Struktur mit Verschlüsselung (ggf. ohne eSig)

A= Projektprofile in Anlage

Tabelle 4-4: Identifizierte eSig-Projekte auf Landesebene

Das Projekt P 53 des Landes Niedersachsen stellt auf Länderseite das gegenwärtig größte Projekt sowohl in der Anzahl der Nutzer als auch im Hinblick auf die investierten Mittel dar.

Abgesehen davon ist das generelle Verhalten der Länder durch eine eher abwartende Haltung geprägt. Diese wird insbesondere mit rechtlichen Unsicherheiten (v. a. Novelle SigG, SigVO), Unklarheit über die Aktivitäten des Bundes sowie Unsicherheit über die technische Entwicklung zurückgeführt. Ferner lassen sich folgende allgemeine Feststellungen machen:

SPHINX als Orientierungspunkt – Es zeigt sich, dass vor allem die Erfahrungen aus dem SPHINX-Projekt von Interesse sind. Jedenfalls wurde dies von einer Reihe von Ländern explizit benannt. Es lässt sich nicht beurteilen, inwieweit der Verweis auf SPHINX – ähnlich dem häufigen Verweis auf eine unzureichende Rechtslage – als Erklärung für abwartendes Verhalten herangezogen wird. Die Konzentration auf SPHINX dürfte jedoch vermutlich damit zusammenhängen, dass

- die Entwicklung von SPHINX (siehe hierzu unter ‚Vorhaben des Bundes') von den Ländern besonders intensiv und kritisch begleitet wurde,
- SPHINX der eher ressortübergreifenden Orientierung der Länder entgegenkommt,
- bei vielen Ländern eine „SPHINX-freundliche" Dateninfrastruktur besteht,
- über SPHINX eine gute Datenlage existiert.

Die Fixierung und bemühte Einflussnahme auf SPHINX mag auch mit der skeptischen Haltung der Bundesländer gegenüber dem Bund zusammenhängen, die auskunftsgemäß aus den Erfahrungen mit X.400 herrühren.

Infrastrukturorientierung – Standardisierungsprobleme existieren u. a. aufgrund der durchgängig heterogenen Ländersystemkonzepte (Computertechnologie und Software), die durch unre-

gelmäßige Investitionen von Seiten der Länder, Kommunen und des Bundes in Informationstechnologie begünstigt werden. So werden Investitionen häufig länder- oder ressortspezifisch „nach Kassenlage" – und damit zeitlich unkoordiniert – getätigt, was u.a. zu unterschiedlichen Softwareversionen führt. Positiv ist anzumerken, dass seitens verschiedener Länder vor diesem Erfahrungshintergrund Bestrebungen bestehen, einheitliche Landessystemkonzepte zu entwickeln, in die auch die Kommunen einbezogen werden sollen. Es fehlt gleichwohl an einer abgestimmten Investitionspolitik innerhalb der Ressorts wie auch übergreifend; insgesamt fehlt es an einem eGovernment-Gesamtkonzept.

Weitgehende Übereinstimmung im Hinblick auf die Registrierungsstellen – Auf Landesebene werden vermutlich die Personalstellen die Tätigkeit als Registrierungsstelle in Zukunft übernehmen. Auf Kommunalebene wurden ebenfalls häufig die Personalstellen, aber auch die Meldeämter als Adressaten für die neue Aufgabe benannt.

Unklarheit über die CA – Es gibt in allen Ländern Überlegungen zur Schaffung von „Certification Authorities" (CA). Teilweise liegt bereits auch schon fest, welche Länder eine CA einrichten wollen und welche Länder nicht. Der Großteil der Länder hat sich jedoch im Hinblick auf die zukünftige Strategie noch nicht festgelegt. Vereinzelt existieren in unterschiedlichen Landesverwaltungen und -behörden mehrere Trustcenter (so etwa Nordrhein-Westfalen) .

Länderübergreifende Kooperation – Kooperation auf Landesebene findet institutionalisiert primär im Rahmen des Kooperationsausschusses ADV Bund/Länder/Kommunaler Bereich (KoopA ADV) statt.[15]

Für die unterschiedlichen Thematiken wurden einzelne Arbeitsgruppen eingerichtet. Hierzu zählen die IT-gestützte Vorgangsbearbeitung, die IT-gestützte Schriftgutverwaltung sowie die Arbeitsgruppe IT-Sicherheit. Im Rahmen seiner Arbeit hat der KoopA ADV zahlreiche Empfehlungen und Beschlüsse erarbeitet[16], die zu verschiedenen Maßnahmen geführt haben.[17] Durch die MEDIA@Komm-Initiative des BMWi und auch durch den Zusammenschluss von Computernetzwerken auf europäischer, Bundes-, Landes- und kommunaler Ebene hat die Bedeutung der Koordinierung durch den KoopA ADV zugenommen. So hat zum Beispiel der Arbeitskreis „Querschnittsfragen Technik" der BLK-Arbeitsgruppe „Elektronischer Rechtsverkehr" Empfehlungen erarbeitet, die auch elektronische Signaturen betreffen.

Nachfolgend sollen exemplarisch zwei Bereiche herausgegriffen werden, in denen eine vermehrte Anzahl von eSig-relevanten Aktivitäten identifiziert werden konnte:

- die Justiz (spezifische Bereiche)

---

[15] Der KoopA ADV wurde im Februar 1970 gegründet und stellt die wesentliche IT-Koordinierungsstelle in Deutschland dar. Seine Mitglieder setzen sich aus Vertretern der Bundesländer, Datenzentralen, kommunalen Spitzenverbänden sowie der KGSt zusammen. Die Arbeitsschwerpunkte liegen gegenwärtig auf folgenden Themen: IT-Infrastruktur (Verwaltungsnetz TESTA), Vorgangsbearbeitung (Pilot in der Gemeinde Wellenhorst), Registratur- und Archivierungskonzepte, Schnittstellenbearbeitung (Mail/DMS/Vorgangsbearbeitung).
Relevant für den Untersuchungskontext sind u. a. die zugeordnete AG „Kommunikation und Sicherheit", die ihre Geschäftsstelle beim BMI hat, sowie die von der KoopA ADV unabhängige BLK für Datenverarbeitung und Rationalisierung in der Justiz, in der die IT-Referenten der Landesregierungen (aus den MJs) sitzen (Schwerpunkt Justiz); Thema u. a. elektronischer Rechtsverkehr, Federführung zurzeit: MJ Niedersachsen.

[16] Beschlüsse: (a) Einsatz MailTrusT-konformer Produkte; (b) Der Bund soll auf die Berücksichtigung von S/Mime und SSL bei der Weiterentwicklung von MailTrusT achten (Öffnung SPHINX), (c) Anschluss von Bundesverwaltungen an TESTA-Netz; (4) Aufbau eines OSCI-Standards in Kongruenz mit dem HBCI-Standard der Kreditwirtschaft; (5) Leitungsverschlüsselung im TESTA-Netz soll zunächst zurückgestellt werden; (6) Der Aufbau neuer eigenständiger Fachnetze soll vermieden werden.

[17] So etwa die Aufnahme des Zentralregisters des Kraftfahrtbundesamtes und der Bundesverwaltung für Verkehr in das TESTA-Netz.

- der Universitätsbereich

Nachfolgend wird näher auf diese Bereiche eingegangen.

4.3.2 eSig in der Justizreform

Der Justizbereich steht seit einigen Jahren unter einem besonderen Reformdruck aufgrund struktureller und externer Faktoren (steigender Eingang von Rechtsgesuchen, Arbeitsüberlastung, Prozessdauer, Kosten etc.).

Gekennzeichnet durch eine ausgesprochene

- Heterogenität des Niveaus moderner IuK-Technologie

und durch die

- transparenzerzeugende Wirkung von eGovernment einem besonderen Kulturwandel ausgesetzt,

wird der Abstand zwischen einigen Vorreitern im Justizbereich und zurückhaltenderen Akteuren sehr deutlich.

Große Öffentlichkeitswirkung hat beispielsweise die Bundesnotarkammer erzielt, deren Trustcenter als dritte Einrichtung nach Post und Telekom akkreditiert wurde. Gleichwohl ist hier zukunftsweisendes Engagement vermischt mit dem Ziel einer langfristigen berufsständischen Existenzsicherung, denn die notariellen „Gebietsmonopole“ sind durch die eSig in Frage gestellt.

Sowohl in den Feldern Grundbuch, Handelsregister als auch Mahnverfahren existieren laufende Projekte oder befinden sich in der Konzeptionsphase.

Elektronische Grundbuchämter

In zahlreichen Grundbuchämtern in bundesweit 13 Ländern existieren z.T. Kooperationsprojekte (Bayern, Berlin, Hamburg, Sachsen und Sachsen-Anhalt), in denen das elektronische Grundbuch genutzt wird. Die bisher papiergeführten Grundbücher werden digitalisiert, so dass Änderungen via PC ausgeführt werden können. Die Bediensteten der Amtsgerichte sind ausschließlich dazu autorisiert, Änderungen vorzunehmen, indem sie sich digital mit einer Chipkarte ausweisen. Nutzer sind zurzeit Notare, Banken und Versicherungen sowie berechtigte Privatpersonen, denen ein schnellerer und unkomplizierterer Datenzugriff ermöglicht wird.

Die nächsten Schritte werden in diesen Projekten 1) die vollständige digitale Erfassung der alten, papiergeführten Grundbücher sowie 2) die Ermöglichung von Eintragungen mittels der elektronischen Signatur auch für externe Nutzer sein. Die bisherigen Zugriffsmöglichkeiten sind nur durch eine vorherige Zulassung möglich, wo zur Einsicht der Grundbücher keine elektronische Signatur genutzt wird. In Baden-Württemberg ist die Fernabfrage der Daten über Fernleitung noch nicht möglich. Mittelfristig soll in diesem Projekt das elektronische Grundbuch mit Smartcards und elektronischer Signatur den ca. 2.000 Zeichnungsberechtigten in allen Grundbuchämtern des Landes Baden-Württemberg zur Verfügung gestellt werden.

Aus Sicht von KPMG lassen sich als Gründe für die Aktivitäten im Justizbereich anführen:

- Justizverwaltung und Justiz insgesamt stehen unter Reformdruck.
- Es besteht hohes Interesse an der Sicherheit beim Datentransfer sensibler Inhalte.

- Die Anwendungen umfassen in der Regel geschlossene und professionelle Benutzergruppen (technologische Infrastruktur vorhanden; Investitionsbereitschaft; hoher Organisationsgrad, der Vereinbarungen fördert).
- eSig-Anwendungen im Justizbereich werden durch Investitionen in elektronische und standardisierte Verfahren in der Vergangenheit begünstigt (z. B. Mahnverfahren).
- Der Einsatz ist ökonomisch gerechtfertigt (hoher „Traffic“ aufgrund weitgehend standardisierbarer Massenanwendungen).
- Die Mitarbeiter sind an die bestehenden elektronischen Verfahren gewöhnt; d. h. sie müssen sich nur an die elektronische Signatur anpassen, nicht aber an ein komplett neues technisches System.

Gleichwohl ist der Einsatz der elektronischen Signatur auch im juristischen Bereich nicht durchgängig. Die Problematik liegt zum einen darin, die elektronische Signatur im Nachhinein auf ein bereits vorhandenes System anzupassen – ein Schnittstellenproblem im gesamten eGovernment-Bereich –, zum anderen bestehen erhebliche Probleme aufgrund der ADV-Komplexität bei der ordentlichen Gerichtsbarkeit, die zugleich auch aufgrund dessen zurzeit andere Prioritäten hat.

4.3.3 eSig in der Universitätsreform

Die deutschen Universitäten und Fachhochschulen sehen sich einem zunehmenden externen und internen Handlungsdruck ausgesetzt. Sie müssen ihre Stellung im internationalen Wettbewerb behaupten, ihre zunehmende Budgetverantwortung sinnvoll nutzen sowie steigende Serviceerwartungen ihrer „Klientel“, d. h. Studierende, Dozenten und Professoren, erfüllen.

Fortschritte in der Technologie wie z. B. asynchrones Lernen/eLearning ermöglichen eine Veränderung der klassischen Universität hin zu einer „virtuelleren“ Universität. Chiptechnologie und Internet eröffnen den Universitäten neue Handlungsmöglichkeiten in folgenden Bereichen:

- Abbuchung Semestergebühren, Immatrikulation, Rückmeldung
- Ausweisfunktion
- ÖPNV-Benutzung, Bibliotheksnutzung
- Gebäudezutrittskontrolle
- Bezahlung Mahngebühren
- Mensakarte
- Parkraumbewirtschaftung

Das Präsidium der Hochschulrektorenkonferenz (HRK) hat vor diesem Hintergrund am 8.11.99 eine Arbeitsgruppe eingesetzt, die sich mit den Einsatzmöglichkeiten von Chipkarten befasst hat. Dabei werden von der Arbeitsgruppe folgende Vorteile benannt:[18]

- Medienbrüche fallen weg
- Gleichmäßiger Arbeitsablauf (z. B. Wegfall von Stoßzeiten)
- Online-Aktualisierung Personaldaten (24h)

[18] Empfehlungen des 191. Plenums vom 3./4. Juli 2000.

- Prozesskosteneinsparungen durch Selbstbedienungsterminals (z. B. für Rückmeldungen, Adressänderungen etc.)
- Bessere Kontrolle Zahlungsverlauf

Diesen Vorteilen stehen nach Auffassung der Arbeitsgruppe i.d.R. nur kleinere, überwindbare Probleme entgegen:

- Archivierung
- Authentifizierung
- Kontogebundene Kreditkarten schöpfen Teil Einnahmen ab
- Pfandrückbuchungen, fehlende Stornomöglichkeiten

Die Einbindung elektronischer Signaturen auf den Karten ist denkbar. Wenn allerdings mehr als ein nur lokaler Einsatz mit einer visuellen Identifikation (i. d. R. Lichtbild) angestrebt wird, muss auf EC-Karten verzichtet werden, da sich auf ihnen eine visuelle Identifikation gegenwärtig nicht darstellen lässt. Tatsächlich werden daher zahlreiche Anwendungen von Chipkarten erarbeitet; dabei jedoch durchgängig keine (qualifizierte) eSig angewendet.

Im Einzelnen stellt sich die Lage derzeit wie folgt dar:

Insgesamt 20 Universitäten und Fachhochschulen sind in der Realisierung von Chipkarten-Projekten engagiert. Die Universitäten arbeiten an eigenen „Insellösungen“ und bieten Dienste, wie z. B. Adressänderungen, Semesterrückmeldungen, Bescheinigungsausdruck und Prüfungsanmeldungen über Selbstbedienungsterminals in den Universitäten an. Da in diversen Universitäten die Prüfungsordnung derzeit auf das sog. Credit-Point-System umgestellt wird und in diesem Zuge verstärkt verbindliche Prüfungsanmeldungen erforderlich sind, ist die rechtsverbindliche Online-Anmeldung zu Prüfungen von besonderer Relevanz. Die Nutzungsmöglichkeiten der elektronischen Signatur ist hier sowohl in Kommunikationsbeziehungen zwischen Studierende und der Universitätsverwaltung sowie vor allem auch in verwaltungsinternen Arbeitsabläufen z. B. zwischen Professoren und Prüfungsämtern zu sehen.

Der herkömmliche Studentenausweis ist jedoch bisher nicht überall durch eine Chipkarte ersetzt worden. In der Praxis spielt der Einsatz der gesetzeskonformen elektronischen Signatur derzeit keine Rolle, da zuerst Verwaltungsabläufe identifiziert und die Finanzierung der breitflächigen Distribution der Chipkarten geklärt werden müssen. Hierbei ist zu berücksichtigen, dass Universitäten aufgrund der Autonomie in Selbstverwaltungsangelegenheiten selbst definieren können, welches Sicherheitsniveau den Kommunikationsbeziehungen mit Studierende zu Grunde liegen soll.

Für die vergleichsweise Dynamik lassen sich plausible Aspekte heranziehen. Gründe dafür, dass Universitäten besonders aktiv im Bereich Chipkarte aktiv sind, dürften sein:

- Die Schwelle zur Intra-/Internetnutzung ist bei den Universitätsmitgliedern gering, da Know-how, Technik und eine gewisse Affinität vorhanden sind.
- Die Anwendungsbereiche stellen ein ggf. zu standardisierendes Massengeschäft dar.

Neben der internen Ausrichtung bestehen eine Reihe von Projekten mit konzeptionell-experimentellem Charakter. Hierzu zählen zum Beispiel Forschungsprojekte in Zusammenhang mit eVoting (u. a. LSA, Brandenburg, Osnabrück), an denen Universitäten maßgeblich oder zu großen Teilen beteiligt sind.

4.4 Vorhaben der Kommunen

4.4.1 Überblick

Die Aktivitäten der Kommunen im eGovernment haben sich in den vergangenen zwei Jahren deutlich erhöht. Zu den Aktivitäten zählen:

- Schaffung einer grundsätzlichen Infrastruktur (PCs, Vernetzung, eMail)
- Technische Entwicklung und Integration von Fachanwendungen
- Entwicklung „virtueller Rathäuser“

In jüngster Zeit sind zahlreiche Umfragen zum Thema eGovernment bei den Kommunen durchgeführt worden[19]. Sie belegen ein erheblich gestiegenes Interesse an der Entwicklung von eGovernment-Lösungen und zeugen von bedeutenden Fortschritten im Bereich der Internetpräsenz.

Die meisten Studien konzentrieren sich dabei jedoch auf die größeren Kommunen (> 50.000 Einwohner). Von den insgesamt 14.197 Kommunen in Deutschland machen sie nur einen kleinen Teil aus. Die Situation in den kleineren Kommunen, die mit einer dünnen Personaldecke und drängenden Finanzproblemen noch weit von virtuellen Rathäusern entfernt sind, stellen sich viel grundsätzlicher dar; insbesondere in den ostdeutschen Kommunen (unzureichende Vernetzung, kein/zu wenig IT-Personal, geringe Größe)[20].

Aus einer aktuellen Studie des Deutschen Instituts für Urbanistik geht hervor, dass die Kommunen insbesondere im Bereich der Bürgerinformation, bei Kultur und Tourismus sowie Bildungsangeboten Online-Initiativen gestartet bzw. bereits umgesetzt haben (vgl. nachfolgende Abbildung).[21] Angebote zur Online-Abwicklung von Verwaltungsprozessen innerhalb und außerhalb der Administration befinden sich in einem weniger entwickelten Stadium. Betrachtet man die Situation vor dem Hintergrund der Verwaltungsmodernisierung, so zeigt sich hier wie auch in anderen Studien, dass offenbar mit der Einführung von eGovernment die Außenperspektive im Vordergrund steht; weniger die Binnenziele der Verwaltungsmodernisierung.

Trotz der kritischen Haushaltslage in vielen Kommunen, und obgleich der Mangel an Finanzmitteln als Hemmnis für die Umsetzung von Online-Aktivitäten hervorgehoben wird, besitzen Einsparziele beim Thema eGovernment eine eher untergeordnete Priorität.

[19] Vgl. von Bertelsmann, PwC, als auch KPMG, Universität Leipzig, Difu, a.a.O.
[20] Vgl. auch TU Chemnitz, Umfrage Internetznutzung der Kommunen in Sachsen, unveröffentlichte Ergebnisse, 22.1.2001.
[21] Ähnliche Ergebnisse: vgl. Bertelsmann, a.a.O.

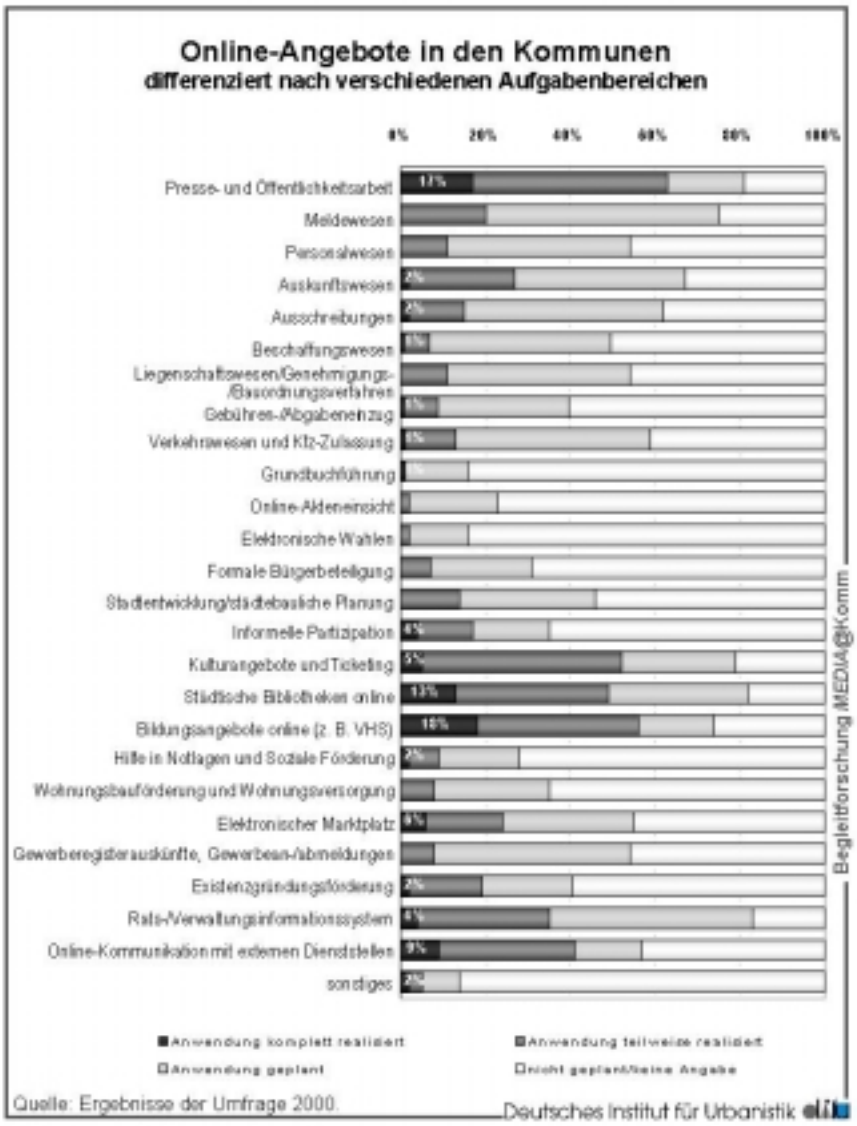


Abbildung 4-4: Online-Angebote in den Kommunen

In den einschlägigen Studien über Kommunen und Internet werden folgende Hemmnisse bei der Einführung von eGovernment-Lösungen genannt:

- Unzureichendes Know-how der Verwaltung (vor allem bei den Entscheidern)
- Komplexe technische Infrastruktur, fehlende Standards/Kompatibilitäten
- Hohe Einführungskosten bei angespannter Haushaltslage
- Aktivitäten nicht als Chefsache „aufgehängt“
- Fehlen von qualifiziertem Fachpersonal, Weiterbildung meist in Eigeninitiative

Diese grundsätzlichen Probleme führen zu einer Verunsicherung im Umgang mit dem neuen Thema und resultieren in einer inkrementalistischen und pilotorientierten Vorgehensweise.

Diese generelle Tendenz schlägt sich auch auf den Umgang mit der Fragestellung der elektronischen Signatur nieder. Nach der o.g. Studie des Difu bei allen Städten und Gemeinden mit mehr als 50.000 Einwohnern werden elektronische Signaturen bei 5% der Städte und Gemeinden bereits eingesetzt; 72% planen, die eSig im Rahmen ihrer eGovernment-Aktivitäten zu nutzen[22]. Daraus geht allerdings nicht hervor, welche Sicherheitsstufe der Signatur (fortgeschrittene, qualifizierte, akkreditierte eSig) zum Einsatz kommen soll.

Die folgende Tabelle gibt einen kurzen Überblick über einige Städte und kommunale Einrichtungen, von deren ersten Überlegungen oder Konzepten KPMG im Laufe des bisherigen Projektverlaufs Kenntnis erhalten hat.

Details zu den markierten Projekten finden sich in der Anlage.

	Identifizierte Projekte auf kommunaler Ebene
Stadt Dortmund	Vorbereitung eines Einsatzes elektronischer Signaturen
Stadt Bonn	Einbindungen eSig in virtuelles Rathaus, ggf. Übernahme Bremer Modell
Gemeinde Memmelsorf	Einsatz eSig im Rahmen des “virtuellen Rathauses“ geplant, wenn Rechtslage eindeutig
Stadt Köln	Studie Difu
Stadt Mannheim	Studie Difu
Stadt Karlsruhe	Studie Difu
Stadt Rathenow	eSig fest geplant im Rahmen „Realisierung elektronischer Melderegisterauskunft“ [A], ggf. auch im Rahmen des Projekts „elektronische Akteneinsicht“ [A],
„Virtuelles Rathaus“ Hagen	Pilotprojekt mit registrierten Benutzern [A]
Bremen	MEDIA@Komm [A]
Esslingen	MEDIA@Komm [A]
Nürnberg	MEDIA@Komm [A]
Kom-On! NRW	Städteverbund-Projekt verschiedener nordrhein-westfälischer Städte, unterschiedliche Diskussions- und Kooperationsforen zur Förderung kommunaler Online-Dienste beinhaltet (Themen u. a. Trust-Center, elektronische Signatur)
Moderne Verwaltung NRW	Planung der Initiative „DigSign NRW 2005“
Multimedia in Rheinland-Pfalz	Multimediawettbewerb

A= Projektprofile in Anlage

Tabelle 4-5: Aktivitäten in Kommunen

[22] Vgl. Deutsches Institut für Urbanistik (Hrsg.): Städte auf dem Weg zum virtuellen Rathaus, 15.3.2001.

Die umfangreichsten Aktivitäten im Bereich der rechtsgültigen eSig werden derzeit von den Gewinnerstädten des Wettbewerbs MEDIA@Komm durchgeführt, auf die hier kurz eingegangen werden soll.

4.4.2 MEDIA@Komm

MEDIA@Komm stellt auf kommunaler Ebene das finanziell größte Gesamtprojekt zum Thema elektronische Signaturen dar. Hervorgegangen aus einem Wettbewerb, ist MEDIA@Komm aufgrund der Begleitforschung das am besten dokumentierte Projekt. Es ist zugleich die größte Einzelfördermaßnahme des BMWi.

Ziel des „Leitprojekts“ MEDIA@Komm ist die breite Einführung von elektronischen Signaturen in ausgewählten Modellregion im Rahmen einer medienbruchfreien sowie rechtsverbindlichen multimedialen Vernetzung von Wirtschaft, Verwaltung und Bürgern. MEDIA@Komm ist Teil des Aktionsprogramms „Innovation und Arbeitsplätze in der Informationsgesellschaft des 21. Jahrhunderts“.

Ziel ist es,

- die Entwicklung und Anwendung von Multimedia in Städten und Gemeinden gezielt zu unterstützen sowie
- modellhafte Lösungen für „virtuelle Rathäuser“ und „virtuelle Marktplätze“ zu entwickeln.

Hierzu wurde 1998 ein Städtewettbewerb veranstaltet, an dem sich 136 Städte und Gemeinden mit ihren Konzepten beteiligt haben.[23] 1999 wurden durch eine Jury die drei Preisträger Bremen, Esslingen und der Städteverbund Nürnberg ermittelt. Die Konzepte dieser Städte werden derzeit und in den nächsten Jahren als Best-Practice-Beispiele umgesetzt, um breitenwirksam zur Nachahmung anzuregen und Investitionen in zukunftsfähige Arbeitsplätze auszulösen.

Hierbei kommt der interdisziplinären Begleitforschung die wichtige Rolle eines Wissenskatalysators zu[24]. Ihre Aufgabe ist es, das Projekt kritisch zu begleiten, es zu dokumentieren und neue Anregungen nach innen wie nach außen zu entwickeln.

Die folgende Tabelle vermittelt einen Überblick über die MEDIA@Komm-Städte Bremen und Esslingen sowie den Städteverbund Nürnberg:

[23] Für eine Liste der Städte siehe unter http://www.mediakomm.net/liste136.html

[24] Die Begleitforschung setzt sich aus Vertretern der folgenden Institutionen zusammen: Hans-Bredow-Institut für Medienforschung in Verbindung mit der Forschungsstelle Recht und Innovation der Universität Hamburg, Deutsches Institut für Urbanistik, Deutsches Institut für Normierung e.V., TÜV Informationstechnik GmbH.

Kommunen / Merkmale	Bremen	Nürnberg	Esslingen
Rahmen	Stadtstaat	Mehrere Städte im Verbund	Mehrere Antragsteller
Ziele/Ansatz	Plattform für G-B und G-C nach Lebenslagenkonzept	Plattform für G-B und G-C mit Multiplizierbarkeit auf Verbundstädte	Plattform für G-B und G-C mit intensiver Partizipation
Beginn	1.9.1999	1.10.1999	28.1.2000
Fördervolumen in Mio DM	42	46,5	32,7
Förderquote BMWi in %	39	36	50
Projektträger	BOS GmbH & Co KG als Dienstleister Externe DL	CuriavantGmbH mit 30 MA, viel Eigenproduktion	Trägerverein viel Eigenproduktion
Status eSig-Nutzung (Januar 2001)	Urkundenbestellung inkl. Zahlungsfunktion realisiert (500 Karten), OSCI-Standard	Anwohnerparkausweis inkl. Zahlungsfunktion realisiert (50 Karten)	50 Karten für das Jugendnetz Esslingen Integration Sig+Zahlungsfunktion geplant

Tabelle 4-6: Überblick MEDIA@Komm-Preisträgerprojekte

Das Bundesministerium für Wirtschaft und Technologie fördert das Projekt MEDIA@Komm mit rd. DM 50 Mio. De facto erhält das Projekt ein Fördervolumen in Höhe von rd. DM 120 Mio. MEDIA@Komm ist damit weltweit vermutlich das größte Förderprojekt zum Thema elektronische Signatur auf kommunaler Ebene. Zu den Preisträgerkommunen im Einzelnen:

Bremen

Bremens Ansatz fußt auf einer Online-Plattform auf Basis des Lebenslagenkonzepts. Innerhalb von drei Jahren sollen rechtsverbindliche Transaktionen zwischen Verwaltung, Wirtschaft und Bürgern realisiert werden. Es handelt sich also um einen Ansatz, der die Elemente von G-G, G-B und G-C gleichzeitig aufgreifen will. Zugleich ist mit der Umsetzung des Konzepts eine grundlegende Reform der Verwaltung verbunden.

Der Ansatz basiert auf sogenannten Lebenslagenbündeln, die sich auf unterschiedliche Adressaten ausrichten:

	Lebenslagenbündel
Bürger	■ Umzug und Wohnen ■ Studium ■ Heirat ■ Online buchen und reservieren
Mittler	■ Bau eines Hauses ■ Kauf eines Autos ■ Schriftverkehr zwischen Rechtsanwälten/Notaren und Gerichten
Unternehmen	■ Öffentliche Auftragsvergabe
Alle	■ Elektronischer Zahlungsverkehr mit der Verwaltung ■ Steuern bzw. Kommunikation Steuerberater-Finanzamt

Tabelle 4-7: Elemente des Lebenslagenkonzepts

Die Lebenslagenbündel umfassen 66 Geschäftsvorfälle mit insgesamt 26 Dienstleistern. In Teilprojekten und ausgewählten Geschäftsprozessen wurde aufbauend auf dem HBCI-Standard der Kreditwirtschaft ein OSCI-Standard entwickelt, der es ermöglicht, Signaturen und Zahlungsfunktion zu koppeln. Dies beinhaltet den Aufbau einer Online-Infrastruktur (u. a. Endgeräte, Benutzerschnittstellen, Chipkarten, Bezahlverfahren, Registrierungsstellen).

Die Aktivitäten wurden in eine eigene Gesellschaft ausgegliedert. Entwicklungs- und Betreibergesellschaft ist die bremen online services GmbH & Co. KG (bos), die von privaten und öffentlichen Gesellschaftern getragen wird (vgl. Tabelle 4-8). Geschäftszweck ist die Entwicklung, der Betrieb und die Vermarktung von sicheren, rechtsverbindlichen und vertrauenswürdigen Infrastrukturen über offene Netze auf der Basis der digitalen Signatur und der Geldkarte der deutschen Kreditwirtschaft.

Die ursprüngliche Planung sah vor, dass im Jahr 2002 ein Break Even-Punkt erreicht werden würde.

	Anteile an bos in %	**Ziele/Erwartungshaltung**
Freie Hansestadt Bremen	50,1	■ Verknüpfung mit bisheriger IuK-Förderung ■ Verknüpfung mit Verwaltungsmodernisierung ■ Verbesserung Standort
Deutsche Telekom	15,0	■ Vermarktung TC, Multimedia, eCommerce, eBusiness
Sparkasse Bremen	10,0	■ Neue Anwendungen für Geldkarte ■ Höhere Kundenbindung ■ Gewinnung neuer Kunden
Brokat **Signum** **VSS** **mcb** **Bremer Straßenbahn** **BREKOM**	5,0 5,0 5,0 4,9 2,5 2,5	■ Erschließung zusätzlicher Geschäftsfelder im Bereich Verwaltungsdienstleistungen

Tabelle 4-8: Gesellschafter der MEDIA@Komm Bremen

Die Entwicklung wurde seitens der Freien und Hansestadt Bremen flankiert durch das Experimentiergesetz von 1999, das allerdings nicht angewendet werden brauchte, weil keine Rechtsverordnung auf seiner Grundlage erlassen wurde. Im Prinzip haben die übrigen Gesetzesanpassungen auf Bundesebene das Experimentiergesetz überholt.

Sachstand und Erfahrungen

Im Herbst 2000 wurden 15 Geschäftsvorfälle der Verwaltung und von Privaten eingerichtet. Am 5. September 2000 konnten die ersten Geschäftsvorfälle aus der Lebenslage „Umzug und Wohnen“ Online digital signiert und bezahlt werden. Gleiches gilt für die Bestellung und Bezahlung von Personenstandsurkunden. Zuvor wurde eine Geschäftsprozessanalyse durchgeführt, der im Vorwege einer DV-Unterstützung den Reorganisationsbedarf bei den Abläufen verdeutlichte. Um die Signatur- mit der Bezahlungsfunktion zu verknüpfen, hat bos einen neuen technischen Standard entwickelt, den *OSCI-Standard* (vgl. Abschnitt Technische Rahmenbedingungen).

Seit Dezember können Urkunden beim Standesamt sowie Busfahrkarten mittels eSig elektronisch bestellt und bezahlt werden. Der Prozess wird maßgeblich verkürzt und bürgerfreundlicher.

Klassischer Prozess Standesamt	**Optimierter Prozess Standesamt**	**Nutzen**
Persönliches Erscheinen	■ Urkundenbestellung Online ■ Gleichzeitige Zahlung per Geldkarte	■ Kunde muss keinen Brief schreiben oder persönlich erscheinen (bekommt Urkunde zugeschickt)
Ausweisen mittels Personalausweis	■ Schicken der Urkunde	■ Rechnung schreiben entfällt
Bezahlung der Gebühr an Kasse		■ Keine Mahnungen da Online-Zahlung (automatisierte Kontrolle) ■ Entlastung Verwaltungsarbeit
Erhalt Urkunde	Erhalt Urkunde	

Tabelle 4-9: Prozessbeispiel Standesamt

Angesichts der bisher eher geringen Nutzerzahlen führt die Bereitstellung von Online-Dienstleistungen in den o.g. Einzelfällen nicht unmittelbar zu Einsparungen. Im Gegenteil, es sind gerade in der Anfangsphase erhebliche Investitionen und ein erhöhter Betreuungsaufwand erforderlich.

Im Vergleich zur ursprünglichen Planung besteht in dem Projekt ein Zeitverzug von 9 Monaten. Dieser ist auf unerwartete bzw. unterschätzte

- formale Anforderungen, insbesondere Neufassung des Wettbewerbsantrages, Kürzung der Fördersumme des Bundes um rd. 3,5 Mio. DM, was u.a. eine Reduktion von Signaturkarten (10.400 statt 30.400) und Kiosken (5 statt 10) sowie die Streichung des bos-Infoladens (Internet-Café mit Betreuung),
- technische Schwierigkeiten (u. a. Komplexität Online-Plattform, Übertragbarkeit HBCI auf OSCI) sowie
- organisatorische Probleme (u. a. Personalgewinnung, späte Chipkarten-Auslieferung)

zurückzuführen. Der Zeitverzug könnte unter Umständen das Erreichen der geplanten wirtschaftlich tragfähigen Basis im Jahr 2002 gefährden bzw. einen erhöhten Verbrauch der zur Verfügung stehenden finanziellen Mittel auslösen, der zu einer Revision der Planungen führt. Außerdem kann sich die Gewinnung von Teilnehmern verzögern; ggf. Kooperationspartner zum Aussteigen bewegen.

Eine zentrale Erkenntnis aus dem Bremer Projekt ist, dass

- der Entwicklungsaufwand für eine Bereitstellung der geplanten kommunalen Prozesse weit über den Förderungszeitraum von 3 Jahren hinausgehen wird und
- eine Amortisation der eingesetzten Finanzmittel sich nur langfristig und über eine Multiplikation der entwickelten Lösungen auf andere Kommunen erzielen lässt.

Vor diesem Hintergrund bietet bos anderen Kommunen eine Unterstützung bei dem Aufbau eigener Plattformen und hat eine „OSCI-Leitstelle“ eingerichtet, in der Standards für die Abwicklung von Geschäftsprozessen der öffentlichen Verwaltung vermarktet werden sollen. Ziel ist

es, bos zum Application Service Provider (ASP) zu machen, der seine Leistungen bundesweit anbietet. Die Dienstleistungen können vom Hosting mit transaktionsbezogener Vergütung über Partnerschaften (Co-Piloten) bis hin zur Vergabe von Lizenzen gehen.

Es ist allerdings noch offen, wie ein Betrieb der Plattform wirtschaftlich entwickelt werden kann. Dies betrifft u. a. die Struktur von Tarifen für einzelne Dienstleistungen und deren Umlage auf Nutzer und Dienstleister. Es bestehen keine sicheren Informationen, was Kunden für derartige Transaktionen bezahlen würden. B-B-Betreiber von Marktplätzen kalkulieren im Rahmen ihrer Geschäftsmodelle mit einer durchschnittlichen Gebühr von 3,5% je Transaktion[25], die allerdings derzeit noch kaum jemand zahlt („Im Internet ist alles gratis“).

Grundsätzlich zu klären ist hierbei, inwieweit Kommunen rechtlich überhaupt kommerziell engagiert sein dürfen (virtuelle Marktplätze, Verkauf von Know-how etc.). Es könnte u. U. wettbewerbsrechtlich problematisch werden, wenn Kommunen eine Refinanzierung ihrer Aktivitäten über die Vermarktung von Lösungen anstreben, die grundsätzlich auch auf dem Markt angeboten werden. Im Rahmen ihrer Expansionsstrategie wäre die bos Wettbewerber von Datenzentralen, Systemhäusern etc.

Städteverbund Nürnberg

Im Mittelpunkt des Projekts des Städteverbundes Nürnberg-Fürth-Erlangen-Schabach-Bayreuth steht der Aufbau einer regionalen Kommunikationsplattform auf Basis der elektronischen Signatur. Das Projekt basiert außerdem auf dem Gedanken, dass die Signaturkarte einen hohen Zusatznutzen bieten muss. So werden zahlreiche G2B und G2C-Lösungen angestrebt.

Die Verbundpartner halten zusammen die Curiavant Internet GmbH, deren Ziel es ist, ein integratives Konzept für multimediale Dienste in Kommunalverwaltungen und privaten Unternehmen zu entwickeln, das den Anforderungen des SigG gerecht wird. Lösungen sollen später vermarktet werden.

	Anteile an Curiavant Internet GmbH in %	**Ziele/Erwartungshaltung**
Städeverbund Nürnberg-Fürth-Erlangen-Schabach-Bayreuth	100	■ Verknüpfung mit Verwaltungsmodernisierung ■ Verbesserung Standort ■ Arbeitsplätze im High-tech-Bereich

Tabelle 4-10: Gesellschafter MEDIA@Komm-Projekt Nürnberg

Die Planung sieht zunächst die Ausgabe getrennter Karten für die Funktionen elektronische Signatur und Geldkarte vor, die jeweils lokale Fenster für Zusatzfunktionen beinhalten, so dass eine Multifunktionalität gewährleistet ist. Derzeit sind zwar die Funktionen getrennt, aber auf zwei Seiten einer Chipkarte appliziert. Sie sollen durch EC-Karten ersetzt werden, sobald hierfür die Voraussetzungen erfüllt sind.

[25] Vgl. Handelsblatt, 16.01.2001 und KPMG: Business-to-Business-Marktplätze im Internet – Einstellungen und Perspektiven von Marktplatzakteuren, 9/2000.

Sachstand und Erfahrungen

Im Herbst 2000 konnte eine erste Anwendung in Betrieb gehen: Der Anwohnerparkausweis wurde als Pilot gewählt, da zum einen 1000 neue Ausweise ausgestellt werden mussten, zum anderen sich hier aufgrund der Komplexität und Integration in die Prozesskette ein geeignetes Pilotierungsfeld bot. Insgesamt werden 7 Ämter in den Prozess integriert, so dass eine organisatorisch und technisch anspruchsvolle Anwendung entsteht. Einen Überblick über den geplanten Projektverlauf bietet die nachfolgende Abbildung:

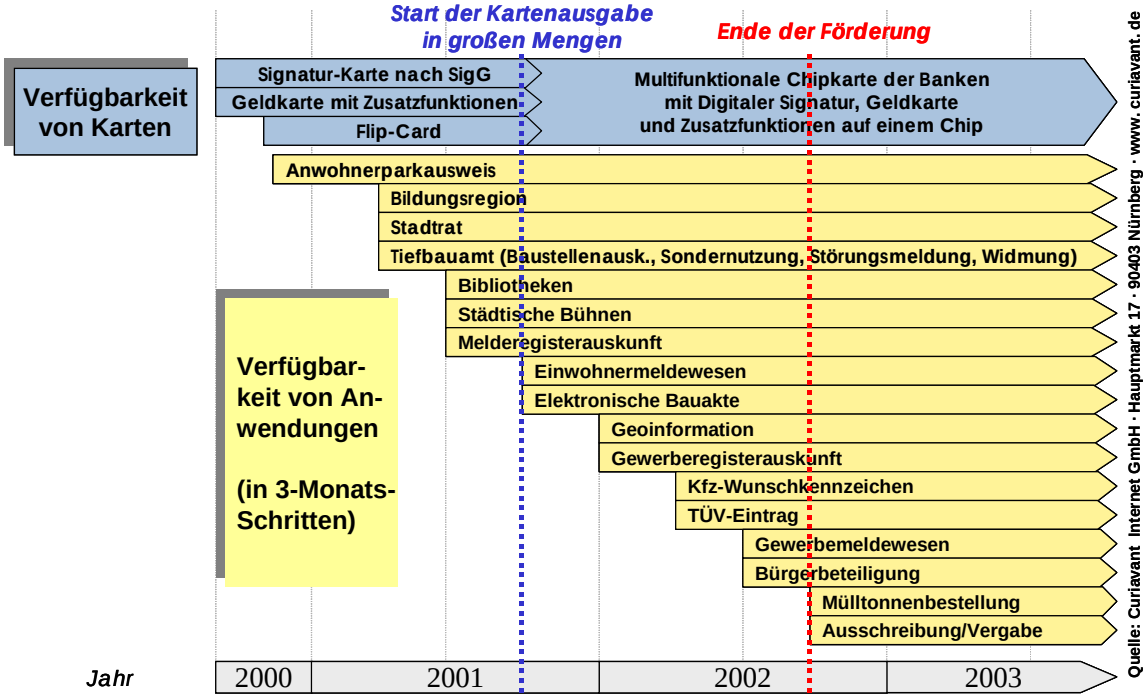


Abbildung 4-5: Projektplanung Nürnberg, Stand Herbst 2000

Die in Nürnberg verwendeten Signaturkarten sind nicht mit denen in Bremen kompatibel, was prinzipiell dem wettbewerblichen Ansatz der Projekte entspricht. Für die Nutzer dürfte dies jedoch nicht befriedigend sein (beim Umzug von Bremen nach Nürnberg kann die Chipkarte nicht weiter verwendet werden). Es wird jedoch daran gearbeitet, die Interoperabilität herzustellen.

Gegenwärtig liegt das Projekt rund ¼ Jahr hinter dem Zeitplan zurück. Neben wettbewerbsrechtlichen Gründen und einem hohen Koordinierungsaufwand innerhalb des Städteverbundes gab es eine Reihe operativer Probleme, wie z. B. aufwendige Verfahren zur Verteilung der Signaturkarten (3 Gänge zur Post).

Esslingen und Ostfildern

Seit dem offiziellen Projektstart am 28. Januar 2000 entwickelt die Stadt Esslingen zusammen mit der Stadt Ostfildern eine Verwaltung, die sich zum Ziel gesetzt hat, die Kundinnen und Kunden in sämtlichen Lebenslagen zu unterstützen. Den Bürgern sollen benutzerfreundliche Angebote bereitgestellt und dabei Wissen vermittelt werden. Erhofft wird so eine Erhöhung der Akzeptanz von Multimedia bei Bürgern und Wirtschaft. Ausdrückliches Ziel ist die Steigerung der Bürgerbeteiligung.

Beide Städte nutzen Public-Private-Partnerships, in dem sie ihre eigenen Angebote mit denen privater Anbieter aus den Bereichen Bildung, Kultur, Soziales und vor allem Wirtschaft verknüpfen. Durch die Einrichtung eines elektronischen „RegioMarktplatzes Esslingen“ sollen außerdem die Wirtschaftförderung und das Standortmarketing der Region verbessert werden. Für das „Sichere Kommunale Unternehmen im Internet“, kurz SKOUT genannt, wird aktiv in einem Netz von kommunalen Marktplätzen für Stadt, Standort und Region geworben.

Im Unterschied zu Bremen und Nürnberg werden im Projekt der Stadt Esslingen Vermarktungs- und Verwertungsinteressen als nachrangig betrachtet. Alle geplanten Einzel- und Teilprojekte sollen vielmehr gleichwertig auf den Weg gebracht werden. Im weiteren Verlauf des Vorhabens soll sich dann erweisen, was wirtschaftlich tragfähig ist und über den Förderzeitraum hinaus weiter bestehen kann. Die Evaluation und Entscheidungsfindung in Fragen eines späteren Betreibermodells sowie hinsichtlich Kommerzialisierungsstrategien erfolgen erst ab Mitte 2001. Da das Projekt keine vorrangig wirtschaftliche Ausrichtung hat, wird es als eingetragener gemeinnütziger Verein durchgeführt. Beteiligte Partner sind die Stadtverwaltung Esslingen, Stadtverwaltung Ostfildern sowie Institute, Verbände und Firmen.

Das gesamte Projekt der Stadt Esslingen setzt sich aus insgesamt sechs Teilprojekten zusammen: „Kommunale Dienste“, „Electronic Business/ Electronic Commerce“, „Soziales“, „Kultur“, „Bildung“ und „Querschnittsaufgaben“.

Sachstand und Erfahrungen

Erste Kenntnisse werden zur Zeit mit folgenden Pilotprojekten des Teilprojektes Bildung gesammelt:

Im Jugendnetz können interessierte Jugendliche beim Stadtjugendring Online mittels der elektronischen Signatur von Kochgeschirr, über einen Kleinbus bis hin zum Ferienhaus in der Toskana buchen. Mit nur wenigen, ausgesuchten Anwendern wird die Nutzung der elektronischen Signatur getestet. Im ersten Schritt werden die an dem Projekt beteiligten Einrichtungen mit Chipkartenlesegeräten sowie die haupt- und ehrenamtlichen Initiator des Jugendnetzes mit Chipkarten ausgestattet. In einem zweiten Schritt steht nochmals ein kleines Kontingent an Karten zur Verfügung, das an interessierte Jugendliche ausgegeben wird. Erste Erfahrungen werden in einem Zwischenbericht Anfang Februar 2001 ausgewertet.

Der Computer-Kreativ-Wettbewerb (C-K-W) richtet sich speziell an Kinder und Jugendliche bis 21 Jahre, die im Zuge dieses Wettbewerbs ihre Visionen zu ihrem zukünftigen Leben mit Computer, Internet und der elektronischen Signatur darstellen sollen. Die Konzeption des Jugendnetzes und des C-K-W beruht auf dem Hintergrund, Nutzungsmöglichkeiten für interaktive Anwendungen im sozialen Sektor zu erforschen, wobei die Jugendlichen als Multiplikatoren der neuen Medien dienen sollen.

Nachdem die Geschäftsprozessanalysen abgeschlossen sind, findet derzeit die Entwicklung der „Kommunalen Dienste“ statt, so dass für die erste Jahreshälfte 2001 Pilotanwendungen wie

Hundesteuer, Fundbüro und Anwohnerparkausweis unter Anwendung der elektronischen Signatur mit einer ausgesuchten Benutzergruppe mit ca. 300 Teilnehmern geplant sind. Etwa 50 kommunale Serviceleistungen sollen im Projektzeitraum bis Ende 2002 onlinefähig gemacht werden.

Da die bisher umgesetzten Teilprojekte in Esslingen ohne Wirtschaftlichkeitsanalysen durchgeführt wurden, erscheint es fraglich, inwieweit insbesondere das Jugendnetz über den Projektzeitraum hinaus finanziert werden wird.

Die Ausrichtung der realisierten Pilotprojekte spricht praktisch ausschließlich Jugendliche an. Für erwachsene Bürger werden in dieser Projektphase kaum Anreize geschaffen, sich mit der elektronischen Signatur auseinander zu setzen, geschweige denn, sie zu nutzen.

4.5 Aktivitäten im Unternehmenssektor

Aufgrund ihrer besonderen potenziellen Relevanz als Multiplikator oder Katalysator für die Verbreitung von eSig werden im folgenden Aktivitäten der Kreditinstitute sowie der berufsständischen Kammern skizziert.

4.5.1 Kreditinstitute

Kreditinstitute sind insbesondere aufgrund der hohen finanziellen Risiken seit langem sehr aktiv im Bereich der sicheren elektronischen Kommunikation. Dabei ist zu unterscheiden zwischen Privat- und Geschäftskunden.

Privatkunden: EC-Karte mit Signatur

In Bezug auf Privatkunden wurde mit dem 1998 vom deutschen Kreditgewerbe verabschiedeten Standard HBCI (vgl. Abschnitt 3.2) ein komfortables und sicheres Homebanking über offene Netze, insbesondere dem Internet ermöglicht. Das HBCI, das mittlerweile von fast allen Geldinstituten in Deutschland angeboten wird, benutzt als Sicherheitsfunktion eine elektronische Signatur, die allerdings nicht dem Standard einer qualifizierten Signatur nach EG-Richtlinie entspricht. Ende 1999 gab es bereits zehn Millionen onlinefähige Konten, das sind etwa 25 % aller Privatkonten.

Es liegt auf der Hand, dass ein derart verbreitetes Medium wie die EC-Karte (derzeit ca. 50 Millionen Kartenbesitzer in Deutschland) sich zur Aggregation von Funktionen ausgesprochen gut eignen würde, um die eSig zu transportieren.

Der Bundesverband der Banken hat im Herbst 2000 eine Presseerklärung abgegeben, in der in Aussicht gestellt wird, dass die neue EC-Kartengeneration ab 2001 signaturschlüsselfähig sein wird. Entsprechende technische Lösung existieren, d.h. auf der neuen EC-Kartengeneration gibt es Kapazitäten, um Signaturschlüssel zu erzeugen. Die Lösung soll nicht nur Bankgeschäfte, sondern auch das Signieren bankunabhängiger Transaktionen (z. B. Bürgerdienste) unterstützen. Bisher ist keine Integration mit den Geldkartenchips erfolgt, denn die vorhandenen Chips der Geldkarten sind Euro-fähig, aber nicht RSA-fähig. Eine RSA-fähige Geldkarte, mit der auch signiert werden kann, wird erst in 2-3 Jahren erwartet[26].

[26] Einschätzung des Sparkasseninformatikzentrums.

Die Kreditinstitute entscheiden derzeit über die nächste Generation von EC-Karten, bei der der Austauschzyklus von 2 auf 4 Jahre verlängert wird. Sollten sich zu diesem Zeitpunkt nur wenige Finanzinstitute entscheiden, eine Signierfunktion bereitzustellen, dann wird es weitere 4 Jahre dauern, bis die nächste Gelegenheit zur Integration der Signatur besteht. Dies könnte zu einer maßgeblichen Verzögerung der eSig-Diffusion führen.

Der Zentrale Kreditausschuss (ZKA), das Gremium, in dem die Finanzinstitute übergreifende Standards definieren (EC-Karten), hat Voraussetzungen geschaffen, um eine Signatur nach dem erarbeiteten Standard in den Mitgliedsinstitutionen umzusetzen. Die ZKA-Beschlüsse sind für alle Mitgliedsorganisationen bindend (wie der HBCI-Standard).

Zwei Großbanken sollen sich für eine eSig-Integration auf den EC-Karten entschieden haben. Das Sparkasseninformatikzentrum hat im Mai 2001 bekanntgegeben, dass es Signierfunktionen in seine EC-Karten integrieren will auf Basis einer Lösung der amerikanischen Firma Verisign, die zu den Pionieren im Bereich elektronischer Signaturen gehört.

Es gibt aus Sicht der Kreditinstitute mehrere Hinderungsgründe dafür, eine (qualifizierte) Signatur zur Verfügung zu stellen:

- ***Geringe wahrgenommene Relevanz der eSig für Kreditgeschäfte/Anwendungen fehlen*** - Aufgrund des Verbraucherschutzgesetzes können die Kreditinstitute praktisch keine zusätzlichen Prozesse online abwickeln, die nicht bereits derzeit mit Hilfe von HBCI angeboten werden. Damit wären keine weiteren Prozesskostenreduzierungen zu realisieren. HBCI bietet darüber hinaus ein hinreichendes Sicherheitsniveaus aus Sicht der Kreditinstitute.
- ***Investitionen und höhere Betriebskosten für Signaturkarten***. Die Integration der Signatur kostet etwa 15 DM pro EC-Karte zusätzlich. Darüber hinaus fallen Infrastrukturkosten, Kosten die Anpassung von SW-Verfahren sowie Kosten der Schulung der Mitarbeiter, der Umsetzung der für Registrierungsstellen erforderlichen Sicherheitskonzepte sowie der Aufwand für die laufende Nutzerbetreuung an.
- ***Fehlende Ausschließbarkeit der eSig-Nutzung*** von der Inanspruchnahme von Leistungen der Wettbewerber, wenn eine nicht proprietäre Chipkarte eingesetzt wird.
- ***Schwierige Durchsetzbarkeit von Tariferhöhungen.*** Das BVerfG hat jüngst eine Klage der Sparkassen zurückgewiesen, für die Nutzung des Lastschrifteinzugsverfahrens von EC-Karten Gebühren zu verlangen. Insofern stellt sich die Frage, inwieweit maßgebliche Gebührenerhöhungen für die Inanspruchnahme von Zusatzleistungen im Rahmen von Signaturanwendungen (z. B. Online Prüfung der Kreditwürdigkeit als Anreiz für Händler, Begrenzung des finanziellen Volumens von Online-Transaktionen als Sicherheit für Kunden) überhaupt durchsetzbar sind.
- ***Schlechte Erfahrungen mit der Geldkarte.*** Die „elektronische Geldbörse“ hat sich, trotz intensiver Bemühungen der Kreditinstitute, bisher nicht durchgesetzt. Höhere Produktionskosten der EC- Karten sowie Investitionen in Lesegeräte etc. haben sich nicht amortisiert, u.a. weil flächendeckende Anwendungen erst langsam zur Verfügung gestellt werden und der Nutzen der Geldkarte nicht ausreichend kommuniziert wurde.
- ***Hoher Organisationsaufwand durch Euroumstellung*** in 2002 betrifft insbesondere die Filialen. Diese oder zumindest ein Teil von ihnen müsste bei Einführung der eSig gleichzeitig als Registrierungsstellen eingerichtet werden (Sicherheitskonzept). Mitarbeiterschulungen, Nutzerbetreuung etc. müssten gewährleistet sein.

Hemmend wirkt sich für das Kreditgewerbe aus, dass im Verbraucherkreditgesetz der Online-Abschluss eines Verbraucherkredites untersagt wird.

Geschäftskunden: Europäisches Signaturmodell versus Globale Signaturstandards

Auf Seiten der Geschäftskunden ist weniger das europäische als das globale Geschäft relevant. Hier gibt es verschiedene Initiativen für eine sichere Kommunikation. Bisher ist unklar, welche sich durchsetzen wird.

Für sichere und verbindliche Geschäftsprozesse im Internet zwischen Unternehmen haben sich z. B. weltweit zahlreiche Banken im Projekt Identrus zusammengeschlossen[27]. Ziel von Identrus ist es, global agierenden Unternehmen über deren jeweilige Bank eine sichere Kommunikation z. B. bei Dokumentengeschäften zu ermöglichen, in dem eine bestimmte (strenge) Zertifikatepolitik vorgegeben wird. Konformität mit der europäischen Signaturrichtlinie wird angestrebt, aber derzeit nicht realisiert.

Deutsche Telekom und Deutsche Bank haben eine Initiative zur Informationssicherheit für die elektronische Kommunikation in und zwischen Unternehmen gegründet, bei der verschlüsselte und signierte Mails ausgetauscht werden sollen[28]. Diese sind mit in der Bundesverwaltung eingesetzten Lösungen für den Austausch sicherer eMail interoperabel.

Beide Unternehmen stellen ihre Corporate PKI jeweils unter ein Dach ("Bridge-CA für Corporate PKIs"). Während die Deutsche Telekom ihre Zertifikate aus dem TeleSec Trust Center bezieht, werden bei der Deutschen Bank die des Beteiligungsunternehmens TC Trust Center genutzt. Unternehmen können sich beteiligen und ihre vorhandenen Corporate Public Key Infrastrukturen weiter verwenden.

4.5.2 Industrie- und Handelskammern

Die Industrie- und Handelskammern (IHK) sind eigenverantwortliche öffentlich-rechtliche Körperschaften, die das Interesse ihrer zugehörigen Unternehmen gegenüber den Kommunen, Landesregierungen, regionalen staatlichen Stellen und durch den Deutschen Industrie- und Handelstag (DIHT) gegenüber der Bundesregierung und der Europäischen Kommission vertreten. Alle deutschen Unternehmen im Inland – ausgenommen Handwerksbetriebe, Freiberufler und landwirtschaftliche Betriebe – sind per Gesetz Mitglied einer IHK. Die Spitzenorganisation der 82 deutschen Industrie- und Handelskammern ist der DIHT

Die DE-CODA, eine 100%ige Tochter des DIHT, hat ein Pilotprojekt in 28 Industrie- und Handelskammern (IHK) ins Leben gerufen, das die Verwendung der gesetzeskonformen elektronischen Signatur im Servicebereich der IHK fördern und durchsetzen soll. Derzeit umfasst das Pilotprojekt zwei Teilbereiche der IHK-Tätigkeit:

- die Eintragung von Berufsausbildungsverträgen in das Verzeichnis der Ausbildungsverhältnisse der IHK sowie
- die Ausstellung von Ursprungszeugnissen durch die IHK

[27] Z. B. ABN Amro, die Bank of America, BNP Paribas sowie Commerzbank, Deutsche Bank, Dresdner Bank und HypoVereinsbank. Im Rahmen von Identrus wurden beispielsweise Anforderungen OCSP-Standard für die Zertifikateprüfung zu verwenden, Betriebsvorgaben für CAS, Prüfungsvorschriften, Schiedsklauseln, Geschäftsbedingungen mit Kunden, Garantiefristen, gegenseitige Anerkennung etc. festgelegt.

[28] Bei den vorhandenen Corporate Public Key Infrastructure (PKI) kommen die Standards PKIX/SPHINX (PKI) und S/MIME-MailTrust zum Einsatz.

Aktiv an der Durchführung dieser beiden Projekte sind 28 IHK, 40-50 Mitgliedsunternehmen, DE-CODA Gesellschaft zur elektronischen Zertifizierung von Dokumenten mbH, D-Trust GmbH sowie ComNetMedia AG beteiligt.

Diese Pilote wurden seitens der IHK gewählt, da die Ausstellung von Ursprungszeugnissen für die Unternehmen oft sehr zeitaufwendig ist, wenn Dokumente nachzureichen sind oder Nachfragen seitens der IHK erfolgen müssen. Durch die Online-Anwendung können die Unternehmen aktiv am Bearbeitungsprozess teilnehmen. Fehler werden durch die Online-Eingabe in der Java-Version vermieden. Die Transaktionszahl hat deutschlandweit ein Potenzial von 800.000 Ursprungszeugnissen pro Jahr.

In puncto verwaltungsübergreifende Vorgänge ist die Ausdehnung der Anwendung der elektronischen Signatur erwünscht (z. B. direkte Online-Weiterleitung der Ursprungszeugnisse an den Zoll).

Die Berufsausbildungsverträge stellen für die IHK intern einen sehr hohen Zeitaufwand (300.000 Berufsausbildungsverträge pro Jahr) dar, da die von den Unternehmen eingereichten Daten per Hand in die IHK-internen Systeme übertragen werden müssen. Durch die Online-Version werden Zeit gespart und Fehler vermieden.

1997 wurde mit der Planung des Einsatzes der elektronischen Signatur begonnen. Die aktuell genutzte Java-Version wurde im Oktober 1999 zum ersten Mal getestet und von den beteiligten Unternehmen positiv aufgenommen. Die Kosten für die Hard- und Software (49,- Euro) trägt jedes Unternehmen selbst. Dies ist derzeit noch eine Komplettlösung, da viele handelsübliche Lesegeräte nicht mit den technischen und sicherheitstechnischen Anforderungen kompatibel sind. In der fehlenden Kompatibilität wird auch im Allgemeinen der größte Hindernisfaktor für die Verbreitung der elektronischen Signatur gesehen.

Ein weiteres Projekt ist die IHK 24, das mit Hilfe der elektronischen Signatur die Unternehmen dazu ermächtigt, branchenspezifische Informationen oder Informationen über die eigene Firma im IHK-Netz abzurufen. Ferner soll die Chipkarte künftig auch für den Zugang zu Online-Akademien genutzt werden.

4.5.3 Berufsständische Kammern

Die berufsständischen Kammern waren im Rahmen ihrer Selbstverwaltung von jeher zuständig für professionsbezogene Ausweise und Berufszulassungen. Grundsätzlich ist denkbar, dass Kammern jeglicher Art zu virtuellen Trustcentern werden, d.h. sie übernehmen die Registrierung; die „Hardware“ im Sinne der technischen Sicherheitsinfrastruktur wird als Serviceleistung von einem Trustcenter in Anspruch genommen. Auch freiwillige Berufsvereinigungen zeigen ggf. Interesse auch an einer Zusammenarbeit mit berufsständischen Kammern, die über ein Trustcenter verfügen (z. B. Ingenieurverbände).

Nachfolgend soll an einigen ausgewählten Beispielen der aktuelle Diskussionsstand in den berufsständischen Kammern dargestellt werden. Die Tabelle gibt einen Überblick über Mitgliederzahlen und verdeutlicht somit den „Hebel“, der durch das Ausstatten der Mitglieder mit eSig zu erreichen ist bzw. wäre.

Berufskammer	Anzahl der Mitglieder*	Quelle
Bundesärztekammer	363 396, davon sind 72 255 ohne ärztliche Tätigkeit (Stand 1999)	http://www.baek.de
Bundeszahnärztekammer	78 068, davon 15 504 ohne zahnärztliche Tätigkeit (Stand 1999)	http://www.bzaek.de
Bundestierärztekammer	ca. 30 000 organisiert in 17 Tierärztekammern und 14 freien Berufsvereinigungen	Auskunft der BTK
Bundesapothekerkammer	ca. 53 000	http://www.abda.de
Bundesrechtsanwaltskammer	104 501	http://www.bmj.bund.de
Deutsche Patentanwaltskammer	ca. 1 700	http://www.patentanwaltskammer.de
Bundesnotarkammer	10 496, davon 1 657 „Nur-Notare“ und 8 839 Anwaltsnotare, die bereits in den Rechtsanwälten enthalten sind	http://www.bnotk.de und http://www.bmj.bund.de
Wirtschaftsprüferkammer	10 387 Wirtschaftsprüfer (Stand 1.8.2000) sowie 4 099 Buchprüfer. Von den Wirtschaftsprüfern sind ferner gleichzeitig 8 462 als Steuerberater und weitere 498 zusätzlich noch als Rechtsanwalt zugelassen	Auskunft der WPK
Bundessteuerberaterkammer	59 702 Steuerberater, 3 475 Steuerbevollmächtigte, 411 Personen nach § 74 Abs. 2 StBerG (Stand 1.1.2001)	Auskunft der BStbK
Bundesarchitektenkammer	106 592	http://www.bak.de
Bundesingenieurkammer	39 381 Mitglieder, davon 16 622 Pflichtmitglieder, 21 022 freiwillige Mitglieder und 1 737 Altmitglieder (Stand 31.12.2000)	http://www.bundesingenieurkammer.de
Bundeslotsenkammer	739 Mitglieder	Auskunft der Bundeslotsenkammer
Landwirtschaftskammern	ca. 182 000 Mitglieder (Betriebe > 2 ha landwirtschaftlich genutzte Fläche und Betriebe mit Viehhaltung und Spezialkulturen (Stand 31.12.1999)	Statistisches Jahrbuch 2000
Deutscher Handwerkskammertag	457 662 Mitglieder (Stand 31.12.1999)	Statistisches Jahrbuch 2000
Deutscher Industrie- und Handelstag	3 576 619 Mitglieder (Stand 31.12.1999)	Statistisches Jahrbuch 2000
Summe	**ca. 5 078 135**	

*Hinweis: Bei einigen Berufen gibt es Überschneidungen – z. B. Rechtsanwälte, Notare, Steuerberater und Wirtschaftsprüfer; die möglichen Doppelerfassungen konnten nicht überall herausgearbeitet werden. Ähnliches dürfte auch für die Ingenieure und die Patentanwälte gelten. Ferner beziehen sich die Mitgliedszahlen auf die Mitglieder der örtlichen Kammern. In den Bundeskammern als solchen sind jeweils nur die örtlichen Kammern Mitglieder.

Tabelle 4-11: Mitglieder der Berufskammern

Bundesnotarkammer

Seit August 2000 findet bei der Bundesnotarkammer ein Pilotprojekt mit Nutzung von akkreditierten Signaturen statt. Das Notarnetz mit 11.000 Mitgliedern ist von der RegTP Ende 2000 als Zertifizierungsstelle (CA) registriert worden. Das heißt, sämtliche Mitglieder und deren Angestellte erhalten dort ihre Schlüssel. Die notwendige Technik stellt das Trustcenter der Post, Signtrust, zur Verfügung. Aktuell sind 30-40 Notare in der Testphase; das Interesse für den Einsatz der akkreditierten elektronischen Signatur haben mittlerweile 450 Notare bekundet, so dass ab Mai/ Juni 2001 mit ca. 1000 Teilnehmern (Notare plus Mitarbeiter des Notariats) zu rechnen ist.

Wirtschaftsprüferkammer

Die Wirtschaftsprüferkammer plant, in Zusammenarbeit mit der DATEV e.G., Nürnberg, einen Feldversuch zum elektronischen Rechtsverkehr durchzuführen. Berufsangehörige sollen dabei untereinander, mit der Wirtschaftsprüferkammer und mit ausgewählten Dritten mittels eMail kommunizieren. Kernstück des Versuchs ist dabei der Einsatz gesetzeskonformer elektronischer Signaturen sowie die Verschlüsselung des Mail-Verkehrs. Ziel des Feldversuches ist es, berufsspezifische Erfahrungen im Umgang mit digitalen Signaturen im Besonderen und dem Elektronischen Rechtsverkehr im Allgemeinen zu sammeln.

Die DATEV betreibt für interne Zwecke ein Trustcenter, das allerdings nicht den Anforderungen des SigG von 1997 entspricht. Es werden DATEV-eigene Produkte eingesetzt; für die Dateisignierung z. B. GERVA, das in einem Projekt bei dem Hamburger Finanzgericht zum Einsatz kommt.

Bundesärztekammer

Die Bundesärztekammer (BÄK) und die Kassenärztliche Bundesvereinigung (KBV) erarbeiten unter Beteiligung des Zentralinstituts für kassenärztliche Versorgung (ZI) eine Health Professional Card in Deutschland für Ärzte (HPC-D (Arzt)). Es handelt sich dabei um einen elektronischen Arztausweis, der verschiedene Zusatzfunktionen wie den elektronischen Sichtausweis, die elektronische Signatur, die Authentifizierung, die Transportverschlüsselung sowie die elektronische Basisfunktion des Arztausweises beinhaltet.

Geplant ist eine deutschlandweite flächendeckende Einführung dieser elektronischen Arztausweise. Erste Pilotanwendungen wird es voraussichtlich im März 2001 geben. Ziel ist eine eindeutige elektronische Identifizierung der Gesprächspartner, ohne die eine Online-Kommunikation nicht stattfinden kann. Hierzu zählen u.a. die Übermittlung von elektronischen Patientenakten und elektronischen Arztbriefen, Einweisungen in Krankenhäuser etc.

Bislang ist die HPC-D (Arzt) auf die Spezifizierung Arzt begrenzt. Eine Ausdehnung dieser Chipcard auf andere Berufe im Gesundheitsbereich wie Apotheker und Hebammen ist jedoch geplant.

4.6 Zusammenfassende Bewertung der Bestandsaufnahme

Die Nutzung der eSig steckt noch in der Experimentierphase. In Deutschland wurden im Rahmen dieser Studie 23 Projekte und Vorhaben identifiziert, bei denen elektronische Signaturen eingesetzt werden oder geplant sind. Insgesamt sind dabei weniger als 15.000 Nutzer mit qualifizierter eSig involviert.[29] Die Situation ist geprägt durch eine Vielzahl von Pilotprojekten mit Inselcharakter, bei denen Fragen der Interoperabilität und Standardisierung nur eine untergeordnete Rolle spielen.

Durch den Wettbewerb MEDIA@Komm wurde eine erhebliche Dynamik in den Kommunen erzeugt. Wichtig war, dass die Förderung des Bundes erstmals maßgebliche Anreize geschaffen hat, Anwendungen für rechtsgültige Signaturen zu entwickeln und insbesondere *operative Probleme* zu lösen. Denn ansonsten, so zeigen andere Studien, wird die eSig im Rahmen von eGovernment-Initiativen eher nachrangig behandelt.

Im Einzelnen lassen sich die Erkenntnisse aus der Bestandsaufnahme bei den drei wesentlichen Verwaltungsebenen sowie bei wichtigen potenziellen Multiplikatoren wie folgt zusammenfassen.

Der Bund als Treiber der Entwicklung **–** Konkrete eSig-Anwendungen finden sich häufig in den Bereichen, in denen der Bund gezielt fördert oder zahlt (z. B. Gesetzgebung, SPHINX, eProcurement, MEDIA@Komm etc.). Kommunen schaffen auch auf lokaler Ebene Fakten. Die Länder hatten bisher eine eher abwartende Rolle eingenommen. Wenn eGovernment effizient umgesetzt werden soll, ist eine stärkere Koordination/Kooperation der drei Verwaltungsebenen wünschenswert.

Piloten auf Nebenschauplätzen – Manche Pilotprojekte, insbesondere solche auf kommunaler Ebene, befassen sich mit sekundären Prozessbereichen (z. B. Anwohnerparkausweise, Hundesteuer, Jugendveranstaltungen). Dies kann möglicherweise darauf hindeuten, dass der ökonomische Nutzen im Sinne von Einsparungen bei Prozessoptimierungen nicht im Vordergrund steht, sondern ein Experimentieren in „risikoarmen“ Bereichen bevorzugt wird. Dies kann auch auf das Fehlen einer klaren eGovernment-Strategie hindeuten. Die Auswahl sehr spezifischer (Klein-)Anwendungen hat in der Praxis den Nachteil, dass bundes- oder landesweit oft nur jeweils *ein* vereinzelter Pilot in einem bestimmten Einsatzbereich läuft. Die Möglichkeiten eines gegenseitigen Austausches sind aufgrund der fehlenden Parallelbearbeitung gering, die Spezifitäten der jeweils anderen Anwendungen so unterschiedlich, dass ein Wissenstransfer nur schwer möglich ist.

Asymmetrie zwischen mindestoptimaler Betriebsgröße für eGovernment-Plattform und Kommunen - Eine zentrale Erkenntnis der Projekte ist, dass die „mindestoptimale Betriebsgröße“ für eine eGovernment-Plattform aufgrund der erforderlichen Größeneffekte in der Informations- und Kommunikationstechnologie mit elektronischer Signatur deutlich über der Dimension einer einzigen (großen) Kommune liegt. Insofern stellen die Kooperation von Städten wie im Nürnberger Projekt oder auch die Diffusionsstrategie der Bremer bos zukunftsträchtige Ansätze zur Einführung von virtuellen Rathäusern etc. dar. Dass selbst im überschaubaren Projektkontext wie der MEDIA@Komm Standardisierungsprobleme zwischen den drei Städten entstanden sind (Chip-

[29] Davon gehört das Gros zum Land Niedersachsen (Automatisiertes Haushaltswirtschaftsystem mit derzeit 12.000 Anwendern).

karten nicht austauschbar), zeigt einen erheblichen intra- und interkommunalen Koordinierungsbedarf.

Das gilt auch für die Fördermittelpolitik, wenn sich etwa Projekte auf Finanzmittel und weniger auf klar definierte Eigenbedürfnisse ausrichten. Für die Fördermittelpolitik erwächst daraus eine besondere Verantwortung hinsichtlich des Fördermittelzuschnitts, denn das Schauen auf Finanzmittel darf die eigene strategische Erschließung des Themas nicht überdecken oder behindern.[30]

Darüber hinaus werden die technischen Möglichkeiten die bestehende territoriale Organisations- und Verantwortlichkeitsstruktur der Verwaltung in Frage stellen. Internetprojekte setzen gegenwärtig konzeptionell i.d.R. auf den bestehenden Strukturen auf und versuchen, diese elektronisch nachzubilden bzw. zu kopieren. Zwar kommt es hierdurch zu Prozessvereinfachungen – die damit verbundenen Effekte beinhalten jedoch nur einen Bruchteil des theoretischen Einsparpotenzials. Dieses Potenzial würde sich in einigen Feldern aber erst dann entfalten, wenn die gegenwärtig territorial orientierte Strukturausrichtung (z. B. Finanzämter) einem grundsätzlichen Reengineering unterzogen würde.

Komplexe Lösungen behindern schnelle Umsetzung – In Bezug auf die Signatur im Speziellen hat sich außerdem gezeigt, dass komplexe Lösungen, die die Einbeziehung zahlreicher Akteure erfordern (v.a. die Bündelung von Signier- und Bezahlfunktionen) gerade in der Anfangsphase die Projekte erheblich bremsen können. Die Frage der Signatur an sich (Was ist eine rechtsgültige Signatur? Was muss überhaupt signiert werden?) ist bereits in sich komplex. Eine aus Sicht von Experten sinnvolle Addition von Funktionen erschwert eine pragmatische Umsetzung der Signatur.

Fehleinschätzungen durch Lücke zwischen Erwartungen durch PR-Information und Realität Es wird häufig davon gesprochen, dass ökonomische und prozessuale Aspekte im Zusammenhang mit eGovernment im Allgemeinen und in Bezug auf die elektronische Signatur im Besonderen unterschätzt werden. Dies trifft vor allem auf diejenigen zu, die mit den technischen Details wenig vertraut sind, vornehmlich Medien, Politik, Öffentlichkeit, Verwaltungsspitze. Angesichts der geschätzten Investitionsvolumina im mehrstelligen Millionen-Bereich im eGoverment im Allgemeinen und in Bezug auf die elektronische Signatur kann diese Einstellung dazu führen, dass bei hohem Erwartungsdruck zu schnell in Insellösungen investiert wird. Es drohen vor allem bei zukünftigen „Innovatoren“ Fehlplanungen.

Fortschrittliche Außenwirkung vor nachhaltiger Binnenmodernisierung – Die Kommunen stehen in einem ambivalenten Spannungsverhältnis, das bereits im Modell des neuen Steuerungsmodells angelegt ist. Auf der einen Seite soll sich die Kommune als Dienstleister beim Kunden (Bürger) anbieten – in diesem Sinne ist die Verwaltung stärker politisiert (politisch gewünschtes „Vermarktungserfordernis“). Auf der anderen Seite muss sie angesichts der Haushaltsentwicklung ökonomisch effizient sein. Dieser Zielkonflikt wird zur Zeit zu Ungunsten einer weniger öffentlichkeitswirksamen ökonomischen Betrachtung gelöst. Ein Großteil der gegenwärtigen Planungen und Projekte orientiert sich an der Servicefunktion; die (Teil-) Refinanzierung, die in erster Linie nur durch Prozessoptimierung erzielt werden kann, wird dabei jedoch oft ausgeklammert. Es überwiegen Lösungen in Bereichen, in denen eine Gegenfinanzierung der erforderlichen Investitionen ungesichert erscheint.

[30] So hat etwa die Stadt Karlsruhe ihre Prioritäten neu definiert, nachdem sie mit ihrer Multimedia-Initiative beim Wettbewerb MEDIA@Komm nicht unter die Preisträger gewählt wurde.

Angesichts dieser offensichtlichen Hindernisse bzw. Risiken für eine erfolgreiche Durchsetzung der eSig stellt sich die Frage, ob der Markt geeignete Lösungen hervorbringen wird oder ob ggf. ein Eingreifen des Staates erforderlich ist.

4.6.1 Akteursinteressen und Handlungsbedarf

Diese Situation soll anhand einer Analyse der (vermuteten) Interessenlage der wesentlichen Akteure erläutert werden.

Als zentrale Akteure seien hier auf Anbieterseite Chipkartenhersteller, Softwareproduzenten, Trustcenterbetreiber und Banken genannt, auf Nachfragerseite Privatpersonen, Unternehmen, die Entscheidungsträger in Ministerien und Behörden sowie berufsständische Organisationen.

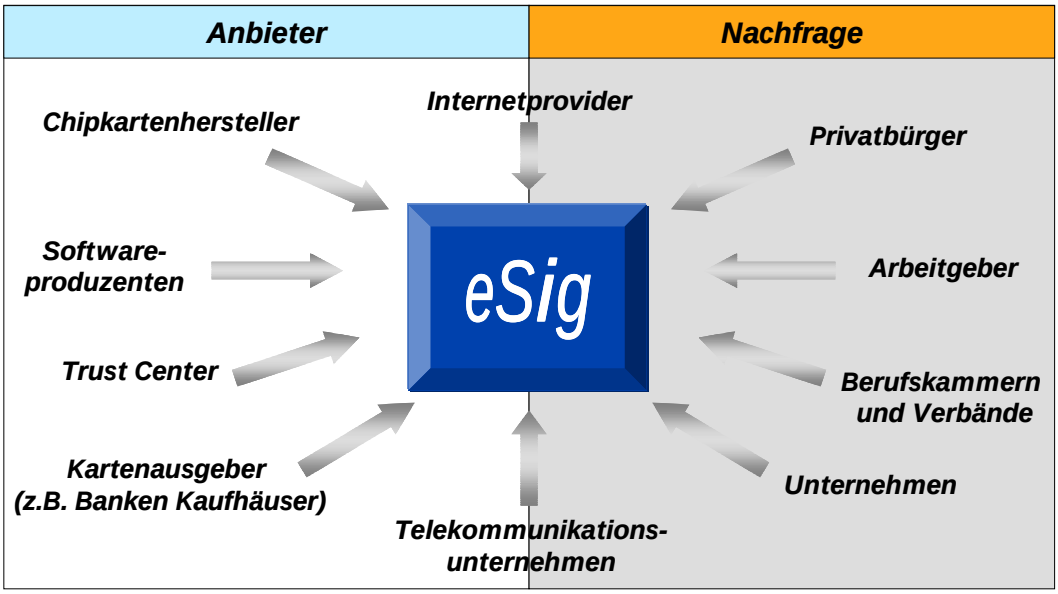


Abbildung 4-6: Marktteilnehmer eSig

4.6.2 Interessen der Akteure auf Anbieterseite

Sowohl Chipkartenhersteller als auch Softwareproduzenten und Trustcenterbetreiber dürften unter der Annahme einer Gewinnmaximierung ein Interesse daran besitzen, möglichst (ihre) proprietäre Lösung in den Markt zu bringen und Standardisierungen nur dort zuzulassen, wo das Internet bereits Standards gesetzt hat (z. B. S/MIME), oder wo große Auftragnehmer dies nachdrücklich einfordern (z. B. ISIS). Zu den Annahmen über Interessen im Einzelnen:

Um ihre spezielle Lösung abzusichern haben *Chipkartenhersteller* ein Interesse daran, den deutschen Markt vor ausländischer Konkurrenz zu schützen. Gleichzeitig trägt eine hohe Komplexität der technischen Basis des Chips dazu bei, spezielle Produkte zu schaffen, z. B. dadurch, dass mehrere Funktionen auf der Chipkarte gebündelt werden.

Softwareproduzenten, die auf Sicherheitslösungen spezialisiert sind, haben ein Interesse daran, langfristige Kundenbeziehungen dadurch zu schaffen, dass ihre proprietären Systeme tief in Verwaltungsprozesse integriert sind, so dass ihnen bei Veränderungen der Softwareumgebung bzw. Prozessänderungen Wartung bzw. Anpassungen ein sicheres langfristiges Auftragsvolumen

praktisch garantiert ist. Je kleiner Unternehmen sind, umso bedeutsamer ist dabei ein (einziger) großer Kunde.

Trustcenterbetreiber konzentrieren sich derzeit auf unterschiedliche Kundengruppen und deren jeweilige Rollen, so dass die Märkte relativ abgegrenzt sind. Man versucht, in den jeweiligen Teilmärkten Standards zu setzen. Beispiel: virtuelle Trustcenter als neuer Leistungsbereich der Signtrust, Vermarktung des nicht SigG-konformen Identrus-Konzeptes durch TC Trustcenter. Die Vereinbarung des ISIS-Standards ist zwar ein erster Schritt innerhalb des Oligopols der Trustcenter, er sichert jedoch die Interoperabilität lediglich im „back-office“ der Trustcenter, in dem er z. B. unternehmensübergreifend Verzeichnisdienstabfragen möglich macht.

Unternehmen können prinzipiell sowohl Anbieter als auch Nachfrager von eSig sein. Der Anbieterseite werden hier all jene Unternehmen zugerechnet, die ihren Endkunden Signaturen (mit-) anbieten. Hierfür sind insbesondere solche Unternehmen prädestiniert, die bereits in Chipkarteninfrastrukturen auf Kundenseite investiert haben (z. B. Finanzinstitute, Kaufhäuser, Fluggesellschaften, Mietwagenfirmen, Versicherungen).

Entscheidungsträger in *Finanzinstituten* seien hier gesondert erwähnt, da sie in dem bisherigen Diskussionsprozess über eSig eine zentrale Rolle gespielt haben (vgl. Abschnitt 4.5.1). Finanzinstituten kann ein primäres Interesse an ihrem Kerngeschäft unterstellt werden. Für dieses besitzen sie mit dem HBCI-Standard ein funktionsfähiges Produkt (ohne eSig), das von ca. 15-20% der Kunden bereits genutzt wird. Die Neuregelung des Signaturgesetzes schafft aufgrund der verbraucherschutzrechtlichen Regelungen keine zusätzlichen Möglichkeiten für die Banken, den Umfang der Online-Transaktionen zu erweitern. Der Einsatz der eSig wird damit nicht offensichtlich zu Prozesskosteneinsparungen führen. Ein anderer Nutzen, z. B. in Form einer höheren Kundenbindung, ist derzeit mangels Anwendungen zumindest kurzfristig nicht erkennbar. Insofern haben die Finanzinstitute aktuell eher wenig Anreize, Investitionen in die Nutzung einer eSig zu tätigen, zumal die Filialen als prädestinierte Registrierungsstellen mit der Euroumstellung im nächsten Jahr nicht unbeträchtlich belastet sein werden.

Unter den *Internetprovidern* besteht ein starker Wettbewerb. Aufgrund der Netzwerkeffekte (vgl. Abschnitt 3.3) besitzen sie ein besonderes Interesse daran, schnell zahlreiche Nutzer an sich zu binden. Dies wird mit Gratisangeboten der „Basisleistungen“ (eMail-Account, Postverwaltung, Benachrichtigungsservice) sowie zahlreichen Zusatzleistungen (z. B. Grußkartenversand, Klingeltöne Handys) erreicht. Hierzu gehört auch das Angebot einer Sicherheitsinfrastruktur. Unter den einschlägigen deutschen Internetprovidern hat zuerst web.de eine eSig angeboten, allerdings auf Softwarebasis. Andere Provider haben mittlerweile nachgezogen. Die Einführung qualifizierter Signaturen ist allerdings zumindest im Privatkundengeschäft derzeit auskunftsgemäß nicht geplant.

4.6.3 Interessen der Akteure auf Nachfragerseite

Auf der Nachfragerseite lässt sich der Nutzen der eSig übergreifend mit Sicherheitsgewinn, Zeitersparnis und Kostensenkung/-vermeidung überschreiben. Allerdings sind die konkreten Interessen von Privatpersonen, Unternehmen und berufsständischen Organisationen im Einzelnen sehr unterschiedlich.

Der Nutzen einer eSig ergibt sich aus Sicht der *Privatbürger* insbesondere aus der Zeitersparnis und dem erhöhten Komfort. Bei größeren Transaktionen dürfte auch die Sicherheit eine wichtige Rolle spielen. Bei einem Teil der Bevölkerung kann außerdem eine gewisse Technikaffinität unterstellt werden. Diese hat z. B. bisher dazu geführt hat, dass über 200.000 Personen ihre

Steuererklärung Online abgegeben haben, obwohl die Unterlagen danach trotzdem in Papierform zu übersenden sind. Angesichts der durchschnittlich 2,5 Verwaltungskontakte pro Jahr und der Möglichkeit, Online-Geschäfte auch ohne Chipkarte zu tätigen, dürfte die Bereitschaft zur Beschaffung einer Signaturkarte inkl. Lesegeräte etc. für Zwecke des privaten Gebrauchs allerdings eher eingeschränkt sein. Hinzu kommt, dass der Komfortgewinn sich nur dann realisiert, wenn die technischen Anwendungen problemlos funktionieren, wovon derzeit nicht ausgegangen werden kann.

Bei *Entscheidungsträgen in öffentlichen Einrichtungen* dürfte die Interessenlage in Bezug auf die eSig ambivalent sein. Entscheidungsträger, die die Umsetzung von eGovernment fördern wollen, dürften ein starkes Interesse besitzen, die Nutzung der eSig zu unterstützen. Erst mit Hilfe der eSig kann typischen Vorgaben der Verwaltung , insbesondere das Primat der Rechtsbindung des öffentlichen Handelns in jedem Einzelfall, Rechnung getragen werden. All jene, die eGovernment eher kritisch gegenüberstehen, dürften rechtliche Unsicherheiten, hohe fachliche Komplexität und (nicht zu Unrecht) die bisher unzulänglichen technischen Lösungen hervorheben.

Die inhärent konfliktären Interessen der Verwaltungsebenen mit den Autonomiebestrebungen auf kommunaler Ebene einerseits und hoher Sichtbarkeit der Länderpolitik andererseits führen jedoch (bislang) nicht zu einer gleichgerichteten Nachfrage, sondern eher zu auseinanderlaufenden als konzertierten Aktivitäten.

Vertreter berufsständischer Organisationen sind in hohem Maße daran interessiert, ihren Mitgliedern eine sichere und effiziente Autorisierung zu ermöglichen. Gleichzeitig stärkt eine Ausweitung der Kompetenzen der Kammer ihren Status und damit die Handlungsmöglichkeiten der Kammervertreter. Darüber hinaus lassen sich mit der eSig Prozesskosten reduzieren.

Insgesamt lässt sich als Ergebnis der Bestandsaufnahme ein akuter Handlungsbedarf konstatieren. Die Interessen der beteiligten Akteure sind zu unterschiedlich, als dass die technischen und wirtschaftlichen Probleme, die eine flächendeckende Diffusion der (qualifizierten) Signatur bisher verhindert haben, sich zügig lösen würden. Ein konzertiertes Vorgehen kommt nicht zu Stande, da die Nachfrage (noch) zu gering ist bzw. in Kleinaufträgen jeweils nur ein Anbieter aus jeder Leistungsstufe zum Zuge kommt.

5 Empfehlungen für die Diffusion der eSig

5.1 Prämissen und Erfolgsfaktoren

Den nachfolgenden Empfehlungen liegen Annahmen über bestimmte Rahmenbedingungen und Ziele zugrunde, die nach unserem Verständnis mit der eSig verfolgt werden.

- Der „aktivierende Staat" bleibt das Leitbild der Verwaltungsreform.
- Es gilt die Zielsetzung der Bundesregierung, ab 2005 alle onlinefähigen Dienstleistungen des Bundes über das Internet anzubieten.
- Das Bundesverwaltungsverfahrensgesetz und die einschlägigen Ländergesetze werden noch in 2001/2002 hinsichtlich einer Gleichstellung der elektronischen mit der händischen Unterschrift angepasst.

Auftragsgemäß sind bei der Ausarbeitung von Empfehlungen die folgende Aspekte besonders zu berücksichtigen:

- Schnelle Umsetzung
- Breiten- und Signalgebung
- Aufnahmefähigkeit von Verwaltungen für neue Technologien
- Einbindung in bestehende und neue Workflow-Prozesse
- Verbindungen zur mittelständischen Wirtschaft

Auf der Grundlage der Bestandsaufnahme und unter Berücksichtigung der technischen, rechtlichen und sozioökonomischen Rahmenbedingungen lassen sich für die zukünftige Verbreitung der eSig einige übergreifende Empfehlungen formulieren, aus denen kurzfristige Maßnahmen und mittel- bis langfristiger Handlungsbedarf abgeleitet wird. Angesichts der Komplexität der Materie können nicht alle Aspekte berücksichtigt bzw. ausführlich erläutert werden. Sie werden hier aber skizziert, da die Empfehlungen als Anregung und Diskussionsbeitrag zum Thema elektronische Signatur dienen sollen.

5.2 Übergreifende Empfehlungen

1. Die Signaturlösungen müssen einfach sein, keine Mehrfachfunktionen auf der Chipkarte selbst. Aber: die Verschlüsselungsfunktion muss integriert sein.

Begründung: In der bisherigen Praxis wurde versucht, über die Aggregation von Signatur- und Zahlungsfunktionen sowie anderen Anwendungen (z. B. Studentenausweis, Zugangsberechtigung, Fahrschein etc.), die Nutzungsmöglichkeiten und damit die Attraktivität der Signaturkarte zu erhöhen. Dieser grundsätzlich sehr sinnvolle Ansatz führt derzeit aufgrund unausgereifter technischer und neuer organisatorischer Prozesse in der Praxis zu einem hohen Abstimmungs- und Koordinationsaufwand (z. B. zwischen RegTP und ZKA) und u.U. zu technischen Problemen (z. B. Antwortzeiten bei Java-Applets). Dies verlangsamt bzw. verhindert eine Realisierung von eSig-Lösungen.

Die Integration der Verschlüsselungsfunktion ist technisch nicht problematisch, organisatorisch aber erfolgskritisch, da zahlreiche signaturrelevante Transaktionen (z. B. Steuererklärung, Übermittlung von Gesundheitsdaten, eVergabe, eVoting) vertraulich versandt werden müssen. Es wäre äußerst ineffizient, in allen Verfahren eine separaten Verschlüsselungsmechanismus zu installieren. Daher sollte die Verschlüsselung integraler Bestandteil der Signaturkarten sein.

2. Die elektronische Signatur sollte wie die händische Unterschrift mit der natürlichen Person verknüpft bleiben und sich nicht zu einem Dienstsiegel/Stempel u.ä. entwickeln.

Begründung: Das Signaturgesetz knüpft die eSig explizit an die natürliche Person; sie soll die händische Unterschrift der Privatperson elektronisch ermöglichen. In der (bisherigen) Praxis werden eSig insbesondere dafür eingeführt, dass bestimmte, mit definierten Kompetenzen besetzte Funktionen innerhalb von Organisationen (z. B. Vorstand, Geschäftsführung, Amtsleiter) wahrgenommen werden. Die Zertifikatspolitik stellt daher primär auf das Organisationsinteresse ab (z. B. bei Attributen), so dass eine Anwendung der eSig in anderen Zusammenhängen (z. B. Signieren privater Mails) eingeschränkt wird oder datenschutzrechtlich problematisch ist. Ein Abgehen von der natürlichen Person, der eine Unterschrift zugeordnet wird, hin zur Rolle, der eine Unterschrift zugeordnet wird, ist auch in der papierbasierten Kommunikation nicht zu beobachten. Immer wird durch zusätzliche Attribute, die nicht zur Unterschrift gehören, eine Rolle in einem spezifischen Kontext ausgeformt (Unterschrift vs. Urkunde). Attribute sollten daher, wenn möglich, nicht in das Hauptzertifikat aufgenommen werden.

3. Bei der Verbreitung der eSig sollte der Staat nicht nur auf die Initiative einer einzelnen Akteursgruppe setzen (z. B. Kreditinstitute). Durch das Angebot nützlicher Online-Fachanwendungen im eigenen Bereich sollte die eSig ein für verschiedenste Unternehmen attraktiver Wettbewerbsparameter werden.

Begründung: Bisher stand die Argumentation im Vordergrund, dass durch die Aggregation von Funktionen auf Chipkarten eine Kostendegression herbeizuführen sei, die ein Verbreitungshemmnis beseitigen würde. Trotz zum Teil mehrjähriger Ankündigung sind aber z. B. Signierkarten mit EC-Funktion, die sowohl von RegTP als auch ZKA zertifiziert sind, nicht im Einsatz. Bei der Beschränkung auf die reine Signierfunktion würde der Staat den Wettbewerb auf einen größeren Teilnehmerkreis ausweiten. Zudem scheinen die Wettbewerbsvorteile, die sich durch Ausgabe von Signierkarten ergeben, auf Seiten der Wirtschaft noch nicht hinreichend präsent zu sein (höhere Kundenbindung, höhere Auslastung flächenintensiver Geschäftsstellen).

4. In einer Sensibilisierungs- und Aufklärungsoffensive muss das Bewusstsein für die Sicherheitsrisiken des Geschäftsverkehrs im Internet und der Nutzen der eSig in der Öffentlichkeit verstärkt publiziert werden.

Begründung: Bei der eSig handelt es sich um ein erklärungsbedürftiges Produkt. Sowohl öffentliche als auch private Entscheidungsträger müssen über Inhalt und Anwendungsmöglichkeiten der eSig informiert werden. Für Unternehmen ist der Vorteil der Rechtswirksamkeit von Transaktionen mit qualifizierter Signatur herauszustellen. Bürger sollten über die Signatur im Kontext *konkreter* Anwendungen informiert werden.

Die Neuheit und Dynamik des Internetmarktes und der angrenzenden Bereiche hat bereits häufiger Fehlprognosen hervorgerufen. Daher laufen langfristige Empfehlungen schnell auf Spekulation hinaus. Wir konzentrieren uns daher im Folgenden auf eher kurzfristige Maßnahmen. Je nachdem, wie erfolgreich sich diese erweisen, werden sich mittelfristig unterschiedliche Heraus-

forderungen ergeben. Bereits heute absehbarer Handlungsbedarf wird im Anschluss daran allerdings formuliert.

5.3 Empfehlungen zur Diffusionsstrategie

Die Forderung nach einer schnellen massenhaften Verbreitung der eSig macht sehr deutlich, das eine grundlegende Änderung in der Handlungsstrategie der öffentlichen Verwaltung einkehren muss. Dabei sind die folgenden Schritte erforderlich:

- Standardisierung der Basiskomponenten der eSig
- Zusätzlich zu Pilotversuchen sind breite Anwendungen mit hoher Signalfunktion zu schaffen
- Zunächst Fokussierung auf die Querschnittsfunktion eMail
- Maßnahmen zur Diffusion von Signaturkarten (Big Bang oder Multiplikatoren)
- Schaffen von medienbruchfreien Fachanwendungen durch eSig

Die untenstehende Abbildung soll den Kontext dieser Empfehlungen deutlich machen. Die technische Basisinfrastruktur kann durch Vorgaben, die Nachfrager von Signaturleistungen generieren, beeinflusst werden. Hier sollte bei der Auswahl der Basiskomponenten insbesondere die Interoperabilität von Chipkarten und Zertifikaten gefordert werden. Unter den vier technischen Anwendungsbereichen wird die Querschnittsanwendung Messaging empfohlen, weil die anderen Anwendungen Probleme aufwerfen, die einer kurzfristigen Umsetzung entgegenstehen (siehe Abschnitt Technische Rahmenbedingungen).

Hinsichtlich der Fachfunktionen sollte man sich auf eingeführte bzw. in der Entwicklung befindliche Verfahren mit hoher Öffentlichkeits- und Multiplikatorwirkung konzentrieren. Eine universelle Einsetzbarkeit der Chipkarte gewährleistet dabei, dass Bürger eine Karte in unterschiedlichen Rollen (z. B. als Arzt, Mitarbeiter eines Landesbetriebes, Steuerzahler) nutzen können.

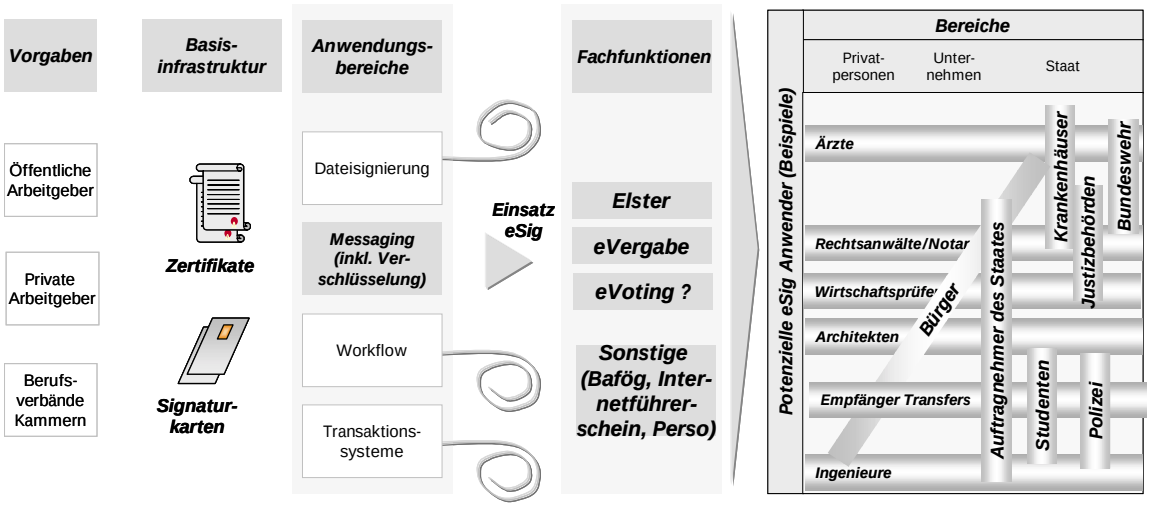


Abbildung 5-1: Überblick optionale Vorgehensweise

1. Die Standardisierung der Basiskomponenten sollte stärker vorangetrieben werden.

Begründung: Voraussetzung für eine schnelle Verbreitung der eSig ist die konsequente Standardisierung der Basiskomponenten und ihrer Schnittstellen. Außerdem sollte die Komplexität der Lösung möglichst gering gehalten werden. Im Einzelnen bedeutet dies:

Die universelle Einsetzbarkeit von Chipkarten ist herzustellen, d.h. die Benutzung von X.509v3, PKCS 15 und die DIN Vornorm muss standardisiert werden. Dies erfordert eine Harmonisierung von bestehenden Standards wie Mailtrust, HBCI, OSCI und ISIS. Eine solche Harmonisierung kann grundsätzlich durch die Wirtschaft selbst oder durch hoheitliche Vorgabe geschehen.

KPMG empfiehlt,

- unterstützend zu Bemühungen in der Wirtschaft seitens der RegTP Interoperabilitätstests zu veröffentlichen. Dies ist bereits 1998 von der EESSI dringend empfohlen worden. Hierfür müsste seitens der RegTP ein Referenzmodell entwickelt werden, mit dem letztlich Vorschläge für eine Harmonisierung gemacht werden.
- Festlegung eines Standards für den Zugriff der Funktionsbibliotheken auf Anwendungen (z.B. PKCS #11) .
- Definition der S/MIME-Parameter für die Signierung beim Messaging.
- Vereinheitlichen der Definition der Zusatzattribute bei Zertifikaten nach X.509v3, damit die Zertifikate von beliebigen Anwendungen verwendet werden können.

2. Einzelne Piloten sollten durch Massenanwendungen ergänzt werden.

Begründung: Ziel sollte es sein, eine kritische Masse von 15-20% der Internetnutzer zu erreichen, das waren im Januar 2001 3,3-4,4 Mio. Personen, bei einer zunehmenden Wachstumsrate[31]. Das bisherige Vorgehen, einzelne Pilotprojekte zu fördern, hat zu zahlreichen Insellösungen geführt und die für eine breiten Einsatz der eSig erforderliche Standardisierung eher verlangsamt. Zukünftig sollte darauf abgezielt werden, große Nutzerzahlen zu erreichen. Da die eSig Netzwerkeffekten unterliegt, steigt ihr Nutzen überproportional mit der Anzahl der Nutzer. Die qualifizierte eSig wird sich nur dann durchsetzen, wenn eine hinreichende Anzahl der Nutzer sie regelmäßig verwendet. Gleichzeitig wird nur so eine hinreichende Standardisierung erreicht. Als Zielgröße bis 2004 wird gemäß der o.g. wachsenden Quote von einem Nutzerkreis von 4-5 Mio. Personen ausgegangen.

3. Elektronische Signaturen sollten primär mit der Querschnittsfunktion eMail verknüpft werden.

Begründung: In der Praxis hat sich gezeigt, dass der Ansatz, im ersten Schritt den technisch komplexesten Verfahrenstypus, Transaktionssysteme, mit eSig zu verknüpfen (siehe MEDIA@Komm), zu großen Herausforderungen führt. Dies gilt insbesondere dann, wenn individuell programmierte Fachverfahren angepasst bzw. ganze Geschäftsprozesse (z. B. auf der kommunalen Ebene die Bestellung von Dokumenten) analysiert, neu definiert und dann neu programmiert werden müssen.

[31] Im Januar 2001 nutzten 22,2 Mio. Deutsche älter als 14 Jahre das Internet. Dies entspricht 34,8% der Gesamtbevölkerung. Vgl. „Cyberdemographics“, in: GFK-online-monitor, ard-werbung.de, forsa, mediengruppedigital.de.

Der Einsatz der eSig im Rahmen von Workflowprozessen ist grundsätzlich sinnvoll; angesichts der geringen Verbreitung eSig-fähiger Workflowanwendungen jedoch als Einstiegsszenario für eine Durchsetzung der Signatur nicht geeignet.

Dateisignierungen eignen sich nicht als Ansatzpunkt, da Dateiformate nicht standardisiert sind.

Es wird daher empfohlen, im Rahmen der Einführung von eSig auf Messaging zu setzen, da es sich um eine fachverfahrensunabhängige Querschnittsanwendung handelt, die mit gängigen Bürosoftwareprodukten abgebildet wird, bei der auch größere Datenmengen in Form von Dateianhängen transportiert werden können und bei dem auch das Problem der Verschlüsselung relativ einfach mitgelöst werden kann.

4. Die Diffusion der elektronischen Signatur sollte durch eine „Big Bang-Strategie" oder eine „Multiplikatoren-Strategie" unterstützt werden.

Begründung: Sollte das Gros der Kreditinstitute entsprechend ihrer Ankündigung in der nächsten EC-Kartengeneration eine (qualifizierte) Signierfunktion applizieren, so würden in den nächsten Jahren knapp 50 Mio. Signaturkarten im Umlauf sein. Unter diesen Voraussetzungen ist anzunehmen, dass der Markt sowohl für eGovernment als auch für eCommerce Anwendungen entwickelt, wird, bei denen rechtsgültig elektronisch unterschrieben werden kann.

Für den Fall, dass nur wenige Kreditinstitute bezüglich der qualifizierten eSig aktiv werden, stellt sich das Problem, wie eine kritische Masse von 4-5 Mio. Anwendern erzeugt werden kann.

Prinzipiell besitzen Bund, Länder und Kommunen für diesen Fall mehrere „Hebel", um aktiv zu werden. Hierfür gibt es u.E. die beiden folgenden Optionen:

„Big Bang-Strategie" (Zielgruppe: Privatbürger)

„Multiplikatorenstrategie" (Zielgruppe: professionelle Mittler, Unternehmen)

Option A: Big Bang-Strategie

Hier steht der Bürger im Vordergrund. Die Idee besteht darin, bei einer konkreten Gelegenheit, z. B. anlässlich der Europawahlen 2004, Signaturkarten an alle Bundesbürger über 16 Jahre zu verteilen. Eine solche öffentlichkeitswirksame „Zugpferd"-Anwendung müsste von verschiedenen zusätzlichen Einsatzmöglichkeiten begleitet werden. Damit der Nutzen der Karte nicht vom Besitz eines PCs bzw. Internetanschlusses abhängt, kann auch ein breites Netz an Kiosken aufgestellt werden, über die – ähnlich der intelligenten Bank-Terminals – Transaktionen mit der Verwaltung und anderen Stellen durchgeführt werden können.

In Bezug auf das erforderliche Investitionsvolumen lassen sich nur die Materialkosten schätzen. Unter der Annahme einer (realistischen, eher konservativ angesetzten) Stückkostendegression in Höhe von 70 % ergibt sich bei Kosten von ca. 50 DM für ein „Signaturgesamtpaket" (Chipkarte inkl. Kartenleser) ein Investitionsbedarf in Höhe von 3,5 Mrd. DM. Zu diesem sind die Prozesskosten sowie Kosten für Kioske, Kommunikationsmaßnahmen etc. hinzuzuzählen.

Geht man davon aus, dass diese Investitionen dazu beitragen, das eGovernment schneller breitflächig umzusetzen, so könnten sich die Investitionskosten jedoch sehr schnell amortisieren.[32]

Blickt man auf die wirtschaftspolitischen Zielsetzungen der letzten beiden Dekaden zurück, die geprägt waren von einer Zurückführung der Regulierung und der aktiven Beteiligung öffentlicher Institutionen am Produktionsprozess, so mag die oben vorgeschlagene Handlungsstrategie fremd anmuten. Gleichwohl lässt sich diese Empfehlung streng ökonomisch begründen, wenn Sicherheit im Internet als externer Effekt aufgefasst wird.

Als externe Effekte werden Nebenwirkungen von Konsum- und Produktionsakten auf Dritte verstanden, die nicht über den Markt entgolten oder auf anderem Weg als einzelwirtschaftliche Kosten bzw. Erträge zugerechnet werden (können). In diesem Fall treffen einen Akteur weder alle positiven noch alle negativen wirtschaftlichen Folgen einer Ressourcennutzung in vollem Umfang. Unter diesen Bedingungen wird sich möglicherweise kein Akteur bereit erklären, die Kosten der Produktion eines solchen Gutes in vollem Umfang zu tragen. Das Gut wird nicht oder nur in unzureichendem Umfang bereitgestellt.

In einer solchen Situation fordert die ökonomische Theorie staatliche Eingriffe in ein wettbewerbliches System, wenn sie dazu dienen, positive externe Effekt zu unterstützten (z. B. Grundlagenforschung) bzw. negative externe Effekte zu vermeiden (z. B. Umweltverschmutzung). Sicherheit im Internet kann als ein solcher positiver externer Effekt aufgefasst werden, wenn man unterstellt, dass heute zahlreiche Transaktionen deshalb nicht online durchgeführt werden, weil die Sicherheitsanforderungen nicht ausreichen. Produktivitäts- und Wachstumspotenziale des eCommerce und des eGovernment werden nicht genutzt.

Hinzu kommt das Eigeninteresse des Staates, Effizienz und Effektivitätspotenziale des eGovernment auszuschöpfen. Die Verfügbarkeit der rechtsgültigen elektronischen Unterschrift in allen Bevölkerungsgruppen ist dabei eine wichtige Voraussetzung. Die „Big Bang-Strategie“ kann durch die gleichgerichtete Streuung der Karten dazu beitragen, einen „digital divide“ im Sinne einer Trennung von Anwendern und Nicht-Anwendern aufgrund sozialer oder qualifikatorischer Ursachen zu vermeiden. Sie folgt der Erkenntnis, dass die Unterschriftsfähigkeit in einer digitalen Form ein zukünftiges individuelles „Grundbedürfnis“ für die persönliche Existenz in einer von Informationstechnik nachhaltig geprägten Gesellschaft darstellt.

Option B: Multiplikatorenstrategie

Als Alternative kommt ein eher evolutionärer Ansatz zur Verbreitung der eSig in Frage, der dementsprechend erst längerfristig Wirkungen zeigen wird. Hier steht die Nutzung der eSig in einem professionellen Kontext durch Mittler und Unternehmen im Vordergrund, wobei drei Gruppen zu unterscheiden sind. So kann der Einsatz der eSig

I. im Rahmen von Prozessen innerhalb der Verwaltung,

II. bei Geschäftsbeziehungen zwischen der Verwaltung und Mittlern bzw. Unternehmen sowie

III. bei spezifischen Bürgergruppen

erfolgen.

[32] So rechnet etwa der Bayerische Rechnungshof in seinem Jahresbericht 2000 im Bereich des Projekts FISCUS mit einem Einsparpotenzial allein in Bayern mit rd. 100 Mio. DM innerhalb von zehn Jahren (Handelsblatt, 30.1.2001, S. 7).

I. Verbreitung von eSig innerhalb der Verwaltung

Der unmittelbare und mittelbare öffentliche Dienst hat einen Anteil von 12,5 % an den Erwerbspersonen und macht ca. 6 % der Bevölkerung aus. Insgesamt sind in Bundesbehörden 590.000 Personen (inkl. Bundeseisenbahnvermögen), in Landesbehörden ca. 2,3 Mio. und in Kommunen und kommunalen Zweckverbänden ca. 1,6 Mio. Mitarbeiterinnen und Mitarbeiter tätig.

Unmittelbarer öffentlicher Dienst	Jahr 2000
Gebietskörperschaften	4 359 701
Bund	510 219
Länder	2 312 103
Gemeinden/ Gv.	1 537 379
Kommunale Zweckverbände	72 676
Bundeseisenbahnvermögen	78 432
Zusammen	**4 510 809**
Mittelbarer öffentlicher Dienst	
Sozialversicherungsträger unter Aufsicht des Bundes bzw. der Länder	257 106
Bundesanstalt für Arbeit	92 418
Deutsche Bundesbank	16 430
Rechtlich selbständige Anstalten, Körperschaften und Stiftungen	91 129
Zusammen	**457 083**
Insgesamt	***4 967 892***

Tabelle 5-4: Personal der öffentlichen Haushalte[33]

Ziel sollte es sein, die Mitarbeiter mit Signaturkarten für den Dienst auszustatten und gleichzeitig den Mitarbeitern explizit zu erlauben, die Signaturkarte auch privat einzusetzen. Die Nutzung der eSig bei DOMEA und SPHINX ist bereits implementiert bzw. in Planung. Im Rahmen der Ausweitung von DOMEA auf weitere Behörden und Nutzer sollte eine Kompatibilität der Signaturkarten mit diesen Anwendungen sichergestellt werden.

II. Verbreitung der eSig bei Unternehmen und Mittlern

Als Mittler werden hier Berufsgruppen bezeichnet, die als Dienstleister für die Verwaltung tätig werden (z. B. Vermessungsingenieure, Anwälte), oder die zwischen Verwaltung und Bürger stehen (z. B. Kfz-Händler).

Berufsständische Organisationen sollten dazu angehalten werden, bei Auswahl und Implementierung von Signaturkarten die Belange der Fachverfahren zu berücksichtigen, die für die Kommunikation mit der öffentlichen Verwaltung online abgewickelt werden können.

Außerdem sollte dafür gesorgt werden, dass bei der Vergabe von Signaturkarten als elektronische Ausweise Attribute auf Wunsch in separaten Attributzertifikaten gespeichert werden, so dass eine neutrale Anwendung im privaten Bereich möglich ist.

Den Mittlern kommt aus verschiedenen Gründen eine zentrale Bedeutung zu:

[33] Quelle: Statistisches Bundesamt, 2001.

- Als ***Know-how-Träger*** sind sie über fachbezogene Technologien besser informiert als der Durchschnittsbürger.
- Als ***professionelle Nutzer*** ziehen sie große Vorteile aus Internettechnologien. Die Technik hat daher eine erhöhte Akzeptanzwahrscheinlichkeit und Erfolgsaussicht.
- Sie verfügen über die erforderlichen ***finanziellen Ressourcen*** und können als Nutznießer der Technologie von der Verwaltung auch als Finanzierungspartner herangezogen werden.
- Sie tragen durch unterschiedliche Funktionen zu einer Streuung der Technologie bei (***Multiplikatorenfunktion***).

III. Verbreitung der eSig bei spezifischen Bürgergruppen

Es wird vorgeschlagen, im Rahmen der Umstellung von Fachverfahren des Bundes auf Online-Abwicklung regelmäßig zu prüfen, ob relevante Bevölkerungsgruppen mit einer eSig ausgestattet werden, die es ihnen ermöglicht, rechtsgültige Transaktionen vorzunehmen.

Derartige Nutzergruppen sollten sich durch einen vergleichsweise hohen Harmonisierungsgrad sowie durch regelmäßigen Kontakt mit einer staatlichen Organisation in einem prozessoptimierbaren Bereich auszeichnen. In Frage kommen z. B.

- Studierende, z. B. im Zusammenhang mit dem Studentenausweis
- Dauerarbeitslose, z. B. im Zusammenhang mit Weiterbildungsmaßnahmen wie den geplanten Internetführerschein

Bei der Durchführung der Multiplikatorenstrategie ist zu bedenken, dass zahlreiche Benutzergruppen zunächst ausgeschlossen werden. Der Ansatz unterstellt, dass sich durch Nachahmungseffekt und Vorbildfunktion eine Verbreitung elektronischer Signaturen in einem evolutionären Prozess ergeben wird. Die Rolle des Staates reduziert sich dann darauf, die flächendeckende Verbreitung zu beobachten und nur bei ggf. sich einstellenden „weißen Flächen“ durch aktive Handlung ein „digital divide“ zu vermeiden.

5. Die medienbruchfreie Integration elektronischer Signaturen sollte zunächst nur in ausgewählten Fachverfahren angestrebt werden.

Begründung: Im Rahmen des Programms BundOnline2005 sowie seitens einiger Bundesländer sind verschiedene Initiativen gestartet worden, an die mit der eSig angeknüpft werden kann. Im ersten Schritt kann dies durch Einsatz von Messaging geschehen (siehe oben). Die direkte Eingabe in Transaktionssysteme erfordert aufwendige Anpassungen. Diese sollten erst in einem zweiten Schritt durchgeführt werden, wenn Erfahrungen mit der Online-Kommunikation vorliegen.

Innerhalb des ***Bundes*** sind u.E. die folgenden Behörden und Einrichtungen besonders für die Nutzung von eSig-Anwendungen geeignet:

- Bundeswehr. Die höchste Reichweite hat der Bereich des Bundesministeriums der Verteidigung mit über 326.000 Mitarbeitern, das sind 65% des gesamten Personals des Bundes. Als Vorteil stellen sich zentrale Personalführung, zentralisierter Aufbau und ein relativ hoher Standardisierungsgrad bei Abläufen und Strukturen dar. Zudem werden sicherheitsrelevante Informationen ausgetauscht; es bestehen eine häufige Ausweispflicht und wechselnde Verwendungen der Mitarbeiter. Große IT-Vorhaben sind in der Planung (SAP). Ungeachtet einer reduzierten Wehrpflicht besteht ein intensiver Austausch mit dem zivilen Bereich. Auch

zeichnet sich die Bundeswehr durch eine überdurchschnittliche Technikaffinität aus. Verwiesen sei auch auf das Defense Messaging System der USA, wo seit Mitte der 90er Jahre Chipkarten der NSA zur Authentifizierung und Verschlüsselung eingesetzt werden.

- Bundesgrenzschutz: praktisch gleiche Argumentation
- Justiz: ebenfalls hohe Relevanz von rechtsgültiger Kommunikation (vgl. Kapitel 4.3.2)

Als weitere Anwendungsbereiche kommen in Frage:

- ***die elektronische Signatur im Rahmen der eVergabe.*** Bei der elektronischen Vergabe handelt es sich um ein Schlüsselprojekt im eGovernment, für dessen Realisierung eSig zum einen aufgrund des Vergaberechts zwingend benötigt wird, und das zum anderen einen hohen Multiplikatoreffekt auf den Unternehmenssektor besitzt. Gerade im Bereich der eVergabe bieten sich durch eine elektronische Abwicklung erhebliche Einsparpotenziale. Expertenschätzungen gehen von 10% Einsparquote aus, das sind bezogen auf das Beschaffungsvolumen der öffentlichen Hand etwa 50 Mrd. DM.
- ***die elektronische Signatur der Steuererklärung.*** Hohe Öffentlichkeitswirkung, hohe Transaktionszahlen. Umsatzsteuerpflichtige Unternehmen müssen 4 x im Jahr die Umsatzsteuer voranmelden (2,86 Mio. x 4 = 11,44 Mio. Anwendungsfälle), zzgl. der vierteljährlichen Lohnanmeldungen für Arbeitnehmer. Um die eSig der elektronischen Steuererklärung medienbruchfrei zu vollziehen, ist die Anpassung einiger Rechtsvorschriften (z. B. Umstellung auf Stichprobenverfahren bei Belegen) nötig. Hier ist auch zu überlegen, ob das Verfahren nicht einfach auf Messaging mit Signatur und Verschlüsselung umgestellt wird, statt aufwendiger, fehleranfälliger Individualsoftware-Entwicklung, die zudem auf ein einziges Betriebssystem (MS-Windows) abgestellt ist.
- ***Beantragung von BAföG***. Mit Hilfe des Dokumentenmanagement- und Vorgangsbearbeitungssystems FAVORIT werden bereits heute Darlehens*rückzahlungen* an das Bundesverwaltungsamt (BVA) papierlos bearbeitet. Gleichwohl ist die *Beantragung* von BAföG bei den einzelnen Universitäten bzw. Ämter derzeit aufwendig. Durch den Einsatz der elektronischen Signatur wird diese lückenlose und vollständige elektronische Vorgangsbearbeitung auch auf eine sichere Rechtsgrundlage gestellt.

In der Verwaltung der ***Länder*** sind bei der Polizei, Justiz, Finanzen, Kultus und Wissenschaft die meisten Beschäftigten zu finden. Die genannten Bereiche eignen sich ebenfalls für den Einsatz der eSig.

Die bereits beim BAföG genannte Gruppe der Studierenden ist auch auf Landesebene von Interesse. Entscheidende Argumente sind hier vor allem die

- Multiplikatorfunktion von Studierenden
- niedrige Schwelle zur Nutzung von Online-Kommunikation
- Affinität von Studierenden für moderne Technologien, intensiver Dokumentenaustausch mit verschiedensten Verwaltungen sowie
- der überdurchschnittlich häufiger Wohnortwechsel und die damit einhergehenden häufigen Verwaltungskontakte (Änderung des Erstwohnsitzes bzw. eine Anmeldung des Zweitwohnsitzes, Kfz-Ummeldung, Beantragung von Anwohnerparkausweisen).

Die Länder sollten daher in Zusammenarbeit mit dem BVerwAmt die Universitäten dabei unterstützen, eine multiplizierbare Pilotanwendung zu entwickeln.

Bei den ***Kommunen*** erscheint eine Differenzierung nach einzelnen Ressorts nicht sinnvoll, da fast alle Bereich direkte oder indirekte Kontakte mit dem Bürger besitzen und im Rahmen von Workflows in Verwaltungsprozesse eingebunden sind. Statt dessen empfiehlt sich folgende generelle Herangehensweise im operativen Bereiche:

Verwaltungen leisten Wertschöpfung[34]

- durch Produkte ihres Arbeitsprozesses, die in einer bestimmten Qualität und zu bestimmten Kosten hergestellt werden (Fokus: Prozesse),
- durch Synergien in der Bearbeitung spezifischer Problemlagen (Fokus: Kommunikation) sowie
- durch die Förderung von Netzwerkbeziehungen unterschiedlicher, zumeist verwaltungsexterner Akteure (Fokus: Information).

Legt man diese idealtypischen Wertschöpfungsfelder zu Grunde, so finden sich Schwerpunkte der gegenwärtigen eGovernment-Bestrebungen größtenteils in der letztgenannten Gruppe mit dem Informationsfokus. Ein Grund hierfür ist das Vermarktungspotenzial nach außen, ein anderer Grund ist die immer noch unterentwickelte Prozessorientierung des Verwaltungshandelns.

Im Ergebnis beläuft sich die IT-Anbindung schwerpunktmäßig auf den Front-Office-Bereich, während der Back-Office-Bereich und die damit verbundenen Schnittstellenprobleme und Inkonsistenzen ausgeklammert wird.

Aus Sicht von KPMG liegt jedoch gerade im Back-Office-Bereich, also der Prozess-Gruppe das größte wirtschaftliche Potenzial. Um dieses Potenzial zu erschließen, sollte die Standardisierung von Abläufen forciert werden. Der Bund sollte daher eine generelle Prozessorientierung seiner Behörden anstreben und durch Organisationsuntersuchungen erschließen. Es sind die Fachanwendungen zu identifizieren, die die höchste Modernisierungsrendite erwarten lassen.

6. Langfristig sollte ein genereller Einsatz der qualifizierten eSig im öffentlichen Bereich angestrebt werden.

Begründung: Im Rahmen der Fachanwendungen besteht, wie bereits erwähnt, ein durchaus unterschiedliches Niveau an Formanforderungen, d. h. es gibt verschiedene Erfordernisse für die jeweiligen Prozessschritte bei einzelnen Verfahren. Insofern stellt sich die Frage, ob man durchgängig bei allen, oder nur bei ausgewählten Austauschprozessen Signaturen einsetzen sollte.

Für den ausschließlichen Einsatz der eSig bei ausgewählten formal relevanten Prozessen spricht, dass in Zeiten einer Deregulierung und Entbürokratisierung das Anheben des Sicherheitsniveaus mit der Forderung, jegliche Geschäftsprozesse zu signieren, nur schwer begründet werden kann.

Gleichwohl dürfte es für einen Anwender darauf ankommen, die Vorgaben leicht zu verstehen und darauf, ob das Signieren einen Zusatzaufwand erfordert oder nicht. Die Differenzierung verschiedener Signaturniveaus je nach Prozess erscheint aus Gründen der einheitlichen Handhabe problematisch. Es kann kaum erwartet (bzw. zugemutet) werden, dass der Anwender sich bei jeder Aktion das erforderliche Sicherheitsniveau vergegenwärtigt. Auch wird in Zukunft die Mobilität weiter steigen (Telearbeit, flexiblere Arbeitseinsätze), so dass sich bei den Mitarbeitern geringere Routinen und Verhaltenssicherheiten ausbilden dürften als bei einer langjährigen Funktionsverwendung.

[34] Vgl. KGSt.

Daher wird hier dafür plädiert, eine möglichst einheitliche Lösung (Datenfreigeben und immer Signieren) zu wählen. Bei ausgereifter Technik sollte dies durch einen „click" möglich sein und insofern keinen maßgeblichen Mehraufwand darstellen. Diese Lösung wird aber vermutlich erst langfristig zur Verfügung stehen.

5.4 Empfehlungen zur Förderpolitik des Bundes und zu flankierenden Maßnahmen

1. Die horizontale und vertikale Kooperation und Koordination der Verwaltungsebenen sollte durch ein „Competence Center" verbessert werden.

Begründung: Gegenwärtig werden Informationen über eGovernment-Projekte informell oder über klassische Wege, d. h. vor allem über Kongresse, Wettbewerbe oder Bereitstellung von Unterlagen, vermittelt. Daneben bestehen einzelne Gremien, die dem Informationsaustausch dienen, die aber nicht systematisch angelegt sind und in die in der Regel nur ein kleiner Kreis von „Insidern", vorwiegend IT-Experten und/oder Juristen, eingebunden ist.

Auf Basis der Untersuchung lässt sich auf eine generell verbesserungsfähige Transparenz innerhalb der Verwaltung über die bestehende Projektlandschaft, Anbieter und technologische Entwicklungen schließen. Die Bestandsaufnahme, insbesondere die Erfahrungen in den MEDIA@Komm-Projekten zeigen[35], dass Alleingänge einzelner Kommunen noch nicht das notwendige Maß von Know-how überall heben, den notwendigen Investitionsbedarf für alle minimieren und neue Interoperabilitätsfragen aufwerfen können. Korrespondierend mit diesen Ergebnissen zeigen die jüngsten Studienergebnisse in den USA auf, dass nur 28% der IT-Projekte in der amerikanischen Verwaltung und Industrie im Hinblick auf Kosten, Funktionalität und Zeitplanung erfolgreich durchgeführt werden konnten, 23% wurden gestoppt, der Rest suboptimal umgesetzt.[36]

Planungsdefizite sind aus Sicht von KPMG unter anderem Resultat der gegenwärtig praktizierten Art der Informationsvermittlung, die nicht den steigenden Anforderungen einer „Wissensgesellschaft" Rechnung trägt. Zum einen deshalb, weil auf die traditionelle Art und Weise immer nur ein Bruchteil der benötigten Informationen einem ausgewählten Kreis übermittelt wird, zum anderen, weil Informationen nicht zeitnah zur Verfügung stehen. Auch werden gelegentliche Treffen komplexen Themen wie die der elektronischen Signatur nicht gerecht. Überdies fehlt es aufgrund des dominierenden Tagesgeschäfts auch an den vorhandenen „Wissensknoten" an ausreichenden zeitlichen Ressourcen.

KPMG hält eine Koordination der kommunalen Entwicklungs- und Implementierungsaktivitäten der eSig im Rahmen einer durchaus individuellen eGovernment-Strategie für erfolgskritisch.

Vor diesem Hintergrund wird als zentrale Maßnahme die Einrichtung eines „Competence Centers" (CC) im Sinne eines Think-Tanks vorgeschlagen.

Das CC sollte sich aus IuK- und Verwaltungsexperten zusammensetzen. Es sollte nicht weisungsgebunden arbeiten und ein eigenes Budget zur Verfügung haben. Die Arbeit des CC sollte folgende Kernaufgaben umfassen:

---

[35] Hier ist insbesondere die Erkenntnis der unzureichenden Möglichkeit einer Amortisation der Investition innerhalb einer Kommune gemeint.

[36] „The hidden threat to e-Government. Avoiding large government IT failures". OECD Public Management Policy Brief No. 8, March 2001

- Aufbau und Pflege einer internetbasierten Wissensdatenbank über laufende und geplante Projekte sowie über vorhandene IuK-Fachkräfte innerhalb und außerhalb der Verwaltung
- Aufbau des strategischen Controlling (siehe vorherige Empfehlung)
- Organisation eines aktiven Wissenstransfers über den Austausch einzelner IuK-Experten
- Aufbau eines „Springer- und Know-How-Pools" an IuK-Experten zur Unterstützung eines aktiven Risiko- und Qualitätsmanagements
- Beratung der Ministerien bei der Fördermittelvergabe, vor allem für die Förderung von zeitgleichen länder- und kommunenübergreifenden Kooperationsvorhaben
- Organisation von Patenschaften für kleine Kommunen, um einem Auseinanderlaufen der technologischen Entwicklung entgegenzuwirken.

Neben diesen Kernaufgaben kann das CC weitere Unterstützungsleistungen erbringen, wie etwa

- Hilfestellung bei der Entwicklung eines Einführungspfads für eGovernment auf Basis von Wertschöpfungsüberlegungen in Abstimmung mit den kommunalen Spitzenverbänden und anderen Akteuren (z. B. KGSt, KoopA ADV, KBSt, BSI usw.)
- Unterstützung bei der Entwicklung von Referenzmodellen, für die Muster-Softwarelösungen entwickelt und dann multipliziert werden, ähnlich der Aufgabenaufteilung unter den Ländern.
- Mitwirkung bei den vorhandenen Austauschgremien und Foren zwischen den Verwaltungen (z. B. Arbeitskreis „Digitale Signatur" des Deutschen Städtetages) und zwischen Wirtschaft und Verwaltung (z. B. T7 und D-21).

2. Der Bund sollte ein Unterstützungs- und Anreizkonzept zur Förderung kleiner Kommunen und öffentlicher Zugänge (Kioske) entwickeln.

Begründung: Die Steuerreform führt bei den Kommunen nach Selbstauskunft zu Einnahmeverlusten von DM 8,3 Mrd.; Bundesgesetze (z. B. Kindergeld) erhöhen die Kosten bzw. führen zu Steuerausfällen in Höhe von mehreren Mrd. DM bei den Einkommenssteuern (geplante Grundsicherung und die Förderung der Privaten Altersvorsorge) bzw. den Ertragssteuern (steuerliche Absetzungsfähigkeit von der UMTS-Lizenzkosten bei Telekommunikationsunternehmen). Der Städtetag geht für 2001 von einem Defizit der kommunalen Haushalte in Höhe von 5,6 Mrd. DM aus (2.000 Überschuss in Höhe von 2,2 Mrd. DM)[37]. Er schätzt zugleich das Investitionsvolumen für die „digitale Modernisierung" der Kommunen auf DM 12 Mrd. bis 2005. Das Deutsche Institut für Urbanistik (Difu) geht von Aufwendungen in Höhe von DM 23 Mrd. bis 2009 für Hard- und Software aus.

Wie die kleineren Kommunen angesichts der Finanzknappheit die erheblichen Anfangsinvestitionen für eGovernment aufbringen können, bleibt offen; denn Ergebnisse in Form von Reformrenditen stellen sich erst mit erheblichem zeitlichen Verzug ein.

Die Finanzkrise kann jedoch als Chance gesehen werden, innovative Lösungen zu entwickeln. In diesem Sinne sollte der Bund „aktivierend" tätig werden und in Abstimmung mit Ländern und Kommunen ein Unterstützungs- und Anreizkonzept für kleinere Kommunen erarbeiten, das u. a. verschiedene Formen von Zwischenfinanzierung umfassen könnte.

[37] Vgl. Handelsblatt, 23.1.2001.

3. Der Bund sollte für seinen Verantwortungsbereich ein strategisches Controlling für e-Sig/eGovernment entwickeln.

Begründung: Für den nachhaltigen Erfolg der eSig-Initiativen in Deutschland ist es von entscheidender Bedeutung, dass nicht nur auf Ebene einzelner Projekte ein straffes Controlling durchgeführt wird; sondern auch, dass auf einer übergeordneteren Ebene, z. B. der technische Fortschritt im Bereich der Sicherheitsinfrastruktur und die Entwicklungen im Ausland systematisch verfolgt werden. Aus dem Bereich der strategischen Unternehmenssteuerung stehen verschiedene Methoden für ein solches strategisches Controlling zur Verfügung.

Es wird empfohlen, eine systematische Beobachtung der verschiedenen relevanten internationalen, insbesondere der europäischen Aktivitäten aufzubauen bzw. bereits bestehende Ansätze in einem konzeptionellen Rahmen zu integrieren. Hierbei sollten nicht nur die Aktivitäten an sich, sondern insbesondere auch Ziele und Prämissen überprüft werden, die die Grundlage für verschiedene Initiativen bildeten. Im Rahmen der Beobachtung von Umsetzungsfortschritten und -resultaten sollten u.a. die Ergebnisse der Begleitforschung verschiedener Projekte ausgewertet und konsolidiert werden, auch um ggf. beispielhafte Indikatoren für Fortschritte beim eSig-Einsatz zu entwickeln, wie Reichweite (relativer Anteil von Nutzern mit eSig) oder Integrationsgrad (Anzahl der Anwendungen je Arbeitsplatz mit und ohne eSig).

6 Weiteres Vorgehen

In einer mittel- bis langfristigen Perspektive zeichnen sich folgende Aspekte ab:

- Nutzen technischer Fortschritte bei Hardware- und Software-Komponenten
- Verwaltungsstrukturelle Konsequenzen durch die Umsetzung von eGovernment
- Erhöhen von Komfort und Effizienz
- Harmonisierungen auf europäischer Ebene

Langfristig wird es im Rahmen der technischen Weiterentwicklung darum gehen, kontaktlose Chips v.a. in Verbindung mit mobilen Kommunikationskomponenten und biometrische Verfahren zu integrieren. Eine Durchsetzung biometrischer Verfahren wird jedoch nicht vor 2003/4 erwartet.[38] Dabei kann auch die Aggregation von Funktionen vorangetrieben werden.

Die Umsetzung von eGovernment innerhalb der dezentralen Verwaltungsstrukturen in Deutschland birgt eine Reihe von Herausforderungen, die jede für sich Stoff für eine umfangreiche Erörterung bieten.

Genannt werden soll hier insbesondere die Zentralisierungstendenz des IT- Betriebes auf kommunaler Ebene in Verbindung mit speziellen Fragen der einzelnen Verwaltungsebenen, u.a. der Zuständigkeitslockerung. Für eine breitflächige politische Debatte erscheint es hier zu früh. Diese Frage sollten zunächst auf der Praxisebene behandelt werden.

Daneben wird sich zukünftig die Frage einer Verbindung der eSig mit anderen Trägermedien, z. B. auf dem Personalausweis, stellen. Auch werden Überlegungen zur gegenseitigen Anerkennung auf europäischer Ebene vertieft werden, die auch in konkreten Projekten münden werden (wie z. B. die Einführung der eSig auf dem geplanten europäischen Führerschein für LKWs).

Die im vorigen Abschnitt grob skizzierten Ideen zur Durchsetzung der eSig sollten im Rahmen eines „Masterplanes elektronische Signatur“ konkretisiert und inhaltlich, ressourcenbezogen sowie zeitlich detailliert werden. Gegenstand des Masterplanes sollten sein:

- ***ein Fachkonzept:*** In dem Fachkonzept sollte die Umsetzbarkeit der eSig-Integration in der hier vorgeschlagenen Form geprüft und detailliert werden. Daneben sollte eine Durchführbarkeitsstudie zur medienbruchfreien Umstellung der ausgewählten Fachverfahren, inkl. Amortisationsrechnung durchgeführt werden. Dabei können systematisch weitere eSig-taugliche Fachverfahren identifiziert werden.
- ***ein Informations- und Kommunikationskonzept:*** Das Konzept sollte einen Leitfaden
  - zur Akzeptanzförderung bei Entscheidungsträgern
  - zur Erzielung einer Signalwirkung in Wirtschaft und Gesellschaft
  - zum internationalen Standortmarketing

  beinhalten.
- ***Projektmanagement:*** Ein umfassendes Projektmanagement kann maßgeblich dazu beitragen, den Projektfortschritt regelmäßig zu prüfen und mit Informations- und Kommunikationsmaß-

[38] Angaben der Meta Group (a.a.O.). So auch die Planungen des von der EU geförderte Fasme-Forschungsprojekt (Facilitating Administrative Services for Mobile Europeans) zur Entwicklung einer einheitlichen Smart Card.

nahmen abzustimmen. Das heißt, die Projektplanung ist so auszurichten, dass schnell sichtbare, politisch verwertbare Ergebnisse entstehen. Dies sollte in enger Abstimmung/Zusammenarbeit des vorgeschlagenen CC mit den Verantwortlichen im Programm BundOnline2005 durchgeführt werden.

Sowohl die Erstellung als auch die Umsetzung des Masterplanes könnte durch externe Berater begleitet werden, die ggf. im Rahmen der Koordination verschiedener Kontraktpartner eine Generalunternehmerschaft übernehmen könnten.

Hamburg, 8. November 2001

Dr. Manfred J. Pfaff
Partner

Wolfgang Ksoll
Senior Manager

Anlage I

Projektprofile

Vorbemerkung

Nachfolgend werden im Rahmen der Bestandsaufnahme identifizierte Projekte und Vorhaben in Bund, Ländern und Kommunen mit ihren wesentlichen Merkmalen dargestellt. Für Zwecke der Vertiefung sind Internet-links oder Quellenhinweise genannt. Es handelt es sich durchgängig um Vorhaben, in denen die elektronische Signatur eine Relevanz besitzt; d. h. sie besteht entweder als konkreter Projektinhalt oder als umsetzungsnaher Bestandteil von Planungen existiert.

Für die hier genannten Projekte kann angesichts der Vielzahl von Aktivitäten im Bereich eGovernment und ihrer Dynamik keine Gewähr der Vollständigkeit übernommen werden. Durch die Erhebungsmethode ist aber sichergestellt, dass die wichtigen Vorhaben genannt sind.

Bundesebene

DOMEA

1. Eckdaten des Projektes	
Name des Vorhabens	DOMEA
Kommune, Land, Bundesbehörden	Bund
Eckdaten der Verwaltungseinheit (Verwaltungsmitarb., Einwohner, Internetanschlüsse etc.)	k. A.
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	s. u.
Anwendungsbeziehung (G-B, G-G, G-C etc)	G-G
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	k. A.
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	k. A.
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	DOMEA: Pilotsystem für Dokumenten-management und elektronische Archivierung im IT-gestützten Geschäftsgang Stufenweise Nutzung des Systems möglich: ■ Elektronische Registratur ■ Vorgangsbearbeitungssystem ■ „elektronische Akte“ Wie bei der konventionellen Bearbeitung von Akten, gibt es auch bei der elektronischen Bearbeitung die Notwendigkeit der Mitzeichnung bzw. Schlusszeichnung. Die Unterschrift kann dabei durch die digitalen Signatur realisiert werden ***Anzahl der Projekte/Nutzer:*** ■ Es gibt zahlreiche Behörden, in denen das DOMEA-Konzept umgesetzt wird. Dabei handelt es sich aber zum Großteil um Implementierungen in einzelnen Referaten bzw. um nachgeordnete Behörden mit wenigen Nutzern. ■ Untenstehende Tabelle gibt einen Überblick über die Anzahl der Nutzer in ausgewählten Behörden

	Einsatz von elektronischen Signaturen: ■ Kein Einsatz in den zur Zeit bestehenden Projekten. Die Zeichnung von Dokumenten wird statt dessen mit der Eingabe des Benutzernamens und eines persönlichen Passwortes realisiert ■ Allerdings besteht in mehreren Behörden Interesse an der elektronischen Signatur ■ Es werden aber tendenziell zunächst die für 2001 geplanten Gesetzesänderungen abgewartet.
Integration Elektronischer Zahlungsverkehr	k. A.
Verwendete technische Standards, ggf. Chipkartentypus	k. A.
Zugangsmöglichkeiten (welche, wo, wer)	k. A.
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	k. A.
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	k. A.
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	■ Steigerung der Effizienz
Hindernisse im Projekt	■ Teilweise Akzeptanzprobleme bei den Anwendern ■ Schwierigkeiten bei der Anpassung von organisatorischen Abläufen im Rahmen der Einführung von DOMEA

5. Integration in eGovernment Umfeld	
Einbindung in regionale/organisationseigene Plattform mit eCommerce	k. A.
6. Weitere Informationen	-
7. Sonstiges (nur sofern relevant)	**-**

SPHINX

1. Eckdaten des Projektes	
Name des Vorhabens	SPHINX
Beteiligte	■ BSI als Auftraggeber (und Teilnehmer) des Projekts ■ ca. 600 Anwender in über 50 Organisationen aus Bund, Länder, Kommunen und der Privatwirtschaft (siehe Tabelle 1) ■ Hersteller der eingesetzten Software-Produkte: – Giesecke & Devrient – Lotus – Secude – SSE ■ Beratungsunternehmen: – Competence Center Informatik CCI – GMD Forschungszentrum Informationstechnik – Secorvo Security Consulting
Anwendungsbeziehung (G-B, G-G, G-C etc)	G-G, G-B
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	■ Das Pilotprojekt wurde in 3 Phasen von 1998 bis Ende 2000 durchgeführt ■ Kerninhalte je Phase: – Phase 1: Erstellung Gesamtkonzept Aufbau piloteigener PKI – Phase 2: Aufbau und Integration eines Verzeichnisdienstes – Phase 3: Umsetzung MailTrust Version 2 ■ Wirkbetrieb seit Ende 2000
2. Projektgegenstand	Austausch von signierten bzw. verschlüsselten Emails
	Mit dem Pilotprojekt wurden folgende Ziele verfolgt: ■ Test der Interoperabilität von Produkten verschiedener Hersteller ■ Gewinn von Erkenntnissen über die Akzeptanz bei den Anwendern ■ Ermittlung der Aufwände, die mit der Einführung der eingesetzten Produkte in der öffentlichen Verwaltung verbunden sind

	■ Es soll eine Basis zur breiten Einführung von Produkten geschaffen werden, die konvergent zum Signaturgesetz sind Gegenstand/Ziele des Wirkbetriebs: ■ Aufbau einer neuen PKI, deren Wurzelzertifizierungsstelle (Root-PCA) durch das BSI betrieben wird ■ Zertifizierungsstellen, die die Interoperabilitäts- und Sicherheitsrichtlinien der Root-PCA erfüllen, können von der Root-PCA zertifiziert werden und werden dadurch Teil der PKI. Zertifizierungsstellen aus folgenden Bereichen sind zertifiziert bzw. haben die Zertifizierung beantragt: – Bundesverwaltung (IVBB, Bundeswehr) – Landes- und Kommunalverwaltung – private Zertifizierungsstellen (z. B. Telesec und TC Trustcenter) ■ Anstreben eines Sicherheitsniveaus, das den Anforderungen an qualifizierte, elektronische Signaturen nach dem neuen Signaturgesetz entspricht
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse ■ Anzahl der Nutzer (Ist/Plan) ■ Einsatz von elektronischen Signaturen	■ Anzahl der Anwender von digitalen Signaturen in der Phase 3 ca. 600 (siehe Tabelle 2) → Hohe Anwenderzahl war nicht oberstes Ziel, sondern – Einbindung von mehreren Organisationen – Mischung der Organisationen aus öffentlicher Verwaltung (Bund, Länder, Kommunen) und Wirtschaft Elektronische Signatur gem. SigG 97: ■ Im Pilotbetrieb wurde keine der Zertifizierungsstellen bzw. keines der eingesetzten Produkte gem. SigG 97 geprüft ■ Grund: – Erstellung von Produkten gem. SigG97 sehr aufwendig – Evaluierung war aufgrund der geforderten Fortentwicklung der Produkte nicht möglich → Konzentration auf Interoperabilität
Verwendete technische Standards, ggf. Chipkartentypus	■ Grundlage für die Interoperabilität zwischen den eingesetzten Produkten ist die MailTrust-Spezifikation Version 1.1 (Phase 1) bzw. die Version 2 (Phase 3)

	■ Seit der Phase 3 wird S/MIME als Austauschformat für Nachrichten verwendet ■ (kaum Chipkarteneinsatz)
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	Die Phasen 1 und 2 wurde durch das Bundesministerium des Innern finanziert, Phase 3 vom BSI
4. Sonstiges	Es ist geplant, dass sich die Root PCA des BSI an einem Zusammenschluss mehrer Root-PCAs (u.a. von der Dt. Bank und Dt. Telekom) beteiligt, die durch den Mechanismus einer Bridge-CA miteinander verbunden werden sollen
5. Integration in eGovernment Umfeld	k. A.
6. Weitere Informationen	-

Tabelle 1 Teilnehmende Behörden und Organisationen
(Quelle: http://www.bsi.bund.de/aufgaben/projekte/sphinx/)

Auswärtiges Amt

Bayrisches Staatsministerium des Innern,
Bayrisches Landesamt für Statistik und Datenverarbeitung

Bundesamt für Anerkennung ausländischer Flüchtlinge

Bundesamt für Seeschifffahrt und Hydrographie

Bundesamt für Sicherheit in der Informationstechnik

Bundesanstalt für Arbeit

Bundesausfuhramt

Bundesdruckerei

Bundeskanzleramt

Bundeskriminalamt

Bundesministerium der Finanzen

Bundesministerium der Justiz

Bundesministerium der Verteidigung

Bundesministerium des Innern

Bundesministerium für Arbeit und Sozialordnung

Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie

Bundesministerium für Raumordnung, Bauwesen, Städtebau

Bundesministerium für Wirtschaft und Technologie

Bundesministerium für Verkehr

Bundesverwaltungsamt

CCI

Datenverarbeitungszentrum Mecklenburg-Vorpommern

DATEV

DeTeSystem GmbH

Deutscher Bundestag

Deutsche Telekom

Deutsches Zentrum für Luft- und Raumfahrt e.V.

Die Landesbeauftragte für den Datenschutz NRW

Europäische Union

GMD - Forschungszentrum Informationstechnik

Gora, Hecken & Partner

Hessische Zentrale für Datenverarbeitung

HiServ GmbH

Innenministerium des Landes Schleswig-Holstein

Informatikzentrum Niedersachsen, darunter
- Landesbeauftragter für den Datenschutz Niedersachsen
- Nieders. Finanzministerium
- Nieders. Ministerium der Justiz und für Europaangelegenheiten
- Nieders. Ministerium für Wirtschaft, Technologie u. Verkehr

Justizministerium Mecklenburg-Vorpommern
Kraftfahrt Bundesamt
Land Rheinland-Pfalz
Landesbeauftragter für den Datenschutz Mecklenburg-Vorpommern
Netfox AG
Regulierungsbehörde für Telekommunikation und Post
Sächsisches Staatsministerium des Inneren
Secorvo Security Consulting GmbH
Senatskommission für das Personalwesen Bremen
Stadt Nordhorn
Stadt Osnabrück
Stadtwerke München
TEKO Ingenieurbüro GmbH

Tabelle 2 Anzahl der Teilnehmer je Phase

Phase	Zeitraum	Anzahl der Endanwender
1	April 1998 – September 1998	180
2	Oktober 1998 – März 1999	350
3	Dezember 1999 – Dezember 2000	600

eVergabe

1. Eckdaten des Projektes	
Name des Vorhabens	eVergabe
Kommune, Land, Bundesbehörden	■ Bundesbehörden ■ bei erfolgreichen Piloten: Angebot an Länder und Kommunen, das System einzusetzen
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	■ Pilotprojekt im: – Bundesamt für Bauwesen und Raumordnung – Beschaffungsamt des BMI – Bundesamt für Wehrtechnik und Beschaffung BWB
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	■ Zur Zeit nur der Bund ■ In der Implementierung weitere Beteiligte möglich; aber noch keine konkreten Absichten
Anwendungsbeziehung (G-B, G-G, G-C etc)	G-B, G-G
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	■ Abschluss des Feinkonzepts Dezember 2000 bis Januar 2001 ■ Ausschreibung für die Implementierung des Feinkonzepts Anfang 2001 ■ Auftragsvergabe geplant für das Frühjahr 2001 ■ Erster Testbetrieb im Sommer oder Herbst 2001 (eher Herbst) ■ Aufnahme Pilotbetrieb Anfang 2002
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	k. A.
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) – Wird der Workflow komplett abgebildet? – ...	■ Projektgegenstand ist elektronische Vergabe von öffentlichen Aufträgen des Bundes ■ Zur Zeit befindet sich das Projekt in der Phase der Feinkonzeption. Es sind daher noch keine Anwendungen vorhanden ■ Folgende Teilprozesse der Auftragsvergabe sollen abgebildet werden:

■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	– Bekanntmachung der Ausschreibung – Anforderung der Verdingungs-unterlagen durch die Bieter – Angebotsaufforderung – Angebotsabgabe des Bieters / Eingang des Angebots in der Behörde – Sammeln und Öffnen gem. §22 VOL/A – Prüfung und Bewertung der Angebote – Mitteilung an die Bieter – Zuschlag / Vertragsabschluss ■ Es ist kein Medienbruch vorgesehen ***Einsatz von elektronischen Signaturen:*** ■ Anwendung/Signatur muss konform zum SigG sein ■ Jeder Mitarbeiter (ca. 1.000) bekommt eine eigene Chipkarte ■ bis jetzt kein spezielles Trustcenter vorgesehen ***Gesetzliche Rahmenbedingungen*** ■ die für die eVergabe notwendige Änderung der Vergabeordnung wird am 01.02. 2001 in Kraft treten.
Integration Elektronischer Zahlungsverkehr	■ Bezahlfunktion ist bis jetzt noch nicht berücksichtigt
Zugangsmöglichkeiten (welche, wo, wer)	k. A.
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	k. A.
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	■ Identifizierung von relevanten Branchen
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	■ Kosteneinsparungen auf beiden Seiten ■ Steigerung der Effizienz des Verfahrens
Die größten erwarteten Hindernisse im Projekt	■ Akzeptanz bei den Bietern ■ In den Behörden werden keine Hemmnisse erwartet

5. Integration in eGovernment Umfeld	k. A.
6. Weitere Informationen	-
7. Sonstiges (nur sofern relevant)	-

BMWi – Elektronischer Projektträger

1. Eckdaten des Projektes	
Name des Vorhabens	Elektronischer Projektträger (EPT)
Kommune, Land, Bundesbehörden	Bundesministerium für Wirtschaft und Technologie
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	k. A.
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	BMWi, Gutachter, Projektträger, Zuwendungsempfänger
Anwendungsbeziehung (G-B, G-G, G-C etc)	G-B, G-G
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Seit ca. 1997
2. Projektgegenstand	Fortentwicklung des bestehenden Kommunikationsnetzwerks zwischen BMWi-Referat, Projektträger, Gutachtern und Antragsstellern/ Zuwendungsempfänger – EPT – zu einem elektronischen Kommunikations- und Informations-Managementsystem zwischen den Beteiligten mit den Eigenschaften eines Dokumentenmanagement- und Workflowmanagementsystems unter Einsatz der elektronischen Signatur zur Gewährleistung der rechtsverbindlichen und sicheren Information.
Auswahlkriterien für Prozesse, Gewichtung	k. A.
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird (Ist/Plan) ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	Kommunikations- und Transaktionsprozesse
Integration Elektronischer Zahlungsverkehr (wenn relevant)	

Verwendete technische Standards, ggf. Chipkartentypus	SQL-Datenbank Electronic-Formularfrontend XML-Frontend MS-Access-Frontend SSL
Zugangsmöglichkeiten (welche, wo, wer)	k. A.
Signaturgesetzkonformität (ja/nein – Begründung)	Gegenwärtig nein
3. Projektkosten/Investitionen (ggf. geschätzt)	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	Kosten für das elektronische Kommunikations- und Informationsmanagementsystem, für das Dokumentenmanagementsystem und für die elektronische Signatur (Kooperation mit D-Trust GmbH) Bisher für das Projekt: DM 400.000,- Neu: ca. DM 400.000,-
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Rechtliche Rahmenbedingungen müssen fortentwickelt werden Mitarbeiter müssen geschult und überzeugt werden
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	Nutzen für Antragsteller: Antragsteller können sich jeweils unabhängig von der Öffnungszeit der Behörde über Antragsunterlagen/ Verfahren informieren Antragsteller können rechtsverbindlich über das Internet einen Antrag stellen Antragsteller können jederzeit den aktuellen Bearbeitungsstand verfolgen Antragsteller können für die Antragsbearbeitung notwendige Dokumente zeitnah rechtsverbindlich beibringen Nutzen für Zuwendungsempfänger: Zeitlich unabhängige Informationsmöglichkeit Schneller Kontakt zu zuständigem Bearbeiter per eMail

	Eingereichte und vorliegende Dokumente können auf elektronischem Wege eingelesen und eingesehen werden Rechtsverbindliche Kommunikation mittels eSig zu jedem Zeitpunkt des Projekts (Mittelabforderung, Änderungsträge einreichen, gewünschte Dokumente beibringen etc.) Nutzen für Gutachter: u. a.: Rechtsverbindliche Zusendung von Gutachten an den Projektträger Nutzen für das BMWi und andere Projektträger, u. a.: Kosteneinsparungen durch einheitliche Software-Umgebung Doppelförderungen können eher ausgeschlossen werden Schnelle und sichere Kommunikation zwischen zuständigem Referat und Projektträger Kosteneinsparungen durch Prozessvereinfachung und Reduktion Durchlaufzeiten Größere Transparenz des Verwaltungshandelns Entlastungen durch elektronische Plausibilitätsprüfungen
Die größten Hindernisse im Projekt	Hohe Anforderungen an Verfahrenssicherheit Rechtliche Rahmenbedingungen Akzeptanzprobleme hinsichtlich Umgang mit digitaler Signatur und den entsprechenden Softwareprogrammen
5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	k. A.
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	k. A.
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	Eingebunden in die Fördermaßnahme „Förderung von Forschung, Entwicklung und Innovation in kleinen und mittleren

	Unternehmen und externen Industrieforschungseinrichtungen in den neuen Bundesländern“ des BMWi. Eingebunden in Initiative „Moderner Staat – moderne Verwaltung“
6. Weitere Informationen	-
7. Sonstiges (nur sofern relevant)	-

BSI – Digitaler Dienstausweis

1. Eckdaten des Projektes	
Name des Vorhabens	Digitaler Dienstausweis
Kommune, Land, Bundesbehörden	Bundesamt für Sicherheit in der Informationstechnik
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	Ca. 350 Beschäftigte
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Bundesbehörden
Anwendungsbeziehung (G-B, G-G, G-C etc)	G-G
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	z. Zt. Ausschreibungsverfahren, in dem das Generalunternehmen festgelegt werden soll, das einen Piloten durchführt. Nach Pilotphase (100 Beschäftigte BMI) ist Einführung in der Bundesverwaltung geplant. Geplanter Zeitraum des Piloten: 3/2001 – 12/2001
2. Projektgegenstand	Der bisherige Dienstausweis im Bereich der Bundesbehörden soll durch einen Dienstausweis in Form einer multifunktionalen Chipkarte ersetzt werden. Funktionen: Optische Ausweisfunktion, Zutrittskontrolle / Zeiterfassung, Zugangskontrolle zu Rechner und Server, digital signierte Speicherung von Ausweisdaten, digitale Signatur, Verschlüsselung, Authentisierung.
Auswahlkriterien für Prozesse, Gewichtung	k. A.
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird (Ist/Plan) ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	k. A.

Integration Elektronischer Zahlungsverkehr (wenn relevant)	k. A.
Verwendete technische Standards, ggf. Chipkartentypus	TeleTrust-Chipkartenspezifikation (Office Identity Card 1.0) ISIS als Basis für Schnittstelle zu Verzeichnisdiensten/Zeitstempeldiensten eMail auf Basis der vom Sphinx-Projekt festgelegten Standards Chipkarte mit 2 Chips (Zugriffskontrolle, andere Funktionen) Geplante PKI-Infrastruktur innerhalb des IVBB (Informationsverbund Berlin-Bonn) soll für Piloten genutzt werden
Zugangsmöglichkeiten (welche, wo, wer)	k. A.
Signaturgesetzkonformität (ja/nein – Begründung)	Geplant
3. Projektkosten/Investitionen (ggf. geschätzt)	Wegen aktueller Ausschreibung nicht öffentlich
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	k. A.
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	k. A.
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	Eine Chipkarte für mehrere Anwendungen Wegfall von Transportzeiten und Transportwegen und somit auch Transportkosten Verbindliche Kommunikation per eMail durch Absicherung mittels digitaler Signatur (erleichtert elektronische Vorgangsbearbeitung)

	Gesicherter Zugriff auf Daten über Netze als Grundbedingung für Telearbeit Verbesserung von Information und Kommunikation Vorreiterrolle des Bundes bei der Einführung qualifizierter elektronischer Signaturen
Die größten Hindernisse im Projekt	Denkbare Risiken: -Mangelnde Akzeptanz seitens der Benutzer -Festlegung der Standards nicht ausreichend für Interoperabilität -Zu hohe Kosten wegen der hohen Anforderungen an die Qualität des Sichtausweises -Zu hohe Austauschfrequenz der Chipkarte, da u. U. zu viele Funktionen realisiert sind -Mangelnde Verfügbarkeit bei Verlust der Chipkarte
5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	Anbindung an IVBB und Sphinx
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	k. A.
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	Sichere Infrastruktur auf Basis elektronischer Signaturen als Grundlage für Verwaltung der Zukunft (Telearbeit, mobiler Zugriff, elektronische Vergabe, elektronische Abrechnungen etc.)
6. Weitere Informationen	-
7. Sonstiges (nur sofern relevant)	-

Landesebene

Land Niedersachsen – Projekt 53

1. Eckdaten des Projektes	
Name des Vorhabens	Projekt P 53 – Aufbau eines integrierten, automatisierten Haushaltswirtschaftssystems
Kommune, Land, Bundesbehörden	Land Niedersachsen
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	rd. 180.000 Stellen, 46.000 vernetzte PC davon ca. 16.000 PC im Zusammenhang mit P 53 und dig. Signatur
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Niedersächsisches Finanzministerium, Landesbehörden (incl. Hochschulen); TeleSec, secude, Baan, IZN
Anwendungsbeziehung (G-B, G-G, G-C etc.)	G2G
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Konzeptphase und Softwareauswahl je 7 Monate + 3 Monate Kabinett, landesweite Einführung 21 Monate
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	Ziel: Integriertes Haushaltswirtschaftssystem In diesem Kontext: ■ Verkürzung von Arbeitsabläufen, Vermeidung von Doppelarbeit, Ersatz der Papierkassenanordnung durch elektronische Kassenanordnung mit digitaler Signatur ■ Verlagerung von Kassenfunktionen auf mittelbewirtschaftende Dienststellen, dadurch Auflösung der Regierungsbezirkskassen möglich
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird (Ist/Plan) ■ Anzahl der Nutzer (Ist/Plan)	Mittelverteilung, Mittelbewirtschaftung, Buchführung, Zahlungsverkehr, neue Steuerungsinstrumente (KLR, Controlling, Budgetierung) IST 2000: rd. 8,5 Mio. jährl. = 34.000 täglich s.o. Nutzer Ist: 12.000, Nutzer Soll: 16.000

■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	Art: Mitarbeiter der Landesverwaltung
Integration Elektronischer Zahlungsverkehr (wenn relevant)	Ja – Kernmodul
Verwendete technische Standards, ggf. Chipkartentypus	Chipkarten: TeleSec Chip: Siemens Betriebssystem: Tecos Chipkartenleser-Software: Secude
Zugangsmöglichkeiten (welche, wo, wer)	Gegenwärtig 12.000 Nutzer innerhalb der Landesverwaltung
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen (ggf. geschätzt)	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Vernetzung ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	Auf 5 Jahre ca. 280 Mio. LAN, WAN, MAN incl. Baumaßnahmen Zentrale Server, DB-Server, 9.000 neue PC, Drucker, ... Landeslizenz Baan ERP (HKR, KLR, Fibu), PPM , ORACLE-Lizenzen, MS-Office, .. Schulungskosten: ca. 28 Mio. Wartungsvertrag Baan, Oracle Ca. 8.000 Beratertage Konzept : 4 MA Ausschreibung: 5 MA Einführung: 8 – 12 MA (je nach Projektverlauf)
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	■ IuK-Koordinierung, Aufsicht IZN, Projekt und Mittelbereitstellung durch ein Ressort (MF) ■ Zeitdruck (Projekt musste bis 1.1.2000 fertig sein) ■ angemessene Freistellung (des Kernteams) für Wahrnehmung der Projektaufgabe ■ gemeinsames Projektbüro Baan/ Land ■ konstantes Kernteam ■ Zusammenarbeit mit Generalunternehmer

Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit)	Verkürzung von Arbeitsabläufen (Dauer einer Zahlung von 14 Tage auf 2 Tage verkürzt) Haushaltsentlastung durch Personaleinsparung von 349 Stellen („Reformarbeitsmarkt“ - Verzicht auf Neueinstellungen anstelle von Entlassungen)
Die größten Hindernisse im Projekt	■ Registrierung der MA durch TeleSec, da Formulare auf >MA/TeleSec< und nicht auf >Land für seine MA/TeleSec< zugeschnitten sind ■ Umzug und Umstellung des IZN auf Landesbetrieb kurz vor Beginn Echtbetrieb ■ hohe Arbeitsbelastung des Projektteams ■ wechselnde Projektleiter ■ hohe Fallzahlen (Nutzer, Buchungen, Abbildung der Aufbaustruktur des Landes sowie ■ unerwartet hoher Änderungsdienste hinsichtlich Zugriffsrechte
5. Integration in eGovernment-Umfeld	
Einbindung in allgem. Internet-Strategie	Schaffung einer informationellen Grundstruktur
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	Ab Mitte 2001 auf 16.000 Arbeitsplätzen flächendeckend möglich
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	Projekt im Rahmen der Verwaltungsreform Niedersachsen – Prozessverschlankung
6. Weitere Informationen	-
7. Sonstiges	-

Finanzgericht Hamburg – Elektronischer Rechtsverkehr

1. Eckdaten des Projektes	
Name des Vorhabens	Elektronischer Rechtsverkehr (Feldversuch seit 2. August 1999) Ziel: Erprobung, unter welchen Bedingungen Klagen und Anträge per eMail im Finanzgericht eingereicht werden können. Text von Verschlüsselung und digitaler Signatur; Einführung der elektronischen Verfahrensakte.
Kommune, Land, Bundesbehörden	Land
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	46 Beschäftigte
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Finanzgericht HH und in der 1. Aufbaustufe: 25 Steuerberater- und Anwaltsbüros (2. Aufbaustufe: 50) sowie 16 Hamburger Finanzämter (geplant: Hauptzollämter)
Anwendungsbeziehung (G-B, G-G, G-C etc.)	G-B
2. Projektgegenstand	
Verwendete technische Standards, ggf. Chipkartentypus	Outlook, Gerva, GEORG, hd solon, Winword, Proxess
Zugangsmöglichkeiten (welche, wo, wer)	Alle Arbeitsplätze
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen (ggf. geschätzt)	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	Die Kosten des Probeverfahrens wurden durch die Partnerfirmen DATEV und herbert dahm datensysteme übernommen. Software: Gerichtsverwaltungsprogramme hd solon (Richterarbeitsplatz; eVerfahrensakte) u. GEORG (Geschäftsstellenprogramm) wurden erweitert. Verschlüsselungssoftware: GERVA (DATEV)
4. Projektnutzen/Projekterfahrungen	
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit)	Kundenorientierung; Beschleunigung der Verfahrensabläufe; Einführung der elektronischen Verfahrensakte (ständige Verfügbarkeit, übersichtlich

	(ständige Verfügbarkeit, übersichtlich, vielfältige [elektronische] Bearbeitungsmöglichkeiten)
Die größten Hindernisse im Projekt	Schriftstücke lassen sich am Bildschirm nur unter großen Schwierigkeiten erfassen (ideal: elektronisches Papier, ist aber noch nicht marktreif). Die gegenwärtige Rechtsprechung ist noch nicht ausreichend, um das System in Realität zu betreiben.
5. Integration in eGovernment-Umfeld	
Einbindung in allgem. Internet-Strategie	Alle Arbeitsplätze sind mit EDV ausgestattet und untereinander vernetzt.
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	Ausbaufähiges Projekt: eAkte um eingescannte Dokumente erweitern; Einführung eAkte in allen Verfahren; elektronische Archivierung; Einbindung von Spracherkennungssystemen Sämtliche Verfügungsformulare liegen als „Ankreuzformulare“ elektronisch vor; sämtliche Arbeitsgänge sind automatisiert.
6. weitere Informationen	k. A.
7. Sonstiges	Zustimmung von Hamburgischer Datenschutzbeauftragter (http://www.hamburg.datenschutz.de) sowie Richterrat und Personalrat Das Schriftlichkeitsgebot für Klagen und bestimmende Schriftsätze ist bisher nicht endgültig gelöst. Der Gemeinsame Senat der Obersten Gerichtshöfe des Bundes hat in seinem Beschluss v. 5. April 2000 (GmS-OGB 1/98) entschieden, dass bestimmende Schriftsätze formwirksam durch elektronische Übertragung einer Textdatei mit eingescannter Unterschrift des Prozessbevollmächtigten auf ein Faxgerät des Gerichts übermittelt werden können → bei elektronischer Übermittlung des Schriftsatzes ist die persönliche Unterschrift nicht zwingend notwendig.

Elektronisches Grundbuch

Baden-Württemberg – Elektronisches Grundbuch

1. Eckdaten des Projektes	
Name des Vorhabens	Elektronisches Grundbuch
Kommune, Land, Bundesbehörden	Land
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	ca. 2000 Zeichnungsberechtigte in den Grundbuchämtern sollen Zugang bekommen
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Debis Systemhaus GEI (Generalunternehmer), Utimaco Safeware AG
Anwendungsbeziehung (G-B, G-G, G-C etc.)	G-B
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Am 20.04.1998 wurde beschlossen, das elektronische Grundbuch bis Ende 2003 flächendeckend einzuführen. Pilotphase in 8 Notariaten/ Grundbuchämtern vom 14.08.2000 bis 12.2000, Fernabfrage erst ab Anfang 2002 möglich.
2. Projektgegenstand	
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	Abruf von GB-Blättern, die in einem Fenster des WWW-Browsers angezeigt werden Elektronische Datenübernahme in andere Anwendungen Recherche nach Grundbuchblättern Notare, Banken, Bausparkassen
Integration Elektronischer Zahlungsverkehr	nein
Verwendete technische Standards, ggf. Chipkartentypus	FOLIA/EGB 1, SmartCards
Zugangsmöglichkeiten (welche, wo, wer)	Notariatssitze, kommunale Einsichtstellen, per Fernabfrage sofern Zulassung erteilt
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.

3. Projektkosten/Investitionen	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	Einmalige Einrichtungsgebühr beträgt 1000,00 DM monatlich fällt eine Grundgebühr in Höhe von 100,00 DM an
4. Projektnutzen/Projekterfahrungen	
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit)	Grundbuchämter haben jederzeit elektronischen Zugriff schnellere und kostengünstigere Einsichtnahmen andere Behörden können das GB über Fernabfrage nutzen Entlastung der Kommunen Zugriff auf GB für Bürger und Großkunden möglich
5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	k. A.
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	k. A.
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	k. A.
6. weitere Informationen	http://justiz.baden-wuerttemberg.de/Egb-web/html/start.htm
7. Sonstiges	Landesregierung in Schleswig-Holstein setzt dasselbe System für das dortige el.GB ein

Sachsen-Anhalt – Elektronisches Grundbuch

1. Eckdaten des Projektes	
Name des Vorhabens	Elektronisches Grundbuch in Sachsen-Anhalt
Kommune, Land, Bundesbehörden	Ministerium der Justiz
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	23 GB-Ämter sind bereits EDV-geführt
Anwendungsbeziehung (G-B, G-G, G-C etc.)	G-G, G-B
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Einführung des EGB in allen 35 Grundbuchämtern innerhalb von 5 Jahren
2. Projektgegenstand	
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	eSig wird z.Zt. nur für interne Eintragungen genutzt Die Einsicht durch externe Nutzer bedarf keiner eSig Für externe Nutzer wären durch die eSig auch Eintragungen möglich (z.Zt. Zukunftsmusik); technische Tests wurden bisher erfolgreich ausgeführt GB werden 620.000 Mal eingesehen/Jahr Notare, Kreditinstitute/Versicherungen, Katasterbehörden u.a.
Integration Elektronischer Zahlungsverkehr	nein
Verwendete technische Standards, ggf. Chipkartentypus	Solum Star (Verfahren zur Dateneingabe) wurde von Bayern, Hamburg, Sachsen und Sachsen-Anhalt entwickelt. Berlin schloss sich am 05.03.99 als fünftes Land an.
Zugangsmöglichkeiten (welche, wo, wer)	Intern durch Pin, extern durch spezielle Zulassung
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.

3. Projektkosten/Investitionen	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	Finanzierung aus Landeshaushalt Kosten für externe Nutzer: Einmalige Einrichtungsgebühr beträgt 1000,00 DM monatlich fällt eine Grundgebühr in Höhe von 100,00 DM an
4. Projektnutzen/Projekterfahrungen	
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit)	Nutzen liegt auf Seiten der externen Nutzer bzw. wirtschaftlicher Nutzen durch beschleunigte Bauanträge (schwer messbar)
Die größten Hindernisse im Projekt	Kosten für elektronische Erfassung der GB-Daten (Transparenz nur bei vollständiger Erfassung gewährleistet) Gesetzeslage des SigG z.T. mangelnde EDV-Ausstattung kleiner Notare im ländlichen Raum
5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	k. A.
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	k. A.
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	k. A.
6. Weitere Informationen	http://www.mj.sachsen-anhalt.de/min/eff_justiz.html
7. Sonstiges	13 Länder verfügen bisher über ein EGB

Landesamt für Datenverarbeitung und Statistik des Landes Brandenburg – Wahlen im Internet

1. Eckdaten des Projektes	
Name des Vorhabens	Wahlen im Internet – die Alternative für das 21. Jahrhundert
Kommune, Land, Bundesbehörden	Landesamt für Datenverarbeitung und Statistik (Landesbetrieb)
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	551 Bedienstete (Stand: Nov. 2000)
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	BMWi, Forschungsgruppe Internetwahlen, D 21
Anwendungsbeziehung (G-B, G-G, G-C etc)	Primär G-C
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Bis ca. 2006 Bisherige Meilensteine: Sozialwahl TKK 1999 Wahl Studierendenparlament UOS 2/2000 Personalratswahlsimulation LDS BB (6/2000)
2. Projektgegenstand	Demokratische Entscheidungsprozesse über das Internet planen, entwickeln und testen Schaffung einer akkreditierten Zertifizierungsstelle für online-Wahlsoftware Nutzung des Internet zu Wahlen in einem ganzheitlichen Ansatz: Elektronische Wahlmaschinen im Wahllokal, Briefwahl und Internetwahl Pilotierung des Einsatzes elektronischer Signaturen in der Verwaltung zur Sicherstellung von Identität und Authentizität elektronisch übermittelter Daten Aufbau von Ident-points für die Brandenburger Verwaltung zur Versorgung der Beschäftigten mit elektronischen Signaturen langfristig: Erhöhung der Transparenz über Kandidaten und Wahlprogramme
Auswahlkriterien für Prozesse, Gewichtung	k. A.

Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird (Ist/Plan) ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	Wahlprozesse, insbesondere zunächst Personalratswahlen
Integration Elektronischer Zahlungsverkehr (wenn relevant)	langfristig für eGovernment-Anwendungen G-C geplant
Verwendete technische Standards, ggf. Chipkartentypus	Informationelle Gewaltenteilung durch strikte organisatorische und physische Trennung von Wahlamtsserver (Validator), Zertifikator (TC) und digitaler Urne (Psephor) unter permanenter Gewährleistung von Datenschutz und Datensicherheit, Einhaltung des SigG (nach Neufassung des SigG: qualifizierte elektronische Signaturen) Blindingverfahren nach David Chaum 1024 Bit RSA-Verschlüsselung der eSig Releasetransparenz (CD-Version) eSig und Statusabfrage des Zertifikats DNS-Server Firewall für Server und Rechner am Arbeitsplatz Clusterlösung für Firewall USV für alle Servertechnologien und geschütztes Rechenzentrumsumfeld in Anlehnung an die ISO 9001
Zugangsmöglichkeiten (welche, wo, wer)	k. A.
Signaturgesetzmäßigkeit (ja/nein – warum?)	s.o.
3. Projektkosten/Investitionen (ggf. geschätzt)	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware, Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten, Eigener Personalaufwand	Haushaltsmittel wurden durch LDS BB bereitgestellt (für die Haushaltsjahre 200 und 2001 insgesamt 100.000 EURO). Es erfolgte keine gesonderte Bezuschussung durch Dritte.

VBV Baden-Württemberg – Digitale Leistungsabwicklung

1. Eckdaten des Projektes	
Name des Vorhabens	Digitale Bekanntmachung, Ausschreibung und Vergabe von Leistungen nach VOB und VOL
Kommune, Land, Bundesbehörden	Staatliche Vermögens- und Hochbauverwaltung Baden-Württemberg (VBV)
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	2500 Beschäftigte
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	VBV, Bieter aus Handwerk und Wirtschaft
Anwendungsbeziehung (G-B, G-G, G-C etc)	G-B
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird (Ist/Plan) ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	Sendung Bekanntmachung über ein upload-System an den Staatsanzeiger-Verlag. Verteilung der Bekanntmachungstexte an die vom Amt ausgewählten Tageszeitungen und ggf. das Bundesausschreibungsblatt. Spätere Phase: Vorhaltung Vergabeunterlagen in Datenbank ; Bieter kann Unterlagen downloaden und bezahlen. Angebot wird digital signiert und verschlüsselt in Datenbank „zurückgestellt“. Durchführung der Submission im Amt mittels PC.
Integration Elektronischer Zahlungsverkehr (wenn relevant)	Internetbezahlsystem für das Downloaden der Vergabeunterlagen(in späterer Phase)
Verwendete technische Standards, ggf. Chipkartentypus	Vergabedatenbank auf Basis von MS ACCESS Benutzerrechte zur Zeit über Windows NT
Zugangsmöglichkeiten (welche, wo, wer)	

3. Projektkosten/Investitionen (ggf. geschätzt)	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	Keine Kosten für das Land Baden-Württemberg; Finanzierung des Projekts durch Staatsanzeiger.
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Die Bieterbetriebe müssen parallel zum Aufbau des elektronischen Versandweges ihre Arbeitsweise auf elektronische Datenverarbeitung umstellen
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	Amt: -Einsparung Kopiersysteme -Andere Einsatzmöglichkeiten des freigestellten Personals -Senkung der Veröffentlichungskosten -Preisspiegel bei PC-gestützter Submission mit weniger Aufwand sichtbar -Nachrechnungen können automatisiert werden Bieterbetriebe: -durch Internetrecherche ist die Information schneller und mit weniger Aufwand zu beschaffen -Einsicht in Leistungsverzeichnis erspart unnötige Bestellungen von Vergabeunterlagen -Vergabeunterlagen werden günstiger im Bezug -Kalkulation mit einem nach GAEB standardisiertem Leistungsverzeichnis beansprucht weniger Zeit -Abgabe und Änderung von Angeboten ist bis zum Submissionstermin jederzeit möglich
Die größten Hindernisse im Projekt	Technische und organisatorische Probleme in Verbindung mit der elektronischen Signatur Betriebe, die nicht EDV-gestützt arbeiten wollen, können nicht vom Vergabeverfahren ausgeschlossen werden → Nebeneinander von EDV und Papier für eine noch nicht definierte Übergangszeit

5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	Projekt wird auf Grundlage der im Landessystemkonzept vorgegebenen Standards realisiert und ist insofern Bestandteil einer einheitlichen IuK-Infrastruktur des Landes Baden-Württemberg.
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	Anbindung der Dienststellen der VBV an das Landesdatennetz , Nutzung des elektronischen Bürgerinformationsdienstes etc.
6. Links und Literatur	
7. Sonstiges	

Bezirksregierung Münster – Kommunale Kooperation

1. Eckdaten des Projektes	
Name des Vorhabens	Kommunale Kooperation – Internet-Antragstellung für den Bereich des Schwerbehindertengesetzes
Kommune, Land, Bundesbehörden	Bezirksregierung Münster, Abt. 10: Soziales, Arbeit, Landesversorgungsamt
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	Nachgeordnet sind 11 Versorgungsämter: 2526 Beschäftigte
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	In ausgewählten Kommunen (Bochum, Borken, Hagen, Hamm, Lünen, Meschede, Solingen und Duisburg) kann online auf den Datenbestand der elf Versorgungsämter in NRW zurückgegriffen werden. Online-Antragstellung im Bereich des Schwerbehindertengesetzes können bei „vertrauenswürdigen Partnern“ getätigt werden (VdK-Kreisverbände Köln, Rhein-Ruhr und Siegen-Olpe-Wittgenstein)
Anwendungsbeziehung (G-B, G-G, G-C etc)	G-G; G-C
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Unbefristet (flächendeckender Einsatz ab 3. Quartal 2002 geplant) Gegenwärtig Evaluation der Piloterfahrungen sowie Entwurf Datensicherheitskonzept einschließlich datenschutzrechtlicher Prüfung und Genehmigung Feinkonzept für den Einsatz digitaler Signaturen soll Ende 2001 vorliegen
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	k. A.
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird (Ist/Plan)	Antragstellung über Internet Statusabfrage über Internet

■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	
Integration Elektronischer Zahlungsverkehr (wenn relevant)	Erziehungsgeld, soziales Entschädigungsrecht (spätere Phase),
Verwendete technische Standards, ggf. Chipkartentypus	Antragstellung ggf. über html-Formulare, die über eine SSL-Verbindung zu einem Server im Landesbehördennetz übermittel werden → dort neue Verschlüsselung → Bezirksregierung Münster → ggf. an das zuständige Versorgungsamt Statusabfrage ggf. über SAP-Clients → Entwicklung Browser-Lösung KOMKO: ISDN-Wählleitung, PPP-Verbindung mit Authentifizierung via CHAP
Zugangsmöglichkeiten (welche, wo, wer)	k. A.
Signaturgesetzkonformität (ja/nein – Begründung)	geplant
3. Projektkosten/Investitionen (ggf. geschätzt)	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	Pilotinstallationen wurden bisher aus dem laufenden Haushalt finanziert. IT-Budget 2001 = DM 50.000,- Zusätzliche ggf. erforderliche Finanzmittel durch Ministerium für Arbeit und Soziales, Qualifikation und Technologie des Landes NRW sichergestellt.
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	k. A.
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	Wegfall Doppelarbeiten Reduktion Aufwand Poststelle Reduktion Durchlauf- und Transportzeiten Erweiterung Bürgerorientierung (Erleichterung Auskunft und Beratung, Verkürzung der Antragslaufzeiten)

Die größten Hindernisse im Projekt	Fehlende bundesgesetzliche Regelungen im Sozialgesetzbuch (Anerkennung digitaler Signaturen) Datenschutzrechtliche Genehmigung befindet sich in der Abstimmung: Einem direkten Zugriff der Kommunen auf die Daten des Schwerbehindertenverfahrens will die Landesbeauftragte für den Datenschutz unter vertraglich mit den Kommunen festgelegten Bedingungen zustimmen. Das Datensicherheitskonzept der Internetantragstellung ist akzeptiert.
5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	k. A.
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	Internetantragstellung soll auch in anderen Bereichen der Bezirksregierung pilotiert werden
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	Verbesserung der Bürgerfreundlichkeit, Verwaltungsvereinfachung
6. Weitere Informationen	-
7. Sonstiges	-

Bezirksregierung Düsseldorf – Die virtuelle Bezirksregierung

1. Eckdaten des Projektes	
Name des Vorhabens	Die virtuelle Bezirksregierung
Kommune, Land, Bundesbehörden	Bezirksregierung Düsseldorf
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	1.400 Beschäftigte
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Primär andere Behörden und Bürger, die an speziellen Themenstellungen interessiert sind (z. B. Schüler, Eltern, Lehrer beim „Mathe-Treff“)
Anwendungsbeziehung (G-B, G-G, G-C etc)	Primär G-C; G-G
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Fort- und Weiterentwicklung bestehender Verfahren
2. Projektgegenstand	Entwicklung und Einführung eines Content-Management-Systems Weiterentwicklung des redaktionellen Konzepts Weiterentwicklung interaktiver Angebote zur dezentralen Anwendung im Land NRW Organisatorische und technische Entwicklung didaktischer Foren insbesondere von Lern-Treffs (z.B. „Mathe-Treff“) Entwicklung eines Diskussionsforen- und Chatsystems, das bestehende Teillösungen ablösen soll Bereitstellung elektronischer Formulare und einer elektronischen Signatur Herausgabe einer signaturgesetzkonformen SmartCard (Company Card) für die Beschäftigten zur Unterstützung aller eGovernment-Initiativen im Land NRW
Auswahlkriterien für Prozesse, Gewichtung	k. A.
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?)	Zu gleichen Teilen Informations-, Kommunikations- und Transaktionsdienste, an denen unterschiedliche Zielgruppen beteiligt sind.

■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird (Ist/Plan) ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	
Integration Elektronischer Zahlungsverkehr (wenn relevant)	Keine
Verwendete technische Standards, ggf. Chipkartentypus	Content-Management: J2EE-Application-Server, Oracle 8.05 (Datenbank-Backend). Server unterstützt SSL-Verbindungen, Zugriff auf LDAP-Server. Webcast: Bereitstellung Audio- und Videosignale über Encoder via ISDN auf einem Video-Server der Telekom. Von dort Bezug via Internet. EFI: als Java-Applet realisiertes elektronisches Formular mit elektronischer Signatur (Microsoft o. Netscape Browser, Windows 95, 98 oder NT erforderlich). Schlüssellänge 1024 bit für Privat-/Public-Key Paar. Zugriff durch PIN geschützt. Im Internet Tripel-DES. SmartCard: geplant
Zugangsmöglichkeiten (welche, wo, wer)	k. A.
Signaturgesetzkonformität (ja/nein – Begründung)	Keine – signaturgesetzkonforme PKI wird mit Dritten als PPP angestrebt. Im Hinblick auf IT-technische Integration muss eine Anpassung auf die Verwendung von Zertifikaten erfolgen.
3. Projektkosten/Investitionen (ggf. geschätzt)	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	k. A.

4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Verbreitung Internettechnologien Technische Integration der Verfahren
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	Aktueller Produktion von Webangeboten Personaleinsparung in Verwaltungsverfahren (Gründe: weniger Medienbrüche, Verlagerung von Eingaben auf Bürger, Zentralisierung von Spezialfunktionen [z.B. Layout], Auslagerung Formularbereitstellung [z.B. SB-System], Reduktion Bearbeitungsaufwand Daten durch Eingabe in eFormulare) Synergieeffekte durch Übertragung aller organisatorischen und technischen Module auf gleiche oder ähnliche Behörden Verbesserung der Standortqualität des Regierungsbezirks (z. B. „Bioguide“) Transparenz von Entscheidungsabläufen durch Webcast wichtiger Veranstaltungen Verbesserter Informationsstand aller Mitarbeiter Erhöhung Medienkompetenz der Beteiligten
Die größten Hindernisse im Projekt	Bei den Zielgruppen der Bezirksregierung liegt noch keine ausreichende Penetration mit Internettechniken vor. Die Nutzung ist gegenwärtig gering.
5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	Nutzung des Behörden-Intranet im Verbund mit dem Landesintranet
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	Unterstützung der e-Initiative (ehem. „Schulen ans Netz“) Unterstützung des Projekts „Telearbeit bei der Bezirksregierung“
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	Angestrebt: Verknüpfung des Geschäftsprozess-Reengineering mit der Bereitstellung eines Dokumentenmanagement- und Workflow-Systems
6. Weitere Informationen	-
7. Sonstiges (nur sofern relevant)	-

Universitäten

Universität Leipzig – UNICARD

1. Eckdaten des Projektes	
Name des Vorhabens	UNICARD - Leipzig
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Techniker Krankenkasse, Sparkasse Leipzig
Anwendungsbeziehung (G-B, G-G, G-C etc.)	G-G, G-C
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Start eines Pilotprojektes 01.04.1998, Projektstart 01.04.2001
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	Entlastung der Hochschulverwaltung, da akuter Stellenabbau Kosteneinsparungen nach ca. 3 Jahren
Integration Elektronischer Zahlungsverkehr	Sparkasse Leipzig
Verwendete technische Standards, ggf. Chipkartentypus	InterCard
Zugangsmöglichkeiten (welche, wo, wer)	SB-Terminals
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	k. A.
4. Projektnutzen/Projekterfahrungen	k. A.
5. Integration in eGovernment-Umfeld	k. A.
Einbindung in regionale/organisationseigene Plattform mit eCommerce	Nutzung der eSig ist in Zukunft bei Prüfungsanmeldungen sowie Notenmitteilung geplant
6. Weitere Informationen	http://www.uni-leipzig.de/vorles/card/
7. Sonstiges	Chipkarte ist ab 01.04.01 Pflicht für 25.000 Studierende in Leipzig, z.Zt. aber keine Nutzung der elektronischen Signatur. Leipzig war beim MEDIA@Komm-Wettbewerb unter den ersten fünf

Universität Freiburg – UNICARD

1. Eckdaten des Projektes	
Name des Vorhabens	UNICARD - Freiburg
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	5.000 Verwaltungsmitarbeiter, 17.000 Studierende
Anwendungsbeziehung (G-B, G-G, G-C etc.)	G-G, G-C
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Ausgabe von ca. 1000 ChipKarten ist für Januar 2001 geplant
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	Entlastung der Hochschulverwaltung, da akuter Stellenabbau
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	Die Umstellung auf die neue Prüfungsordnung nach dem Credit-Point System, bietet Einsatzmöglichkeiten der eSig, z.B. bei der Klausuranmeldung Sinnvolle Nutzung im Workflow der dezentralen Finanzverwaltung bei der Abwicklung von Zahlvorgängen Studenten, Lehrkräfte und Verwaltungsmitarbeiter
Integration Elektronischer Zahlungsverkehr	EC-Cash
Verwendete technische Standards, ggf. Chipkartentypus	Mayfair
Zugangsmöglichkeiten (welche, wo, wer)	SB-Terminals
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	
4. Projektnutzen/Projekterfahrungen	
Die größten Hindernisse im Projekt	Finanzierung der Chipkarten für alle Beteiligten
5. Integration in eGovernment-Umfeld	

Einbindung in regionale/organisationseigene Plattform mit eCommerce	Nutzung der eSig ist in Zukunft bei Prüfungsanmeldungen sowie Notenmitteilung geplant
6. Weitere Informationen	http://www.verwaltung.uni-freiburg.de/
7. Sonstiges	BW-Card liegt unter Obhut des Innenministeriums (Herr Schäfer) im Projekt „Elektronische Bürgerdienste“

Universität Bremen - Elektronische Dienstleistungen

1. Eckdaten des Projektes	
Name des Vorhabens	Elektronische Dienstleistungen für Studierende (Angebot des Bremer Online Service-Teilprojekt von MEDIA@Komm)
Kommune, Land, Bundesbehörden	Land (Hochschule/Uni Bremen und Bremerhaven)
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Firma HEC, Siemens Business Services, TZI
Anwendungsbeziehung (G-B, G-G, G-C etc.)	G-C
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Nov. 99-April 00: Analyse und Optimierung von Geschäftsprozessen; Auswahl und Priorisierung geeigneter Anwendungsfelder. Mai-Okt. 00: Entwurf der fachlichen Ablauflogik erster Anwendungen; Ausschreibung für die Entwicklung eines DV-technischen Feinkonzepts. Nov. 00-April 01: Entwicklung des DV-technischen Feinkonzepts, Programmierung erster Online-Dienste. SS 01: Beginn der Ausgabe von Signaturkarten an Interessierte und Bereitstellung erster elektronischer Dienstleistungen. ab April 01: Fortlaufende Entwicklung weiterer elektronischer Dienstleistungen
2. Projektgegenstand	Abwicklung von Verwaltungsangelegenheiten wie z.B.: Beantragung von Urlaubssemestern, Mitteilung von Adressänderungen, An- und Abmeldungen zu Prüfungen, Ausdruck von Studienbescheinigungen und Leistungsnachweisen, Nutzung von Bibliotheksdiensten, u.a.
Integration Elektronischer Zahlungsverkehr	siehe Aktivitäten BOS
Zugangsmöglichkeiten (welche, wo, wer)	online im Internet
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	Finanzierung durch MEDIA@Komm
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Verbreitung von Signaturkarten an interessierte Studenten

5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	k. A.
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	k. A.
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	k. A.
6. Weitere Informationen	http://www.signatur.uni-bremen.de/
7. Sonstiges	Zusammenarbeit mit Uni Trier und Uni Bochum

Ruhr-Universität Bochum – Chipkarten

1. Eckdaten des Projektes	
Name des Vorhabens	Chipkarten an der RUB
Kommune, Land, Bundesbehörden	Universität
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	Verbreitung bei ca. 17.000 Studenten, welches ca. 98% entspricht
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Einführung im SS 1997
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	Analyse der Abläufe 1992 von Mummert & Partner
	■ z.Zt. nur Universitäts-intern nutzbar ■ mind. 70.000 Anwendungen pro Jahr ■ kein Einsatz der eSig
Integration Elektronischer Zahlungsverkehr	nein; sieht Zukunft in Bezahlung per Handy
Verwendete technische Standards, ggf. Chipkartentypus	Firma Gemplus Chip GPK 2000
Zugangsmöglichkeiten (welche, wo, wer)	SB-Terminals in der Universität
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	k. A.
4. Projektnutzen/Projekterfahrungen	
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit)	■ Komfort für Studierende erhöhen ■ Verwaltungsprozesse vereinfachen ■ Infrastruktur für „virtuelle Universität“ schaffen
Die größten Hindernisse im Projekt	■ bei vorhandenen Vertrauenskulturen sind schwache und somit kostengünstigere elektronische Signaturen für die Kommunikation zwischen Studenten und Universität ausreichend. Vermehrte Prüfungsanmeldungen bei der Umstellung auf neue Prüfungsordnungen und Abschlusstitel wie MBA lassen die Nutzung von Online-Anmeldungen mittels eSig sinnvoll erscheinen.

	■ flächendeckender Einsatz der eSig ist erschwert auf Grund von Kompatibilitätsproblemen ■ Einsatzmöglichkeiten bei speziellen Benutzergruppen im B2B-Bereich (Notare, Ärzte) ■ Zuerst müssen Verwaltungsabläufe umstrukturiert werden, so dass sinnvolle Einsatzmöglichkeiten der eSig entwickelt werden.
5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	k. A.
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	k. A.
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	k. A.
6. Weitere Informationen	http://www.uv.ruhr-uni-bochum.de/chipcard/
7. Sonstiges	Problematik von Urheberrechten im Internet (Echtheit von online Dokumenten ist oft fraglich) Entwicklung des Internets ist um ein Vielfaches schneller, als die Bewilligungsmechanismen von Förderprojekten

Kommunalebene

MEDIA@Komm Bremen

1. Eckdaten des Projektes	
Name des Vorhabens	MEDIA@Komm Bremen; Plattform für G-B und G-C nach Lebenslagenkonzept
Kommune, Land, Bundesbehörden	Stadtstaat Bremen
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Universität-Bremen, Bremer Straßenbahn AG, Stadtwerke Bremen Enordia, Sparkasse Bremen
Anwendungsbeziehung (G-B, G-G, G-C etc.)	G-C, B-C
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Urkundenbestellung inkl. Zahlungsfunktion realisiert (500 Karten) Bestellung per Email z.Zt. nur möglich, wenn die Urkunde persönlich beim Standesamt abgeholt wird
2. Projektgegenstand	diverse personenbezogene Dokumente als Online-Dienste (Urkundenanforderung, Wohnberechtigungsschein etc.), Adressänderungen
Integration Elektronischer Zahlungsverkehr	Kooperation mit Sparkasse
Verwendete technische Standards, ggf. Chipkartentypus	Sämtliche Softwareprodukte können unentgeltlich als CD-ROM von bremen online services (support@bos-bremen.de) angefordert werden, Datenübermittlung über SSL-Verbindung (verschlüsselt und zertifiziert)
Zugangsmöglichkeiten (welche, wo, wer)	online im Internet
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	Browser: MS Internet Explorer o. Netscape Communicator Kartenleser: PKS-Crypt 2.22 eFormulare: TwisterSign für Windows Infrastruktur: OSCI (Online Services Computer Interface)

4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt	Frage, ob Geschäftsmodell funktioniert, wenn Umstellung der GeldKarte auf EC-Karte von den Banken nicht vorangetrieben wird
Die größten Hindernisse im Projekt	Zeitverzug gegenüber Planung auf Grund von Verzögerungen Leistungen Externer (Abnahme Chipkartenleser durch ZKA) Änderung Konzept durch Streichung von zugesagten Mitteln
5. Integration in eGovernment-Umfeld	
Einbindung in regionale/organisationseigene Plattform mit eCommerce	Auf OSCI-Baisis
6. Weitere Informationen	-
7. Sonstiges (nur sofern relevant)	Das verwendete OBCI-Verfahren der Sparkassen ist neu und soll das HBCI-Verfahren der Banken ersetzen

MEDIA@Komm Esslingen

1. Eckdaten des Projektes	
Name des Vorhabens	Jugendnetz Esslingen (Teilprojekt Bildung im Rahmen von MEDIA@Komm)
Kommune, Land, Bundesbehörden	Kommune
Eckdaten der Verwaltungseinheit (Verwaltungsmitarb., Einwohner, Internetanschlüsse etc.)	Pilotprojekt mit 30 Anwendern
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	IBM Deutschland, Gemplus GmbH, Alcatel SEL AG, Steinbeis-Transferzentrum Mediakomm
Anwendungsbeziehung (G-B, G-G, G-C etc.)	G-C, (B-C)
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	13.10.2000 Jugendnetz geht online
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	Jugendliche sollen als Multiplikator dienen.
	Pilotanwendung des Stadtjugendrings, wo die Angebote online mittels eSig bezogen werden können.
Integration Elektronischer Zahlungsverkehr	nein
Zugangsmöglichkeiten (welche, wo, wer)	Pilotanwendung mit einer Testgruppe von 30 Personen
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	k. A.
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Sensibilisierung der Bevölkerung für neue Medien durch bürgernahe Projekte
Die größten Hindernisse im Projekt	Distribution der Signaturkarten (300 Stück geplant für erste „SKOUT-Anwendungen“ ab 01.2001 Beantragung der Chipkarte ist als große Hürde zu sehen
5. Integration in eGovernment-Umfeld	
Einbindung in regionale/organisationseigene Plattform mit eCommerce	„RegioMarktplatz Esslingen“ und „Sicheres kommunales Unternehmen im Internet-SKOUT“ sind geplant

6. Links und Literatur	http://www.esslingen.de/
7. Sonstiges	Jugendratswahlen sind im Sommer 2001 mit Chipkarten und Zertifikaten von Signtrust geplant „Regiomarktplatz Esslingen“ und „SKOUT“ (virtuelles Rathaus) ist mit folgenden Anwendungen in Planung: Hundesteuer, Anwohnerparkausweis und Fundbüro

MEDIA@Komm Nürnberg

1. Eckdaten des Projektes	
Name des Vorhabens	MEDIA@Komm: Rechtsverbindliche Multimedia-Dienste mit Digitaler Signatur des Städteverbundes Nürnberg
Kommune, Land, Bundesbehörden	Kommunen
Eckdaten der Verwaltungseinheit (Einwohner, Verwaltungsmitarbeiter, Internetanschlüsse etc.)	Nürnberg: 490 000 / 9 500 / 3 000 Erlangen: 100 000 / 2 200 / 1 000 Fürth: 110 000 / 2 400 / 450 Schwabach: 40 000 / 450 / 10 Bayreuth: 75 000 / 480 / 30 Bei den angegebenen Zahlen handelt es sich um ca.-Angaben. Die Zahl der Internetanschlüsse entspricht dem Bestand vor MEDIA@Komm. Die Spannweite der Mitarbeiterzahlen begründet sich in der unterschiedlichen Struktur (Oberzentrum, Kreisfreie Stadt, ...) und der damit verbundenen unterschiedlichen Aufgabenumfänge der Städte
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Curiavant Internet GmbH (vormals Logicard Internet GmbH) für den Städteverbund Nürnberg (Nürnberg, Fürth, Erlangen, Schwabach und Bayreuth) als Projektgesellschaft; die Curiavant Internet GmbH entwickelt und implementiert in den beteiligten Kommunen - und später darüber hinaus - ein System für die rechtsverbindliche Online-Kommunikation zwischen Bürgern, Unternehmen und Verwaltung. Darüber hinaus sind als Banken die Sparkasse Nürnberg, die HypoVereinsBank sowie zur Zeit ca.20 weitere Unternehmen in die Realisierung eingebunden
Anwendungsbeziehung (G-B, G-G, G-C etc)	Grundsätzlich sind aufgrund der multifunktionalen Chipkarte alle Anwendungsbeziehungen möglich. Derzeit konzentriert sich die Curiavant Internet GmbH auf die Entwicklung kommunaler und privatwirtschaftlicher Online-Anwendungen im Auftrag der fünf Städte. G-C, G-B

Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Preisverleihung: März 1999 Umarbeitung in ein förderfähiges Konzept und Zuwendungsbescheid: Oktober 1999 Zeitraum für Implementierung: noch bis 30.09.2002 Es ist eine Plattform für G-B und G-C mit Übertragbarkeit auf alle Verbundstädte (ca.70 bürgerorientierte Online-Lösungen) geplant. Bisher sind bereits Pilotanwendungen mit eingeschränkter Benutzergruppe mit Flip-Chip-Karte im Einsatz. Diese enthält die Digitale Signatur nach deutschem Signaturgesetz (Partner: Deutsche Post Signtrust) und eine Bezahlfunktion (Partner: Sparkasse Nürnberg, Deutscher Sparkassenverband, kontoungebunden).
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	Der Schwerpunkt der Entwicklung liegt bei Anwendungen der Kommunen für Bürger und Unternehmen; darüber hinaus werden Anwendungen anderer Institutionen (z.B. IHK) und kommerzielle Angebote zur Abrundung des Angebotsportfolios eingebunden.
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird (Ist/Plan) ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	In allen Fällen wird ein durchgängiger elektronischer Workflow unter Einbeziehung der vorhandenen Fachverfahren ohne Medienbrüche realisiert. Die Digitale Signatur wird eingebunden um Identifizierung, Authentifizierung und Rechtsverbindlichkeit zu gewährleisten. Nutzer sind bereits heute Bürger, Mittler, Unternehmen und andere Institutionen. Die Anzahl der Nutzer hängt maßgeblich von der Verbreitung der Signaturkarten durch Banken, Versicherungen etc. ab.
Integration Elektronischer Zahlungsverkehr (wenn relevant)	Erfolgt immer dann, wenn ein Geschäftsprozess einen Bezahlvorgang beinhaltet.

Verwendete technische Standards, ggf. Chipkartentypus	Multifunktionale Karte mit Digitaler Signatur nach Signaturgesetz; z.Zt. die sogenannte Curiavant-Flip-Chip-Karte mit Signatur und Geldkarten-Funktion in Zusammenarbeit mit Signtrust und der Sparkasse Nürnberg.
Zugangsmöglichkeiten (welche, wo, wer)	Zunächst über (Home)-PC; später auch über Info-Kioske, Internet-TV, Handy ...
Signaturgesetzkonformität (ja/nein – Begründung)	Signaturgesetz-konform, da für verschiedene kommunale Aufgaben die gesetzliche Erfordernis hierfür besteht und zudem Missbrauchsrisiken ausgeschlossen werden sollen.
3. Projektkosten/Investitionen (ggf. geschätzt)	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	Insgesamt werden im MEDIA@Komm-Projekt Nürnberg im Verlauf von 3 Jahren ca. 45 Mio. DM eingesetzt.
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Gleichzeitige Verfügbarkeit von Infrastruktur, Anwendungen und Signaturkarten. Information und Akzeptanz der Bürger/Nutzer Schaffung von durchgängigen elektronischen Prozessen trotz mehrstufiger Verwaltung.
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	Großer Nutzen letztendlich für alle Bürger / Steuerzahler durch Effizienzsteigerung in der öffentlichen Verwaltung; diese wird zudem Sekundäreffekte in der gesamten Wirtschaft erzeugen.
Die größten Hindernisse im Projekt	Die Vielzahl und Vielschichtigkeit der Einflussgrößen auf Infrastruktur, Anwendungen und Kartenverfügbarkeit.
5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	erfolgt bei allen beteiligten Kommunen
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	erfolgt z.Zt. in enger Abstimmung mit der Maßnahmen zur Einrichtung der regionalen virtuellen Marktplätze Bayern

Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	MEDIA@Komm ist Teil der Verwaltungsreformansätze aller 5 Kommunen.
6. Weitere Informationen	
7. Sonstiges (nur sofern relevant)	

Stadt Hagen – Virtuelles Rathaus

1. Eckdaten des Projektes	
Name des Vorhabens	Das „Virtuelle Rathaus“ Hagen
Kommune, Land, Bundesbehörden	Kommune
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	k. A.
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	FernUniversität GHS Hagen, InteractiveWorld GmbH, HABIT Hagener Betrieb für Informationstechnologie-
Anwendungsbeziehung (G-B, G-G, G-C etc)	G-C
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Seit 15.11.2000 online unter www. Hagen.de
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	k. A.
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	■ Verwaltungsinfos über Dienstleistungen mit Formularen und Direktkontakt per Email ■ Zugriff auf EWO-Daten, Liegenschaftsbuch, Liegenschaftskarte, KfZ-Daten ■ Pilotanwendungen in registrierten Benutzergruppen (z. B. ÖbVI; Notare Autohändler), die nicht SigG-Konform sind.
Integration Elektronischer Zahlungsverkehr	Geldkarte der Sparkassenorganisation und Kreditkarten VISA und Mastercard
Verwendete technische Standards, ggf. Chipkartentypus	Transon – Siemens und Signaturkarte des Deutschen Sparkassenverlages SignCard der Post in Vorbereitung
Zugangsmöglichkeiten (welche, wo, wer)	Internet
Signaturgesetzkonformität	nein

3. Projektkosten/Investitionen	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	k. A.
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Akzeptanz durch Bürgerinnen und Bürger und andere Dienstleistungsnutzer
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	Bürger- und Kundenorientierung, Wirtschaftlichkeit
Die größten Hindernisse im Projekt	Fehlende Massenverbreitung der Signaturkarten und des E-Cash
5. Integration in eGovernment Umfeld	
Einbindung in regionale/organisationseigene Plattform mit eCommerce	Es besteht ein enger Kontakt zu Kollegen in Bremen, so dass eine Orientierung am OSCI-Standard wahrscheinlich ist.
6. Weitere Informationen	http://www.virtuellesrathaus.de/
7. Sonstiges	KOM-ON!- Vereinigung zum gegenseitigen Informationsaustausch

Stadtverwaltung Rathenow – Elektronische Akteneinsicht

1. Eckdaten des Projektes	
Name des Vorhabens	Elektronische Akteneinsicht
Kommune, Land, Bundesbehörden	Stadtverwaltung Rathenow
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	150 Verwaltungsmitarbeiter 26.600 Einwohner 30 Internetarbeitsplätze in der Verwaltung
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	▪ Stadtverwaltung Rathenow ▪ Siemens AG ▪ D2y AG
Anwendungsbeziehung (G-B, G-G, G-C etc)	(G-B, G-G, G-C)
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	10/2000 – 09/2002
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	Akteneinsichts- und Informations-zugangsgesetz (AIG) (siehe Anlage)
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird (Ist/Plan) ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	Siehe Anlage Projekt wurde erst begonnen. Es können noch keine Aussagen zu Transaktionszahlen gemacht werden.
Integration Elektronischer Zahlungsverkehr (wenn relevant)	Noch nicht! Es wird aber gegenwärtig geprüft, ob zukünftig Gebühren für eine umfassende Auskunft erhoben werden müssen.
Verwendete technische Standards, ggf. Chipkartentypus	Noch nicht geklärt.
Zugangsmöglichkeiten (welche, wo, wer)	Alle Bürger, Firmen und Institutionen – über das Internet

3. Projektkosten/Investitionen (ggf. geschätzt)	Ca. 4.150.000 DM
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	 ■ 250.000 DM ■ 2.500.000 DM (Forschung-Entwicklungsarbeit) ■ 150.000 DM ■ 50.000 DM ■ 400.000 DM ■ 800.000 DM
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Zugänglichkeit der Verwaltungsakten über das Internet
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	Der Bürger, Firmen und Institutionen haben die Möglichkeit unabhängig von Tageszeit und Standort Einsicht in Akten zu nehmen
Die größten Hindernisse im Projekt	Verbreitungsgrad der Digitalen Signatur
5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	Das Projekt ist in die allgemeine IT- und Internetstrategie der Stadt Rathenow eingebunden.
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	Einbindung in des Rathenower CityInformationsSystem (CIS-RN)
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	Bürgerbüro
6. Ansprechpartner/Interviewpartner	Dr.Hans-Jürgen Lemle
7. Links und Literatur	www.rathenow.de
8. Sonstiges	-

Stadtverwaltung Rathenow – Elektronische Melderegisterauskunft

1. Eckdaten des Projektes	
Name des Vorhabens	Elektronische Melderegisterauskunft
Kommune, Land, Bundesbehörden	Stadtverwaltung Rathenow
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	150 Verwaltungsmitarbeiter 26.600 Einwohner 30 Internetarbeitsplätze in der Verwaltung
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	4 Pilotpartner ▪ Polizei ▪ Finanzamt ▪ Energieversorger ▪ Ergasversorger Softwareentwicklung – Firma HSH (Soft- und Hardwarevertriebs GmbH) Trust Center – Deutsche Telekom AG
Anwendungsbeziehung (G-B, G-G, G-C etc)	(G-B, G-G, G-C)
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Projektdauer 04/2000 – 03/2002 Pilotversuch ab 03/2001
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	Anzahl der anfallenden Vorgänge pro Tag und die elektronische Realisierbarkeit einer geschlossenen Prozesskette
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird (Ist/Plan) ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	▪ Melderegisterauskunft ▪ 40 – 50 Vorgänge pro Tag ▪ Ist 0 / Plan 20 ▪ Ist 0 / Plan 35 (bis 03/2002) danach werden weitere Nutzer einbezogen ▪ Bis 03/2002 nur Pilotpartner (Polizei, Finanzamt, Energieversorger und Erdgasversorger)

Integration Elektronischer Zahlungsverkehr (wenn relevant)	Ja
Verwendete technische Standards, ggf. Chipkartentypus	Public Key Service (Deutsche Telekom AG)
Zugangsmöglichkeiten (welche, wo, wer)	Über www.rathenow.de Hauptgruppe – Verwaltung ab 03/2001
3. Projektkosten/Investitionen (ggf. geschätzt)	Ca. 395.000 DM
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	 ▪ 100.000 DM ▪ 180.000 DM ▪ 20. 000 DM ▪ 20.000 DM ▪ 25.000 DM ▪ 50.000 DM
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Ständige Verfügbarkeit der Melderegisterauskunft
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	Zeit- und Kostenersparnis für die Nutzer
Die größten Hindernisse im Projekt	Verfügbarkeit der Digitalen Signatur beim Bürger, Verfahren ist sehr kompliziert
5. Integration in eGovernment Umfeld	
Einbindung in allgem. Internet-Strategie	Das Projekt ist in die allgemeine IT- und Internetstrategie der Stadt Rathenow eingebunden.
Einbindung in regionale/organisationseigene Plattform; ggf. mit eCommerce (wenn relevant)	Einbindung in des Rathenower CityInformationsSystem (CIS-RN)
Einbindung in Verwaltungsmodernisierung (NSM); Kontext mit anderen Modernisierungsmaßnahmen	Bürgerbüro
6. Ansprechpartner/Interviewpartner	Dr.Hans-Jürgen Lemle
7. Weitere Informationen	www.rathenow.de
8. Sonstiges	-

Vorhaben im Unternehmenssektor

Industrie- und Handelskammern - IHK 24

1. Eckdaten des Projektes	
Name des Vorhabens	Ursprungszeugnisse Berufsausbildungsverträge IHK 24
Organisation	In den Piloten sind zur Zeit 28 IHKs und 40-50 Unternehmen vertreten: 28 IHKs mit Ursprungszeugnissen, 8 IHKs mit Berufsausbildungsverträgen und 12 IHKs mit IHK 24
Eckdaten der Organisation	82 IHKs, 3,5 Mio. Mitgliedsunternehmen
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	D-Trust (Trust-Center) ComNetMedia (Softwarelösungen im Securitybereich) DeCoda Gesellschaft zur Zertifizierung von elektronischen Dokumenten mbH (richten Registrierungsstellen im Sinne des SigG ein) IHK (Selbstverwaltung der Wirtschaft) Unternehmen SmartTrust (früher iD2) (Signatursoftware) TOWITOKO (Chipkartenleser)
Anwendungsbeziehung (G-B, G-G, G-C etc)	B-G, später G-G (wobei die IHK hier als Verwaltung angesehen wird)
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	1997 wurde mit der Überlegung begonnen Die Java-Version wurde im Oktober 1999 getestet, mit der seitdem gearbeitet wird
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	Prozesse wurden seitens der IHKs gewünscht: Häufig waren zusätzliche Behördengänge seitens der Unternehmer nötig, wenn bestimmte Dokumente/ Nummern etc für die Ausstellung der Ursprungszeugnisse nachgeliefert werden mussten. Schnittstellen zur Standard-Exportsoftware sind gegeben (open sources). Bei der Berufsausbildungsverträgen war die interne Zeitersparnis ein wichtiges Argument – die Daten werden automatisch in verschiedene Systeme (z.B. mit Zahlungserinnerungen etc.) übertragen. Fehler bei der

	erneuten Dateneingabe werden vermieden. Schnittstellen zur Standard-Personalverwaltungssoftware sind gegeben (open sources)
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?)	Berechtigungssysteme sollen künftig eingesetzt werden, die den Unternehmen einen begrenzten Zugriff auf das Intranet der IHKs ermöglichen – gespeicherte Daten über die eigene Firma, spezifische Brancheninformationen. Ferner soll die Chipcard für die Online-Akademie genutzt werden Die Zusammenarbeit mit Kommunen sind vielfältig und werden in Angriff genommen (z.B.: Gewerbeanmeldungen etc.)
■ Transaktionsanzahl und –volumen (ggf. Plan/Ist)	800 000 Ursprungszeugnisse/ Jahr in Bezug auf alle IHKs 300 000 Berufsausbildungsverträge in Bezug auf alle IHKs
■ Anzahl der Nutzer (Ist/Plan)	40-50 Unternehmen von insgesamt 3,5 Mio., für das Jahr 2001 ca. 1.500 User
■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	Unternehmen aus den Bereichen Industrie, Handel und Dienstleistung
Integration Elektronischer Zahlungsverkehr	Langfristig soll der HBCI-Standard unterstützt werden, allerdings ohne eigene Bonität
Verwendete technische Standards, ggf. Chipkartentypus	Chipkarte: Gemplus GPK 8000, in Zukunft IT-Sec-Card (höhere Speicherkapazitäten) Software: ID2 Software Smart Trust Chipkartenleser: TOWITOCO (Dt. Unternehmen), Chipdrive Micro Anwendungen erfolgen über Java
Zugangsmöglichkeiten (welche, wo, wer)	z.Z. häufig Abteilungsleiter in den Unternehmen und zuständige Sachbearbeiter in den IHKs
Signaturgesetzeskonformität	ja (qualifizierte Zertifikate)
3. Projektkosten/Investitionen	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software	Hard- und Software zusammen 49 EUR p.a. auf 3 Jahre (Komplettlösung) keine für Anwender/ 590 DM Schulungskosten für IHK-

■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	Mitarbeiter, die die Registrierung ab 1. Mai 2001 übernehmen, Kosten je RA-Platz (je Lizenz) DM 3.000 (einmalig) + 12,5 % Jahresgebühr für die Wartung 3-4 Personen (ComNetMedia)
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Die Installation der Technik muss einfacher werden – Kompatibilität! Derzeit gibt es Probleme mit der Softwarewartung, die viele Unternehmen outgesourct haben bzw. deren Hauptsitz im Ausland liegt und von dort aus erledigt wird; die Firewall akzeptiert oft nicht die Zertifikate. Im Sachbearbeiterbereich der IHKs fehlt es oft noch an der Motivation, sich mit den Technikern der IHK und des jeweiligen Unternehmens zusammenzusetzen – bei jüngeren Sachbearbeitern gibt es dieses Problem nicht. Probleme gibt es auch mit dem handelsüblichen Lesegeräten, die oft nicht mit den Sicherheits- und Technikanforderungen kompatibel sind.
Nutzen des Projektes	Kosten- und Zeiteinsparungen Fehlervermeidung, dadurch dass die Personalverwaltungssysteme miteinander verbunden sind und bei den Ursprungszeugnissen durch die Java-Anwendung keine falschen Angaben mehr gemacht werden können.
Die größten Hindernisse im Projekt	Kompatibilität der Technik s.o.
5. Integration in eStrategie	
Einbindung in regionale/organisationseigene Plattform mit eCommerce	Mitgliedskarte für IHK-Mitgliedsunternehmen: Es soll das erste Mal zwischen IHK-Mitgliedern und nicht Mitgliedern (z.B. Notare, Rechtsanwälte, Studenten etc.) unterschieden werden. Ziel: Extranet mit großer Serviceorientierung der IHKs (Wissensmanagement, Firmeninformationen etc.) www.ihk24.de
6. Weitere Information	http://www.de-coda.de
7. Sonstiges	D-Trust wird am 1. Mai zertifiziert (zeitgleich mit der Novellierung des SigG); dann werden die ersten Registrierungsstellen bei den IHKs eingerichtet

Bundesnotarkammer – NOTARNETZ

1. Eckdaten des Projektes	
Name des Vorhabens	Notarnetz
Kommune, Land, Bundesbehörden	Körperschaft des öffentlichen Rechts
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	Testphase von 01.-03-2001 mit ca. 30 Notaren, 450 Notare haben schriftl. Interesse bekundet, aber Vertrag noch nicht verbindlich geschlossen
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Bundesnotarkammer, debis Systemhaus CSS, Deutsche Post Signtrust
Anwendungsbeziehung (G-B, G-G, G-C etc)	G-B, B-C
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Seit 1992 ist der elektronische Rechtsverkehr ständiges Thema. Projekt-Start: 07.08.2000
2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	Analyse der Kommunikationsbeziehungen
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anteil der Transaktionen bei denen eSig genutzt wird ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	■ Vielfältige Kommunikationsbeziehungen bei z.B. Grundstückskäufen, elektronische Grundbucheinsichten ■ Notare, Klienten, Grundbuchämter, Register, Behörden
Integration Elektronischer Zahlungsverkehr	nein
Verwendete technische Standards, ggf. Chipkartentypus	Virtual Private Network (VPN)-„Netz im Netz“, eTrust, Chipkarte mit Lesegerät der Signtrust
Zugangsmöglichkeiten (welche, wo, wer)	Online im Internet
Signaturgesetzkonformität	ja

3. Projektkosten/Investitionen	
Kosten für das Projekt/Investitionen nach Beteiligten ■ Hardware ■ Software ■ Schulungen ■ Sonstige IT-Kosten (z.B. Pflege, Wartung) ■ Beraterkosten ■ Eigener Personalaufwand	■ Starterpaket mit Chipkarten, Chipkartenleser und Signier- sowie Verschlüsselungssoftware (ca. 550,-DM) ■ mtl. Grundgebühr (95,00 DM für einen Notar, einen Mitarbeiter und einen PC) ■ Anschubfinanzierung des Projektes durch Notarkammer. ■ annähernd Kostendeckend durch Grundgebühr ■ Profit eher für Debis und Signtrust
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Breite Beteiligung der Notare
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit	Schnellere Vertragsabwicklung durch schnellere Verständigung
Die größten Hindernisse im Projekt	■ geringe Bereitschaft staatlicher Stellen zur Herstellung von Interkonnektivität ■ bisherige Gesetzeslage ■ Kompatibilitätsproblem ■ Schwache Nutzung des Netzes befürchtet, da konservative Branche z.T. Investitionen in Höhe von 600,-DM scheut. Teilweise kein sofortiger Nutzen erkennbar
5. Integration in eGovernment Umfeld	
Einbindung in regionale/organisationseigene Plattform mit eCommerce	Zugriff auf Grundbuchämter und Handelsregister
6. Weitere Informationen	http://www.bnotk.de/, http://www.debis-ac.de/
7. Sonstiges	BNotk als dritte Zertifizierungsstelle nach SigG ab 15.12.2000 genehmigt

Bundesdruckerei – DIGANT

1. Eckdaten des Projektes	
Name des Vorhabens	DIGANT – Digitales Antragsverfahren
Kommune, Land, Bundesbehörden	Bundesdruckerei GmbH
Eckdaten der Verwaltungseinheit (Verwaltungsmitarb., Einwohner, Internetanschlüsse etc.)	ca. 6500 Meldebehörden bundesweit
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Einwohnermeldeämter, Fahrererlaubnisbehörden, Zentrales Fahrererlaubnisregister ZFER des Kraftfahrt-Bundesamtes, u.a.
Anwendungsbeziehung (G-B, G-G, G-C etc.)	G-G, B-G
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Die BD bietet ab dem Jahr 2000 das Modul DIGANT für kommunale Einwohnerverfahren an.
2. Projektgegenstand	
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang, d.h. ■ Informations-, Kommunikations- oder Transaktionsprozesse (Anpassung der Fachverfahren?) ■ Transaktionsanzahl und –volumen (ggf. Plan/Ist) ■ Anzahl der Nutzer (Ist/Plan) ■ Art der Nutzer, z.B. Privatbürger, Mittler (Rechtsanwälte, Kfz-Händler)	Digitales Antragsverfahren für Reisepässe und Personalausweise bzw. für den EU-Kartenführerschein Anwendung z.Zt. noch unbedeutend gering Nutzung z.Zt. nur in wenigen Pilotprojekten Mitarbeiter der öffentlichen Verwaltung
Integration Elektronischer Zahlungsverkehr	Nein
Verwendete technische Standards, ggf. Chipkartentypus	DIGANT-Signaturkarte mit Kartenlesegerät
Zugangsmöglichkeiten (welche, wo, wer)	Ordnungsämter
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	stark abhängig von bereits vorhandener Hard- und Software
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Förderung der Verbreitung der DIGANT-Software

Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit)	spürbare Kosteneinsparung in Städten ab ca. 100.000 Einwohnern Automatische Bestellvorgänge DV-gestützte Überprüfungen der Antragsdaten Kostengünstige Bestellübermittlung Schnelle Bearbeitung, kurze Wartezeiten, mehr Bürgerservice
Die größten Hindernisse im Projekt	Bereitstellungszeiten für Gelder in den Kommunen
5. Integration in eGovernment-Umfeld	
Einbindung in regionale/organisationseigene Plattform mit eCommerce	Zukunftsweisendes System im one-Stop-Gov.: (Bürger-Ordnungsamt-Bundesdruckerei)
6. Weitere Informationen	http://www.bundesdruckerei.com/
7. Sonstiges	Studie über Prozesskosten von Unic Consult, Göttingen erstellt (www.unicconsult.de)

Bundesärztekammer

Bundesärztekammer (BÄK) und Kassenärztliche Bundesvereinigung (KBV) - Health Professional Card – D (Ärzte)

1. Eckdaten des Projektes	
Name des Vorhabens	HPC-D (Ärzte) – Health Professional Card in Deutschland (Ärzte) Es handelt sich um einen elektronischen Arztausweis mit verschiedenen Funktionen (Sichtausweis, elektronischer Sichtausweis/elektronische Basisfunktion des Arztausweises, Digitale Signatur, Authentifizierung, Ver-/Entschlüsselung,). Die HPC-D (Ärzte) ist der Prototyp eines elektronischen Heilberufeausweises für alle Heilberufe in Deutschland.
Organisation	Arbeitsgemeinschaft von Bundesärztekammer (BÄK) und Kassenärztlicher Bundesvereinigung (KBV) unter Beteiligung des Zentralinstituts für die Kassenärztliche Versorgung (ZI).
Eckdaten der Organisation	1. BÄK – vertritt alle 363 396 Ärzte in Deutschland. 2. KBV – vertritt 110 000 Vertragsärzte (in Stückzahl zu Nr. 1 enthalten).
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Ist noch nicht weiter festgelegt. Beabsichtigt sind Kooperationsverträge zwischen der jeweiligen Ärztekammer (ÄK) und der jeweiligen Kassenärztlichen Vereinigung (KV) mit Trustcentern gem. SigG, wobei eine spezifische Sicherheitspolitik und bestimmte Standard-Profile verlangt werden. Die LÄK übernimmt die Rolle einer Registrierungsstelle und einer Attribut-Instanz, die KV die Rolle einer Attribut-Instanz. Weitere Attribut-Zertifikate können z. B. durch Krankenhäuser für ihre angestellten Ärzte ausgegeben werden, wobei in diesem Fall die Attribute die Organisationszugehörigkeit, die Funktion und die Vertretungsmacht beschreiben können. Beispiel 1: Pilot CHIN (Community Health Integrated Network) in Westfalen-Lippe – derzeit am weitesten fortgeschritten: Hier werden die Telekom, 1 Krankenhaus mit

	umliegenden Ärzten und zuständige Organisationen im Umfeld (örtliche Krankenkassenverbände, örtliche Kassenärztliche Vereinigung, Ärztekammer, die beteiligte Industrie) beteiligt sein. Es wird der Einsatz einer einrichtungsübergreifenden elektronischen Befunddokumentation getestet. Beispiel 2: Die Ärztekammer Württemberg testet zusammen mit der Deutsches Gesundheitsnetz GmbH (D/G/N) die organisatorischen Abläufe bei der Ausgabe einer HPC anhand einer derzeit im Intranet des D/G/N als Vorläufer benutzten Chipkarte. Beispiel 3: Die Ärztekammer Nordrhein entwirft derzeit einen Muster-Kooperationsvertrag mit einem Trustcenter.
Anwendungsbeziehung (G-B, G-G, G-C etc)	Zunächst B-B.
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Erste Überlegungen für einen elektronischen Arztausweis erfolgten bereits 1996. Ende 1997 fand ein Gespräch der Einrichtungen des Gesundheitssystems zur Zusammenarbeit bei der Definition einer Sicherheitspolitik, der Definition einer HPC und der Organisation von Zertifizierungsstellen statt. In diesem Gespräch wurde vereinbart, dass zunächst für die Ärzte die Erprobung einer HPC – stellvertretend für alle Heilberufe - erfolgen soll. Die weiteren Arbeiten werden vom Anfang 2000 gegründeten Aktionsforum Telematik im Gesundheitswesen (ATG) koordiniert (http://atg.gvg-koeln.de). Der konkrete Auftrag für die technische Spezifikation erfolgte im März 1998 und wurde durch die Gesellschaft für Mathematik und Datenverarbeitung (GMD) durchgeführt. Seit Juli 1999 liegt die Version 1 (jetzt 1.1) der technischen Spezifikation vor, die offiziell für Pilotprojekte/Feldversuche freigegeben ist. Das erste Pilotprojekt startet voraussichtlich im März 2001.

2. Projektgegenstand	
Auswahlkriterien für Prozesse, Gewichtung	Ziel ist die eindeutige Identifizierung der Kommunikationspartner im Gesundheitswesen, um daraus Rechte abzuleiten zu können, ohne die eine Online-Kommunikation nicht zustande kommen kann (z. B. bei der Übermittlung von elektronischen Arztbriefen, dem Zugriff auf elektronische Patientenakten, der Ausstellung eines elektronischen Rezepts etc.). Die Identifizierung erfolgt anhand der elektronischen Identität: dies sind jeweils asymetrische Schlüsselpaare und zugehörige Zertifikate. Für die Funktionen Digitale Signatur, Authentisierung und Ver- / Entschlüsselung werden separate Schlüsselpaare verwendet. Die (digital signierte) Ausweisdatei ist als Grundfunktion lesbar, ohne das kryptografische Funktionen zum Ansprechen des Ausweises benutzt werden.
Integration Elektronischer Zahlungsverkehr	Nein.
Verwendete technische Standards, ggf. Chipkartentypus	DIN-Normen und ISO-Normen, soweit bereits festgelegt. Hinsichtlich gesundheitssystemspezifischer Normen führt das ZI den Vorsitz in der entsprechenden Arbeitsgruppe des ISO TC 215.
Zugangsmöglichkeiten (welche, wo, wer)	Ärzte und später Ausdehnung auf andere Heilberufe.
Signaturgesetzkonformität	Ja. Zusätzliche Anforderungen an die Trustcenter, die in einer Sicherheitspolitik definiert werden, welche derzeit erarbeitet wird.
3. Projektkosten/Investitionen	
Kosten für das Projekt/Investitionen nach Beteiligten	Derzeit läuft noch vieles über Sponsoren– z.B. Telekom, Hersteller von Lesegeräten und Karten - bzw. durch eigene Leistungen der beteiligten Organisationen. Es gibt noch keine Ausschreibung, nur grobe Kostenschätzungen: Ausweis DM 20,-. Lesegerät höherer Funktionalität DM 200,- (MKT-Spezifikation).

	Jährliche Bereithaltung von Verzeichnisdiensten etc. DM 80,-.
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	Definition einer allgemeinen Sicherheitsinfrastruktur für alle Kommunikationsanwendungen im Gesundheitssystem (ATG) und Realisierung flächendeckender Anwendungen (E-Arztbrief, E-Rezept: ATG). Konsens aller Organisationen des Gesundheitssystems.
Nutzen des Projektes	Bestandteil einer Infrastruktur, die für alle IT-Anwendungen des Gesundheitssystems von Bedeutung ist. Der Nutzen ergibt sich aus dem Nutzen aller Projekte, welche die Infrastruktur benutzen werden. Elektronische Anwendungen im Gesundheitssystem, welche die Infrastruktur nutzen sollen, können zu jährlichen Einsparungen in der Größenordnung von 10 Milliarden DM führen, die zu Qualitätsverbesserungen und Serviceverbesserungen im Gesundheitssystem benutzt werden können, ohne dass die Gesamtkosten des Systems weiter steigen müssen. Die Investitionen können sich nach ca. 3 Jahren amortisieren, während der beschriebene Gesamtnutzen nach Zustandekommen adäquater Anwendungen in einem Zeitraum von ca. 10 Jahren erreichbar erscheint.
Die größten Hindernisse im Projekt	Fehlende Anwendungen. Noch nicht vorhandene Interoperabilität von Public-Key-Infrastrukturen und von vertrauenswürdigen elektronischen Kommunikationsanwendungen. Noch fehlende Standards, z. B. zum Inhalt von Attribut-Zertifikaten oder zum Inhalt elektronischer Adressbücher/Adressen. Noch keine Verständigung des Gesundheitssystems auf eine gemeinsame Sicherheitspolitik. Keine Finanzierung für den flächendeckenden Aufbau einer Publik-Key-Infrastruktur für das Gesundheitswesen, darunter für die Ausgabe einer HPC für alle Heilberufe. Finanzierungsbedarf für die Infrastruktur und für erste flächendeckende Anwendungen: ca. 1 Milliarde DM, aufzubringen durch die Regierung und durch alle Organisationen des Gesundheitssystems anhand eines zu

	definierenden Finanzierungsschlüssels. Konsensbildung erfolgt derzeit im ATG.
5. Integration in eStrategie	
Einbindung in regionale/organisationseigene Plattform mit eCommerce	Der Aufbau einer Infrastruktur – als gesellschaftliche Aufgabe – ermöglicht das Entstehen von eCommerce-Anwendungen, die diese Infrastruktur voraussetzen können. Außerhalb der Zuständigkeit der Körperschaften öffentlichen Rechts müssen Lösungen im freien Wettbewerb angeboten werden. Sie können leicht entstehen, sobald die Infrastruktur aufgebaut ist und allen zur Verfügung steht. Hierdurch entstünde ein nicht abschätzbarer Zusatznutzen in erheblicher Höhe. Der Aufbau einer Infrastruktur als Basis für Wettbewerb und Innovation ist deshalb als gesamtgesellschaftliche Aufgabe zu verstehen.
7. Weitere Informationen	http://www.hcp-protocoll.de und http://atg.gvg-koeln.de
8. Sonstiges	Es gibt bei der Bundesärztekammer und der Kassenärztlichen Bundesvereinigung keinen zentral gesteuerten Test, aber es gilt, zwei Voraussetzungen zu beachten: - die zuständige Ärztekammer muss involviert sein - der Ausweis muss der Spezifikation der Version 1.1 genügen. Es ist zu erwarten, dass im Verlauf der Pilotprojekte (z.B.: CHIN oder Health Care Professionals Protocol (HCPP), siehe Links) weitere Anwendungen diskutiert werden. Spezifiziert ist diesbezüglich nichts, da Anwendungen in der Regel auch von anderen Partnern/ der Industrie realisiert werden müssen; die HPC ist ein Infrastrukturelement. Erst bei einer flächendeckenden Einführung der Infrastruktur werden flächendeckende Anwendungen bezahlbar und sinnvoll. Elektronische Kommunikation wird erst nützlich, wenn möglichst viele Partner erreichbar sind. Entscheidend wird der weitere Fortschritt der Arbeiten des ATG und die Akzeptanz seiner Umsetzungsempfehlungen sein.

Unfallkrankenhaus Berlin

1. Eckdaten des Projektes	
Name des Vorhabens	Einführung der Digitalen Signatur in das UKB
Organisation	Unfallkrankenhaus Berlin
Eckdaten der Verwaltungseinheit (Verwaltungsmitarbeiter, Einwohner, Internetanschlüsse etc.)	1 100 Mitarbeiter, zur Zeit ca. 30-35 Hauptzuweiser (Ärtze) und 1 Unfallbehandlungsstelle
Beteiligte (z.B. Kommune, Banken, Onlineprovider, Softwarehersteller, Trust Center)	Ist noch nicht entschieden. Das UKB beabsichtigt, sämtliche Systeme in die Chipkarte zu integrieren (automatische Zeiterfassung, Berechtigungssystem z.B. für den Zutritt zu OP-Räumen, digitale Signatur). Das Lesegerät soll in der Tastatur der Rechners enthalten sein. Es stellt sich derzeit noch als schwierig heraus, einen solchen Anbieter zu finden.
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	Gedankliche Auseinandersetzung des Projektes seit Gründung des UKB 1997; konkretere Ausgestaltung seit Herbst 1998 In der zweiten Jahreshälfte 2001 soll die digitale Signatur flächendeckend in dem Krankenhaus eingesetzt werden
Anwendungsbeziehung (G-B, G-G, G-C etc.)	B-B
2. Projektgegenstand	
Prozesse, die unterstützt werden nach Anzahl, Qualität, Komplexität und Umfang	jedwede Form der Dokumentation
Verwendete technische Standards, ggf. Chipkartentypus	noch nicht geklärt
Zugangsmöglichkeiten (welche, wo, wer)	alle Mitarbeiter der Krankenhauses und angeschlossenen Ärzte
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	k. A.
4. Projektnutzen/Projekterfahrungen	k. A.
5. Integration in eGovernment-Umfeld	k. A.
6. Weitere Informationen	k. A.
7. Sonstiges	k. A.

Deutscher Sparkassen- und Giroverband e.V.

1. Eckdaten des Projektes	
Name des Vorhabens	Aktivitäten des DSGV bzgl. eSig und EC-Karte
Dauer des Projektes/Sachstand, Zeit für Vorbereitung und Implementierung	SET-Abwicklung wird wenig genutzt (Misstrauen)
2. Projektgegenstand	bisher noch kein Businessplan erstellt Vorteile, da Banken hohes Vertrauen genießen
Integration Elektronischer Zahlungsverkehr	Ziel: Massenanwendungen für EC-Karten
Verwendete technische Standards, ggf. Chipkartentypus	evtl. mCommerce
Signaturgesetzkonformität (ja/nein – Begründung)	k. A.
3. Projektkosten/Investitionen	k. A.
4. Projektnutzen/Projekterfahrungen	
Erfolgsfaktoren für das Projekt nach Einschätzung der Beteiligten	enge Zusammenarbeit der einzelnen Institutionen
Nutzen des Projektes (Einsparungen bei Bürger, Kommune inkl. Opportunitätskosten, Kundenfreundlichkeit)	z.Zt. noch nicht erkennbar
Die größten Hindernisse im Projekt	fehlender Businessplan Identifizierung von Einsatzmöglichkeiten der eSig
5. Integration in eGovernment-Umfeld	
Einbindung in regionale/organisationseigene Plattform mit eCommerce	mCommerce evtl. zukunftsträchtig
6. Weitere Informationen	http://www.dsgv.de
7. Sonstiges	http://www.bdb.de/bdbsearch/01_presse/sub_01_pinfo/05-00/presse_0130.asp http://www.trustcenter.de/

Anlage II Erläuterungen über Trägermedien

Geht man davon aus, dass elektronische Signaturen möglichst weit verbreitet sein sollen, so liegt es auf der Hand, Trägermedien zu verwenden, die alle oder die meisten Bundesbürger besitzen. Hierbei kommen grundsätzlich amtliche und nicht-amtliche Träger in Frage.

Bei den amtlichen Trägern könnte - wie in Finnland - die Signatur mit dem Personalausweis verknüpft werden. Da jeder Krankenversicherte eine Versichertenkarte besitzt, könnte diese eine Signatur tragen; ähnliches gilt für den Sozialversicherungsausweis oder den Führerschein.

Unter den nicht-amtlichen Trägern sind die Überlegungen zur Integration der Signatur in die EC-Karte bereits am weitesten fortgeschritten.

Eine weitere Entwicklung bringt das Patent für die mobile digitale Signatur (*des Software-Herstellers Brokat*) mit sich. Diese ermöglicht eine standort- und infrastrukturunabhängige Signierung via Mobiltelefon. Außerdem kommen auch „stand-alone"-Lösungen in Frage, die auf Uhren, Schmuckstücke, Schlüsselanhänger oder andere persönliche Gegenstände appliziert werden könnten.

Im Einzelnen sind bei den genannten Trägern die folgenden Aspekte zu berücksichtigen

1. Amtliche Trägermedien

1.1 Personalausweis/ Reisepass

Die Zusammenführung von elektronischer Signatur und Personalausweis bzw. Reisepass ist derzeit auf Grund der gesetzlich vorgeschriebenen Inhalte dieser beiden Dokumente nicht möglich. Sowohl inhaltlich als auch abstrakt sind die Muster amtlich festgelegt (Passgesetz § 4 I, II und Personalausweisgesetz § 1 I). Da der Bundesinnenminister die Ausweis-Muster durch Rechtsverordnung (im Falle des Reisepasses im Benehmen mit dem Auswärtigen Amt) bestimmt, die der Zustimmung des Bundesrates bedarf, erscheint dieser Ansatz nicht kurzfristig umsetzbar und von daher zunächst für die rasche Verbreitung der elektronischen Signatur nicht geeignet.

1.2 Krankenversichertenkarte

Die Krankenversichertenkarte ist dem ersten Anschein nach ein geeignetes Trägermedium, um eine breite Masse zu erreichen. Jeder Krankenversicherte (abgesehen von den Mitgliedern der DBK) ist im Besitze einer solchen Karte. Allerdings ist die Einstellung der Krankenversicherungen gegenüber dem Einsatz der elektronischen Signatur auf diesem Medium zurückhaltend. Sie sehen die Notwendigkeit der elektronischen Signatur im Gesundheitswesen im Informationsaustausch zwischen Ärzten und sonstigen Heilberuflern, nicht jedoch bei den Versicherten selbst. Ferner ist auch hier – wie bei dem Personalausweis – eine Gesetzesänderung (SGB V § 291 II bzw. §15 IV) vonnöten, die sich ebenfalls nicht für eine rasche Durchdringung des Marktes eignet.

1.3 Sozialversicherungsausweis

Ähnliche gesetzliche Hindernisse sind auch im Sozialversicherungsausweis zu finden, dessen Inhalt ebenfalls genau geregelt ist (SGB VI § 97 I). Vorteil auch dieses Mediums gegenüber nicht-amtlichen Trägermedien ist, dass der Sozialversicherungsausweis sämtliche Arbeitnehmer in der Bundesrepublik Deutschland erreicht; ausgenommen sind Beamte ohne Nebenjob und

Obdachlose. Abgesehen von einigen spezifischen Berufsgruppen[1] wird der Sozialversicherungsausweis jedoch nicht üblicherweise mit sich geführt.

Bislang liegt der Sozialversicherungsausweis noch in Papierform vor – offensichtlich haben Kostengesichtspunkte dabei eine Rolle gespielt.

Zusammenfassend lässt sich feststellen, dass sich die amtlichen Trägermedien auf Grund ihres Verbreitungsgrades grundsätzlich gut für eine flächendeckende Einführung der elektronischen Signatur eignen würden. Die damit verbundenen gesetzlichen Änderungen stellen jedoch - abgesehen von ungeklärten finanziellen und organisatorischen Fragen - in der zeitnahen Umsetzung ein großes Hindernis dar.

2. Nicht-amtliche Trägermedien

Der Einsatz von EC-Karten als Trägermedium für die eSig wird ausführlich in Abschnitt 4.5.1 erörtert.

2.1 Kommunikationsmedien (Mobilfunk und Internetprovider)

Bedingt durch die rasche Verbreitung der Kommunikationsmedien in den letzten Jahren würde die elektronische Signatur in Kombination mit der Chipcard bzw. bei den Internetprovidern ebenfalls eine breite Masse der Bevölkerung erreichen. Allerdings zeigt dieser Ansatz in der Internet-Branche ein sehr heterogenes Bild. Während einige Unternehmen bereits jetzt die Möglichkeit zum Signieren der eMails geben (z.B. Web.de), sehen sich andere Anbieter (z.B. AOL) derzeit nicht dazu veranlasst, elektronische Signaturen bereitzuhalten. Da Verträge via Internet nur zwischen dem Hersteller und dem Kunden geschlossen werden, ist es ihres Erachtens Aufgabe des Herstellers bzw. des Kunden selbst, sich um eine elektronische Signatur zu bemühen.

2.2 Mobile elektronische Signaturen

Die technische Grundlage von mCommerce-Anwendungen bilden mobile Endgeräte wie Mobiltelefone (Handys), Palmtops oder PDAs (persönliche digitale Assistenten). Die Vorteile des Handys im Vergleich zum PC liegen sozusagen auf der Hand: Jedes Mobiltelefon ist bereits heute mit einer Chipkarte ausgestattet, welche als idealer Aufbewahrungsort für den geheimen Signaturschlüssel gilt. Die zusätzliche Anschaffung eines Kartenlesegerätes entfällt demnach bei der Nutzung von Handys.

Die Marktprognosen für mCommerce-Anwendungen sind vielversprechend. Dieses liegt nicht zuletzt daran, dass es allein in Deutschland ca. 48 Millionen Handy-Besitzer gibt. Das Forschungsinstitut Durlacher Research rechnet in Europa 2003 mit Umsätzen von mehr als 23 Milliarden Euro im mCommerce:

[1] Baugewerbe, Gaststätten- und Beherbergungsgewerbe, Personen- und Güterbeförderungsgewerbe, Schaustellergewerbe, Gebäudereinigungsgewerbe und Unternehmen, die Messen und Ausstellungen auf- und abbauen.

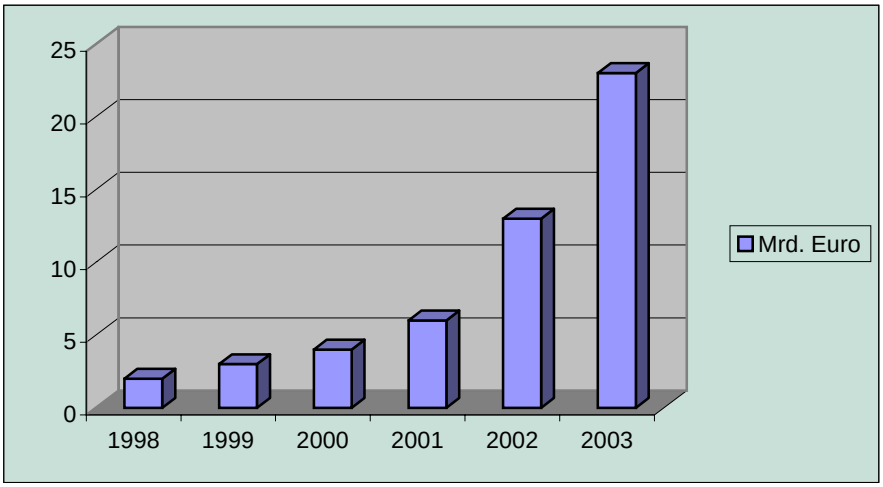


Abbildung 0-1: Marktentwicklung für mCommerce in Europa

Quelle: In Anlehnung an Durlacher Research Ltd (1999)

Zu diesem Zeitpunkt soll es auch schon mehr mobile Nutzer als Festnetznutzer im Internet geben. Den endgültigen Durchbruch soll der mCommerce nach Expertenmeinung erst mit der Einführung von UMTS im Jahre 2003 erreichen, da dieser weltweite Standard als Nachfolger von GSM mit einer bis zu 200fach höheren Datenübertragungsrate aufwarten wird. Nach Ansicht der Gartner Group sollen bis 2004 zwischen 30 und 50 Prozent aller Business-to-Consumer-Transaktionen per Handy erfolgen.

Die Softwarefirma Brokat AG hat beispielsweise im Februar 2001 ein Patent für eine qualifizierte mobile Signatur angemeldet.[2]. Laut Brokart wird das Patent jedoch nicht exklusiv genutzt, sondern in das Mobile Electronic Signature Consortium (msign) eingebracht. Das Konsortium, dem neben Brokat auch Netzbetreiber sowie Hersteller von Handys, Chipkarten und eCommerce-Software angehören, hat bereits ein Protokoll für die elektronische Signatur mit dem Handy vorgestellt und möchte dieses als internationalen Standard etablieren. In der Praxis soll es mehrere Sicherheitsstufen geben. Erst im Endausbau werde das Handy oder die Mobilfunkkarte den geheimen Schlüssel für die elektronische Signatur enthalten. Bis dahin wird eine serverbasierte Signatur angeboten.

Von neuen Technologien wie beispielsweise Bluetooth ist zu erwarten, dass sie schon bald in mobile Endgeräte integriert werden und hierdurch neue Anwendungen generieren, die die zukünftigen Entwicklungen maßgeblich beeinflussen könnten.[3]

2.3 Integration von Zahlungs- und mobilen Funktionen

Den jüngsten Vorstoß in Kombination von Zahlungsmedien und Mobilfunk unternahmen im Januar 2001 die MobilCom AG und die Landesbank Baden-Württemberg. Sie beabsichtigen die Gründung der weltweit ersten Bank für mobile Zahlungs- und Wertpapierdienstleistungen. Noch

---

[2] Patent DE 197 47 03 A 1. Dabei liegt der Schlüssel auf einem Server, etwa beim Betreiber des Mobilfunknetzes, und wird durch Eingabe einer PIN aktiviert. Wie die einzelnen Verfahren nach dem neuen Gesetz zur elektronischen Signatur einzustufen sind, steht derzeit noch nicht fest.

[3] Die Generierung neuer Technologien ist jedoch kein Automatismus. Skeptisch zu Bluetooth äußert sich etwa die Financial Times Deutschland, 28. März 2001: „Funktechnik Bluetooth droht zu scheitern“.

im ersten Halbjahr 2001 soll der Geschäftsbetrieb aufgenommen werden. Mit Hilfe dieser MobilBank sollen mobile Zahlungssysteme (mobile payment) und mobiler Wertpapierhandel (mobile brokerage) ermöglicht werden. Für sichere Transaktionen sollen auch elektronische Signaturen und Tresore angeboten werden. Hier ergeben sich mittel- und langfristig erhebliche Synergiepotenziale.