Universität Koblenz-Landau
Abteilung Koblenz
Fachbereich 4: Informatik
Institut für Wirtschafts- und Verwaltungsinformatik
Arbeitsgruppe Verwaltungsinformatik

Elektronische Signaturen im europäischen eGovernment im Jahr 2020

Eine Szenario-Analyse

Diplomarbeit
im Studiengang Informatik

Christoph Moritz
Walderdorffstraße 15
56566 Neuwied
Matrikelnummer 119920075

23. September 2007

Betreut von
Prof. Dr. M. Wimmer
Melanie Bicking

ÜBERBLICK

INHALTSVERZEICHNIS

ABBILDUNGSVERZEICHNIS

TABELLENVERZEICHNIS

1 Zielsetzung und Vorgehensweise

1.1 Zielsetzung

Ziel der vorliegenden Arbeit ist die Entwicklung von Zukunftsszenarien, anhand derer die Entwicklung der Technik und des Einsatzes elektronischer Signaturen im europäischen eGovernment im Jahr 2020 untersucht werden kann.
Mit Hilfe der Ergebnisse im Vergleich zur aktuellen Situation soll ein Forschungsplan entworfen werden, der vorhandene Lücken schließt und die Weiterentwicklung des Themas auf die zukünftigen Veränderungen unserer Gesellschaft vorbereitet.

Der verstärkte Einsatz elektronischer Kommunikations- und Informationstechnologie führt zu immer mehr tief greifenden Veränderungen. Dieser Beeinflussung können sich auch der Regierungsapparat und die öffentlichen Behörden nicht entziehen. Sowohl die Kommunikation innerhalb der Ämter als auch der Kontakt zum Bürger wird sich verstärkt auf elektronische Medien verlagern [LaUl02]. Sicherheit und Verlässlichkeit müssen jedoch weiterhin gewährleistet werden. Eine Technologie, die diese Vorgaben erfüllen soll, ist die elektronische Signatur.

Aufgrund einer dynamischen, sich rasch wandelnden Umwelt ist es angebracht, Entwicklungstrends bereits im aktuellen Forschungsdesign zu berücksichtigen [Geis00]. Dieses Konzept der Vorausschau gilt sowohl für technologische als auch für gesellschaftliche oder wirtschaftliche Entwicklungen [Schr03]. Diese Arbeit beschäftigt sich daher mit der Beantwortung folgender Fragen:

- Welche Faktoren in Technologie, Gesellschaft oder Wirtschaft beeinflussen die Technik der elektronischen Signatur und ihren

Einsatz, und welche möglichen Entwicklungen sind für den Zeitraum bis zum Jahr 2020 für diese Faktoren zu erwarten?

- Welche Konsequenzen ergeben sich hieraus für die aktuelle Forschung an elektronischen Signaturen, welche Maßnahmen müssen frühzeitig ergriffen, welche Forschungsaspekte intensiviert werden?

Der primäre Schwerpunkt liegt auf der Fragestellung, wie eine Infrastruktur elektronischer Signaturen etabliert und wirtschaftlich genutzt werden kann. Dieser technologische Ansatz kann jedoch nur dann zu den gewünschten Verbesserungen führen, wenn nicht-technologische Einflussfaktoren im Sinne einer ganzheitlichen Betrachtungsweise berücksichtigt werden [Reib91]. Aus diesem Grunde wird in dieser Arbeit zur Entwicklung der Zukunftsszenarien die Methode der Szenario-Analyse gewählt, da diese Prognosemethode die Berücksichtigung sowohl technologischer als auch nicht-technologischer Faktoren erlaubt.

Die erstellten Szenarien sind Denkansätze, die mögliche extreme Entwicklungen darstellen. Die Darstellung dieser möglichen alternativen Entwicklungsverläufe dient der Anregung der am Forschungs- und Entwicklungsprozess beteiligten Personen, sich frühzeitig über die Auswirkungen ihrer Handlungen bewusst zu werden, und mit Hilfe dieses Bewusstseins auf zukünftige Entwicklungen einzuwirken und dabei das technologisch Machbare mit dem gesellschaftlich Erwünschten zu verbinden. Die Bearbeitung dieses Ansatzes in der Arbeit wird im folgenden Unterkapitel dargelegt.

1.2 Vorgehensweise

Die Arbeit ist dreigeteilt in einen Grundlagenteil sowie einen methodischen und einen empirischen Teil, was sich im Gang der Darstellung widerspiegelt.

Kapitel 2 und enthält die erforderlichen technischen und rechtlichen Grundlagen elektronischer Signaturen. Kapitel 3 deckt den methodischen Teil ab, Kapitel 4 umfasst den empirischen Teil, d.h. die Anwendung der Methode auf den Untersuchungsgegenstand. In Kapitel 5 werden sowohl das methodische Vorgehen als auch die inhaltlichen Ergebnisse bewertet und einer kritischen Würdigung unterworfen.

Im ersten Unterkapitel von Kapitel 2 wird der Begriff des eGovernment erläutert.
Im zweiten Unterkapitel werden die Grundlagen elektronischer Signaturen beschrieben. Im ersten Teil wird die Technik der elektronischen Signatur erklärt. Im zweiten Teil wird ausführlich auf die rechtliche Grundlage auf europäischer Ebene, die Signaturrichtlinie, eingegangen, sowie ihre Umsetzung in verschiedenen Mitgliedsstaaten der Europäischen Union dargestellt.

Der methodische Teil – Kapitel 3 – beginnt im ersten Unterkapitel mit einer kurzen Einführung in die Zukunftsforschung und der Definition einiger wichtiger Begriffe. Im zweiten Unterkapitel werden verschiedene Methoden der Zukunftsforschung vorgestellt. Im Anschluss daran wird die Auswahl der Szenario-Analyse als methodische Grundlage für diese Arbeit begründet. Unterkapitel 3 befasst sich mit einer detaillierten Darstellung der Szenario-Analyse und erläutert die Vorgehensweise, die als Grundlage für Kapitel 4 dient.

In Kapitel 4 wird die gewählte Methode auf den Untersuchungsgegenstand angewandt. Im ersten Unterkapitel wird die aktuelle Situation elektronischer Signaturen in ihrer Umwelt vom Expertenteam untersucht Das zweite inhaltliche Unterkapitel beschreibt die Einflussfaktoren der Szenario-Analyse sowie ihre mögliche Entwicklung. Das dritte Unterkapitel umfasst die Trendanalyse, d.h. es werden die verschiedenen alternativen

Entwicklungsmöglichkeiten der ermittelten Einflussfaktoren betrachtet. In Unterkapitel 4 werden über eine Konsistenzmatrix die möglichen Szenarien entwickelt. Daran schließt sich in Unterkapitel 5 die Interpretation der ausgewählten Szenarien an. Unterkapitel 6 beinhaltet die verschiedenen Aktions- und Reaktionsmöglichkeiten, die sich aus der ermittelten Zukunftsentwicklung ergeben, Unterkapitel 7 die möglichen Fehler- und Gefahrenherde. Im Unterkapitel 8 wird schließlich ein Maßnahmenkatalog erstellt, der der Vorbereitung elektronischer Signaturen auf die Zukunft helfen soll.

Kapitel 5 beginnt mit einer kritischen Würdigung der Anwendung der Szenario-Analyse aus methodischer Sicht. Die Arbeit schließt mit der inhaltlichen Bewertung der Ergebnisse im zweiten Unterkapitel.

2 Elektronische Signaturen im europäischen eGovernment

Elektronische Medien gewinnen in unserer schnelllebigen Zeit immer mehr an Bedeutung [Schr03]. Im geschäftlichen Bereich erfolgt ein großer Teil der Kommunikation über das Internet und andere Netzwerke und spart allen Beteiligten viel Zeit und Aufwand, die bei persönlichen Besuchen oder bei Nachrichtenübermittlung via Telefon, per Brief oder über andere Kommunikationsmedien erforderlich wäre. Auch im privaten Bereich nimmt die Nutzung elektronischer Medien immer mehr zu. Neben Kleinartikeln wie Bekleidung oder Literatur werden heute auch teure Objekte wie Fahrzeuge und Häuser im Internet angeboten. Bei solchen Transaktionen spielen Sicherheit und Vertrauen eine wichtige Rolle und erfordern eine objektive Technologie, die dies gewährleistet.

Auch die öffentliche Verwaltung kann sich diesem Trend nicht verschließen. Ein Eindämmen der so genannten ‚Behördengänge', also persönlicher Besuche von Bürgern beim Amt, und eine Verlagerung dieser Prozesse auf elektronische Medien, was Zeit- und Geldersparnis bringt [Bert02], wird angestrebt [Schr03]. Doch in vielen Fällen bedürfen bei Behörden gestellte Anträge der persönlichen Unterschrift des Antragstellers. Eine handschriftliche Unterschrift ist auf elektronischem Weg jedoch nicht möglich. Als Ersatz für eine solche Unterschrift dient die elektronische Signatur: eine Verschlüsselung des übermittelten Dokumentes, die zweifelsfrei die Identifikation des Absenders zulässt und juristischen Beweiswert hat.

Mit der Richtlinie 1999/93/EG [1999/93/EG] hat die Europäische Union im Jahr 1999 eine Vorlage erstellt, die den Mitgliedsstaaten als Grundlage bei der Etablierung elektronischer Signaturen in der elektronischen Verwaltung

(eGovernment) dienen soll, deren Umsetzung in den verschiedenen Staaten aber unterschiedlich gehandhabt wird [Roßn].
In diesem Kapitel werden die Technik der elektronischen Signatur erklärt und die Signaturrichtlinie sowie ihre Umsetzung dargelegt.

Eingangs wird kurz der Begriff eGovernment definiert und erläutert.

Nach der Begriffsdefinition ‚elektronische Signatur' und ihren unterschiedlichen Ausprägungen folgt eine Einführung in ihre technischen Grundlagen.
Zunächst werden die grundlegenden Verfahren der symmetrischen und asymmetrischen Verschlüsselung vorgestellt. Diese Vorstellung wird ergänzt durch eine Erklärung der Hash-Funktion.
Zur Verwaltung der Signaturen bedarf es des Schlüssel- und Zertifikatsmanagements, was das Thema des nächsten Abschnitts bildet und um die ergänzende Technik des Zeitstempels erweitert wird.
Schließlich werden Varianten zur vorgestellten Konstruktion der elektronischen Signatur aufgeführt.

Im dritten Unterkapitel werden anschließend die rechtlichen Grundlagen der elektronischen Signatur dargelegt.
Nach der ausführlichen Vorstellung der Richtlinie 1999/93/EG folgt eine Diskussion der Umsetzung in Deutschland und Österreich sowie einigen weiteren, ausgewählten Mitgliedsstaaten der EU.
Im Anschluss an die Beschreibung des Einsatzes elektronischer Signaturen in der europäischen Union werden abschließend die dabei vorhandenen Probleme aufgezeigt.

2.1 eGovernment

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder Deutschlands, also ein großer Teil der in Deutschland vom eGovernment beeinflussten Institutionen, definiert eGovernment wie folgt:

„Der Begriff eGovernment – zusammengesetzt aus den beiden Wörtern „electronic“ (engl.: elektronisch, rechnergestützt) und „Government“ (engl.: Verwaltung, Regierung) – bezeichnet die Bemühungen der öffentlichen Verwaltung, ihre Aufgaben und die darauf bezogenen Verwaltungsabläufe mittels der modernen Informations- und Kommunikationstechnologie zu erfüllen. […] Auszugehen ist von folgender Grunddefinition: eGovernment bezeichnet die Durchführung von Prozessen der öffentlichen Willensbildung, der Entscheidung, sowie der Leistungserstellung und -abwicklung in Politik, Regierung und Verwaltung unter Nutzung der modernen Informations- und Kommunikationstechnologien, insbesondere das Internet. Einbezogen ist der gesamte öffentliche Sektor. Drei Interaktionsformen sind bestimmend für Aufbau, Struktur und Abwicklung von eGovernment, nämlich Information, Kommunikation und Transaktion. Diesen drei Formen können nahezu alle Aktivitäten im Bereich des eGovernment zugeordnet werden. Nach einem vorsichtigen Anfang im Bereich der Information (z.B. Öffnungszeiten des Hallenbades) ist zurzeit der Schwerpunkt der Aktivitäten noch im Bereich der Kommunikation (z.B. eMail-Kontakt zur Verwaltung) angesiedelt. Als Kernbereich des eGovernment muss jedoch die Transaktion gesehen werden, also die für beide Seiten verbindliche und möglichst vollständige Abwicklung von Verwaltungsaufgaben unter Einschluss der abschließenden Entscheidung und deren Bekanntgabe auf elektronischem Wege.“ [Konf02]

Man erkennt in dieser Definition die große Bandbreite an Vorgängen, die durch den Begriff eGovernment abgedeckt wird; Willensbildungs- und Entscheidungsprozesse sind ebenso Bestandteil des eGovernments wie

Leistungserstellungs- und -abwicklungsprozesse in den unterschiedlichen Bereichen Politik, Regierung und Verwaltung. Die drei Interaktionsformen Information (Bereitstellung derselben), Kommunikation (Informationsaustausch und -abruf) und Transaktion (Durchführung von Dienstleistungen) finden sowohl innerhalb einer Institution und in der Interaktion verschiedener Institutionen untereinander als auch im Kontakt mit dem Bürger als Kunden Anwendung. Motivation zur Einführung des eGovernment sind der verbesserte Service (Abgabe von Anträgen und Anfragen und Erteilung von Genehmigungen zu jeder beliebigen Zeit von jedem beliebigen Ort über das Internet) sowie eine Effizienzsteigerung der Behörden in Form von Arbeitsvereinfachung für die Mitarbeiter, Beschleunigung von Genehmigungsprozessen für die Wirtschaft und Kosteneinsparungen [Schr03].
Der Kernbereich des eGovernment liegt also darin, dass *„die für beide Seiten verbindliche […] Abwicklung“* und die Bekanntgabe der *„abschließenden Entscheidung“* [Konf02] auf elektronischem Wege erfolgen. Man benötigt folglich eine Technik, die diesen Aktionen ihren Bestand vor dem Gesetz garantiert.

Die elektronische Signatur ist unter bestimmten Bedingungen (in Form einer fortgeschrittenen elektronischen Signatur mit qualifiziertem Zertifikat, siehe 2.2.2) der eigenhändigen Unterschrift rechtlich gleichgestellt und ermöglicht daher die rechtsverbindliche Willensbekundung beider beteiligter Seiten einer Interaktion im eGovernment. Die bereits oben zitierte Konferenz der Datenschutzbeauftragten des Bundes und der Länder schreibt dazu: *„Die elektronische Signatur stellt die wichtigste technisch-organisatorische Maßnahme zur Sicherstellung der Authentizität und Integrität für elektronische Daten dar, die im elektronischen Rechts- und Geschäftsverkehr ausgetauscht werden.“* [Konf02]
Zusätzlich dient die elektronische Signatur als wichtige Bedingung für die volle Entfaltung der Effizienz des eGovernment durch die Vermeidung von

Medienbrüchen – durch die Verwendung elektronischer Signaturen erhalten elektronische Dokumente vollständige Rechtsverbindlichkeit und machen Dokumentenversionen auf Papier überflüssig.
Schließlich ist die elektronische Signatur auch ein Instrument der Rückverfolgung und dient somit der Datensicherheit und dem Datenschutz. Mit ihrer Hilfe kann unter Verwendung von Zeitstempeln genau überprüft werden, wer zu welchem Zeitpunkt ein bestimmtes Dokument bearbeitet hat, welche Daten entfernt oder ergänzt wurden und ob der Empfänger davon ausgehen kann, dass ein rechtsgültig signiertes Dokument nach der Signierung nicht mehr verändert wurde.

2.2 Elektronische Signaturen

Elektronische Signaturen sind eine unverzichtbare Technik zur Feststellung und Wahrung der Authentizität digitaler Dokumente. In der Literatur werden die Begriffe ‚digitale Signatur', ‚elektronische Signatur' und ‚elektronische Unterschrift' oftmals synonym verwendet, was jedoch nicht korrekt ist.

Während der Terminus ‚digitale Signatur' eine konkrete technische Lösung bezeichnet, meint der Begriff ‚elektronische Unterschrift' den Ersatz einer eigenhändigen Unterschrift in elektronischer Form, beispielsweise auch schon die Unterschrift auf einem PDA bei Annahme eines Paketes. Eine ‚digitale Signatur' ist also die technische Realisierung einer rechtsgültigen ‚elektronischen Unterschrift' [Preu05].

Der Begriff ‚elektronische Signatur' ist im Gegensatz zu den beiden vorgenannten nicht einheitlich definiert. Basierend auf der ursprünglichen Fassung des deutschen Signaturgesetzes von 1997 schreiben etwa Hoeren und Schüngel: *„Nach der Legaldefinition des §2 I SigG ist eine digitale Signatur im Sinne des SigG ein mit einem privaten Schlüssel erzeugtes*

Siegel zu digitalen Daten, das mit Hilfe eines zugehörigen Schlüssels, […], den Inhaber des Signaturschlüssels und die Unverfälschtheit der Daten erkennen lässt.“ [HoSc99] Dem gegenüber spricht aber das Signaturgesetz [SigG.de] selbst in seiner aktuellen Fassung vom 13. Juli 2005 in §2 von ‚elektronischen Signaturen’ und übernimmt damit die Bezeichnung aus der Richtlinie 1999/93/EG vom 13. Dezember 1999.

Grundsätzlich sollte der Begriff ‚elektronische Signatur’ als verallgemeinernder Oberbegriff für alle Techniken gesehen werden, die das Ziel einer ‚elektronischen Unterschrift’ umsetzen, während die ‚digitale Signatur’ eine konkrete Ausprägung zur Umsetzung dieser Zielvorgabe ist [GlReSt95].

Die Richtlinie 1999/93/EG (‚Signaturrichtlinie’) dient als Ausgangspunkt für alle europäischen Signaturgesetze. Diese Richtlinie verwendet den Begriff ‚fortgeschrittene elektronische Signatur’ für Signaturen, die verschiedenen Anforderungen genügen. Beruht eine solche fortgeschrittene elektronische Signatur zusätzlich auf einem qualifizierten Zertifikat und wurde sie mit einer sicheren Signaturerstellungseinheit erstellt, hat sie die gleiche rechtliche Bedeutung wie eine eigenhändige Unterschrift. Ein solcher Fall wird in Deutschland als ‚qualifizierte elektronische Signatur’, in Österreich als ‚sichere elektronische Signatur’ bezeichnet [SigG.at]. Durch die Bezeichnung als ‚elektronische Signatur’ erfolgt in den Richtlinien und Gesetzen keine Festlegung auf die spezifische Technik [Roßn]. Im Folgenden wird für diesen Typus einer Signatur der deutsche Begriff ‚qualifizierte elektronische Signatur’ verwendet.

Die unterschiedliche Verwendung der Begriffe wird in der Literatur als vertretbar im Rahmen der Verständlichkeit betrachtet. Langenbach und Ulrich schreiben dazu: *„Aus praktischen Erwägungen wird jedoch im Allgemeinen der Ausdruck „elektronische Signatur“ verwendet – um von der Allgemeinverständlichkeit dieser Sprechweise profitieren zu können,*

werden diese gelegentlich auftretenden terminologischen Unschärfen in Kauf genommen.“ [LaUl02]
Konkret bedeutet das für diese Arbeit, dass die Technik der digitalen Signatur als Grundlage dient. Da die rechtlichen Grundlagen sich aber nicht auf diese Technik beschränken, ist die Entwicklung und gesetzmäßige Anwendung neuer Verfahren in der Zukunft möglich.

2.2.1 Technische Grundlagen

Im deutschen Signaturgesetz wird mehrfach der Begriff ‚Schlüssel' erwähnt. §2 Abs. 4f. definiert Signaturschlüssel wie folgt:

Im Sinne dieses Gesetzes sind
[…]
4. "Signaturschlüssel" einmalige elektronische Daten wie private kryptographische Schlüssel, die zur Erstellung einer elektronischen Signatur verwendet werden,
5. "Signaturprüfschlüssel" elektronische Daten wie öffentliche kryptographische Schlüssel, die zur Überprüfung einer elektronischen Signatur verwendet werden,[…] [SigG.de]

Mit privatem und öffentlichem Schlüssel werden also zwei verschiedene Typen von Schlüsseln unterschieden.

2.2.1.1 Symmetrische Verschlüsselung

Die Sicherheit der symmetrischen Verschlüsselung beruht auf einem gemeinsamen Geheimnis von Sender und Empfänger: dem geheimen Schlüssel (engl. *secret key*). Sender und Empfänger müssen sich bereits vor dem Senden der Nachricht auf ein gemeinsames Verschlüsselungsverfahren sowie einen Schlüssel einigen, den kein Dritter erfahren darf. Der Sender

verschlüsselt dann mit seinem Schlüssel die Nachricht und schickt sie an den Empfänger, der sie mit demselben Schlüssel wieder entschlüsselt.
Diese Art der Verschlüsselung gewährleistet Vertraulichkeit, da ein Dritter den abgefangenen Geheimtext ohne Kenntnis des Schlüssels nicht entschlüsseln kann (nach dem Kerckhoff'schen Prinzip gilt das sogar dann, wenn der Angreifer das eingesetzte Verfahren und dessen Spezifikation kennt).

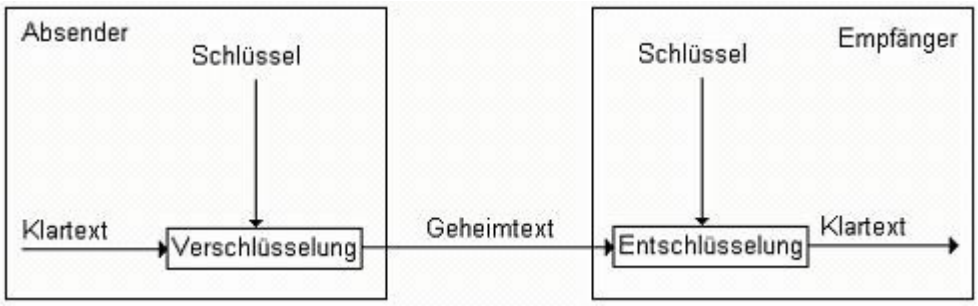

Abbildung 1: Symmetrische Verschlüsselung

Zu den wichtigsten Vertretern symmetrischer Verschlüsselungsverfahren gehören DES (Data Encryption Standard) sowie dessen Varianten und Nachfolger (z.B. Triple-DES, AES (Advanced Encryption Standard)).

Es wird leicht deutlich, wo das Problem der symmetrischen Verschlüsselung liegt: Sender und Empfänger müssen beide denselben geheimen Schlüssel besitzen. Das heißt, dass ein Sender jedes Mal, wenn er mit einer neuen Person geheim kommunizieren will, dieser erst den geheimen Schlüssel zukommen lassen muss, ohne dass ein Dritter ihn abfangen und damit das komplette System gefährden kann.

2.2.1.2 Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung beruht die Sicherheit des Verfahrens im Gegensatz zur symmetrischen Verschlüsselung nicht auf

einem gemeinsamen Geheimnis (dem Schlüssel). Vielmehr ist die asymmetrische Verschlüsselung dadurch charakterisiert, dass beide Kommunikationspartner ein eigenes Schlüsselpaar besitzen, das neben dem geheimen Schlüssel (engl. *private key*) auch einen öffentlichen Schlüssel (engl. *public key*) umfasst.
Während der geheime Schlüssel weiterhin geheim gehalten werden muss, bleibt er bei diesem Verfahren in alleinigem Besitz einer Person und muss nicht an den Kommunikationspartner weiter gegeben werden. Stattdessen ist der öffentliche Schlüssel für jeden frei zugänglich, vergleichbar der Telefonnummer in einem Telefonbuch. Hieraus leitet sich die Bezeichnung Public-Key-Verfahren ab.

Die Asymmetrie dieses Verfahrens liegt in der Verwendung der unterschiedlichen Schlüssel. Zur Verschlüsselung verwendet man den öffentlichen Schlüssel des Empfängers und die dazu gehörige Verschlüsselungsfunktion. Beides ist frei verfügbar, womit jeder die Möglichkeit hat, dem Empfänger eine sicher verschlüsselte Nachricht zu senden. Zum Entschlüsseln wird der geheime Schlüssel des Empfängers benötigt, womit nur dieser die an ihn gerichteten Nachrichten lesen kann.
Neben der Sicherheit des Verfahrens sind die korrekte Zuordnung der öffentlichen Schlüssel an die zugehörige Person sowie der Schutz der Integrität des öffentlichen Schlüssels für den sicheren Einsatz der asymmetrischen Verschlüsselung unumgänglich. Andernfalls können Nachrichten zwar korrekt verschlüsselt, aber an den falschen Adressaten geschickt werden. Zur Verifizierung dieser Zuordnung und zum Schutz der Integrität können Zertifikate verwendet werden (siehe unten).
Im Rahmen elektronischer Signaturen werden die Schlüssel genau umgekehrt verwendet: der Sender verschlüsselt seine Botschaft mit seinem privaten Schlüssel, er setzt sozusagen seine Signatur unter den Text. Nun ist es jeder anderen Person möglich, mit Hilfe des frei zugänglichen öffentlichen Schlüssels den Text zu entschlüsseln. Allerdings ist es in

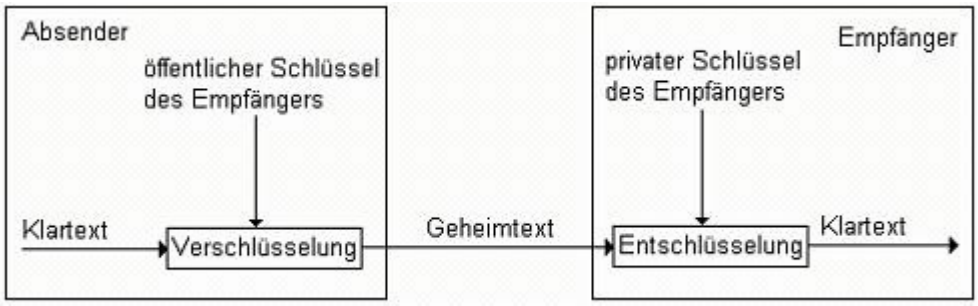

Abbildung 2: Asymmetrische Verschlüsselung

diesem Fall nicht das Ziel, den Inhalt der Nachricht geheim zu halten. Vielmehr erfährt der Empfänger dadurch, dass der öffentliche Schlüssel des Absenders genau auf die verschlüsselte Signatur passt, dass es sich tatsächlich um eine Nachricht des Senders handeln muss und kein Dritter die Nachricht verfasst haben kann. Die Nachricht ist damit also eindeutig einer bestimmten Person zugeordnet. Die symmetrische Verschlüsselung, die ohne Personen fest zugeordnete Schlüssel arbeitet, ist folglich ungeeignet für diese Verwendung.

2.2.1.3 Hash-Funktionen

Die Verschlüsselung alleine reicht aber noch nicht aus [BSIeSig]. Zwar ist damit sichergestellt, dass die Nachricht tatsächlich vom Absender stammt, aber es ist nicht auszuschließen, dass sie nachträglich verändert worden ist. Daher werden beim Einsatz elektronischer Signaturen zusätzlich zu dieser Verschlüsselung – und über die Anforderungen der Signaturrichtlinie hinausgehend – so genannte Hash-Funktionen verwendet. Eine Hash-Funktion ist eine mathematische Funktion, die Eingabetexte beliebiger Länge komprimiert und einen Hashwert vorgegebener Länge erzeugt. Beim Übertragen einer Nachricht wird der so erzeugte Hashwert an die eigentliche Nachricht angehängt. Der Empfänger wendet die Hashfunktion auf die Nachricht an. Da eine bestimmte Hashfunktion bei gleichem Eingabetext immer den gleichen Hashwert erzeugt, reicht ein einfacher Vergleich der Hashwerte des Senders und des Empfängers um sicher zu stellen, dass die

Nachricht nicht manipuliert wurde. Essentiell für diese Anwendung ist die Verwendung einer nicht umkehrbaren Funktion, einer so genannten Einwegfunktion (*„eine (mathematische) Funktion, die einfach (d.h. ohne großen Aufwand) zu berechnen, deren Inverses zu berechnen jedoch sehr schwierig ist.“* [GlReSt95]). Eine Hash-Funktion komprimiert also Eingabedaten beliebiger Länge auf einen Ausgabewert fester Länge, ohne dass diese Komprimierung – dank der Einweg-Eigenschaft - umgekehrt werden kann.

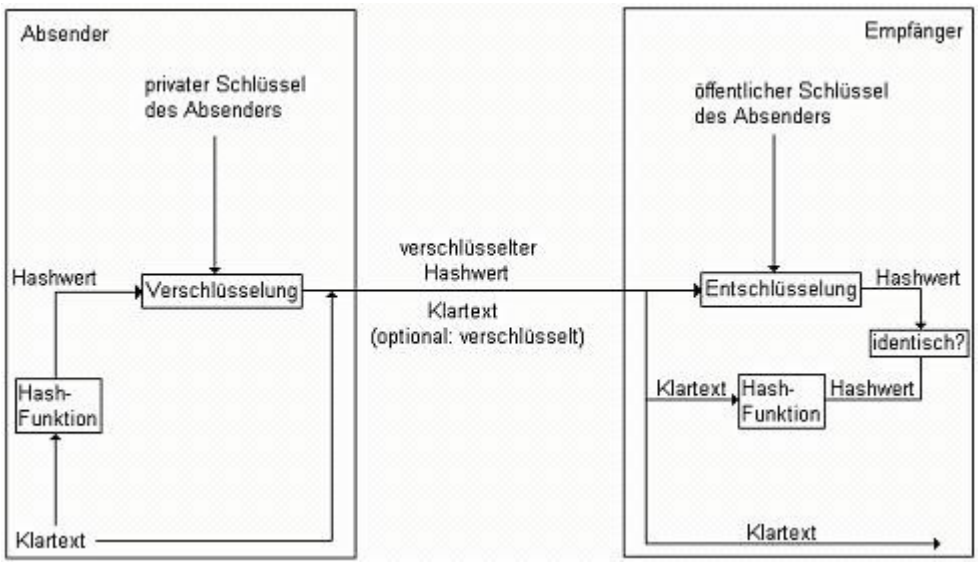

Abbildung 3: Verwendung der Hash-Funktion

2.2.1.4 Schlüssel- und Zertifikatsmanagement

Ein Problem bei dieser Art der Verschlüsselung ist die Verteilung des Schlüssels [SiSi00] – jeder Absender muss einen privaten Schlüssel besitzen, diesen Schlüssel darf kein anderer Absender verwenden, und alle potentiellen Empfänger müssen Zugriff auf den öffentlichen Schlüssel haben. Außerdem müssen alle potentiellen Teilnehmer die verwendete Hash-Funktion kennen. Ein System, dass für die Verteilung und Weiterleitung der erforderlichen Schlüssel sorgt, wird als Schlüssel-Infrastruktur (engl. *Public-Key-Infrastructure*, PKI) bezeichnet. Innerhalb

einer PKI werden für jeden Schlüssel durch ein Zertifikat seine Authentizität sowie sein Anwendungs- und Geltungsbereich bestätigt.
Glade/Reimer/Struif definieren ‚Zertifikat' wie folgt:

„Zertifikat – certificate
Die Bestätigung (Beglaubigung) bestimmter Zusammenhänge bzw. Zusammengehörigkeiten (z.B. Teilnehmer A gehört der Signatur-Schlüssel X) oder Eigenschaften

a) *von Personen (z.B. Teilnehmer B hat die Prokura der Firma Y) oder*
b) *von IT-Systemen (z.B. die Konformität mit vorgegebenen Sicherheits-/Qualitätskriterien)*

durch die Zertifizierungs-Instanz." [GlReSt95]

Das Zertifikat selbst ist wiederum durch eine eigene elektronische Signatur geschützt, deren Echtheit mit dem öffentlichen Schlüssel des Zertifikatsausstellers geprüft werden kann. Zur Überprüfung dieses öffentlichen Schlüssels erfordert es erneut ein Zertifikat, so dass sich eine Kette von Schlüsseln und Zertifikaten bildet – ein so genannter Validierungspfad – an dessen Ende in jedem Fall ein nicht validierbares Zertifikat stehen muss [Geis00]. Auf die Echtheit dieses letzten Zertifikates muss man sich unbedingt verlassen können [Geis00]. Grundsätzlich ist die Ausstellung von Zertifikaten jedem Anbieter erlaubt, die Signaturrichtlinie stellt es den Mitgliedsstaaten aber frei, Zertifizierungsdienstanbietern die Möglichkeit der Akkreditierung (d.h. der Bescheinigung über die Erfüllung bestimmter DIN-Normen von staatlicher Seite) zu bieten, was effektiv zu staatlich anerkannten Zertifizierungsdienstanbietern führt, die qualitativ höherwertige Zertifikate ausstellen [Schr03]. Zertifizierungsdienstanbieter werden auch in den gesetzgebenden Texten zur elektronischen Signatur mehrfach erwähnt und als Aufgabenträger von besonderer Bedeutung hervorgehoben. Die Unterscheidung von einfachen, fortgeschrittenen und qualifizierten Signaturen ist hier insofern relevant, dass an einen

Zertifizierungsdienstanbieter für qualifizierte Signaturen besondere Anforderungen personeller, technischer und verfahrenstechnischer Art gestellt werden. Ein Zertifizierungsdienstanbieter agiert als ‚vertrauenswürdiger Dritter', der die Identität eines Absenders und die Gültigkeit einer Signatur eindeutig und zuverlässig bestätigen kann [Schr03].

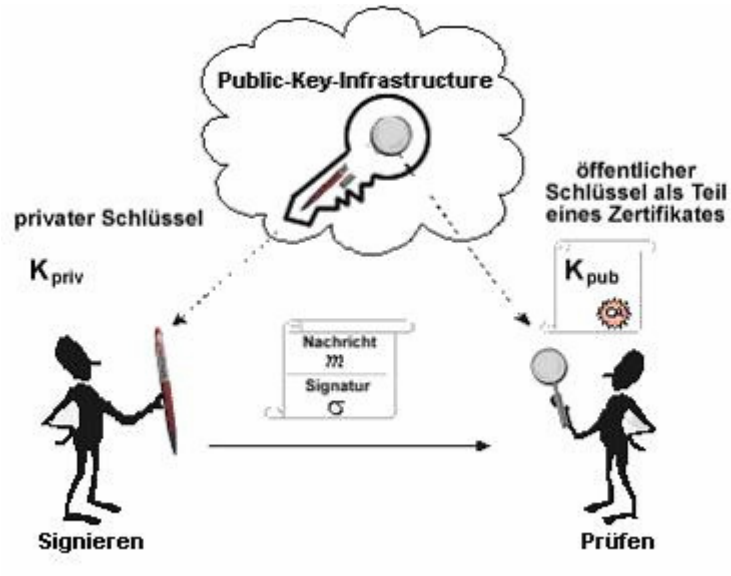

Abbildung 4: Signatursystem [BSIFBeSig]

Damit die Herkunft eines Zertifikats zweifelsfrei festgestellt werden kann, enthält es neben dem öffentlichen Signaturschlüssel zur Signaturprüfung und dem Namen des Zertifikatinhabers zusätzlich eine Zertifikatsnummer, eine Gültigkeitsdauer und insbesondere den Namen und die Signatur des Zertifikatausstellers. Darüber hinaus enthält ein Zertifikat weitere Angaben, die zum Teil optional sind [Preu05].

2.2.1.5 Zeitstempel

Zeitstempel (engl. *time stamps*) sind eine nachprüfbare Bestätigung, dass bestimmte Daten zu einem bestimmten Zeitpunkt existiert haben. Ein einfacher Zeitstempel ist etwa die Datumsangabe in einem Briefkopf. Die

Vertrauenswürdigkeit selbst erzeugter Zeitstempel ist allerdings als gering einzustufen. Für ein höheres Maß an Vertrauenswürdigkeit benötigt man einen Zeitstempel, der von einer vertrauenswürdigen Instanz ausgestellt wurde – bestehend üblicherweise aus Zeitangabe, vorgelegten Daten und Signatur des Zeitstempeldienstes. Die Daten liegen einem solchen Zeitstempeldienst üblicherweise nur in verschlüsselter Form und als Hashwert vor – das Versehen dieses Hashwerts mit einem Zeitstempel entspricht etwa einem gestanzten Zeitstempel auf einem verschlossenen Briefumschlag [Preu05]. Der Hashwert gewährleistet die Vertraulichkeit der Daten gegenüber dem Dienstleister, während der Zeitstempel direkt auf den Hashwert erfolgt, der ihn indirekt an die Daten überträgt.

Nach dem deutschen Signaturgesetz werden Zeitstempel in Deutschland als qualifizierte Zeitstempel bezeichnet, wenn sie von Dienstanbietern erzeugt werden, die zugleich die Anforderungen des Signaturgesetzes und der Signaturverordnung erfüllen [SigG.de]. Elektronische Signaturen in der Kombination mit qualifizierten Zeitstempeln entsprechen Beglaubigungen durch vertrauenswürdige Dritte [Schr03].

2.2.1.6 Alternative Konstruktion elektronischer Signaturen

Neben dem am häufigsten verwendeten und hier behandelten digitalen Signaturverfahren auf Basis von asymmetrischen Kryptoalgorithmen gibt es weitere Möglichkeiten, elektronische Signaturen zu konstruieren. Diese Varianten basieren auf der Verwendung von Hashfunktionen [Merk80], symmetrischen Kryptoalgorithmen [Merk87] oder biometrischen Verfahren [BSIeSig]. Da die grundsätzliche Funktionsweise von Hashfunktionen und symmetrischen Kryptoalgorithmen bereits vorgestellt wurden, folgt nun die Erläuterung biometrischer Verfahren.

2.2.1.6.1. Biometrische Signaturverfahren

Biometrische Verfahren stellen die wichtigste Variante zu auf asymmetrischen Kryptoalgorithmen basierenden digitalen Signaturen dar. Bei biometrischen Signaturverfahren wird kein (ggf. zertifizierter) Schlüssel erworben, sondern ein unveränderliches körperliches Merkmal, z.B. ein Fingerabdruck, dient als Schlüssel. Die bietet den Vorteil, dass der Signierende bei festem Verschlüsselungsverfahren keinen Schlüssel z.B. in Form einer Chipkarte benötigt. Gleichzeitig kann sich der Inhaber eines mitgeführten Ausweises, auf dem biometrische Daten gespeichert sind, jederzeit authentisieren. Neben dieser Authentisierung ermöglicht die Verwendung biometrischer Daten nach Einrichtung einer Datenbank auch die Identifikation von Personen [Behr01].

Allerdings existieren verschiedene Hindernisse und Probleme, die den Vorteil und die Einfachheit biometrischer Daten gegenüber zufälligen Schlüsseln (und deren Speicherung) in Frage stellen.

Das größte Problem ist die Leistungsfähigkeit. Ein biometrisches Erkennungssystem basiert auf einer Akzeptanzschwelle, bis zu der Abweichungen in der Aufnahme (z.B. des Fingerabdrucks) akzeptiert werden. Hierbei besteht die Gefahr, dass affine Merkmale fälschlicherweise zurückgewiesen (FNMR, False Non-Match Rate) oder nicht affine Merkmale akzeptiert (FMR, False Match Rate) werden. Je höher bzw. niedriger die Akzeptanzschwelle ist, desto größer wird der Anteil der FNMR bzw. FMR. Die Wahl der Akzeptanzschwelle ist daher für die Sicherheit des Systems von großer Bedeutung, eine absolute Sicherheit kann jedoch nie garantiert werden. Bei möglichst günstiger Wahl der Akzeptanzschwelle ist der Fehlerbereich allerdings sehr gering [BSIBio].

Neben diesem technischen existieren im Zusammenhang mit biometrischen Verfahren weitere Probleme. Das so genannte ‚Safety-Problem der Biometrie' bezeichnet das erhöhte Risiko des Körperteil-Diebstahls z.B. dann, wenn biometrische Merkmale zur Entriegelung biometrisch

gesicherter Sperren verwendet werden. Weitere Probleme verursacht die Biometrie im Bereich des Datenschutzes, z.B. bei Erfassung mehrerer biometrischer Daten (Mosaiktheorie [TiEhGe04]) [BiJäWo05].

2.2.1.7 Zusammenfassung: technische Grundlagen

Zusammenfassend lässt sich festhalten, dass eine elektronische Signatur mit Hilfe von Zertifikaten mehr als bloße Datensicherheit leistet. Vielmehr ermöglicht sie die zweifelsfreie Identifizierung des Absenders einer Nachricht sowie – durch die Verwendung von Hash-Funktionen – den Nachweis der Nichtmodifizierung der Originalnachricht und führt damit zur Eignung digital signierter Dokumente als Beweismittel. Im Fall der zusätzlichen Verwendung von Zeitstempeln wird neben der Identifizierung auch die zeitliche Zuordnung ermöglicht. Das Zertifikat selbst (vgl. etwa §7 [SigG.de]) enthält alle relevanten Informationen inklusive der verwendeten Algorithmen und seiner Gültigkeit, mit denen die Sicherheit der elektronischen Signatur überprüft werden kann.
Die Kombination aus Verschlüsselung, Hashwert und Zertifikat garantieren somit die rechtliche und technische Sicherheit des verwendeten Verfahrens.
Neben dem vorgestellten auf asymmetrischen Kryptoalgorithmen basierenden Verfahren existieren weitere Möglichkeiten, elektronische Signaturen zu konstruieren, von denen insbesondere die auf Biometrie basierende Variante von Bedeutung ist.

2.2.2 Rechtliche Grundlagen

Die elektronische Signatur ist das Kernelement des eGovernments. Für den elektronischen Austausch und die elektronische Aufbewahrung rechtlich relevanter Dokumente in eGovernment bestehen mehrere Anforderungen: Authentizität und Integrität, Vertraulichkeit sowie Nachweisbarkeit [SaEGov].

Authentizität und Integrität bedeutet, dass jedes Dokument zweifelsfrei einem Urheber zugeordnet und jede nachträgliche Änderung festgestellt werden können muss. Beides wird durch den Einsatz elektronischer Signaturen gewährleistet.
Vertraulichkeit bedeutet, dass Unbefügte nicht in der Lage sein dürfen, Einblick in Dokumente zu erhalten. Dies wird durch die in der elektronischen Signierung enthaltene Verschlüsselung erreicht.
Nachweisbarkeit schließlich ist die Beweisbarkeit des Vorliegens eines Dokumentes zu einem bestimmten Zeitpunkt. Dieser Aspekt wird durch Zeitstempel erfüllt.
Elektronische Signaturen sind also in der Lage, all diese Anforderungen zu erfüllen.

Aber nicht jeder Schriftverkehr mit einer öffentlichen Behörde erfordert zwangsläufig den Einsatz elektronischer Signaturen. Maßgeblich ist hier die Art des Schriftverkehrs. Unabhängig davon, wer den Kontakt anstößt, ist ausschlaggebend, ob der Kontakt ‚formfrei' sein darf oder in der ‚Schriftform' erfolgen muss. Ein formfreier Kontakt liegt vor, wenn der Zweck dieses Kontaktes das Kommunikationsmedium keinen gesetzlichen Zwängen unterwirft (z.B. Anfragen bei einer Gemeinde über Volksfesttermine) – in diesem Fall genügt ein einfacher Anruf, eine eMail oder ein Fax. Ist dagegen die Schriftform zwingend per Gesetz oder Rechtsverordnung vorgeschrieben – etwa bei Anträgen oder Bescheiden – so kann die eigenhändige Unterschrift beim elektronischen Schriftverkehr mit der Verwaltung nur durch eine elektronische Signatur ersetzt werden, die den rechtlich gestellten Bedingungen genügt [Schr03].

Die Grundlage für die Anwendung elektronischer Signaturen in der Europäischen Union bildet die Richtlinie 1999/93/EG vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische

Signaturen. Die Europäische Kommission beschreibt den Zweck dieser Richtlinie auf ihrer Informations-Website wie folgt:

„Mit dieser Richtlinie werden die juristischen Rahmenbedingungen für elektronische Signaturen und bestimmte Zertifizierungsdienste auf europäischer Ebene festgelegt. Diese Richtlinie soll die Verwendung elektronischer Signaturen erleichtern und zu ihrer rechtlichen Anerkennung innerhalb der Mitgliedstaaten beitragen.“ [SCADPlus]

Inhaltlich beschäftigt sich diese Richtlinie mit der Festlegung von Kriterien als Grundlage für die rechtliche Anerkennung elektronischer Signaturen mit einem Schwerpunkt auf Zertifizierungsdiensten. Speziell werden folgende inhaltlichen Punkte gelistet:

- gemeinsame Verpflichtungen für Zertifizierungsdienstanbieter, um die grenzüberschreitende Anerkennung der Signaturen und der Zertifikate in der Europäischen Gemeinschaft sicherzustellen;
- gemeinsame Haftungsregeln, um eine Vertrauensgrundlage sowohl bei den Verbrauchern, die sich auf die Zertifikate stützen, als auch bei den Dienstanbietern zu schaffen;
- Verfahren der Zusammenarbeit, um die grenzüberschreitende Anerkennung der Signaturen und Zertifikate in Drittländern zu erleichtern. [SCADPlus]

Darüber hinaus definiert die Richtlinie die Begriffe ‚fortgeschrittene elektronische Signatur’ und ‚qualifiziertes Zertifikat’. Eine fortgeschrittene Signatur liegt dann vor, wenn die folgenden Bedingungen erfüllt sind.
Eine fortgeschrittene elektronische Signatur

- darf ausschließlich dem Unterzeichner zugeordnet sein,
- muss die Identifizierung des Unterzeichners ermöglichen,
- wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle haben kann und

- ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Ein qualifiziertes Zertifikat muss insbesondere beinhalten:

- die Angabe, dass das Zertifikat als qualifiziertes Zertifikat erstellt wird,
- die Angabe des Zertifizierungsdienstanbieters,
- den Namen des Unterzeichners,
- Platz für ein spezifisches Attribut des Unterzeichners, das je nach Bestimmungszweck des Zertifikats aufgenommen wird,
- Signaturprüfdaten, die den vom Unterzeichner kontrollierten Signaturerstellungsdaten entsprechen,
- Angaben über den Beginn und das Ende der Gültigkeitsdauer des Zertifikats,
- den Identitätscode des Zertifikats und
- die fortgeschrittene elektronische Signatur des ausstellenden Zertifizierungsdienstanbieters.

Zusätzlich muss der Zertifizierungsdienstanbieter, der das Zertifikat ausstellt, einigen in der Richtlinie festgelegten Anforderungen entsprechen, die hier nicht näher erläutert werden.

Außerdem definiert die Richtlinie weitere beim Einsatz elektronischer Signaturen wichtige Aspekte.

Im Bereich ‚Marktzugang' wird unter anderem festgeschrieben, dass kein Staat die Bereitstellung von Zertifizierungsdiensten von vorheriger Genehmigung abhängig machen darf, aber die Möglichkeit hat, freiwillige Akkreditierungssysteme einzuführen, die auf höherwertige Zertifizierungsdienste abzielen, womit letztlich das Angebot „sicherer Signaturerstellungseinheiten" doch von einer Überprüfung abhängig ist. Im öffentlichen Bereich darf der Einsatz elektronischer Signaturen zusätzlichen Einschränkungen unterworfen werden. Außerdem darf die Bereitstellung von Zertifizierungsdiensten aus anderen Mitgliedsstaaten in den unter die Richtlinie fallenden Bereichen nicht eingeschränkt werden.

Zum Thema ‚Rechtswirkung elektronischer Signaturen' wird festgelegt, dass eine auf einem qualifizierten Zertifikat beruhende fortgeschrittene elektronische Signatur in jeder Beziehung mit einer handschriftlichen Unterschrift gleichzusetzen ist.

Weiter werden außerdem Haftungsbestimmungen der Zertifizierungsdienstanbieter gegenüber jeder Person, die auf ein solches Zertifikat vertraut, sowie einige internationale Aspekte wie die gegenseitige Anerkennung der elektronischen Signaturen der Mitgliedsstaaten geregelt.

Schließlich wird in der Richtlinie eine Rückmeldung der Mitgliedsstaaten zu Akkreditierungssystemen, Akkreditierungs- und Aufsichtsstellen sowie akkreditierten Zertifizierungsanbietern erwünscht.

Die konkrete Umsetzung dieser Vorgaben unterscheidet sich je nach Mitgliedsland. Im Folgenden werden die Umsetzungen einiger Mitgliedsstaaten, die in englischer oder deutscher Sprache vorliegen, näher erläutert.

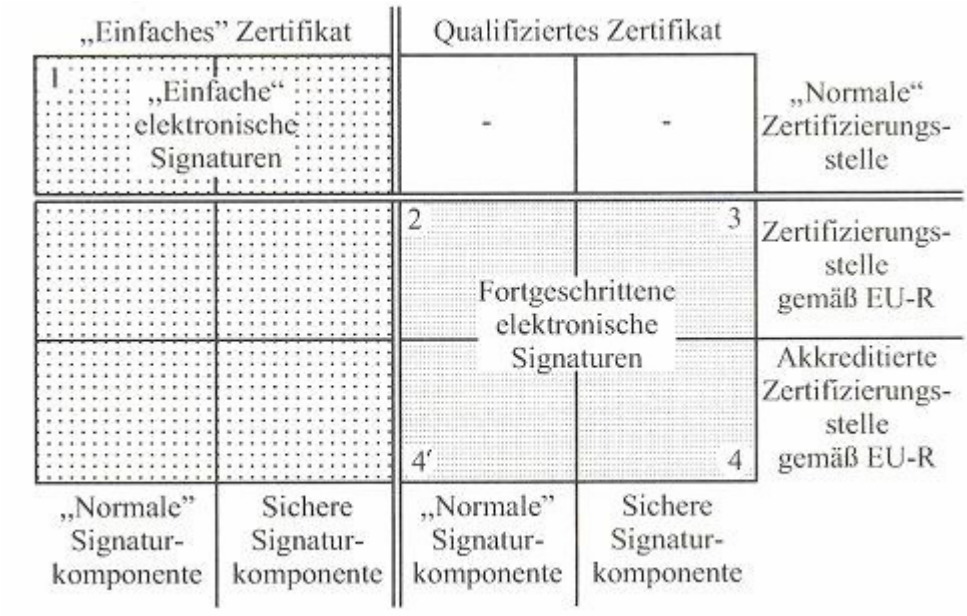

Abbildung 5: Varianten elektronischer Signaturen [Bert02]

2.2.2.1 Umsetzung der Richtlinie 1999/93/EG in Deutschland

Grundlegend für den Einsatz elektronischer Signaturen in Deutschland ist das „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften“, das so genannte Signaturgesetz (SigG) vom 16. Mai 2001 [SigG.de]. Erweitert wird das Signaturgesetz durch die „Verordnung zur elektronischen Signatur“ (Signaturverordnung, SigV) vom 16. November 2001 [SigV.de]. Dieses Signaturgesetz ist eine Weiterentwicklung des Signaturgesetzes vom 1.8.1997, dem ersten Gesetz weltweit [Preu05], das die Infrastruktur elektronischer Signaturverfahren für den gesamten Rechtsraum eines Staates regelt. Es enthält die bewährten Aspekte des Gesetzes von 1997, kommt aber zugleich den Anforderungen der Signaturrichtlinie nach.

Wird eine eigenhändige Unterschrift für einen Verwaltungsvorgang verlangt, so muss in dieser Situation in Deutschland eine qualifizierte elektronische Signatur verwendet werden [SigG.de]. Der Begriff der qualifizierten elektronischen Signatur wird im Signaturgesetz definiert und bezeichnet eine fortgeschrittene elektronische Signatur nach Richtlinie 1999/93/EG, die zusätzlich ein zum Zeitpunkt der Signaturerstellung gültiges Zertifikat sowie die Erstellung mit einer sicheren Signaturerstellungseinheit erfordert. In ihren Anforderungen geht das Signaturgesetz also über die durch die Signaturrichtlinie geforderten Voraussetzungen hinaus.

Die qualifizierte elektronische Signatur stellt ein rechtlich vollwertiges Substitut für eine eigenhändige Unterschrift dar. Allerdings kann sie keine weiteren Formvorschriften wie etwa eine notarielle Beglaubigung ersetzen [SigG.de]. Im Zivil- und Verwaltungsrecht wird die qualifizierte elektronische Signatur bereits eingesetzt und im Rahmen der Prozessordnungen von den zuständigen Gerichten anerkannt.

Neben der qualifizierten elektronischen Signatur definiert das Signaturgesetz in §2 zwei weitere Formen: die (einfache) elektronische Signatur und die fortgeschrittene Signatur (Auszug):

„Im Sinne dieses Gesetzes sind

1. „elektronische Signaturen“ Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen,

2. „fortgeschrittene elektronische Signaturen“ elektronische Signaturen nach Nummer 1, die

a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,

b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,

c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und

d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann,

3. "qualifizierte elektronische Signaturen" elektronische Signaturen nach Nummer 2, die

a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und

b) mit einer sicheren Signaturerstellungseinheit erzeugt werden, […].“ [SigG.de]

In der ersten Stufe – elektronische Signaturen oder auch einfache elektronische Signaturen – handelt es sich lediglich um Daten, die anderen Daten zugeordnet sind und diese authentifizieren, ohne Anforderungen in Bezug auf ihre Sicherheit, Einzigartigkeit oder Unveränderlichkeit erfüllen zu müssen. Fortgeschrittene elektronische Signaturen gehen einen Schritt weiter und entsprechen den fortgeschrittenen elektronischen Signaturen der europäischen Signaturrichtlinie. In der dritten und höchsten Stufe schließlich – den qualifizierten Signaturen – sind die Sicherheit der Technik

und die Verwendung von Zertifikaten als Instrument der sicheren Identifizierung des Signatur-Inhabers zwingend verankert. Diese Anforderungen verhelfen einem Dokument mit qualifizierter elektronischer Signatur zum Status eines sicheren Dokumentes, bei dem der Anwender Rechtssicherheit hat, das es vor Gericht als Beweis gültig ist – dies ist bei fortgeschrittenen Signaturen nicht der Fall, auch wenn sie als Mittel der Absicherung von Kommunikation und Datenübertragung eingesetzt werden können [SigG.de]. Im Zweifelsfall wird vor Gericht die Wahrscheinlichkeit der unrechtmäßigen Veränderung des elektronischen Dokumentes abgewägt und dessen Verwendung gegebenenfalls abgelehnt – es gilt der Ermessensspielraum des Richters [Preu05]. Dieser Ermessensspielraum ermöglicht die Zulassung jeglicher elektronischer Dokumente als Beweismittel – im Falle der qualifizierten elektronischen Signatur besteht aber keine Möglichkeit zur Ablehnung, da der Gesetzgeber die Regeln zur Sicherheit qualifizierter elektronischer Signaturen selbst getroffen hat und ihre Verwendung in vielen Fällen zulässt.

Abbildung 6: Signaturarten [BSIFBeSig]

Ein Beispiel für die Verwendung fortgeschrittener Signaturen gemäß 1999/93/EG ist das Programm Pretty Good Privacy (kurz PGP [PGP]). Hier werden die Forderungen nach Einzigartigkeit, Identifizierungsfunktion,

Anwenderbezogenheit und Veränderungssicherheit der erzeugten Dokumente voll erfüllt. Jedoch lässt das Konzept des gegenseitigen ‚Vorstellens' der Teilnehmer des Verfahrens (siehe [HoSc99]) gerade bei großen Nutzerzahlen keine Identifizierung des Einzelnen zu, welche vor einem deutschen Gericht in jedem Fall Bestand haben kann. Eine Technik wie PGP bildet somit nur eine Zwischenstufe, welche den Anforderungen an fortgeschrittene Signaturen genügt, aber nicht die Sicherheit qualifizierter Signaturen in den Punkten Technik der Erstellung und Identifizierung des Autors bietet.

Neben den Anforderungen an die Signatur selbst nennt das SigG weitere Vorgaben für Zertifikate sowie Zertifikatsersteller wie etwa Vorgaben bezüglich Akkreditierung, zeitlicher Fristen oder Aufbewahrung. Die SigV ergänzt das SigG unter anderem um Einzelregelungen zu den Anforderungen an die Zertifizierungsdienstanbieter sowie an die bei der Zertifikats- und Signaturerstellung einzusetzenden Produkte und Verfahren

Zusammenfassend lässt sich festhalten, dass der Gesetzgeber in Deutschland die EU-Richtlinie zu elektronischen Signaturen vollständig umgesetzt hat und sogar darüber hinausgegangen ist, um größtmögliche Sicherheit zu gewährleisten.

2.2.2.2 Umsetzung der Richtlinie 1999/93/EG in Österreich

Österreich war das erste Land, das die Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen umgesetzt hat [Roßn].

Die Grundlage für die Verwendung und rechtliche Anerkennung elektronischer Signaturen in Österreich bildet das Bundesgesetz über elektronische Signaturen (ebenfalls als Signaturgesetz bezeichnet und mit

SigG abgekürzt), BGB1I 1999/190 [SigG.at]. Erweitert wird es durch die Signaturverordnung [SigV.at].

Das österreichische Signaturgesetz unterscheidet zwischen zwei Signaturformen: der (einfachen) elektronische Signatur und der sicheren elektronischen Signatur, welche im Wesentlichen der deutschen qualifizierten elektronischen Signatur entspricht. Ein Auszug aus §2 des österreichischen SigG:

„Im Sinne dieses Bundesgesetzes bedeuten
1. elektronische Signatur: elektronische Daten, die anderen elektronischen Daten beigefügt oder mit diesen logisch verknüpft werden und die der Authentifizierung, also der Feststellung der Identität des Signators, dienen;
[…]
3. sichere elektronische Signatur: eine elektronische Signatur, die
a) ausschließlich dem Signator zugeordnet ist,
b) die Identifizierung des Signators ermöglicht,
c) mit Mitteln erstellt wird, die der Signator unter seiner alleinigen Kontrolle halten kann,
d) mit den Daten, auf die sie sich bezieht, so verknüpft ist, daß jede nachträgliche Veränderung der Daten festgestellt werden kann, sowie
e) auf einem qualifizierten Zertifikat beruht und unter Verwendung von technischen Komponenten und Verfahren, die den Sicherheitsanforderungen dieses Bundesgesetzes und der auf seiner Grundlage ergangenen Verordnungen entsprechen, erstellt wird; […]“ [SigG.at]

Mit der unter e) aufgeführten Bedingung geht die österreichische sichere elektronische Signatur über die Anforderungen an eine fortgeschrittene elektronische Signatur gemäß Richtlinie 1999/93/EG hinaus (vgl. qualifizierte elektronische Signatur in Deutschland).

Zusätzlich wird in der Verwaltungssignaturverordnung eine Verwaltungssignatur definiert, welche gemäß §25 E-Government-Gesetz bis zum 31. Dezember 2007 für eGovernment mit der Bürgerkarte (einer Kombination aus Ausweis und eigenhändiger Unterschrift im elektronischen Verwaltungsverfahren) gleichgestellt ist und für sichere Signaturen verwendet werden kann.
Weitere Einzelheiten werden durch die *Bestätigungsstellenverordnung – BestV* (BGBl. II Nr. 299/2002 26.7.2002) [BGB1. II 02], die *Feststellung der Eignung* des Vereins "Zentrum für sichere Informationstechnologie – Austria“ (A-SIT) *als Bestätigungsstelle* (BGBl. II Nr. 31/2000 2.2.2000) [BGB1. II 00] und das *Berufsrechts-Änderungsgesetz für Notare, Rechtsanwälte und Ziviltechniker 2006 - BRÄG 2006* [BRÄG06] geregelt.

Ähnlich wie bei der Umsetzung in Deutschland lässt sich auch hier festhalten, dass die Vorgaben der EU-Richtlinie umgesetzt wurden und die rechtlichen Bestimmungen in Österreich tatsächlich sogar darüber hinausgehen.

2.2.2.3 Umsetzung der Richtlinie 1999/93/EG in weiteren ausgewählten EU-Mitgliedsstaaten

In **Großbritannien** wurde die EU-Richtlinie im Jahr 2000 im ‚Electronic Communications Act 2000’ aufgegriffen [ElCA00]. In diesem Gesetz wird der Sachverhalt der elektronischen Signaturen wesentlich oberflächlicher behandelt als beispielsweise im deutschen Signaturgesetz. Im Wesentlichen legt das Gesetz lediglich die rechtlichen Rahmenbedingungen darüber fest, wer ‚*cryptography support services*’ ernennen darf, welcher Geheimhaltung elektronische Signaturen unterliegen und inwiefern Ausnahmen von dieser Geheimhaltung zu Gunsten staatlicher Ermittlungen getroffen werden dürfen. Außerdem legt das Gesetz fest, dass jeder das Recht auf einen eigenen privaten Schlüssel hat. Über verschiedene Formen der elektronischen Signaturen, insbesondere qualifizierte Signaturen, trifft das

Gesetz keine Aussage. Eine Regelung zur Gleichstellung qualifizierter Signaturen mit handschriftlichen existiert im britischen Recht nicht, ist aber auch nicht nötig, da handschriftliche Unterschriften vor einem britischen Gericht lediglich Indiz-Status haben, deren Beweiswert von Fall zu Fall unterschiedlich betrachtet wird.

Wesentlich detaillierter gestaltet sich die **schwedische** Umsetzung im ‚Qualified Electronic Signatures Act (SFS 2000:832)' aus demselben Jahr [QESA00]. In diesem Gesetz werden – vergleichbar dem deutschen Signaturgesetz – drei verschiedene Formen der Signatur definiert: die (einfache) elektronische Signatur, die fortgeschrittene elektronische Signatur und die qualifizierte elektronische Signatur. Der Unterschied zwischen der bereits in der EU-Richtlinie definierten fortgeschrittenen elektronischen Signatur und der qualifizierten besteht auch hier, ebenso wie in Deutschland, in einem zugrunde liegenden Zertifikat sowie der Erstellung der Signatur mit Hilfe eines sicheren Verfahrens (d.h. die Signatur muss fälschungssicher, einmalig, nicht ableitbar und vom Inhaber ausreichend schützbar sein). Außerdem dürfen die zu signierenden Daten nicht durch Anwendung der Signatur geändert und dem Inhaber der Signatur vor dem Signierungsprozess vorenthalten werden.

Einer qualifizierten Signatur muss ein qualifiziertes Zertifikat zugrunde liegen, an das bestimmte Anforderungen gestellt werden, etwa bezüglich des Inhalts. So muss es zum Beispiel eine Bestätigung beinhalten, dass es als qualifiziertes Zertifikat anerkannt wurde; es muss Name und Adresse des Zertifikatausstellers enthalten, den Namen oder ein Pseudonym des Inhabers; den Staat, in dem es ausgestellt wurde etc. Zertifikate, die außerhalb Schwedens ausgestellt wurden, werden anerkannt, wenn der Aussteller aus einem anderen EU-Staat stammt und dort die Genehmigung hat, qualifizierte Zertifikate auszustellen, wenn er die in diesem Gesetz später genannten Bestimmungen erfüllt und in einem anderen EU-Staat

akkreditiert ist und wenn das Zertifikat von einem anerkannten Zertifikataussteller als qualifiziertes Zertifikat garantiert wird.
Das Recht zur Ausstellung qualifizierter Zertifikate ist grundsätzlich jedem offen, allerdings muss zuvor eine Genehmigung der zuständigen Behörde eingeholt werden.
Qualifizierte elektronische Signaturen gelten vor Gericht und in Behörden als handschriftlichen Signaturen gleichgestellt. Im Kommunikationsverkehr mit oder zwischen Regierungsmitarbeitern sind allerdings zusätzliche, im Gesetz nicht näher ausgeführte Anforderungen möglich.
Im Weiteren regelt das Gesetz Schadensfälle und Weitergabe persönlicher Daten.
Schließlich wird festgelegt, dass eine Aufsichtsbehörde für die Einhaltung vorgenannter Bestimmungen sorgen und eine Liste der staatlich anerkannten Zertifikatsaussteller führen und veröffentlichen muss [QESA00].

Auch die **tschechische Republik** hat ihre Umsetzung der Richtlinie bereits im Jahr 2000 im ‚ACT of 29 June on electronic signatures and on the amendment to certain other acts (Electronic Signatures Act) as subsequently amended' beschlossen [AElS00].
Das Gesetz definiert fortgeschrittene elektronische Signaturen in der bekannten Form, verzichtet jedoch auf die Einführung und Definition des Begriffs der qualifizierten elektronischen Signatur. Dafür kommt der Bindung der Signatur an einen Zeitstempel eine große Bedeutung zu.
Im Wesentlichen legt der Gesetzestext ähnlich dem Gesetz im Vereinigten Königreich Rechte und Pflichten bei Ausstellung und Nutzung von Zertifikaten und Signaturen fest. Die in einem qualifizierten Zertifikat verlangten Angaben entsprechen ebenfalls dem, was weiter oben schon für das deutsche und schwedische Signaturgesetz genannt wurde. Zertifikate, die von Ausstellern in anderen EU-Staaten ausgestellt wurden, werden anerkannt; Zertifikate aus anderen Staaten müssen zusätzliche Bestimmungen erfüllen [AElS00].

Das **rumänische** ‚Law on the Electronic Signature (no. 455/2001)' [LElS01] schließlich ist der umfangreichste Gesetzestext der genannten Umsetzungen der EU-Richtlinie. Jedoch wird auch im rumänischen Gesetz keine qualifizierte elektronische Signatur definiert, sondern nur mit den Begriffen aus der EU-Richtlinie gearbeitet.

2.2.2.4 Verwendung elektronischer Signaturen in den Mitgliedsstaaten der europäischen Union

Die Artikel 29-Datenschutzgruppe hat in ihrem ‚Arbeitsdokument zur elektronischen Verwaltung (E-Government)' vom 8. Mai 2003 den damals aktuellen Stand der Entwicklung zusammengefasst [ADeV29]. Absatz ‚F: elektronische Signaturen und PKI (Public Key Infrastructure)' führt zahlreiche auch heute noch gültige grundsätzliche Gegebenheiten auf.
Der Arbeitsbericht betont die geringe Verbreitung elektronischer Signaturen zum damaligen Zeitpunkt. Ursächlich hierfür wird neben den Kosten und der Komplexität der benötigten Systeme der fehlende juristische Rahmen genannt – die Signaturrichtlinie liefert lediglich einen Rahmen für den Einsatz der Signatur an sich, hält sich aber sehr bedeckt bzgl. der Zertifizierung. Zertifikate müssen in allen EU-Staaten gleichgestellt sein, vorausgesetzt sie erfüllen die rechtlichen Bedingungen des jeweiligen Landes, in dem sie eingesetzt werden sollen. Ohne einen einheitlichen juristischen Rahmen entstehen hier zwangsläufig Komplikationen. Aufgrund der Kosten und der Komplexität unterstreicht die CNIL (*Commission Nationale de l'Informatique et des Libertés* (französische Datenschutzbehörde)) zusätzlich, dass die Einführung solcher Systeme nicht als Voraussetzung für die Umstellung der Behörden auf Online-Verwaltung gelten darf. Infolgedessen haben viele Verwaltungen noch keinerlei öffentlich zugängliches allgemeines Verfahren in Verbindung mit einem System zur Verarbeitung elektronischer Signaturen eingerichtet. Als Ausnahme ist hier Dänemark zu nennen; dort wurden bereits Systeme zur

Nutzung elektronischer Signaturen entwickelt und dem Bürger kostenlos zur Verfügung gestellt [ADeV29] [CiKu07].

Die meisten Staaten beteiligen zum Zeitpunkt der Verfassung des Arbeitsdokumentes private Zertifizierungsdienstanbieter an der Verwendung elektronischer Signaturen in Verbindung mit bestimmten Verfahren der Online-Verwaltung. Rechtliche Fragen zu Geschäftsbedingungen werden meist über nationales Recht gelöst. In einigen Ländern (Deutschland, Spanien) ist jedoch die Einbeziehung externer Anbieter ausgeschlossen, weil nur der Staat selbst diese Rolle übernehmen darf. In Frankreich dürfen private Anbieter zu diesem Zeitpunkt nur Online-Umsatzsteuererklärungen zertifizieren, in allen anderen Fällen übernimmt ebenfalls der Staat diese Rolle [ADeV29].

Die tatsächlichen Anwendungsbereiche der elektronischen Signatur hängen stark von den Prioritäten des jeweiligen Staates ab, etwa Steuerwesen und Sozialsektor in Frankreich oder Volkszählungen in Finnland. Die Nutzung erfolgt in den meisten Fällen von Einzelpersonen, Unternehmen und der Verwaltung gleichermaßen. Der Zugriff auf das System ist in den verschiedenen Ländern ebenfalls unterschiedlich geregelt. In einigen Ländern haben Einzelpersonen Zugriff (z.B. Deutschland), in anderen werden die Systeme zunächst für Mitarbeiter, Unternehmen und Server eingesetzt und sind folglich nicht vorrangig für die Bevölkerung verfügbar (z.B. Dänemark), und in wiederum anderen Ländern werden die Systeme zunächst von der Verwaltung genutzt (z.B. Norwegen). Bezüglich der Vertreter der Verwaltung ist es weniger relevant, dass die Signatur die jeweilige Person ausweist; von größerem Interesse ist die Bestätigung der erforderlichen Entscheidungskompetenz der unterzeichnenden Person [ADeV29].

Die Datenschutzbehörden der Mitgliedsstaaten stehen den Systemen mit elektronischer Signatur als Mechanismus zum Schutz personenbezogener Daten im Allgemeinen positiv gegenüber. In einigen Staaten konnten die Datenschutzbehörden den öffentlichen Stellen ihre Standpunkte mitteilen, manchmal wurden die Behörden auch bei der Verabschiedung von Gesetzen und Regulierungsbestimmungen zur Gestaltung von Prozessen mit elektronischen Signaturen angehört oder nahmen Stellung nach der Aufforderung der Überprüfung bestimmter Anwendungen. Hierbei wurde seitens der Datenschutzbehörden besonders die Empfehlung ausgesprochen, den Nutzern eindeutige Informationen der Zertifizierungsdienstanbieter zur Weitergabe der Daten zukommen zu lassen, welche die Rechtsvorschriften betreffend der Weitergabe personenbezogener Daten erfüllen, und so den Benutzer ausführlich darüber zu informieren, welche der ihn betreffenden Daten weitergegeben werden [ADeV29].

In ihrem Bericht vom 15. März 2006 stellt die Kommission der Europäischen Gemeinschaften in Abschnitt 2.2 fest, dass alle (zu diesem Zeitpunkt 25) Mitgliedsstaaten die allgemeinen Grundsätze der Richtlinie umgesetzt haben [KdEG06].

In Deutschland wurde 2006 eine eGovernment-Basiskomponente eingeführt, die auf Fachkonzepten des Bundes und von den Bundesländern gemeinsam entwickelter Standardsoftware basiert. Diese Basiskomponente bot den Landesregierungen 2006 folgende Funktionen:

- Erstellung und Prüfung rechtskonformer, qualifiziert elektronischer Signaturen;
- Ver- und Entschlüsselung von Daten;
- Erstellung und Prüfung digitaler Zeitstempel;
- Sicherer und nachweisbarer Transport signierter und verschlüsselter Dokumente per OSCI-Protokoll und
- Elektronische Abwicklung von Verwaltungsverfahren.

Für 2007 ist die schrittweise Bereitstellung weiterer Funktionen geplant [SaEGov].

2.2.2.5 Einsatzgebiete elektronischer Signaturen

Elektronische Signaturen dienen der zweifelsfreien Identifikation einer Person. Dank dieser Identifikation ist es dem Identifizierenden möglich, die Person einzuordnen. Dieses Identitätsmanagement (engl. *‚Identity Management'*) spielt zum Beispiel eine große Rolle bei der Identifizierung eines Handelspartners, insbesondere im World Wide Web. Indem beide Beteiligten ihren Parten eindeutig identifizieren, wird eine Vertrauensbasis geschaffen, die die Abwicklung der Transaktionen ermöglicht [BeFe00]. Ein wichtiges Beispiel für diesen Einsatz elektronischer Signaturen im Identitätsmanagement in der öffentlichen Verwaltung ist z.B. die elektronische Auftragsvergabe [eVergabe].
Neben der Identifikation zur Vertrauensbildung dient die Identifikation auch der Zuordnung persönlicher Rechte, etwa Zugriffsrechte auf (elektronische) Daten, Weisungsbefugnis oder Zutrittsrechte. Die Identifikation erfolgt in diesem Fall über elektronische Ausweise und Chip-Karten [DuE06].

Die zwei vorherrschenden konkreten Einsatzgebiete elektronischer Signaturen betreffen elektronische Behördendienste und persönliche elektronische Bankdienste [KdEG06].

Im März 2006 haben zahlreiche Mitgliedsstaaten der Europäischen Union sowie mehrere andere europäische Länder Anwendungen elektronischer Behördendienste bereits eingeführt oder planen dies. In Deutschland findet die elektronische Signatur Anwendung z.B. bei der elektronischen Abgabe eines Angebotes für einen öffentlichen Auftrag (eProcurement), bei elektronischer Antragstellung und Genehmigung der Ein- und Ausfuhr geschützter Tiere und Pflanzen, bei verschiedenen Aspekten des

Rechnungswesens in der Sozialversicherung, beim elektronischen Patentantrag, in der elektronischen Justizkommunikation oder im Einwohnermeldewesen [BSIeSig]. Zur Teilnahme am signaturbasierten eGovernment ist in Deutschland der Erwerb einer Signaturkarte eines Zertifizierungsdienstanbieters obligatorisch [IDABC-GER].

In anderen Ländern stützt sich die Nutzung des signaturbasierten eGovernments auf die Verwendung eines elektronischen Ausweise (z.B. die Bürgerkarte [BuKaAm] in Österreich) [KdEG06].

Ein solcher elektronischer Ausweis bietet neben seiner Ausweisfunktion die Möglichkeit des Online-Zugangs zu öffentlichen Diensten. Zumeist umfassen solche Ausweise drei Funktionen: Identifizierung, Authentifizierung und Unterschreiben [KdEG06]. In Deutschland wird der elektronische Ausweis voraussichtlich im Jahr 2009 eingeführt und auch biometrische Daten enthalten [KSA07].

Die Einführung einer spezielleren Version des elektronischen Ausweises, der elektronische Reisepass (‚ePass'), wurde bereits am 13. Dezember 2004 vom Rat der Europäischen Union beschlossen [2252/2004]. Am 22. Juni 2005 billigte das deutsche Bundeskabinett einen Vorschlag des damaligen Bundesinnenministers Otto Schily zur Einführung eines solchen Reisepasses [Hand05]. Der deutsche elektronische Reisepass enthält maschinenlesbare biometrische Daten des Inhabers sowie aufgrund der Verabschiedung eines neuen Passgesetzes vom 23. Mai 2007 ab dem 01. November 2007 zusätzlich die Daten von zwei Fingerabdrücken [TS07].

Die Einführung des elektronischen Ausweises ist Bestandteil der eCard-Strategie der Bundesregierung, deren Ziel es ist, „*elektronische Dienstleistungen kostengünstig, sicher, auf einem hohen Datenschutzniveau und einfach zur Verfügung zu stellen.*" [BMWI05] Neben der Einführung des elektronischen Ausweises ist auch die Einführung der elektronischen Gesundheitskarte im Jahr 2006 ein Element dieser Strategie. Beide Karten sind technisch so vorbereitet, dass sie „*auf Wunsch der nutzenden Person auch für qualifizierte Signaturen genutzt werden können.*" [BMWI05]

Weitere Elemente sind das JobCard-Verfahren und die elektronische Steuererklärung ELSTER [BMWI05].

Die zweite wichtige Anwendung elektronischer Signaturen in persönlichen elektronischen Bankdiensten (‚Online Banking') befindet sich seit mindestens Anfang 2006 in den meisten EU-Ländern im Aufschwung [KdEG06]. Die meisten Bank-Authentifizierungssysteme stützen sich auf einmalig einsetzbare Passwörter, so genannte ‚Tranksaktionsnummern' (TAN), bei denen es sich gemäß der Richtlinie 1999/93/EG um die einfachste Form der elektronischen Signatur handelt [KdEG06]. Bei elektronischen Bankgeschäften zwischen Unternehmen sowie beim Bankenclearing ist es dagegen üblich, als sicherer geltende intelligente Chipkarten zu verwenden [KdEG06].

Zugleich wird in mehreren Mitgliedsstaaten das Spektrum der Dienste erweitert, die einen der einfachen Form der elektronischen Signatur entsprechenden Authentifizierungsgrad erfordern [KdEG06].

Ein zentrales Einsatzgebiet in Deutschland ist die Vergabe öffentlicher Aufträge [eVergabe] [IDABC-GER].
Mit der Initiative Media@Komm (seit 1999) und deren Nachfolger Media@Komm-Transfer (seit 2003) wird außerdem die Verbreitung des eGovernments in der Bundesrepublik forciert, indem ein Netzwerk kommunaler Akteure etabliert und ausgebaut wird [M@KT03].
Die IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens) führt derzeit eine Studie durch, die unter anderem den Status der Mitgliedstaaten in der Umsetzung der elektronischen Signatur zum Thema hat und im Jahr 2009 abgeschlossen sein soll [IDABC05].

2.2.2.6 Probleme beim Einsatz elektronischer Signaturen

Ein grundsätzliches Problem ist die langsame Entwicklung des Marktes für elektronische Signaturen. Eine Ursache hierfür ist die Komplexität der PKI-Technologie. Hauptsächlich aus Gründen der Haftung existiert jedoch derzeit wenig Interesse seitens der Dienstanbieter daran, ihren Kunden die Nutzung ihrer Authentifizierungseinrichtung für andere Dienste zu gestatten und damit die Nutzung des „vertrauenswürdigen Dritten“ zu ermöglichen. Die Nutzung dieser Authentifizierungseinrichtung ist jedoch unumgänglich, um eine Vertrauensbasis zwischen Handelspartnern im Internet zu schaffen [KdEG06].
Für diese langsame Einführung können noch weitere Faktoren verantwortlich sein. Zu diesen Faktoren gehören das Fehlen von Kriterien in der Richtlinie für Dienste zur Prüfung elektronischer Signaturen auf Seiten des Endnutzers oder das Fehlen von Bestimmungen über die gegenseitige Anerkennung von Zertifizierungsdienstanbietern. Je nach Staat existieren verschiedene Lösungen zur Validierung eines Zertifikats (streng hierarchische PKI mit einer ‚Root-CA’ (Stamm- oder Wurzel-Zertifizierungsstelle), Cross-Zertifizierung zwischen Zertifizierungsstellen durch eine Bridge-CA (überbrückende Zertifizierungsstelle) oder Vertrauensliste). Das Pilotprojekt „Bridge/Gateway CA“, das im Rahmen grenzüberschreitender elektronischer Geschäftstransaktionen im IDA II-Programm entstand [BGCA], hat weitere technologische, aber auch rechtliche und organisatorische Probleme aufgezeigt [KdEG06].

Ein weiteres Hindernis für die Marktakzeptanz elektronischer Signaturen bildet die fehlende technische Interoperabilität auf nationaler und insbesondere internationaler Ebene. Dadurch haben sich bei Anwendungen elektronischer Signaturen zahlreiche Insellösungen ergeben, bei denen Zertifikate nur für eine einzige Anwendung gebraucht werden können [KdEG06].

Außerdem führt dies dazu, dass eine Vielzahl technischer Ausstattungen benötigt wird, um mit verschiedenen Partnern rechtsverbindlich kommunizieren zu können. Daher wird eine allgemein verbindliche Spezifikation benötigt, die sich auf die Sicherheitsfunktionen elektronische Signatur, Authentisierung und Verschlüsselung bezieht. [Zezs01].
Eine EU-weite einheitliche Infrastruktur für elektronische Signaturen (eSig-Infrastruktur) ist das Ziel, dass es zu erreichen gilt, wenn elektronische Signaturen EU-weit zum Einsatz kommen sollen [Schr03].

In der PKI-Umgebung ist die intelligente Chipkarte das am häufigsten verwandte Mittel zur Erzeugung einer Signatur, da sie die sichere Speicherung des privaten Schlüssels ermöglicht. Diese Technologie ist aber teuer und erfordert Investitionen in die physische Infrastruktur (z.B. Verteilung von Karten und Kartenlesegeräten) [KdEG06].

Zu den Problemen an der Basis der Technologie gehört die Verwendung der ‚richtigen' Signatur. Einfache und fortgeschrittene Signaturen liefern keine ausreichende Sicherheit; nur qualifizierte Signaturen können als absolute Vertrauensbasis dienen (vgl. 2.2.2 Abs. 1). Daher ist es wichtig, dass dies von allen Anwendern verstanden wird und entsprechend qualifizierte Signaturen verwendet werden [Roßn].

Ein weiteres Problem, das auch aus der langsamen Marktentwicklung resultiert, ist das Fehlen der Software. So wäre es z.B. wünschenswert und situationsabhängig auch aus Datenschutzgründen erforderlich, einzelne Anhänge einer eMail digital signieren zu können, anstatt die gesamte Mail signieren zu müssen.
Die vorhandene Software ist in Kosten und Einsatzaufwand der gewünschten Anwendung vielfach nicht angemessen [Zezs01].

Schließlich genießen qualifizierte signierte elektronische Dokumente im Falle einer rechtlichen Auseinandersetzung denselben Beweiswert wie Original-Papierdokumente. Daher ist die Archivierung solcher Dokumente unumgänglich [KdEG06]. Der Papierausdruck eines solchen Dokumentes ist wertlos, da er lediglich einer nicht beglaubigten Kopie eines Papierdokumentes entspricht. Selbst eine beglaubigte Überführung in Papierform ersetzt nach aktueller rechtlicher Lage nicht das Original [Preu05].

Neben den benötigten Verfahren und Dienstleistungen zur langfristigen Archivierung müssen darüber hinaus die Bürger informiert werden, dass sie erhaltene qualifiziert signierte elektronische Dokumente nicht löschen dürfen, da damit Beweiswert vernichtet würde [Zezs01].

Außerdem verursacht die Archivierung weitere Probleme, da nicht nur die Unverfälschtheit und Authentizität der Daten bei der Übertragung gewährleistet werden, sondern das Zertifikat auch nach jahrelanger Archivierung noch gültig und überprüfbar sein muss. Neben dieser Frage der dauerhaften Überprüfbarkeit stellt sich auch das Problem, dass die Soft- und Hardware verfügbar sein muss, mit der die Dokumente wieder in ihrer ursprünglichen Form angezeigt werden können [Zezs01].

2.2.2.7 Zusammenfassung: rechtliche Grundlagen

Mit der Signaturrichtlinie hat die Europäische Union eine Grundlage zum Einsatz elektronischer Signaturen geschaffen. Allerdings geht diese Grundlage nicht weit genug und hilft nicht dabei, die wesentlichen Probleme wie die konkrete technische Realisierung und die qualitative Sicherheit zu beheben. Dementsprechend fällt die Umsetzung der Richtlinie in den verschiedenen betrachteten EU-Staaten sehr unterschiedlich aus. Außerdem fehlen Anreize für Unternehmen, ihre Zertifizierungsdienste als „vertrauenswürdiger Dritter“ zur Verfügung zu stellen. Das hieraus

resultierende geringe Marktwachstum führt zu einem seltenen Einsatz dieser Technik.
Ein detaillierterer rechtlicher Rahmen wird benötigt, um Einheitlichkeit zu schaffen und einen flächendeckenden Einsatz elektronischer Signaturen auch über Ländergrenzen hinweg zu ermöglichen.

2.3 Zusammenfassung: elektronische Signaturen

Nach einer Definition des Begriffes eGovernment wurde in diesem Kapitel zunächst auf die Technik der elektronischen Signatur eingegangen. Die Grundlagenvermittlung mit der Gegenüberstellung von symmetrischer und asymmetrischer Verschlüsselung sowie der Erläuterung der Hash-Funktion machte deutlich, dass es sich bei der elektronischen Signatur um eine sichere und verlässliche Technologie handelt. Mit Hilfe einer öffentlichen Schlüsselverwaltung sowie des Managements der Zertifikate, die die Identität jeder Signatur bestätigen, ist es möglich, eine zuverlässige Infrastruktur aufzubauen, in der kein Zweifel am Absender einer Nachricht besteht. Allerdings existieren noch immer Schwachpunkte; neben der Gefährdung des Systems auf technischer Ebene bei einem Verlust des privaten Schlüssels oder der Entschlüsselung des verwendeten Verschlüsselungsverfahrens drohen weitere Gefahren durch unzuverlässige Zertifizierungsdienstanbieter.

Auch auf rechtlicher Ebene, die im nächsten Teil dieses Kapitels erläutert wurde, ist die Entwicklung noch nicht abgeschlossen. Nach der ausführlichen Vorstellung der Signaturrichtlinie wurde ihre Umsetzung in verschiedenen EU-Staaten dargestellt und aufgezeigt, wie stark sich diese Umsetzungen zum Teil voneinander unterscheiden. Die Signaturrichtlinie ist ein erster Schritt, eignet jedoch noch nicht als ultimative Grundlage zur Errichtung einer EU-weiten eSig-Infrastruktur. Aufwand und Kosten ihres Einsatzes, mangelnde Standardisierung und Probleme bei der erforderlichen

Archivierung elektronisch signierter Dokumente, vor allem aber das geringe Marktwachstum sind weitere Probleme, deren Lösung erforderlich ist.

3 Zukunftsforschung

Im vorhergehenden Kapitel wurden die technischen und rechtlichen Grundlagen der elektronischen Signatur im europäischen eGovernment dargelegt. Aufgabenstellung dieser Arbeit ist es, auf Basis dieser Grundlagen ein Zukunftsszenario zu entwickeln, anhand dessen Aussagen über die erforderlichen Maßnahmen zu treffen sind, die benötigt werden, um die elektronischen Signaturen zukunftsfähig zu machen und sie frühzeitig auf eventuell auftretende Gefahren vorzubereiten und an Veränderungen anzupassen.
Zur Entwicklung solcher Szenarien bedient man sich der wissenschaftlichen Disziplin der Zukunftsforschung. Innerhalb der Zukunftsforschung existieren verschiedene Methoden der Prognose oder Vorausschau, von denen einige in diesem Kapitel vorgestellt werden und eine ausgewählt wird.

Das Kapitel beginnt mit einer einleitenden Vorstellung zweier Begrifflichkeiten. Zunächst wird der Begriff der Zukunftsforschung erläutert. Dem folgen die Beschreibung der historischen Entwicklung des Begriffs Szenario sowie eine Definition desselben.
Anschließend werden verschiedene populäre Methoden der Zukunfts-forschung vorgestellt und erläutert. Nach einer Diskussion, welche dieser Methoden am besten für die gestellte Aufgabe geeignet ist, wird diese gewählte Methode – die Szenario-Analyse – im Detail vorgestellt.

3.1 Definition ‚Zukunftsforschung'

„Zukunftsforschung ist die wissenschaftliche Befassung mit möglichen, wünschbaren und wahrscheinlichen Zukunftsentwicklungen und Gestaltungsoptionen sowie deren Voraussetzungen in Vergangenheit und Gegenwart." [Krei06]

Die Geschichte der Zukunftsforschung ist so alt wie die Menschheit selbst. Schon in der Vorzeit versuchten Schamanen, mit geworfenen Knochen die Zukunft vorherzusagen. Weltberühmt ist das antike Orakel von Delphi in Griechenland. Die Römer versuchten den Ausgang bedeutender Schlachten aus den Innereien von Tieren zu lesen. Später entwickelten sich Methoden wie Handlesen, Kartenlegen oder die Kristallkugel, die dem kundigen Anwender einen Blick in die Zukunft gewähren soll. Die letztgenannten Verfahren haben sich bis heute erhalten, dienen jedoch zumeist als Jahrmarktunterhaltung.

Der tatsächliche Wert der vorgenannten Methoden, die auf Spekulationen und bewusster Herbeiführung einer vorhergesagten Zukunft basieren, mag sicherlich bezweifelt werden. Die modernen Formen der Zukunftsforschung haben nicht viel mit dieser Wahrsagerei gemein, lediglich das Ziel ist dasselbe: es werden Informationen gesucht, um für die Zukunft gewappnet zu sein. Doch während die Wahrsagerei behauptet, die Zukunft vorhersagen zu können, ist es die Zielsetzung der Zukunftsforschung, mögliche Zukunftsentwicklungen zu ermitteln, um beim Eintreten einer solchen darauf vorbereitet zu sein.

Im Gegensatz zur spekulativen Ausübung der Wahrsagerei basiert die moderne Zukunftsforschung auf der Empirik und dem Erfahrungswissen der Experten [Bove06].

Mit der Entfaltung der modernen Wissenschaft (der Entwicklung des westlichen Denkens seit etwa 1600, basierend auf einem Wechselspiel aus Theorie und Praxis und der Überprüfung durch Experimente, Statistiken und Berechnungen [Chal85]) nahm die Beschleunigung technischer, ökonomischer und sozialer Veränderungen derart zu, dass sich für den Menschen der Neuzeit das Verhältnis zu den drei Zeitdimensionen Vergangenheit, Gegenwart und Zukunft grundlegend wandelte. Zuvor lebte die Menschheit in nahezu stationären Kulturen, in denen sich die Zeitdimensionen kaum voneinander unterschieden. Moderne Innovationen

jedoch bewirkten in immer kürzeren Zeitintervallen grundlegende Veränderungen, seien sie sozialer, wirtschaftlicher oder kultureller Natur. Der Mensch fühlt sich immer stärker selbst als Gestalter der Zukunft, die nicht länger von den Mächten der Natur oder dem Schicksal bestimmt wird.

Obwohl revolutionäre Entwicklungen schon im 18. und 19. Jahrhundert eine zunehmende Rolle für das Leben in der Gegenwart spielten, kam es erst in den 30er und 40er Jahren des 20. Jahrhunderts zur Herausbildung einer eigenständigen erfahrungswissenschaftlich basierten Zukunftsforschung, die die bis dahin vorherrschenden spekulativen Zukunftsmodelle ablöste (etwa Thomas Mores ("Utopia"), Tommaso Campanella ("Der Sonnenstaat"), oder die Entwürfe der Frühsozialisten (Saint-Simon, Charles Fourier, Robert Owen) sowie von Karl Marx und Friedrich Engels, Oswald Spengler und Herbert George Wells) [Krei06].

Lange Zeit war kein Platz für ein wissenschaftlich begründetes Vorausdenken, Entwerfen und Darstellen möglicher Zukünfte zwischen den beiden Polen der spekulativ-philosophischen Gesellschaftsmodelle und den eng begrenzten naturwissenschaftlich-technischen Projektionen. Systematische Beobachtung und strukturierte Kombination empirischer Daten der Vergangenheit bildeten das eherne Fundament einer kausaldeterministischen erfahrungswissenschaftlichen Methodik, die immer mehr auch zur Erklärung sozialer und ökonomischer Prozesse dienen sollte.
In Zeiten ungebrochenen Wachstums mit lediglich geringfügigen Änderungen der Umwelt funktionierte diese Methodik berechenbarer Prognosen durchaus. Die für den Großteil der Planer überraschend auftretende Ölkrise Anfang der 70er Jahre des 20. Jahrhunderts zeigte jedoch die Grenzen dieser Zukunftsberechnung auf. Unvorhersehbare Ereignisse großen Ausmaßes überstiegen ihre Fähig- und Möglichkeiten und machten jegliche auf reinen Erfahrungswerten basierende Zukunftsplanung unter Annahme unveränderter Umweltbedingungen

hinfällig. In dieser Zeit erinnerte man sich der Methode der Verwendung von Szenarien zur Gestaltung möglicher Zukünfte [Brei97] [Krei06].

3.2 Die Geschichte des Begriffs ‚Szenario'

Der Begriff ‚Szenario' stammt aus der Welt des Theaters (und findet heute auch beim Film Verwendung) und bezeichnet dort einen szenisch gegliederten Entwurf eines Theaterstücks, d.h. ein erstes Bild einer Szene, in der nicht sämtliche Details Berücksichtigung finden. Analog wird der Begriff auch in der Zukunftsforschung verwendet: Szenarien sind Abbilder der Zukunft, die naturgemäß nicht detailgetreu sein können, es in den wichtigen Punkten aber möglichst sein sollten.

Im Zusammenhang mit der Zukunftsforschung wurde die Idee des Szenarios das erste Mal im frühen 19. Jahrhundert im militärischen Umfeld verwendet. Die preußischen Generäle und Militärtheoretiker Moltke und Clausewitz entwickelten als erste militärische Planspiele, mit deren Hilfe sie ihre Schlachten vorbereiteten. Diese Planspiele stellen die ersten historischen Ansätze für strategische Planung und die Verwendung und Entwicklung von Szenarien dar [Reib87].
Carl von Clausewitz schreibt in seinem Werk „Vom Kriege": *„Die Strategie ist der Gebrauch des Gefechts zum Zwecke des Krieges; sie muss also dem ganzen kriegerischen Akt ein Ziel setzen, welches dem Zweck dessen entspricht, […]"*[Clau78].
Tatsächlich haben Moltke und Clausewitz als erste die Prinzipien einer echten strategischen Planung formuliert. Dazu gehörten etwa:
- den Gegner dort anzugreifen, wo er Schwächen hat,
- die Strategie auf den eigenen Stärken basieren zu lassen,
- das langfristige Ziel des Feldzuges nicht aus dem Auge zu verlieren – nicht der Ausgang der Schlacht, sondern der des Krieges ist entscheidend!

Das Wort ‚Szenario' tauchte zum ersten Mal etwa 150 Jahre später auf, als Herman Kahn, damals Mitarbeiter der RAND Corporation, im Rahmen der strategischen Planung der USA Anfang der 50er Jahre militärstrategische Planspiele entwickelte, die er Szenarien nannte. Hierbei handelte es sich überwiegend um Beschreibungen von Gefechtsfeldsituationen, in denen die Militärplaner so erfolgreich wie möglich operieren mussten, um den Sieg sicherzustellen. Diese so genannte amerikanische Variante der Szenarien wird auch als ‚contextual scenarios' bezeichnet, da die Szenarien ähnlich einem Bühnenbild bei einer Theateraufführung den Rahmen für bestimmte Aktivitäten vorschreiben. In der so genannten französischen Variante werden Szenarien als Handlungsstrategie sowie deren Ergebnis betrachtet. Diese Variante entstand etwa zeitgleich in Frankreich und wurde dort zur Regionalplanung eingesetzt. Beide Arten von Szenarien prägten die erste Phase der Szenario-Analyse. In dieser Phase wurden Szenarien überwiegend für politische und militärische Zwecke verwendet und hatten größtenteils visionären Charakter [Reib87].

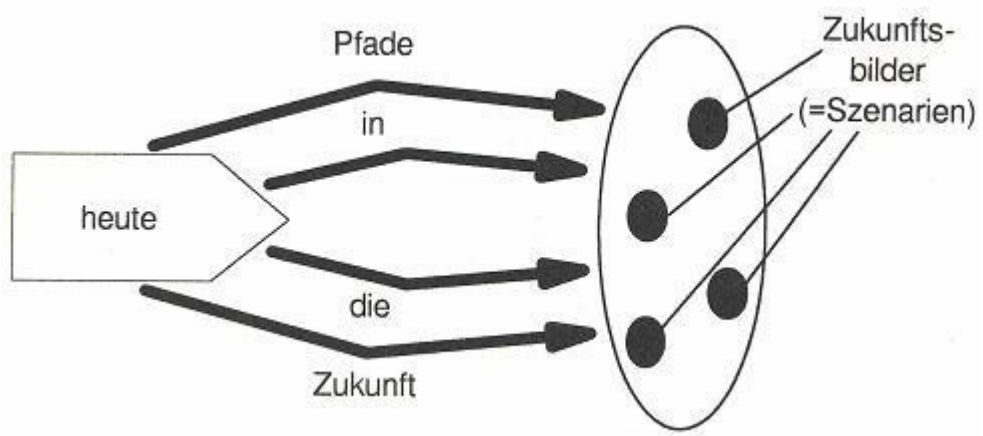

Abbildung 7: Zum Verständnis von Szenarien [GeWi89]

Wirtschaftliche Anwendung fanden Szenarien erst ab den 1970er Jahren. Wie vorstehend erwähnt unterbrach die Ölkrise Anfang der 70er überraschend das gleichmäßige und ungebrochene Wirtschaftswachstum der

westlichen Welt. Einfache Planungsmethoden reichten nicht mehr aus, die Idee der Szenarien wurde für Wirtschaft und Forschung entdeckt. Pionier der Szenarioentwicklung war die Shell-Gruppe, die versuchte, quantitativ orientierte Planungsmethoden durch qualitative Aspekte und Alternativen zu verbessern. Ebenfalls aus dieser Zeit stammen die Studien des Club of Rome „Die Grenzen des Wachstums“ [Mead72] und „Menschheit am Wendepunkt“ [Pest74]. Diese Studien werden oft als Szenarien bezeichnet, waren jedoch quantitativ orientiert. In ihnen wurden zum ersten Mal komplexe Zusammenhänge und Wechselwirkungen konsequent aufgezeigt – Ziel der Autoren war es laut eigener Aussage nicht, Recht zu behalten, sondern die Verantwortlichen aufzurütteln, um die beschriebenen Szenarien zu verhindern [Reib87].

Nach der Ölkrise gewann der Einsatz von Szenarien zusehends an Popularität und wurde schließlich zum unverzichtbaren Planungsinstrument in den USA und Europa. Bis zum heutigen Zeitpunkt hat sich die Szenario-Analyse in der strategischen Planung zunehmend etabliert, allerdings hat sich bis heute weder eine standardisierte Vorgehensweise noch eine einheitliche Definition durchgesetzt [Reib87].

3.3 Definition ‚Szenario’

Kahn und Wiener definieren Szenarien folgendermaßen:

„…hypothetical sequences of events constructed for the purpose of focusing attention on casual processes and decision points. They answer two kinds of questions: (1) Precisely how might some hypothetical situation come about, step by step? And (2) What alternatives exist, for each actor, at each step, for preventing, diverting or facilitating the process?“ [KaWi67]

Nach dieser Definition hat ein Szenario prozessualen Charakter, d.h. es stellt einen möglichen Weg hin zu einer zukünftigen Situation dar. Dieser Prozessorientierung steht die zustandsorientierte Definition von Szenarien als konsistente Beschreibung möglicher zukünftiger Situationen gegenüber. In den meisten Definitionen jedoch werden Szenarien als Verbindung beider Aspekte beschrieben – sowohl als Beschreibung einer zukünftigen Situation als auch als Entwicklungsverlauf, der zu dieser Situation führt.

Ausgehend von dieser Definition, die in Deutschland wesentlich in den 80er Jahren von den Mitarbeitern des Battelle-Instituts geprägt wurde [Reib87], können nach verschiedenen Kriterien verschiedene Arten von Szenarien unterschieden werden. Allgemein lassen sich vier Hauptbereiche unterscheiden [GeWi89]:

- Globalszenarien (Weltpolitische Entwicklungen, Welthandel)
- Branchenszenarien
- Technologieszenarien
- Unternehmensspezifische Strategieszenarien

Es gibt noch zahlreiche weitere Unterscheidungskriterien:

- Unterscheidung nach Art der verwendeten Daten in quantitative, qualitative und gemischte Szenarien [Beck88]. Da der Vorteil der Szenario-Analyse jedoch gerade in der vermischten Verwendung qualitativer und quantitativer Daten liegt, ist diese Einteilung weniger nutzbringend.
- Unterscheidung anhand des grundlegenden Szenario-Charakters in normative und deskriptive Szenarien [Bijl92]. Normative Szenarien projizieren einen Zustand und konstruieren rückwärts einen möglichen Verlauf, wie dieses Szenario vom heutigen Zustand aus erreicht werden kann. Deskriptive Szenarien arbeiten genau gegenläufig; hier wird die aktuelle Situation auf verschiedenen Wegen weiterentwickelt bis zu alternativen Ergebnissen in Form von Zukunftsszenarien.

- Unterscheidung nach der Eintrittswahrscheinlichkeit eines Szenarios [Schn87]. Bei dieser Klassifikation wird meist ein Szenario, das so genannte Referenz-Szenario, als wahrscheinlich eingestuft, während alle anderen Szenarien als weniger wahrscheinlich gelten.
- Unterscheidung nach dem Geltungsbereich des Szenarios in Umfeldszenario und Untersuchungsfeld-Szenario [Schn87]. Das Umfeldszenario beschreibt hierbei die möglichen Entwicklungen im Umfeld des Untersuchungsgegenstandes; das Untersuchungsfeld-Szenario beschreibt die Wirkungen des Umfelds auf den Untersuchungsgegenstand sowie Maßnahmen für Handlungsalternativen.

3.4 Methoden der Zukunftsforschung

Es gibt viele verschiedene Methoden der Zukunftsforschung – etwa 200 mehr oder weniger unterschiedliche Konzepte sind bekannt, die aber in ihren Anforderungen zu stark differieren, als dass man sie eindeutig systematisieren könnte. Für Datengewinnung, Erklärungen und die Darstellung von Zusammenhängen sind die Dimensionen quantitativ und qualitativ wichtig für die Methodenwahl. Bei vielen Zukunftsstudien spielen manchmal eher heuristische, analytische oder intuitive Zugänge bei der Erarbeitung von Zukunftswissen eine Rolle. Unterschiedliche Zeithorizonte und gesellschaftliche oder geographische Reichweiten erfordern unterschiedliche methodische Ansätze. Normative, kreative und prospektive Elemente sind besonders wichtig bei der Erstellung von Zukunftsbildern oder -strategien. Angesicht der Differenziertheit und Vielfältigkeit der Anforderungen an die Methodik sind die folgenden Tendenzen und Grundsätze von Relevanz, die sich in den letzten Jahrzehnten herausgebildet haben.

Einfache Extrapolationen und Analogietechniken werden mehr und mehr von komplexeren Prognose- und Prospektivverfahren zur Erstellung von

Zukunftsbildern abgelöst. Qualitative Forschungsansätze nehmen einen immer größeren Raum ein, während quantitative Methoden zunehmend zurückhaltender eingesetzt werden. Explorative Verfahren, projektive Techniken und normative Vorgehensweisen zur Modellbildung prägen heute einen großen Teil der Zukunftsforschungsmethodik [Krei06].

Es lassen sich vier grundlegende Vorgehensweisen in Bezug auf Explikation und Nutzung von Zukunftswissen hervorheben [Krei06]:

- Exploratives empirisch-analytisches Vorgehen: Ausgehend vom Bestand gespeicherten Wissens sowie von neuen Tatsachen, Daten und Trends werden wahrscheinliche und mögliche Entwicklungen unter genau bestimmten Annahmen und Voraussetzungen systematisiert und nach spezifischen Regeln analysiert. Das kann in qualitativer und quantitativer Form erfolgen.
- Normativ-intuitives Vorgehen: Erfahrungen und Sachinformationen, die im Allgemeinen empirisch-analytisch gewonnen wurden, werden in Zukunftsstudien und Zukunftsprojekten mit Phantasie und Kreativität zur Erstellung von Zukunftsbildern bzw. wünschbaren Zukunftsprojektionen verdichtet.
- Planend-projektierendes Vorgehen: Wissens- und Erfahrungsbestände werden im Hinblick auf Zukunftsziele und Zukunftsstrategien für die Umsetzung in die (politische, ökonomische oder gesellschaftliche) Praxis so aufbereitet, dass Kommunikations-, Entscheidungs-, Partizipations- und Implementierungsprozesse zur Zukunftsgestaltung durch wissenschaftliche Konzepte, Zukunftsprojekte und Maßnahmenempfehlungen unterstützt werden.
- Kommunikativ-partizipativ gestaltendes Vorgehen: Die Einbeziehung von Akteuren aus gesellschaftlichen Praxisbereichen erhöht den Gehalt an Zukunftswissen, die Phantasie und die Kreativität bei der Erstellung von Zukunftsbildern und führt insbesondere die Aspekte der Wünschbarkeit, Gestaltbarkeit und

Umsetzung in den Prozess von Zukunftsforschung und Zukunftsgestaltung ein. Die Zukunftsforschung verfügt mittlerweile über ein breites Spektrum von Diskurs-, Kreativitäts- und Konsensfindungsmethoden, durch die vor allem Nichtexperten, Betroffene und Beteiligte sowie Meinungs- und Entscheidungsträger einbezogen werden können [Krei06].

Allerdings lassen sich nur wenige Methoden der Zukunftsforschung klar einem der vier genannten Gebiete zuordnen; die meisten Methoden nutzen Elemente mehrerer oder aller Bereiche. Einige wichtige Zukunftsforschungsmethoden sind etwa: Trendanalyse/-extrapolation, Analogietechnologie, Fragebogentechnik, Delphi-Methode, Cross-Impact-Analyse, Modellbildung und Simulation, Brainstorming, Szenario-Methode, Rollenspiel oder Kreativitätsmethode.

3.4.1 Vorstellung verschiedener Methoden

Im Folgenden werden verschiedene ausgewählte Methoden der Zukunftsforschung genauer erläutert. Die Auswahl erfolgte derart, dass ein möglichst großes Spektrum verschiedener populärer Ansätze vorgestellt und ein breiter Überblick gewährt wird. Die vorgestellten Methoden gehören zu den wichtigsten der modernen Zukunftsforschung. Zudem entsprechen sie den fünf von Porter et al. unterschiedenen Hauptbereichen für die technologische Vorhersage, denen sich nach deren Auffassung alle Methoden zuordnen lassen. [Port91]

3.4.1.1 Delphi-Methode

Die Idee der 1964 von der RAND-Corporation entwickelten Delphi-Methode gründet auf den so genannten Delphi-Effekt. Dieser bezeichnet das Phänomen, dass die gemittelte Meinung einer Masse von gleich kompetenten Beobachtern zuverlässigere Vorhersagen ergibt als die

Meinung eines zufälligen Individuums [Raym97]. Dementsprechend ist die Delphi-Methode ein systematisches Befragungssystem, in dem eine ausgewählte Gruppe von Experten einen Fragenkatalog des betreffenden Fachgebiets erhält. Die schriftlichen Antworten werden mittels einer speziellen Mittelwertbildung zusammengefasst und den Fachleuten erneut anonym vorgelegt. Die neuen Daten werden von den Experten diskutiert und verfeinert. Dieser Prozess wird mehrfach in verschiedenen Stufen wiederholt und resultiert in einer aufbereiteten Gruppenmeinung, die die Aussagen selbst und Angaben über die Bandbreite vorhandener Meinungen enthält.

Die Strategie der Delphi-Methode lässt sich wie folgt zusammenfassen: In einem mehrstufigen, teilweise rückgekoppelten Editierprozess werden durch Konzentration auf das Wesentliche und Zulassen statistischer fuzzyartiger Ergebnisse sichere und umfassende Aussagen ermittelt. Problematisch an dieser Methode ist die mangelnde Meinungsänderung der Experten in den zusätzlichen anonymen Befragungsrunden, so dass der Effekt der Zusatzrunden oft sehr gering ist.

Grundsätzlich werden zwei Varianten der Delphi-Methode unterschieden.
In der Standard-Delphi-Methode gibt es keinerlei Diskussionen unter den Experten; jegliche Kommunikation ist untersagt. Damit wird zwar einerseits verhindert, dass sich aufgrund ungewollter Gruppendynamik Tendenzen herausbilden; andererseits geht die Möglichkeit verloren, durch den kommunikativen Austausch Fehleinschätzungen zu verhindern.
Die Breitband-Delphi-Methode erlaubt den Experten frei miteinander zu kommunizieren, was eine Konsens-Bildung beschleunigt. Die Vor- und Nachteile sind gerade gegenteilig zu den oben beschriebenen der Standard-Delphi-Methode.

3.4.1.2 Modellbildung und Simulation

Die Methode der Modellbildung beschreibt den Vorgang des Abbildens von Teilstücken der Realität, um sie besser diagnostizieren und mit ihrer Hilfe Aussagen über die Zukunft prognostizieren zu können. Ein Modell im Sinne der Modellbildung ist ein abstraktes Abbild eines Systems, das stellvertretend für das System untersucht wird.

Die Modellbildung abstrahiert von der Realität, da diese zu komplex wäre, um sie angemessen zu untersuchen, und beschränkt sich auf die Abbildung der für die Untersuchung wesentlichen Elemente – das Modell muss nicht absolut, sondern nur hinreichend exakt sein. Die Wahl dieser Elemente hängt maßgeblich von der Problemstellung ab, die mit dem Modell behandelt wird.

In Simulationen werden Modelle erzeugt, an denen Experimente zur Analyse dynamischer Systeme durchgeführt werden. Ein konkreter Simulationsablauf mit konkreten Werten wird als Simulationsexperiment bezeichnet.

Modelle und Simulationen werden meist verwendet, wenn eine Untersuchung am realen System zum Beispiel aufgrund der entstehenden Kosten oder der bei einer solchen Untersuchung bestehenden Gefahren nicht möglich ist.

Simulationen unterliegen vier Paradigmen:

1. Prozessanalyse. Simulationen bilden keine statischen Momente ab, sondern beobachten den Verlauf eines Prozesses im Ganzen.
2. Abstraktion. Eine Simulation ist keine Beschreibung der Realität, sondern abstrahiert von dieser auf den benötigten Level.
3. Makro und Mikro. Simulationen sind nicht atomar zerlegbar, sondern funktionieren als Ganzes. Es werden sowohl Mikrokosmos als auch Makrokosmos modelliert.

4. Experimentell. Simulationen dienen nicht einfach dazu, Prozessabläufe zu beobachten, sondern ermöglichen es, die Prozesse – z.B. durch Veränderung der Eingangsdaten – zu manipulieren.

Es gibt zahlreiche verschiedene Simulationsformen wie z.B. Warteschlangenmodelle, Multiagentensysteme oder Weltmodelle. Ihnen allen sind grundsätzliche Grenzen gesetzt. Jede Simulation ist begrenzt durch die zur Verfügung stehenden Ressourcen: Energie (z.B. Rechenkapazität des Simulationscomputers), Zeit oder Geld. Dadurch, dass ein Modell möglichst einfach sein muss, um wirtschaftlich sinnvoll zu sein, stellen die Ergebnisse eine grobe Vereinfachung der Realität dar. Weiter liefert das Simulationsmodell nur in einem bestimmten Kontext auf die Realität übertragbare Ergebnisse; in anderen Parameterbereichen können die Ergebnisse schlichtweg falsch sein. Daher ist die Verifikation der Modelle für den jeweiligen Anwendungsfall ein wichtiger Bestandteil der Simulationstechnik. Mögliche weitere Beschränkungen erfährt ein Modell durch Ungenauigkeit der Ausgangsdaten oder subjektive Hindernisse wie mangelnden Informationsfluss über Produktionsfehler.

3.4.1.3 Monitoring

Monitoring dient der Untersuchung von Ereignissen während ihres Auftretens oder unmittelbar danach. Diese Methode dient der systematischen und objektiven Untersuchung bestimmter Aspekte verschiedener Informationen, wie Bücher, Magazine, Zeitungen, Interviews etc. Damit diese Methode verlässliche und gültige Daten liefert, bedarf es äußerst kompetenten Einsatzes. Außerdem lassen sich mit dieser Methode nur sehr kurzfristige Ereignisse vorhersagen. Monitoring-Methoden dienen der generellen Informationssammlung und sind letztendlich Grundlage jeder Zukunftsforschung als Ergänzung zu anderen Methoden.

3.4.1.4 Szenario-Analyse

Die Szenario-Analyse als Planungsmethode beruht auf der Entwicklung und Analyse in der Zukunft liegender Szenarien, die mögliche Zukünfte darstellen. Sie fokussiert auf die Analyse von Extremszenarien (positives und negatives Extremszenario) oder besonders relevanter/typischer Szenarien (Trendszenario).
Die bevorzugten Anwendungsbereiche der Szenario-Analyse sind Entscheidungsvorbereitung, die Orientierung hinsichtlich zukünftiger Entwicklungen und die Strategieentwicklung und -überprüfung. Außerdem wird die Szenario-Analyse auch verwendet im Krisen-, Kontinuitäts-, Projekt- und Risikomanagement.

Die übliche Darstellung geht vom so genannten Szenario-Trichter aus: die Engstelle des Trichters symbolisiert den aktuellen Zustand; je weiter sich der Trichter öffnet, umso mehr Zeit vergeht. Am Ende des Trichters liegt auf der Horizontalachse ein Trendszenario, an entgegen gesetzten Punkten auf dem Rand der Trichteröffnung ein positives (oben, *‚best case'*) und negatives (unten, *‚worst case'*) Extremszenario. Das Trendszenario stellt die zukünftige Entwicklung unter der Annahme stabiler Umweltbedingungen dar (*Ceteris paribus*). Da im Regelfall aber von stark schwankenden Umweltbedingungen und überraschenden Einflüssen ausgegangen werden muss, wird das Trendszenario in vielen Analysen vernachlässigt und der Fokus auf die Extremszenarien gelegt.

Der Ablauf der Szenario-Analyse wird in verschiedene Phasen eingeteilt. Es gibt viele konkrete Verwirklichungen der Theorie der Szenario-Analyse, in denen zahlreiche unterschiedliche und unterschiedlich viele Phasen verwendet werden. Grob lassen sich die Phasen dennoch wie folgt einteilen:

1. Situationsanalyse. Der Untersuchungsgegenstand wird festgelegt und Problem- und Aufgabenstellung beschrieben. Anschließend

werden Faktoren ermittelt, die den Untersuchungsgegenstand beschreiben und einen Einfluss auf ihn oder zukünftige Szenarien nehmen können.

Output dieser Phase ist die Faktorenliste.

2. Einflussanalyse. In dieser Phase wird der wechselseitige Einfluss der verschiedenen, in Phase 1 erarbeiteten Faktoren untersucht und in einer Vernetzungstabelle festgehalten. Man unterscheidet verschiedene Einflussstufen (kein, niedrig, hoch). Anschließend lassen sich die Faktoren in passive (werden nur beeinflusst) und aktive (beeinflussen selbst) gruppieren und in einer Einflussmatrix miteinander vergleichen.

   Output dieser Phase sind die Vernetzungstabelle und die Einflussmatrix.

3. Trendprojektion und Szenarioermittlung. Zunächst werden die unterschiedlichen Entwicklungsmöglichkeiten der einzelnen Faktoren ermittelt. Durch mathematische Kombination unterschiedlicher Faktoren werden verschiedene mögliche Szenarien erzeugt. Da einige Kombinationen nicht sinnvoll sind oder sich ausschließen, andere aufgrund ihrer Ähnlichkeit oder Bedeutung zusammengefasst werden können, erfolgt eine Bündelung der Alternativen und damit eine Beschränkung der möglichen Szenarien. Man sollte als Untersuchungsgegenstand für den weiteren Verlauf die zwei Extremszenarien wählen, die in den meisten Punkten gegensätzlich sind.

   Output dieser Phase sind die möglichen Ausprägungen der einzelnen Faktoren sowie eine Beschreibung der Szenarien mit jeweiliger Faktorausprägung.

4. Bewertung und Interpretation. Die ausgewählten Szenarien werden in dieser Phase bezüglich ihrer Eintrittswahrscheinlichkeit sowie den mit ihnen verbundenen Chancen und Risiken gegenübergestellt.

Nach dieser Betrachtung können Maßnahmen definiert werden, mit denen man sich für die Szenarien rüsten kann.

Output dieser letzten Phase ist die Bewertung und Gegenüberstellung der ausgewählten Alternativen, sowie eine Nachbearbeitung und Interpretation, die die zu ergreifenden Maßnahmen erklärt.

3.4.1.5 Trendextrapolation

Die Trendextrapolation ist eine Prognosetechnik, bei der ein bereits beobachteter Trend mittels mathematischer und statistischer Analysen in die Zukunft fortgeschrieben wird. Die Zeit wirkt hierbei als zusammengefasster Ursachenkomplex aus verschiedenen Variablen auf die abhängige Variable ein. Der Trendextrapolation liegt immer die Annahme zugrunde, dass die ermittelte Gesetzmäßigkeit auch in der Zukunft ihre Gültigkeit behält. Diese Annahme ist zugleich der Nachteil dieser Methode. Zukünftige Ereignisse, die den Trend stark beeinflussen oder gar umkehren könnten, werden nicht berücksichtigt.

3.4.2 Wahl der Methode

Die Eignung einer Methode muss grundsätzlich anhand der Aufgabenstellung sowie deren Zielsetzung geprüft werden. Eine inhaltliche Zielsetzung dieser Arbeit ist es, Anregungen für die langfristige Forschungsplanung zu geben. Die Aufgabe besteht in der Untersuchung, welche Faktoren die Technik und den Einsatz digitaler Signaturen in der Zukunft beeinflussen und welche möglichen Entwicklungen für diese Faktoren langfristig denkbar sind, sowie explizit im Entwurf eines Szenarios. Betrachtet man den Untersuchungsgegenstand elektronische Signaturen, so handelt es sich um ein sicherheitskritisches Forschungsgebiet, das beständig weiterentwickelt werden muss, um neuen, dem Angriff auf elektronische

Signaturen dienenden Forschungen entgegen zu steuern. Einflussfaktoren von elektronischen Signaturen sind sowohl quantitativer als auch qualitativer Natur. Eine geeignete Methode muss daher die Berücksichtigung qualitativer Informationen berücksichtigen. Das Umfeld, in dem elektronische Signaturen eingesetzt werden, ist sehr vielfältig und dynamisch. Auch diese Eigenschaften müssen von der gewählten Methode berücksichtigt werden. Darüber hinaus schränkt der langfristige Zeithorizont, der für diese Untersuchung angestrebt wird, die Auswahl an Methoden weiter ein.

Die Methode des Monitoring ist für diesen langfristigen Zeithorizont ungeeignet; als Grundlage zur Informationsbeschaffung ist sie ohnehin ergänzend in jeder anderen Methode enthalten. Die Methoden der Trendextrapolation und der Modellbildung berücksichtigen lediglich quantitative Informationen. Vor allem die Trendextrapolation ist für eine dynamische, sich schnell ändernde Umwelt unpassend, da die Trendextrapolation auf der Annahme gleich bleibender Bedingungen beruht. Der entscheidende Nachteil des Simulationsmodells liegt nicht im Modell selbst, sondern in den Möglichkeiten des menschlichen Gehirns, das die erhaltenen Informationen auswerten muss: bei aller Intelligenz ist das Gehirn nicht in der Lage, so viele komplexe und vielschichtige Situationen zu verarbeiten, zu bewerten und zu einem Gesamtbild zusammen zu fügen, das als Entscheidungs- und Planungsgrundlage dienen kann. Innerhalb der Szenario-Analyse können Simulationen eingesetzt werden, um Störereignisse zu simulieren – Simulationsmodelle können in ihrer Komplexität Vernetzungen und Wechselwirkungen aufzeigen, die sonst eventuell nicht oder nicht richtig erkennbar wären.

Eine weitere inhaltliche Zielsetzung dieser Arbeit ist es, eine Kommunikationsgrundlage für verschiedene Akteure im Forschungsprozess zu erstellen. Aufgrund ihrer ganzheitlichen Sichtweise und ihrer anschaulichen Beschreibung möglicher Zukünfte ist die Szenario-Analyse der Delphi-Methode überlegen.

Außerdem ermöglicht die Szenario-Analyse die Integration verschiedener Methoden. Mit dem Ziel, ein besseres Verständnis der verschiedenen Faktoren zu bekommen, will die Zukunftsforschung zukünftige Entwicklungen auf dem jeweils betrachteten Gebiet beeinflussen. Es ist möglich und sinnvoll, verschiedene Methoden gleichzeitig anzuwenden, da dies die Gewinnung unterschiedlicher Informationen erleichtert. Verwendet man verschiedene Methoden zur Informationsgewinnung, so bedarf es einer methodischen Unterstützung zur Integration der Informationen zu einem Gesamtbild. Diese Integrationsmöglichkeit ist durch die Anwendung der Szenario-Analyse gegeben – als Gesamtbild erhält man schließlich die Szenarien.

Vergleicht man die Szenario-Analyse mit konventionellen Methoden wie z.B. der Trendextrapolation, die ausgehend von einer quantitativen Beschreibung des Ist-Zustands mittels mathematischer und statistischer Berechnungen und Analysen einen zukünftigen Zustand prognostizieren, so ist auch die Berücksichtigung quantitativer und qualitativer Informationen sowie das Einbeziehen externer Einflussfaktoren bei der Szenario-Analyse als Vorteil zu nennen. Im Gegensatz zu klassischen Prognosen akzeptiert die Szenario-Analyse Unsicherheiten über zukünftige Entwicklungen und bezieht diese Unsicherheiten mit in die Szenarioerstellung ein.

„Scenario writing is based on the assumption that the future is not merely some mathematical manipulation of the past, but the influence of many forces, past, present and future can best be understood by simply thinking about the problem.“ [Schn87]

Schließlich liegt ein weiterer Grund für die Überlegenheit der Szenario-Analyse gegenüber klassischen Verfahren in der Berücksichtigung verschiedener Alternativen, die lediglich eine einzige Annahme treffen müssen. Während dies in relativ stabilen Zeiten ausreichend ist, versagt diese Form der Zukunftsforschung in einer dynamischen, sich ständig wandelnden Umwelt: Erweist sich die getroffene Annahme als falsch, ist die gesamte Prognose hinfällig. Ziel der Szenario-Analyse ist nicht die exakte

Vorhersage der zukünftigen Entwicklung, sondern vielmehr sollen verschiedene mögliche Entwicklungen aufgezeigt werden.

Die Möglichkeit der Verarbeitung quantitativer und qualitativer Informationen in Kombination mit der Einbeziehung gegensätzlicher Alternativen macht die Szenario-Analyse äußerst flexibel. Ihre hohe Anschaulichkeit hilft bei der Vermittlung der Arbeitsweise und der Ergebnisse. Aufgrund dieser Überlegenheit gegenüber anderen Methoden wurde die Szenario-Analyse ausgewählt, um die zukünftige Entwicklung elektronischer Signaturen zu prognostizieren. Im folgenden Unterkapitel wird diese Methode detailliert in ihren einzelnen Arbeitsschritten erläutert, bevor in Kapitel 4 ihre Anwendung auf den Einsatz und die Entwicklung elektronischer Signaturen erfolgt.

3.4.3 Im Detail: Szenario-Analyse

Die Szenario-Analyse lässt sich anhand des so genannten Szenario-Trichters anschaulich erklären. Der engste Punkt des Trichters symbolisiert die Gegenwart. Je weiter man sich von diesem Punkt entfernt, umso größer werden Unsicherheit und Komplexität: der Trichter öffnet sich immer weiter. Bezogen auf die Gegenwart sind die Einflussfaktoren festgeschrieben und haben eine bestimmte Struktur, die erfassbar ist und deren Einflüsse im Augenblick für die gegenwärtige Aktivität genutzt werden können.
Versucht man, diese Faktoren auf die nähere Zukunft zu projizieren, so zeigt sich, dass sie sich teilweise, allerdings meist nicht signifikant, verändern. Dies gilt jedoch nur für einen vergleichbar kurzen Zeitraum von zwei bis drei Jahren. Versucht man nämlich – und dies ist für die strategische Planung meist erforderlich – diese Faktoren weiter in die Zukunft zu projizieren, kommt man sehr schnell an den Punkt, an dem man nicht mehr sicher sein kann, wie sich die Situation weiter entwickeln wird, welche

neuen Faktoren auftreten und welche Auswirkungen diese neuen Faktoren haben.

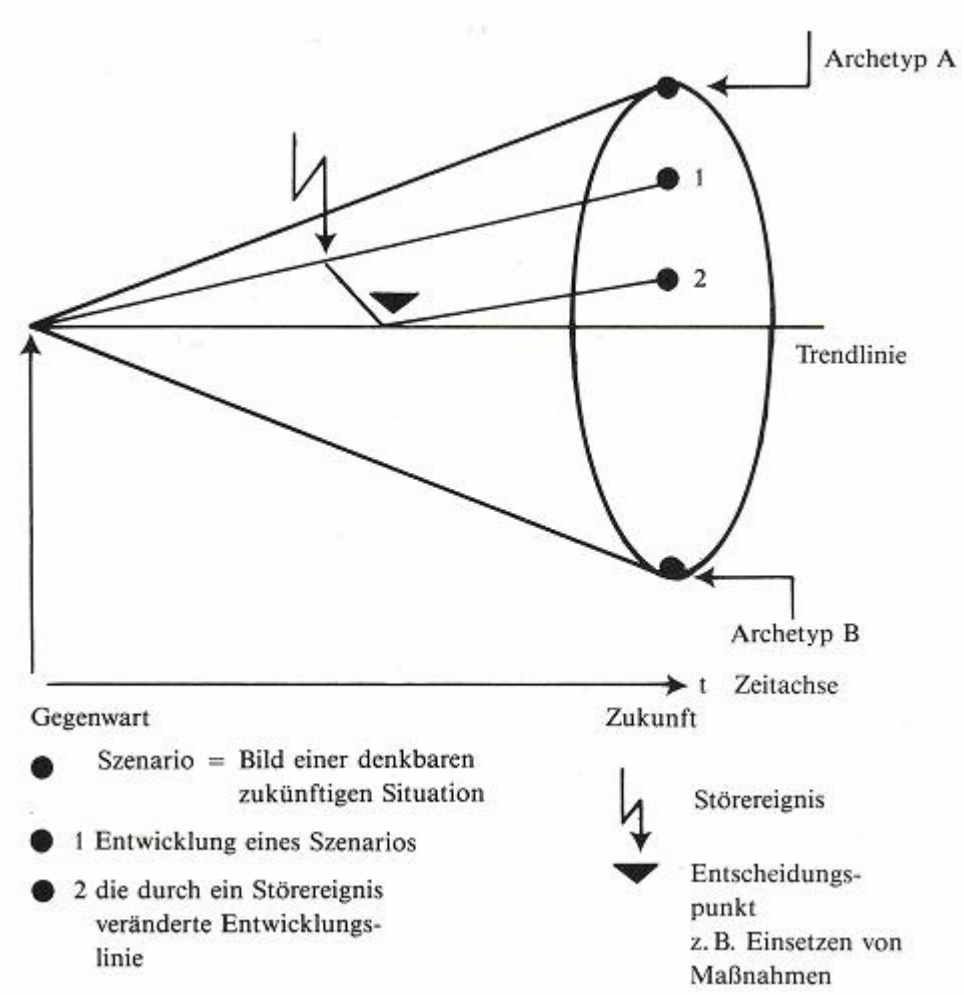

Abbildung 8: Denkmodell zur Darstellung von Szenarien [Reib91]

Zieht man an einer beliebigen Stelle einen senkrechten Schnitt durch den Trichter, dann liegen alle zu diesem Zeitpunkt denkbaren, theoretisch möglichen Zukunftsszenarien auf der Schnittfläche. Aus dieser unendlich großen Zahl möglicher Zukunftssituationen müssen jene herausgefiltert werden, die weiter untersucht werden sollen.

Shell als Pionier der Szenario-Entwicklung hat bereits Anfang der 70er Jahre erkannt, dass zwei Szenarien völlig ausreichen, sofern sie einigen Kriterien entsprechen [Reib87]:

- Größtmögliche Stimmigkeit, Konsistenz und Widerspruchsfreiheit innerhalb eines Szenarios,
- Größtmögliche Stabilität eines Szenarios und
- Größtmögliche Zahl an Unterschieden zwischen den beiden gewählten Szenarien.

Die beiden so erhaltenen Szenarien sind so genannte Szenario-Archetypen.
Es gibt auch die Möglichkeit, zusätzlich mit einem dritten Szenario zu arbeiten, dem so genannten Trend-Szenario. Dieses Szenario ist eine Fortschreibung der heutigen Situation in die Zukunft, entspricht also einer einfachen Trend-Extrapolation, und hat damit dieselben Nachteile, weshalb in dieser Arbeit von der Untersuchung eines Trend-Szenarios Abstand genommen wird.

Eine wichtige Besonderheit der Szenario-Methode ist die Möglichkeit, Störereignisse – überraschend und abrupt auftretende, den Trend beeinflussende Ereignisse – in den Planungsprozess mit einzubinden. Ermittelte mögliche Störereignisse können direkt in die Szenarioentwicklung mit einfließen, so dass Präventivmaßnahmen sowohl zur Verhinderung dieser Ereignisse als auch – so sie sich nicht verhindern lassen – zum Umgang mit ihnen frühzeitig entwickelt und ergriffen werden können.

Der entscheidende Punkt in der Szenariobetrachtung ist die Konsequenzanalyse aus der Zukunft für die Gegenwart. Es gilt, nicht wie üblich die Zukunft aus der Vergangenheit zu extrapolieren, sondern bewusst aus den Informationen und Kombinationen zukünftiger Entwicklungen Chancen und Risiken abzuleiten und Aktivitäten hierfür zu entwickeln, um besser für die Unsicherheiten und Veränderungen der Zukunft gerüstet zu

sein. Die für beide Szenarien entwickelten Aktivitäten müssen anschließend in einen Maßnahmenkatalog integriert werden – eine flexible, robuste Strategie, die in jedem Fall unter den Rahmenbedingungen beider Szenarien erfolgreich realisiert werden kann.

3.4.3.1 Die acht Stufen des Szenario-Prozesses

Die komplette Szenario-Methode, von der Aufgabenanalyse über die Szenarioerstellung bis hin zur Interpretation, lässt sich in acht aufeinander folgende Schritte untergliedern [Reib91].

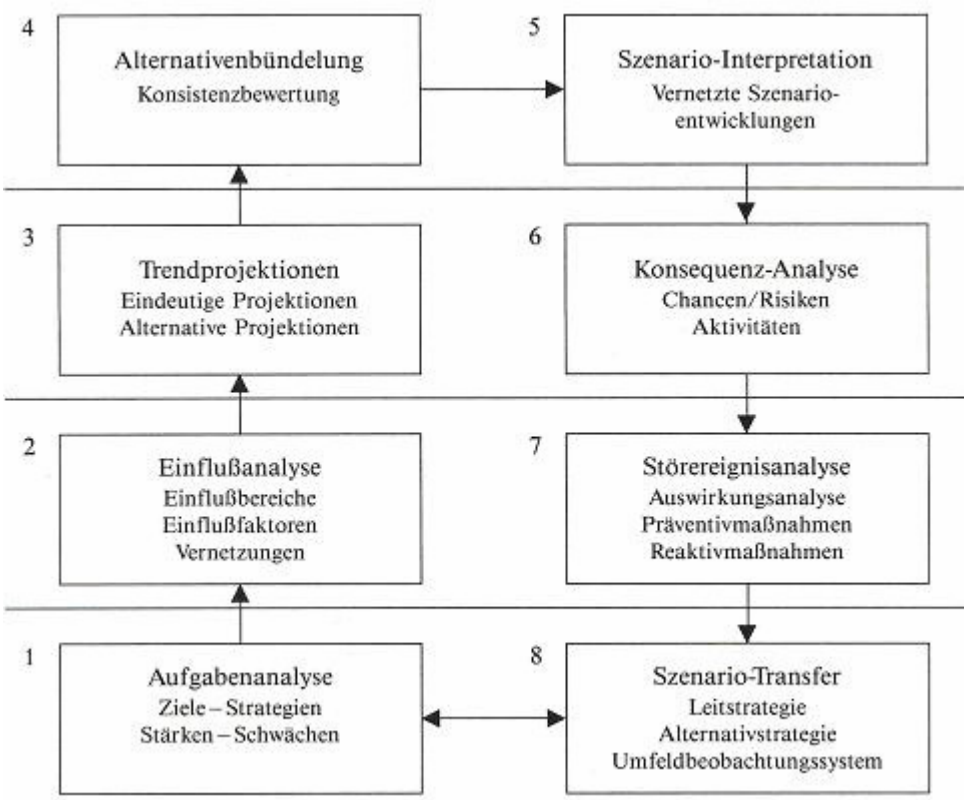

Abbildung 9: Die acht Schritte der Szenario-Technik [Reib91]

Schritt 1: Aufgabenanalyse

Ziel des ersten Schrittes ist es, den Untersuchungsgegenstand zu ermitteln und in der gegenwärtigen Situation zu analysieren.

Noch vor dem ersten Schritt erfolgt die Bildung des Szenarioteams. Dieses soll im Idealfall aus 10-20 Fachexperten sowie einem geschulten Moderator bestehen [Reib87].
Erste Aufgabe des Szenarioteams ist es, folgende Daten des Untersuchungsgegenstandes zu ermitteln: die aktuelle Form des Untersuchungsgegenstandes; die Idee, die hinter seinem Einsatz steht (Leitbild); die verfolgten Ziele und Strategien (ggf. zusätzlich unterteilt in kurz- (bis 5 Jahre), mittel- (bis 10 Jahre) und langfristig (mehr als 10 Jahre)); eine Stärken-/Schwächen-Analyse sowie die Rahmenbedingungen, unter denen der Untersuchungsgegenstand Anwendung findet.
Nach Analyse dieser Daten muss geprüft werden, ob das ursprünglich definierte Thema übernommen werden kann oder aufgrund der vorgenommenen Analyse modifiziert werden muss. Schließlich muss der Zeithorizont der Untersuchung festgelegt werden.

Schritt 2: Einflussanalyse
Ziel des zweiten Schrittes ist es, externe Einflussbereiche, die auf den Untersuchungsgegenstand einwirken, festzulegen. Die in diesen Einflussbereichen enthaltenen Einflussfaktoren werden ermittelt und anschließend bewertet und vernetzt, um eine Aussage über die Systemdynamik des Umfeldes zu erhalten.

Ein Untersuchungsgegenstand ist üblicherweise vielen Einflussbereichen ausgesetzt. Dazu gehören unabhängig vom tatsächlich untersuchten Objekt zum Beispiel oft Gesetzgebung, technologischer Fortschritt oder Gesellschaft. Bei einer sehr komplexen Umfeldsituation können diese Einflussbereiche weiter unterteilt werden. Diese Einflussbereiche müssen zunächst identifiziert und in ihrer Struktur und Funktion voneinander abgegrenzt werden.
Die Einflussbereiche selbst enthalten unterschiedliche Einflussfaktoren, die unterschiedlich stark und nicht alle auf das Untersuchungsobjekt einwirken.

Daher müssen die konkreten Faktoren ermittelt werden. Einmal ermittelt können die Faktoren nach der Stärke ihres Einflusses bewertet und dadurch eine Rangfolge der Bereiche gebildet werden.
Nachdem die Analyse der einzelnen Einflussbereiche fertig gestellt ist (es darf keinerlei Überschneidungen bzgl. Funktion und Struktur zwischen den Bereichen geben), werden mit Hilfe der Vernetzungsmatrix die Einflüsse der einzelnen Bereiche aufeinander ermittelt, bei der links und oben alle Einflussbereiche aufgeführt sind. Für jede Beziehung zweier Einflussbereiche wird einer von drei möglichen Werten vergeben: 0 bedeutet, dass der aktuelle linke Einflussbereich den ausgewählten oberen Einflussbereich nicht beeinflusst. Eine 1 wird vergeben, wenn der aktuelle linke Einflussbereich nur schwachen oder indirekten Einfluss auf den Zielbereich der oberen Zeile ausübt. Eine 2 schließlich bedeutet einen starken Einfluss.

Systemelemente	A	B	C	D	E	F	G	Aktiv-summe	
A	X	2	2	2	2	1	2	11	
B	1	X	1	1	0	0	0	3	
C	0	2	X	2	2	1	2	9	
D	0	2	2	X	2	1	1	8	
E	1	2	1	1	X	0	0	5	
F	0	1	0	0	1	X	0	2	
G	1	1	1	0	0	0	X	3	
Passivsumme	3	10	7	6	7	3	5	41	: 7 = 5,9

Abbildung 10: Vernetzungsmatrix [Reib91]

Addiert man die Werte einer Zeile auf, erhält man für den Einflussbereich, der links an dieser Zeile aufgeführt ist, die zugehörige Aktivsumme (die Stärke, mit der der Einflussbereich insgesamt auf die anderen Bereiche

einwirkt). Addiert man umgekehrt alle Werte einer Spalte auf, ergibt sich die Passivsumme (die angibt, wie stark der Einflussbereich von allen anderen Bereichen insgesamt beeinflusst wird) des am Spaltenkopf stehenden Einflussbereiches.
Es ist empfehlenswert, zusätzlich die Art des ausgeübten Einflusses sowie die Begründung der Einflussstärke festzuhalten, damit später die Analyse nachvollzogen werden kann.

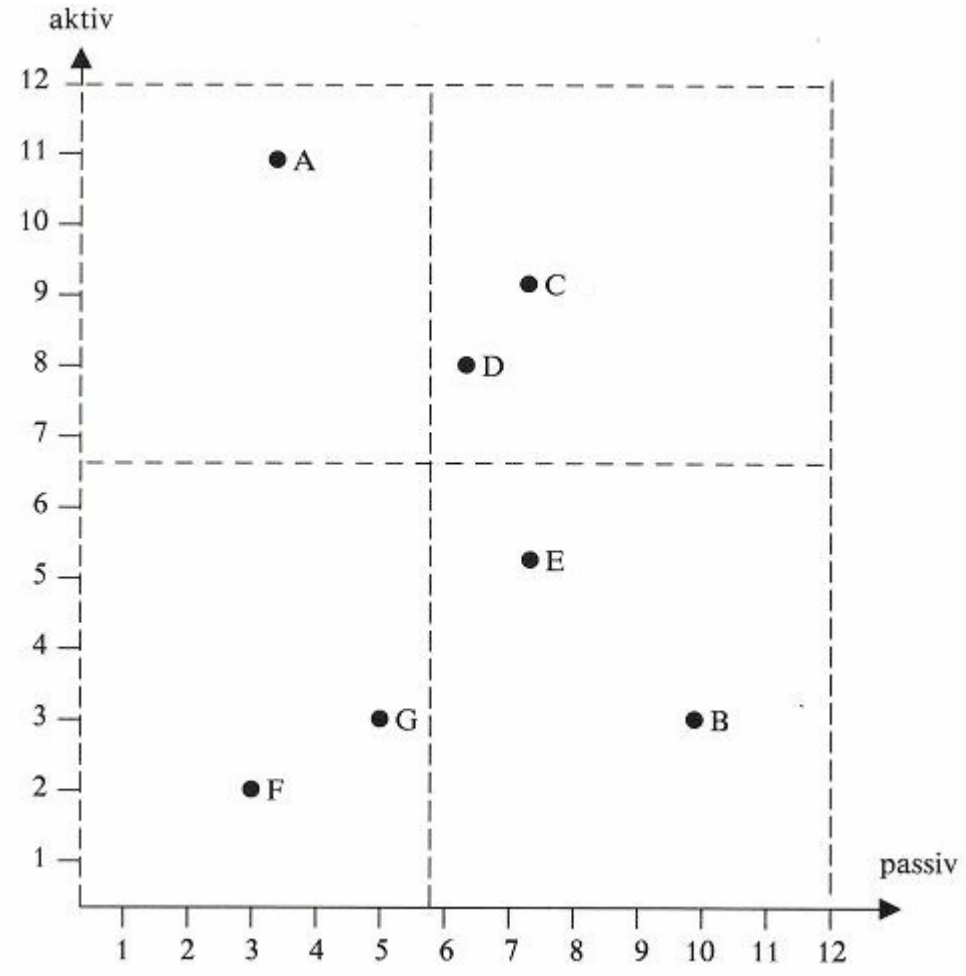

Abbildung 11: System-Grid mit eingetragenen Werten [Reib91]

Zusätzlich können die ermittelten Werte zur besseren Anschaulichkeit in ein Koordinatensystem übertragen werden, bei dem auf der X-Achse die Passiv-, auf der Y-Achse die Aktivwerte eingetragen werden. Durch die

Unterteilung der Passiv- und Aktiv-Achsen (abhängig von der Aktiv-/Passivsumme geteilt durch die Zahl der Einflussbereiche) wird das System in vier Felder eingeteilt.

Feld 1 (links oben) ist der Bereich der aktiven Einflussbereiche. Hier positionierte Bereiche zeichnen sich durch sehr hohe Aktivität und relativ niedrige Passivität aus. Die Aktivität gibt an, wie stark ein Bereich das System als Ganzes beeinflusst; umgekehrt gibt die Passivität an, wie stark ein Bereich vom System beeinflusst wird. Einflussbereiche in diesem Feld beeinflussen das System also sehr stark, ohne umgekehrt selbst stark vom System beeinflusst zu werden.

Feld 2 (rechts oben) ist das Feld der so genannten ambivalenten Einflussbereiche: sie zeichnen sich durch gleichermaßen hohe Aktivität und Passivität aus – diese Bereiche beeinflussen das System sehr stark und werden gleichzeitig sehr stark beeinflusst.

Feld 3 (links unten) ist das Feld der puffernden (niedrig ambivalenten) Einflussbereiche; Bereiche, die weder viel Einfluss ausüben, noch stark beeinflusst werden.

Feld 4 (rechts unten) schließlich enthält die passiven Einflussbereiche – sie üben kaum Einfluss auf das System aus, werden selbst aber stark beeinflusst.

Soll Einfluss auf ein System ausgeübt werden, so empfiehlt es sich, die aktiven Einflussbereiche zu verändern, da hier mit geringstem Aufwand die größtmögliche Wirkung erzielt werden kann. Umgekehrt würde eine Beeinflussung der passiven Elemente nur minimale Veränderungen am System hervorrufen, aber einen sehr großen Aufwand bei der Beeinflussung der Elemente erfordern.

Beeinflusst man Elemente in aktiven Einflussbereichen so, dass sie den eigenen Zielvorstellungen entsprechen, erzielt man die besten Synergieeffekte, d.h. in einer Kettenreaktion werden auch die anderen Systemelemente in gewünschter Weise beeinflusst. Daher ist es wichtig, dass sämtliche Aktivitäten dort angesetzt werden müssen, wo die größte Verstärkerwirkung im System erzielt werden kann. Dies sind in der Regel

die aktiven Einflussbereiche, oder ambivalente Bereiche mit einer deutlichen Aktivdominanz. Umgekehrt sollten passive und puffernde Elemente nach Möglichkeit nicht nur direkt, sondern auch indirekt über die aktiven Elemente beeinflusst werden, da sie von diesen abhängig sind.
Es wird leicht deutlich, dass somit Entwicklungen in Bereichen, die nicht direkt beeinflusst werden können, über andere, besser beeinflussbare Einflussbereiche gesteuert werden können. Es ist folglich sehr wichtig, eine sorgfältige Systemanalyse durchzuführen, um die komplexe Vernetzung der Elemente zu erkennen und sich selbst nutzbar zu machen. Grundsätzlich bietet sich eine solche Systemanalyse in allen Situationen an, in denen man mit einer sehr komplexen und nicht klar durchschaubaren Systemstruktur konfrontiert wird.

Schritt 3: Trendanalyse

Ziel dieses Schrittes ist es, auf der Basis der in Schritt 2 ermittelten Einflussfaktoren Deskriptoren zu ermitteln, die den jetzigen und zukünftigen Zustand der jeweiligen Entwicklungen beschreiben.

In diesem Schritt liegt der Schwerpunkt auf der wertneutralen Formulierung der Deskriptoren. Andernfalls besteht die Gefahr, dass bei der Szenarioentwicklung nicht in Alternativen, sondern nur in eine bestimmte Richtung gedacht wird. Würde man z.B. den nicht neutralen Begriff ‚Wirtschaftswachstum' statt ‚Wirtschaftsentwicklung' verwenden, so unterscheidet man automatisch in starkes oder weniger starkes Wachstum – korrekt wäre aber eine Unterscheidung in Wachstum und Schrumpfung!
Formulierte Deskriptoren müssen zunächst in ihrem Ist-Zustand beschrieben werden. Anschließend werden sie auf den nächsten Zeithorizont projiziert. Falls die Entwicklung eines Deskriptors zum neuen Zeithorizont eindeutig beschrieben werden kann, so erfolgt diese Beschreibung als nächstes und sollte begründet werden. Bestehen verschiedene Möglichkeiten der Zukunftsentwicklung, müssen die verschiedenen Alternativen aufgezeigt

und begründet werden. Man erkennt also, ob es sich um einen eindeutigen oder einen Alternativdeskriptor handelt.
Die Wahrscheinlichkeiten der jeweiligen Alternativen spielen in diesem Schritt keine Rolle.

Schritt 4: Alternativenbündelung
Ziel dieses Schrittes ist es, die verschiedenen in Schritt 3 erarbeiteten Alternativen auf Konsistenz und Logik untereinander zu prüfen.

In diesem Schritt wird eine detaillierte Problemanalyse mit Hilfe einer Konsistenzmatrix durchgeführt. Dazu werden folgende Bewertungen vergeben:

1. Wenn beide in einem Feld aufeinander treffenden alternativen Auswirkungen eines Deskriptors keine direkte Korrelation haben, wird eine 0 eingetragen. Besteht jedoch eine Beziehung zwischen zwei Alternativ-Ausprägungen, muss weiter untersucht werden:
2. Ist die Beziehung konsistent oder sind beide Ausprägungen widersprüchlich? Wenn sie konsistent ist, wird ein positiver Wert eingetragen, andernfalls ein negativer.
3. Ist die Beziehung konsistent, ohne dass sich die beiden Elemente gegenseitig verstärken, wird der Wert +1 eingesetzt. Liegt eine wechselseitige Verstärkung vor, ist der Wert +2.
4. Ist die Beziehung teilweise inkonsistent, wird der Wert -1 eingetragen; bei absoluter Inkonsistenz wird dagegen -2 eingetragen.

Nach dem Ausfüllen der Konsistenzmatrix, was mit detaillierter Begründung erfolgen sollte, müssen folgende Schritte ausgeführt werden:

- Berechnung aller theoretisch möglichen Szenario-Konstellationen.
- Aus diesen Auswahl der Szenarien mit größtmöglicher Konsistenz.
- Aus diesen Auswahl der Szenarien mit der größtmöglichen inneren Stabilität. Innere Stabilität bedeutet, dass sich diese Szenarien unter

Einfluss von Störungen nicht in Richtung einer größeren Konsistenz verbessern und damit über einen längeren Zeitraum Gültigkeit haben. Instabilität bedeutet umgekehrt, dass unter Einfluss von Störgrößen eine Verbesserung zu höherer Konsistenz erfolgt. Der Zweck der Planung besteht in der Generierung von stabilen und damit lange gültigen Szenarien.

- Aus diesen Auswahl von zwei Szenarien, die möglichst unterschiedlich sind, d.h. möglichst viele gegensätzliche Alternativen enthalten.

In vielen Problemsituationen können die Zielszenarien intuitiv-ganzheitlich ermittelt werden. Bei komplexen Problemen (mehr als ein Dutzend Deskriptoren) sollte entsprechende Software hinzugezogen werden.

Konsistenzmatrix			1		2		3		4		5		6		7		8		9		10		11	
			a	b	a	b	a	b	a	b	a	b	a	b	a	b	a	b	a	b	a	b	a	b
1) Neue Technologien	a)	Erfolg		x																				
	b)	Flop																						
2) Wirtschaftsentwicklung	a)	Wachstum	2	0																				
	b)	Rückgang	0	1		x																		
3) Strukturwandel	a)	Erfolg	2	−1	2	−1																		
	b)	Flop	−1	2	0	2		x																
4) Arbeitslosenquote	a)	höher	0	1	0	2	0	1																
	b)	niedriger	1	0	2	−1	1	0		x														
5) Einstellung der Gesellschaft zur Technik	a)	Akzeptanz	2	0		1	0		2	0	−1	1												
	b)	Ablehnung	−1	1	−1	1	−1	2		1	0		x											
6) Gesetzgebung	a)	liberal	1	0	1	0	0	0	0	0	0	0	0											
	b)	verschärft	0	1	0	1	0	0	0	0	0	0		x										
7)	a)															x								
	b)																							
8)	a)																	x						
	b)																							
9)	a)																			x				
	b)																							

Abbildung 12: Beispiel einer Konsistenzmatrix [Reib91]

Schritt 5: Szenario-Interpretation

Ziel dieses Schrittes ist es, auf der Basis der in Schritt 4 erfolgten Konsistenzanalyse unter Hinzuziehung der in Schritt 3 ermittelten Deskriptoren und unter Berücksichtigung der Ergebnisse aus der Vernetzungsanalyse die Szenarien auszugestalten und zu interpretieren.

In diesem Schritt erfolgt die Ausformulierung der Szenarien. Dies sollte vom Moderator alleine vorgenommen werden, der anschließend seine Ergebnisse der Gruppe zum Redigieren vorlegt.

Die Schwierigkeit dieses Schrittes liegt darin, dass die Szenarien sich nicht statisch in die Zukunft entwickeln, sondern eine Eigendynamik haben. Diese Veränderungen müssen bei der Interpretation berücksichtigt und verarbeitet werden. Gleichzeitig erhöht eine solche innere Dynamik die Plausibilität der Szenarien sowie die Identifikationsbereitschaft der Planer mit den Szenarien.

Ergebnis dieses Schrittes sind zwei konträre, aber in sich logisch-stimmige und plausible Zukunftsbilder. Es empfiehlt sich, an diesem Punkt erneut gemäß Schritt 2 eine Vernetzungsanalyse und ein Koordinatensystem für die jeweiligen Szenarien zu erstellen. Im Gegensatz zu Schritt 2 sind nun aber die Einflussfaktoren in ihrer unterschiedlichen Zukunftsprägung inhaltliche Grundlage für die Analyse. Dadurch lässt sich folgendes ermitteln:

1. Unterschied der Szenarien zur gegenwärtigen Situation und Dynamik der Weiterentwicklung von der Gegenwart in eine Zukunft A oder B.
2. Unterschied zwischen beiden Zukunftsszenarien und ihrer Systemdynamik.

Die Ergebnisse dieser Analyse werden in Schritt 8 zu den Parametern der Strategie rückgekoppelt um sicher zu stellen, dass die Strategie hauptsächlich auf dem Systemverhalten der aktiven Einflussbereiche aufbaut und diese optimal ausgenutzt werden.

Schritt 6: Konsequenzanalyse

Ziel dieses Schrittes ist es, auf Basis der Szenarien mögliche Chancen und Risiken abzuleiten, diese zu bewerten und sie mit geeigneten Maßnahmen zu versehen.

Chancen und Risiken bilden die Brücke zwischen den beiden Szenario-Aussagen und dem Untersuchungsgegenstand. Die Aktivitäten beinhalten, dass Chancen so früh wie möglich genutzt und Risiken soweit möglich vermindert werden. Bei Szenarien mit mehreren Zeithorizonten muss zusätzlich berücksichtigt werden, ob die Chancen und Risiken kurz-, mittel- oder langfristig relevant sind. Außerdem wird bewertet, wie wichtig Chancen und Risiken in Bezug auf den Untersuchungsgegenstand sind.
Dieser Schritt ist der wichtigste für die Planung, da eine zukunftsorientierte Stoffsammlung entwickelt werden muss, auf deren Basis später die Strategie entwickelt wird. Wichtig ist hierbei die klare Trennung zwischen kreativer Aktivitätenentwicklung und späterer Bewertung der Aktivitäten. Weiterhin ist es wichtig, dass die aufgezeigten Aktivitäten konkret und detailliert sind.
Aus den unterschiedlichen Ergebnissen der Konsequenzanalyse (jeweils eine auf Basis jedes Szenarios) wird vom Moderator eine vorläufige Strategie generiert.

Schritt 7: Störereignisanalyse

Ziel dieses Schrittes ist es, mögliche externe und interne, abrupt auftretende Ereignisse, die den Untersuchungsgegenstand erheblich beeinflussen oder verändern können, zu sammeln, ihre Signifikanz zu bewerten und mit entsprechenden Präventiv- und Reaktivmaßnahmen zu versehen.

Eine Wahrscheinlichkeitsbewertung der verschiedenen Störereignisse sollte nicht vorgenommen werden. Die Wahrscheinlichkeit, mit der ein bestimmtes Störereignis eintritt, ist weitaus weniger von Belang als der tatsächliche Einfluss, den ein Störereignis ausübt. Gerade viele Ereignisse,

die aufgrund ihrer geringen Eintrittswahrscheinlichkeit vernachlässigt werden, verfügen über ein enormes Potential. Es finden sich in der jüngeren Geschichte zahlreiche Beispiele für solche Ereignisse wie z.B. die Öffnung Osteuropas oder die deutsche Wiedervereinigung.

Daher genügt es für die Auswahl von Störereignissen, sich auf die Signifikanzbewertung zu beschränken: Es werden nur solche Störereignisse ausgewählt, die einen entscheidenden Einfluss auf den Untersuchungsgegenstand nehmen können.

Nach der Auswahl dieser Störereignisse (die möglichst aus verschiedenen Bereichen stammen sollten) werden sie kurz definiert. Dies hilft, ihre Auswirkungen zu erkennen und Missverständnisse zu vermeiden.

Katastrophenartige Ereignisse (z.B. ein Weltkrieg) müssen in der Störereignisanalyse nicht berücksichtigt werden. Üblicherweise ist es ohnehin unmöglich, Präventiv- oder Reaktivmaßnahmen gegen ein solches Ereignis zu erarbeiten [Reib87].

Die Auswirkungsanalyse der Störereignisse wird wie folgt durchgeführt: Wenn ein Störereignis die Szenarien betrifft und verändert, werden sowohl die Auswirkungen auf die Szenarien als auch auf den Untersuchungsgegenstand selbst betrachtet. In solchen Fällen können sich Szenarien in eine andere Richtung entwickeln (gestörte Szenarien). Dann gilt es, sowohl die Auswirkungen der Szenario-Änderungen (indirekte Auswirkungen) als auch die direkten Auswirkungen des Störereignisses auf den Untersuchungsgegenstand zu berücksichtigen.

Präventivmaßnahmen bedeuten in erster Linie: Wie kann der betroffene Bereich den Störereignissen gegenüber stabiler oder immun gemacht werden? Gerade bei globalen Störereignissen ist eine Immunisierung meist nicht möglich, geeignete Maßnahmen können jedoch eine Krise verhindern.

Die Präventivmaßnahmen werden später in die Strategie integriert, damit sie auch tatsächlich umgesetzt werden können. Hierbei werden zunächst alle Präventivmaßnahmen verglichen. Maßnahmen, die gegen eine Reihe von Ereignissen helfen, werden mit größter Priorität in die Strategie integriert,

während solche, die nur gegen einzelne Ereignisse helfen, eine geringere Priorität erhalten.
Reaktivmaßnahmen auf Störereignisse entsprechen Krisenplänen. Tritt eines der berücksichtigten Störereignisse auf, wird sofort der entsprechende Krisenplan angewandt.

Schritt 8: Szenario-Transfer

Ziel dieses Schrittes ist es, auf der Basis der in Schritt 6 erarbeiteten Aktivitäten zu Chancen und Risiken Maßnahmen zu formulieren, eventuell Alternativstrategien festzulegen und ggf. ein Umfeldbeobachtungssystem zu etablieren.

Hierbei muss noch mal zu den Ergebnissen der Konsequenzanalyse rückgekoppelt werden. Auf der Basis gleichartiger und innovativer Aktivitäten wird jetzt eine Strategie formuliert.
Gleichartige Aktivitäten zu beiden Szenarien reichen jedoch nicht für eine fundierte Strategie aus. Es müssen also weitere, besonders innovative und attraktive Aktivitäten, die für ein Szenario entwickelt wurden, analysiert und ihre Anwendbarkeit auf das jeweils andere Szenario überprüft werden. Auf diesem Weg lassen sich etwa zwei Drittel der in Schritt 6 erarbeiteten Aktivitäten in den Maßnahmenkatalog integrieren. Gegebenenfalls ist eine Umformulierung der Aktivitäten vorzunehmen, um sie zu beiden Szenarien kompatibel zu machen. Hierbei ist darauf zu achten, dass der Innovationsgehalt einer Idee oder Aktivität beim Umformulieren nicht verloren geht. Die Aktivitäten, die als Rest zu den beiden Szenarien A und B übrig bleiben, bilden die Basis für die Alternativstrategien A und B. Diese Alternativstrategien sind eine Ergänzung bzw. Präzisierung der Strategien, falls das betreffende Szenario Realität wird. Alternativstrategien sind meist nur bei Szenarien mit einem Zeithorizont von 15 Jahren und mehr relevant; bei einem kürzeren Zeithorizont erübrigt sich die Entwicklung der Alternativstrategien in den meisten Fällen.

Weiter werden die in Schritt 7 erarbeiteten Präventivmaßnahmen zu Störereignissen in die Strategie integriert.

Anschließend werden die ermittelten Maßnahmen nach den verschiedenen Zielen eingeteilt, die angestrebt werden. Die Ordnung der Ziele wie auch der Maßnahmen, die zur Erfüllung eines Zieles verhelfen sollen, wird nach Priorität und unter Fristigkeitsaspekten vorgenommen. Diese Untergliederung hilft dabei, die Vielzahl strategischer Aspekte in eine geeignete zeitliche und prioritätsmäßige Struktur zu bringen.

Außerdem muss der Maßnahmenkatalog zu den auf Basis der Szenarien in Schritt 5 erarbeiteten Koordinatensystemen rückgekoppelt werden. Hierbei ist zu berücksichtigen, dass die Maßnahmen hoher Priorität vor allem die Kräfte der aktiven Bereiche nutzen und nicht nur auf passive Bereiche zielen. Dieser Überprüfungsschritt kann ggf. eine neue Gewichtung oder Verschiebung in der Akzentsetzung bewirken.

Schließlich wird der so ermittelte Maßnahmenkatalog erneut zur Ausgangssituation in Schritt 1 zurückgekoppelt. Es wird geprüft, in wie weit die in Schritt 1 gelisteten Ziele und Strategien mit den jetzt konzipierten Maßnahmen übereinstimmen. Schwächen, die das Erreichen bestimmter Ziele verhindern, müssen ebenso erkannt werden wie Stärken, die bei der Umsetzung behilflich sein können.

Als nächstes wird ein Umfeldbeobachtungssystem aufgebaut, das die für das Untersuchungsobjekt wichtigsten externen Entwicklungen (Deskriptoren in ihrer Alternativ-Entwicklung und eindeutigen Entwicklung) mit den Strategie-Aspekten verknüpft und die daraus resultierenden einflussstärksten Deskriptoren in ein Beobachtungssystem überführt. Aus der Korrelation, welche Faktoren für den Untersuchungsgegenstand wichtig sind, und der Analyse, welche Einflussfaktoren die größte Dynamik im System haben, ergibt sich eine Konzentration der Beobachtung auf die für den Untersuchungsgegenstand wichtigsten externen Faktoren. Darüber hinaus ist es Aufgabe der Beobachter, den Eintritt möglicher Störereignisse rechtzeitig zu erkennen.

Das Beobachtungssystem hat die Aufgabe, die aktuelle, tatsächliche Entwicklung der externen Faktoren mit dem Maßnahmenkatalog zu verknüpfen und gegebenenfalls bei Abweichungen diesen vorsichtig anzupassen.

3.5 Zusammenfassung: Zukunftsforschung

In diesem Kapitel erfolgte eine Einführung in die wissenschaftliche Disziplin der Zukunftsforschung. Nach der Erklärung einiger Begrifflichkeiten wurden verschiedene Methoden vorgestellt und eine von ihnen ausgewählt: die Szenario-Analyse. Es folgte eine detaillierte Untersuchung dieser in mehrere konsekutive Schritte unterteilten Methode.
Die Szenarioanalyse ist aus verschiedenen Gründen am Besten für die vorliegende Aufgabe geeignet, zu deren wichtigsten die Alternativenberücksichtigung, die Reaktionsmöglichkeit auf Störereignisse sowie die hohe Anschaulichkeit zählen. Ihr schrittweiser Aufbau macht sie äußerst leicht nachvollziehbar und ermöglicht es, bei veränderten Bedingungen eine neue Analyse unter Übernahme weiter Teile des schon vorhandenen durchzuführen.

4 Anwendung der Szenario-Analyse für Prognosen zur elektronischen Signatur

In den vorhergehenden Kapiteln wurden zunächst die Grundlagen der elektronischen Signatur und der Zukunftsforschung vermittelt, bevor aus der Vielzahl an Prognosemethoden die Szenario-Analyse aufgrund ihrer besonderen Eignung ausgewählt wurde. In diesem Kapitel werden die einzelnen zuvor beschriebenen Schritte der Szenario-Analyse auf den Untersuchungsgegenstand angewandt.

4.1 Aufgabenanalyse

Der Beginn der Szenario-Analyse wurde durch die Zusammenstellung des Expertenteams markiert. Die Literatur empfiehlt für die Durchführung einer Zukunftsforschungsmethode die Beteiligung von 10-20 Experten, die sich gemeinsam an einem Ort einfinden sollen. Als Experten gelten hierbei Personen, die sich in der Vergangenheit intensiv mit elektronischen Signaturen auseinander gesetzt haben oder aktuell, ggf. beruflich, damit beschäftigen [Albe01] [Reib87].

Diese Empfehlungen gelten auch im Fall der Szenario-Analyse. Abweichend davon wurde für die vorliegende Szenario-Analyse auf das Medium Internet ausgewichen; die gesamte Kommunikation fand über eMails statt. Grund hierfür war die sich damit bietende Möglichkeit, auf die körperliche Anwesenheit der Experten zu verzichten und einer größeren als der empfohlenen Zahl an Experten die Teilnahme zu ermöglichen. Dies war erforderlich, da sich aus persönlichen und zeitlichen Gründen nicht alle Experten über die gesamte Zeit an der Szenario-Analyse beteiligen konnten.

Nach ausgiebiger Recherche wurden knapp 40 Experten kontaktiert, darunter Universitätsprofessoren, Juristen und Angestellte sowohl aus der öffentlichen Verwaltung als auch aus der freien Wirtschaft. Die Auswahl der Experten erfolgte anhand der Themen und der Qualität ihrer im Internet

und in gedruckter Form veröffentlichten wissenschaftlichen Schriften sowie – insbesondere im Fall der Nicht-Akademiker – anhand ihres aktuellen Berufsfeldes.

Die Zahl der Experten, die sich letztlich an der Analyse beteiligten, lag allerdings nur bei neun zu Beginn der Arbeit und nahm schnell weiter ab. Die Beteiligung im folgenden Schritt 4.2 schwankte (je nach Teilschritt) zwischen zwei und sechs; ab Schritt 3 erfolgte keine Rückmeldung der Experten mehr. Die Analyse wurde ab diesem Schritt in Einzelarbeit durchgeführt.

Die Methodik der Vorgehensweise in dieser Szenario-Analyse entspricht einer formativen Szenario-Analyse, d.h. einer Abschätzung der Zusammenhänge, Einflussnahmen und Konsistenzen durch die Experten. Diese Vorgehensweise führt zu einem systematischen, nachvollziehbaren Vorgehen und verlässlicher Szenarienbestimmung, bei gleichzeitig großer Abhängigkeit von der Qualität der Experten. Diese Vorgehensweise ist dem einer holistischen Szenario-Analyse (intuitive Zusammensetzung der verschiedenen Szenario-Elemente mit dem Ergebnis beliebiger Szenarien) überlegen. Eine Modell-Szenarioanalyse (Ableitung der Konsistenzen aus einer Datenbank oder Modellrechnungen; führt zur verlässlichen Szenariobestimmung bei großer Abhängigkeit von der Qualität der vorhandenen Datenbank und Modelle sowie deren Gültigkeit für den gewählten Zeithorizont) war aufgrund fehlender Daten und Modellrechnungen nicht durchführbar [Tiet03].

Der erste Schritt der Szenario-Analyse dient der Einführung in das untersuchte Thema. Verschiedene die Technik und den Einsatz elektronischer Signaturen charakterisierende Fragen wurden gestellt und beantwortet. Ausgehend von persönlichem Wissen und Erfahrungen formulierte jeder Teilnehmer Fragen, die den Einsatz und die Entwicklung elektronischer Signaturen eingrenzen, treffend beschreiben und hinterfragen. Wichtige Anhaltspunkte waren dabei elementare Gegebenheiten wie

Einsatzgebiet, Häufigkeit der Verwendung sowie eine Betrachtung der Stärken und Schwächen. Anschließend erhielt jeder Beteiligte den vollständigen, vom Moderator zusammengefassten Fragenkatalog und gab wiederum aus seiner persönlichen Sicht und Erfahrung Antworten auf die formulierten Fragen. Eine breite Diskussion über die verschiedenen Fragestellungen war den Experten, die an der Diskussion parallel zu ihrer Berufstätigkeit teilnahmen, aus Zeitgründen nicht möglich. Die Antworten wurden vom Moderator zusammengefasst und ausformuliert. Kriterien für die abschließende Anordnung waren die aktuelle Bedeutung der Fragen und Antworten sowie ihre zu erwartende Bedeutung in der betrachteten Zukunft.

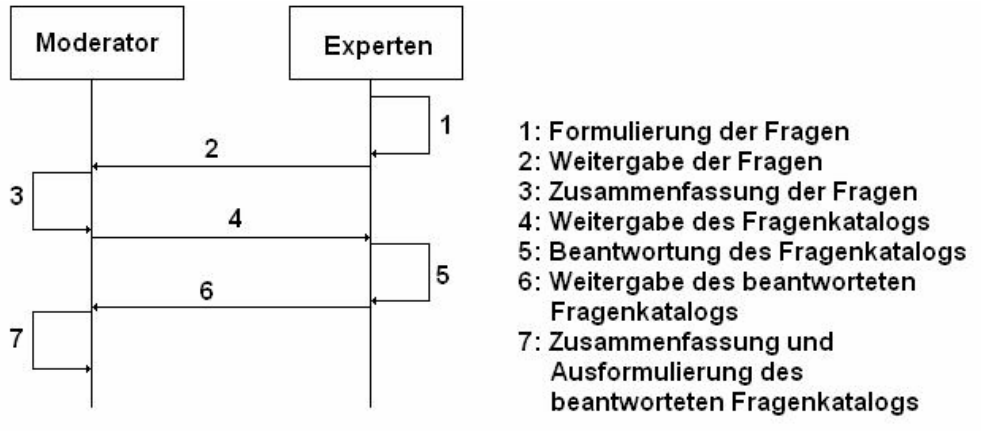

Abbildung 13: Ablauf der Aufgabenanalyse

Die zentrale Frage, die sich beim Analysieren der derzeitigen Situation elektronischer Signaturen stellt, ist die Frage nach der **Rolle, die elektronische Signaturen heute spielen**. Die sichere, aber aufwändige Form der qualifizierten elektronischen Signatur spielt in Deutschland zurzeit keine signifikante Rolle und findet nur geringfügige Verwendung. Im europäischen Ausland ist diese Rolle unterschiedlich stark ausgeprägt, mit Ausnahme von Dänemark wird die qualifizierte elektronische Signatur aber in keinem Land verstärkt eingesetzt [ADeV29] [Exp]. Andere, weniger sichere Formen der elektronischen Signatur (also die ‚einfache' und die fortgeschrittene elektronische Signatur) spielen eine größere, in der

Öffentlichkeit oft nicht wahrgenommene Rolle und finden zum Beispiel bei Webseiten oder Betriebssystemtreibern Verwendung [Exp]. Aufgrund der niedrigeren Anforderungen sind nicht qualifizierte Signaturen deutlich einfacher verwendbar, aber wegen der geringeren Sicherheit und der fehlenden Zertifizierung für die Zielbereiche dieser Arbeit nicht einsetzbar.

Dies führt zur Frage nach den heutigen **Einsatzgebieten qualifizierter elektronischer Signaturen**. Derzeit werden qualifizierte elektronische Signaturen im behördlichen Informationsverkehr mit dem Bürger selten genutzt, obwohl ihr Einsatz in vielen Bereichen denkbar und sinnvoll ist (Steuererklärungen, Rentenauskünfte, Zeugnisauskunft etc) [BSIeSig] [Exp] [Körn06] [SiPe06]. Ebenso werden viele sensible Anwendungen z.B. im Bank- oder Postverkehr, bei denen der Einsatz qualifizierter Signaturen nötig ist, aufgrund des zu betreibenden Aufwandes nicht online durchgeführt. Zum eher kleinen tatsächlichen Einsatzgebiet gehören in einigen wenigen Behörden z.B. der interne Datenverkehr oder die externe Abfrage von Daten.
Ursache für diesen geringen Einsatz sind die verschiedenen **Schwächen**, die qualifizierte elektronische Signaturen in ihrer heutigen Anwendung und technischen Realisierung aufweisen [Exp] [LaUl02] [Zezs01]. Das größte Problem ist der erforderliche hohe Aufwand bei vergleichsweise selten erforderlichem Einsatz. Dieser resultiert aus der notwendigen Installation einer PKI (Public Key Infrastructure), dem hohen Implementierungsaufwand und dem aufgrund gesetzlicher Vorgaben hohen organisatorischen Aufwand, der durch oftmals erforderliche Änderungen des Ablaufs weiter steigt. Außerdem hemmt die derzeit uneinheitliche Technik mit geringem Standardisierungsgrad die Verbreitung qualifizierter elektronischer Signaturen (es existieren zu viele zum Teil widersprüchliche Normen und vorhandene Standards sind in alle Richtungen erweiterungsoffen, daher ist keine einheitliche Implementierung möglich

[Exp]); die unterschiedlichen Identifikationsmethoden machen stets eine Zuordnung zu einem ausgewählten Benutzer notwendig.
Daneben bestehen auch Probleme bei der Verwaltung elektronischer Signaturen. Zum einen ist für eine dauerhafte Signaturprüfung die Speicherung umfangreicher Zusatzinformationen nötig (bei Langzeitarchivierung ggf. auch Neusignatur [Preu05]); zum anderen müssen die Zertifizierungsdienstanbieter absolut zuverlässig und vertrauenswürdig sein; dies gilt insbesondere für das letzte, ungeschützte Zertifikat eines Validierungspfades (vgl. Kapitel 2.2.1.4).
Schließlich existieren triviale Sicherheitsprobleme auf Anwenderebene: Der private Schlüssel, den jeder Nutzer, letztlich also jeder Bürger, besitzt, darf nicht erfahrbar sein. Grobe Fahrlässigkeit oder Manipulation, etwa durch Trojaner, können Fremden Zugriff gewähren und die Vertrauenswürdigkeit des gesamten Systems in Frage stellen [Bert02] [Exp].

Neben diesen Schwächen und Problemen weisen qualifizierte elektronische Signaturen aber auch eindeutige **Stärken** auf, die sie jeder aktuellen alternativen Technologie überlegen machen. Insbesondere zeichnen sich qualifizierte elektronische Signaturen durch eine hohe inhärente Sicherheit (bedingt durch die Zertifizierung) aus [Bert02] [Exp]. Damit ermöglichen sie auch die zweifelsfreie Identifikation in Onlineprozessen und folglich die globale Steuerung von Anwendungen. Gleichzeitig ist die Identifikation unmittelbar an eine Benutzerrolle koppelbar, z.B. bzgl. der Entscheidungsbefugnis. Daneben erhöhen sie die Qualität elektronischer Abläufe [Geis00].

Nach Feststellung der aktuellen Situation und Beurteilung der Stärken und Schwächen elektronischer Signaturen stellt sich die Frage nach den **potentiellen Einsatzgebieten**, für die sie **in der Zukunft** relevant sind, sowie den **Aspekten**, die qualifizierte elektronische Signaturen für diesen Einsatz prädestinieren.

Das in dieser Arbeit betrachtete Einsatzgebiet der qualifizierten elektronischen Signatur in der Zukunft ist das *eGovernment*, also die Abwicklung von Verwaltungsprozessen auf rein elektronischer Basis. Dazu gehört ebenso der verstärkte Einsatz im Umgang mit juristischen Personen wie auch mittel- bis langfristig der Einsatz bei der Kommunikation mit Privatpersonen, z.B. die Abwicklung von Wahlen oder Behördengängen online.

Ein weiterer wichtiger Aspekt der Nutzung elektronischer Signaturen zum Schutz sensiblen Datenverkehrs in der Zukunft ist das *Identity Management* [BSIeSig] [Exp] [SiPe06] – die globale Identifikation natürlicher und juristischer Personen über qualifizierte elektronische Signaturen. Dazu gehört etwa die Ankopplung von Befugnissen und Zugangsrechten im eGovernment, aber auch der Anbieterschutz, in dem die Signaturen als Ersatz für Identifikationsnummern wie TAN-Listen dienen, oder der Kundenschutz durch Identifikation des Anbieters, womit z.B. Phishing verhindert wird.

Ebenso gewährt der Einsatz qualifizierter elektronischer Signaturen *Schutz vor elektronischen Bedrohungen* wie Spam, Viren etc [Exp].

Beim zukünftigen Einsatz elektronischer Signaturen ebenfalls zu berücksichtigen ist die bereits erfolgte *rechtliche Gleichstellung qualifizierter elektronischer Signaturen mit der eigenhändigen Unterschrift* (vgl. Kapitel 2.2.2).

Darüber hinaus ermöglicht der flächendeckende Einsatz qualifizierter elektronischer Signaturen *sicheren Onlineverkehr* und bringt damit Zeit-, Weg- und Kostenersparnisse [BSIeSig] [Schr03].

Grundsätzlich wird die Relevanz der elektronischen Signatur mit verstärktem Einsatz zunehmen. Diese Entwicklung wird stark davon beeinflusst, ob elektronische Signaturen durch günstigere und weniger aufwändigere Verfahren verdrängt werden und es damit nie zu einem flächendeckenden Einsatz kommen wird. Eine frühzeitige *Ablösung durch alternative Verfahren* ist nicht auszuschließen [Exp].

Für eine Wahrung der Relevanz und Anerkennung der qualifizierten elektronischen Signatur ist es wichtig, dass die staatlich vorgegebenen Standards auch langfristig sicher sind und diese Sicherheit kontrolliert wird. Die Frage nach dieser *langfristigen Sicherheit* ist der letzte Punkt, der von den Experten debattiert wurde. Grundsätzlich bleibt festzuhalten, dass der technologische Fortschritt die aktuell verwendeten Verschlüsselungsverfahren zusehends unsicherer machen wird, wodurch eine stärkere Verschlüsselung nötig wird, was zusätzlichen Umstellungs- und Anpassungsaufwand verursacht und zu mehr Aufwand beim Einsatz führt [Exp]. Die derzeit vorhandenen gesetzlichen Vorgaben beschreiben jedoch nur das Konzept der elektronischen Signatur, nicht aber die konkrete technische Umsetzung. Insbesondere gibt es keine gesetzlichen Vorgaben zur Stärke der Verschlüsselung [LaUl02] [Roßn].

Zum *überstaatlichen Einsatz* ist eine enge Zusammenarbeit zwischen den Staaten und den Zertifizierungsdienstanbietern nötig. Eine übergeordnete, EU-weite Kontrollinstanz könnte deren Überwachung übernehmen. Insbesondere ist eine einheitliche Regelung zur Benennung der Zertifizierungsdienstanbieter (Akkreditierung) nötig [Roßn].

4.2 Einflussanalyse

Nachdem elektronische Signaturen im ersten Schritt in ihrem Umfeld beschrieben wurden, wurde im zweiten Schritt untersucht, wie stark seinerseits das Umfeld den Einsatz und die Entwicklung elektronischer Signaturen beeinflusst. Dieser Schritt, der der Identifizierung und Strukturierung der Einflussfaktoren dient, wurde in mehreren Teilschritten absolviert.

4.2.1 Einflussbereiche

Zunächst wurden die relevanten Einflussbereiche gesucht, die auf Einsatz und Entwicklung elektronischer Signaturen einwirken können. Jeder Experte nannte hierzu Bereiche, die Einfluss auf elektronische Signaturen ausüben. Ähnliche und identische Nennungen unter unterschiedlichen Namen wurden zusammengefasst, so dass schließlich sechs Einflussbereiche ermittelt wurden, die einen direkten Bezug zu elektronischen Signaturen haben und Einfluss auf diese ausüben.

Als wichtigster Bereich wurde von allen Experten der Bereich **Technologie** genannt. Die elektronische Signatur ist selbst eine Technologie und damit stark vom technologischen Forschritt abhängig. Ebenso beeinflusst die technologische Entwicklung durch Verbesserung und Vereinfachung den Einsatz elektronischer Signaturen.

Neben der Technologie wird die elektronische Signatur insbesondere in ihrem Einsatz in der Europäischen Union von einem weiteren Bereich maßgeblich beeinflusst: der **Gesetzgebung**. Der Bereich Gesetzgebung umfasst den Einsatz elektronischer Signaturen betreffende Gesetze sowie Vorgaben und Anforderungen an elektronische Signaturen, die von staatlicher bzw. von EU-Seite gestellt werden.

Ein weiterer Bereich, der Einfluss auf elektronische Signaturen nimmt, macht dies deutlich indirekter: der Bereich **Gesellschaft**. Die Gesellschaft umfasst die Gesamtheit der Menschen, die mit elektronischen Signaturen in Berührung kommen, insbesondere aber die Bürger. Dieser Bereich enthält indirekte oder nicht direkt beeinflussbare Aspekte wie Sicherheitsbewusstsein oder demographische Entwicklung, aber auch direktere Beziehungen wie etwa die Akzeptanz der Technologie beim Bürger [Exp].

Mit diesen drei Bereichen sind wichtige Einflüsse erfasst: der Einfluss durch die Entwickler, die Gesetzgeber und die Anwender. Doch es existieren

weitere Bereiche, die für elektronische Signaturen von Bedeutung sind. Der Einflussbereich **Wirtschaft** steht für Unternehmen, die sich mit elektronischen Signaturen befassen, indem sie die Forschung daran unterstützen (und damit indirekt auch Einfluss über den Einflussbereich Technologie ausüben), Soft- und Hardware für elektronische Signaturen vertreiben oder Zertifikate anbieten. Eng an den Bereich Wirtschaft ist der Bereich **Wettbewerb** gekoppelt, der die Beziehung der Unternehmen untereinander und die daraus resultierende hemmende oder fördernde Wirkung für elektronische Signaturen widerspiegelt. Schließlich wurde als letzter Einflussbereich die **Öffentliche Verwaltung** definiert, die alle staatlichen Behörden und damit einen großen Teil der potentiellen Anwender in einer Infrastruktur elektronischer Signaturen umfasst.

Einflussbereiche
Technologie
Gesetzgebung
Gesellschaft
Wirtschaft
Wettbewerb
Öffentliche Verwaltung

Abbildung 14: Übersicht über die Einflussbereiche

4.2.2 Einflussfaktoren

Nach der Ermittlung der Einflussbereiche wurde im Detail festgehalten, welcher Aspekt des jeweiligen Bereiches eine beeinflussende Wirkung ausübt. Diese Aspekte werden als Einflussfaktoren bezeichnet. Die Einflussfaktoren wurden im nächsten Teilschritt ermittelt. Jeder ermittelte Einflussbereich verfügt über in ihm enthaltene Einflussfaktoren, die konkret und in besonderem Maße auf den Einsatz und die Entwicklung

elektronischer Signaturen einwirken. Die Experten wurden aufgefordert, für jeden Bereich eine Liste relevanter Faktoren zu erstellen. Die Ergebnisse wurden vom Moderator zu einer Liste zusammengefasst und an die Experten weitergegeben. Diese ordneten nun die Faktoren jedes Bereichs so an, dass die ihnen am wichtigsten erscheinenden Faktoren vor den weniger wichtigen stehen. Die verschiedenen Listen wurden wiederum vom Moderator unter Verwendung des arithmetischen Mittels zusammengefasst, so dass schließlich eine einzige Liste mit nach abnehmender Priorität geordneten Faktoren vorlag.

Der wichtigste Einflussfaktor im Bereich **Technologie** ist die *Entwicklung von Alternativverfahren*, die einen entscheidenden Faktor für die Entwicklung elektronischer Signaturen darstellt. Sollte ein Verfahren gefunden werden, dass mindestens eben so sicher ist wie die elektronische Signatur, aber mit deutlich weniger Aufwand realisiert werden kann, würde es die elektronische Signatur verdrängen. Umgekehrt können Entwicklungen an alternativen Forschungen aber eventuell auf die elektronische Signatur übertragen werden und helfen, diese zu verbessern [Exp].

Neben der Übernahme von Erkenntnissen aus der Forschung an alternativen Technologien ist aber auch die *Verbesserung der vorhandenen Technologie* ein gewichtiger Faktor. Langfristig kann eine Technologie nur bestehen, wenn sie stetig verbessert wird [Exp]. So muss etwa die Sicherheit der Verschlüsselung gewahrt und die Geschwindigkeit des Verfahrens verbessert werden.

Die Fortentwicklung des Vorhandenen erfordert oftmals die grundlegende Aktualisierung bestehender Soft- und Hardware. Damit dies geschehen kann, muss das System entsprechend aufgebaut sein. Daher ist die *Integrationsfähigkeit neuer Verfahren in bestehende Systeme* der nächste wichtige Faktor [Exp]. Macht z.B. die Einführung eines neuen Verschlüsselungsalgorithmus jegliche vorhandene Software hinfällig und

erfordert eine vollständige Neuimplementierung, kann das Verfahren nicht wirtschaftlich genutzt und angepasst werden.

Einflussbereich	**Einflussfaktoren**
Technologie	- Entwicklung von Alternativverfahren - Verbesserung der vorhandenen Technik - Integrationsfähigkeit neuer Verfahren in bestehende Systeme - Vernetzung - Technischer Standard - Verständlichkeit und Nutzerfreundlichkeit der Anwendungen
Gesetzgebung	- Gesetze zu Datenschutz und Datensicherheit - Rechtlicher Standard - Genehmigungsvergabe an Zertifizierungsdienst-anbieter
Gesellschaft	- Akzeptanz der und Vertrauen in die Technologie - Sicherheitsbewusstsein der Gesellschaft - Anforderungen an die Gesellschaft - Demographie
Wirtschaft	- Wirtschaftlichkeit - Investitionsneigung und -möglichkeit - Wirtschaftlicher Status der Zertifizierungsdienst-anbieter - Kundensupports
Wettbewerb	- Interesse an Standardisierung - Konkurrenz der Zertifizierungsdienstanbieter
Öff. Verwaltung	- Entwicklung eigener Verfahren

Abbildung 15: Übersicht über die Einflussfaktoren, nach Priorität geordnet

Neben der Erforschung und Fortentwicklung elektronischer Signaturen muss aber auch die Infrastruktur eine Grundlage zur Anwendung bieten. Daher ist der Status der *Vernetzung* von großer Bedeutung. Grundlage für den Einsatz elektronischer Signaturen ist die elektronische Kommunikation. Diese erfordert ein Netzwerk, über das kommuniziert werden kann [Exp]. Heute erfüllt das Internet diese Rolle. Verringert sich die Größe des Internets und damit die Zahl der vernetzten Bürger, kommt keine flächendeckende elektronische Kommunikation mehr zustande, und damit nimmt die Bedeutung und Notwendigkeit elektronischer Signaturen ab.
Um sowohl eine hohe Integrationsfähigkeit als auch eine flächendeckende Vernetzung realisieren zu können, ist die *technische Standardisierung* von großem Vorteil. Ohne standardisierte Verfahren, Soft- und Hardware ist der verbreitete Einsatz elektronischer Signaturen in der Kommunikation zwischen ständig wechselnden Partnern nicht möglich [Exp]. Abweichungen führen dazu, dass sich jeder, der mit verschiedenen Partnern kommunizieren will, für jeden Partner (also für jedes Verfahren) spezielle Hard- und Software zulegen muss. Bei Verwendung eines technischen Standards wäre dieser enorme Aufwand nicht mehr nötig.
Schließlich muss in einer Infrastruktur elektronischer Signaturen jeder potentielle Anwender zum Umgang mit ihnen in der Lage sein, wozu es der *Verständlichkeit und Nutzerfreundlichkeit der Anwendungen* bedarf. Die Bedienbarkeit durch Laien ist ein nicht zu unterschätzendes Problem beim Einsatz elektronischer Signaturen! Die Nutzeroberflächen der Software müssen ergonomischer gestaltet werden, um Laien einen einfacheren Zugang zu ermöglichen. Dies ist erforderlich, wenn elektronische Signaturen in der elektronischen Kommunikation mit dem Bürger eingesetzt werden sollen [Exp].

Eine geringere Anzahl unterschiedlicher Faktoren wurde im Einflussbereich **Gesetzgebung** identifiziert. Von grundlegender Bedeutung für Status und Notwendigkeit elektronischer Signaturen sind die *Gesetze zu Datenschutz*

und Datensicherheit. Diese Gesetze beeinflussen die Entwicklung und den Einsatz elektronischer Signaturen stark und stellen damit einen maßgeblichen Faktor dar [Exp].

Außerdem bildet die Gesetzgebung die rechtliche Grundlage zum Einsatz elektronischer Signaturen [Exp] [Roßn]. An der derzeitigen Umsetzung der Richtlinie 1999/93/EG sieht man, wie unterschiedlich ein solcher Text interpretiert werden kann. Dies erschwert den Aufbau eines europaweit kompatiblen Netzwerkes elektronischer Signaturen. Konkrete und detaillierte Anforderungen an Implementierung und Verschlüsselung sowie Vorschriften zu Anwendung und Einsatzgebieten elektronischer Signaturen in Form eines *rechtlichen Standards* sind unabdingbar als Grundlage zur Realisierung eines solchen Netzwerkes [Exp] [Schr03].

Neben diesen elektronische Signaturen betreffenden gesetzlichen Regelungen beeinflusst die Gesetzgebung auch die Zertifikate und Zertifizierungsdienstanbieter durch die Art der *Genehmigungsvergabe an Zertifizierungsdienstanbieter*. Unterschiedliche Verfahren zur Vergabe der Genehmigungen an Zertifizierungsdienstanbieter in verschiedenen Ländern können zu Problemen bei der Anerkennung von Zertifikaten in anderen Ländern als dem, in dem das Zertifikat ausgestellt wurde, führen [Exp] [Roßn]. Derzeit darf jede Person Zertifikate ausstellen. Über die Möglichkeit der Akkreditierung kann der Staat allerdings einigen Anbietern die Möglichkeit zu höherwertigen Diensten bieten, womit eine indirekte Genehmigungserteilung vorliegt.

Der folgende Bereich **Gesellschaft** beschäftigt sich mit den Beziehungen der Gesellschaft zur Technologie. Wichtigster Faktor in diesem Einflussbereich ist die *Akzeptanz der und das Vertrauen in die Technologie* [Exp]. Ein wichtiges Kriterium für den erfolgreichen Einsatz einer Technologie ist die Akzeptanz dieser Technologie durch die Gesellschaft. Wird eine Technologie von der Gesellschaft nicht wahrgenommen oder akzeptiert, so werden die Verbreitung dieser Technologie und ihr Einsatz

beim Bürger scheitern. Ebenso muss die Gesellschaft für den Einsatz einer solch sicherheitskritischen Technik von deren Sicherheit überzeugt werden.
Dabei spielt das *Sicherheitsbewusstsein der Gesellschaft* eine große Rolle [Exp]. Die Notwendigkeit des Einsatzes elektronischer Signaturen ist der Gesellschaft unverständlich, wenn diese nicht über das nötige Sicherheitsbewusstsein verfügt, den Schutz der Kommunikation und der Dokumente zu würdigen. Dieser Punkt ist eng verknüpft mit dem Vertrauen der Gesellschaft in diese Technologie.
Fortschrittliche Technologien wie elektronische Signaturen stellen auch *Anforderungen an die Gesellschaft*, die eng verknüpft sind mit dem Sicherheitsbewusstsein der Gesellschaft und ihrem Vertrauen in die Technologie. Nur eine Gesellschaft, die über das nötige technische Verständnis verfügt, schätzt den Wert einer solchen Technologie [Exp]. Ebenso ist ein gewisses technisches Verständnis zum Einsatz der Signaturen nötig; dies ist eng an den Einflussfaktor aus dem Bereich Technologie ‚Nutzerfreundlichkeit' geknüpft.
Als letzter Einflussfaktor des Bereichs Gesellschaft ist die *Demographie* zu nennen; junge Menschen reagieren aufgeschlossener auf neuartige Technologien und lernen leichter den Umgang damit als ältere Menschen [Exp].

Im Bereich **Wirtschaft** stellt die *Wirtschaftlichkeit des Verfahrens* das primäre Kriterium dar [Exp] [LaUl02]. Dazu gehören Einsatzmöglichkeiten, Geschwindigkeit (vgl. *Technologie: Weiterentwicklung*) und Kompatibilität (vgl. *technische und rechtliche Standards* sowie *Integrationsfähigkeit*).
Stark abhängig von der Wirtschaftlichkeit und den Einsatzmöglichkeiten des Verfahrens ist die *Investitionsneigung* der potentiellen Anwender. Hohe Investitionen in Forschung und Infrastruktur sind aber zur Verbreitung elektronischer Signaturen erforderlich [Exp].
Ein Faktor, der heute eher unbedeutend ist, abhängig von der Entwicklung in der Zukunft aber eine große Rolle spielen kann, ist der *wirtschaftliche*

Status der Zertifizierungsdienstanbieter. Die Entwicklung in diesem Bereich kann maßgeblich zur Verbreitung der elektronischen Signaturen beitragen und wird ihrerseits stark von dieser beeinflusst. Derzeit beschränkt sich das Angebot von Zertifikaten auf wenige Anbieter und ist somit ein Nischenprodukt [Exp]. Sollten sich Signaturen weit verbreiten und spezifisch auf Nutzer zugeschnittene Zertifikate durchsetzen, ist die Entwicklung zur marktfähigen Wirtschaftssparte durchaus denkbar.
Schließlich stellt die Beziehung der in elektronische Signaturen involvierten Wirtschaft zum Bürger, also zur Gesellschaft, in Form des *Kundensupports* einen letzten wichtigen Einflussfaktor dar [Exp]. Insbesondere unter Berücksichtigung der Einflussfaktoren *Nutzerfreundlichkeit* (Einflussbereich *Technologie*) und *Anforderungen an die Gesellschaft* (Einflussbereich *Gesellschaft*) kommt diesem Faktor eine hohe Bedeutung zu, wenn Privatleute und Unternehmen an die Infrastruktur elektronischer Signaturen angebunden werden sollen.

Im Einflussbereich **Wettbewerb** wurden nur zwei Einflussfaktoren ausgemacht, die eine weniger starke Wirkung ausüben als die der vorgenannten Bereiche. Der erste Faktor ist das *Interesse an Standardisierung*. Standardisierung bedeutet beliebige Austauschbarkeit der Anbieter – was im Wettbewerb sowohl Vor- als auch Nachteil sein kann, während es für Forschung und Kunden ein klarer Vorteil wäre [Exp].
Der zweite Einflussfaktor dieses Einflussbereichs ist die *Konkurrenz der Zertifizierungsdienstanbieter*. Konkurrenz kann zu einer Verbesserung von Qualität und Kosten führen, ebenso aber minderwertige Billigangebote provozieren. Beides übt Einfluss auf elektronische Signaturen und ihr Ansehen aus [Exp]. Die Konkurrenzsituation ist stark abhängig vom Einflussfaktor *wirtschaftlicher Status der Zertifizierungsdienstanbieter* (Einflussbereich *Wirtschaft*).

Im letzten Einflussbereich **Öffentliche Verwaltung** wurde schließlich nur ein einzelner Einflussfaktor definiert: die *Entwicklung eigener Verfahren*. Die Entwicklung eigener Verfahren ermöglicht es Behörden, speziell auf ihre Bedürfnisse zugeschnittene Hard- und Software zu entwerfen. Dies ist allerdings mit einem hohen finanziellen Risiko und, selbst im Erfolgsfall, mit hohen Kosten verbunden, die bei Verwendung von auf dem Markt bereits angebotenen Verfahren nicht aufträten [Exp].

4.2.3 Vernetzungsmatrix

Unter Berücksichtigung der vorstehend definierten Einflussfaktoren wurden nun im dritten Teilschritt sämtliche Einflussbereiche miteinander vernetzt, d.h. es wurde untersucht, in wie weit sich die Bereiche gegenseitig beeinflussen. Dieser Schritt wurde mit Hilfe einer Vernetzungsmatrix durchgeführt. Der in die Matrix eingetragene Wert gibt jeweils an, wie stark der links aufgeführte Einflussbereich den oben aufgeführten beeinflusst. 0 bedeutet keine, 1 eine schwache und 2 eine starke Beeinflussung.
Jeder Experte füllte die Matrix aus und vergab subjektiv Einflussstärken. Aus den verschiedenen Tabellen erzeugte der Moderator durch Mittelwertbildung eine einzige Vernetzungsmatrix, die die Summe der Aussagen aller Experten widerspiegelt.
Durch Addition der Zeilen und Spalten erhielt man die Aktiv- respektive Passivsumme der jeweiligen Einflussbereiche, die einen relativen Wert darstellt, wie stark ein Bereich selbst andere Bereiche beeinflusst bzw. von ihnen beeinflusst wird.
Man erkennt, dass der Einflussbereich Technologie alle anderen Einflussbereiche beeinflusst (vgl. erste Tabellenzeile), die Mehrheit davon sogar stark. Dementsprechend ergibt sich für diesen Einflussbereich ein hoher Aktivwert (rechte Spalte). Umgekehrt wird der Bereich Technologie

Durchschnitt	*Tech.*	*Gstzg.*	*Gslls.*	*Wirts.*	*Wettb.*	*ÖV*	*Aktiv*
Technologie	-%-	1	2	2	2	1	8
Gesetzgebung	1	-%-	1	2	1	2	7
Gesellschaft	1	1	-%-	1	1	1	5
Wirtschaft	1	1	2	-%-	2	1	7
Wettbewerb	1	0	1	2	-%-	0	4
Öff. Verwalt.	0	1	1	1	0	-%-	3
Passiv	4	4	7	8	6	5	34/6 = 5,7

Tabelle 1: Vernetzungsmatrix

aber verhältnismäßig schwach von anderen Bereichen beeinflusst, was eine deutlich niedrigere Passivsumme ergibt. Die Bereiche Gesetzgebung und Wirtschaft verfügen über einen ähnlich hohen Aktivwert; die Wirtschaft wird aber gleichzeitig auch sehr stark selbst beeinflusst (höchster Passivwert). Gesellschaft, Wettbewerb und Öffentliche Verwaltung besitzen alle einen höheren Passiv- als Aktivwert, d.h. sie nehmen selbst weniger Einfluss, als dass sie selbst beeinflusst werden.

Zur besseren Anschaulichkeit wurden die ermittelten Werte in ein Koordinatensystem übertragen, bei dem auf der X-Achse die Passiv-, auf der Y-Achse die Aktivwerte eingetragen werden. Durch die Unterteilung der Passiv- und Aktiv-Achsen wird das System in vier Felder eingeteilt – der Schnittpunkt der unterteilenden Achsen entspricht der Summe der Aktiv- bzw. Passivsummen geteilt durch die Anzahl der Elemente (5,7).

Im linken oberen Viertel befinden sich die aktiven Einflussbereiche Technologie und Gesetzgebung. Diese beiden Bereiche bilden die aktiven Bereiche. Optimal für die Beeinflussung des Systems ist die Beeinflussung dieser beiden Bereiche, da sie den größten Einfluss auf das komplette System und damit auf alle anderen Einflussbereiche ausüben.

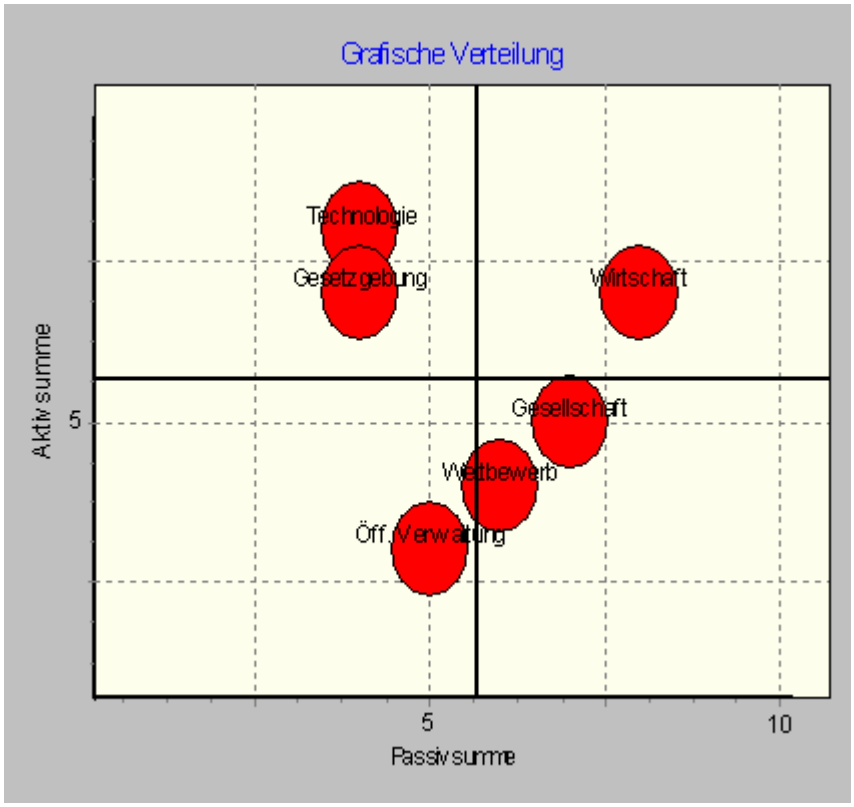

Abbildung 16: Vernetzungsmatrix (angefertigt mit Szeno-Plan [Szeno])

Etwas weniger effizient ist die Beeinflussung des ambivalenten Bereichs Wirtschaft im rechten oberen Viertel. Der Einflussbereich Wirtschaft wird etwa eben so stark von den anderen Bereichen beeinflusst, wie er selbst Einfluss auf sie ausübt. Somit ist auch der Einflussbereich Wirtschaft ein nutzbarer Ansatz zur Veränderung des Systems.

Wenig nutzbringend ist eine Beeinflussung der übrigen drei Bereiche. Der Bereich Öffentliche Verwaltung im linken unteren Viertel ist ein pufferndes Element. Ebenso wie das ambivalente Element Wirtschaft beeinflusst die Öffentliche Verwaltung ungefähr im selben Maße, in dem sie von anderen Bereichen selbst beeinflusst wird. Allerdings ist das Maß dieser beidseitigen Beeinflussung ungleich geringer als beim Einflussbereich Wirtschaft, so dass Änderungen am System nur sehr geringe Auswirkungen auf die Öffentliche Verwaltung und ebenso umgekehrt Änderungen an der

Öffentlichen Verwaltung nur sehr geringe Auswirkungen auf das gesamte System haben.
Die beiden Einflussbereiche Gesellschaft und Wettbewerb im rechten unteren Viertel sind passive Elemente. Während sie stark von Veränderungen am System beeinflusst werden, üben sie selbst wenig Einfluss auf das System aus, so dass Änderungen an diesen Elementen mit dem Ziel der Systembeeinflussung äußerst aufwändig, wenn nicht unmöglich, sind.

Anhand der folgenden zwei grundlegenden Regeln der Systemdynamik lässt sich eine Prioritätsreihenfolge festlegen [Reib91].
Grundregel 1 der Systemdynamik: Immer solche Elemente beeinflussen, bei denen die größte Verstärkerwirkung erzielt werden kann (in der Regel aktive oder ambivalente Elemente mit deutlicher Aktivdominanz). Das bedeutet, dass die höchste Beeinflussungspriorität den beiden aktiven Elementen Technologie und Gesetzgebung zukommt, gefolgt vom ambivalenten Element Wirtschaft.
Grundregel 2 der Systemdynamik: Nach Möglichkeit passive oder puffernde Elemente nicht nur direkt, sondern auch indirekt über die aktiven Elemente beeinflussen. Für Elemente in der unteren Hälfte des Graphs gilt also, dass sie möglichst wenig direkt beeinflusst werden sollen, stark beeinflussbare (passive) Elemente (Gesellschaft, Wettbewerb) aber höhere Priorität haben als solche, die vergleichsweise einflussfrei (puffernd) sind (Öffentliche Verwaltung).

Damit ergibt sich die Priorität der Elemente wie folgt:

1. Technologie
2. Gesetzgebung
3. Wirtschaft
4. Gesellschaft
5. Wettbewerb

6. Öffentliche Verwaltung

Einzelne Faktoren des Einflussbereiches Technologie sind somit besser zur Beeinflussung geeignet als Faktoren der Bereiche Wirtschaft oder Wettbewerb. Z.B. beeinflussen die *Verbesserung des Verfahrens* oder die *Entwicklung von Alternativverfahren* (beides Einflussbereich Technologie) das gesamte System deutlich mehr und sind damit bei der Beeinflussung des Gesamtsystems wesentlich effektiver und daher anstrebenswerter als etwa die Etablierung einer Kundenhotline (*Kundensupport*, Einflussbereich Wirtschaft). Dieses Schema darf jedoch nicht blind verwendet werden, da einzelne Faktoren, ggf. in bestimmten Situationen, immer Sonderfälle sein können.

4.3 Trendanalyse

Der dritte Schritt der Szenario-Analyse, die Formulierung von Deskriptoren und der Projektion dieser auf einen zukünftigen Zeithorizont, hat einen großen Umfang und fordert von den Experten ein hohes Maß an Transferleistung, was ihn zu einem der anspruchvollsten und aufwändigsten Schritte insgesamt macht. In diesem Schritt blieb die Beteiligung der Experten aufgrund des Aufwandes und der Zeitintensität aus.

Die in Schritt 2 ermittelten Einflussfaktoren der jeweiligen Einflussbereiche wurden in diesem Schritt in die Zukunft projiziert, um ihre mögliche Entwicklung festzuhalten. Da die Formulierung der Einflussfaktoren bereits in Schritt 2 wertneutral erfolgte, konnte die Begriffe in diesem Schritt beibehalten werden. Die begriffe Einflussfaktor und Deskriptor sind somit synonym verwendbar; im Weiteren wird der Begriff Deskriptor genutzt.

Im Folgenden wird ein Überblick über den heutigen Zustand der einzelnen Deskriptoren gegeben und deren zukünftig mögliche alternative Entwicklung skizziert. Die verschiedenen Alternativen wurden mit Hilfe einer morphologischen Analyse (eine analytische Kreativitätstechnik zur

Erfassung komplexer Problembereiche und aller möglichen Lösungen [Zwic89]) ermittelt und werden beim entsprechenden Deskriptor aufgeführt.

Einflussbereich: Technologie

Deskriptor: Entwicklung von Alternativverfahren

Im Jahr 2007 sind alternative Verfahren nicht ausreichend ausgereift und zu aufwändig. Anhand der bisherigen Ergebnisse ergeben sich für die zukünftige Entwicklung zwei mögliche extreme Alternativen.

Zum einen ist es möglich, dass eine neue Technologie, die allen Sicherheitsanforderungen genügt, gleichzeitig aber einfacher einsetzbar und im Einsatz weniger aufwändig ist, elektronische Signaturen ablöst.

Zum anderen kann weiterhin eine Situation vergleichbar der heutigen vorherrschen, in der verschiedene alternative Entwicklungen existieren, sich aber keine davon gegen das Verfahren der elektronischen Signatur durchsetzen kann. Solche potentielle Alternativen könnten in verstärktem Maße die Probleme der elektronischen Signaturen aufweisen. Spezialisierte Formen dieser Alternativen werden eventuell innerhalb fest bestimmter, enger Bereiche und Spezialanwendungen, nicht aber flächendeckend genutzt.

Deskriptor: Verbesserung der vorhandenen Technologie

Zum heutigen Zeitpunkt wird kontinuierlich an der vorhandenen Technik gearbeitet, um diese zu verbessern. Für 2020 lassen sich zwei mögliche extreme Alternativen erkennen.

Alternative A entspricht der Fortsetzung der aktuellen Forschung und der Verbesserung der Technologie. In dieser Alternative wird der großflächige Einsatz elektronischer Signaturen möglich. Die ständige Aktualisierung dieser in ihrem Umfeld bedeutenden Technologie ist unumgänglich, größtmögliche Geschwindigkeit und Sicherheit von grundlegender Bedeutung.

In Alternative B hat die Entwicklung seit dem Jahr 2007 aufgrund mangelnden Interesses oder fehlender technischer Möglichkeiten stagniert. Auch der Durchbruch bei einer alternativen, konkurrierenden Technologie kann der Auslöser für das Eintreten dieser Alternative sein.

Deskriptor: Integrationsfähigkeit neuer Verfahren in bestehende Systeme

Heute erfordert der Einsatz größerer Schlüssel die Anpassung des Algorithmus; komplett neue Algorithmen sind nicht kompatibel zur vorhandenen Software, d.h. sie können nicht in die vorhandene Software integriert, sondern es muss neue Software entwickelt werden. Zwei extreme Entwicklungen sind für die Zukunft denkbar.

Die erste Variante ist die absolute Kompatibilität im Jahr 2020. Die Entwicklung neuer Schnittstellen oder die Standardisierung sind mögliche Ursachen für eine freie Austauschbarkeit der Algorithmen. Daraus folgt eine unproblematische Übertragung von an vorhandener Technologie durchgeführten Veränderungen und Verbesserungen auf neue Entwicklungen.

Die gegenteilige Situation liegt in der zweiten Variante vor. Hier ist jeder Algorithmus vollständig anders konstruiert und es existieren keine gemeinsamen, einheitlichen Schnittstellen, die die einfache Verbesserung eines Systems erlauben würden. In diesem Zustand absoluter Inkompatibilität muss jede Entwicklung manuell in ein Programm eingearbeitet werden.

Deskriptor: Vernetzung

Heute ist ein großer Teil der Computer dank des Internets miteinander vernetzt. Für das Jahr 2020 lassen sich auch hier zwei mögliche, extreme Alternativen ermitteln.

Alternative A ist die vollständige Vernetzung. In dieser alternativen Zukunft ist die Vernetzung weiter fortgeschritten, so dass sämtliche Computer

angeschlossen sind und viele Arbeitsabläufe über das Internet abgewickelt werden. Dies führt zu einer Kostensenkung bei enormer Beschleunigung sämtlicher Vorgänge.

In der alternativen Entwicklung B ist die Vernetzung vom heutigen Standpunkt aus gesehen rückläufig; es treten vermehrt so genannte Netzwerkinseln auf. Ursache hierfür können zunehmende Sicherheitsprobleme im Internet sein. Jede Netzwerkinsel verfügt über ein einzelnes Terminal, das einen Internetanschluss besitzt. Das Internet selbst ist aufgrund der hohen Unsicherheit nicht länger ein Medium zur Abwicklung von Arbeitsabläufen und zum Warenabsatz, sondern wird nur noch als mäßig frequentierte Unterhaltungs- und Werbeplattform genutzt.

Deskriptor: Technischer Standard

Im Jahr 2007 existiert kein technischer Standard. Für die Entwicklung bis zum Jahr 2020 sind zwei Varianten denkbar.

Die erste Variante sieht die Einführung eines einheitlichen Standards auf europäischer Ebene vor. Als Grundlage hierfür dient die kontinuierliche Weiterentwicklung der heutigen Verfahren, bis schließlich ein Verfahren vorliegt, das sämtlichen Ansprüchen genügt und als Standard taugt.

Alternativ dazu bleibt in der zweiten Variante eine Einigung auf europäischer Ebene zum Beispiel aufgrund von Sicherheitsmängeln oder nicht zufrieden stellender Geschwindigkeit aus, und es existiert auch im Jahr 2020 noch kein Standard.

Deskriptor: Verständlichkeit und Nutzerfreundlichkeit der Anwendungen

Im Jahr 2007 werden elektronische Signaturen nur von wenigen Personen genutzt; entsprechend ist die Ergonomie für die Nutzung durch ein breites Kundenfeld nicht ausgereift. Bis zum Jahr 2020 ergeben sich auch hier zwei mögliche extreme Alternativen.

Leichte Bedienbarkeit und damit hohe Nutzerfreundlichkeit sind in der ersten Alternative ein Markenzeichen von Software zum Einsatz elektronischer Signaturen. Die zunehmende Verbreitung dieser Technologie hat das Interesse des Marktes an diesem Verfahren und der dazu gehörigen Software ansteigen lassen; ergonomische Software ist eine Grundvoraussetzung an jedes Softwareunternehmen, dass sich im wachsenden Markt etablieren will.
Bleibt der Einsatz elektronischer Signaturen dagegen auf niedriger Stufe oder nimmt er sogar noch weiter ab, ist in der zweiten Alternative die Weiterentwicklung der Ergonomie unattraktiv, und die Nutzerfreundlichkeit stagniert auf dem heutigen, niedrigen Niveau.

Einflussbereich: Gesetzgebung

Deskriptor: Gesetze zu Datenschutz und Datensicherheit
In der heutigen Zeit werden Datenschutz und Datensicherheit aktiv und mit hohem Stellenwert betrieben. Für die zukünftige Entwicklung sind zwei extreme Alternativen denkbar.
Zum einen können die herrschenden Gesetze weiter verschärft werden. Ursache hierfür könnte etwa eine starke Zunahme der Cyber-Angriffe auf persönliche Daten sein.
Zum anderen ist auch ein vollständiger Wegfall des gesetzlichen Datenschutzes und der gesetzlichen Datensicherheit möglich. Ein solches Szenario wäre etwa der so genannte ‚Überwachungsstaat', in dem der ‚Gläserne Mensch' Wirklichkeit geworden ist und von staatlicher Seite jeder Mensch ständig beobachtet und kontrolliert wird. Zum gleichen Resultat führt eine Situation, in der gesetzliche Vorgaben aufgrund der vielfältigen und extrem differierenden Angriffsmöglichkeiten, die Datensicherheit grundsätzlich unmöglich machen, einfach nicht mehr praktikabel und zeitgemäß sind.

Deskriptor: Rechtlicher Standard

2007 existieren allgemeine EU-Richtlinien zum Einsatz elektronischer Signaturen (datierend auf das Jahr 2000); Vorgaben über (z.B. technische) Details gibt es jedoch keine. Für das Jahr 2020 lassen sich aus den bisherigen Ergebnissen zwei mögliche extreme Alternativen ermitteln.

In der ersten Alternative hat sich bis zum Jahr 2020 ein einheitlicher Standard durchgesetzt. In diesem Szenario erfolgt Kommunikation überwiegend über Netzwerke, so dass Standardisierung Kosten spart und den flexiblen Einsatz der Kommunikationstechnologie über Verwaltungs- und Ländergrenzen hinweg ermöglicht.

In der zweiten Alternative kann die Situation auf dem Niveau des Jahres 2000 stagnieren, da die mit dem Standardisierungsvorgang einhergehenden Kosten sowie die differierenden Interessen der Mitgliedsstaaten, die jeweils das in ihrem Land bereits vorhandene und etablierte Verfahren erhalten wollen, die Umsetzung der Standardisierungsideen verhindern.

Deskriptor: Genehmigungsvergabe an Zertifizierungsdienstanbieter

Heute ist jeder Bürger eines EU-Landes berechtigt ohne vorherige Genehmigung Zertifikate auszustellen. Über die Möglichkeit der freiwilligen Akkreditierung steht es den Mitgliedsstaaten der EU frei, Zertifizierungsdienstanbietern die Möglichkeit zum Angebot von Diensten auf höherem Niveau zu bieten. Für das Jahr 2020 sind drei mögliche Entwicklungen denkbar.

Die erste mögliche Entwicklung sieht die Etablierung eines zentralen, von der europäischen Union eingesetzten Gremiums, das als einziges berechtigt ist, Zertifikate auszustellen. Dies kann eine Konsequenz aus der zunehmenden Bedeutung elektronischer Signaturen sein, die die Zahl der Dienstanbieter extrem groß werden ließ, was zu einem gewaltigen Konkurrenzdruck, dadurch zu sinkenden Preisen und schließlich zu mangelhafter Leistung und Sicherheit führte. Dazu kommt die Unüberschaubarkeit der Vielzahl angebotener Zertifikate, die das

Überprüfen eines bestimmten Zertifikats äußerst aufwändig machte. Die Gründung einer zentralen Zertifikatstelle löst diese zunehmend chaotische Situation.

Die zweite mögliche Entwicklung entspricht weitestgehend der heutigen Situation: jeder Bürger hat die Möglichkeit, unter entsprechenden Auflagen ein zertifizierungsdienstanbietendes Unternehmen zu gründen; zur Steigerung der allgemeinen Sicherheit sind die Akkreditierungssysteme aber nicht mehr freiwillig, sondern Pflicht. Grundlage für eine solche Situation ist die Entwicklung des Angebots von Zertifizierungsdiensten zu einer eigenen Wirtschaftssparte. Wenige große Konzerne etablieren sich und beherrschen den europäischen Markt. Aufgrund der Bedeutung elektronischer Signaturen und der marktbeherrschenden Stellung einiger Unternehmen verschwinden nicht-akkreditierte Mitbewerber vom Markt.

In der dritten Variante schließlich hat jeder Staat seine eigene Methode zur Auswahl von Zertifizierungsdienstanbietern. Ursache hierfür ist fehlende Verständigung der EU-Mitgliedsstaaten auf ein einheitliches Akkreditierungsverfahren, was letztlich zu einer chaotischeren Situation führt, als sie 2007 vorherrschte.

Einflussbereich: Gesellschaft

Deskriptor: Akzeptanz der und Vertrauen in die Technologie

Heute ist die Einstellung der Gesellschaft zur Technologie geteilt; teils ist sie zustimmend, teils ablehnend. In der Zukunft können zwei entgegen gesetzte Entwicklungen eintreten.

Entweder hat die Gesellschaft eine überwiegend positive Einstellung zur Technologie. Die jüngere Generation, die mit der Technik groß geworden ist und bei der die Technik daher eine höhere Akzeptanz hat, wird verstärkt zum Hauptnutzer. Außerdem erhöhen positive Erfahrungen im Umgang mit der Technik, z.B. in Form von Arbeitserleichterung oder Beschleunigung der Vorgänge, die Akzeptanz.

Oder aber die Technologie wird von der Gesellschaft mehrheitlich abgelehnt. Die Intransparenz und Komplexität der Technik können hierfür ebenso die Ursache sein wie zunehmende Ängste vor Datentransparenz und Überwachung (Orwell-Syndrom) oder negative Erfahrungen im Zusammenhang mit Technik.

Deskriptor: Sicherheitsbewusstsein der Gesellschaft

Im Jahr 2007 ist Sicherheit ein bedeutender Faktor im Leben jeder Person. Bei der Benutzung neuartiger Technologien wie z.B. dem Internet wird aber oftmals leichtfertig mit der Sicherheit umgegangen. Zwei alternative Extreme sind denkbar.

Die erste extreme Entwicklung sieht im Jahr 2020 ein geschärftes Sicherheitsbewusstsein und erhöhte Sicherheitsansprüche in der Gesellschaft. Grund hierfür ist die täglich zunehmende Bedrohung durch Hacker und Viren, die verstärkt auch PCs angreifen. Die Gesellschaft wird für diese Bedrohungen zunehmend sensibilisiert und nimmt sie endlich ernst.

Keine Weiterentwicklung hat in der zweiten extremen Entwicklung stattgefunden, in der die Gesellschaft fortgesetzt sorglos mit ihrer Sicherheit umgeht. Ursache hierfür kann die zunehmend angepasste und entlastende Software sein, bei deren simplen Anwendung oftmals unwissentlich sicherheitsrelevante Daten freizügig preisgegeben werden.

Deskriptor: Anforderungen an die Gesellschaft

2007 ermöglicht jeder PC den Zugang zum Internet, wenige Nutzer können jedoch mehr als die grundlegenden Funktionen der ihnen zur Verfügung stehenden Technik handhaben. Für das Jahr 2020 sind zwei mögliche extreme Alternativen denkbar.

In Alternative A hat das Vermögen im Umgang mit der Technik zugenommen. Computer prägen in dieser Alternative zunehmend das Leben der Gesellschaft; die jüngere Generation wird mit dieser Technik groß, so dass eine deutlicher ausgeprägte Vertrautheit im Umgang damit besteht als

im Jahr 2007. Die weit verbreitete Nutzung und das tiefere Verständnis der Technik haben dazu geführt, dass Datensicherheit und elektronische Signaturen auch von Privatpersonen ernst genommen werden.
In Alternative B haben die Nutzer weiterhin nur Basis-Grundwissen. Eine mögliche Ursache hierfür ist die zunehmende Anzahl von Spezialisten sowie ausgefeilte Software, die dem Nutzer den Einsatz der Technologie mit lediglich grundlegendem Wissen ermöglichen. Als Konsequenz daraus machen schon geringfügige Veränderungen den Nutzer hilflos.

Deskriptor: Demographie

Im Jahr 2007 hat sich das Gesellschaftsprofil durch Überalterung beträchtlich vom Idealfall der so genannten ‚Alterspyramide' entfernt. Ältere Menschen haben kaum Kontakt zum Medium Computer.
Für die Zukunft wird sich diese Entwicklung mittelfristig nicht ändern; zu diesem Deskriptor sind im vorgegebenen Zeitraum keine alternativen Entwicklungen möglich. Im Jahr 2020 wird die Zahl der älteren Menschen weiter angestiegen sein [BMFS94]; gleichzeitig steigt aber auch die Zahl der Computeranwender hohen Alters. Ältere Menschen tendieren zu höheren Sicherheitsansprüchen, neigen aber auch eher zu, ggf. sicherheitskritischen, Fehlern und stehen Neuerungen zumeist wesentlich voreingenommener gegenüber als jüngere Menschen.

Einflussbereich Wirtschaft

Deskriptor: Wirtschaftlichkeit

Im Jahr 2007 ist die Wirtschaftlichkeit der verfügbaren Verfahren sehr gering. In Relation zum seltenen Einsatz elektronischer Signaturen sind die Anschaffungskosten für das benötigte Equipment (Hard- und Software) viel zu hoch. Für die Entwicklung bis zum Jahr 2020 lassen sich zwei verschiedene gegensätzliche Alternativen erarbeiten.

Eine mögliche Entwicklung führt zu einer hohen Wirtschaftlichkeit elektronischer Signaturen. In diesem Szenario werden elektronische Signaturen bei der elektronischen Kommunikation immer eingesetzt. Aufgrund des häufigen Einsatzes und der Kostenersparnis durch beschleunigte Vorgänge amortisieren sich die Anschaffungskosten sehr schnell.
Die gegenteilige Entwicklung zu (im Vergleich zu heute gleich bleibend) geringer Wirtschaftlichkeit resultiert aus mangelnder Standardisierung, unzureichender Verbreitung oder Konkurrenz durch bessere Alternativverfahren, die eine wirtschaftliche Nutzung des benötigten Equipments verhindern.

Deskriptor: Investitionsneigung und -möglichkeit

2007 ist die Investitionsneigung und -möglichkeit aufgrund knapper öffentlicher Kassen und fehlender Standardisierung (und damit einhergehender mangelnder Einsetzbarkeit) sehr gering. Unternehmen sehen zu geringen Nutzen in der Technik. Für die Zukunft sind zwei alternative Entwicklungen absehbar.
Alternative A schafft ein Szenario, in dem eine hohe Investitionsneigung vorherrscht. Dies resultiert aus der besseren Finanzsituation des Staates gepaart mit verstärktem und einfacherem Einsatz des Verfahrens, was die großflächige Investition in elektronische Signaturen ermöglicht. Wirtschaftsunternehmen schließen sich diesem Trend an.
In Alternative B kann auch 2020 noch wie heute ein Szenario mit geringer Investitionsneigung aktuell sein, da leere öffentliche Kassen in Verbindung mit mangelnder Einsetzbarkeit elektronischer Signaturen die Investition in diese Technologie uninteressant machen.

Deskriptor: Wirtschaftlicher Status der Zertifizierungsdienstanbieter

Heute ist das Anbieten von Zertifizierungsdiensten kein eigener Wirtschaftszweig, sondern wird überwiegend zusätzlich zum eigentlichen

Geschäftsfeld angeboten, oft z.B. von Anwaltskammern, Telekommunikationsanbietern und Öffentlichen Stellen. Für das Jahr 2020 sind zwei Alternativen denkbar.

Zum einen kann sich das Anbieten von Zertifizierungsdiensten bis zum Jahr 2020 zu einer eigenständigen Wirtschaftssparte entwickeln, in der reine Zertifizierungsunternehmen miteinander konkurrieren. Voraussetzung für eine solche Entwicklung ist die Etablierung der elektronischen Signatur, so dass wirtschaftliche Erfordernisse und rechtliche Möglichkeiten zur Gründung von Unternehmen führen, die sich lediglich um das Angebot von Zertifizierungsdiensten sowie die damit direkt zusammenhängenden Serviceleistungen kümmern.

Im Gegensatz dazu kann das Angebot von Zertifizierungsdiensten aber auch ein Nischenprodukt bleiben. Mangelnde wirtschaftliche Bedeutung, strenge rechtliche Vorschriften oder die Etablierung einer einheitlichen europaweit tätigen Vergabestelle sind die wahrscheinlichste Ursache für eine solche Entwicklung; sie machen das Angebot von Zertifizierungsdiensten als primäres Geschäftsfeld unmöglich.

Deskriptor: Kundensupport

Der Kundensupport nimmt heute eine zunehmend wichtige Rolle sowohl für den Kunden als auch für den Anbieter ein. Ein guter Support ist ein Kaufargument für den Kunden, wird gleichzeitig vom Kunden aber auch erwartet. Diese Entwicklung kann sich bis zum Jahr 2020 fortsetzen oder umkehren.

Setzt sich die Entwicklung fort, herrscht im Jahr 2020 eine Situation, in der der Kundensupport einen hohen Status hat. Grund hierfür ist die Forcierung des zunehmenden Einsatzes elektronischer Signaturen, für den ein stetig größer werdendes Nutzerfeld mit dieser Technologie vertraut gemacht werden muss. Solch ein weit verbreiteter Einsatz führt zu einer steigenden Zahl an Problemen bei der Anwendung, die von Support-Unternehmen gelöst werden müssen.

Entwickelt sich der Trend dagegen rückläufig, so findet man 2020 kaum oder keinen Kundensupport. Ursache sind die geringe Bedeutung und der seltene Einsatz elektronischer Signaturen und damit die fehlende Notwendigkeit und Wirtschaftlichkeit eines Support-Angebotes für diese Technologie.

Einflussbereich: Wettbewerb

Deskriptor: Interesse an Standardisierung

Heute ist das Interesse an Standardisierung gering. Die mangelnde Verbreitung macht eine Standardisierung unnötig. Für die Zukunft ergeben sich zwei mögliche extreme Alternativen.

Zum einen kann das Interesse an Standardisierung auch im Jahr 2020 noch gering sein. Verschiedene Möglichkeiten können der Grund hierfür sein: Elektronische Signaturen könnten sich nicht durchgesetzt haben; es könnte mehrere alternative Verfahren geben, die alle ihre Vor- und Nachteile haben, oder der Wettbewerb wünscht schlicht keine Standardisierung.

Zum anderen kann sich bis zum Jahr 2020 bei einem Erfolg elektronischer Signaturen aber auch ein hohes Interesse an Standardisierung entwickelt haben, da die weite Verbreitung elektronischer Signaturen nur bei einem einheitlichen Verfahren effektiv nutzbar ist.

Deskriptor: Konkurrenz der Zertifizierungsdienstanbieter

Aufgrund der staatlichen Vorgaben und Beschränkungen sowie des geringen Interesses an der Technologie ist im Jahr 2007 eine Konkurrenzsituation praktisch nicht vorhanden. Bis zum Jahr 2020 sind zwei entgegen gesetzte Entwicklungen denkbar.

Im Jahr 2020 kann eine starke Konkurrenzsituation herrschen, verursacht durch die Freigabe des Angebots von Zertifizierungsdiensten an jedes interessierte Unternehmen europaweit sowie die zunehmende Bedeutung

von Zertifikaten, die zu einer Entwicklung als eigenes Geschäftsfeld mit zahlreichen beteiligten und konkurrierenden Unternehmen führt.
Alternativ kann im Jahr 2020 noch immer keine Konkurrenz existieren, was an der mangelnden rechtlichen Freigabe der Zertifizierung und der Etablierung einer staatlich geregelten Zertifizierungsstelle (vgl. Genehmigungsvergabe an Zertifizierungsdienstanbieter) oder an der mangelnden Relevanz von Zertifikaten liegen kann, die jeweils den Wettbewerb verhindern.

Einflussbereich: Öffentliche Verwaltung

Deskriptor: Entwicklung eigener Verfahren

Heute verhindern Kosten und Aufwand die Eigenentwicklung im großen Stil; dazu ist sie durch den geringen Einsatz elektronischer Signaturen nicht nötig. Für die zukünftige Entwicklung ergeben sich zwei Alternativen.
In Alternative A betreibt die Öffentliche Verwaltung im Jahr 2020 eine starke Eigenentwicklung. Für Behörden werden eigene Verfahren entwickelt, die speziell auf die Erfordernisse und Anforderungen des jeweiligen Einsatzbereichs zugeschnitten sind. Eigene, nicht uniforme Verfahren versprechen höhere Sicherheit.
In Alternative B findet im Jahr 2020 keinerlei Eigenentwicklung statt. Die Ursache hierfür findet sich in beiden Extremen der möglichen Entwicklung elektronischer Signaturen. Haben sich elektronische Signaturen nicht durchsetzen können, ist eine Eigenentwicklung ebenso wenig nötig wie bei einem mit der vollständigen Verbreitung elektronischer Signaturen einhergehenden umfangreichen Marktangebot unterschiedlicher Software und Zertifikate.

4.4 Alternativenbündelung

Im vorherigen Schritt wurden für alle zuvor ermittelten Einflussfaktoren verschiedene Zukunftsausprägungen erarbeitet. Im Schritt der Alternativenbündelung wurden nun diese erarbeiteten Varianten miteinander verglichen und bestimmt, welche Alternativen einander begünstigen und welche sich ausschließen.

Im ersten Teilschritt der Alternativenbündelung wurde eine Konsistenzmatrix angelegt und diese enorm große Matrix detailliert mit den angemessenen Werten gefüllt. Das Ausfüllen der Matrix kann über eine Diskussion oder in Einzelarbeit bei anschließender Mittelwertermittlung durch den Moderator erfolgen. Tatsächlich wurde dieser Schritt mangels Beteiligung nur mit wenigen Personen diskutiert.

Zum Erstellen der Matrix wurden alle in Schritt 3 ermittelten Alternativen einander gegenüber gestellt und ihre Korrelation festgehalten. Existiert keine direkte Korrelation, wurde eine 0 in die Konsistenzmatrix eingetragen; im Falle von schwacher oder starker Konsistenz eine 1 oder 2, respektive; war die Beziehung dagegen widersprüchlich, entsprechend eine -1 oder -2 (siehe Anhang 1).

Mit Hilfe der kostenlosen Testversion des Szenario-Tools Szeno-Plan (Ver. 4.1.0) der Sinus Software und Consulting GmbH [Szeno] wurden alle möglichen Szenarien ermittelt – weit über 10.000 – und nach Konsistenz geordnet. Als Kritik an der verwendeten Software ist anzumerken, dass sie zumindest in der Testversion keine Möglichkeit bietet, automatisch möglichst gegensätzliche Szenarien zu ermitteln. Nach eingehender Betrachtung der 200 konsistentesten Szenarien, die sich jedoch alle nur in wenigen Punkten unterschieden, wurden daher vom Moderator gezielt Szenarien generiert und vom Tool auf Konsistenz geprüft. Diese Szenarien sind in möglichst vielen Alternativen gegensätzlich, aber in sich absolut stabil, d.h. sie vereinen keine einander ausschließenden Alternativen.

Die Wahl fiel auf zwei Szenarien, die sich in sämtlichen ausgewählten Alternativen widersprechen.

Einflussfaktor	**Szenario A**	**Szenario B**
Entwicklung von Alternativverfahren	Nein	Ja
Verbesserung der vorhandenen Technologie	Ja	Nein
Integrationsfähigkeit neuer Verfahren in bestehende Systeme	Hoch	Niedrig
Vernetzung	Zunehmend	Abnehmend
Technischer Standard	Ja	Nein
Verständlichkeit und Nutzerfreundlichkeit der Anwendungen	Verbessert	Stagnierend
Gesetze zu Datenschutz und Datensicherheit	Streng	Keine
Rechtlicher Standard	Ja	Nein
Genehmigungsvergabe an Zertifizierungsdienstanbieter	Frei	Individuell
Akzeptanz der und Vertrauen in die Technologie	Positiv	Negativ
Sicherheitsbewusstsein der Gesellschaft	Hoch	Niedrig
Anforderungen an die Gesellschaft	Niedrig	Höher
Demographie	Überalterung	Überalterung
Wirtschaftlichkeit	Hoch	Niedrig
Investitionsneigung und -möglichkeit	Hoch	Niedrig
Wirtschaftlicher Status der Zertifizierungsdienstanbieter	Sektor	Nische
Kundensupport	Hoch	Niedrig
Interesse an Standardisierung	Hoch	Niedrig
Konkurrenz der Zertifizierungsdienstanbieter	Hoch	Kaum
Entwicklung eigener Verfahren	Nein	Ja

Tabelle 2: Gegenüberstellung der gewählten Szenarien

4.5 Szenario-Interpretation

Bis zu diesem Schritt dienten alle vorherigen dazu, zwei Zukunftsszenarien zu erarbeiten. Diese beiden Szenarien wurden nach Vorbereitung in den ersten drei Schritten schließlich in Schritt 4 ausgewählt. Im Schritt der Szenario-Interpretation wurden nun die gewählten Szenarien zunächst ausformuliert, d.h. alle gewählten Alternativen wurden einzeln aufgelistet. Anschließend wurde für beide Szenarien analog zu Schritt 2 eine

Vernetzungsanalyse durchgeführt, bei der im Gegensatz zu Schritt 2 die Einflussfaktoren in ihrer unterschiedlichen Zukunftsprägung inhaltliche Grundlage waren. Dies ermöglichte es, die Unterschiede der Szenarien und ihrer Systemdynamik untereinander und zur gegenwärtigen Situation hervorzuheben.

4.5.1 Szenario A

Szenario A zeigt eine Zukunftsvision, in der gesetzliche Regelungen und technische Entwicklung den Bürger im Umgang mit elektronischen Medien stark entlasten. Strenge rechtliche Vorgaben sorgen für ein hohes Maß an Sicherheit, ein Standard für den Einsatz und die Anwendung elektronischer Signaturen hat sich europaweit durchgesetzt und ermöglicht die unkomplizierte und sichere Kommunikation über ein internationales Netzwerk, an das nahezu jeder Rechner europaweit angeschlossen ist. Auf technischer und rechtlicher Ebene verlaufen alle Entwicklungen sehr günstig für elektronische Signaturen. Damit einher geht die positive Einstellung der Gesellschaft zur Entwicklung. Diesem Trend schließt sich auch die Wirtschaft an; das Angebot von Zertifizierungsdiensten hat sich – unter strengen rechtlichen Auflagen – zu einem lukrativen Wirtschaftszweig mit starker Konkurrenz entwickelt.

Hinter dieser perfekten Umwelt stehen jedoch zwei große gesellschaftliche Probleme, die auch in der Gegenwart schon existent sind: die mangelnde technische Qualifikation der Gesellschaft sowie ihre zunehmende Überalterung. Für die Entwicklung und den Einsatz der elektronischen Signatur bedeutet dies, dass die Bürgerschnittstelle oberste Priorität hat. Einfach zu bedienende Oberflächen der Software sind ebenso wichtig wie qualifiziertes Personal in den Bürgerbüros und gute Hilfeleistung durch elektronische Tools, Telefonhotline oder Vor-Ort-Service.

Neben diesen gesellschaftlichen Problemen birgt eine Umwelt mit weitgehender Standardisierung und ohne Konkurrenz immer die Gefahr der

Entwicklungshemmung in sich. Da das Szenario nur den europäischen Raum betrachtet, muss eine andersartige Entwicklung in den Vereinigten Staaten oder Fernost berücksichtigt werden, die Druck auf das europäische System ausüben und dieses beeinflussen kann.

Wie zuvor beschrieben wurde zunächst erneut eine Vernetzungsmatrix angefertigt. Die eingetragenen Werte geben wieder keine (0), eine schwache (1) oder eine starke (2) Beeinflussung an. Aus den Spalten- (Passiv-) und Zeilensummen (Aktivsumme) wurde wieder ein Graph erstellt.

Durchschnitt	*Tech.*	*Gstzg.*	*Gslls.*	*Wirts.*	*Wettb.*	*ÖV*	*Aktiv*
Technologie	-%-	1	1	2	2	2	8
Gesetzgebung	2	-%-	2	2	1	1	8
Gesellschaft	1	1	-%-	1	1	1	5
Wirtschaft	1	0	1	-%-	2	1	5
Wettbewerb	1	0	1	2	-%-	1	5
Öff. Verwalt.	0	0	1	1	1	-%-	3
Passiv	5	2	6	8	7	6	34/6 = 5,7

Tabelle 3: Vernetzungsmatrix Szenario A

Für eine optimale Beeinflussung des Systems muss eine Veränderung an den aktiven Elementen Gesetzgebung und Technologie erfolgen. Es existieren keine ambivalenten oder puffernden Elemente, die ebenso stark beeinflussen wie beeinflusst werden. Alle übrigen Einflussbereiche sind passive Elemente, d.h. ihre Beeinflussung führt kaum zu Veränderungen am System und ist somit wenig nutzbringend.

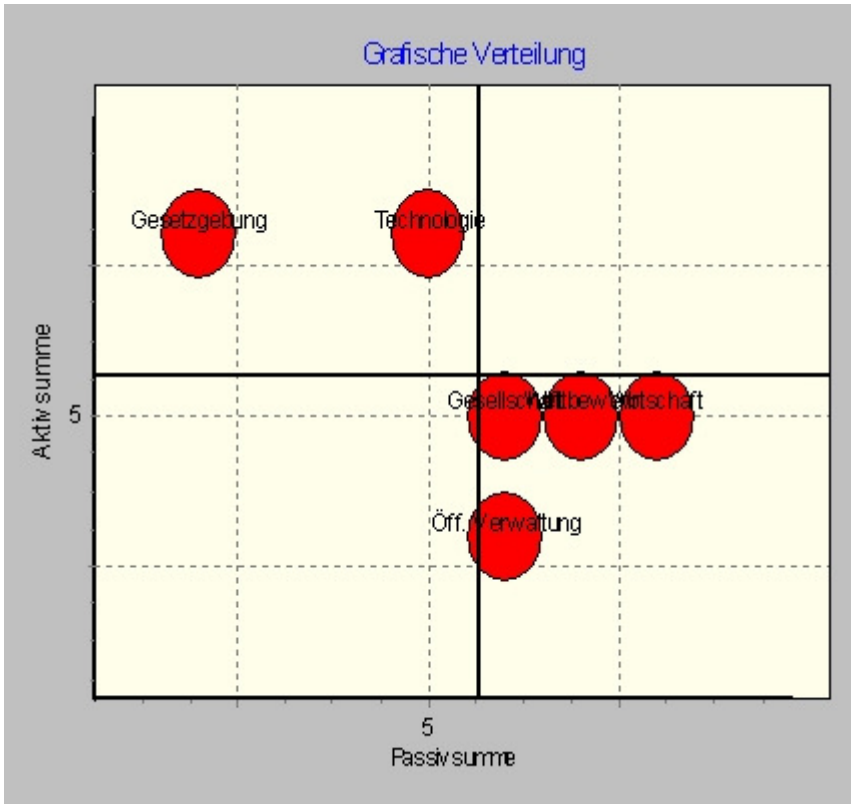

Abbildung 17: Vernetzungsmatrix Szenario A (angefertigt mit Szeno-Plan [Szeno])

Analog zu Schritt 4.2 wurde erneut die Priorität der Bereiche bestimmt. Einflussnahmen auf das System sollten immer in Bereichen mit möglichst hoher Priorität erfolgen, in diesem Szenario also im optimalen Fall im Bereich Gesetzgebung.

1. Gesetzgebung
2. Technologie
3. Gesellschaft
4. Wettbewerb
5. Wirtschaft
6. Öffentliche Verwaltung

Aus Gründen der Übersichtlichkeit wird in der folgenden Auflistung dennoch die Ordnung aus Abschnitt 4.2 beibehalten.

Aus den verschiedenen alternativen Entwicklungen, die in Abschnitt 4.3 für jeden Deskriptor festgelegt wurden, wurde für dieses Szenario jeweils genau eine ausgewählt (vgl. Abschnitt 4.4 – Tabelle 2). Die Summe dieser Alternativen ergab oben beschriebenes Szenario. Im Folgenden werden die ausgewählten Alternativen explizit aufgeführt.

Technologie

Entwicklung von Alternativverfahren: 2020 hat sich die elektronische Signatur als alternativenlose Technologie durchgesetzt, da die existierenden Alternativen technisch und wirtschaftlich deutlich schlechter sind und nur innerhalb weniger Spezialanwendungen Verwendung finden.

Verbesserung der vorhandenen Technologie: Seit 2007 wurde kontinuierlich an der vorhandenen Technik gearbeitet, um diese zu verbessern. Dies führt zu schnelleren und sichereren elektronischen Signaturen im Jahr 2020.

Integrationsfähigkeit neuer Verfahren in bestehende Systeme: 2020 ermöglichen einheitliche Schnittstellen und verbesserte Technik eine unproblematische Aktualisierung der Software. Schlüssel können leicht ausgetauscht und durch deutlich komplexere ersetzt werden. Selbst Algorithmen können ohne großen Aufwand nachträglich eingefügt werden.

Vernetzung: In diesem Szenario herrscht im Jahr 2020 komplette Vernetzung. Jeder Arbeitsplatzcomputer, jeder Home-PC ist an ein weltumspannendes Netzwerk, eine Weiterentwicklung des Internet, angeschlossen.

Technischer Standard: Die Verbesserung der Technik bis 2020 ermöglicht die Etablierung eines technischen Standards, der die besten Aspekte der verschiedenen Verfahren vereint und allen Ansprüchen genügt.

Verständlichkeit und Nutzerfreundlichkeit der Anwendungen: Einhergehend mit technischer Weiterentwicklung und wirtschaftlichem Erfolg hat sich die Ergonomie der Anwendung im Jahre 2020 gegenüber 2007 drastisch verbessert.

Gesetzgebung

Gesetze zu Datenschutz und Datensicherheit: Aufgrund der zunehmenden Vernetzung haben sich Datenschutz und Datensicherheit im Jahr 2020 in diesem Szenario zu beherrschenden Themen nationaler und internationaler Politik entwickelt. Die Zahl der Verstöße und illegalen Angriffe steigt. Die Gesetzgebung ist streng und detailliert.

Rechtlicher Standard: Im Jahr 2007 existieren allgemeine EU-Richtlinien zum Einsatz elektronischer Signaturen; Vorgaben über Details gibt es keine. Dies ändert sich bis zum Jahr 2020; einhergehend mit strengen gesetzlichen Regelungen zu Datenschutz und Datensicherheit werden genaue rechtliche Vorgaben erlassen, auf welche Weise elektronische Signaturen einzusetzen sind. Ein rechtlicher Standard bestimmt Verfahren, Schlüssellänge und Zertifikatsakzeptanz. Dieser einheitliche rechtliche Standard ermöglicht die flexible Kommunikation über Staatsgrenzen hinweg.

Genehmigungsvergabe an Zertifizierungsdienstanbieter: Die strengen rechtlichen Vorgaben schaffen im Jahr 2020 einen Rahmen, innerhalb dessen noch immer jeder Bürger Zertifikate anbieten darf, sich aber akkreditieren muss.

Gesellschaft

Akzeptanz der und Vertrauen in die Technologie: Bis zum Jahr 2020 erkennt die Gesellschaft in diesem Szenario die Bedeutung der Technologie. Im Zuge eines gesteigerten Sicherheitsbewusstseins sowie der breiten Marktdurchdringung elektronischer Signaturen akzeptiert die Gesellschaft diese Technik als hilfreiche und willkommene Unterstützung. Dabei hilft es, dass eine zunehmende Zahl von Menschen bereits mit dieser und ähnlichen Technologien aufgewachsen ist.

Sicherheitsbewusstsein der Gesellschaft: Die steigende Bedrohung in einer zunehmend vernetzten Welt im Jahr 2020 sorgt für ein gesteigertes Sicherheitsbewusstsein und höhere Sicherheitsansprüche der Gesellschaft.

Anforderungen an die Gesellschaft: Im Jahr 2020 ist die technische Qualifikation der Gesellschaft noch immer gering. Leicht zu bedienende Anwendungen, starker Rechtsschutz und sehr guter Kundensupport ermöglichen die Nutzung der Technik ohne Hintergrundwissen. Dies ist auch ein Zugeständnis an die zunehmende Überalterung der Gesellschaft.
Demographie: Der Trend zur Überalterung setzt sich bis zum Jahr 2020 fort. Die Lebenserwartung steigt stetig an, während die Geburtenraten weiter abnehmen. Da die ältere Generation bereits mit Computern aufgewachsen ist, nutzt sie diese Technik weiterhin; das Lernvermögen nimmt jedoch mit zunehmendem Alter ab, während die Sicherheitsansprüche und gleichzeitig die Gefahr der sicherheitskritischen menschlichen Fehler steigen.

Wirtschaft

Wirtschaftlichkeit: Im Jahr 2007 war die Wirtschaftlichkeit des Verfahrens sehr gering. Aufgrund des seltenen Einsatzes elektronischer Signaturen waren die Anschaffungskosten für das benötigte Equipment (Hard- und Software) viel zu hoch. Dies ändert sich grundlegend bis zum Jahr 2020. Elektronische Signaturen werden weiterentwickelt und finden zugleich weite Verbreitung, was ihre unkomplizierte Anwendung mit geringem Aufwand in vielen Situationen ermöglicht und Prozesse beschleunigt und somit zu einer hohen Wirtschaftlichkeit im Jahr 2020 führt.
Investitionsneigung und -möglichkeit: Im Jahr 2020 ist die Investitionsneigung in diesem Szenario sehr groß. Elektronische Signaturen haben sich als Standard etabliert und sind aus der Kommunikation nicht mehr wegzudenken. Die hohe Integrationsfähigkeit neuerer Verfahren in alte Systeme bestärkt den Willen zur Investition.
Wirtschaftlicher Status der Zertifizierungsdienstanbieter: Im Jahr 2007 bildet das Angebot von Zertifizierungsdiensten eine eigene Wirtschaftssparte, in der Unternehmen als reine Zertifizierungs-dienstanbieter agieren.

Kundensupport: Der Kundensupport nahm im Jahr 2007 eine zusehends wichtige Rolle sowohl für den Kunden als auch für den Anbieter ein. Ein guter Support war ein Kaufargument für den Kunden, wurde gleichzeitig vom Kunden aber auch erwartet. Dieser Trend verstärkt sich bis zum Jahr 2020 noch. Die breite Nutzung der Technologie erfordert in Verbindung mit der demographischen Entwicklung und der niedrigen technischen Qualifikation der Gesellschaft zunehmende Unterstützung durch Spezialisten. Die hohe Wirtschaftlichkeit sowie der Konkurrenzdruck verstärken diesen Trend.

Wettbewerb

Interesse an Standardisierung: Die 2007 vorherrschende Situation ändert sich bis zum Jahr 2020. Insbesondere reine Support-Unternehmen, die sich aufgrund der starken Verbreitung und der mangelnden technischen Qualifikation der Gesellschaft entwickelt haben, drängen auf einen einheitlichen Standard. Zulieferer und Programmierer profitieren ebenfalls davon.

Konkurrenz der Zertifizierungsdienstanbieter: Der enorme Erfolg der elektronischen Signatur und ihre Verbreitung sowie die Freigabe des Angebots von Zertifizierungsdiensten durch die EU eröffnen 2020 ein neues und profitables Geschäftsfeld, das regen Zuspruch findet und zu starker Konkurrenz der Anbieter führt.

Öffentliche Verwaltung

Entwicklung eigener Verfahren: Im Jahr 2020 gibt es in diesem Szenario keine Eigenentwicklung, was aber gänzlich andere Ursachen hat als noch 2007: Die Vielzahl spezialisierter Anbieter sowie der sehr gute Support machen eine aufwändige Eigenentwicklung überflüssig und ineffizient. Es existieren spezialisierte Angebote für die angepasste Anwendung in besonderen Umfeldern.

4.5.2 Szenario B

Szenario B stellt eine Zukunftsvision dar, in der elektronische Sicherheit allgemein nicht beachtet wird. Auf Gesetzesebene gibt es praktisch keine Vorgaben bzgl. Datenschutz und Datensicherheit. Der Trend entfernt sich von großen Netzwerken. Immer mehr Unternehmen und Behörden nehmen sämtliche Computer vom zusehends unsicheren und unpraktischeren Internet; kleine Netzwerkinseln prägen das Bild. Diese Entwicklung ist für einen flächendeckenden Einsatz elektronischer Signaturen sehr unvorteilhaft. Hinzu kommt eine schleichende technische Entwicklung, in der viele Alternativtechnologien mit elektronischen Signaturen konkurrieren, ohne dass jedoch einer Technik der Durchbruch gelingt, so dass ein Flickenteppich verschiedener Sicherheitstechnologien vorherrscht. Viele Bürger verlieren aufgrund des mangelnden Angebotes das Interesse am Internet und distanzieren sich ebenfalls. Die technische Qualifikation der Gesellschaft ist zwar höher als 2007, die Überalterung verhindert aber eine schnelle Anpassung an neue Technologien, und aufgrund der großen Vielfalt unausgereifter Technologien sowie dem Mangel an rechtlichen Vorgaben wurde es verpasst, das Sicherheitsbewusstsein der Bürger zu stärken.
In diesem Szenario erscheint es ungleich schwieriger als in Szenario A, eine eSig-Infrastruktur zu etablieren und zu nutzen, da grundlegende Voraussetzungen wie die Akzeptanz durch die Nutzer und ein verfügbares Netzwerk fehlen.

Ein weiteres Mal wurde eine Vernetzungsmatrix angelegt. Die Beschriftung erfolgte wie zuvor beschrieben. Aus den Werten wurden erneut die Aktiv- und Passivsumme gebildet und damit ein Graph angelegt.

Durchschnitt	*Tech.*	*Gstzg.*	*Glls.*	*Wirts.*	*Wettb.*	*ÖV*	*Aktiv*
Technologie	-%-	0	1	2	2	1	6
Gesetzgebung	0	-%-	0	0	0	0	0
Gesellschaft	2	0	-%-	1	2	0	5
Wirtschaft	2	1	1	-%-	2	0	6
Wettbewerb	1	0	2	1	-%-	0	4
Öff. Verwalt.	1	0	1	0	1	-%-	3
Passiv	6	1	5	4	7	1	24/6 = 4

Tabelle 4: Vernetzungsmatrix Szenario B

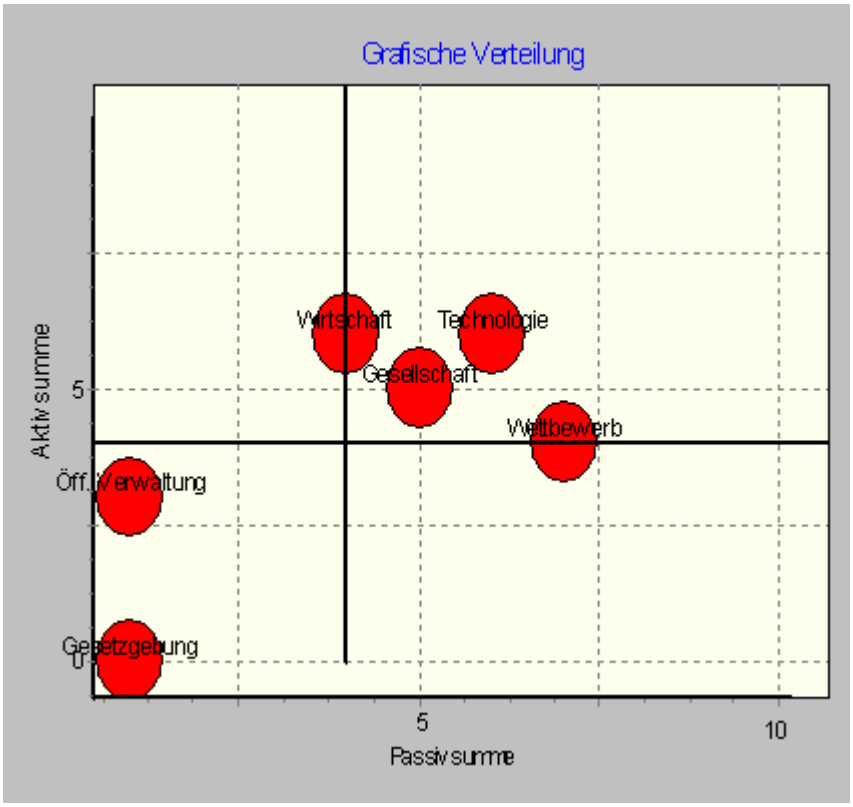

Abbildung 18: Vernetzungsmatrix Szenario B (angefertigt mit Szeno-Plan [Szeno])

In diesem Szenario bildet der genau auf der Trennlinie zwischen aktiven und ambivalenten Elementen liegende Einflussbereich Wirtschaft das

wichtigste zu beeinflussende Element. Hier können mit dem geringsten Aufwand die größten Veränderungen am System erzielt werden.
Ebenfalls sehr gute Ansatzpunkte für Änderungen sind die ambivalenten Elemente Technologie und Gesellschaft, gefolgt vom Wettbewerb, der ebenfalls auf einer Trennlinie (zu passiven Elementen) liegt. Diese drei Elemente üben einen vergleichbar starken Einfluss aus wie die Wirtschaft, werden aber selbst ebenfalls stärker beeinflusst.
Wenig beeinflussenswert sind die puffernden Elemente Öffentliche Verwaltung und Gesetzgebung, die sehr wenig bis – insbesondere im Fall der Gesetzgebung – nahezu keinen Einfluss auf das System ausüben oder von ihm beeinflusst werden.

Die Priorität der Einflussbereiche ergibt sich (analog zu 4.2) wie folgt:

1. Wirtschaft
2. Technologie
3. Gesellschaft
4. Wettbewerb
5. Öffentliche Verwaltung
6. Gesetzgebung

Der wichtigste zu beeinflussende Bereich ist in diesem Szenario der Bereich Wirtschaft, dessen Veränderung die größten Konsequenzen für das gesamte System hat. Am wenigsten effizient ist die Beeinflussung des Bereiches Gesetzgebung, da eine solche Beeinflussung auch bei großem Aufwand kaum Veränderungen am System bewirkt.
Aus Gründen der Übersichtlichkeit wird in der folgenden Auflistung die Ordnung aus Abschnitt 4.2 beibehalten. Diese Auflistung führt explizit alle Alternativentwicklungen (vgl. Abschnitt 4.3) auf, die nach Tabelle 2 (Abschnitt 4.4) für dieses Szenario ausgewählt wurden. Die Summe der Alternativen ergibt oben beschriebenes Szenario.

Technologie

Entwicklung von Alternativverfahren: In diesem Szenario verdrängen im Jahr 2020 neuartige Entwicklungen oder die Weiterentwicklung älterer Technologien elektronische Signaturen. Allerdings kann sich keine dieser Alternativen endgültig durchsetzen; es existieren zahlreiche Technologien nebeneinander.

Verbesserung der vorhandenen Technologie: Die Weiterentwicklung elektronischer Signaturen bis zum Jahr 2020 stagniert in diesem Szenario. Mangelnde Verbesserungsmöglichkeiten sowie zu starke Konkurrenz durch alternative Verfahren verhindern den Durchbruch der elektronischen Signatur.

Integrationsfähigkeit neuer Verfahren in bestehende Systeme: Im Jahr 2020 gibt es noch immer kaum Kompatibilität, da die hohe Vielfalt an Technologien mit ihren zahlreichen verschiedenen Ansätzen und der damit einhergehende fehlende Standard die Anpassung vorhandener Soft- und Hardware an neue Anforderungen schwer bis unmöglich machen.

Vernetzung: Im Jahr 2020 existieren nur noch Netzwerkinseln: Die weltweite Vernetzung der Wirtschaft hat aus Angst vor einer zunehmenden Zahl externer Angriffe durch Hacker, Viren etc. abgenommen. Computer sind nur noch in kleinen Netzwerkinseln (Intranets) zusammengeschlossen, von denen nur wenige, besonders gut abgesicherte Rechner mit den Überresten des Internet verbunden sind, das nun als reine Werbe- und Unterhaltungsplattform dient. Home-PCs sind dank fehlenden Sicherheitsbewusstseins nach wie vor ungeschützt mit dem Internet verbunden, doch aufgrund des geringer werdenden Angebots seitens der Wirtschaft und fehlender Kommunikationsmöglichkeiten zu Behörden nimmt auch deren Zahl ab.

Technischer Standard: 2007 existierte kein Standard, und dies ist auch 2020 noch so. Die Existenz zahlreicher Technologien, von denen sich keine gegen die anderen durchsetzen kann und von denen jede ihre eigenen Fehler und Probleme hat, verhindert eine solche Entwicklung.

Verständlichkeit und Nutzerfreundlichkeit der Anwendungen: Bis zum Jahr 2020 stagniert die Entwicklung ergonomischer Oberflächen aufgrund der mangelnden Weiterentwicklung der Technologie der elektronischen Signatur sowie des geringen wirtschaftlichen Interesses an der Technik.

Gesetzgebung

Gesetze zu Datenschutz und Datensicherheit: Im Jahr 2020 gibt es in diesem Szenario keine einheitlichen gesetzlichen Regelungen. Vielfach werden persönliche Daten zur Überwachung des Bürgers verwendet. Datenschutz und Datensicherheit liegen in der Hand jedes Einzelnen.

Rechtlicher Standard: Im Jahr 2020 gibt es keinen gesetzlichen Standard. Mangelnde Datenschutz- und -sicherheitsgesetze, fehlende Dominanz eines Verfahrens sowie das ausbleibende Interesse und Vertrauen in solche Technologien verhindern einheitliche, EU-weite Vorgaben.

Genehmigungsvergabe an Zertifizierungsdienstanbieter: Im Jahr 2020 existieren individuelle staatliche Regelungen. Jeder Staat erlaubt das Angebot von Zertifizierungsdiensten nach eigenem Maßstab, eine EU-weite Einigung über die Form der Akkreditierung oder ein Zwang dazu besteht nicht.

Gesellschaft

Akzeptanz der und Vertrauen in die Technologie: Im Jahr 2020 wird die Technologie überwiegend abgelehnt. Die Vielfalt an verschiedenen Technologien, die alle individuelle Fehler und Schwächen aufweisen, und die mangelnde Sensibilisierung bzgl. des Themas Sicherheit verhindern eine Auseinandersetzung mit der Technologie.

Sicherheitsbewusstsein der Gesellschaft: Im Jahr 2020 verhält sich die Gesellschaft gegenüber 2007 unverändert leichtsinnig. Sicherheit am Computer interessiert den Großteil der Gesellschaft schlicht nicht. Der chaotische Markt für Sicherheitstechnik verhindert eine großflächige Auseinandersetzung mit dem Thema Computersicherheit. Statt

Schutzmaßnahmen zu treffen werden sicherheitskritische Rechner komplett vom Netzwerk genommen.

Anforderungen an die Gesellschaft: Im Jahr 2020 hat das Vermögen im Umgang mit der Technik gegenüber 2007 zugenommen. Ein Großteil der Generation ist mit dem Medium Computer aufgewachsen und besitzt daher einen deutlich höheren Wissensstand als 2007. Mangelndes Sicherheitsbewusstsein herrscht jedoch noch immer vor. Die zunehmende Überalterung führt zusätzlich dazu, dass die Anpassung an neuartige Techniken nur langsam oder gar nicht funktioniert.

Demographie: Der 2007 vorherrschende Trend zur Überalterung setzt sich bis zum Jahr 2020 fort. Die Lebenserwartung steigt weiter an, während die Geburtenrate immer weiter abnimmt. Da die ältere Generation bereits mit Computern aufgewachsen ist, nutzt sie diese Technik weiterhin; das Lernvermögen nimmt jedoch mit zunehmendem Alter ab, während die Sicherheitsansprüche und gleichzeitig die Gefahr der sicherheitskritischen menschlichen Fehler steigen.

Wirtschaft

Wirtschaftlichkeit: Im Jahr 2020 ist die Wirtschaftlichkeit in diesem Szenario noch immer gering. Gründe hierfür sind die noch immer mangelnde Verbreitung, die fehlende Weiterentwicklung, eine zu hohe Zahl an Konkurrenzprodukten sowie fehlendes Sicherheitsbewusstsein der Gesellschaft.

Investitionsneigung und -möglichkeit: Im Jahr 2020 herrscht eine im Vergleich zu 2007 gleich bleibend geringe Investitionsneigung. Der fehlende Standard, eine zu große Auswahl konkurrierender, aber sehr unterschiedlicher Verfahren, von denen jedoch keines als wirklich zuverlässig betrachtet werden kann, sowie fehlende rechtliche Vorgaben machen Investitionen in die Technologie der elektronischen Signatur risikoreich und wenig interessant.

Wirtschaftlicher Status der Zertifizierungsdienstanbieter: Im Jahr 2020 ist das Anbieten von Zertifizierungsdiensten eine wirtschaftliche Nische. Die geringe Verbreitung elektronischer Signaturen dient der Beibehaltung ihres Status' als Spezialanwendung, mit deren Betreuung sich wenige spezialisierte Anbieter beschäftigen.

Kundensupport: Im Jahr 2020 ist trotz des 2007 vorherrschenden Trends zu verstärktem Kundensupport der Support für elektronische Signaturen und zugehörige Produkte schlecht. Die geringe Verbreitung macht hohen Support unwirtschaftlich, dazu mangelt es aufgrund der geringen Konkurrenz an wirtschaftlichen Anreizen für besseren Support.

Wettbewerb

Interesse an Standardisierung: Im Jahr 2020 ist das Interesse an Standardisierung in diesem Szenario noch immer gering. Noch immer sind aufgrund geringer Verbreitung sowie zunehmender Konkurrenz durch andere Verfahren die grundlegenden Anforderungen für eine Standardisierung nicht erfüllt.

Konkurrenz der Zertifizierungsdienstanbieter: Im Jahr 2020 gibt es – wie schon 2007 – kaum Konkurrenz. Das Fehlen rechtlicher Vorgaben in einigen Staaten bereitet zwar jedem Unternehmen den Weg, ausbleibendes Interesse und schlechte technische Voraussetzungen sowie die daraus folgende geringe Verbreitung elektronischer Signaturen resultieren aber in einer niedrigen Relevanz von Zertifikaten und Zertifizierungsdienstanbietern.

Öffentliche Verwaltung

Entwicklung eigener Verfahren: Im Jahr 2020 ist Eigenentwicklung im Gegensatz zu 2007 vorhanden. In den Behörden, in denen elektronische Signaturen seit langem eingesetzt und auch benötigt werden, werden die benötigten Verfahren und Programme zusehends selbst entwickelt, da ein Anbieter fehlt.

4.6 Konsequenzanalyse

Im weiteren Verlauf der Szenarioanalyse wurden die im vorhergehenden Schritt beschriebenen Szenarien eingehender untersucht. In der Konsequenzanalyse wurden die einzelnen Einflussbereiche für jedes Szenario mit dem Ziel der Erarbeitung von Chancen und Risiken für jeden Einflussbereich betrachtet. Zunächst wurde ihre Situation im Jahr 2020 im durch das Szenario gegebenen Umfeld aufgezeigt. Anschließend folgte eine Erklärung der sich aus dieser Situation ergebenden Chancen, wobei mit den wichtigsten Konsequenzen begonnen wurde. Abschließend erfolgte zu jedem Einflussbereich eine Betrachtung der sich ergebenden Risiken und Gefahren sowie geeigneter Maßnahmen, diesen zu begegnen.
Die geschilderte aktuelle Situation in jedem Einflussbereich ist eine Zusammenfassung der Ergebnisse von Schritt 4.5.

4.6.1 Szenario A

Im Einflussbereich **Technologie** bietet sich im Jahr 2020 folgende Situation: Elektronische Signaturen sind schneller und sicherer und werden standardisiert in einer komplett vernetzten Welt und nutzerfreundlichen Anwendungen eingesetzt, Alternativverfahren konnten sich nicht durchsetzen. Die Erweiterbarkeit und Aktualisierbarkeit auf neuere, sicherere Verfahren ist problemlos möglich.
Aus der vollständigen Vernetzung sowie der Standardisierung und Verbreitung elektronischer Signaturen ergibt sich die Möglichkeit ihres Einsatzes in sämtlichen Bereichen. Die Systeme sind in dieser Zukunftsvision auf rein elektronische Kommunikation umgestellt, wodurch sich eine feste Verankerung elektronischer Signaturen in allen Behördenabläufen ergibt. Der Staat kann über kostenlose Anwendersoftware und Hilfs- und Unterstützungsprogramme den Bürger zur exklusiven Nutzung der Online-Abwicklung animieren. Daneben

ermöglicht die für den elektronischen Behördengang erforderliche Ausstattung aller Arbeitsplätze mit PCs verbesserte Kundenkommunikation und rationalisiert die internen Abläufe.
Die weite Verbreitung und tiefe Integration elektronischer Signaturen in das tägliche Leben ermöglichen die risikofreie Investition in den elektronischen Signatur-Standard zur langfristigen und weiträumigen Nutzung
Schließlich ermöglichen Standardisierung und weite Verbreitung den Zusammenschluss der staatlichen eGovernment-Infrastrukturen zu einem gemeinsamen Netzwerk europäischer Staaten.
Doch es existieren auch Risiken. Die einfache Bedienbarkeit unterstützt die geringe technische Sachkenntnis der Nutzer. Damit besteht die Gefahr, dass schon geringfügige Änderungen an der Software zu Schwierigkeiten der Nutzer bei der Anwendung führen können. Eine Schulung der Nutzer ist empfehlenswert. Ebenso müssen die Anwender für Sicherheitsbelange sensibilisiert und zusätzliche Schutzmechanismen eingerichtet werden, da die alles durchdringende Vernetzung die Gefahr elektronischer Angriffe erhöht.
Schließlich birgt die Existenz eines Standards und das Fehlen konkurrierender Verfahren die Gefahr der Entwicklungsstagnation: eine kontinuierliche Weiterentwicklung und Test der Technologie sowie viel versprechender Alternativen ist unabdingbar, um zukünftigen Gefahren begegnen zu können und auf neuartige Entwicklungen vorbereitet zu sein.

Sehr streng stellt sich der Einflussbereich **Gesetzgebung** im Jahr 2020 in diesem Szenario dar. Die existierende Gesetzgebung zu Datenschutz und Datensicherheit ist äußerst detailliert; der Einsatz elektronischer Signaturen wird darüber hinaus durch einen rechtlichen Standard geregelt. Lockerer ist der Umgang mit den Zertifizierungsdienstanbietern, an die keine über die Akkreditierung hinausgehenden Beschränkungen gestellt werden.
Eine große Chance bieten in diesem Szenario die Normen und gesetzgeberischen Regelungen, die die Modulbauweise forcieren: bei fest

vorgegebenen Schnittstellen ist es möglich, einzelne Komponenten losgelöst zu entwickeln und zu verbessern. Zugleich bergen diese strengen und einengenden Normen und Regelungen jedoch das Risiko einer entwicklungshemmenden Wirkung.
Eine weitere positive Entwicklung ist die durch die fehlenden Beschränkungen an Zertifizierungsdienstanbieter ermöglichte Varianz; ein großer Kreis von Anbietern ist möglich, damit können individuell zugeschnittene Zertifikate erworben werden. Der rechtliche Rahmen verhindert Probleme beim Anbieterwechsel und erlaubt dem Kunden die freie Wahl des Zertifizierungsdienstanbieters.

Die **Gesellschaft** hat in diesem Szenario im Jahr 2020 eine positive Einstellung zur Technologie und pflegt ein hohes Sicherheitsbewusstsein. Zugleich stagniert die Entwicklung der technischen Qualifikation der Bürger, zum Teil aufgrund der Überalterung, aber auch wegen immer leichter anwendbarer Software.
Aufgrund der positiven Einstellung der Gesellschaft kann zur Kostenreduzierung und zum Personalabbau eine verstärkte Verlagerung von Behördengängen auf elektronische Medien angestrebt werden. Bewirkt wird dies durch die Umstellung der behördlichen Abläufe, einhergehend mit Bonus- und Hilfeprogrammen für die Bürger.
Ein Risiko besteht dabei in der geringen technischen Qualifikation der Gesellschaft, die im Falle von Änderungen an der Software nicht überfordert werden darf. Hilfesoftware, Broschüren oder Kursangebote schaffen Abhilfe.
Außerdem muss dem hohen Sicherheitsbewusstsein der Gesellschaft Rechnung getragen werden; es dürfen keine Zweifel an der Sicherheit des öffentlichen Netzes aufkommen. Eine Demonstration der Sicherheit ist hilfreich, die Verhinderung jeglicher Fehlschläge (und insbesondere ggf. deren Bekanntwerdung in der Öffentlichkeit) muss unbedingt gewährleistet sein. Daneben gilt es auch, die Sicherheit der Home-PCs zu wahren und die

auf diesen Computern gespeicherten Dateien zu schützen, die aufgrund der Vernetzung und des niedrigen technischen Grundwissens der Bevölkerung ein leichtes Ziel für Angriffe sind.
Schließlich kann die Überalterung dazu führen, dass die Technologie zwar anerkannt, ihr Einsatz jedoch verweigert wird. Daher muss insbesondere auf die Bevölkerungsgruppen höheren Alters eingewirkt werden.

Weniger Risiken weist in diesem Umfeld der Einflussbereich **Wirtschaft** auf. Die hohe Wirtschaftlichkeit elektronischer Signaturen führt zu einer hohen Investitionsneigung. Das Angebot von Zertifizierungsdiensten boomt; die Anbieter haben eine eigene starke Wirtschaftssparte gegründet. Der Kundensupport ist hoch. Dies alles führt zu einer starken Nutzung elektronischer Vertriebswege durch die Wirtschaft.
Große Abhängigkeit der Wirtschaft vom elektronischen Vertriebsweg birgt aber zugleich einige Risiken, z.B. beim Ausfall der Kommunikationswege oder bei elektronischen Angriffen darauf – hier ist eine Absicherung erforderlich. Zugleich besteht die Gefahr einer zu großen Abhängigkeit von Support-Unternehmen, nicht zuletzt aufgrund der geringen technischen Qualifikation der Anwender.
Die Zahl der sich in diesem Einflussbereich in einem solchen Umfeld bietenden Chancen ist jedoch ungleich höher. Durch eine vollständige Umstellung auf elektronische Netze werden europaweit Kosten gespart, elektronische Signaturen sind günstig einsetzbar. Die Ankopplung der Wirtschaft an das öffentliche Netz ermöglicht eine leichtere Abwicklung und Kontrolle z.B. steuerlicher Vorgänge.
Eine große Zahl von Anbietern bedeutet eine große Auswahl an Zertifikaten, darunter günstige und individuell zugeschnittene Angebote.
Dank der neuen Sicherheit kann der Vertrieb stark über elektronische Medien erfolgen und spricht damit ein größeres Publikum an, wird gleichzeitig flexibler, schneller und weniger aufwändig. Dies erfordert den

Einsatz zusätzlicher Web-Administratoren und Online-Personals sowie den Ausbau des Online-Angebots.
Elektronische Signaturen lassen sich gewinnbringend einsetzen; neben dem Verkauf fertiger Verfahren existieren auch zahlreiche Unternehmen, die keine Eigenentwicklung durchführen, sondern lediglich vom Kundensupport leben. Dies wird durch die große Nachfrage und die standardisierte Technik ermöglicht.

Eng an die Wirtschaft geknüpft ist der Einflussbereich **Wettbewerb**. Der Wettbewerb hat in diesem Szenario großes Interesse an einem einheitlichen Standard (auch nach dessen Einführung); gleichzeitig herrscht eine starke Konkurrenz.
Als Konsequenz der starken Konkurrenz in dieser Zukunftsvision besteht die Möglichkeit der Auswahl eines individuell angepassten Zertifikats, das, im Rahmen der rechtlichen Vorgaben, genau die benötigten und gewünschten Informationen enthält. Dazu führt der Konkurrenzdruck zu einer Senkung der Preise.
Es besteht jedoch die Gefahr, dass sich unter einer großen Zahl an Anbietern auch einige ‚schwarze Schafe' befinden, die mangelhafte Zertifikate ausstellen bzw. die bei der Zertifikatsaustellung einer erhöhten Fehlerquote unterliegen.

Der einzige Faktor im Einflussbereich **Öffentliche Verwaltung** – die Entwicklung eigener Hard- und Softwarelösungen – ist in diesem Szenario im Jahre 2020 irrelevant. Die Übernahme vorhandener Verfahren ist kostengünstiger als eine aufwändige Eigenentwicklung und bietet zugleich den Vorteil, dass in verschiedenen Netzen einheitliche Verfahren verwendet werden und damit Kompatibilität gewährleistet ist.
Ein Risiko besteht hierbei in der Abhängigkeit von angebotenen Fremdverfahren, ein spezieller Zuschnitt auf die eigenen Anforderungen ist dazu nur kostenaufwändig realisierbar.

4.6.2 Szenario B

Die stagnierende Entwicklung sowie die starke Konkurrenz durch gleichwertige oder bessere Alternativverfahren im Jahr 2020 verhindern in diesem Szenario im Einflussbereich **Technologie** eine Etablierung und Standardisierung der elektronischen Signatur. Die Integrationsfähigkeit neuer Verfahren ist gering, ebenso die Anwenderfreundlichkeit. Die globale Vernetzung ist rückläufig.

Als Konsequenz aus der rückläufigen Vernetzung besteht eine relative Sicherheit vor elektronischen Angriffen. Mittels speziell abgesicherter und kontrollierter Kanäle ist eine Anbindung an andere Netzwerkinseln möglich, wobei zugleich das eigene Netz möglichst klein und die Zahl der Knotenpunkte gering gehalten wird.

Dagegen birgt dieses Szenario in diesem Bereich aber viele Risiken und ist für die Verbreitung der elektronischen Signatur äußerst problematisch. Insbesondere ihrem drohenden vollständigen Verschwinden zu Gunsten alternativer Technologien muss durch Anpassung, Weiterentwicklung und Problemfindung entgegen gewirkt werden, wenn die elektronische Signatur als Verfahren erhalten bleiben soll. Die Kernbereiche müssen weiterentwickelt werden, um vorhandene Sicherheitslücken zu schließen und die Entstehung neuer zu verhindern.

Ein weiteres Problem ist die drohende Kostensteigerung durch verstärkte Behördengänge der Bürger, der durch eine Forcierung der Vernetzung, etwa durch ein verstärktes Angebot netzbasierter Aktivitäten in Verbindung mit Bonusprogrammen, entgegengewirkt werden kann.

Auch das mangelnde Umgangsvermögen des Anwenders mit der Technologie schafft weitere Anwendungs- und Sicherheitsprobleme; die gezielte Oberflächenentwicklung sowie das Bereitstellen von Hilfsprogrammen schafft hier Abhilfe.

Zusätzlich erschwert der fehlende Standard die Kommunikation über die eigene Behörde hinaus. Die Einrichtung eines einheitlichen Systems sowie die Bereitstellung sicherer Kanäle muss unbedingt durchgeführt werden.
Schließlich besteht die Gefahr der Kostenexplosion für Behörden und Unternehmen im Falle der erforderlichen Umstellung auf eine neue, deutlich bessere Technologie. In diesem Fall gilt es, die vorhandene Technik möglichst lange effektiv zu nutzen, ohne gleichzeitig zu viel in eine nicht mehr zeitgemäße Technologie zu investieren.

Weniger auffällig verhält sich in diesem Szenario der Bereich der **Gesetzgebung**. Datenschutz- und -sicherheitsgesetze sind kaum vorhanden und dienen mehr der Überwachung als dem Schutz des Bürgers. Vorgaben zu Einsatz und Anwendung elektronischer Signaturen gibt es keine; es existiert weder ein rechtlicher Standard, noch gibt es allgemeingültige Richtlinien beispielsweise für die Durchführung einer Genehmigung für Zertifizierungsdienstanbieter, die von jedem Staat individuell geregelt wird.
Die geringen rechtlichen Beschränkungen bergen eine große Chance: sie ermöglichen die freie Entwicklung der Technologien. Gleichzeitig besteht aber ein Risiko, denn die fehlende Standardisierung über Ländergrenzen hinweg führt zu Kostenerhöhung und geringer Nutzung einhergehend mit mangelnder Anerkennung von Zertifikaten in Ländern mit abweichender Genehmigungsvergabe.

Die **Gesellschaft** im Jahr 2020 ist in diesem Szenario mit der vorhandenen, in ihrer Entwicklung stagnierenden Technologie unzufrieden; die Überalterung macht die Bürger allem Neuen gegenüber skeptisch. Das Sicherheitsbewusstsein hat sich seit dem Jahr 2007 nicht weiter verbessert; immerhin hat sich aber die technische Qualifikation der Gesellschaft seit dieser Zeit leicht gesteigert.
Dieses leicht fortgeschrittene technische Verständnis ist als eine Chance zu begreifen, die die Einführung neuer Technologien etwas vereinfacht; durch

die allgemeine Skepsis der überalterten Gesellschaft wird dem jedoch entgegengewirkt. Bekanntgabe von Forschungsergebnissen, der Appell an die Sicherheit und die Sensibilisierung des Sicherheitsbewusstseins der Gesellschaft ermöglichen erste Erfolge.
Ein Risiko bedeutet der geringe Zuspruch der Bürger zur Technologie; so droht die Gefahr, dass ein teures sicheres Netz aufrechterhalten wird, ohne dass es genutzt wird. Eine Verlagerung der Technik in den Hintergrund, die Demonstration der Sicherheit elektronischer Signaturen, das Aufzeigen der ohne elektronische Signaturen vorhandenen Risiken sowie der Einsatz qualifizierten Personals im Kundenkontakt sind Ansätze, die Bürger zur Nutzung der elektronischen Wege zu animieren.

Die niedrige Wirtschaftlichkeit, daraus resultierend eine niedrige Investitionsneigung, schlechter Kundensupport und das Angebot von Zertifizierungsdiensten als Nischenprodukt sind Indikatoren für die negative Einstellung der Faktoren im Einflussbereich **Wirtschaft** zu elektronischen Signaturen in diesem Szenario.
Konsequenterweise lassen sich aus der Entwicklung in diesem Einflussbereich keinerlei Chancen für dieses Szenario ableiten. Stattdessen existiert eine Vielzahl von Risiken. Die hohen Kosten sowie die aus der niedrigen Einsetzbarkeit resultierende geringe Investitionsneigung verhindern die Weiterentwicklung. Eine interne Entwicklung mit festem finanziellem Rahmen muss durchgeführt werden, um die Möglichkeit eines Erfolges der elektronischen Signaturen zu erhalten. Die Ausbildung des eigenen Personals ist hierzu erforderlich und gleicht dabei den schlechten Support aus.
Außerdem verhindert das geringe Angebot an Zertifizierungsdienstanbietern speziell angepasste Zertifikate zu günstigen Konditionen; auch hier sind zusätzliche Gelder erforderlich.

Analog zur schwachen Stellung der Wirtschaft zu elektronischen Signaturen in diesem Szenario hat auch der Einflussbereich **Wettbewerb** im Jahr 2020 geringen Bezug zur untersuchten Technologie. Der geringe Einsatz und die niedrige Wirtschaftlichkeit hemmen das Interesse an Standardisierung; das geringe Interesse führt gleichzeitig zu geringer Konkurrenz.
Der in diesem Szenario vorherrschende geringe Konkurrenzdruck ermöglicht es den Anbietern, sich auf ihre Angebote zu konzentrieren, ohne die Mitstreiter unterbieten zu müssen. Qualitativ hochwertige Produkte sind das Ergebnis.
Allerdings birgt diese geringe Konkurrenz zugleich das Risiko höherer Preise und mangelnder Individualität und führt aufgrund fehlender Ausweichprodukte zur Akzeptanznotwendigkeit mangelhafter Angebote. Außerdem besteht die Gefahr der Monopolisierung.

Der letzte Einflussbereich, die **Öffentliche Verwaltung**, weist nur einen einzelnen Faktor auf. Dieser Faktor kommt im Umfeld dieses Szenarios allerdings voll zum Tragen; das geringe Angebot in der Wirtschaft führt zur Entwicklung eigener, individuell zugeschnittener Verfahren.
Die Konsequenz dieses Szenarios auf den Bereich Öffentliche Verwaltung ist Chance und Risiko zugleich: Die Eigenentwicklung ermöglicht die perfekte Anpassung an die eigenen Bedürfnisse – allerdings einhergehend mit den entsprechenden Kosten.

4.7 Störereignisanalyse

Im vergangenen Schritt wurden die Chancen und Risiken betrachtet, die sich aus der Entwicklung innerhalb der Einflussbereiche ergeben. Die Analyse der Szenarien wurde in diesem Schritt fortgesetzt, in dem potentielle Störereignisse untersucht wurden, die von außen auf elektronische Signaturen und ihren Einsatz einwirken können.

Die Vernetzungsanalyse hatte ergeben, dass die Bereiche der Technologie, der Gesetzgebung und der Wirtschaft maßgeblich für die Entwicklung des Einsatzes elektronischer Signaturen sind. Denkbare Störereignisse haben jedoch kaum ihre Ursache im wirtschaftlichen Bereich. Probleme in der Wirtschaft resultieren vielmehr üblicherweise aus technischen Unzulänglichkeiten, insbesondere Kommunikations- oder Netzwerkproblemen (z.B. Betriebsspionage in Form des Diebstahls von Kundendaten, was letztlich aber ein Problem mangelnder Sicherheit und damit ein technisches Problem ist, oder Abstimmungsprobleme mit Kunden, die aus Kommunikationsproblemen resultieren und damit ebenfalls einen technischen Ursprung haben). Daher wurden nur Störereignisse aus den Bereichen Technologie und Gesetzgebung betrachtet.

Eine Vielzahl denkbarer Störereignisse tritt in Form kleinerer und alltäglicher Probleme verhältnismäßig häufig auf. Der geringe Umfang dieser Probleme und der häufige Umgang mit ihnen führen aber zu einer einfachen Bewältigung und machen Ereignisse solcher Art für diese Untersuchung uninteressant. Die im Folgenden betrachteten beispielhaft selbst entwickelten Ereignisse verursachen dagegen massive Probleme, da das System bei ihrem Eintritt nicht länger funktionsfähig ist. Diese Ereignisse zeichnen sich folglich durch eine sehr starke Einflussnahme auf die Anwendung elektronischer Signaturen aus und erfordern umfangreiche und bedeutende Maßnahmen.

4.7.1 Störereignisse auf technischer Ebene

Die Störereignisse technischer Art sind eng gekoppelt an den Sicherheitsaspekt elektronischer Signaturen. Konkret muss einerseits die Verschlüsselung sicher sein, andererseits dürfen aber auch gespeicherte Zertifikatsdaten keinesfalls angreifbar sein. Im Folgenden werden zwei exemplarische Störereignisse betrachtet, die die Verschlüsselung betreffen,

sowie ein weiteres, das auf die gespeicherten Daten und deren Verlust abzielt.

Angriffe auf das Verschlüsselungsverfahren wären z.B. die Entwicklung eines Superschlüssels oder die Ermittlung des *Private Key* der Nutzer.

Die Entwicklung eines Superschlüssels bedeutet, dass ein Schlüssel erzeugt wurde, mit dem jede aktuell für elektronische Signaturen verwendete Verschlüsselung decodiert werden kann. In diesem Fall ist die Geheimhaltung der übermittelten Daten nicht mehr gewährleistet, was zu einer Sicherheitslücke und zu einem Vertrauensverlust der Anwender in das System führt. Wichtigste Präventivmaßnahme ist die kontinuierliche Weiterentwicklung des verwendeten Systems; mangelnde Entwicklung ist zugleich die größte Gefahrenquelle für dieses Störereignis. Bei konsequenter Entwicklung und entsprechend regelmäßiger Aktualisierung der verwendeten Verfahren auf neuere, bessere Algorithmen wird es potentiellen Angreifern sehr schwer gemacht, den verwendeten Algorithmus zu entschlüsseln. Gleichzeitig müssen aber auch alternative Verfahren weiter entwickelt werden, um im Notfall bei Eintreten dieser Situation geeignete reaktive Maßnahmen ergreifen zu können. In diesem Fall muss das System schnellstmöglich auf ein alternatives Verschlüsselungsverfahren umgestellt werden, welches sich deutlich vom bislang verwendeten Verfahren unterscheidet, aber keine Einbußen bzgl. der Sicherheit hat.

Das zweite Störereignis betrifft weniger das Gesamtsystem als vielmehr einzelne Nutzer: Die Ermittlung des *Private Key* durch Unbefugte. Sobald sich eine fremde Person den *Private Key* eines Systemnutzers angeeignet hat, bietet sich ihm die Möglichkeit, unter dem Namen des Betrogenen Nachrichten und Dokumente zu verschicken. Es gibt für den Empfänger in diesem Fall keine Möglichkeit, den wahren Absender zu ermitteln. Daher ist es ungemein wichtig, dass jeder Nutzer seinen *Private Key* absolut geheim hält. Sollte es dennoch zu einem Verlust des *Private Key* kommen, so muss dem Betroffenen schnellstmöglich ein neues Schlüsselpaar zugewiesen werden, dass sofort ins Schlüsselregister eingetragen wird und dort den alten

Eintrag ersetzt. Ab dem Datum des Verlustes verliert die alte Signatur ihre Gültigkeit; ab Eintrag des neuen Schlüssels gilt nur noch dieser. Für die zwischen diesen beiden Terminen liegende Zeit lässt sich nicht zweifelsfrei nachweisen, welche Dokumente von welchem Absender stammen. Dieser Zeitraum ist im jeweiligen Fall individuell zu behandeln. Daher ist die schnellstmögliche Meldung des Schlüsselverlustes wichtig; Zeit ist von größter Bedeutung.

Neben diesen Angriffen auf den direkten Ablauf des Systems bergen auch Störereignisse mit Bezug auf abgelegte Daten ein hohes Risiko in sich.
Ein Angriff auf die Datenbank eines Zertifizierungsdienstanbieters bietet z.B. die Möglichkeit die Zuordnung der Zertifikate zu ändern. Wird dies nicht rechtzeitig bemerkt, können sich Personen mit fremden Zertifikaten identifizieren und somit beispielsweise unberechtigt Zugriff auf geschützte Systeme erlangen. Sämtliche elektronischen Unterschriften ab dem Zeitpunkt des Tausches wären fragwürdig, da die sie identifizierenden Zertifikate nicht länger zweifelsfrei korrekt wären. Das Vertrauen in die Infrastruktur elektronischer Signaturen wäre in einem solchen Fall massiv gefährdet. Daher ist es von großer Bedeutung, angemessene Präventivmaßnahmen zu ergreifen. Am Wichtigsten ist es, die gespeicherten Daten vor dem direkten Zugriff von außen bestmöglich zu schützen. Zusätzlich sollten die Daten nie in unverschlüsselter Form abgelegt werden, damit eventuelle Eindringlinge sie nicht selbst nutzen oder verändern können. Sollte dieses Störereignis trotz aller Sicherheitsmaßnahmen dennoch eintreten, müssen sofort jegliche Zertifizierungsdienste, die ihre Zertifikate von der betroffenen Datenbank beziehen, eingestellt werden. Sämtliche dort abgelegten Zertifikate müssen einzeln überprüft und korrekt zugeordnet werden, bevor weitere Zertifizierungen vorgenommen werden können. Ein Backup der Daten hilft, diese Phase zu überbrücken – so können zum einen weiterhin Dienste angeboten werden, zum anderen erleichtert das Backup die korrekte Zuordnung der Zertifikate.

Einen ähnlichen Effekt erzielt der Verlust der Daten in einer Zertifizierungsstelle – dies kann durchaus auch ohne Fremdeinwirkung durch menschliche oder technische Fehler erfolgen. Zwar besteht in diesem Fall nicht das Risiko der unrechtmäßigen Nutzung fremder Zertifikate, die sich aus diesem Störereignis ergebenden Konsequenzen und Gegenmaßnahmen wären aber letztlich dieselben; das Vorhandensein einer Backup-Datenbank wäre allerdings noch ungleich wichtiger, da ohne diese sämtliche Daten unwiderruflich verloren wären.
Besonders kritisch sind Störereignisse mit Bezug auf die Speicherung der Zertifikate in Szenario B in Staaten, die über eine einheitliche Zertifizierungsstelle verfügen, bei der sämtliche Informationen zentral gespeichert sind.

4.7.2 Störereignisse auf rechtlicher Ebene

Neben technischen Störereignissen verursachen auch Ereignisse auf der rechtlichen Ebene erhebliche Probleme. Insbesondere und exemplarisch sei hier eine Veränderung am Rechtsstatus elektronischer Signaturen genannt. Das gesamte System elektronischer Signaturen ist nur so lange effektiv nutzbar, wie die Signaturen eine rechtliche Bewandtnis haben. Verlieren elektronische Signaturen ihren Status als gleichwertiges Substitut für handschriftliche Unterschriften, ist die gesamte Infrastruktur elektronischer Signaturen überflüssig, da elektronisch signierte Dokumente nicht länger Beweiswert hätten. Eine derartige Aufhebung oder Veränderung des rechtlichen Status elektronischer Signaturen ist in Szenario A sehr unwahrscheinlich. Würde dieser Fall in diesem Szenario jedoch tatsächlich eintreten, so hätte dies katastrophale Auswirkungen, da das gesamte Kommunikationssystem auf diesem Verfahren und der damit verbundenen Rechtssicherheit beruht. Weniger gravierend wären die Auswirkungen in Szenario B, in dem rechtliche Aspekte eine untergeordnete Rolle spielen.

Es ist kaum möglich, Präventivmaßnahmen für den Eintritt eines solchen Ereignisses zu ergreifen, da nur bedingt Einfluss auf den Gesetzgeber genommen werden kann. Sollten elektronische Signaturen ihren Status zu Gunsten einer anderen Technologie verlieren, so gilt es, die gesamte Infrastruktur schnellstmöglich auf dieses alternative Verfahren umzustellen. Dazu bedarf es zuvor neben der genauen Beobachtung der politischen Entwicklung der intensiven Forschung an und Investition in entsprechende Technologien; außerdem müssen Hard- und Software möglichst generisch und damit kompatibel gehalten werden. Für den unwahrscheinlichen Fall, dass elektronische Signaturen ihren Status verlieren, ohne dass eine alternative Technologie diesen erhält, muss die Verlagerung der Kommunikation auf elektronische Wege rückgängig gemacht und der Zustand wieder hergestellt werden, der zu Beginn des 21. Jahrhunderts herrschte – Kommunikation persönlich mit Hilfe des Mediums Papier und eigenhändiger Unterschrift.

4.8 Szenario-Transfer

In den ersten vier Schritten wurde auf die Erzeugung zweier Szenarien hingearbeitet. Dieser Arbeitsabschnitt war in Schritt 4 mit der Darstellung der Szenarien abgeschlossen. Die folgenden Schritte dienten der Erläuterung und Untersuchung dieser Szenarien. In diesem letzten Schritt werden nun die Ergebnisse der Analyse der verschiedenen Aspekte zusammen getragen und daraus eine Strategie entwickelt.

Eine gleichzeitige Betrachtung aktueller wie zukünftiger Risiken und Möglichkeiten bildete die Grundlage für ihre Erarbeitung. Ausgangspunkt hierfür waren die Ergebnisse der Konsequenzanalyse (Schritt 6). In diesem Schritt wurden die beiden zuvor erarbeiteten exemplarischen und sehr unterschiedlichen Szenarien betrachtet und auf Chancen und Risiken untersucht, die sich aus einer solchen Entwicklung ergeben. Diese Chancen und Risiken bildeten das Grundgerüst der nachfolgenden Strategien und

wurden an die in Schritt 1 (Aufgabenanalyse) ermittelten heute vorhandenen Stärken und Schwächen elektronischer Signaturen rückgekoppelt, um auch diese zu berücksichtigen und die Strategien entsprechend anzupassen.

Um möglichst großen Einfluss auf die Entwicklung nehmen zu können, müssen Veränderungen an den richtigen Bereichen vorgenommen werden. Diese Bereiche wurden in den Vernetzungsmatrizen sowohl für den heutigen Zustand (Schritt 2, Einflussanalyse) als auch für die verschiedenen untersuchten Zukunftsszenarien (Schritt 5, Szenario-Interpretation) ermittelt. Schließlich durften auch die Ergebnisse des letzten Schritts – der Störereignisanalyse – nicht unberücksichtigt bleiben. Daher wurden auch die dort ermittelten Präventivmaßnahmen in die Strategie aufgenommen.

Da diese Untersuchung in erster Linie die Entwicklung elektronischer Signaturen betrachtet und die hierfür verantwortlichen Stellen keinen oder nur geringen Einfluss auf die Art und das Verhalten der Zertifizierungsdienstanbieter und der Zertifikate haben, werden Zertifikate betreffende Sachverhalte ausgeblendet.

Verschiedene Maßnahmen für alternative Szenarienentwicklungen sind in den Katalog eingearbeitet.

Die Strategien lassen sich vier verschiedenen Zielen zuordnen, deren Verwirklichung in fester Reihenfolge anzustreben ist. Grundlage für eine Infrastruktur elektronischer Signaturen ist die Etablierung der Technologie selbst, d.h. die Technologie muss sich gegenüber ihren Alternativen durch Sicherheit, Zuverlässigkeit, Wirtschaftlichkeit und einfache Bedienbarkeit durchsetzen. Erst dann kann damit begonnen werden, die gewünschte Infrastruktur zu errichten. Kern einer solchen Infrastruktur ist das Netzwerk innerhalb der staatlichen Behörden. Das Einrichten einer solchen und damit einhergehend die Abwicklung innerbehördlicher Kommunikation über elektronische Medien ist das nächste Ziel. Ist ein solches Grundgerüst vorhanden, kann im dritten Schritt Kontakt zum Bürger aufgenommen werden, so dass zwischen Bürgern und Behörden ein festes und sicheres Kommunikationsnetzwerk existiert. Im letzten Schritt erfolgt schließlich die

Vernetzung sämtlicher potentieller Kommunikationspartner, auch über Staatsgrenzen hinweg. Mit diesem vierten Schritt ist dann eine europäische Infrastruktur elektronischer Signaturen geschaffen.

1. Ziel: Absicherung gegen Alternativentwicklung

Alternative Technologien können in dem Moment eine Gefahr darstellen, in dem massiv in elektronische Signaturen investiert wird und die alternativen Entwicklungen nicht mehr berücksichtigt werden. Die Entwicklung an Alternativtechnologien muss beobachtet und auch selbst betrieben werden, um dort erarbeitete Ergebnisse auf elektronische Signaturen übertragen oder im Extremfall von elektronischen Signaturen zu einer besseren Alternative wechseln zu können. Dazu bedarf es einer flexiblen und generischen Grundausrichtung in Soft- und Hardware.

Verschiedene Strategien helfen dabei, dieses Ziel zu realisieren. Von höchster Priorität ist die kontinuierliche Weiterentwicklung elektronischer Signaturen. Diese muss auch nach der eventuellen Einführung eines Standards erfolgen.

Während der Forschung an alternativen Technologien muss immer die Option der Umstellung auf eine andere Technologie offen gelassen werden, z.B. durch Modularisierung (ggf. nach rechtlichen Vorgaben) der verwendeten Technik. Diese Modularisierung darf sich nicht zu eng an die rechtlichen Vorgaben binden, da immer die Möglichkeit einer Veränderung des Rechtsrahmens einkalkuliert werden muss – das Verfahren muss flexibel genug bleiben, um auf solche Veränderungen reagieren zu können.

Ein letzter wichtiger Punkt ist das Ausreizen der vorhandenen Möglichkeiten elektronischer Signaturen, so dass eine Vernachlässigung des Verfahrens und die teure Umstellung auf eine Alternativtechnologie nicht zu früh und eventuell sogar unnötigerweise erfolgt.

2. Ziel: Effizienter Einsatz elektronischer Signaturen innerhalb des eGovernments

Grundlegend für das Erreichen dieses Ziels ist die Ausrüstung jedes Arbeitsplatzes mit einem PC, einhergehend mit der Verlagerung sämtlicher interner Abläufe auf elektronische Medien und der Schulung des Personals. Steht kein externer Supportanbieter zur Verfügung, muss zusätzlich eigenes Supportpersonal ausgebildet werden.

Zusätzlich muss speziell angepasste Software verwendet werden; je nach Entwicklung bis zum Jahr 2020 entweder durch Auswahl der Software aus dem Angebot des Marktes oder durch spezifische Eigenentwicklung in kompatibler Modulbauweise.

3. Ziel: Abwicklung der Kundenkontakte über elektronische Medien

Ist der effiziente Einsatz elektronischer Signaturen innerhalb des eGovernments möglich, wird im nächsten Schritt auch die Kommunikation mit dem Bürger auf elektronische Kommunikationsmedien verlagert. Höchste Priorität hat hierbei die Sicherheit der versendeten und abgelegten Dokumente. Dass diese Sicherheit unabdingbar ist, muss dem Bürger ggf. zunächst bewusst gemacht werden, ebenso wie Vertrauen des Bürgers in die verwendete Technologie aufgebaut werden muss. Der Bürger muss erkennen, dass der Schutz und die Unverfälschtheit seiner Daten notwendig und wichtig ist, und dass elektronische Signaturen in der Kommunikation genau dies leisten. Analog dazu gilt es, die Daten auf dem Home-PC des Bürgers, insbesondere seinen Private Key, ausreichend zu schützen. Hierzu bedarf es der Entwicklung eines Schutzsystems, dass dem Bürger zur Verfügung gestellt wird.

Sind diese grundsätzlichen Sicherheitsvoraussetzungen erfüllt, muss der Bürger zur Nutzung dieser Kommunikationsart animiert werden. Zunächst gilt es, sämtliche Abläufe online anzubieten, so dass keinerlei Behördengänge mehr erforderlich sind. Dazu muss dem Bürger leicht zu bedienende Software zur Verfügung gestellt werden. Diese Software muss

über ein einfaches Bediensystem verfügen und klar strukturiert, die Technik im Hintergrund versteckt sein. Anpassungen und Aktualisierungen der Software sollten möglichst ohne Veränderung (oder nur mit Vereinfachung) der gewohnten Anwenderoberfläche geschehen. Unterstützend muss Support für den Bürger eingerichtet werden, etwa in Form einer Hotline, für die geschultes und qualifiziertes Personal zur Verfügung steht. Außerdem bedarf es eines Anreizes für den Bürger, sich die Fähigkeiten zur Nutzung der elektronischen Kommunikation anzueignen; die Einführung eines Bonussystems für die Nutzung der Online-Abwicklung wird empfohlen.
Schließlich gilt es bei allen vorgenannten Aspekten Rücksichtsnahme auf das durchschnittlich hohe Alter der Bürger zu üben und notwendige Maßnahmen ggf. entsprechend anzupassen.

4. Ziel: Etablierung einer eSig-Infrastruktur

Ist die elektronische Signatur als Technologie gesichert, Behördenintern auf elektronische Medien umgestellt und die elektronische Kommunikation mit dem Bürger möglich, erfolgt als letzter Schritt die Etablierung einer Infrastruktur elektronischer Signaturen zuerst auf Staats- und später auf EU-Ebene.
Grundvoraussetzung hierfür ist die Verwendung einheitlicher Hard- und Software im öffentlichen Netz, bei Vorhandensein eines technischen und rechtlichen Standards natürlich auf diesem basierend. Existiert kein Standard, muss die Hard- und Software möglichst flexibel entwickelt werden, so dass bei Einführung eines Standards eine schnelle und unproblematische Umstellung auf diesen möglich ist.
Neben den technischen Voraussetzungen müssen durch Einstellung und Ausbildung speziellen Web-Personals auch jene auf personeller Ebene erfüllt werden.
Zur Verbindung der Behörden bedarf es spezieller sicherer Webkanäle zwischen ihnen; diese Verbindungen können ggf. auch zur Anbindung an andere europäische Staaten und zur Errichtung eines einzigen EU-weiten

1. **Absicherung gegen Alternativentwicklung**
   - Kontinuierliche Weiterentwicklung der elektronischen Signaturen, auch nach erfolgter Standardisierung
   - Parallele Forschung an Alternativtechnologien
   - Möglichkeit der Umstellung auf alternative Technologie bereithalten (z.B. durch Modularisierung)
   - Ausreizen der vorhandenen Möglichkeiten
2. **Effizienter Einsatz elektronischer Signaturen innerhalb des eGovernments**
   - Ausrüstung jedes Arbeitsplatzes mit einem PC
   - Verlagerung sämtlicher interner Abläufe auf elektronische Medien
   - Schulung des Personals, ggf. Ausbildung eigenen Supportpersonals
   - Verwendung spezialisierter Software (Auswahl angepasster Software aus dem Angebot des Marktes oder spezifische Eigenentwicklung)
3. **Abwicklung der Kundenkontakte über elektronische Medien**
   - Sicherheitssensibilisierung der Bürger sowie Vertrauensaufbau in die verwendete Technologie
   - Entwicklung eines Schutzsystems für PCs
   - Online-Angebot aller Abläufe
   - Angebot einfach zu bedienender Software und Hilfetools
   - Geschultes, qualifiziertes Personal im Kundenkontakt (Hotline) Anreiz-/Bonussysteme für Bürger bei Nutzung der Online-Abwicklung
4. **Etablierung einer eSig-Infrastruktur**
   - Verwendung einheitlicher Hard- und Software im öffentlichen Netz
   - Einstellung und Ausbildung von Web-Personal
   - Einrichtung spezieller, sicherer Webkanäle zwischen verschiedenen Behörden und ggf. EU-weit
   - Forcierung der Vernetzung

Abbildung 19: Übersicht über die entwickelten Ziele und Strategien

Netzwerks verwendet werden. Grundsätzlich sollte die Vernetzung von staatlicher Seite aus forciert werden, da eine ausgedehnte Vernetzung die Etablierung einer eSig-Infrastruktur enorm erleichtert.

4.9 Zusammenfassung: Szenario-Analyse

In diesem Kapitel wurden die konsekutiven Schritte der Szenario-Analyse auf den vorgegebenen Untersuchungsgegenstand ‚elektronische Signaturen im europäischen eGovernment' angewandt. Nach der Charakterisierung elektronischer Signaturen und der Untersuchung ihrer Stärken und Schwächen sowie Einsatzbereiche erfolgte die Erarbeitung der auf elektronische Signaturen, ihren Einsatz und ihre Entwicklung Einfluss nehmenden Faktoren. Diese Faktoren wurden im dritten Schritt der Szenario-Analyse in die Zukunft projiziert und auf verschiedene Entwicklungsalternativen untersucht. Durch die gezielte Bündelung dieser Alternative in Schritt 4 wurden zwei gegensätzliche Szenarien erzeugt, die im fünften Schritt detailliert beschrieben wurden. Basierend auf dieser Beschreibung erfolgte im sechsten Schritt die Untersuchung der Chancen und Risiken, die diese Szenarien bieten. Schritt 7 zeigte beispielhafte Störereignisse auf, die den Einsatz und die Entwicklung elektronischer Signaturen beeinflussen hemmen können. Im letzten Schritt schließlich wurde aus den zuvor ermittelten Ergebnissen ein zukunftsweisender Maßnahmenkatalog erstellt. Dieses Endergebnis der Szenario-Analyse ist eine Strategie, die in einem stufenweisen Aufbau vielseitige Maßnahmen vorschlägt, um elektronische Signaturen zukunftsfähig zu machen, gegen Gefahren zu schützen und auf Veränderungen vorzubereiten.

5 Fazit

Nach der Einführung in das behandelte Thema wurden in Kapitel 2 die technischen und rechtlichen Grundlagen elektronischer Signaturen und ihres Einsatzes im europäischen eGovernment detailliert erläutert. In weiterer Vorbereitung auf den empirischen Teil erfolgte in Kapitel 3 eine Einführung in die Zukunftsforschung, in deren Rahmen mit der Szenario-Analyse eine Prognosemethode begründet für die Anwendung im empirischen Teil ausgewählt wurde. Diese erfolgte anschließend in Kapitel 4, mit dem Ergebnis eines breit gefächerten Maßnahmenkatalogs, der der positiven Entwicklung des Einsatzes elektronischer Signaturen helfen soll. In diesem letzten Kapitel zunächst eine kritische Würdigung der verwendeten Methode, bevor im letzten Unterkapitel der Arbeit differenziert die empirischen Ergebnisse betrachtet und bewertet werden.

5.1 Bewertung der verwendeten Methode: Szenario-Analyse

Die verwendete Methode der Szenario-Analyse ist für die Anwendung gemäß der Aufgabenstellung gut geeignet. Der schrittweise Aufbau gestaltete die Anwendung nachvollziehbar und ermöglicht zugleich den Aufbau auf die und den Vergleich mit den vorhandenen Analyseergebnissen für eine erneute Anwendung unter veränderten Bedingungen.

Beginnend mit der Aufgabenanalyse, die einen guten Einstieg in das behandelte Thema bietet, nähert sich die Analyse mit jedem weiteren Schritt den gesuchten Szenarien an. Die verschiedenen Schritte stellen ein unterschiedliches Maß an Anforderungen an die Experten; besonders zu erwähnen ist die Trendanalyse (Schritt 3), die zugleich ein hohes Maß an Transferleistung und Aufwand von den Experten fordert, und der äußerst zeitaufwändige Schritt der Alternativenbündelung (Schritt 4). Ab Schritt 5 (Szenario-Interpretation) wandelt sich das Ziel der Szenario-Analyse: die

gesuchten Szenarien sind erstellt; in den folgenden Schritten werden diese Szenarien genauer untersucht und Einflüsse ermittelt. Der Unterschied ist auch methodisch spürbar; während die Arbeit der ersten Schritte überwiegend eine Ableitung aus der Gegenwart darstellte, ist nun in höherem Maß Transferleistung und vorausschauendes Denken gefragt, da vorhandenes Wissen aus gegenwärtigen und vergangenen Situationen auf zuvor unbekannte zukünftige Situationen angewandt und entsprechend angepasst werden muss (insb. in der Konsequenz- und der Störereignisanalyse (Schritte 6 und 7)).

Insgesamt muss die Entwicklung der Szenarien kritisch betrachtet werden, da Szenarien durch die persönliche Meinung der Experten eine eher subjektive Prägung erhalten. Ebenso ist der erarbeitete Maßnahmenkatalog ein Ergebnis der subjektiven Meinungen der Experten. Eine geringe Beteiligung wie in der vorliegenden Analyse birgt die Gefahr in sich, dass das Ergebnis besonders stark von wenigen Meinungen beeinflusst wird und dadurch nicht ausreichend differenziert ist. Dies ist ein grundsätzliches Problem der Zukunftsforschung und keine Schwäche der verwendeten Methode; da jegliche Zukunftsforschung sehr spekulativ ist und in weiten Teilen von Wissensstand und Transferleistung der einzelnen Anwender abhängt, sollte die Erarbeitung eines Zukunftsszenarios durch Einzelpersonen nach Möglichkeit vermieden werden.

Aber auch bei objektiver Beteiligung einer großen Anzahl von Experten an der Diskussion sind bei der ersten Anwendung der Szenario-Analyse Unvollkommenheiten zu erwarten. Gründe hierfür sind mangelnde Rückkopplung mit bisherigen Ergebnissen oder nicht ausreichende Auseinandersetzung mit der Aufgabe aufgrund z.B. herrschenden Zeitdrucks, aber auch fehlende qualitativ-verbale Beschreibung der Ergebnisse oder die Beschränkung des Blickfeldes auf die aus heutiger und persönlicher Sicht wahrscheinlicheren Entwicklungen.

Weitere Probleme ergeben sich mit dem hohen Abstraktionsgrad; die stark theoretische Ausrichtung erschwert oftmals die weitere Arbeit für

Teilnehmer, die sich in ihrem beruflichen Umfeld überwiegend mit den praktischen Aspekten der Materie beschäftigen. Auch dies ist aber ein Problem, das bei jeder Form der Zukunftsforschung auftritt.
Die Diskussion der einzelnen Schritte wurde im vorliegenden Fall zudem durch die vorhandenen Möglichkeiten erschwert. Eine Versammlung aller Experten vor Ort mit Möglichkeit zur persönlichen Diskussion hätte diesen Punkt deutlich vereinfacht. Aus den vorgenannten Gründen war eine solche Versammlung der Experten zur Durchführung der Analyse leider nicht möglich. Jedoch hätte auch diese Lösung Probleme aufgeworfen, sind doch für viele Teilschritte aufwändige Vorarbeiten erforderlich, die zu langen Phasen der Einzelarbeit oder zu Arbeitspausen für alle Beteiligten mit Ausnahme des Moderators geführt hätten. Als beste Lösung erscheint die Durchführung wiederholter Workshops in mehrwöchigem Abstand, so dass jeder Beteiligte zwischenzeitlich ausreichend Möglichkeit zur Reflexion des Erreichten und Vorbereitung des nächsten Schrittes hat.

Unter Berücksichtigung der genannten Probleme ist die Szenario-Analyse als Zukunftsforschungsmethode dennoch unbedingt empfehlenswert: die geschilderten Probleme sind sämtliche nicht Eigenart der Szenario-Analyse, sondern liegen in der Natur der Zukunftsforschung begründet. Die Eignung der Szenario-Analyse zur Untersuchung der Aufgabenstellung andererseits jedoch wurde in Kapitel 2 ausführlich dargelegt und macht sie zur Methode der Wahl.
Insgesamt lässt sich rückblickend festhalten, dass die Szenario-Analyse als ein Lernprozess verstanden werden muss, bei dem ständig methodische und inhaltliche Verbesserungen vorgenommen werden müssen. Trotz einiger Verbesserungsvorschläge kann das inhaltliche Ergebnis dazu beitragen, die Personen, die sich mit elektronischen Signaturen beschäftigen, zum Nachdenken und Diskutieren über zukünftige Entwicklungen in diesem Bereich anzuregen, und genau dies ist ein wesentliches Ziel der Zukunftsforschung.

5.2 Bewertung der empirischen Ergebnisse

Im letzten Unterkapitel wird die inhaltliche Dimension der Szenarien kritisch gewürdigt. Eine ausführliche Diskussion der Szenarien und ihrer Unterschiede findet sich bereits in Tabelle 2 und Kapitel 4.5.
Im ersten Teil dieses Kapitels werden auf diese Szenarienbeschreibungen aufbauend die Auswirkungen der Szenarien auf verschiedene Aspekte des Forschungsmodells untersucht.
Im zweiten Teil werden die im Einführungskapitel formulierten inhaltlichen Forschungsfragen rückblickend diskutiert.

5.2.1 Analyse der Auswirkungen anhand der Komponenten des Forschungsmodells

Dieser Abschnitt greift die Probleme und Möglichkeiten der drei in den Szenarien zentralen Komponenten Technologie, Gesellschaft und Gesetzgebung in ihrem Bezug zu elektronischen Signaturen erneut auf und fasst sie zusammen.

5.2.1.1 Technische Entwicklung

Die technische Entwicklung ist die zentrale Komponente der Entwicklung elektronischer Signaturen in der Zukunft. Die Entwicklung wird von nahezu allen Faktoren direkt oder indirekt beeinflusst. Der Schwerpunkt potentieller Veränderungen muss auf der Weiterentwicklung der elektronischen Signatur zu einem leichter und schneller einsetzbaren Verfahren bei gleichzeitiger Forschung an Alternativen liegen. Im aktuellen Zustand sind elektronische Signaturen zu teuer und aufwändig, um sich durchsetzen zu können. Doch auch kein Alternativverfahren kann sich von diesen Problemen lossagen, womit zurzeit eine Situation existiert, in der keine Technologie vorherrscht.

Ebenso gilt es die technischen Probleme zu lösen, die an anderer Stelle auftreten können. Hierzu gehört insbesondere die Sicherung der beim Bürger gespeicherten Daten. Aufgrund des Beweisstatus' elektronischer Signaturen müssen derart signierte Dokumente sicher aufbewahrt werden. Diese Sicherheit ist heute auf einem typischen Home-PC nicht gewährleistet. Der Staat als Anbieter der Dienstleistungen muss dem Bürger helfen, diese Dokumente sicher zu verwahren, etwa durch das Angebot spezieller Sicherheitssoftware. Dasselbe gilt in noch stärkerem Maße für den privaten Schlüssel des Bürgers.

Ein weiteres Problem auf technischer Ebene ist die potentielle Gefahr des Datenverlusts oder -diebstahls bei Zertifizierungsdienstanbietern. Hier kann das eGovernment nur bedingt Einfluss nehmen. Eine Maßgabe über Sicherheitsvorkehrungen sowie die enge Zusammenarbeit zum Schutz der Signaturen wird dringend empfohlen; insbesondere letztere ist je nach Szenario aber nur schwer durchführbar – Szenario A mit seiner Vielzahl an unterschiedlichen Anbietern macht eine grundlegende, intensive und enge Zusammenarbeit nahezu unmöglich.

5.2.1.2 Vernetzte Gesellschaft

Eine wichtige Grundlage für die Etablierung einer funktionierenden eSig-Infrastruktur ist das Vorhandensein eines Netzwerkes. Heute bildet das Internet eine solche Grundlage. Sollte es jedoch zum Rückgang der Vernetzung aus Szenario B kommen, ist die Grundlage für das System elektronischer Signaturen in Frage gestellt. Es ist daher sehr wichtig, die vorhandenen Netzwerkstrukturen zu erhalten und stetig zu erweitern. Gleichzeitig muss die Sicherheit des Teils des Netzes, der für das eGovernment verwendet wird, gewährleistet werden.

Zusätzlich muss jedem Bürger die Möglichkeit geboten werden, den Nutzen des Netzwerkes wahrzunehmen. Dabei muss beachtet werden, dass der Bürger mit den ihm zur Verfügung stehenden Geräten und der entsprechenden Software sicher und zuverlässig umzugehen weiß – eine der größten Herausforderungen.

Die Entwicklung ergonomischer Software sowie die Verlagerung der eigentlichen Technik in den Hintergrund hilft dem Bürger, elektronische Signaturen sicher und schnell zu verwenden, machen ihn aber zugleich anfällig für Probleme bei kleineren Veränderungen. Ebenso fördert mangelnde technische Qualifikation die Gefahr des unbemerkten elektronischen Einbruchs in das häusliche System und damit die Gefährdung sämtlicher abgelegter Dokumente.

5.2.1.3 Rechtlicher Rahmen

Ein rechtlicher Rahmen, wie er derzeit existiert, ist grundsätzlich ausreichend als erstes Fundament, auf dem die weitere Entwicklung aufgebaut werden kann. Eine Änderung der rechtlichen Bestimmungen zur Situation vor der Richtlinie 1999/93/EG (d.h. eine Abkehr von jeglichen einheitlichen Richtlinien) wäre äußerst kontraproduktiv. Rechtssicherheit ist erforderlich, um die weitere Forschung sowie den Aufbau einer eSig-Infrastruktur zu rechtfertigen.

Allerdings reicht der vorhandene Rechtsrahmen nicht aus, um ein Europa umspannendes Netwerk einer eSig-Infrastruktur aufzubauen. Eine Rechtssituation wie in Szenario B beschrieben droht damit, jegliche Bemühungen im Keim zu ersticken. Strengere und konkretere Regelungen sind notwendig, um die stark voneinander abweichenden Interpretationen und Umsetzungen der verschiedenen Mitgliedsstaaten zu vereinheitlichen. Zugleich muss jedoch dafür Sorge getragen werden, dass ein zu strenger

rechtlicher Rahmen die Weiterentwicklung nicht einschränkt oder gar verhindert und das System damit anfällig gegen externe Angriffe gemacht wird.

5.2.2 Zusammenfassende Diskussion der inhaltlichen Forschungsfragen

Das inhaltliche Ziel dieser Arbeit war es, mögliche relevante Entwicklungen im Umfeld elektronischer Signaturen aufzuzeigen und Maßnahmen zu entwickeln, mit denen sich eine eSig-Infrastruktur fest im eGovernment der Zukunft verankern lässt.

Forschungsfrage: Welche Faktoren in Technologie, Gesellschaft oder Wirtschaft beeinflussen die Technik der elektronischen Signatur und ihren Einsatz, und welche möglichen Entwicklungen sind für den Zeitraum bis zum Jahr 2020 für diese Faktoren zu erwarten?

Die Identifikation der Faktoren im Umfeld elektronischer Signaturen, die diese beeinflussen, erwies sich als vergleichsweise schwierig, da sich schwer abschätzen lässt, wo eine Einfluss nehmende Beziehung zum abstrakten Untersuchungsbegriff besteht. Die Bestimmung dieser Einflussfaktoren erfolgte in Einzelarbeit der interdisziplinär zusammengesetzten Gruppe von Experten, wobei die Ergebnisfindung in mehreren Schritten stattfand und die Ergebnisse jedes einzelnen Schrittes allen Experten zugänglich gemacht wurden. Eine Vielzahl von Ideen, die jedoch aufgrund der geringen im Expertenteam ungenügend abgestimmt waren und denen zumeist eine begleitende Erläuterung fehlte, stellte den Moderator vor die schwierige Aufgabe, die Ideen im Sinne der Experten zu interpretieren, Duplikate zu entfernen und alle vorhandenen Vorschläge in geordneten Gruppen zusammen zu fassen.

Diese von den Experten identifizierten und anschließend vom Moderator in Individualarbeit verdichteten Einflussfaktoren müssen als eine mögliche Sichtweise auf elektronische Signaturen und die beeinflussenden Faktoren in deren Umwelt betrachtet werden – eine Allgemeingültigkeit ist nicht gegeben und war auch nicht die Zielsetzung der Arbeit. Sowohl das Forschungsmodell als auch die Einflussfaktoren können als Grundlage weiterer Forschungsarbeiten dienen und müssen entsprechend ergänzt und überarbeitet werden. Diese Forschungsarbeiten sollten sich darauf konzentrieren, die Entwicklung elektronischer Signaturen als komplexes System zu betrachten, bei dem eine Vielzahl von Faktoren in gegenseitiger Wechselwirkung steht. Dieser Gedanke des vernetzten Systems muss verstärkt heraus gearbeitet werden.

Aus den Szenarien kann abgeleitet werden, dass die eingleisige Entwicklung elektronischer Signaturen zu beschränkt ist und durch die Entwicklung an alternativen Methoden ergänzt werden muss. Es erscheint daher angebracht, den Untersuchungsbegriff dieser Arbeit zu erweitern und alternative Technologien, d.h. konkurrierende Methoden, in zukünftige Analysen stärker mit ihren Eigenheiten, Stärken und Schwächen einzubeziehen. Nur dadurch kann gewährleistet werden, dass durchgängige, prozessorientierte Konzepte und Werkzeuge entstehen.

Der zweite Teilaspekt dieser Forschungsfrage beinhaltet die zukünftige Entwicklung der Einflussfaktoren. Im Sinne einer kontinuierlichen Zukunftsforschung ist es notwendig, diese Trendentwicklungen in regelmäßigen Zeitabständen zu überprüfen.

Probleme bei der Operationalisierbarkeit und der Fundierung der Projektionen ergaben sich vor allem bei solchen Faktoren, deren Entwicklungsmöglichkeiten in entgegen gesetzter Richtung zu sehen sind. Diese Orthogonalität der möglichen Trends verschweigt eine große

Grauzone zwischen den beiden Extremen, die aber eine eigene Dynamik entwickeln und neue, nicht berücksichtigte Entwicklungen und Probleme provozieren kann. Weitere Forschung kann sich damit beschäftigen, die Deskriptoren schärfer zu formulieren und ggf. mehrfache alternative Trends zu identifizieren. Letztendlich könnte für die Beschreibung und Trendfundierung jedes einzelnen Faktors eine Abhandlung geschrieben werden, deren Umfang dem der vorliegenden Arbeit gleichkommt. Hierbei muss jedoch eine Kosten-Nutzen-Abschätzung hinsichtlich des Erkenntnisgewinns für den Untersuchungsgegenstand sowie im Hinblick auf die Einflussstärke und damit Bedeutung eines Faktors vorgenommen werden.

Abschließend bleibt festzustellen, dass die Identifikation der Einflussfaktoren und ihre Entwicklung und die daraus resultierende Vernetzung und Wirkungszusammenhänge die Grundlage der Szenario-Analyse bilden. In diesem Bereich liegt ein großes Forschungspotential, um der wachsenden Bedeutung sicherer elektronischer Kommunikation im Umfeld des eGovernment gerecht zu werden.

Forschungsfrage: Welche Konsequenzen ergeben sich hieraus für die aktuelle Forschung an elektronischen Signaturen, welche Maßnahmen müssen frühzeitig ergriffen, welche Aspekte intensiviert werden?

Als Grundlage zur Beantwortung dieser Frage wurden zwei gegensätzliche Szenarien erarbeitet, aus denen gemeinsame Maßnahmen abgeleitet werden konnten. Diese Maßnahmen wurden bereits im Schritt des Szenario-Transfers in Kapitel 4.8 und bei der Analyse der Auswirkungen auf die Komponenten des Forschungsmodells früher in diesem Kapitel ausführlich besprochen und in Abbildung 21 im Überblick dargestellt. Die folgenden Ausführungen beziehen sich auf die Frage, welche Konsequenzen sich für die Forschung an elektronischen Signaturen ergeben.

Ausgangspunkt für die Unterschiede in beiden Szenarien ist die Intensität der Forschung an elektronischen Signaturen und alternativen Verfahren. Wird die elektronische Signatur schneller und weniger aufwändig einsetzbar und kann sie sich gegen alternative Verfahren durchsetzen, so ist die Akzeptanz in Gesellschaft und Wirtschaft wahrscheinlich. Im umgekehrten Fall wird es kaum zur Etablierung einer genutzten eSig-Infrastruktur kommen. Zusätzlich ist im letzteren Fall eine rechtliche Unterstützung unwahrscheinlich, während dies im ersten Fall durchaus denkbar ist.

Folglich lässt sich die Forschung an elektronischen Signaturen in drei wesentliche Bereiche einteilen: 1. Schnelligkeit und geringer Aufwand, was letztlich auch geringe Kosten bedeutet; 2. hohe Sicherheit und 3. einfache Bedienbarkeit.
Mangelnde Schnelligkeit und zu großer Aufwand halten derzeit die Wirtschaft von dieser Technologie fern. Ein wichtiger Aspekt ist hierbei die Kompatibilität verschiedener Systeme. Ein einzelnes Hard- und Softwaresystem muss ausreichend sein, um mit verschiedensten Kontakten kommunizieren zu können. Hierzu bedarf es der Einführung standardisierter Schnittstellen, die diese Kommunikation ermöglichen. Eine im Vergleich zur Richtlinie 1999/93/EG strengere und detailliertere Vorgabe wäre hierfür äußerst hilfreich.
Das Kriterium der Sicherheit wird heute am besten erfüllt. Allerdings darf die Forschung in diesem Punkt nicht nachlassen, denn auch die Entschlüsselungsverfahren werden immer besser. Eine kontinuierliche Weiterentwicklung der verwendeten Verfahren ist unumgänglich. Zur Integration dieser verbesserten Verfahren in bestehende Systeme ist wiederum ein Standard erforderlich, an den neue Verfahren angepasst werden können. Dies zeigt, dass eine enge Verknüpfung der ersten beiden Punkte von enormer Bedeutung für den langfristigen Einsatz elektronischer Signaturen ist.

Die einfache Bedienbarkeit schließlich dient mehreren Zwecken. Zum einen erhöht sie die Akzeptanz beim Nutzer und damit die Bereitschaft zur Anwendung der Technologie. Zum zweiten erhöht eine zuverlässig erstellte Oberfläche die Sicherheit bei der Nutzung der Technologie, indem sie die Wahrscheinlichkeit von Fehlern auf Seiten des Nutzers verringert. Schließlich ermöglich eine klar strukturierte und einfach zu bedienende Oberfläche mit standardisierter Schnittstelle gleichzeitig, die dahinter liegende Technik zu verbergen, und dabei die leichte Austauschbarkeit der Technik und des Verfahrens ohne Beeinträchtigung des Nutzers zu gewährleisten. Für diesen letzten Unterpunkt ist erneut eine enge Bindung an Punkt 1 erforderlich.

Die Szenarien haben gezeigt, dass der Einsatz elektronischer Kommunikationsmedien Prozessabläufe enorm beschleunigen kann. Der klassische persönliche Besuch kann mehr und mehr durch den Einsatz sicherer elektronischer Kommunikationswege abgelöst werden. Dazu ist es aber notwendig, technische Unterstützung verstärkt an die Bedürfnisse der Umwelt und insbesondere der Nutzer anzupassen. Aufgrund der zunehmenden Bedeutung der Sicherheit persönlicher elektronischer Daten sollten alle potentiellen Nutzer an Forschungsergebnissen interessiert sein, die zur Verbreitung und Sicherheit elektronischer Signaturen beitragen.

6 Anhang

6.1 Konsistenzmatrix

		Technologie												Gesetzgebung							Gesellschaft							Wirtschaft								Wettbewerb			
		Alternative		Verbesser		Integration		Vernetzun		Standardis		Ergonomie		DS&DS		Rechtssta		Zertifizierungs			Einstellung		Sicherheit		Qualifikati		Dem	Wirtschaft		Investition		Status		Kundensu		Standardis		Konkurren	
		Ja	Nein	Ja	Nein	Hoch	Niedr	Zune	Abne	Ja	Nein	Verb	Stag	Strer	Gelo	Ja	Nein	Grem	Frei	Indiv	Posit	Nega	Gesc	Sorg	Hoch	Niedrig		Hoch	Gerin	Hoch	Gerin	Sekt	Nisc	Hoch	Kein	Hoch	Gerin	Viel	Weni
Technologie																																							
Verbesserung	Ja	-1	2																																				
	Nein	2	0																																				
Integrationsfä	Hoch	-1	1	1	0																																		
	Niedrig	0	0	0	1																																		
Vernetzung	Zunehm	0	0	1	-1	0	0																																
	Abnehm	0	0	0	1	0	0																																
Standardisieru	Ja	-2	2	2	0	2	-1	1	0																														
	Nein	2	0	0	0	0	1	0	0																														
Ergonomie	Verbes	-1	1	1	0	1	0	0	0	2	0																												
	Stagnie	0	0	0	0	0	0	0	0	0	0																												
Gesetzgebung																																							
DS&DS	Streng	0	0	0	0	0	0	0	0	0	0	0	0																										
	Gelockert	0	0	0	0	0	0	0	0	0	0	0	0																										
Rechtsstandar	Ja	-2	1	1	0	1	0	1	-1	1	0	0	0	2	-1																								
	Nein	1	0	0	0	0	1	0	0	0	0	0	0	0	1																								
Zertifizierungs	Gremium	0	0	0	0	0	0	0	0	1	0	0	0	2	0	1	0																						
	Frei	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0																						
	Individu	0	0	0	0	0	0	0	0	-1	1	0	0	-1	0	-1	1																						
Gesellschaft																																							
Einstellung	Positiv	0	1	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0																			
	Negativ	1	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0	0	0	0																			
Sicherheitsbe	Geschi	0	0	0	0	0	0	0	0	0	0	0	0	1	-1	0	0	0	0	0	1	0																	
	Sorglos	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0																	
Qualifikation	Hoch	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0															
	Niedrig	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0															
Demographie		0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	-1	0													
Wirtschaft																																							
Wirtschaftlichl	Hoch	-1	1	1	-1	1	-1	1	0	1	0	1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0												
	Gering	1	0	-1	1	0	0	0	0	-1	1	-1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0												
Investitionen	Hoch	-1	0	1	-1	1	0	1	-1	2	-1	1	0	0	0	0	0	0	0	0	0	0	1	-1	0	0	0	2	-1										
	Gering	2	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1										
Status	Sektor	-2	1	1	0	0	0	1	-1	1	0	1	0	1	0	0	0	-2	1	0	2	-1	1	-1	1	0	0	2	-1	2	-1								
	Nische	0	-1	-1	1	0	0	0	0	0	0	0	1	0	0	0	0	-2	1	0	0	1	-1	2	0	0	0	-1	1	-1	0								
Kundensuppor	Hoch	-1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	-1	0	0	1	0						
	Kein	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	1						
Wettbewerb																																							
Standardisieru	Hoch	-1	1	1	0	1	0	1	0	1	-1	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	2	0	0	0	0	0				
	Gering	1	0	0	1	0	1	-1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	-1	0	0	0	0	0				
Konkurrenz	Viel	0	0	0	0	2	-1	1	0	-1	0	0	0	0	0	-1	0	-2	2	1	1	0	2	-1	0	0	0	2	-1	1	0	2	-1	2	-1	-1	1		
	Wenig	0	0	0	0	-1	1	0	0	0	0	0	0	0	0	0	0	2	-1	0	0	1	0	0	0	0	0	-1	1	1	0	-2	2	-1	1	0	0		
Öffentliche Verwaltung																																							
Eigenentwicklu	Ja	-1	1	1	-1	1	-1	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	-1	1	-1	0	0	0	1	-1	0	0	0
	Nein	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

7 Quellen

7.1 Literatur

[Albe01] Albers, Olaf: „Gekonnt moderieren: Zukunftswerkstatt und Szenariotechnik – schnell und innovativ die Unternehmenszukunft gestalten“, Walhalla-Verlag, Regensburg 2001.

[Beck88] Becker, H.A: „Social Impact Assessment by Scenario Projects Combining Quantitative and Qualitative Analyses”, in: Impact Assessment Bulletin, Vol. 6 (1988), S. 89-102.

[Behr01] Behrens, Michael: „Biometrische Identifikation . Grundlagen, Verfahren, Perspektiven“; DuD-Fachbeiträge, Vieweg Verlag 2001.

[Bert02] Bertsch, Andreas: „Digitale Signaturen“, Xpert.press, Springer, Berlin Heidelberg 2002.

[BiJäWo05] Biebler, Karl-Ernst ; Jäger, Bernd; Wodny: Michael: „Biometrie“; Shaker 2005

[Bijl92] Bijl, R.: “Delphi in a Future Scenario Study on Mental Health and Mental Health Care”, in: Futures, April 1992, S. 232-250.

[Bove06] Bovenkerk, Eva: „Trendforschung. Darstellung, Bedeutung, Anwendungsbeispiel“. Vdm Verlag Dr. Müller, 1. Auflage 2006.

[Brei97] Breiner, Sibylle: „Die Sitzung der Zukunft – Eine Vorausschau mit Groupware-Szenarien“, Technik, Wirtschaft und Politik – Schriftenreihe des

Fraunhofer-Instituts für Systemtechnik und Innovationsforschung (ISI); Physica Verlag – ein Unternehmen des Springer-Verlags, Heidelberg 1997.

[Chal85] Chalmers, A.F.: „What Is This Thing Called Science: An Assessment of the Nature and Status of Science and Its Methods", University of Queensland, 2. Auflage 1985.

[Clau78] Clausewitz, Carl von: „Vom Kriege", Rowohlt Taschenbuch, 15. Auflage 1978.

[Fisch06] Fischer-Dieskau, Stefanie: „Das elektronisch signierte Dokument als Mittel zur Beweissicherung. Anforderungen an seine langfristige Aufbewahrung.", Nomos 2006.

[Geis99] Geis, Dr. Ivo (Hrsg.): „Rechtsaspekte des elektronischen Geschäftsverkehrs – Auf dem Weg zur Informationsgesellschaft; Kryptographietechnologien: Digitale Signatur und Verschlüsselung; Rechtliche Rahmenbedingungen", AWV – Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.B., AWV-Eigenverlag, Eschborn 1999.

[Geis00] Geis, Dr. Ivo (Hrsg.): „Die digitale Signatur – Eine Sicherheitstechnik für die Informationsgesellschaft. Ein Leitfaden für Anwender und Entscheider.", AWV – Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V., AWV-Eigenverlag, Eschborn 2000

[GeWi89] Geschka, H; Winckler, B.: „Szenarien als Grundlagen strategischer Unternehmensplanung", in: technologie und management, 38. Jahrgang, Nr. 4, 1989, S. 16-23.

[GlReSt95] Glade, Albert; Reimer, Helmut; Struiff, Bruno (Hrsg.): „Digitale Signatur & Sicherheitssensitive Anwendungen“, DuD Fachbeiträge, Vieweg, Braunschweig/Wiesbaden 1995.

[GWKHK07] Gruhn, Volker; Wolff-Marting, Vincent; Köhler, Andre; Haase, Christian; Kresse, Torsten: „Elektronische Signaturen in modernen Geschäftsprozessen“, Vieweg 2007.

[Heib04] Heibel, Heiko: „Die qualifizierte elektronische Signatur: Rechtliche Grundlagen, informationstechnische Konzepte und kritische Überlegungen zum ökonomischen Nutzen.“, Tectum 2004.

[Hoch01] Hochmann, Stephan: „Elektronische Signatur“, Books on Demand GmbH 2001.

[HoSc99] Hoeren, Thomas; Schüngel, Martin (Hrsg.): „Rechtsfragen der digitalen Signatur – Eine Einführung in Recht und Praxis der Zertifizierungsstellen“, Erich Schmidt Verlag, Berlin 1999.

[Jouv67] Jouvenel, Bertrand de: „Die Kunst der Vorausschau“, Luchterhand, Neuwied 1967.

[KaWi67] Kahn, H; Wiener, A.J.: The Year 2000 – A Framework for Speculation on the Next Thirty-Three Years“, The Macmillan Company, New York 1968.

[Konf02] Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Der Landesbeauftragte für den Datenschutz Niedersachsen (Hrsg.): „2002: Handlungsempfehlungen – Datenschutzgerechtes eGovernment“, Schlütersche Druck, Langenhagen 2002.

[Krei06] Kreibich, Rolf: „Zukunftsforschung“, ArbeitsBericht Nr. 23/2006, IZT – Institut für Zukunftsstudien und Technologiebewertung, Berling 2006.

[LaUl02] Langenbach, Christian; Ulrich, Otto (Hrsg.); „ Elektronische Signaturen – Kulturelle Rahmenbedingungen einer technischen Entwicklung“, Springer Verlag, Berlin/Heidelberg 2002.

[LeSc04] Lenz, Jörg W.; Schmidt, Christiane: „Die elektronische Signatur - eine Analogie zur eigenhändigen Unterschrift?“, Deutscher Sparkassen Verlag 2004.

[Mead72] Meadows, Dennis L; Meadows, Donella; Zahn, Erich; Milling, Peter: "Die Grenzen des Wachstums. Berichte des Club of Rome zur Lage der Menschheit", Deutsche Verlags-Anstalt, München 1972.

[Merk80] Merkle, Ralph C.: „Protocols for public key cryptosystems.”, in „Symposium on Security and Privacy”, Oakland, CA, USA, Seiten 122–134, 1980.

[Merk87] Merkle, Ralph C.: „A Digital Signature Based on a Conventional Encryption Function“, In „A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology”, Seiten 369–378, Springer-Verlag 1987.

[Pest74] Pestel, Eduard; Misahovic, Mihailo: "Menschheit am Wendepunkt. 2. Bericht des Club of Rome zur Weltlage", Deutsche Verlags-Anstalt, München 1974.

[Port91] Porter, A.L.; Roper, A.T.; Mason, T.W.; Rossini, F.A.; Banks, J.; Widerholt, B.J.: “Forecasting and Management of Technology”, John Wiley & Sons, New York et al 1991.

[Preu05] Preuss, Thorsten: „Digitale Signaturen im eGovernment – Archivierung im Langzeiteinsatz“. Hochschularbeit an der Universität Koblenz-Landau, Koblenz 2005.

[Raym97] Raymond, Eric S.: „The Cathedral & the Bazaar. Musings on Linux and Open Source by an Accidental Revolutionary“, Essay zum vierten Internationalen Linux-Kongress, Würzburg 1997.

[Reib87] Reibnitz, Ute von: „Szenarien – Optionen für die Zukunft“, McGraw-Hill, Hamburg 1987.

[Reib91] Reibnitz, Ute von: „Szenario-Technik: Instrumente für die unternehmerische und persönliche Erfolgsplanung“, Gabler, Wiesbaden 1991.

[ReNu00] Relyea, Harold C.; Nunno, Richard M.: „Electronic Government And Electronic Signatures”, Novinkar Books, Huntington, NY 2000.

[RoSc05] Roßnagel, Alexander; Schmücker, Paul: „Beweiskräftige elektronische Archivierung - Bieten elektronische Signaturen Rechtssicherheit?“, Economica Verlag 2005.

[Schn87] Schnaars, S.P.: „How to Develop and Use Scenarios“, in: Long Range Planning, Vol. 20, No. 1, 1987, S. 105-114.

[Schn07] Schneider, Sebastian: „eHealth in Europa. Szenarioanalyse für das Jahr 2020“, Vdm Verlag Dr. Müller 2007.

[Schr03] Schreiber, Lutz: „Elektronisches Verwalten – Zum Einsatz der elektronischen Signatur in der öffentlichen Verwaltung“, Schriften zur

rechtswissenschaftlichen Innovationsforschung, Nomos-Verlagsgesellschaft, Baden-Baden 2003.

[SiSi00] Singh, Simon: „Geheime Botschaften. Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet.“, Carl Hanser Verlag, 2000.

[Spah02] Spahni, Dieter: „eGovernment 2. Perspektiven und Prognosen.“, Haupt 2002.

[Thie70] Thieme, Hans (Hrsg.): „Die Vorausschau in den Wissenschaften“, Schulz, Freiburg im Breisgau 1970.

[TiEhGe04] Tinnefeld, Marie-Theres; Ehmann, Eugen; Gerling Rainer W.: „Einführung in das Datenschutzrecht. Datenschutz und Informationsfreiheit in europäischer Sicht“, Oldenbourg 2004.

[Tiet03] Tietje, O.: „Identificationof a small reliable and efficient set of consistent scenarios.“, European Journal of Operational Research (in press), 2003.

[Tule07] Tuletz, Holger: „eGovernment und aktivierender Staat. Möglichkeiten zur Lösung des staatlichen Steuerungsproblems.“, Vdm Verlag Dr. Müller 2007.

[Zwic89] Zwicky, Fritz: „Morphologische Forschung“, Baeschlin, 2. Auflage 1989.

7.2 Online

[1999/93/EG] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen;
http://eur-lex.europa.eu/LexUriServ/
LexUriServ.do?uri=CELEX:31999L0093:DE:HTML

[2252/2004] Verordnung (EG) Nr. 2252/2004 des Rates vom 13. Dezember 2004 über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten;
http://europa.eu.int/eur-lex/lex/LexUriServ/site/de/oj/2004/
l_385/l_38520041229de00010006.pdf

[ADeV29] Arbeitsdokument zur elektronischen Verwaltung (E-Government); Artikel 29-Datenschutzgruppe, 8. Mai 2003;
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/
e-government_de.pdf

[AElS00] 227/2000 Coll, ACT of 29 June 2000 on electronic signatures and on the amendment to certain other acts (Electronic Signatures Act) as subsequently amended, Umsetzung der EU-Richtlinie 1999/93/EG in der tschechischen Republik;
http://www.micr.cz/scripts/detail.php?id=1542

[Ar1106] ARENA Working Paper Series: 11/2006 „Decision-making under Pressure: The Negotiation of the Biometric Passports Regulation in the Council", 25. 09. 2006;
http://www.arena.uio.no/publications/working-papers2006/
papers/wp06_11.xml

[ATRUST] A-Trust, Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH;
http://www.a-trust.at/

[BeFe00] Berthold, Oliver; Federrath, Hannes: "Identitätsmanagement", Beitrag zur Sommerakademie 2000, Kiel;
http://www-sec.uni-regensburg.de/publ/2000/
BeFe2000IDMgmtSoAk/BeFe2000IDMgmt.pdf

[BGB1. II 00] Feststellung der Eignung des Vereins „Zentrum für sichere Informationstechnologie - Austria (A-SIT)" als Bestätigungsstelle (BGBl. II Nr. 31/2000 2.2.2000);
http://www.a-sit.at/pdfs/A-SIT_VO.pdf

[BGB1. II 02] Bestätigungsstellenverordnung – BestV (BGBl. II Nr. 299/2002 26.7.2002);
http://www.a-sit.at/pdfs/2002b299.pdf

[BGCA] BGCA-Maßnahme des IDA II-Programms: „Bridge/Gateway Certification Authority";
http://europa.eu.int/idabc/en/document/2318/556

[BMFS94] www.praxisinstitut.de: „Die Alten der Zukunft". Band 32 Schriftenreihe des Bundesministeriums für Familie und Senioren, 1994;
http://www.praxisinstitut.de/motzko/downloads/pdf/0205.pdf

[BMWI05] Bundesministerium für Wirtschaft und Technologie: „Chipkarten-Strategie der Bundesregierung (eCard-Strategie)", 2005;
http://www.bmwi.de/BMWi/Redaktion/PDF/E/
ecard-strategie,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf

[BRÄG06] Berufsrechts-Änderungsgesetz für Notare, Rechtsanwälte und Ziviltechniker 2006 - BRÄG 2006 geregelt;
http://www.a-sit.at/pdfs/BRAEG2006.pdf

[BSIBio] Bundesamt für Sicherheit in der Informationstechnik: „Einführung in die technischen Grundlagen der biometrischen Authentisierung“;
http://www.bsi.de/fachthem/biometrie/dokumente/
Technische_Grundlagen.pdf

[BSIeGov] eGovernment-Handbuch des BSI, Bundesamt für Sicherheit in der Informationstechnik;
http://www.bsi.bund.de/fachthem/egov/6.htm

[BSIeGov2] Projektgruppe E-Government im Bundesamt für Sicherheit in der Informationstechnik (BSI): „Authentisierung im E-Government: Mechanismen und Anwendungsfelder der Authentisierung“;
http://www.bsi.de/fachthem/egov/download/4_Authen.pdf

[BSIeSig] Grundlagen der elektronischen Signatur, Bundesamt für Sicherheit in der Informationstechnik;
http://www.bsi.bund.de/esig/esig.pdf

[BSIFBeSig] BSI-Faltblatt: „Elektronische Signatur“, Bundesamt für Sicherheit in der Informationstechnik;
http://www.bsi.de/literat/faltbl/F10ElektronischeSignatur.htm

[BSIFBKry] BSI-Faltblatt: „Kurzinformationen zur Sicherheit der Verschlüsselung“, Bundesamt für Sicherheit in der Informationstechnik;
http://www.bsi.de/literat/faltbl/F27Verschluesselung.htm

[BuKaAm] Bundeskanzleramt: „Bürgerkarte“, IKT-Strategie des Bundes; http://www.cio.gv.at/identity/

[CiKu07] Cimander, Ralf; Kubicek, Herbert: „eGovernment – Interoperability at Local and Regional Level. Good Practice Case. eInvoicing in Denmark – Case Study.”, eGovernment Unit – DG Information Society and Media, European Commission 2007; http://www.egov-iop.ifib.de/downloads/ Interoperability_in_eInvoicing_in_Denmark.pdf

[DOL] Deutschland Online; http://www.deutschland-online.de/DOL_Internet/broker

[DuE06] Dienstvereinbarung zu Einführung und Betrieb eines Identitätsmanagement, Universität Duisburg-Essen, 2006; http://www.uni-duisburg-essen.de/imperia/md/content/zentralverwaltung/ formulare/dienstvereinbarung_neufassung_zim_08_09_2006.pdf

[ElCA00] Electronic Communications Act 2000, Umsetzung der EU-Richtlinie 1999/93/EG im Vereinigten Königreich; http://www.opsi.gov.uk/acts/acts2000/20000007.htm

[ESI] Signaturbündnis; http://www.signaturbuendnis.de/

[eVergabe] e-Vergabe, die Vergabeplattform des Bundes; http://www.evergabe-online.de/

[Hand05] www.Handelsblatt.com: „Elektronische Pässe sind beschlossene Sache“, 22.06.2005;
http://www.handelsblatt.com/news/
Default.aspx?_p=200050&_t=ft&_b=916452

[ICRI] Interdisciplinary Center for Law and IT: „European Electronic Signatures Study”;
http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl

[IDABC-GER] IDABC European eGovernment services: „Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications - National Profile Germany”;
http://ec.europa.eu/idabc/servlets/Doc?id=29077

[IDABC-WP] IDABC European eGovernment services: „IDABC Work Programme - Third Revision. SECTION I: Project of common interest, Horizontal measures“;
http://ec.europa.eu/idabc/servlets/Doc?id=25302

[IDABC05] Interoperable Delivery of European eGovernment Services to public Administrations, Business and Citizens: Preliminary study on mutual recognition of eSignatures for eGovernment applications, IDABC – European eGovernment Services;
http://ec.europa.eu/idabc/en/document/6485/5938

[KdEG06] Kommission der Europäischen Gemeinschaften: „Bericht über die Anwendung der Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen“, Bericht der Kommission an das Europäische Parlament und den Rat, 2006;
http://ec.europa.eu/information_society/eeurope/i2010/docs/
single_info_space/com_electronic_signatures_report_de.pdf

[Körn06] Körner, Peter: „Die elektronische Signatur ist massentauglich“, Senior Strategic Business Development Manager Enterprise, Adobe Systems GmbH, 2006;
http://www.ffpress.net/Kunde/ADO/ATL/33751/

[KSA07] Kölner Stadtanzeiger: „PIN-Code und Fingerabdruck“, 21.09.2007;
http://www.ksta.de/html/artikel/1190059930159.shtml

[LElS01] Law on the Electronic Signature (no. 455/2001), Umsetzung der EU-Richtlinie 1999/93/EG in Rumänien;
http://www.legi-internet.ro/lgsemel.htm; inoffizielle Übersetzung ins Englische auf http://www.legi-internet.ro/en/e-sign.htm

[M@KT03] Media@Komm-Transfer;
http://www.innovatorsclub.de/

[MIS] Ministerium des Inneren und für Sport Rheinland-Pfalz:
„Aktionsplan eGovernment – Bericht und Handlungsleitfaden zur Verwirklichung von eGovernment in Rheinland-Pfalz“;
http://www.egovernment.rlp.de/eGovernment-Plan.pdf

[ÖBK] Website zur Österreichischen Bürgerkarte;
http://www.buergerkarte.at/

[PGP] Pretty Good Privacy;
http://www.pgp.com/de/company/index.html

[QESA00] Qualified Electronic Signatures Act (SFS 2000:832), Schwedische Umsetzung der Richtlinie 1999/93/EG;
http://www.pts.se/Archive/Documents/SE/
engelsk%20oversattning%20av%20lag%20elektroniska%20signaturer.pdf

[Roßn] Roßnagel, Prof. Dr. Alexander: „Die Signaturrichtlinie der EG und ihre Umsetzung“, Universität GH Kassel und Institut für Europäisches Medienrecht (EMR), Saarbrücken;
http://www.emr-sb.de/news/signatur.htm

[SaEGov] www.sachsen.de – Egovernment: „Basiskomponente elektronische Signatur und Verschlüsselung“;
http://www.egovernment.sachsen.de/55.htm

[SCADPlus] Website der Europäischen Kommission: Zusammenfassungen der Gesetzgebung der Union;
http://europa.eu/scadplus/

[SigG.at] (Österreichisches) Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG);
http://www.a-sit.at/pdfs/SigG.pdf

[SigG.de] (Deutsches) Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, Signaturgesetz (SigG); 16. Mai 2001;
http://bundesrecht.juris.de/bundesrecht/sigg_2001/index.html

[SigV.at] Signaturverordnung – SigV**;** Verordnung des Bundeskanzlers über elektronische Signaturen (incl. Änderung);
http://www.a-sit.at/pdfs/SigV.pdf

[SigV.de] Verordnung zur elektronischen Signatur (Signaturverordnung, SigV) vom 16. November 2001;
http://bundesrecht.juris.de/bundesrecht/sigv_2001/index.html

[SiPe06] Signature Perfect: Leitfaden Elektronische Signatur, 2006;
http://www.signature-perfect.com/docs/
Leitfaden_Elektronische_Signatur.pdf

[TS07] www.Tagesschau.de: „Fingerabdrücke künftig in Pässen“,
25.05.2007;
http://www.tagesschau.de/inland/meldung28784.html

[Zezs01] Dreißigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten Professor Dr. Friedrich von Zezschwitz, 2001;
http://www.datenschutz.hessen.de/TB30/Inhalt.htm

7.3 Sonstige

[Exp] Aussagen und Meinungen der beteiligten Experten (vgl. Kapitel 4.1)

8 Software

[Szeno] Szeno-Plan, Sinus Software und Consulting GmbH;
http://sinus-online.de

Erklärung der Urheberschaft

Hiermit erkläre ich, dass ich die vorliegende Arbeit allein und nur unter Verwendung der aufgeführten Quellen und Hilfsmittel angefertigt habe.

Christoph Moritz

Neuwied, 23. September 2007