



Diplomarbeit

eID als Enabler für eGovernment Applikationen

ausgeführt zum Zweck der Erlangung des akademischen Grades
Dipl.-Ing. für technisch-wissenschaftliche Berufe
am Fachhochschul-Masterstudiengang „Telekommunikation und Medien“ St. Pölten

von:

Mag. Carina Isabella Freudenthaler
tm0810262089

Erstbegutachter und Betreuer:
Univ.Prof. DI Dr. Thomas Grechenig

Zweitbegutachter:
FH-Prof. DI Grischa Schmiedl

St. Pölten, 01.11.2011



eID als Enabler für eGovernment Applikationen

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des FH-Masterstudienganges

Telekommunikation und Medien

eingereicht von

Mag. Carina Isabella Freudenthaler

tm0810262089

ausgeführt am

Institut für Rechnergestützte Automation

Forschungsgruppe Industrial Software

der Fakultät für Informatik der Technischen Universität Wien

Betreuung: Univ.Prof. DI Dr. Thomas Grechenig

Wien, 01.11.2011

Eidesstattliche Erklärung

Hiermit erkläre ich an Eides statt, dass ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Die Arbeit wurde bisher in gleicher oder ähnlicher Form keiner Prüfungskommission vorgelegt und auch nicht veröffentlicht.

St. Pölten, am

Name

Danksagung

An dieser Stelle möchte ich all jenen danken, die mich während meines Studiums begleitet haben und durch ihre fachliche und persönliche Unterstützung zum Gelingen der vorliegenden Diplomarbeit beigetragen haben.

Besonderer Dank gebührt Herrn Univ.-Prof. DI DR. Thomas Grechenig für die Betreuung meiner Diplomarbeit und der wissenschaftlichen Unterstützung sowie steten Förderung während der letzten Jahre.

Weiters möchte ich mich bei Herrn FH-Prof. DI Grischa Schmiedl für die Betreuung während meiner Studienlaufbahn auf der Fachhochschule bedanken.

Ich bedanke mich bei meinen engen Freundinnen und Freunden für ihre alltägliche Unterstützung und große Geduld während der gesamten Studienlaufzeit.

Herbert, ich danke Dir für die stete Unterstützung im beruflichen Bereich und für Deine Freundschaft in den letzten Jahren (f) !

Michi und Babsi, danke für die Entlastung vor allem während meines Auslandsaufenthaltes, ohne Euch hätte ich das nicht geschafft!

Sali, geteiltes Leid ist halbes Leid, danke!

Im Besonderen möchte ich meiner Mutter und meiner Großmutter danken, die mir dieses Studium durch ihre fortwährende Unterstützung überhaupt ermöglicht haben und mir stets Liebe und moralischen Beistand entgegengebracht haben.

Ich möchte diese Arbeit meinem Dad, Ing. Hannes Schneider, widmen, der 2002 von uns gegangen ist und furchtbar stolz auf mich wäre. Dad, ich bin jetzt Diplom Ingenieur!

Kurzfassung

Heutzutage leben wir in einer eArea, neue Begriffe wie eCommerce, eBusiness oder eGovernment prägen unser Leben. Neue Informations- und Kommunikationstechnologien ermöglichen gerade im Bereich der öffentlichen Verwaltung, dass Informationen und traditionelle Dienstleistungen auch über das Internet bereitgestellt werden. Durch die Schaffung eines eGovernment-Angebotes kann die Regierung näher an die BürgerInnen gebracht werden und BürgerInnen verstärkt in Prozesse und Entscheidungen eingebunden werden.

Verwaltungsverfahren setzen jedoch eine Identifikation der BürgerInnen voraus. In der digitalen Welt kann dies durch die Schaffung einer digitalen Identität ermöglicht werden. Diese digitale Identität ermöglicht es BürgerInnen, sich sicher für Anwendungen zu identifizieren und authentifizieren und gewährleistet eine sichere Übertragung von Daten durch Verschlüsselung und elektronische Signatur von Dokumenten.

Die Einführung von digitaler Identität bedarf der Schaffung einiger Grundlagen betreffend rechtlichen, organisatorischen und technischen Rahmenbedingungen sowie einer geeigneten Sicherheitsinfrastruktur. Die elektronische Identität kann unterschiedlich realisiert werden und bedarf technischer Hilfsmittel, wie Verschlüsselungsverfahren, Algorithmen und Protokolle. Als Träger der elektronischen Identität können unterschiedliche Token dienen, sowohl softwarebasiert als auch hardwarebasiert. Die am häufigsten eingesetzten Lösungen sind elektronische Identitätskarten (eID-Karten).

Einige Länder sind auf den „eGovernment-Zug“ aufgesprungen und haben Rahmenbedingungen für den Einsatz von eID geschaffen oder bereits eID-Lösungen etabliert. Anhand von Fallbeispielen unterschiedlicher Länder wird gezeigt welche Barrieren dabei entstehen können und vor welche Herausforderungen Länder gestellt sind. Für eine Etablierung eines sicheren und erfolgreichen eGovernments bedarf es mehr als einer reinen Realisierung von elektronischen Identitäten. Effizientes eGovernment hängt vor allem von der Nutzung seitens der BürgerInnen ab. Voraussetzung dafür ist eine Akzeptanz und Nutzung der angebotenen Dienstleistungen und Verfahren der öffentlichen Stellen. Diese Akzeptanz fördert eine intensive Nutzung von eGovernment Dienstleistungen und trägt damit wesentlich zum Erfolg von eGovernment bei.

Keywords: *elektronische Identität,, Authentisierung, Autorisierung, Identifikation, elektronische Signatur, Datensicherheit, Akzeptanz, eGovernment, eServices*

Abstract

Today we live in an eArea, new terms like eCommerce, eBusiness or eGovernment form our lives. New information and communication technologies enable - especially in the area of public administration - the supply of information and services via internet. With establishing an eGovernment supply the public authorities and citizen can be brought closer together and citizens will be integrated within processes and decisions.

Administrative procedures often require an identification of the Citizen. In the digital World, this can be realised by creation of a digital identity. This digital Identity enables a person, to identify and authentify for an application and guarantees a secure data transfer by means of encryption and electronic signature.

The introduction of digital identity requires the establishment of some fundamentals regarding legal, organizational and technical aspects as well as an appropriate security infrastructure. The electronic identity can be realised differentially by technical means as encryption procedures, algorithms and protocols. Different tokens, both software and hardware based, serve as carrier for electronic identities, there under smart cards are most commonly used.

Some countries have already jumped on the „eGovernment train“ and set up basic conditions for an implementation of eID, some have already established an eID solution. On the basis of case studies of different countries it will be shown which barriers can arise and how countries meet existing challenges. The establishment of a secure and effective eGovernment requires more than the realisation of electronic identity. Efficient eGovernment relies on the usage of its applications. Precondition is the consumer's acceptance and use of offered electronic services and procedures of public administration offices. This acceptance brings an intensive use of eGovernment services and so contributes to the success of eGovernment.

Keywords: *electronic identity, authentication, authentication, identification, electronic signature, data security, acceptance, eGovernment, eServices*

Inhaltsverzeichnis

Kurzfassung	iii
Abstract	iv
1 Einleitung	1
1.1 Problemstellung	2
1.2 Zielsetzung und wissenschaftliches Interesse	3
1.3 Aufbau der Arbeit	4
1.4 Methodik.....	6
2 Grundlagen	7
2.1 eGovernment.....	7
2.2 Die elektronische Identität	20
3 Realisierung von eID	27
3.1 Programme und Initiativen.....	27
3.2 Rahmenbedingungen.....	33
3.3 Grundlagen	42
3.4 Realisierung.....	61
4 eID im Einsatz	77
4.1 eID-Lösungen	77
4.2 eServices	90
4.3 ePortale.....	103
5 Herausforderungen	105
5.1 Rechtmäßigkeit	105
5.2 Organisation, Projekt- und Veränderungsmanagement	105
5.3 Infrastruktur, Technologien und Technikeinsatz	107
5.4 Digitale Spaltung	109
5.5 Akzeptanz.....	110
6 Zusammenfassung und Ausblick	115
ANHANG.....	119
Anhang A: Literaturverzeichnis.....	119
Anhang B: Abbildungsverzeichnis.....	135
Anhang C: Tabellenverzeichnis	136
Stich- und Fachwörterverzeichnis	137

Inhaltsverzeichnis

Kurzfassung	iii
Abstract.....	iv
1 Einleitung.....	1
1.1 Problemstellung.....	2
1.2 Zielsetzung und wissenschaftliches Interesse	3
1.3 Aufbau der Arbeit	4
1.3.1 Theoretische Begriffsabgrenzung	4
1.3.2 Voraussetzungen für die Realisierung.....	4
1.3.3 Praktische Umsetzung.....	5
1.3.4 Analyse der Erkenntnisse	5
1.3.5 Zusammenfassung und Ausblick.....	5
1.4 Methodik.....	6
2 Grundlagen	7
2.1 eGovernment.....	7
2.1.1 Was ist eGovernment?.....	7
2.1.2 Grundlagen und Charakteristika	8
2.1.2.1 Beziehungsebenen	8
2.1.2.2 Interne und externe Perspektive.....	9
2.1.2.3 Interaktionsniveau.....	10
2.1.2.4 Generationen des eGovernments	11
2.1.2.5 Charakteristika.....	13
2.1.3 Dienstleistungen und Portale.....	14
2.1.3.1 eServices	14
2.1.3.2 ePortale	17
2.1.4 Vorteile und Potentiale	18
2.2 Die elektronische Identität	20
2.2.1 Was ist eID?.....	20
2.2.2 eID-Lösungen.....	22
2.2.3 Anwendungsgebiete.....	24
2.2.4 Potentiale und Visionen	25
3 Realisierung von eID	27
3.1 Programme und Initiativen.....	27
3.1.1 Initiative „Europas Weg in die Informationsgesellschaft“	27
3.1.2 Initiative „eEurope – Eine Informationsgesellschaft für alle“	27

3.1.2.1	eEurope 2002	28
3.1.2.2	eEurope Smart Cards.....	29
3.1.2.3	eEurope 2005	29
3.1.3	Initiative „i2010 – Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung“.....	29
3.1.4	Ministererklärung zum eGovernment bis 2015	30
3.1.5	Initiative „Europe 2020 – Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum“	30
3.1.6	Gegenseitige Anerkennung von nationalen eID-Lösungen.....	30
3.1.7	Projekte und Initiativen von kleinerem Rahmen	31
3.2	Rahmenbedingungen.....	33
3.2.1	Sicherheit.....	34
3.2.1.1	Datenschutz	35
3.2.1.2	Datensicherheit	35
3.2.1.3	Sicherheitsinfrastruktur.....	36
3.2.2	Rechtlicher Rahmen	36
3.2.2.1	Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signatur.....	36
3.2.2.2	Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr	37
3.2.2.3	Richtlinie über die Verarbeitung personenbezogener Daten und deren Schutz der Privatsphäre in der elektronischen Kommunikation	38
3.2.2.4	Nationale Gesetze und Normen	38
3.2.2.5	Aktionsplan für elektronische Signaturen und die elektronische Identifizierung zur Förderung grenzübergreifender öffentlicher Dienste im Binnenmarkt	38
3.2.3	Technische Entwicklung.....	39
3.2.3.1	Auf der Nachfragerseite (BürgerIn)	39
3.2.3.2	Auf der Anbieterseite (Verwaltung)	39
3.2.4	Organisatorische Umsetzung	41
3.2.4.1	Umstrukturierung.....	41
3.2.4.2	Projekt- und Veränderungsmanagement.....	41
3.2.4.3	Koordination und Kooperation.....	42
3.3	Grundlagen	42
3.3.1	Hash-Verfahren	42
3.3.2	Verschlüsselung.....	43
3.3.2.1	Symmetrische Verschlüsselung (Secret Key).....	44
3.3.2.2	Asymmetrische Verschlüsselung (Public und Private Key).....	44
3.3.3	Verschlüsselungsalgorithmen	46

3.3.3.1	DES und AES.....	46
3.3.3.2	CAST.....	46
3.3.3.3	IDEA.....	46
3.3.3.4	RSA.....	47
3.3.3.5	DSA.....	47
3.3.4	Protokolle.....	48
3.3.4.1	Datenübertragungsprotokolle für Kartenlesegeräte.....	48
3.3.4.2	Authentifizierungsprotokolle für Webserver.....	50
3.3.5	Hardware.....	52
3.3.5.1	Smart Cards.....	52
3.3.5.2	Kartenlesegeräte.....	56
3.3.5.3	RFID.....	59
3.3.5.4	USB Token.....	60
3.3.5.5	Mobiltelefon und PDA.....	60
3.4	Realisierung.....	61
3.4.1	Elektronische Signatur.....	61
3.4.2	Zeitstempel.....	65
3.4.3	Digitale Zertifikate.....	65
3.4.4	Authentisierung und Autorisierung.....	68
3.4.4.1	Authentisierung.....	68
3.4.4.2	Autorisierung.....	71
3.4.4.3	eID-Anwendung.....	72
3.4.5	Implementation.....	73
3.4.5.1	Kerberos.....	73
3.4.5.2	Public Key Infrastruktur PKI.....	73
3.4.5.3	PKI mit X.509 Zertifikaten.....	74
3.4.5.4	PKI mit PGP.....	75
4	eID im Einsatz.....	77
4.1	eID-Lösungen.....	77
4.1.1	Username/Passwort Systeme.....	77
4.1.1.1	Länderbeispiel Norwegen.....	77
4.1.2	Soft Identity Token.....	78
4.1.2.1	Länderbeispiel Dänemark.....	78
4.1.3	Hard Identity Token.....	78
4.1.3.1	Smart Cards.....	78
4.1.3.2	Biometrische Daten.....	82
4.1.3.3	Mobile Token.....	83
4.1.4	eID-Systeme.....	83

4.1.4.1	Länderbeispiel Niederlande.....	83
4.1.5	Initiativen zur Förderung von eID	85
4.1.5.1	Länderbeispiel Belgien.....	85
4.1.5.2	Länderbeispiel Estland.....	85
4.1.5.3	Länderbeispiel Norwegen.....	85
4.1.6	Schwierigkeiten bei eID Implementierung.....	86
4.1.6.1	Länderbeispiel Spanien.....	86
4.1.6.2	Länderbeispiel Vereinigtes Königreich	87
4.1.6.3	Länderbeispiel Dänemark.....	87
4.1.6.4	Länderbeispiel Slowakei	89
4.1.7	Grenzüberschreitender Einsatz von eID.....	89
4.2	eServices	90
4.2.1	Good-Practice	91
4.2.1.1	Länderbeispiel Island	91
4.2.1.2	Länderbeispiel Finnland.....	91
4.2.2	Die gebräuchlichsten eServices.....	92
4.2.2.1	eTax.....	93
4.2.2.2	eVoting.....	95
4.2.3	Neue eServices	96
4.2.3.1	Antrag auf Pensionsförderungen	96
4.2.3.2	Online Jobsuche.....	96
4.2.3.3	Meldung von Polizeidelikten	96
4.2.3.4	Online Bahnticket	96
4.2.3.5	Online Football Tickets	97
4.2.3.6	DATEN BOX	97
4.2.4	Initiativen zur Förderung der Entwicklung und des Nutzens von eServices.....	97
4.2.4.1	Länderbeispiel Belgien.....	97
4.2.4.2	Länderbeispiel Malta	99
4.2.4.3	Länderbeispiel Island	100
4.2.5	Schwierigkeiten bei der Entwicklung von eServices	101
4.2.5.1	Länderbeispiel Lettland	101
4.3	ePortale.....	103
4.3.1.1	Belgium.be - Belgien.....	103
4.3.1.2	IRISbox - Belgien	103
4.3.1.3	Help.gv - Österreich.....	104
5	Herausforderungen	105
5.1	Rechtmäßigkeit	105

5.2	Organisation, Projekt- und Veränderungsmanagement	105
5.2.1	Kooperation, Kommunikation und Koordination.....	105
5.2.2	Kompetenzen, Qualifizierung und Motivation.....	106
5.2.3	Einbindung der Politik	107
5.3	Infrastruktur, Technologien und Technikeinsatz	107
5.4	Digitale Spaltung	109
5.5	Akzeptanz.....	110
5.5.1	eServices.....	110
5.5.1.1	Verfügbarkeit.....	110
5.5.1.2	Rasche Abwicklung	111
5.5.1.3	Bedienungsfreundlichkeit.....	111
5.5.1.4	Vollständigkeit des Angebots	112
5.5.1.5	Gebündeltes Angebot.....	112
5.5.2	Sicherheit.....	113
5.5.2.1	Vertrauen.....	113
5.5.2.2	Datenschutz und Datensicherheit	113
5.5.2.3	Security und Privacy Policies	113
5.5.3	Beispiel eVoting.....	114
6	Zusammenfassung und Ausblick	115
	ANHANG	119
	Anhang A: Literaturverzeichnis.....	119
	Anhang B: Abbildungsverzeichnis.....	135
	Anhang C: Tabellenverzeichnis	136
	Stich- und Fachwörterverzeichnis	137

1 Einleitung

Heutzutage leben wir in einer eArea: eBusiness, eCommerce, eGovernment und weitere Begriffe prägen unser alltägliches Leben. Ohne diese Stichworte ist unsere Gesellschaft und Wirtschaft nicht mehr vorstellbar. Informations- und Kommunikationsnetzwerke sind von großer Wichtigkeit geworden. Über 250 Million Europäer nutzen das Internet regelmäßig, 80 Prozent davon via Breitbandverbindung. In Europa sind 60 Prozent der öffentlichen Dienstleistungen online zugänglich (Europäische Kommission, 2008).

Doch der Informations- und Kommunikationsprozess ist in den letzten Jahren starken Veränderungen unterworfen worden: Eine ganze Reihe von Verfahren der öffentlichen Verwaltung wurden bereits online umgesetzt. Es existiert ein breites Spektrum an elektronischen Dienstlungen, welchen es BürgerInnen und Unternehmen ermöglicht, mit öffentlichen als auch privaten Einrichtungen und Institutionen auf unterschiedlichen Ebenen, auf Basis von Information bis hin zu Interaktion zu agieren.

Der Einsatz von digitalen Informations- und Kommunikationstechnologien sowie die Bereitstellung von Online-Dienstleistungen seitens der Regierungen bis hin zu einem „elektronischen Regieren“ werden als „Electronic Government“ (eGovernment) bezeichnet.

Durch das Angebot eines eGovernments werden Institutionen erreichbar und erlangen mehr Transparenz gegenüber der Öffentlichkeit. Auch interne Funktionen, Beziehungen, Interaktionen und Transaktionen werden durch eGovernment vereinfacht. Immer mehr nationale und lokale Regierungen stellen kritische Informationen online, automatisieren einst mühsame Prozesse und interagieren über elektronische Wege mit ihren BürgerInnen und Unternehmen.

Doch die Interaktion zwischen Verwaltung und BürgerIn erfordert die Einhaltung einiger Rahmenbedingungen, wie die Wahrung von rechtlichen Aspekten, oder einer organisatorischen Umsetzung, sondern auch die Beachtung wichtiger Faktoren.

Ein kritischer Faktor für den erfolgreichen und effektiven Einsatz von elektronischen Dienstleistungen ist die Wahrung von Sicherheit. Vor allem bei Amtsgeschäften die online durchgeführt werden ist der Schutz von Persönlichkeitsrechten im Umgang mit personenbezogenen Daten von großer Bedeutung. Die Sicherheit datenschutzrelevanter Informationsflüsse vor Verlust als auch Missbrauch ist notwendig. Weiters ist eine Einführung von hohen Sicherheitsstandards erforderlich um Daten und Systeme vor Missbrauch und unerlaubtem Zugriff zu schützen und Datensicherheit zu gewähren.

Viele Verwaltungsprozesse erfordern einen Nachweis der Identität einer Person. Es handelt sich hier hauptsächlich um Informationen zur eindeutigen Identifikation wie Name, Geburtsdatum, Geburtsort oder Nationalität.

Bei einer Umsetzung von Prozessen als Online-Dienstleistungen ist dieser Identifikationsnachweis ebenfalls notwendig und muss digital erfolgen.

Eine Möglichkeit der eindeutigen Identifikation einer Person bietet der Einsatz von „digitalen Identitäten“. Digitale Identitäten können auf mehreren Ebenen existieren, von der reinen Verwaltung verschiedenster Personendaten über Informationen zur Authentifikation und Autorisierung einer Person bis hin zum eindeutigen digitalen Identitätsnachweis. Verwaltungsverfahren setzen jedoch eine eindeutige Identifikation einer Person voraus, so bedarf dies einiger Voraussetzungen, wie beispielsweise der Implementierung von Sicherheitsfunktionen zur Authentisierung, Authentifizierung oder Identifikation. Neben der technischen Realisierung gilt es auch rechtliche Bestimmungen zu wahren.

Der Einsatz von elektronischen Medien bietet vor allem durch die Einbindung von eID-Lösungen viele Vorteile, sowohl auf Seiten der BürgerIn als auch der Regierung. So kann eine Optimierung, Automatisierung oder sogar eine gänzliche elektronische Abwicklung von Verfahren erfolgen. Potentiale wie eine Erhöhung der Wirtschaftlichkeit und der Dienstleistungsorientierung der administrativen Geschäfts- und Verwaltungsvorgänge können durch effektiven Einsatz von eID-Lösungen innerhalb von eGovernment ausgeschöpft werden.

Seitens der EU wurden bereits Programme gestartet, um das Potential einer vernetzten Gesellschaft zu demonstrieren und die Entwicklung und Verbesserung von eGovernment zu fördern.

Viele Länder haben bereits einen rechtlichen, technischen oder organisatorischen Rahmen geschaffen um eGovernment zu realisieren und durch den Einsatz von eID effektiv und effizient zu gestalten. Einige Länder starteten selbst Initiativen für den Einsatz elektronischer Identitäten und schufen einen Rahmen um eGovernment zu realisieren um den Einsatz von eID effektiv und effizient zu gestalten.

1.1 Problemstellung

In den letzten Jahren wurden seitens der EU und der Länder Programme und Initiativen geschaffen, um das Potential von eGovernment zu demonstrieren und eine Entwicklung zu fördern. Viele Länder nahmen diese Initiativen wahr, um ein effizientes und effektives eGovernment zu errichten. So begannen einige Länder, elektronische Dienstleistungen

(eServices) und eID-Lösungen zu entwickeln, welche in unterschiedlichsten Bereichen Einsatz finden.

Doch trotz erfolgreicher Implementierung von eID-Lösungen in einigen Ländern, stehen viele Regierungen noch Barrieren gegenüber. Aufgrund fehlender Voraussetzungen konnten viele transaktionsorientierte Geschäftsprozesse noch nicht als elektronische Anwendung umgesetzt und implementiert werden, manche Prozesse können nicht gänzlich medienbruchfrei über das Internet abgewickelt werden. Regierungen stehen vor Herausforderungen. Es gilt Probleme zu identifizieren und Barrieren hinsichtlich einer erfolgreichen Umsetzung und Anwendung von eID-Lösungen zu überwinden, um ein effektives und effizientes eGovernment zu ermöglichen.

Welche Potentiale bei einer erfolgreichen Überwindung dieser Barrieren durch einen erfolgreichen Einsatz von eID innerhalb von eGovernment möglich sind, soll diese Arbeit anhand von praxisnahen Beispielen zeigen. Der Fokus der Betrachtung liegt auf Ländern innerhalb der Europäischen Union.

1.2 Zielsetzung und wissenschaftliches Interesse

Die Zielsetzung der Arbeit ist die Wichtigkeit der Einbindung von eID in eGovernment zu untersuchen. Dabei werden folgende Fragestellungen behandelt und diskutiert:

- Wie wird eID im Rahmen von eGovernment eingesetzt?
- Welcher Voraussetzungen bedarf es dafür?
- Welche Barrieren gilt es zu überwinden und welche Potentiale können dadurch ausgeschöpft werden?

Einleitend werden Begrifflichkeiten abgegrenzt und ein theoretischer Hintergrund zu den Termini „eGovernment“ und „elektronische Identität“ gegeben. Folgend wird präsentiert, welche Initiativen seitens der EU und der Länder gestartet wurden, um die Schaffung und den Einsatz von eID-Lösungen innerhalb von eGovernment voranzutreiben. Gleichzeitig werden rechtliche, organisatorische und technische Rahmenbedingungen diskutiert, welche Voraussetzung für die Ermöglichung von elektronischen Identitäten darstellen.

Im Hauptteil der Arbeit werden einige Fallbeispiele präsentiert und es wird anhand verschiedener eID-Lösungen unterschiedlicher Länder gezeigt, wie eID in der Praxis um- und eingesetzt wird. Es wird diskutiert, welche Regierungen bereits Online-Lösungen unter Einsatz von eID bereitstellen und in welchem Entwicklungsstadium sich diese befinden. Bei der Länderwahl wurde der Fokus auf Europa gelegt und die Entwicklung von eGovernment-Lösungen in Ländern der Europäischen Union betrachtet.

Basierend auf diesen praxisbezogenen Beispielen wird betrachtet, welche Potentiale der Einsatz von eID innerhalb von eGovernment bietet. Parallel wird diskutiert vor welchen Herausforderungen Regierungen stehen, um einen effektiven und effizienten Einsatz von eID-Lösungen innerhalb der bereitgestellten elektronischen Dienstleistungen zu gewährleisten.

Das wissenschaftliche Interesse hinter der Arbeit begründet sich in der zentralen Fragestellung, wie eID als „Enabler“ für eGovernment Dienstleistungen dienen kann. Um dies zu beantworten werden unterschiedlichste eID-Lösungen an Fallbeispielen verschiedener Länder dargestellt und es wird gezeigt, welche Barrieren in der Umsetzung entstehen können und wie Potentiale ausgeschöpft werden. Interessant dahinter ist die Frage, weshalb einige Länder trotz der Schaffung vieler Grundlagen eine erfolgreiche Einbindung von eID nicht realisieren konnten.

1.3 Aufbau der Arbeit

Der/Die LeserIn wird anfänglich an das Thema herangeführt und mit den Begrifflichkeiten vertraut gemacht, welche als Basis für die weitere Arbeit dienen. Fortführend werden Rahmenbedingungen sowie die technische Realisierung von eID erläutert Anhand dieser Grundlagen und einiger Fallbeispiele unterschiedlicher Länder wird gezeigt, wie die eID in der Praxis realisiert wurde, vor welche Probleme Länder gestellt waren und welche Potentiale bei erfolgreicher Umsetzung ausgeschöpft werden konnten. Der/Die LeserIn bekommt in der Zusammenfassung noch einmal einen kurzen Überblick über behandelte Theorien und Erkenntnisse sowie einen Ausblick auf zukünftige Entwicklungen und Potentiale. Dementsprechend gliedert sich die Arbeit in folgende Abschnitte:

1.3.1 Theoretische Begriffsabgrenzung

Der erste Teil der Arbeit wurde dem theoretischen Ansatz gewidmet. Kapitel 2 behandelt sowohl Definitionen als auch Grundlagen der Begriffe „eGovernment“ und „eID“. Dabei werden sowohl die terminologischen als auch systematisierenden Grundlagen beider Begriffe beschrieben. Es wird ein Überblick über die wesentlichen Charakteristika, Ausprägungen und Anwendungsfelder von eID und eGovernment gegeben, die als Basis für die weitere Arbeit dienen.

1.3.2 Voraussetzungen für die Realisierung

Die Grundlagen für den Einsatz von elektronischer Identität werden in Kapitel 3 beschrieben. Vorab werden Initiativen und Programme auf internationaler sowie nationaler Ebene vorgestellt, welche gestartet wurden, um den Einsatz von eGovernment

und eID-Lösungen voranzutreiben und Vorgaben bezüglich deren Umsetzung zu erarbeiten.

Folgend werden Rahmenbedingungen betrachtet, welche sowohl rechtliche Gesetze und Normen umfassen, als auch Voraussetzungen für organisatorische Umsetzung, öffentliche Einbindung oder die Wichtigkeit von Sicherheit beschreiben.

Schlussendlich wird der technische Hintergrund, welcher Voraussetzung für die Erstellung, Implementierung und Anwendung von elektronischer Identität ist, dargestellt. Weiters wird auf die technische Realisierung, wie Verfahren der Verschlüsselung, Algorithmen, Protokolle etc. eingegangen.

1.3.3 Praktische Umsetzung

Kapitel 4 vereint die Theorie mit der Praxis. Basierend auf der Definition von Rahmenbedingungen für eine erfolgreiche und effiziente Realisierung von eID in eGovernment-Anwendungen werden in Kapitel 4 Anwendungsszenarien vorgestellt, wie weit existierende Konzepte bereits auf nationaler und internationaler Ebene praktisch umgesetzt wurden. eID-Lösungen unter realen Bedingungen werden an Fallbeispielen unterschiedlicher Länder präsentiert und deren Entwicklung, Potentiale, Defizite und Barrieren aufgezeigt.

Dabei wird der Fokus auf den Einsatz von elektronischen Identitätskarten bei elektronischen Dienstleistungen und eGovernment-Portalen gelegt. Weiters wird der grenzüberschreitende Einsatz von eID-Lösungen betrachtet und anhand von Lösungen aus der Praxis präsentiert.

1.3.4 Analyse der Erkenntnisse

Basierend auf der Präsentation unterschiedlicher Umsetzungen von eID-Lösungen in Kapitel 4 setzt sich Kapitel 5 mit Potentialen des Einsatzes von eID im eGovernment auseinander, listet Schwächen und Barrieren auf, welche es zu überwinden gilt und befasst sich mit konkreten Herausforderungen, denen unterschiedliche Länder gestellt sind.

1.3.5 Zusammenfassung und Ausblick

Abschließend fasst Kapitel 6 die wesentlichen Erkenntnisse aus Theorie und Praxis zusammen. Es wird ein Ausblick auf zukünftige Entwicklungen und Aktionspläne seitens der EU und der Länder bezüglich einer Digitalisierung von Dienstleistungen gegeben. Der Abschluss der Arbeit gibt einen Blick in die Zukunft, wie elektronische Identität zukünftig umgesetzt und eingebunden werden könnte, um eGovernment effektiv und effizient zu gestalten.

1.4 Methodik

Um einen allgemeinen Eindruck über die aktuelle Situation in unterschiedlichen Ländern zu gewinnen, wurde eine erste Internetrecherche gestartet. Offizielle Länderseiten, Informationsseiten von Außenministerien und öffentliche Einrichtungen, sowie Homepages von IT- und Kommunikationsunternehmen wurden aufgerufen um allgemeine Informationen sowie Kontaktadressen einzuholen.

Im Laufe der Arbeit wurden Kontakte zu unterschiedlichen Institutionen und Firmen sowohl per eMail, telefonisch als auch persönlich hergestellt.

Ein großer Teil des Kapitels, welches den Einsatz von eID in der Praxis zeigt, wurde den eGovernment Factsheets der Europäischen Union entnommen. Diese werden unter epractice.eu bereitgestellt, einem Informationsservice der Europäischen Kommission. Die Factsheets, eines von vielen Services die auf epractice.eu angeboten werden, bieten einen Überblick über den eGovernment Status und Fortschritt in Europäischen Ländern. Sie werden zwei Mal im Jahr erstellt und publiziert.

2 Grundlagen

In diesem Kapitel werden die theoretischen Grundlagen der Begriffe „eGovernment“ und „eID“ erläutert, welche als Basis für die weitere Arbeit dienen.

2.1 eGovernment

2.1.1 Was ist eGovernment?

„E-Government ist ... die elektronische Abwicklung der Geschäftsprozesse von Verwaltung und Regierung“ (Bundesministerium für Inneres, 2010).

Die Interaktion zwischen BürgerInnen und Regierung erfolgt traditionell in einer Behörde. Durch Einsatz von Informations- und Kommunikationstechnologien wird es möglich, diese Dienstleistungen näher zum Kunden zu bringen (The World Bank, 2011) und ermöglicht der Regierung über neue Wege mit BürgerInnen und Unternehmen zu agieren. Informationen und Dienstleistungen können durch Einsatz neuer Medien einer breiten Öffentlichkeit online zur Verfügung gestellt werden.

Dieser Einsatz von digitalen Informations- und Kommunikationstechnologien und die Bereitstellung von eServices seitens der Regierungen bis hin zu einem „elektronischen Regieren“ werden als „Electronic Government“ (eGovernment) bezeichnet.

Dementsprechend definieren Lucke und Reiner mann Electronic Government als „...die Abwicklung geschäftlicher Prozesse im Zusammenhang mit Regieren und Verwalten (Government) mit Hilfe von Informations- und Kommunikationstechniken über elektronische Medien“ (von Lucke & Reiner mann, Speyerer Definition von Electronic Government, 2000).

Der Begriff „Electronic Government“ bezieht sich dabei auf den elektronischen Austausch von Informationen, dem elektronischen Angebot von Dienstleistungen sowie elektronischen Transaktionen zwischen Regierung, BürgerInnen und Organisationen (Bundeskanzleramt, 2011).

Mit der Errichtung von eGovernment wird eine neue Kommunikationsplattform geschaffen (Dridi & Pernul, 2002).

eGovernment bezeichnet vor allem den Einsatz von elektronischen Datenbanken zur Aufbereitung und Abrufbarkeit von Informationen bei Ämtern und Behörden, sowie der Errichtung eines papierlosen elektronischen Verkehrs zwischen BürgerInnen und Behörde (Kahl & Weber, 2008).

Der scheinbar homogene Begriff „eGovernment“ ist dabei sehr vielschichtig und entzieht sich der einheitlichen Definition. Er umfasst verschiedene Prozesse zwischen dem öffentlichen Sektor und dem/r BürgerIn, zwischen Verwaltungen an sich und zwischen dem öffentlichem Sektor und der Wirtschaft. Die einzelnen Anwendungsfelder reichen vom Online-Informationsservice, über die Möglichkeiten der Kommunikation bis hin zur Durchführung von Transaktionen (Schaffry, 2004).

Durch die Verwendung von Informations- und Kommunikationstechnologie fördert eGovernment Effizienz und Effektivität, ermöglicht den Zugang zu Dienstleistungen zu vereinfachen und gewährleistet einen breit gefächerten öffentlichen Zugang zu Informationen. Dadurch wird es möglich, Government transparenter zu gestalten und näher an die BürgerInnen zu bringen (Basu, 2004).

2.1.2 Grundlagen und Charakteristika

2.1.2.1 Beziehungsebenen

eGovernment kommuniziert auf unterschiedlichen Beziehungsebenen, sowohl innerhalb der öffentlichen Verwaltung also auch zwischen der Verwaltung und der Bevölkerung, Wirtschaft und Organisationen (von Lucke & Reiner mann, Speyerer Definition von Electronic Government, 2000):

- Government-to-Citizen (G2C): Beinhaltet Informations- und Kommunikationsprozesse sowie Transaktionen zwischen Verwaltung, Politik und BürgerInnen
- Government-to-Business (G2B): Beinhaltet Interaktion zwischen der öffentlichen Verwaltung und Unternehmen. Letztere stellen beispielsweise Anträge, melden Daten oder fungieren als Auftragnehmer oder Lieferant (zum Beispiel bei öffentlichen Ausschreibungen)
- Government-to-Government (G2G): Beinhaltet alle Beziehungen zwischen den Verwaltungen untereinander, Weitergabe oder Abruf von Daten und Lieferbeziehungen
- Government-to-Employee (G2E): beinhaltet Angebot der Verwaltung für beschäftigte Arbeitgeber wie beispielsweise Beantragung von Materialbeschaffungen, oder Meldung von Dienstreisen und Urlaub

eGovernment richtet sich an unterschiedliche Adressatenkreise, nach außen an BürgerInnen oder Unternehmen (G2C, G2B) als auch innerhalb der Regierung an Ministerien, Behörden oder Angestellte um Prozesse und Leistungen innerhalb der Regierung auszuführen und zu vereinfachen (G2G, G2E).

2.1.2.2 Interne und externe Perspektive

Betrachtet man die Beziehungsebenen, auf welchen eGovernment stattfinden kann, so wird ersichtlich, dass eGovernment sowohl eine interne als auch externe Perspektive vereint. Die interne Perspektive betrachtet dabei den Einsatz von Informations- und Kommunikationstechnologien innerhalb der Verwaltung, beispielsweise Datenbankmanagementsysteme oder Workflow-Managementsysteme.

Die externe Perspektive betrachtet dagegen den Einsatz von Informations- und Kommunikationstechnologien an der Schnittstelle BürgerInnen, Unternehmen und Verwaltung (Dridi & Pernul, 2002).

Diese beiden Perspektiven werden durch die Begriffe „eDemokratie“ und „eAdministration“ repräsentiert: eDemokratie, welche sich nach außen und damit an die Beteiligung der BürgerInnen über neue Medien richtet und eAdministration, welche die Vereinfachung der Prozesse innerhalb der Regierung umfasst.

eDemokratie

Unter eDemokratie versteht man die Vereinfachung der Prozesse zur Information, Kommunikation sowie Transaktion zwischen und innerhalb von Institutionen, BürgerInnen, Unternehmen und Verwaltungen mittels Informations- und Kommunikationstechnologie. eDemokratie muss vor allem „people centered“ sein. eDemokratie umfasst Begriffe wie ePartizipation und eVoting, bei welchen eine öffentliche Meinungsbildung und Willensbildung eine zentrale Rolle einnehmen (SATW ICT-Kommission, 2007). Durch die Bereitstellung von Informationen kann eine elektronische Willensbildung gefördert werden und Bürger können über das Internet Einfluss auf politische Entscheidungen nehmen, beispielsweise durch Realisierung von elektronischen Wahlen (eVoting) (Prosser & Müller-Török, 2002).

eAdministration

Unter eAdministration versteht man den Einsatz von Informations- und Kommunikationstechnologie zur Vereinfachung der Verwaltungsprozesse innerhalb von Behörden sowie zwischen Behörden und BürgerInnen, Unternehmen und staatlichen Institutionen. Durch eAdministration können Prozesse vereinfacht oder automatisiert werden und somit Kosten gespart werden (Lalive d’Epinay, 2002).

Diese Arbeit konzentriert sich auf die Betrachtung der externen Perspektive und dem Einsatz von Informations- und Kommunikationstechnologien zur Bildung einer Kommunikationsplattform zwischen Verwaltung, BürgerInnen und Unternehmen (eDemokratie).

2.1.2.3 Interaktionsniveau

Bezugnehmen auf die Definitionen und dem internen und externen Ansatz von eGovernment wird ersichtlich, dass das Angebot von eGovernment vielseitig gestaltet ist. Es kann dabei auf unterschiedlichen Ebenen (Interaktionsniveaus) erfolgen, vom Angebot eines reinen Informationsportals bis hin zu Interaktionsmöglichkeiten mit Behörden. eGovernment kann auf folgenden Interaktionsstufen stattfinden (von Lucke, Internet-Technologien in der gesetzlichen Rentenversicherung, 1999):

Information

Diese Ebene umfasst das Bereitstellen von Informationen. Dazu zählen Informationssysteme, wie beispielsweise Bürgerinformationssysteme, Gremieninformationssysteme zur Unterstützung von Ausschüssen oder auch Fachinformationssysteme und Wissensdatenbanken (Prorok & Sallmann, 2001).

Kommunikation

Die Ebene der Kommunikation dient als Ergänzung der Informationsdienste beinhaltet neben dem interaktiven Aufruf von Informationen auch die Möglichkeit des Austauschs und der Partizipation. Hierzu zählen Angebote wie eMail, Foren oder Chatrooms bis hin zu Audio- oder Videokonferenzsystemen (Prorok & Sallmann, 2001).

Transaktion

Die Ebene Transaktion befasst sich mit der Durchführung von Dienstleistungen. eTransaktion reicht dabei von einfachen elektronischen Formularen bis hin zu ganzheitlichen Lösungen der öffentlichen Verwaltung sowie zum Angebot von öffentlichen Dienstleistungen (Prorok & Sallmann, 2001). In der höchsten Ebene der Transaktion werden Formulare nicht nur online ausgefüllt und versendet, sondern auch elektronische weiterbearbeitet.

Die beschriebenen Ebenen werden in Abbildung 1: Übergang von Information über Kommunikation zu Transaktion veranschaulicht.

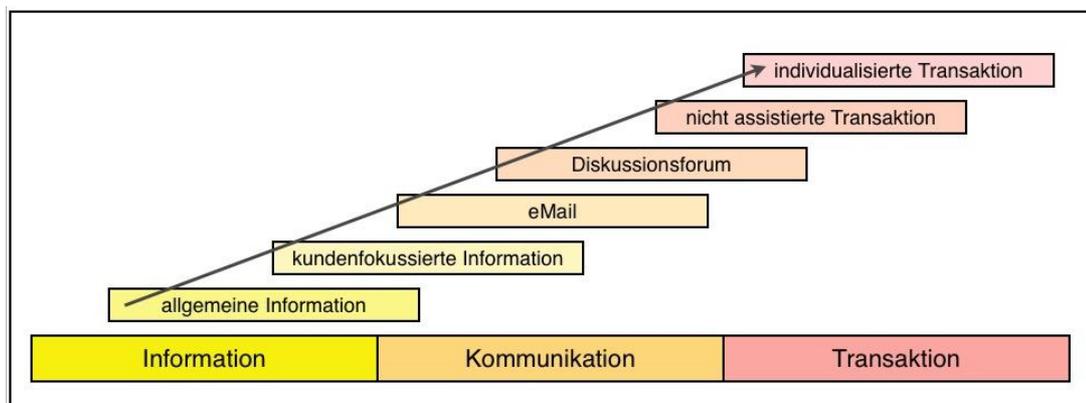


Abbildung 1: Übergang von Information über Kommunikation zu Transaktion (Mehlich, 2002)

Diese Ebenen unterscheiden sich in ihrem Interaktionsniveau. Bei reinen Informationsdiensten ist das Interaktionsniveau sehr niedrig, da sich die Interaktion nur auf ein Durchsuchen des Informationsangebotes beschränkt.

Die höchste Stufe der Interaktion bieten Transaktionsdienste, welche eine aktive Beteiligung der BürgerInnen durch elektronische Eingaben über das Internet sowie Reaktionen darauf ermöglichen. Diese bilden das Kernelement des elektronischen Geschäftsverkehrs (Dridi & Pernul, 2002).

Prorok und Sallmann bezeichnen diese Stufe als „True e-Government“ („echtes eGovernment“). „Echtes eGovernment“ liegt dann vor, wenn alle Prozessphasen auf elektronischem Weg und ohne Medienbrüche ablaufen (Prorok & Sallmann, 2002).

2.1.2.4 Generationen des eGovernments¹

Basierend auf den drei Interaktionsstufen des eGovernments startete die Europäische Kommission KEeLAN², welches zum Ziel hatte Internetangebote in der Praxis zu untersuchen. Durch eine systematische Untersuchung wurden 700 kommunale Internetauftritte aller EU Mitgliedsstaaten auf Serviceebene untersucht auf

- Verfügbarkeit von Informationen
- Funktionalität und Interaktionsgrad sowie
- Sicherheitsaspekte

Bei der Analyse wurde deutlich, dass die untersuchten Länder einen unterschiedlichen Ausprägungsgrad im Angebot von eGovernment Lösungen aufweisen; einige Länder bieten eine reine Informationsseite über Regierung, Entwicklung oder Neuerungen für Ihre BürgerInnen, andere wiederum ermöglichen interaktive Kommunikation mit einzelnen Ministerien.

¹ Sofern nicht anders angegeben, bezieht sich der Inhalt dieses Kapitel auf die Studie von KEeLAN (Elanet, 2003)

² Das Projekt KEeLAN (Key Elements for electronic Local Authorities' Networks) wurde im Februar 2002 als Teil des „IST-Programmes“ der Europäischen Kommission gestartet KEeLAN wurde durch Elanet koordiniert und hatte eine Projektlaufzeit von einem Jahr mit einem Budget von 1,25Mio €. Projektwebsite verfügbar unter <http://www.elanet.org/about-us/projects/keelan> (Zugriff am 01.10.2011)

KEeLAN teilte das Angebot von eGovernment in folgende Stufen (Generationen):

- Generation 0 – nicht online: Kein eigenes Internetangebot der Kommune beziehungsweise kein Angebot in einem spezifischen Servicebereich
- Generation 1 – Information: Grundlegende Informationen über Regierungsleistungen, Basisinformationen zu Themen und Dienstleistungen werden online angeboten
- Generation 2 – Ein-Weg-Interaktion: Abruf von Informationen, herunter ladbare Formulare und Dokumente, die auf konventionellem Weg an die Verwaltung geschickt werden können. Die verwendeten Systeme (zum Beispiel Formularserver) haben keine Anbindung an das Back-Office
- Generation 3 – Zwei-Weg-Interaktion: Elektronischer Austausch von Formularen und Informationen
- Generation 4 – Transaktion: Gänzliche elektronische Handhabung, Bestätigung und Bezahlung mit sicherer Authentifizierung
- Generation 5 – Integration von Dienstleistungen: Vollständiger Zugang zu elektronischen Dienstleistungen mit Verbreitung der Daten über Geschäftsstellen und Ämter hinaus

Die Generationen werden in Abbildung 2: Generationen des eGovernments, Eigendarstellung angelehnt an und grafisch dargestellt.

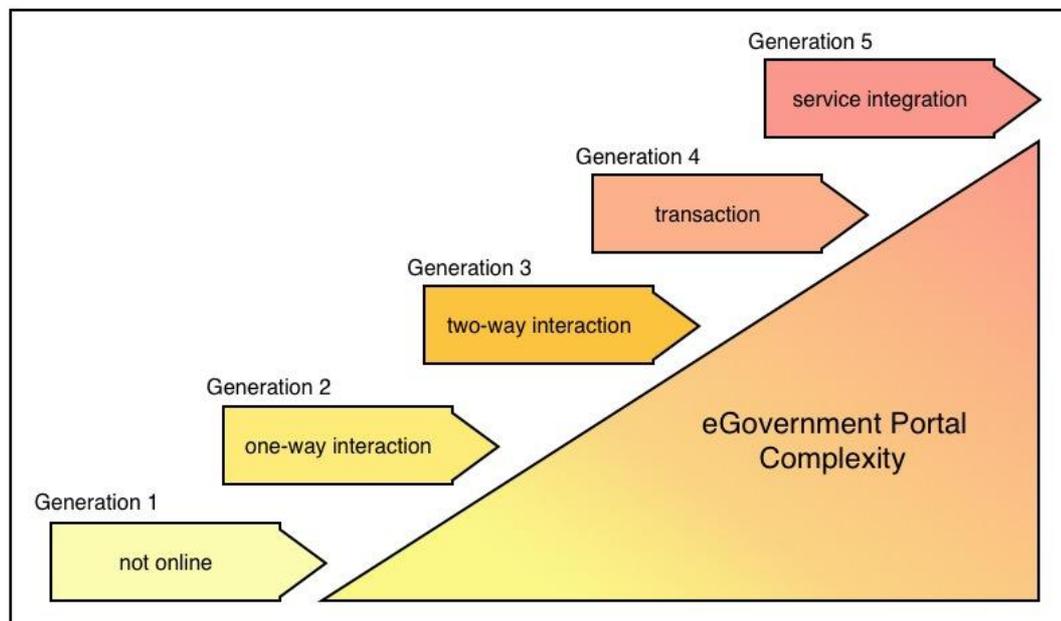


Abbildung 2: Generationen des eGovernments, Eigendarstellung angelehnt an (Elanet, 2003) und (Gisler & Spahni, Electronic Government – Ein Überblick, 2000)

Die Untersuchungen von KEeLAN brachten zum Ergebnis, dass sich die meisten angebotenen eServices in Generation 2 und 3 befinden. Die meisten Länder bieten reine Informationsseite über Regierungsangelegenheiten für Ihre BürgerInnen, nur wenige ermöglichen interaktive 2-Wege-Kommunikation mit einzelnen Ministerien. Der Sprung von Generation 2 zu 3 erscheint hier als der „Knackpunkt“.

Dieses Ergebnis wird auch durch andere Studien belegt. Capgemini führe im Auftrag der Europäischen Kommission einen Benchmark³ der Basisdienste im eGovernment durch und untersuchte diese nach „Verfügbarkeit“ und „Online Reifegrad“. Der Durchschnitt der erhobenen Staaten beim Indikator „Verfügbarkeit“ liegt bei 82 Prozent (Capgemini, 2010). Um den Grad der Online-Ausprägung der untersuchten Basisdienste zu messen, wurden diese in fünf Stufen unterteilt, von Stufe 1 Information bis Stufe 5 Automatisierung. Dieses 5-Stufenmodell gleicht dem Generationenmodell von KEeLAN.

2.1.2.5 Charakteristika

Die unterschiedlichen Ebenen und Dimensionen von eGovernment ermöglichen eine Bandbreite an Möglichkeiten, mit BürgerInnen, Unternehmen oder Institutionen zu interagieren. Dies macht eGovernment dynamisch und es ist gekennzeichnet durch folgende Charakteristika:

- Veränderung: Technologie verändert die Arbeitsweise der Regierung.
- Nahtloser Zugriff: BürgerInnen und Unternehmen erlangen Zugriff zu Regierungsdienstleistungen ohne Wissen über die Organisation der Regierung.
- Vielfache Zugangskanäle: BürgerInnen und Unternehmen können Dienstleistungen durch unterschiedliche Kanäle in Anspruch nehmen. Jene, welche Dienstleistungen nicht online nutzen können, haben nach wie vor die Möglichkeit, die Regierung auf traditionellem Wege zu kontaktieren.
- Überall und jederzeit: Dienstleistungen können überall und zu jeder Zeit elektronisch erbracht werden wie beispielsweise in der Schule, der Arbeit, zu Hause, vierundzwanzig Stunden pro Tag, sieben Tage die Woche. Dadurch kann die Interaktion mit BürgerInnen und Unternehmen einfacher, zuverlässig und effizient gestaltet werden.

³ Die Studie wurde in 27 EU-Mitgliedstaaten sowie Kroatien, Türkei, Island, Norwegen und der Schweiz durchgeführt und das Ergebnis im Rahmen der eGovernment Ministerkonferenz in Brüssel am 15. Dezember 2010 veröffentlicht.

2.1.3 Dienstleistungen und Portale

2.1.3.1 eServices

Viele Länder sind bereits auf den eGovernment-Zug aufgesprungen und bieten Informations-, Kommunikations- und Interaktionsmöglichkeiten zwischen BürgerInnen, Unternehmen und Verwaltung an.

Anhand der in Kapitel 2.1.2 beschriebenen Interaktions- und Beziehungsebenen kann die Breite des eGovernment-Angebotes an Dienstleistungen erahnt werden.

Vorab muss jedoch abgegrenzt werden, was der Begriff „Dienstleistung“ im Sinne des eGovernments bedeutet.

Dienstleistungen sind sowohl Tätigkeiten, die eine Behörde aufgrund eines gesetzlichen Auftrages als auch aufgrund einer Kundenanfrage ausführt. Darunter fallen beispielsweise Bereitstellung von Informationen zu einem Gesetzgebungsverfahren oder die Ausstellung eines Reisepasses.

Weiters umfasst der Begriff Dienstleistungen Tätigkeiten, die ein Kunde von der Behörde, beispielsweise aufgrund gesetzlicher Regelungen, in Anspruch nehmen muss. Auch hier wird von einer Dienstleistung der Behörde gesprochen.

Der Begriff der Dienstleistung wird hier, besonders in Bezug auf Verwaltungshandlungen, sowohl für die Tätigkeit und Leistung, welche Behördenmitarbeiter ausführen, als auch für das Produkt, das Ergebnis dieser Tätigkeiten, verwendet.

Dienstleistungen umfassen neben Transaktionsangeboten auch die reine Bereitstellung von Informationen und den Vertrieb von Produkten (Bundesamt für Sicherheit in der Informationstechnik, 2006).

Werden Dienstleistungen durch neue Informations- und Kommunikationstechnologien elektronisch umgesetzt und online zur Verfügung gestellt, so kann man von eServices sprechen. Unter eService werden alle Aktivitäten und Dienste zusammengefasst, die mit Computern erstellt wurden und über elektronische Medien interaktiv angeboten sowie ausgeführt werden (DATACOM, 2011).

eServices werden in vielen Bereichen angeboten (DATACOM, 2011):

- Online Informations- und Bildungsdienste, wie eEducation, eTeaching, eLearning, ePublishing, eBook, eZine oder eCatalog
- Online Beschaffungs-, Handels- und Bestelldienste, wie eBusiness, eProcurement, eCommerce, eCash, eShop, eAuction oder eIntermediary
- Elektronische kulturelle Dienste, wie eCulture
- Elektronische Beratung, wie eAdvising oder eConsulting
- Elektronische administrative Dienste, wie eGovernment

Im Fokus der Arbeit liegt das Angebot von administrativen Diensten. Administrative Dienste können sowohl für verwaltungsinterne Zwecke elektronisch umgesetzt, als auch BürgerInnen und Unternehmen zur Verfügung gestellt werden, um mit Behörden und Ämtern zu kommunizieren und interagieren⁴.

Diese Dienstleistungen werden von unterschiedlichsten Behörden der Regierung online angeboten, wie beispielsweise vom Einwohnermeldeamt, Finanzamt, Standesamt, oder dem Arbeitsamt (Güngöz & Seel, 2003). Diese bieten verwaltungsbezogene Prozesse online an und stellen sie als eServices zur Verfügung.

Daraus ergibt sich ein großes Angebot unterschiedlichster eServices, welche in Tabelle 1: Dienstleistungsangebot seitens der Behörde gelistet werden.

Tabelle 1: Dienstleistungsangebot seitens der Behörde (Zumsteg, 2004)

Bürgerdienst	Unternehmensdienste
Abstimmen und Wählen (eVoting)	Gewerbeanmeldung
Steuererklärung (eTaxes)	Steuererklärungen (eTaxes)
Soziale Sicherheit (Kindergeld, Stipendien, Arbeitslosenunterstützung)	Sozialversicherungsangaben für Mitarbeiter
Ausweispapiere (Pass, ID, Führerschein)	Arbeitsbewilligung für ausländische Arbeitskräfte
Baugenehmigung	Umweltrechtliche Genehmigungen
Heirats- und Geburtsurkunden	eProcurement
Wohnsitzanmeldung	Datentransfer zu statistischen Ämtern
Strafregisterauszug	Handelsregistereintrag
Polizeiliche Anzeigenerstattung	Markenanmeldung, Patentierung
Rechtsauskunft	Zollerklärung

Die Arbeit konzentriert sich hier auf eServices, welche von der Regierung für BürgerInnen angeboten werden und beschränkt sich hiermit auf den Bereich G2C⁵.

Viele Länder bieten bereits Informationen, Kommunikationsmöglichkeiten und Dienstleistungen für ihre BürgerInnen an. Das eGovernment Angebot ist dabei unterschiedlich fortgeschritten und reicht von dem reinen Informationsangebot bis hin zur Interaktion mit Behörden⁶.

⁴ für Details siehe Kapitel 2.1.2 Grundlagen und Charakteristika, Seite 9

⁵ siehe auch Kapitel 2.1.2 Grundlagen und Charakteristika, Seite 8

⁶ siehe auch Kapitel 2.1.2 Grundlagen und Charakteristika, Seite 8

Die einfachste Form umfasst das Angebot von Informationen (Alighierei, 2002). Die meisten Regierungen bieten bereits ein Informationsportal für BürgerInnen mit Informationen zur Regierung, den Ministerien und der Verwaltung und Interaktionsmöglichkeit mit einzelnen Behörden oder Institutionen an.

eGovernment schafft auch eine neue Kommunikation zwischen BürgerInnen und Behörden. So können BürgerInnen in die Gestaltung der Gesellschaft eingebunden werden, indem Diskussionsforen oder Chats mit politischen Entscheidungsträgern eingerichtet werden (Prorok & Sallmann, 2002).

„Echtes eGovernment“⁷ bedeutet jedoch, dass Transaktionen online durchgeführt werden. Alle Prozessphasen sollen auf elektronischem Weg ohne Medienbrüche ablaufen. Ein Beispiel dafür wäre eine Einbringung eines Antrages über das Internet, die Möglichkeit den Verfahrensstatus darüber abzufragen sowie die Zustellung eines Bescheides auf elektronischem Weg (Alighierei, 2002).

Ein Beispiel für eGovernment Dienstleistungen auf höchster Stufe ist das Angebot der elektronischen Teilnahme an Wahlen durch eVoting.

eVoting bezeichnet alle Formen von elektronischen Wahlen und umfasst sowohl den Einsatz von Wahlcomputern in Wahllokalen als auch Internetwahlen vom Computer zu Hause. Elektronisches Wählen wird für viele unterschiedliche Prozesse im öffentlichen Sektor verwendet. Der Begriff beinhaltet den Gebrauch von elektronischen Medien für die Einholung von Meinungen. Einen Teil davon bildet die Anwendung von elektronischem Wählen zur Evaluierung und Übermittlung von elektronischen Ergebnissen (Buchsbaum, 2004).

Ein elektronisches System zur Wahl muss folgende Voraussetzungen erfüllen (Andersson, Bylund, Olsson, Olsson, Seipel, & Sjödin):

- nur auserwählten Wählern ist es genehmigt zu wählen
- die Zählung muss korrekt und beweisbar sein
- die Stimmabgaben müssen anonym sein
- die Wähler müssen authentifiziert werden um eine Verfälschung der Wahl zu verhindern

⁷ „Echtes eGovernment“, „true eGovernment“, siehe Kapitel 2.1.2 Grundlagen und Charakteristika, Interaktionsniveau, Seite 10

eVoting Systeme müssen die eindeutige Identifikation des Wählers und die Anonymität der Stimmabgabe gewährleisten. Die Authentifizierung kann durch den Einsatz einer digitalen Signatur gelöst werden, sowie durch Passwort Authentifizierung, Smart Cards oder elektronischem Fingerabdruck (DATACOM, 2011).

2.1.3.2 ePortale

Das Angebot von elektronischen Dienstleistungen kann weit gefächert sein.

So kann der Nutzer seine Gesundheitsdaten beim Gesundheitsamt einsehen, seine Steuererklärung über die Seite der Steuerbehörde einreichen oder sich Informationen über politische Geschehen auf der Webseite der Regierung beschaffen. Den Überblick über das ganze Informations- und Service-Angebot zu wahren, fällt hier oft schwer.

Ein weiteres Problem ist, dass Dienstleistungen unterschiedlicher Behörden oft unterschiedliche Methoden zur Anmeldung oder Ausführung von Transaktionen einsetzen. Institutionen setzen unterschiedliche EDV Systeme ein, welche oft nicht kompatibel miteinander sind (Friedrichs, Hart, & Schmidt, *Balanced E-Government*": Visionen und Prozesse zwischen Bürgernähe und Verwaltungsmodernisierung, 2002). Dies erschwert zusätzlich die Verwendbarkeit unterschiedlicher Services.

Die Entwicklung von neuen Informations- und Kommunikationstechnologien sowie der Einsatz von neuen Medien fördern den Trend zur Standardisierung von Anwendungen und Systemen. Behörden versuchen ihre Dienstleistungen zu konsolidieren und eine einheitliche Plattform zu erstellen (Friedrichs, Hart, & Schmidt, *Balanced E-Government*": Visionen und Prozesse zwischen Bürgernähe und Verwaltungsmodernisierung, 2002).

So bieten einige Regierungen bereits sogenannte eGovernment-Portale an, welche Informationen und Dienstleistungen unterschiedlicher Institutionen, Ministerien und Behörden vereinen (Dridi & Pernul, 2002).

Unter dem Begriff eGovernment Portal versteht man die Portale der Gebietskörperschaften. Sie verweisen auf das elektronische Angebot von Informationen und Dienstleistungen der Behörden und Einrichtungen sowie unter- und übergeordneter Verwaltungsebenen (von Lücke, 2004).

Über diese Plattformen werden alle verfügbaren Informationen, Daten und Serviceangebote an einem Punkt gesammelt und aufbereitet (Dridi & Pernul, 2002). Das ePortal stellt damit einen zentralen Eintrittspunkt dar. Es hat die Aufgabe, den Benutzer zu Services der Institution zu leiten, welche die verschiedenen Dienstleistungen anbietet (Alighierei, 2002). Der/Die BürgerIn erhält die Möglichkeit, direkt mit den über das ePortal bereitgestellten eServices zu kommunizieren. Daneben hat das ePortal auch die Aufgabe,

Dokumente für die Darstellung oder Verarbeitung zu formatieren oder zu übersetzen (Alighierei, 2002).

ePortale bringen öffentliche Aspekte näher zu den BürgerInnen (Joswig & Stember, 2002). Das ePortal verfolgt das Prinzip "One face to the customer": Es bündelt alle öffentlichen Leistungen, der Kunde erhält alle notwendigen Leistungen „aus einer Hand“ (Güngöz & Seel, 2003), ohne sich Gedanken über die dahinter stehende Behörde oder eingesetzten Systeme machen zu müssen (Joswig & Stember, 2002).

Die Vorteile eines solchen Verwaltungsportals lassen sich folgend zusammenfassen (Joswig & Stember, 2002):

- Verwaltungsübergreifendes Dienstleistungsangebot
- Kompaktes Angebot an Dienstleistungen
- Bündelung von Service Angeboten
- Transparenz

Ein Bürgerportal soll eine sichere Kommunikation und Datenaustausch zwischen BürgerInnen und Verwaltung ermöglichen. Sicherheitsziele wie Vertraulichkeit, Authentizität, Integrität sowie Nachvollziehbarkeit sind hier kritische Faktoren. Dies erfordert, dass Dokumente und Daten welche von einem Nutzer an das Bürgerportal übergeben werden, von Seiten des ePortals integritätsgeschützt und verschlüsselt weitergeleitet werden um die Integrität zu gewährleisten. Dies kann durch den Einsatz von elektronischen Identitäten realisiert werden, welche die Identifikation und Authentisierung der BürgerInnen und eine Integrität der Daten ermöglicht⁸ (Krüger, 2009).

Laut Untersuchungen der Bertelsmann sind die Dienstleistungen im öffentlichen Sektor, welche über ePortale angeboten werden, generell sehr gut in Bezug auf Qualität und Quantität (Bertelsmann Stiftung, 2002).

2.1.4 Vorteile und Potentiale

Mit der Einführung von eGovernment schaffen Regierungen eine Kommunikationsplattform welche zahlreiche Möglichkeiten in unterschiedlichsten Bereichen der Gesellschaft, Politik und Wirtschaft eröffnen (Dridi & Pernul, 2002). Der Begriff eGovernment steht dabei als Synonym für moderne, sichere und effiziente Verwaltung (Bundeskanzleramt, 2011).

⁸ für Details siehe Kapitel 2.2.1 Was ist eID?, Seite 21

eGovernment ermöglicht es den Behörden - über den traditionellen Weg hinaus - Informationen und Dienstleistungen online einer breiten Öffentlichkeit verfügbar zu machen (Bundeskanzleramt, 2011). Amtliche Informationen werden über das Internet verbreitet. Schedler und Proeller sprechen hier von einer „Schaufensterfunktion“ des eGovernments (Schedler & Proeller, New Public Management, 2006). Weiters haben BürgerInnen und Unternehmen Zugang zu eServices der Verwaltung. Interaktive Dienstleistungen ermöglichen es, komplette Verwaltungsakte elektronisch abzuwickeln in denen keine persönliche Interaktion zwischen BürgerInnen und Verwaltung mehr notwendig ist (Schedler & Proeller, New Public Management, 2006). Es kommt zu einer Beschleunigung der Abwicklung, Prozesse und Verfahren erlangen höhere Transparenz (von Lucke & Reineremann, Speyerer Definition von Electronic Government, 2000).

Damit wird ein „One-Stop-Shop“ geschaffen, welcher den elektronischen Zugang zu Verwaltungen, losgelöst von Raum und Zeit, anbietet (Dridi & Pernul, 2002).

Lucke und Reineremann sprechen dabei von der „Neuen Erreichbarkeit“ von Daten, Abläufen und Personen (von Lucke & Reineremann, Speyerer Definition von Electronic Government, 2000).

Weiters kann durch den Einsatz von neuen Technologien eine Förderung von demokratischen Prozessen erfolgen (Schedler & Proeller, New Public Management, 2006). So können BürgerInnen aktiv und direkt an demokratischen Entscheidungsprozessen online teilnehmen, beispielsweise durch online Diskussionsforen oder der Teilnahme an elektronischen Wahlen (eVoting). Der/Die BürgerIn erfährt dadurch eine starke Einbindung in politische Prozesse (Bundeskanzleramt, 2011).

Durch diese Erreichbarkeit von Informationen und Dienstleistungen sowie der Einbindung der BürgerInnen in politische Prozesse wird die Bürgernähe zur Regierung verstärkt:

„Die neuen Informationstechnologien sind wichtige Instrumente für ein bürgernahes, modernes Verhältnis zwischen Staat und BürgerIn. Mit einer eGovernment – Offensive werden wir neue Maßstäbe setzen: Steuererklärung, Inskription, Gewerbeanmeldung und elektronische Signatur - all das kann künftig über ein Bürgerportal per Internet durchgeführt werden. ... Kurz gesagt: Wir machen Internet für alle.“⁹ (Schüssel, 2000)

⁹ Dieses Zitat stammt von Dr. Wolfgang Schüssel, welcher von 1995-2007 die Position des Bundesparteiobmannes der ÖVP inne hatte und von 2000 – 2007 Bundeskanzler der Republik Österreich war. Persönliches Profil unter <http://cmsbund.oedata.net/wolfgang-schuessel/> (Zugriff 29.9.2011)

Mit Schaffung dieser „virtuellen Verwaltung“ werden der Umgang und die Abwicklung von Prozessen nicht nur extern sondern auch intern vereinfacht und beschleunigt (Dridi & Pernul, 2002) und Amtsverfahren können automationsunterstützt abgewickelt werden.

„The Government can execute the procedure cost effectively, transparently and promptly, the citizens can be served anywhere and anytime, and the business is provided with the world’s best level on-stop service, be it domestic or foreign.“ (Yoon, 2007)

2.2 Die elektronische Identität

2.2.1 Was ist eID?

Das Internet hat uns in vielerlei Hinsicht bereichert. Dennoch weist es im Vergleich zu anderen Netzen erhebliche Defizite auf. Dazu gehört, dass Personen, welche sich im Internet bewegen, nicht immer eindeutig identifiziert werden können und anonym agieren. Dies ist meist bedenkenlos, jedoch gibt es zahlreiche potenzielle Anwendungsbereiche im Internet, in denen Anonymität kritisch ist. Hierbei geht es um Vorgänge, welche eine Verbindlichkeit oder zumindest Vertrauen erfordern wie in der Geschäftswelt oder in der Kommunikation und Interaktion mit der Verwaltung (Quade & Wölfle, 2010).

„Ohne gegenseitiges Vertrauen würden die Zusammenarbeit und das Zusammenleben nicht möglich sein“ – Fredy Knie Junior, artistischer Direktor des Schweizer National-Circus Knie¹⁰

Besonders in der digitalen Welt gilt es, dieses Vertrauen herzustellen. Es stellt sich die Frage, wie der Staat eine Atmosphäre gegenseitigen Vertrauens zwischen Verwaltung, BürgerInnen und Unternehmen schaffen kann (Riedl, 2011).

Die Grundlage verbindlicher Äußerungen oder Vorgängen ist eine sichere Identifikation der Beteiligten (Quade & Wölfle, 2010). In der analogen Welt würde die Identifikation von Person zu Person stattfinden und durch einen Identitätsnachweis, wie einem Ausweis, passieren. In der digitalen Welt ist dies nicht möglich. Der Nachweis der Identität bedarf hier mehr. Es muss ein elektronisches Äquivalent erzeugt werden, welches auch in der digitalen Geschäftswelt eine Identifikation der Geschäfts- und Handelspartner garantiert. Besonders für elektronische Verwaltungsprozesse und eGovernment Dienstleistungen ist ein sicherer Identitätsnachweis eine notwendige Voraussetzung (Eifert, Schreiber, & Stapel-Schulz, 2000).

¹⁰ Quelle des Zitats (Knie, 2001)

Der Staat steht bei der Einführung von eGovernment vor der Aufgabe, eine Grundversorgung an Sicherheit, Vertraulichkeit und Verbindlichkeit der Kommunikation zu sorgen (Schallbruch, 2009). Die Lösung für diese Problematik besteht in der Einführung einer digitalen Identität. Daten, welche eine Identifikation konventionell ermöglichen, müssen elektronisch abgespeichert und abgerufen werden können. So wird es möglich seine eigene Identität auch digital zu belegen (Französische Botschaft in Deutschland, 2009).

Die Frage ist jedoch, was ist Identität und wie lässt sich diese definieren, sodass eine Übertragung und Abbildung dieser in die digitale Welt erfolgen kann.

Üblicherweise wird von der Identität als Singular gesprochen, jedoch besitzen Personen meist viele unterschiedliche Identitäten zugleich. Ein Arbeitgeber sieht hinter der Identität des Arbeitnehmers Name, Geburtstag, Adresse, Bankverbindung, Steuernummer und Krankenversicherung. Im Gegensatz dazu spricht ein Versandhaus von Identität des Käufers und meint Name, Geburtstag, Adresse, Bankverbindung, Kundennummer und Kaufhistorie. Diese beiden Identitäten sind unterschiedlich und lassen sich voneinander trennen, haben jedoch überlappende Teilmengen, welche eindeutig genug sind, um sie zu einer Identität einer Person zusammenzuführen. Lutters spricht hier von Teilidentitäten, deren Summe die Identität einer Person bildet (Lutters, 2009).

Eine Identität ist damit alles, was sich zu einer Person zuordnen lässt. Diese Definition der Identität lässt sich auch auf digitale respektive elektronische Identität übertragen:

Nach Bernold ist die digitale Identität „gleich der Menge aller auf eine Person bezogenen digitalen Daten“ (Bernold, Ausgabe "Digitale Identäten", 2011). Eine digitale Identität verkettet damit alle im Internet vorhandenen Informationen über diese Person. Diese einzeln verteilten Informationen können als digitale Teilmengen der digitalen Identität angesehen werden. Die Summe der Teilmengen ergibt dann die digitale Identität (Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein, 2007).

Diese Beziehung zwischen Identität und technisch abgebildeter digitalen Identität wird in Abbildung 3: Identität, digitale Identität und digitale Teilidentität veranschaulicht.

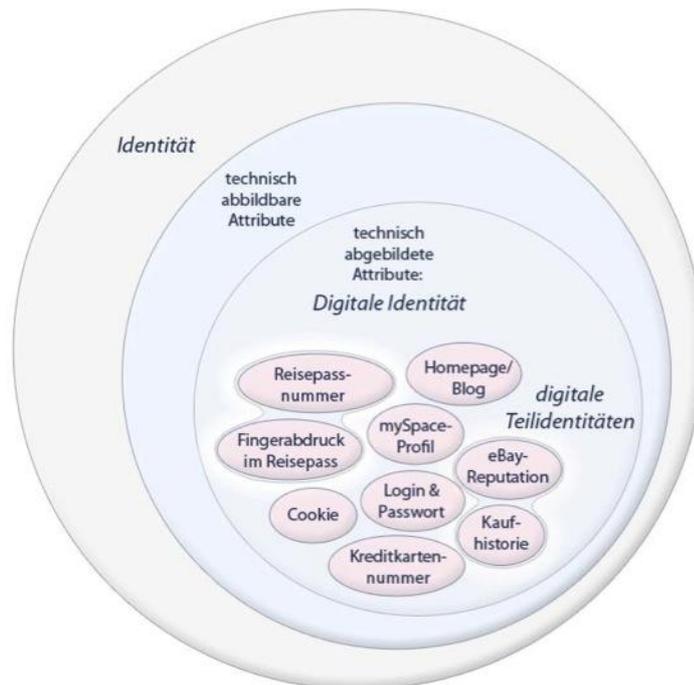


Abbildung 3: Identität, digitale Identität und digitale Teilidentität (Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein, 2007)

Durch den Einsatz neuer Technologien wird es möglich, die eigene Identität digital zu belegen (Französische Botschaft in Deutschland, 2009). Digitale Identitäten repräsentieren den Nutzer in der Informationsgesellschaft und bestehen aus allen Identitätsdaten, die dem Nutzer zugeschrieben werden können. Für eine Übertragung der Identität in die digitale Welt müssen diese Daten technisch abgebildet werden, beispielsweise durch Abspeicherung von Texten oder Bildern zu den Attributen (Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein, 2007).

2.2.2 eID-Lösungen

Der Nachweis der Identität in der digitalen Welt ist heute auf vielfältige Art möglich. Auf europäischer Ebene existiert bereits eine Unzahl an eID Konzepten, von der Verwendung von Username und Passwort über rein softwarebasierte Zertifikate bis hin zu Smart Card Lösungen (Sánchez, Pérez, Gómez, & Carracedo, 2010).

Um eine Identifikation zu ermöglichen, werden digitale Signaturen, Zugangskarten oder Wasserzeichen¹¹ eingesetzt. Doch diese Systeme haben eingeschränkte Geltungsbereiche

¹¹ Durch digitale Wasserzeichen-Verfahren werden digitale Medien um Informationen angereichert, welche nicht wahrnehmbar eingebettet werden. Diese Informationen können Urheberkennungen oder Transaktionsnummern sein. Diese Wasserzeichen helfen somit, Kopien von einem Original zu unterscheiden (Steinebach, 2009).

und werden für einen bestimmten Einsatz und unter gewissen Nutzungsbedingungen von Stellen ausgegeben (Krüger, 2009).

Ein Herzstück von eGovernment ist der elektronische Ausweis zur sicheren und eindeutigen Gewährleistung der Identität (Krüger, 2009). Dies ermöglicht einen sicheren Zugang zu Dienstleistungen und Informationen durch eindeutige Identifikation und Authentifizierung.

Der Ausweis dient bereits traditionell dazu, Personen bei unterschiedlichen Behörden zu identifizieren. Manche europäische Länder haben für diesen Zweck nationale Identitätskarten ausgegeben, welche die Identität der BürgerInnen enthält. Dieses Dokument hat sich über die Zeit von einem einfachen Blatt Papier mit einem Set von persönlichen Informationen bis hin zu digitalen Identitätsdokumenten entwickelt. Der Inhalt dieser Dokumente unterscheidet sich in unterschiedlichen Ländern nur gering und beinhaltet Attribute wie Foto, Unterschrift oder Fingerabdruck zur Identifikation des Inhabers.

Bieten Behörden nun die Möglichkeit, Verwaltungsprozesse rein elektronisch abzuwickeln, so erfordert dies ebenso einen Identitätsnachweis, welcher elektronisch erbracht werden muss. Es wird notwendig, dass BürgerInnen eine elektronische oder digitale Identität besitzen, welche ihnen erlaubt, sich im Internet zu identifizieren. Dies muss auf demselben Level passieren wie traditionell mit dem nationalen ID Dokument oder Karte. Viele Länder haben daher eine Infrastruktur aufgebaut welche den BürgerInnen erlaubt, sich mittels elektronischer Identitätskarten (eID-Karten) zu identifizieren. Diese sind dem traditionellen Identifikationsdokument sehr ähnlich, beinhalten aber einen Chip welcher Informationen über die Identität abspeichert. Solche Identitätskarten wurden bereits in Österreich, Belgien, Estland, Finnland, Italien, Portugal, Schweden und Spanien ausgegeben (Sánchez, Pérez, Gómez, & Carracedo, 2010).

Der Ausweis als traditionelles Mittel der Identifikation hat sich damit ebenso technologisch fortentwickelt (Eifert, Schreiber, & Stapel-Schulz, 2000) und wurde in die digitale Welt übertragen. Diese Identitätskarten können mit diversen zusätzlichen Funktionen ergänzt werden, wie digitale Signatur oder eine eindeutige Identifikation der BürgerInnen mittels eID-Funktion¹² (Bürge, 2002).

¹² siehe Kapitel 3.3 Grundlagen, Seite 45

2.2.3 Anwendungsgebiete

Durch standardisierte elektronische Identitätsnachweise ist es möglich, Nutzer von Informationen und Dienstleistungen eindeutig zu identifizieren und authentifizieren (Krüger, 2009). Durch Erweiterung der Identitätsdokumente um eine elektronische Signatur-Funktion sowie Authentifizierungsfunktion (Donath, 2009) wird es möglich, eine eID eindeutig einer natürlichen Person zuzuordnen (Eifert, Schreiber, & Stapel-Schulz, 2000). Mit eID kann sich der/die BürgerIn sicher authentisieren oder ein Dokument rechtsverbindlich unterschreiben. Dadurch können elektronische Transaktionen sicher abgewickelt werden (Bürge, 2002).

Diese Funktionen digitaler Identitätskarten ermöglichen den Gebrauch von einer Vielzahl an Anwendungen, da ein zertifizierter Identitätsnachweis meist notwendige Voraussetzung für eGovernment Prozesse ist. Ein zertifizierter elektronischer Identitätsnachweis für BürgerInnen darstellt. Damit wird es erst möglich, Verwaltungsakte bei Behörden einer bestimmten Person zuzuordnen (Eifert, Schreiber, & Stapel-Schulz, 2000).

Der Einsatz von elektronischer Identität ermöglicht die Nutzung digitaler Dienste wie beispielsweise Anmeldung an Computersystemen, rechtsverbindliche Vertragsabschlüsse über elektronische Wege sowie eine rein elektronische Übermittlung von Formularen der Verwaltung (Donath, 2009). Dadurch kann eine vollständige elektronische Abwicklung von unterschiedlichen Verwaltungsprozessen, wie eTax realisiert werden und Transaktionen medienbruchfrei genutzt werden (Schallbruch, 2009).

Durch Übertragung des Identitätsnachweises in die elektronische Welt können viele Dienstleistungen auch online erbracht und ausgeführt werden, welche eine eindeutige Identifikation des Nutzers voraussetzen. Ein gutes Beispiel dafür ist die Teilnahme an Wahlen. eVoting Systeme müssen die eindeutige Identifikation des Wählers und die Anonymität der Stimmabgabe gewährleisten. Die Authentifizierung kann durch den Einsatz digitaler Signatur gelöst werden, sowie durch Passwort Authentifizierung, Smart Cards oder durch einen elektronischen Fingerabdruck (DATACOM, 2011).

Ein weiterer Einsatz von elektronischen Identitätsnachweisen liegt im Gesundheitssektor. Hier werden Chipkarten eingesetzt, um Identitätsdaten und medizinische Daten und Befunde von Patienten zu speichern. Ein großer Vorteil dieses Netzwerkes liegt in der ständigen Verfügbarkeit der Patientenaufzeichnungen. Dadurch kann auf Daten jederzeit und überall zugegriffen werden. Diese Identitätskarten werden in ein System integriert, welches auch die Sozialversicherungsstelle miteinschließt. So wird ein medizinisches Netzwerk geschaffen.

2.2.4 Potentiale und Visionen

Der Einsatz von neuen Informations- und Kommunikationstechnologien haben das Verhalten und die Art der Interaktion in den letzten Jahren stark geprägt und die Welt schnelllebig gemacht. In der digitalen Welt stellt sich oft die Frage, wen man vor sich hat. Identitäten sind zweifelhaft.

Der Umgang mit Identitätsdaten im Internet gewinnt mehr und mehr an Bedeutung. Das Internet bringt viele Vorteile mit sich, birgt jedoch auch neue Risiken, besonders durch ungeschützte und unkontrollierte Herausgabe von Daten während der Kommunikation und Transaktion im Internet (Schallbruch, 2009). Emails können von unberechtigten Personen gelesen werden, Inhalt und Absender können gefälscht werden, Webserver sind in der Lage eine gefälschte Identität vorzugeben, Daten oder Software können manipuliert werden.

Grundvoraussetzung für eine digitale Kommunikation und Interaktion im digitalen Geschäftsverkehr ist Sicherheit, Vertraulichkeit sowie Integrität und Authentizität. Daher verlangen eine große Anzahl an eServices eine Identifikation (Bernold, Digitale Identitäten als Grundstein des Vertrauens im Internet, 2011). Notwendige Voraussetzung für eGovernment Prozesse ist ein zertifizierter elektronischer Identitätsnachweis von BürgerInnen.

Durch den Einsatz von standardisierten Mitteln wird es möglich, Identitäten zu belegen (Bernold, Digitale Identitäten als Grundstein des Vertrauens im Internet, 2011). Durch die Einführung einer elektronischen Identität wird es möglich, aus der Anonymität der Masse herauszutreten und sich als klar identifizierbarer Kommunikations- und Geschäftspartner zu erkennen zu geben. Dies schafft Vertrauen in sensiblen Bereichen durch Unverwechselbarkeit von Personen, Urhebern und Absendern (Donath, 2009).

ID-Karten ermöglichen dem Nutzer, seine Daten selbst zu verwalten und nur für den Nutzungszweck notwendigen Umfang an Identitätsmerkmalen zur Verfügung zu stellen. Es wird den BürgerInnen möglich werden, ihre elektronischen Daten und deren Übermittlung zu kontrollieren (Schallbruch, 2009). Gleichzeitig wird durch die Nutzung der Karten in der digitalen Form ein Zugang zu digitalen Diensten durch eine verlässliche Identifikation und Authentifizierung ermöglicht (Krüger, 2009).

Für den User bedeutet der Einsatz von digitalen Identitäten somit, Vertrauen in die Kommunikation und Anwendung des Internets aufzubauen (Französische Botschaft in Deutschland, 2009).

Auch eGovernment profitiert auf allen Ebenen von dem Einsatz von elektronischen Identitäten und die Ziele des eGovernments werden erreichbar.

So können viele Prozesse zur Abfrage von Standarddaten automatisiert, Verträge vollelektronisch signiert und Prozesse elektronisch abgewickelt werden (Schallbruch, 2009), da die digitale Identität des Schriftformerfordernis entbehrlich wird und die BürgerInnen eindeutig identifiziert werden können.

Transaktionen können medienbruchfrei genutzt werden. Dies wiederum fördert den Abbau von Bürokratie und die Last von Papierarbeit kann reduziert werden.

Durch den Einsatz digitaler Identität wird auch die Sicherheit und Zuverlässigkeit der Kommunikation und Identifikation erhöht (Schallbruch, 2009). Dadurch wird es möglich, Nutzern das notwendige Vertrauen in die Kommunikation und Anwendungen im Rahmen des Internets zu geben (Französische Botschaft in Deutschland, 2009). Dies macht die eID zum wichtigsten Schlüssel für eine sichere und vertrauenswürdige Beziehung im virtuellen Raum (Donath, 2009).

3 Realisierung von eID

3.1 Programme und Initiativen

eGovernment gilt weltweit als wichtiger Beitrag der Behörden und Regierungen zur Modernisierung der Verwaltungen und Verbesserung der Wettbewerbsfähigkeit der Standorte. Auch die Europäische Union hat die Wichtigkeit von eGovernment erkannt und startete einige Initiativen zur Etablierung einer globalen Informationsgesellschaft. Inhalt dieser ist die Schaffung von globalen Standards um den Kontakt zu öffentlichen Behörden für BürgerInnen und Unternehmen zu vereinfachen und eine Veränderung auf gesellschaftspolitischer Ebene herbei zu führen.

3.1.1 Initiative „Europas Weg in die Informationsgesellschaft“

Bereits 1994 startete die Europäische Union die erste europäische Initiative im Bereich des eGovernments mit einem Aktionsplan der Europäischen Kommission „Europas Weg in die Informationsgesellschaft“¹³. Ziel des Aktionsplanes war der Anschluss Europas an die globale Informationsgesellschaft, um Europa wettbewerbsfähig zu machen. Alle Mitgliedsstaaten der EU wurden aufgefordert, alle gemeinschaftlichen Vereinbarungen des Aktionsplanes, wie beispielsweise Ermöglichung des Zugangs für alle BürgerInnen zu neuen Technologien, zu erfüllen (Europäische Kommission, 1994). Weitere Entschlüsse innerhalb dieses Aktionsplanes in den Jahren 1996 und 1997 umfassten Bereiche des Urheberrechtes, Normen und Rechtsbestimmungen, verschlüsselte Dienste, elektronische Unterschriften und elektronischer Handel. Es wurde ein mehrjähriges Programm zur Anregung der Entwicklung dieser Technologien entworfen, mit dem Ziel der Förderung der Vielfalt der Informationsgesellschaft.

3.1.2 Initiative „eEurope – Eine Informationsgesellschaft für alle“

Ende 1999 wurde die eEurope Initiative¹⁴ seitens des Europäischen Rates und der Europäischen Kommission gestartet. Es war eine breit angelegte Initiative und der nächste Versuch, positive Änderungen der Informationsgesellschaft hervorzurufen und den europäischen Mitgliedsstaaten dadurch Vorteile zu verschaffen (Panayiotou, 2004).

Ziel war es, neue Innovations- und Kommunikationstechnologien in den Mitgliedsstaaten zu fördern und dadurch BürgerInnen, Firmen und Verwaltungen in das digitale Zeitalter zu

¹³ Aktionsplan verfügbar unter http://aei.pitt.edu/947/1/info_society_action_plan_COM_94_347.pdf (Zugriff am 01.10.2011)

¹⁴ eEurope war Teil der Lissabonner Strategie, einer globalen Strategie des Europäischen Rates um Europa zu einem weltweit wettbewerbsfähigen Wirtschaftsraum zu machen (Europäische Kommission, 2002)

führen. Durch die Schaffung eines digitalen Europas sollten alle Europäer die Vorteile der neuen Informationsgesellschaft nutzen können und damit zu einer Verbesserung der Lebenssituation beitragen (Europäische Kommission, 1999).

Mitgliedsstaaten wurden aufgefordert Zugang zu öffentlichen Informationen und Diensten für BürgerInnen und Unternehmen durch Einsatz des Internets zu vereinfachen. Damit sollte die Transparenz der öffentlichen Verwaltung erhöht werden. Weiters konnte der/die BürgerIn interaktiv in den Entscheidungsprozess eingebunden werden.

Mit der eEurope Initiative verpflichteten sich die Mitgliedsstaaten unter anderem zur Erfüllung folgender Maßnahmen (Europäische Kommission, 1999):

- Führung ins digitale Zeitalter
- Preisgünstigere Internetangebote
- Schnelleres Internet für Wissenschaftler und Studenten
- Förderung des elektronischen Geschäftsverkehrs
- Sicherer elektronischer Zugang durch intelligente Chipkarten
- Einbindung von Personen mit körperlichen Einschränkungen in die Informationsgesellschaft
- Elektronische Gesundheitsvorsorge
- Elektronische Regierung im Internet

Einer der Maßnahmen war die Einführung von Smart Cards für einen Zugriff auf Gesundheitsservices, elektronischen Zahlungen, mobiles Internet oder öffentlichen Transport (Europäische Kommission, 1999). Damit hat Europa einen wichtigen Grundstein gelegt in Bezug auf Realisierung von sicheren eServices.

3.1.2.1 eEurope 2002

Um die Ziele von eEurope zu erreichen wurde ein Maßnahmenkatalog erstellt „eEurope 2002“, mit dem Ziel, Europa bis 2010 durch Einsatz von Informations- und Kommunikationstechnologie dynamisch und wettbewerbsfähig zu machen.

Hauptziele von „eEurope 2002“ waren (Europäische Kommission, 2001):

- Das Angebot eines billigen, schnellen und sicheren Internets
- Investition in Menschen und Fertigkeiten sowie
- Die Förderung der Nutzung des Internets

Eines der Hauptziele war die Gewährleistung eines sicheren Internets und somit wurde die Schaffung sicherer Netzwerke und Smart Cards Teil dieses Ziels. Es sollte Entwicklung von eServices und damit die Einbeziehung der BürgerInnen und Unternehmen gefördert werden. Als Maßnahme wurde die Verwendung von digitalen Signaturen gesehen (Europäische Kommission, 2001).

3.1.2.2 eEurope Smart Cards

Mit dem Aktionsplan eEurope 2002 erkannte die Europäische Kommission die Wichtigkeit von Smart Cards als Schlüsselement zu einem sicheren Zugang zu elektronischen Anwendungen und Dienstleistungen. Anfang 2000 wurde die Smart Card Charter gegründet, welche technische Hindernisse und deren Bewältigung definierte. Die Erkenntnisse der Charter wurde in einen Aktionsplan¹⁵ übertragen, welcher allgemeine Voraussetzungen für den Einsatz von Smart Cards definiert. Die Vision der Initiative ist ein uneingeschränkter Einsatz von Smart Card Funktionen sowie ein flächendeckender Einsatz von Smart Card Technologien als Vertrauens-Plattform (van Arkel & Martiny, 2002).

3.1.2.3 eEurope 2005

Nach der Initiative eEurope 2002 folgte eEurope 2005. eEurope 2005 griff die Ansätze von 2002 auf, ergänzte diese oder passte sie an und sah weiters die Schaffung von notwendigen Rahmenbedingungen vor.

Ziel war es, öffentliche Dienstleistungen in Hinblick auf Qualität zu verbessern und damit die wirtschaftliche Produktivität zu steigern. Weiters sollte eine Grundlage geschaffen werden, dass jede/r BürgerIn Teil der globalen Informationsgesellschaft werden kann (Europäische Kommission, 2002), wie beispielsweise der Bereitstellung einer Breitband-Infrastruktur (Trauner, 2006).

Die Entwicklung eines sicheren und nahtlosen Zugangs zu eGovernment Dienstleistungen hängt weiters von der Einführung effektiver elektronischer Authentifizierungsmitteln ab. Eine Maßnahme zur Verbesserung der Qualität und des Zugangs zu öffentlichen Dienstleistungen bietet der Einsatz von eID. Fokus der eEurope 2005 Initiative war daher unter anderem sicheres eGovernment und Identitätsmanagement (Europäische Kommission, 2002).

3.1.3 Initiative „i2010 – Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung“

Die jüngste Initiative ist i2010 und bildet das Nachfolgeprogramm von eEurope. Die Initiative i2010 ist eine umfassende Strategie zur Modernisierung und Verbesserung der Gemeinschaftsinstrumente um die digitale Wirtschaft in Europa voranzutreiben (Commission of the European Communities, 2006).

Es soll eine Informationsgesellschaft gefördert werden, welche alle Menschen mit einbezieht. Dies beinhaltet beispielsweise die Schaffung eines zentralen

¹⁵ Projektdetails unter http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=5226877 (Zugriff 01.10.2011)

Informationsraums, welcher allen BürgerInnen zahlreiche Vorteile bietet, wie sichere innovative Dienstleistungen, Transparenz, Verlässlichkeit, sichere und kompatible Authentifizierung um die Effizienz und Effektivität für alle Teilnehmer in Europa zu steigern (Commission of the European Communities, 2006).

Eines der Hauptziele befasst sich mit der Entwicklung von elektronischen Identitäten als Zugangsvoraussetzung für elektronische Dienstleistungen (Europäische Kommission, 2006). Traditionelle Identitätskarten sollen um die Funktion der elektronischen Identität erweitert werden. Dadurch kann eine eindeutige Identifikation der BürgerInnen gewährleistet und der Zugang zu öffentlichen Diensten vereinfacht werden (Sánchez, Pérez, Gómez, & Carracedo, 2010). Dies soll BürgerInnen zur Nutzung dieser Dienste motivieren.

3.1.4 Ministererklärung zum eGovernment bis 2015

Die EU-Initiative "i2010 - Eine europäische Informationsgesellschaft für Wachstum und Beschäftigung" und der im April 2006 beschlossene Aktionsplan eGovernment geben derzeit den Mitgliedsstaaten den Rahmen zum weiteren Ausbau der elektronischen Behördendienste in Europa vor. Auf der eGovernment Ministerkonferenz 2009 in Malmö wurde eine Ministererklärung zum eGovernment bis 2015 verabschiedet. Diese bildet die Grundlage eines neuen EU-Aktionsplans eGovernment, der derzeit erarbeitet wird (Bundesministerium für Inneres, 2010).

3.1.5 Initiative „Europe 2020 – Eine Strategie für intelligentes, nachhaltiges und integratives Wachstum“

Ziel der Initiative Europe 2020 ist es, die EU zu einer intelligenten, nachhaltigen und integrativen Wirtschaft mit hohem Beschäftigungs- und Produktivitätsniveau sowie ausgeprägten sozialen Zusammenhalt zu wandeln. Um dies zu erreichen, wurden Maßnahmen vorgegeben und Leitinitiativen vorgeschlagen, darunter eine „Digitale Agenda für Europa“. Diese Initiative soll den Ausbau schnellen Internets und damit schneller eServices beschleunigen. Die Aufgabe ist es, einen Binnenmarkt für Online-Informationen und Dienstleistungen mit hohem Vertrauensgrad und ausgewogenem Rechtsrahmen zu schaffen (Europäische Kommission, 2010).

3.1.6 Gegenseitige Anerkennung von nationalen eID-Lösungen

„Für den mobilen EU-Bürger ist die heutige elektronische Identifikation noch nicht gut genug“, sagte Viviane Reding die für die Informationsgesellschaft und Medien zuständige EU-Kommissarin. „Indem das neue EU-Projekt Vorteile aus der Entwicklung der nationalen eID-Systeme nutzt und die gegenseitige Anerkennung elektronischer Identitätsnachweise vorantreibt, bringt es uns einen Schritt weiter auf dem Weg zur

wirklichen Freizügigkeit zwischen den EU-Ländern, die sich die Europäer zu Recht von einem grenzenlosen europäischen Binnenmarkt erwarten.“ (Europäische Union, 2008)

Verschiedene Länder entwickelten bereits eID Lösungen und standen nach den Initiativen der EU vor der Herausforderung, einen Pan-Europäischen Einsatz dieser Lösungen zu ermöglichen, da Interoperabilität von eID-Lösungen ein wesentliches Element für den Erfolg dieser darstellt (Walloschke, 2008).

Im Juni 2008 startete die Europäische Kommission ein Pilotprojekt mit dem Namen STORK¹⁶ (Secure Identity across borders linked) mit dem Ziel, eine grenzüberschreitende Erkennung von nationalen elektronischen Identitätssystemen von dreizehn Mitgliedsstaaten zu gewährleisten und damit eine Bereitstellung von grenzüberschreitenden eServices zu ermöglichen (Europäische Kommission, 2009). STORK ermöglicht es Unternehmen, BürgerInnen und Staatsbediensteten ihre nationale elektronische Identität in allen Mitgliedsstaaten der EU zu nutzen.

Das Pilotprojekt testete die meist genutzten europäischen eServices und legte den Focus auf (Europäische Kommission, 2009):

- Eine allgemeine Service-Architektur, welche BürgerInnen erlaubt, auf eGovernment Portale grenzüberschreitend mittels nationaler eID zuzugreifen
- Eine Plattform für sichere online Kommunikation
- Eine Dienstleistung welche die Mobilität von Studenten innerhalb Europas erhöht
- den Einsatz von eID für grenzüberschreitende Zustellung für BürgerInnen und Unternehmen
- das Testen des elektronischen Prozesses für die Änderung der Wohnadresse von EU-BürgerInnen, welche in ein anderes Mitgliedsland umziehen

Das Projektkonsortium bestand aus 29 teilnehmenden Staaten, darunter dreizehn Mitgliedsstaaten der EU – Österreich, Belgien, Estland, Frankreich, Deutschland, Italien, Luxemburg, Niederlande, Portugal, Slowenien, Spanien, Schweden, Großbritannien und Island (Europäische Kommission, 2009).

3.1.7 Projekte und Initiativen von kleinerem Rahmen

Neben den großen Initiativen der Europäischen Union wurden unterschiedliche kleinere Projekte und Initiativen gestartet, um die Entwicklung oder den Einsatz von elektronischen Dienstleistungen und elektronischen Identitäten zu fördern.

¹⁶ Siehe <http://www.eID-stork.eu> (Zugriff am 01.10.2011)

- CEN¹⁷

CEN, das Europäische Komitee für Standardisierung, machte sich zum Ziel, eine Open Smart Card Infrastruktur in Europa zu fördern. CEN versucht: eID-funktionale Architekturen, sowie einheitliche eID Karten für verschiedene Applikationen wie unterschiedliche Arbeitsgruppen europäischer BürgerInnen einzusetzen, als auch Workshops über eAuthentifikation für Smart Cards und eGovernment Dienste abzuhalten (European Committee for Standardization, 2009).
- IDABC¹⁸

Das Programm IDABC (Interoperable Delivery of European eGovernment Services to Public Administrations, Business and Citizens) wird durch das Direktorat für Informatik der Europäischen Kommission gelenkt. Es wurde entwickelt um die Zusammenarbeit und folglich die Effizienz zwischen Europäischen öffentlichen Verwaltungseinrichtungen zu verbessern und Unternehmen und BürgerInnen in Europa öffentliche Dienstleistungen grenzüberschreitend anzubieten. Um Europa in einen attraktiven Platz zum Arbeiten, Investieren und Leben zu machen, entwickelte IDABC Lösungen, gib Empfehlungen und bietet Dienstleistungen an um nationale und grenzüberschreitende Administration sowie Kommunikation durch den Einsatz der neuesten Technologien zu ermöglichen. IDABC wirkt bei der i2010 Initiative mit (Europäische Kommission, 2011).
- eTEN¹⁹

eTEN ist ein Programm der Europäischen Gemeinschaften um Applikationen und elektronische Dienstleistungen in der Europäischen Union anzubieten und soll den Einsatz und die Verwendung von innovativen und transeuropäischen eServices stimulieren. Prioritäre Bereiche umfassen eGovernment, eHealth, eInclusion, eLearning, Sicherheit und Vertrauen und SME (European Commission, 2011).
- EUCLID²⁰

EUCLID (European Initiative for a Citizen Digital ID Solution) ist eine europäische Initiative für BürgerInnen zur Unterstützung digitaler ID-Lösungen (A-SIT, 2004). Ziel der Initiative ist es, Einigkeit über die Implementierung von digitalen ID-

¹⁷ CEN Website verfügbar unter <http://www.cen.eu> (Zugriff am 01.10.2011)

¹⁸ IDABC Programm unter <http://ec.europa.eu/idabc/> (Zugriff am 01.10.2011)

¹⁹ eTEN Programm unter http://ec.europa.eu/information_society/activities/eten/index_en.htm (Zugriff am 01.10.2011)

²⁰ Details zu EUCLID unter http://cordis.europa.eu/fetch?CALLER=PROJ_ICT_TEMP&ACTION=D&CAT=PROJ&RCN=61482 (Zugriff am 01.10.2011)

Dokumenten in Europa zu fördern. EUCLID unterstützt damit die Prioritäten, welche im eEurope Smart Card Charter Action Plan festgelegt wurden und trägt dazu bei, die Entwicklung von eGovernment und eCommerce Applikationen zu vereinfachen und zu beschleunigen (Europäische Kommission, 2007).

- PRIME²¹
PRIME (Privacy and Identity Management for Europe) ist ein europäisches Projekt und untersucht Identity Management Projekte in Hinblick auf Sicherheitsaspekte (PRIME, 2011).
- eEPOCH²²
eEPOCH ist ein Programm der Europäischen Kommission und untersucht die Interoperabilität von Smart Cards und eID-Lösungen (Europäische Kommission, 2004).
- FASME²³
Das Projekt FASME (Facilitating Agent in Multicultural Exchange) der Europäischen Kommission befasste sich mit der Entwicklung eines Chipkarten-Prototyps, welcher Administrationsprozesse innerhalb der EU erleichtern soll (Europäische Kommission, 2007).
- GUIDE²⁴
Das Projekt GUIDE (Government User Identity for Europe) hatte zum Ziel, sichere und interoperable Architektur für digitale Identitäten innerhalb der EU und der Schweiz zu entwickeln (Europäische Kommission, 2007).

3.2 Rahmenbedingungen

Zur Realisierung erfolgreicher eGovernment Dienste ist es wichtig, eine gesamtheitliche Betrachtung von eGovernment Diensten zu erlangen. Die Basis von eGovernment Diensten bildet eine Back-Office-Infrastruktur, welche das Verwaltungsnetzwerk, Dokumenten- und Workflow-Managementsystem und Datenbanksystem umfasst.

²¹ Details zu PRIME unter <https://www.prime-project.eu/> (Zugriff am 01.10.2011)

²² Details zu eEPOCH unter <http://www.eepoch.net/> (Zugriff am 01.10.2011)

²³ Details zu FAME unter http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&CAT=PROJ&R CN=58337 (Zugriff am 01.10.2011)

²⁴ Details zu GUIDE unter http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RC N=6526790 (Zugriff am 01.10.2011)

Auf diesem Back-Office baut das Front-Office auf, welches die externe Perspektive von eGovernment widerspiegelt. Und dies Schnittstelle zu BürgerInnen und Unternehmen darstellt. Die Basis für eine vertrauenswürdige Realisierung von eGovernment Dienstleistungen bildet eine effiziente Sicherheitsinfrastruktur. Damit eng verbunden ist die Schaffung von Rahmenbedingungen, welche die Säulen des eGovernments bilden. Dridi und Pernul sprechen hier von dem eGovernment-Haus, welches alle Komponenten erfolgreicher eGovernment Dienste vereint (Dridi & Pernul, 2002). Dieses Konstrukt wird in Abbildung 4: eGovernment Haus dargestellt.

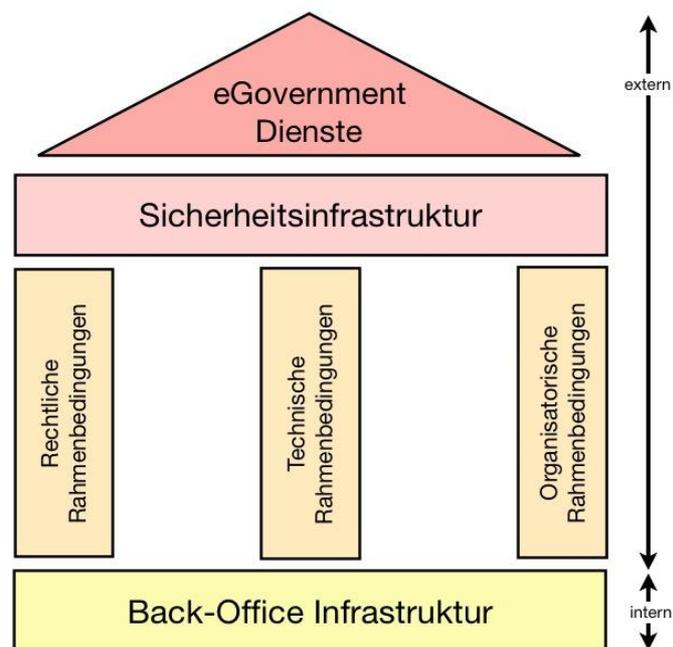


Abbildung 4: eGovernment Haus (Dridi & Pernul, 2002)

Die Rahmenbedingungen sowie die Sicherheitsinfrastruktur werden in den folgenden Kapiteln beschrieben. Hierbei wird insbesondere auf den Einsatz von eID eingegangen, da dieser einen kritischen Faktor für eine sichere Anwendung von elektronischen Diensten darstellt.

3.2.1 Sicherheit

Teil der eGovernment Lösung muss die Schaffung einer effizienten Sicherheitsinfrastruktur sein, welche die Basis für eine vertrauenswürdige Realisierung von eGovernment Dienstleistungen bildet (Dridi & Pernul, 2002).

In einer Umfrage der internationalen Marktforschungsgruppe Taylor Nelson Sofres plc (TNS)²⁵ halten 81 Prozent der deutschen BürgerInnen das Internet zu unsicher, um online behördliche Dienstleistungen zu verwenden (TNS Emnid, 2003), weltweit sind es 58 Prozent der BürgerInnen (TNS Global, 2003).

Eine Studie von KPMG²⁶ bestätigt die Notwendigkeit des Einsatzes einer Sicherheitsinfrastruktur. Als einer der Haupt-Hinderungsgründe für die Nutzung von eGovernment Applikationen sehen 67 Prozent der Befragten Sicherheitsfragen (KPMG Consulting AG, 2000).

Da der Erfolg von eGovernment vom Vertrauen und der Akzeptanz der BürgerInnen abhängt ist es unabdingbar Datenschutz und Datensicherheit zu gewährleisten (Daum & Eichhorn, 2005).

3.2.1.1 Datenschutz

Grundgedanke des Datenschutzes ist es, Persönlichkeitsrechte und personenbezogene Informationen vor Verletzung und Missbrauch zu schützen²⁷. Der/Die BürgerIn soll davor geschützt werden, dass die große Menge an personenbezogenen Daten, welche durch eGovernment Anwendungen elektronisch gespeichert, bearbeitet oder übertragen werden, missbräuchlich verwendet werden (Tino, 2004). Vor allem die breite Streuung von Informationen innerhalb von eGovernment sowie neue Methoden der Informationsverarbeitungen bieten ein Risikopotential für Datenschutzverstöße (Haldenwang, 2002).

3.2.1.2 Datensicherheit

Bei der Datensicherheit geht es im Kontext von eGovernment um den Schutz der Daten und Systeme vor unerlaubtem Zugriff und missbräuchlicher Verwendung. Speziell im Bereich der öffentlichen Verwaltung müssen daher hohe Sicherheitsstandards eingeführt werden um der Sensibilität von persönlichen Daten gerecht zu werden (Schedler & Proeller, New Public Management, 2006).

²⁵ Die Meinungsforschung von TNS Emnid führte in Deutschland die Studie "Government-Online- 2003" durch. Insgesamt wurden von den Sozial- und Meinungsforschern der internationalen Marktforschungsgruppe TNS 31.823 telefonische und/oder Face-to-Face Interviews in 31 Ländern im Zeitraum von Juli bis Oktober 2003 durchgeführt.

²⁶ KPMG dokumentiert seit einigen Jahren die Internetnutzung der deutschen Wirtschaft und beleuchtet die Entwicklung von eGovernment in der öffentlichen Verwaltung. Die Ergebnisse der bundesweiten Umfrage von Behörden der Bundesländer und Kommunalverwaltung werden in der Studie "Electronic Commerce: Status Quo und Perspektiven" zusammengefasst und einmal jährlich publiziert.

²⁷ Siehe auch Kapitel 3.2.2 Rechtlicher Rahmen, Seite 36

3.2.1.3 Sicherheitsinfrastruktur

Datenschutz und Datensicherheit kann durch eine adäquate rechtliche Gesetzgebung sowie Schaffung einer sicherheitstechnischen Infrastruktur gewährleistet werden.

Rechtliche Vorgaben seitens der Europäischen Union, welche Richtlinien für eine Umsetzung von eID und eGovernment Lösungen vorgeben, werden im Kapitel 3.2.2 Rechtlicher Rahmen, Seite 36, detailliert angeführt.

Neben rechtlichen Rahmenbedingungen muss eine Sicherheitsinfrastruktur geschaffen werden, welche Sicherheitsdienste wie Identifikation, Authentifikation, Autorisierung oder Verschlüsselung²⁸ bereitstellt (Dridi & Pernul, 2002).

Durch Einbindung dieser Sicherheitsdienste kann eine neben der eindeutigen Identifikation der beteiligten Parteien auch die Korrektheit der gesandten und empfangenen Daten garantiert werden (Dridi & Pernul, 2002).

Einige dieser Dienste können durch Einbindung der digitalen Signatur und der damit einhergehenden Bildung einer „Public-Key-Infrastructure“ realisiert werden.²⁹

3.2.2 Rechtlicher Rahmen

Um einen rechtlichen Rahmen zu bilden und die Einführung und den Einsatz von eGovernment, insbesondere von eID-Lösungen, zu stützen, dienen verschiedenste Gesetze und Normen. Mit der zunehmenden Wichtigkeit von eGovernment und eCommerce, wo Transaktionen elektronisch durchgeführt werden, ist der Schutz und der Nachweis der Identität besonders wichtig. Vor allem bei der Umsetzung einer elektronischen Verwaltung sowie dem Einsatz von elektronischen Diensten haben Sicherheit und Datenschutz höchste Priorität. Oft wird der Einsatz von elektronischen Identitäten hier als Schlüsselfaktor gesehen um in der Kommunikation und Transaktion zwischen BürgerInnen und Behörden sichere Identifikation und Authentisierung zu gewährleisten. Um sicher zu stellen, dass diesen auch legale Bedeutung zukommt, muss ein entsprechender rechtlicher Rahmen geschaffen werden (Schweitzer, 2004).

3.2.2.1 Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signatur

Da eine große Anzahl an Verwaltungsprozessen nach wie vor eine eigenhändige Unterschrift verlangen (Eifert, Schreiber, & Stapel-Schulz, 2000), ist es sehr wichtig, eine Regelung für den Einsatz digitaler Signaturen zu schaffen, welche festlegt, unter welchen Bedingungen elektronische Signaturen einer eigenhändigen Unterschrift rechtlich gleich

²⁸ Siehe Kapitel 3.3.2 Verschlüsselung, Seite 47

²⁹ Siehe Kapitel 3.4.5.2 Public Key Infrastruktur PKI, Seite 81

kommt³⁰ (Europäisches Parlament und Rat, 1999). Um diesem gerecht zu werden und eine globale Richtlinie für sicherheitstechnische Aspekte zu bieten, verabschiedete die Europäische Union einen gemeinschaftlichen Rahmen für den Einsatz elektronischer Signaturen. Die EU-Richtlinie legt fest, wann elektronische Signaturen einer eigenhändigen Unterschrift rechtlich gleich kommen, in Gerichtsverfahren als Beweismittel zugelassen werden und regelt die Rahmenbedingungen. Voraussetzungen sind, dass eine elektronische Signatur auf einem qualifizierten Zertifikat beruht und von einer sicheren Signaturerstellungseinheit erstellt wurde. Damit ist gewährleistet, dass elektronischen Verträgen mit Signatur dieselbe Wirkung zukommt wie Verträge, die mit der Hand unterschrieben wurden. Weiters befinden sich im Signaturgesetz eine Reihe an Anforderungen an Unternehmen, welche Zertifikate ausstellen, sowie Regelungen über die Anerkennung von Zertifikaten anderer Länder (Europäisches Parlament und Rat, 1999).

3.2.2.2 Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr

Die Richtlinie zur elektronischen Signatur beinhaltet ebenso einen Abschnitt den Datenschutz betreffend. Mitgliedsstaaten sind angehalten, die Anforderungen zum Schutz natürlicher Personen bei Verarbeitung personenbezogener Daten zu erfüllen. Hierzu wurde die Richtlinie 95/46/EG festgesetzt und hat zum Ziel, Rechte und Freiheiten von Personen zu schützen. Dafür wurden Grundprinzipien festgesetzt, die eine Rechtmäßigkeit der Verarbeitung dieser Daten schützt. Diese Grundprinzipien umfassen unter anderem (Europäisches Parlament und Rat, 1995):

- Personenbezogene Daten dürfen nur für eindeutig festgelegte und rechtmäßige Zwecke eingeholt und verarbeitet werden
- Die Verarbeitung der Daten darf nur erfolgen, wenn die betroffene Person ihre Zustimmung gegeben hat
- Es muss dafür gesorgt werden, dass die Daten gegen Zerstörung, Verlust, unberechtigte Änderung oder Weitergabe geschützt sind
- Die betroffene Person hat das Recht, Widerspruch gegen die Verarbeitung der Daten einzulegen
- Bei der Verletzung der Rechte hat die betroffene Person Recht auf Schadenersatz

Diese Richtlinie soll eine Ausarbeitung gemeinschaftlicher und nationaler Verhaltensregeln fördern (Europäisches Parlament und Rat, 1995).

³⁰ Zusammenhang zwischen elektronischen Signaturen und digitalen Identitäten siehe Kapitel 2.2.3 Anwendungsgebiete, Seite 25

3.2.2.3 Richtlinie über die Verarbeitung personenbezogener Daten und deren Schutz der Privatsphäre in der elektronischen Kommunikation

Im Jahr 2002 wurde vom Europäischen Parlament und dem Rat eine neue Richtlinie verabschiedet, welche Rahmenbedingungen für die elektronische Kommunikation festlegt. Diese enthält Bestimmungen zu sensiblen Aspekten, wie Aufbewahrung von Verbindungsdaten zum Zweck der Strafverfolgung, Verwendung von Cookies oder Speicherung von personenbezogenen Daten in beispielsweise öffentliche Verzeichnisse (Europäisches Parlament und Rat, 2002).

3.2.2.4 Nationale Gesetze und Normen

Die von der Europäischen Gemeinschaft vorgegebenen Richtlinien beschreiben die Mindestanforderungen für Bereiche betreffend Datenschutz und Datensicherheit, welche in allen Mitgliedsstaaten durch nationale Gesetze gesichert werden müssen.

Bei der Schaffung rechtlicher nationaler Rahmen durch die Regierung gilt es, diese Punkte zu behandeln und an die jeweilige Landessituation, wie den Entwicklungsgrad und die technischen Besonderheiten, anzupassen (Dridi & Pernul, 2002).

Besonders die Regelung für den Einsatz digitaler Signatur ist sehr wichtig, da eine große Anzahl an Verwaltungsprozessen nach wie vor eine eigenhändige Unterschrift verlangt und ein rechtlicher Rahmen für die Anerkennung von digitalen Signaturen geschaffen werden muss. Für den Fall von Missbrauch oder die Angabe falscher Daten bei der Verwendung von eGovernment-Diensten ist es nötig, rechtliche Sanktionen vorzusehen (Dridi & Pernul, 2002).

Bei einer Entwicklung einer nationalen Lösung für digitale Identitäten und digitale Signatur muss darauf geachtet werden, dass diese auch den globalen Anforderungen, wie Interoperabilität oder grenzüberschreitende Anwendung, gerecht werden kann. Eine Kommunikation über Rechtsräume hinweg sollte möglich sein (Schweitzer, 2004).³¹

3.2.2.5 Aktionsplan für elektronische Signaturen und die elektronische Identifizierung zur Förderung grenzübergreifender öffentlicher Dienste im Binnenmarkt

Viele Länder entwickelten bereits nationale elektronische Ausweise, welche für die Inanspruchnahme von elektronischen Dienstleistungen eingesetzt wird. Diese sind jedoch rein national ausgerichtet und orientieren sich nicht an internationalen Standards (Europäische Kommission, 2008).

Um die Mitgliedsstaaten bei der Einführung von gegenseitig anerkannten interoperablen Lösungen zu unterstützen, schlug die Europäische Kommission einen Aktionsplan vor, welcher drei zentrale Bereiche umfasst (Europäische Kommission, 2008):

³¹ Siehe Kapitel 3.1 Programme und Initiativen, insbesondere Kapitel 3.1.6 Gegenseitige Anerkennung von nationalen eID-Lösungen, Seite 33

- Kurzfristige Aktionen, um die Interoperabilität der Lösungen zu verbessern und Vorschriften in anderen Staaten zu klären
- Mittelfristige Aktionen für eine Interoperabilität von fortgeschrittenen elektronischen Signaturen, wie beispielsweise eine Prüfung der Gültigkeit einer Signatur aus einem anderen Land
- Mittelfristige Aktionen für eine Interoperabilität von elektronischer Identifikation

3.2.3 Technische Entwicklung

„True eGovernment“³² bietet ein durchgängiges eGovernment und geht über den Status „Service für den Kunden“ hinaus. Ziel von eGovernment ist es, medienbruchfreie Dienste anzubieten: Daten sollen elektronisch versandt, empfangen und weiterverarbeitet werden. Dies setzt Infrastruktur voraus, sowohl extern als auch verwaltungsintern (Prorok & Sallmann, 2001).

3.2.3.1 Auf der Nachfragerseite (BürgerIn)

eGovernment bedeutet elektronische Kommunikation und Transaktion zwischen BürgerInnen und Verwaltung. Der Kunde muss über Infrastruktur verfügen, wie beispielsweise einen Computer und Internetzugang (Prorok & Sallmann, 2001) um elektronische Informationen und Dienstleistungen nutzen zu können.

Neben diesen Mindestanforderungen an Hardware ist je nach Interaktionsgrad von eGovernment³³ zusätzliche Hardware und Software notwendig. Für den Einsatz von elektronischer Identität ist beispielsweise sowohl ein Träger der elektronischen Identität als auch ein Kartenlesegerät erforderlich³⁴.

3.2.3.2 Auf der Anbieterseite (Verwaltung)

Die Verwaltung als Anbieter von elektronischen Informationen und Dienstleistungen sowie Empfänger von Daten muss über geeignete Infrastruktur verfügen, um eine reibungslose Abwicklung zu gewährleisten.

Neben der Grundausstattung wie Computer und Internetzugang, gehören ebenso Fachbereichssoftware, Individualsoftware oder Zugriff auf Datenbanken zur notwendigen Infrastruktur.

Für das Angebot von eGovernment Dienstleistungen ist es notwendig, die einzelnen Komponenten der bestehenden Infrastruktur zu verknüpfen und eine durchgängige elektronische Geschäftsprozessstruktur zu erschaffen. Dafür können

³² „true eGovernment“ Begriff siehe Kapitel 2.1.2.3 Interaktionsniveau, Seite 10

³³ siehe Kapitel 2.1.2.3 Interaktionsniveau, Seite 10

³⁴ siehe Kapitel 3.3.5 Hardware, Seite 57

Dokumentenmanagementsysteme oder Workflow-Managementsysteme eingesetzt werden. Weiters bedarf es an Systemen, welche eine medienbruchfreie Bearbeitung der elektronischen Daten ermöglichen (Prorok & Sallmann, 2001). Dies bedeutet, dass alle Stufen der Transaktion elektronisch erfolgen können (Dridi & Pernul, 2002). Auf technischer Ebene muss hier für eine sichere Übertragung, Speicherung sowie Verwaltung von Informationen gesorgt werden (Schweitzer, 2004).

Besonders wichtig ist in diesem Zusammenhang der Schutz elektronischer Personendaten sowie die Wahrung der Sicherheit elektronischer Systeme³⁵. Es muss eine entsprechende Sicherheitsinfrastruktur geschaffen werden, wie beispielsweise eine flächendeckende Ausstattung mit Kartenlesegeräten um einen Einsatz von digitaler Signatur mittels Chipkarten zu ermöglichen (Dridi & Pernul, 2002).

Bei dem Einsatz von Informations- und Kommunikationstechnologien ist es nicht zwingend, als Vorreiter des Einsatzes von neuen Technologien aufzutreten, sondern ratsam, auf etablierte und ausgereifte Lösungen zurückzugreifen (Schmidt, 2003).

Es muss jedoch darauf geachtet werden, keine Insellösungen zu schaffen. Vielmehr sollte eine Architektur entworfen werden, welche eine modulartige Erweiterbarkeit und Interoperabilität zwischen unterschiedlichen Anwendungen ermöglicht (Dridi & Pernul, 2002). Daten und Informationen müssen ohne Schnittstellenprobleme oder –Verluste zwischen und innerhalb von Behörden transferiert werden können.

Wichtig hierbei ist es, sich nicht auf Technologien eines bestimmten Anbieters zu stützen, sondern eine Standardisierung zu fördern (Schweitzer, 2004). Offene Schnittstellen und gemeinsame Datenformate und Protokolle dienen hier zum Austausch über nationale und administrative Grenzen hinweg und gewährleisten Interoperabilität (Haldenwang, 2002).

Für eine Akzeptanz der BürgerInnen ist eine Erreichbarkeit der Systeme zentral. Daher ist dafür zu sorgen, dass Informationen und Dienste für die BürgerInnen verfügbar sind (Gisler, Einführung in die Begriffswelt des E-Governments, 2001). Um dies zu ermöglichen, muss eine geeignete Netzwerkinfrastruktur geschaffen werden.

³⁵ siehe auch Kapitel 3.2.1 Sicherheit, Seite 37

3.2.4 Organisatorische Umsetzung

3.2.4.1 Umstrukturierung

Verwaltungsabläufe im öffentlichen Dienst sind oft langsam aufgrund von lang gewachsenen Strukturen und engen Zuständigkeitsbereichen. Dies führt beispielsweise dazu, dass bei wenig komplexen Abläufen oft mehrere Stellen involviert sind.

eGovernment soll hier zu Verbesserungen führen. Es reicht jedoch nur selten aus, bestehende Verfahren einfach in elektronische Medien umzuwandeln. Vielmehr sind grundlegende Umstrukturierungen dieser traditionellen Verfahrensabläufe und Kommunikationswege erforderlich (Bundeskanzleramt, 2011).

Voraussetzung dafür sind vorab klar definierte Aufgaben und Prozesse innerhalb der Verwaltung (Dridi & Pernul, 2002). Bei der Umstellung von Verwaltungsprozessen und Dienstleistungen auf ein elektronisches Government ist es ratsam, diese zusammenzufassen und auf Internetfähigkeit zu überprüfen. Die Produkte und Dienstleistungen müssen dabei auf die Bedürfnisse von BürgerInnen und Unternehmen ausgerichtet werden. Die Prozessabläufe der Dienstleistungen müssen schließlich analysiert und optimiert werden, denn ein reines online zur Verfügung stellen von vorhandenen Dienstleistungen stellt kein eGovernment dar und bewirkt weder Vereinfachung noch Einsparung (Friedrichs, Hart, & Weizel, 10-Punkte-Plan für gutes E-Government, 2002).

3.2.4.2 Projekt- und Veränderungsmanagement

Zur Unterstützung und zur Förderung der Umstrukturierung muss eine neue interoperable, effiziente und nutzerorientierte Verwaltungsarchitektur geschaffen werden. Der Einsatz von Projekt- und Veränderungsmanagement ist hier unerlässlich.

Für den Erfolg von eGovernment ist es notwendig, Verantwortlichkeiten festzulegen (Dridi & Pernul, 2002) sowie zu definieren, wer in dem System welche Aufgabe erfüllen muss. Rechte und Pflichten der Teilnehmer müssen für sämtliche Prozessphasen und Aktionen klar festgelegt werden (Schweitzer, 2004).

Für die Projektsteuerung ist ein Management notwendig, welches die strategische Planung mit der operativen Planung und dem Personalmanagement verknüpft. Diese Instanz ist ebenso mit der Verantwortung beauftragt (Haldenwang, 2002).

Ein Veränderungsmanagement kann nur mittels moderner betriebswirtschaftlicher Methoden gelenkt werden. Durch Controlling wird es nachvollziehbar, inwieweit erhoffte Effizienzgewinne eingetreten sind und ob ein Strategiewechsel notwendig ist (Bertelsmann Stiftung, 2002).

3.2.4.3 Koordination und Kooperation

Grundlage jeder Verwaltungsreform ist eine umfassende Koordination (Dridi, Pernul, & Sabol, 2001), Kommunikation und kompetente Kooperation innerhalb der Regierung (Kubiec, 2008) zwischen Bund, Land, Stadt, Gemeinden, BürgerInnen und dem Privatsektor.

3.3 Grundlagen

Das folgende Kapitel beschäftigt sich mit Technologien, welche Grundlage für die Realisierung von digitalen Identitäten sind.

3.3.1 Hash-Verfahren

Mittels eines Hash-Verfahren wird ein so genannter Hash-Wert aus allen Eigenschaften des Dokuments ermittelt (Signature Perfect KG, 2008). Man spricht auch von einem „digitalen Fingerabdruck“ eines Dokuments (Schlauri, 2002).

Der Hash-Wert ist eine Zahl mit einer genau bestimmten Anzahl an Stellen, zum Beispiel 128Bit. Er wird mittels hochkomplexer Prüfsummenverfahren ermittelt. Die Funktion berechnet aus einer Nachricht eine bestimmte kryptografische Prüfsumme (Hash-Wert) mittels der Formel

$$h = H(M)$$

wobei M die Nachricht, H die Hashfunktion und h die Prüfsumme bezeichnet (Pohlmann & Hesse, 2007).

Um die Berechnung des Hash-Wertes zu veranschaulichen wird ein simples Beispiel gezeigt³⁶ (Limacher & Schickel, 2002).

Nachricht M:	0011 1011
Hash-Funktion H:	zuerst die ersten 4 Bits, danach die restlichen Bits
Hash von M H(M):	0 XOR 0 XOR 1 XOR 1 = 0 ³⁷
	1 XOR 0 XOR 1 XOR 1 = 1
Prüfsumme h:	h=H(M)=01

³⁶ Hierbei handelt es sich nur um ein vereinfachtes Beispiel zur Demonstration der Prüfsummenberechnung. Es entsteht große Kollisionsgefahr, da mehrere Nachrichten zu demselben Fingerprint führen (Nachricht 1100 1011 erzeugt ebenso die Prüfsumme 01) (Limacher & Schickel, 2002).

³⁷ XOR ist das Produkt einer Exklusiv-Oder-Verknüpfung (XOR) zwischen zwei Eingängen. Sind beide Eingänge gleich, ist das Ergebnis „0“, sind sie ungleich, so ist das Ergebnis der Verknüpfung „1“: 0 XOR 0 = 0 -> 0 XOR 1 = 1 -> 1 XOR 1 = 0 (DATACOM, 2011).

Die folgende Abbildung 5: Hash-Wert im hexadezimalen Zahlensystem zeigt einen Hash-Wert, dargestellt im hexadezimalen Zahlensystem. Das hexadezimale Zahlensystem beinhaltet Ziffernwerte zwischen 0 und 15, wobei die Werte von 10 bis 15 durch die Buchstaben A bis F ersetzt werden (Schlauri, 2002).



```
FD:3C:8B:87:76:28:39:A5:CD:AA:BB:2A:18:2E:50:2D
```

Abbildung 5: Hash-Wert im hexadezimalen Zahlensystem (Schlauri, 2002)

Die Ermittlung des Wertes ist einseitig und darf nicht umkehrbar sein. Aus Daten wird der Hash-Wert gewonnen, aus einem solchen können die Daten jedoch nicht ermittelt werden (Signature Perfect KG, 2008). Von der Prüfsumme h lässt sich somit nicht auf den Klartext der Nachricht M schließen. Es existiert somit keine Funktion $f()$, mit derer M aus h reproduziert werden kann (Pohlmann & Hesse, 2007).

Dieser Hash-Wert gleicht keinem anderen Hash-Wert eines anderen Dokuments und ist einzigartig und kollisionsresistent. Dies bedeutet, es darf nicht möglich sein, eine Prüfsumme $h=H(M)'$ zu erzeugen, welche der ursprünglichen Nachricht entspricht. Damit ist es nicht möglich, zu einer Nachricht M eine andere identische Nachricht M' zu finden und die Gleichung $H(M) = H(M)'$ darf nicht zutreffen (Pohlmann & Hesse, 2007).

Wird jedoch zu einem späteren Zeitpunkt das Hash-Verfahren erneuert und auf dieselbe Nachricht angewandt, so ergibt sich der exakt selbe Hash-Wert daraus. Ist der Wert nicht ident, so wurden das Dokumenten oder die Daten nach der Signierung verändert (Signature Perfect KG, 2008).

3.3.2 Verschlüsselung

Sicherheit und Vertrauen sind die Grundlage für den Einsatz digitaler Identitäten. Kryptografische³⁸ Verfahren haben hierbei einen großen Stellenwert, da ein Schlüssel als gutes Authentifikationsmerkmal dienen kann. Kryptografische Verfahren werden zur Verschlüsselung beim Datenaustausch, zur Authentifikation und zur digitalen Signierung eingesetzt. Als Schlüssel wird eine Information bezeichnet, welche aus einem kryptografischen Algorithmus resultiert. Es wird zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren unterschieden (Pfitzmann, Waidner, & Pfitzmann, 1990).

³⁸ Der Begriff Kryptographie bezeichnet die Disziplin in der Informatik, welche sich mit der Entwicklung sowie Bewertung von Verfahren zur Verschlüsselung geheimer Daten befasst (Weber, 1997).

3.3.2.1 Symmetrische Verschlüsselung (Secret Key)

Symmetrische Verschlüsselung bedeutet, dass Sender und Empfänger einer Nachricht den gleichen geheimen Schlüssel besitzen um Nachrichten zu verschlüsseln und entschlüsseln. Vor der Kommunikation müssen die Kommunikationspartner daher diesen Schlüssel austauschen. Der Austausch des geheimen Schlüssels kann auf unterschiedliche Art erfolgen. Eine Möglichkeit bietet der Austausch durch einen sicheren Kommunikationskanal, oder physisch mittels eines Speichergerätes. Eine andere Möglichkeit ist der Austausch des Schlüssels über eine Schlüsselverteilzentrale, auch genannt „Key Distribution Center“ (KDC) (Pfitzmann, Waidner, & Pfitzmann, 1990).

Das Prinzip der Symmetrischen Verschlüsselung wird in Abbildung 6: Symmetrische Verschlüsselung dargestellt.

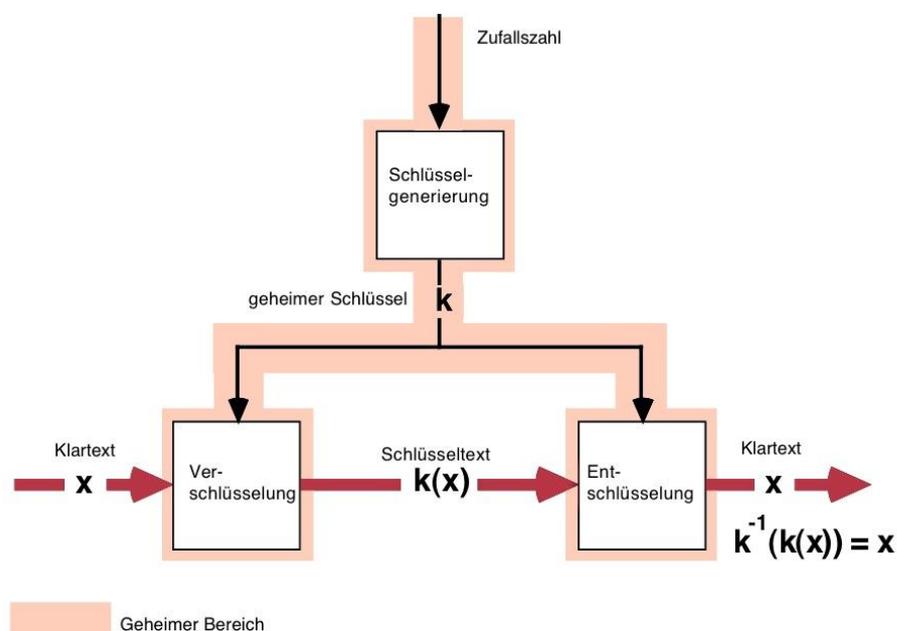


Abbildung 6: Symmetrische Verschlüsselung (Pfitzmann, Waidner, & Pfitzmann, 1990)

3.3.2.2 Asymmetrische Verschlüsselung (Public and Private Key)

Bei der asymmetrischen Verschlüsselung sind der Schlüssel zur Verschlüsselung von Daten und der Schlüssel zur Entschlüsselung nicht ident. Dieses Verfahren setzt drei verschiedene Algorithmen ein: Verschlüsselung, Entschlüsselung sowie zur Generierung zwei weiterer Schlüssel.

Jeder Kommunikationsteilnehmer verfügt über zwei Schlüssel zum Ver- als auch Entschlüsseln. Der Verschlüsselungsalgorithmus wird öffentlich bekannt gemacht (Public Key), der Entschlüsselungsalgorithmus wird geheim gehalten (Private Key). Der Public Key

kann beispielsweise in einem Schlüsselverzeichnis veröffentlicht werden. Die Veröffentlichung des Public Keys stellt kein Risiko dar, da von diesem Schlüssel nicht auf den Private Key geschlossen werden kann.

Möchte ein Teilnehmer einem Kommunikationspartner eine verschlüsselte Nachricht zukommen lassen, so verschlüsselt er diese mithilfe des Public Keys des Partners. Dieser verfügt über den passenden Private Key, welcher ihm ermöglicht, die Nachricht zu entschlüsseln. Bei dem asymmetrischen Verschlüsselungsverfahren ist somit eine Kommunikation ohne vorherigen Schlüsseltausch möglich (Pfitzmann, Waidner, & Pfitzmann, 1990).

Das asymmetrische Verschlüsselungsverfahren wird in Abbildung 7: Asymmetrische Verschlüsselung dargestellt.

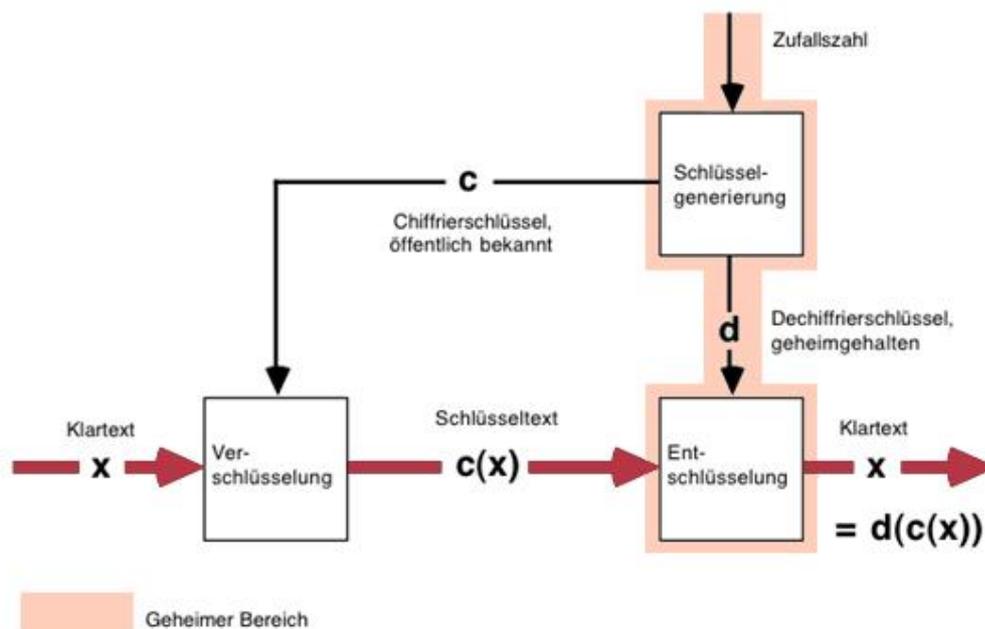


Abbildung 7: Asymmetrische Verschlüsselung (Pfitzmann, Waidner, & Pfitzmann, 1990)

Diese Verschlüsselung mittels Private Key wird nicht nur zur Verschlüsselung von Nachrichten eingesetzt, sondern ist auch ein wesentlicher Bestandteil für die elektronische Signatur von Botschaften (Pfitzmann, Waidner, & Pfitzmann, 1990).

3.3.3 Verschlüsselungsalgorithmen

In diesem Kapitel werden einige kryptografische Algorithmen vorgestellt, welche eine Verschlüsselung ermöglichen.

3.3.3.1 DES und AES

Das heute am weitesten verbreitete Verschlüsselungsverfahren ist der Data Encryption Standard (DES), welcher 1977 vom National Bureau of Standard als offizieller Standard veröffentlicht wurde. DES gehört zu den symmetrischen Verschlüsselungsverfahren und arbeitet mit 56 Bit-Schlüsseln, welche Blöcke von 64 Bit chiffriert (Pfitzmann, Waidner, & Pfitzmann, 1990). Da dies heutzutage den steigenden Attacken sicherheitsrechtlich nicht mehr gerecht wird, werden Triple DES Verfahren angewandt, welche eine Botschaft mit drei verschiedenen Schlüsseln hintereinander verschlüsselt.

Eine Erweiterung bietet auch der Advanced Encryption Standard (AES), welcher mit einem 128-Bit, 192-Bit oder 256-Bit langem Schlüssel arbeitet und Blöcke von 128 Bit chiffriert. Dadurch soll die nötige Sicherheit für eine verschlüsselte Kommunikation geboten werden (Schweitzer, 2004).

3.3.3.2 CAST³⁹

Der Carlisle Adamns und Stafford Tavares (CAST) Algorithmus gehört zu den symmetrischen Verschlüsselungsalgorithmen und chiffriert in Blöcken. CAST existiert in zwei Varianten (Network Sorcery inc., 2011):

- Cast-128: Verschlüsselung von 64bit Blöcken mit einer Schlüssellänge von 40 bis 128 Bits
- Cast-256: Verschlüsselung von 128 Bit Blöcken mit einer Schlüssellänge von 128, 160, 192 oder 256 Bits

CAST ist dem DES Algorithmus sehr ähnlich und gilt aufgrund der Schlüssellänge als besonders sicher.

3.3.3.3 IDEA

Der International Data Encryption Algorithmus (IDEA) ist ein symmetrischer Verschlüsselungsalgorithmus, welcher mit 64 Bit langen Blöcken arbeitet und einen 128 Bit langen Schlüssel verwendet. IDEA wird oft in PKIs mit PGP⁴⁰ eingesetzt und gilt aufgrund der Länge der Schlüssel als besonders sicher (Biham, Dunkelman, Keller, & Shamir, 2011).

³⁹ Spezifikation des CAST-128 Algorithmus unter <http://www.networksorcery.com/enp/rfc/rfc2144.txt>
Spezifikation des CAST-256 Algorithmus unter <http://www.networksorcery.com/enp/rfc/rfc2612.txt> (Zugriff am 01.10.2011)

⁴⁰ siehe Kapitel 3.4.5 Implementation, Seite 81

3.3.3.4 RSA

Den Standard für asymmetrische Verschlüsselung bildet der RSA Algorithmus, welcher neben der Verschlüsselung von Dokumenten auch zur Erzeugung digitaler Signatur verwendet wird. Wie in der Einführung der asymmetrischen Verschlüsselung beschrieben, basiert dieser Algorithmus auf der Erzeugung von zwei Schlüsselpaaren.

Die Generierung dieser Paare funktioniert durch die zufällige Auswahl von zwei Primzahlen p und q . Das Produkt n dieser Primzahlen wird Modulus genannt und beschrieben durch $n=p*q$.

Im nächsten Schritt wird eine beliebige Zahl e ausgewählt, welche $e < n$ und relativ prim zu $(p-1)*(q-1)$ ist. Nun wird eine Zahl d gewählt, sodass $e*d=1 \pmod{((p-1)*(q-1))}$ ist. Der Public Key setzt sich aus n und e zusammen, der Private Key ist d .

Die Verschlüsselung wird so ausgeführt, dass die Nachricht m in gleich lange Blöcke m_i geteilt wird, welche kleiner als n sind. Jeder Block wird dann durch $c_i = m_i^e \pmod{n}$ verschlüsselt. Der Empfänger der Nachricht entschlüsselt diese durch $m_i = c_i^d \pmod{n}$.

RSA arbeitet hier mit einem 512-Bit, 768-Bit, 1024-Bit oder 2048-Bit langem Schlüssel (Rivest, Shamir, & Adleman, 1987).

3.3.3.5 DSA

Der Digital Signature Algorithm (DSA) ist ein asymmetrisches Verschlüsselungsverfahren und Teil des Digital Signature Standards (DSS)⁴¹. DSA wird für die digitale Signatur verwendet, kann jedoch nicht für eine asymmetrische Verschlüsselung angewandt werden. Für die Bildung der digitalen Signatur und deren Verifikation wird ein Secure Hash Algorithm (SHA) erzeugt. Die Schlüssellänge liegt zwischen 512-Bit und 1024 Bit.

Der Algorithmus wird von verschiedenen Systemen unterstützt ist jedoch kritisiert, da es mit RSA bereits einen Standard für digitale Signatur gibt, welcher gleichzeitig auch für eine asymmetrische Verschlüsselung eingesetzt werden kann (National Institute of Standards and Technology, 1994).

Der Einsatz von SHA mit DSA wird in Abbildung 8: SHA mit DSA dargestellt.

⁴¹ Spezifikation des Digital Signature Standards (DSS): U.S. Department of Commerce, National Institute of Standards and Technology, Federal Information Processing Standards Publication 186-2, 27. Januar 2000, Digital Signature Standard (DSS), verfügbar unter <http://www.itl.nist.gov/fipspubs/fip186.htm> (Zugriff am 29.9.2011)

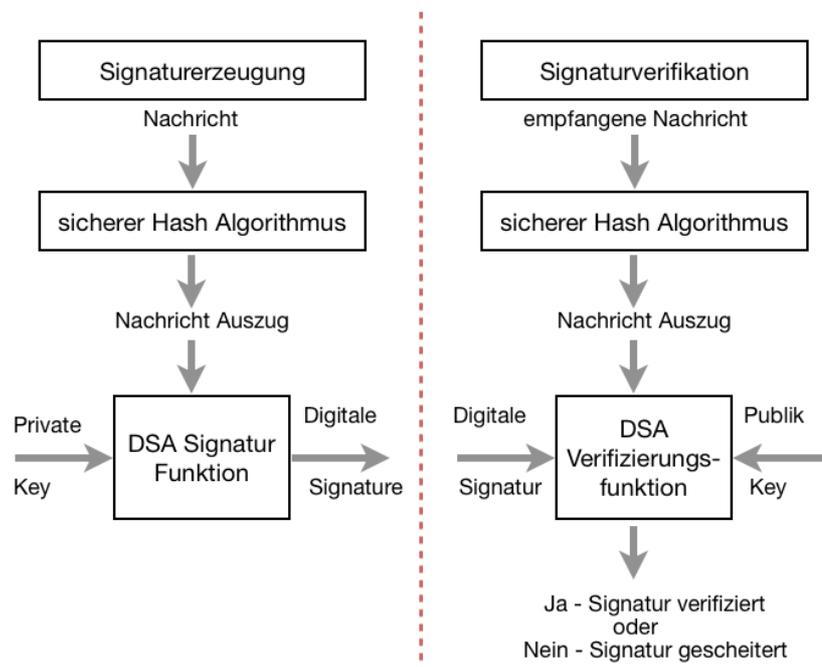


Abbildung 8: SHA mit DSA (National Institute of Standards and Technology, 1994)

3.3.4 Protokolle

Für eine sichere Übertragung von Daten werden Protokolle eingesetzt, sowohl für die Übertragung zwischen einer Smart Card und einem Kartenlesegerät, also auch zur sicheren Nutzung von Dienstleistungen über das Internet.

3.3.4.1 Datenübertragungsprotokolle für Kartenlesegeräte

Für die Datenübertragung zwischen Smart Cards und Kartenlesegeräten werden zwei standardisierte Übertragungsprotokolle eingesetzt (Rankl & Effing, 1998).

Protokolle für kontaktbehaftete Schnittstellen

Protokolle für kontaktbehaftete Schnittstellen werden durch ISO/IEC 7816-2 definiert:

- T=0, byteorientiertes Halbduplex Protokoll
Das T=0 Übertragungsprotokoll war der erste internationale Standard für Smart Card Protokolle und wurde hingehend auf eine minimalen Speicherverwendung (300 Byte) und maximale Einfachheit entwickelt. Es wird durch den Standard ISO/IEC 7816-3 definiert. Das Protokoll ist byteorientiert, somit ist die kleinste Einheit ein einzelnes Byte.
- T=1, blockorientiertes Halbduplex Protokoll
Das T=1 Protokoll ist ein asynchrones Halbduplex Protokoll, basierend auf dem Standard ISO/IEC 7816-3. Das Protokoll ist ein blockorientiertes Protokoll, somit

stellt die kleinste Dateneinheit im Transfer zwischen Smart Card und Lesegerät einen Block dar. Der Speicherbedarf dieses Protokolls liegt bei 1.100 Byte.

- T=2 und T=3, Vollduplex Protokoll
- T=4, asynchron, byteorientiertes Halbduplex Protokoll, Erweiterung von T=0
- T=5 bis T=13, reserviert für zukünftige Anwendungen
- T=14, für nationale Anwendungen, nicht ISO genormt
- T=15, reserviert für künftige Anwendungen

Protokolle für kontaktlose Schnittstellen

Das Protokoll T=CL (contact less) wird für die Übertragung von Daten zwischen kontaktlosen Lesegeräten und Smart Cards eingesetzt und wird durch die Standards ISO/IEC 10536, ISO/IEC 14443 und ISO/IEC 15693⁴² definiert (Bundesamt für Sicherheit in der Informationstechnik, 2009).

Ein weiteres Protokoll ist das PACE Protokoll. Es wird für eine sichere Kommunikation zwischen Chip Card und Terminal verwendet und erfüllt folgende Aufgaben während der Kommunikation (Bundesamt für Sicherheit in der Informationstechnik, 2009):

- Es autorisiert den Terminal zur Kommunikation mit der Smart Card
- Es authentisiert das Passwort und den Benutzer gegenüber der Smart Card
- Es vereinbart gemeinsame Schlüssel für die Kommunikation, baut einen sicheren Kommunikationskanal auf und gewährt Integrationsschutz

Das PACE Protokoll beruht auf einem gemeinsamen Passwort der Smart Card und des Terminals. Dieses wird bei einer Vereinbarung festgelegt und sorgt anschließend für eine sichere Verbindung. Der Benutzer gibt dieses Passwort am Terminal ein. Ist diese korrekt, vereinbaren Terminal und Smart Card gemeinsame Sitzungsschlüssel. Ist das Passwort falsch, kommt keine Kommunikation zwischen Terminal und Smart Card zustande. Bei erfolgreicher Autorisierung wird ein Sicherheitszustand hergestellt und damit verknüpfte Zugriffsrechte für den Terminal werden nutzbar⁴³. Die technischen Einzelheiten von PACE werden in der technischen Richtlinie TR-03110 spezifiziert.⁴⁴

⁴² Siehe dazu insbesondere ISO/IEC FCD 14443-4 - Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol (ISO, 2006), verfügbar unter http://wg8.de/wg8n1344_17n3269_Ballot_FCD14443-4.pdf (Zugriff am 01.10.2011)

⁴³ Für den genauen Ablauf der Authentisierung und Autorisierung siehe Kapitel 3.4.4 Authentisierung und Autorisierung, Seite 76

⁴⁴ Siehe BSI, TR-03110: Technical Guideline TR-03110: Advanced Security Mechanisms for Machine Readable Travel Documents – Extended Access Control (EAC), Password Authenticated Connection Establishment (PACE), and Restricted Identification (RI), Version 2.0, 2008

3.3.4.2 Authentifizierungsprotokolle für Webserver

eGovernment-Dienstleistungen werden über das Internet angeboten. Um den BürgerInnen eine sichere Verbindung zu garantieren, werden Protokolle für eine sichere Verbindung vom Client zum Webserver verwendet.

Um einen Server sicher zu identifizieren (Server Authentifizierung) und eine Verbindung zwischen diesen und einem Client zu verschlüsseln, werden Protokolle verwendet, welche auf Public Key Kryptografie basieren. Diese Protokolle sind Voraussetzung für einen Server, welcher sichere Dienste anbietet.

Soll der Client gegenüber einem Server identifiziert werden (Client Authentifizierung), werden das Zertifikat und der Signierschlüssel am Client eingerichtet. Beim Aufruf einer Website erscheint vorab ein Dialogfeld in welches der User das Zertifikat sowie das Passwort zur Freigabe des Schlüssels eingeben muss (Schlauri, 2002).

Es werden exemplarisch drei der wichtigsten Protokolle beschrieben, welche für den Einsatz mit digitalen Identitäten eingesetzt werden.

SSL/TSL

Das Secure Socket Layer Protokoll (SSL) ist heute Standard für eine sichere Kommunikation. Sämtliche Browser unterstützen dieses Protokoll. SSL besteht aus dem Record Protocol und dem Handshaking Protocol.

Das Handshaking Protocol verwendet asymmetrische Verschlüsselung und ermöglicht eine sichere Authentifikation und den Schlüsselaustausch. Zur Authentifikation werden optional auch Browser-Zertifikate verwendet.

Das Record Protocol ermöglicht danach eine sichere Kommunikation mittels symmetrischer Verschlüsselung. Die symmetrischen Verfahren werden bei Sessions zur vertraulichen Verschlüsselung verwendet, welche sicherstellt, dass alle Inhalte und Daten nur verschlüsselt transportiert werden, die Identität des Servers gewährleistet ist und alle Daten vollständig und unverändert den Empfänger erreichen (Schlauri, 2002).

Zu Austausch der Schlüssel wird ein RSA Algorithmus, für die Kommunikation ein DES, AES oder ein anderer Algorithmus eingesetzt.

TLS⁴⁵ wurde als Nachfolger von SSL entwickelt, die Unterschiede sind jedoch eher gering.

IPSec

IPSec bietet zwei Protokolle: Das Authentication Header Protocol (AH) dient der Authentisierung, bietet jedoch keine Vertraulichkeit und damit werden Daten unverschlüsselt übertragen. Das Encapsulating Security Payload (ESP) ermöglicht eine Verschlüsselung der Daten und bietet so Vertraulichkeit (Network Sorcery inc., 2011).

⁴⁵ Spezifikation des TLS nachzulesen unter <http://www.ietf.org/rfc/rfc2246.txt> (Zugriff am 01.10.2011)

WSS

Der Web Service Security (WSS)⁴⁶ Standard spezifiziert, wie die in SOAP-Nachrichten enthaltenen Sicherheitsinformationen, beispielsweise SAML-Zusicherungen, Kerberos-Tickets oder Public Key Zertifikate⁴⁷, sicher übertragen werden können. Dadurch wird eine Interoperabilität von Web-Services gefördert (OASIS Open, 2004).

WS-Security bietet Erweiterungen für SOAP an, sodass zusätzlich Verschlüsselungen und digitale Unterschriften verwendet werden können. SOAP wird von Web-Services zur sicheren Kommunikation untereinander eingesetzt und verwendet XML für die Kommunikation.

- XML Verschlüsselung

Diese Spezifikation legt fest, wie XML Dokumente Verschlüsselt und im XML Format dargestellt werden können. Es ist auch möglich, nur Teile eines Dokuments zu verschlüsseln. Die XML Spezifikation beinhaltet keine neuen Verschlüsselungsverfahren sondern legt nur die Art fest, wie Informationen über ein verwendetes Verfahren dargestellt werden (Imamura, Dillaway, & Simon, 2002).

- XML Signatur

Diese Spezifikation definiert, wie XML Dokumente digital unterschrieben und als XML dargestellt werden können. Es ist möglich, nur Teile eines Dokumentes zu unterschreiben (Hughes, Imamura, & Maruyama, 2002).

- SAML

Die Security Assertion Markup Language (SAML)⁴⁸ ist ein Standard für die Authentifikation und erlaubt einen Austausch von Authentifikationsinformationen zwischen verschiedenen Systemen. Weiters definiert SAML, wie die Informationen über Authentisierung, Autorisierung in XML dargestellt werden.

Vor allem Single-Sign-On Lösungen können mit diesem Standard realisiert werden. Der Benutzer authentifiziert sich beispielsweise mittels Benutzername und Passwort bei einem Dienst und die Informationen werden mittels SAML in einer SOAP Nachricht übertragen. SAML ist daher Grundlage für Protokolle von aktuellen Identitätsmanagement-Lösungen (Organization for the Advancement of Structured Information Standards, 2008).

⁴⁶ Spezifikation von WSS nachzulesen unter <http://www.oasis-open.org/committees/wss> (Zugriff am 01.10.2011)

⁴⁷ Kerberos und Public Key Zertifikate werden in Kapitel 3.4.5 Implementation, Seite 81, erläutert.

⁴⁸ Spezifikation des SAML nachzulesen unter <http://www.oasis-open.org/committees/security/> (Zugriff am 01.10.2011)

3.3.5 Hardware

Als Träger für digitale Identitäten dienen unterschiedliche Geräte, wie Smart Cards, Token, Mobiltelefone oder PDAs. Für starke Authentifikation existieren weiters SecureID-Karten oder Streichlisten⁴⁹. Weiters bedarf es zum Datenaustausch sicherer Kartenlesegeräte, welche ebenso in diesem Kapitel behandelt werden.

3.3.5.1 Smart Cards

Smart Cards⁵⁰ sind Plastikkarten in Größe einer Bankkarte⁵¹ welche Speicherplatz auf einem oder mehreren Mikrochips enthalten. Smart Cards verfügen teilweise über ein eigenes Betriebssystem, besitzen Speicherplatz im Kilobyte Bereich und können mehrere Applikationen speichern (U.S. General Services Administration Office of Governmentwide Policy, 2004). Die Struktur von Smart Cards wird in den ISO Standards 7810, 7816-1 und 7816-2 definiert.

Für die Speicherung von digitalen Identitäten werden Smart Cards als sichere Geräte betrachtet, da sie nur unter großem Aufwand reproduzierbar sind und aktive Mechanismen enthalten, die ein Auslesen des Inhaltes verhindern (U.S. General Services Administration Office of Governmentwide Policy, 2004). Daher eignen sich Smart Cards speziell für den Zugriff auf eGovernment Dienstleistungen.

Anhand ihrer Funktionalität können Chipkarten in zwei Gruppen unterteilt werden: Speicherkarten und Prozessorkarten. Speicherkarten enthalten einen Speicher zur Sicherung von Daten. Prozessorkarten besitzen einen Mikro Controller zur Ausführung von Anwendungsprogrammen, kryptografischer Operationen oder zur Verwaltung von Dateisystemen.

Der Begriff Smart Card bezieht sich hierbei sowohl auf Prozessorkarten als auch Speicherkarten (Langer & Roland, 2010).

⁴⁹ Streichlisten, auch TANs, sind Zeichenfolgen, welche als Einmalpasswörter dienen. Sie werden vor allem im Finanzdienstleistungssektor zur Authentisierung von Mitarbeitern und Kunden eingesetzt (Schweitzer, 2004). Diese senden Ihren Kunden eine Liste mit Zeichenfolgen zu, welche zum Beispiel beim eBanking zum Login oder weiteren Aktionen verwendet werden können. Wurde eine Zeichenfolge verwendet, so kann er diese streichen und muss beim nächsten Log-In eine neue Zeichenfolge angeben. (Hochschule Luzern, 2011)

⁵⁰ Da Smart Cards die häufigsten Träger von digitalen Identitäten darstellen, werden sie ausführlicher behandelt als andere Modelle.

⁵¹ Die genaue Größe beträgt 85,60 mm*53,98 mm*0,8 mm.

Speicherkarten

Speicherkarten können mit und ohne Sicherheitslogik ausgestattet sein.

Die unterschiedlichen Ausführungen von Speicherkarten werden in Abbildung 9: „Klassifizierung von Speicherkarten nach Funktionsumfang“ dargestellt.

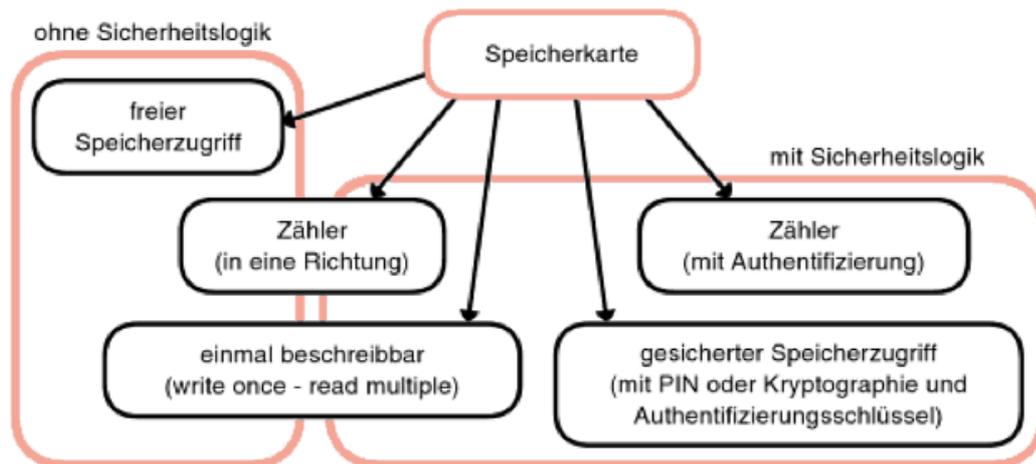


Abbildung 9: Klassifizierung von Speicherkarten nach Funktionsumfang(Langer & Roland, 2010)

Bei Speicherkarten ohne Sicherheitslogik ist der Datenspeicher uneingeschränkt schreibbar, lesbar und löschtbar. Bei Speicherkarten mit gesichertem Speicherzugriff bedarf es jedoch der Eingabe eines PINs oder Authentifizierungsschlüssels. Es gibt jedoch auch Mischformen, bei welchen der Speicher selbst oder eine Zugriffslogik bestimmte Operationen sperrt, beispielsweise Karten, welche nur einmal beschreibbar und danach nur mehr lesbar sind. Weiters gibt es Zählerkarten, welche einen Zählerwert zu Beginn haben welcher mit jeder Abbuchung gesenkt wird (Rankl & Effing, 1998).

Prozessorkarten

Prozessorkarten besitzen einen Mikro Controller (Micro Controller Unit MCU) welche alle Teile eines vollwertigen Computers enthalten. Diese MCU ist der zentrale Baustein der Karte. Der Micro Controller, welcher speziell für Sicherheitsanwendungen konzipiert ist, bezeichnet man als Security Controller (Bürge, 2002).

Neben dem zentralen Micro Controller verfügt die Prozessorkarte noch über weitere Hardwareblöcke, wie beispielsweise ein Coprozessor für die Ausführung kryptografischer Funktionen oder eine Memory Management Unit (MMU). Die MMU regelt den Zugriff der Programme, die im Mikro Controller verarbeitet werden, auf den Speicher (Langer & Roland, 2010).

Die Leistung dieser Mikrochips ermöglichen somit folgende Grundfunktionen (Bürge, 2002):

- Beweis der Identität gegenüber einem System (Authentifizierung)
- Digitale Signatur einer Nachricht (Public Key)
- Entschlüsselung von verschlüsselten Nachrichten (Private Key)

Für die Erzeugung von qualifizierten elektronischen Signaturen ist laut Signaturgesetz eine sichere Signaturerstellungseinheit erforderlich. Chipkarten eignen sich dafür besonders, da diese durch den kryptografischen Coprozessor die Signaturfunktionalität anbieten (Haneberg, 2006). Durch die eigene Rechenleistung können Smart Cards Schlüsselpaare generieren. Der Private Key befindet sich damit nie außerhalb der Smart Card.

Aufgrund der Rechenleistung der Smart Cards dauert die Generierung ungefähr eine Minute, schneller ist jedoch die generieren der Schlüssel extern, also nicht auf der Smart Card, sondern in einer kontrollierten, sicheren Umgebung.

Als Betriebssystem der Prozessoren wird überwiegend Java Card verwendet. Der Vorteil liegt darin, die Chipkarte in der verbreiteten Programmiersprache Java zu programmieren. Die Java Card Spezifikation ermöglicht es, Java-basierte Anwendungen (Applets) auf Smart Cards auszuführen. Weitere Betriebssysteme für Smart Cards sind Windows und Linux (Haneberg, 2006).

Kommunikationsschnittstelle

Chipkarten lassen sich auch anhand der Kommunikationsschnittstelle klassifizieren. Diese können kontaktbehaftet, kontaktlos oder eine Mischform daraus sein.

Kontaktbehaftete Schnittstellen tauschen Daten über physikalische Kontakte mittels Übertragungsprotokolle aus. Bei kontaktlosen Smart Cards werden die Daten über eine berührungsfreie Schnittstelle übertragen⁵².

Es gibt eine große Anzahl von Standards für kontaktlose Kommunikationsschnittstellen für Smart Cards, welche in Tabelle 2: Standards für kontaktlose Smartcards gelistet sind (Langer & Roland, 2010).

⁵² Siehe auch Kapitel 3.3.4 Protokolle, Seite 52

Tabelle 2: Standards für kontaktlose Smartcards (Langer & Roland, 2010)

Typ	Reichweite	Norm
Close Coupling	1cm	ISO/IEC 10536
Proximity Coupling	10cm	ISO/IEC 14443
FeliCa	10cm	JIS X 6319-4
Vicinity Coupling	1m	ISO/IEC 15693
EPCglobal UHF Class 1 Generation 2	10m	ISO/IEC 18000-6C

Die unterschiedlichen Systeme unterscheiden sich in ihrer Funktionalität, der Betriebsfrequenz und der Reichweite und werden für unterschiedliche Anwendungsgebiete eingesetzt. Bei den Close-Coupling Karten kann eine gute Energieversorgung durch geringen Abstand realisiert werden (Langer & Roland, 2010).

Kontaktlose Chipkarten werden begrifflich in Tags und Smart Cards im engeren Sinn aufgeteilt. Tags bezeichnen einfache Speicherkarten, welche als reine Speichermedien eingesetzt werden und nur über geringe Zugriffsschutzmaßnahmen verfügen. Smart Cards bezeichnen kontaktlose Chipkarten welche einen Micro Controller und aufwändige Sicherheitsfunktionen beinhalten (Langer & Roland, 2010).

Es gibt auch Karten, welche mehrere Chips unabhängig voneinander integrieren, diese werden Hybridkarten genannt. Weiters existieren so genannte Dual-Interface-Karten, welche sowohl über eine kontaktlose als auch kontaktbehafte Schnittstelle angesprochen werden können (Cryptas it-Security GmbH, 2011).

Speicherkapazität

Die Aufnahmekapazität von Datenspeichern wird in Byte angegeben. Die Speicherkapazität einer Chipkarte liegt zwischen 3 kByte und 68 kByte (Liu, 2002).

Applikationen bedürfen unterschiedlicher Daten, welche verschieden großen Speicherplatz einnehmen. So bedarf es für die Anwendung von eGovernment Dienstleistungen oder dem Einsatz für elektronisches Wählen der Speicherung des Authentifikationsschlüssels sowie des Zertifikates auf der Karte mit 2KB Speichergröße.

Smart Cards werden auch oft zur Speicherung von biometrischen Daten verwendet und integrieren beispielsweise Fingerabdrücke⁵³.

⁵³ Beispiel für eine Karte mit integriertem Fingerabdruckleser unter <http://www.biometricassociates.com/products-bai> (Zugriff am 01.10.2011)

3.3.5.2 Kartenlesegeräte

Kartenlesegeräte stellen die physikalische Verbindung zwischen der Smart Card und dem zentralen Hostrechner oder der Applikation dar (Bundesamt für Sicherheit in der Informationstechnik, 2011). Sie werden auch als Terminals bezeichnet, es existieren jedoch weitere Bezeichnungen wie Smart Card Reader, Smart Card Adapter, IFD (interface device), CCR (chip card reader) oder CAD (chip accepting device).⁵⁴

Die Grundfunktionalität ist bei allen Geräten gleich: Kartenlesegeräte versorgen die Chipkarte elektronisch, stellen eine datentechnische Verbindung her (Rankl & Effing, 1998) und ermöglichen somit eine Datenübertragung aller ein- und ausgelesenen Daten zwischen der Smart Card und dem Hostrechner. Der zentrale Hostrechner kann beispielsweise ein PC oder ein Gerät zur Zugangskontrolle sein (DATACOM, 2011).

Terminals können als bloße Kontaktierungseinheit verwendet oder technisch komplizierter aufgebaut werden und über einen eigenen Prozessor mit eigenem Speicher verfügen. Der Prozessor kann Teil eines Micro Controllers sein oder Bestandteil eines Einplatinencomputers⁵⁵. Die Terminals werden vorwiegend in der Sprache C, C++ oder Java programmiert (Rankl & Effing, 1998).

Kartenlesegeräte können verschiedene Ausprägungen je nach Nutzen oder Applikationen besitzen:

- Art des Terminals
Es gibt portable und stationäre Terminals. Stationäre Terminals beziehen ihre Energie beispielsweise aus dem Stromnetz, portable Terminals aus Batterien.
- Kartenschnittstelle
Eine weitere Unterscheidung lässt sich anhand der Schnittstelle treffen, diese kann kontaktbehaftet oder kontaktlos ausgeprägt sein⁵⁶.
- Hostschnittstelle
Kartenlesegeräte sind mit dem PC über USB-Schnittstelle oder einen PCMCIA-Slot oder eine andere seriellen Schnittstelle verbunden.

⁵⁴ Die Begriffe Reader oder Leser sind jedoch nicht so zu verstehen, dass Daten nur aus Karten gelesen werden können, ebenso ist ein Schreibvorhang möglich (Rankl & Effing, 1998).

⁵⁵ Einplatinencomputer oder Single-Board-Computer, bezeichnet ein Prozessorboard, das alle notwendigen Systemkomponenten enthält. Die komplette Funktionalität ist damit auf einer einzigen Trägerplatine vorhanden. Weitere Funktionen können durch Aufsteckmodule ergänzt werden (DATACOM, 2011).

⁵⁶ Diese Unterscheidung ist wichtig für den Einsatz von kontaktlosen und kontaktbehafteten Chipkarten, siehe Kapitel 3.3.5.1 Smart Card, Seite 57

- Die unterschiedlichen Eigenschaften können wie in Abbildung 10: Klassifizierung der Eigenschaften von Terminals dargestellt und klassifiziert werden (Rankl & Effing, 1998).

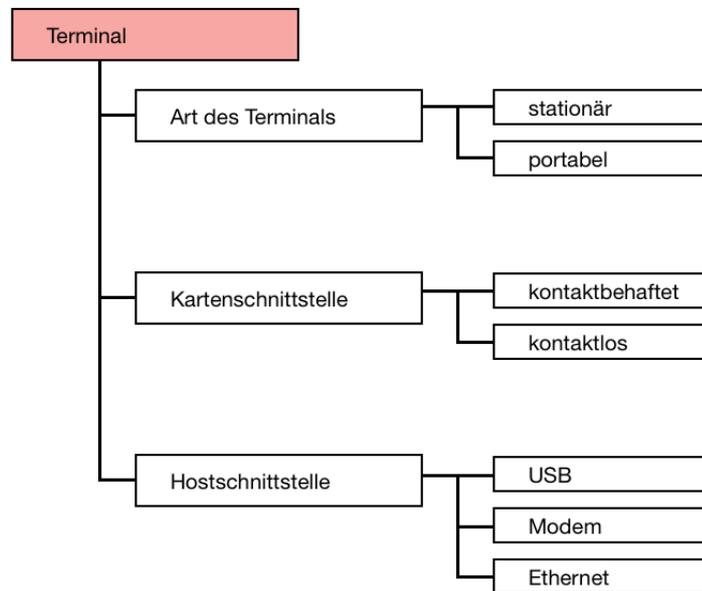


Abbildung 10: Klassifizierung der Eigenschaften von Terminals (Rankl & Effing, 1998)

Kartenlesegeräte haben unterschiedliche Funktionen. So versorgen sie die Chipkarten mit Energie, entweder durch einen physikalischen Kontakt auf dem Mikromodul oder per Antenne bei kontaktlosen Karten (U.S. General Services Administration Office of Governmentwide Policy, 2004). Weiters stellen Terminals die datentechnische Verbindung her (Rankl & Effing, 1998) und ermöglichen somit eine Datenübertragung aller ein- und ausgelesenen Daten zwischen der Smart Card und dem Hostrechner (DATACOM, 2011).

Die Datenübertragung erfolgt entweder über physikalischen Kontakt oder über eine Luftschnittstelle (Contactless Chip Card Interface CCI). Für die Übertragung der Daten werden entsprechende Übertragungsprotokolle eingesetzt, welche in Kapitel 3.3.4 Protokolle, Seite 48, behandelt werden.

Zur Ausübung dieser Funktionen verfügen Kartenlesegeräte oft über Display oder Tastatur, die Ausstattung kann jedoch sehr unterschiedlich sein: Terminals können von einfachen Chipkarteninterfaces ohne Display und Tastatur bis hin zu Kartenlesegeräten mit erweiterten Sicherheitsfunktionen reichen (Bundesamt für Sicherheit in der Informationstechnik, 2011).

Kartenlesegeräte können anhand ihrer unterschiedlichen Ausprägungsgrade wie folgt differenziert werden können:

- Einfache „transparente“ Kartenlesegeräte: Dieser besitzt weder Tastatur noch Bildschirm und liest nur die Karte. Eine Kompatibilität ist ohne Modifikation möglich es müssen lediglich Personal Computer/Smart-Card Standards erfüllt werden
- Kartenlesegeräte mit eingebauter Tastatur oder Bildschirm: Kartenlesegeräte mit sicherem Pin-Pad (Tastatur um eine sichere PIN-Eingabe vorzunehmen), Modifizierung notwendig um PIN-Codes zu erhalten und Nachrichten am Display anzuzeigen
- Kartenlesegeräte für einen PC-Karten-Slot: Kann in den Computer integriert werden
- Tastatur die einen Kartenlesegeräte beinhaltet: Ein gewöhnlicher Kartenlesegeräte der in das Gehäuse der Computertastatur eingebettet ist
- Kartenlesegeräte, der standardisiert in den Computer eingebaut ist

Kartenlesegeräte verfügen über unterschiedliche Sicherheitsmechanismen und Sicherheitsmodule und wurden von dem zentralen Kreditausschuss (ZKA)⁵⁷ in unterschiedliche Sicherheitsklassen geteilt, welche in Tabelle 3: Klassifikation von Kartenlesegeräten erläutert werden (Rankl & Effing, 1998).

Tabelle 3: Klassifikation von Kartenlesegeräten (DATACOM, 2011)

Klassen	Spezifikation
Klasse 1	Bietet keine Sicherheit, da es die Karte nur liest oder beschreibt
Klasse 2	Darf den PIN nicht auf den Computer transferieren, die Nummer muss im Kartenlesegerät gespeichert bleiben
Klasse 3	Ein Display ist notwendig, das die ganze Transaktion zeigt, der User kann den Prozess kontrollieren
Klasse 4	Höchstes Sicherheitslevel, hat eigene Identität, ist ausgestattet mit Signaturschlüssel, kann eigene digitale Signatur erzeugen

Das deutsche ZKA teilt Terminals in vier Klassen. Klasse 1 besteht aus einer Kontaktiereinheit ohne Funktionselemente und eine Schnittstelle, beispielsweise USB, zu anderen Systemen. Klasse 2 verfügt zusätzlich über ein Display. Die nächste Klasse 3 schließt alle Funktionalitäten der vorigen Klassen mit ein und verfügt zusätzlich über eine Tastatur. Klasse 4 enthält alle Funktionselemente von Klasse 3 und verfügt zusätzlich über ein Sicherheitsmodul (HSM) mit Verschlüsselungsfunktionalität (Rankl & Effing, 1998).

⁵⁷ siehe <http://www.zka.de/> (Zugriff am 01.10.2011)

Kartenlesegeräte-Hersteller können ihre Produkte zertifizieren lassen. Dazu wird die Konformität der Geräte zur technischen Richtlinie überprüft und mit einem Zertifikat bestätigt. Diese Zertifikate werden veröffentlicht und die zertifizierten Kartenlesegeräte erhalten ein Prüfsiegel als Kennzeichen der erfolgreichen Zertifizierung (Bundesamt für Sicherheit in der Informationstechnik, 2011).

3.3.5.3 RFID

Der Begriff RFID steht für Radio-Frequenz Identification. Durch RFID ist es möglich, eine kontaktlose Übertragung von Daten zwischen Datenträger und Lesegerät über Radiowellen berührungslos zu realisieren (Finkenzeller, 2008).

Eine RFID Einheit, meist als RFID-Tag bezeichnet, erfüllt den Zweck der eindeutigen Kennzeichnung und Nichtverfolgung eines Objektes.

Radio-Frequency Identification-Technology (RFID) Objekte, auch RFID-Tags, bestehen aus zumindest zwei Teilen. Die Daten werden auf einem elektronischen Datenträger, dem Transponder gespeichert (Finkenzeller, 2008). Dieser Transponder ist ein Mikrochip und ermöglicht neben der Speicherung und Bearbeitung von Informationen, auch die Modulierung und Demodulierung einer Radiofrequenz.

Der Transponder hat weiters eine Antenne zum Empfang und zur Übertragung des Signals. Diese Komponenten werden oft in ein Trägerobjekt integriert, wie beispielsweise einer Plastikarte.

Der Transponder enthält beispielsweise einen Nummerncode, welcher auf weitere Informationen in einer Datenbank verweist. Damit erhält jedes Objekt, welches mit einem Transponder versehen ist, eine eindeutige Identität (Informationsforum RFID, 2009).

Es werden folgende Typen von RFID-Tags unterschieden (Informationsforum RFID, 2009):

- Aktive RFIDs, die über eine eigene Batterie und damit über eine eigene Energieversorgung verfügen, können Signale autonom übertragen. Weiters ermöglicht eine integrierte Batterie die Ausübung eigener Rechen- und Speicherprozesse.
- Passive RFIDs, die über keine eigene Batterie verfügen, benötigen externe Energiequellen um Signale zu übertragen. Diese Transponder kommen ohne eigene Stromversorgung aus, da sie die Energie aus den elektromagnetischen Feldern des Lesegerätes beziehen. Dadurch verringert sich allerdings ihre Reichweite.

Um Identitätsdaten aus der RFID Einheit zu lesen ist ein Abfragegerät oder Lesegerät notwendig, welches sowohl Lesefunktion als auch Schreibfunktion erfüllt. Die Energieversorgung des Datenträgers und der Datenaustausch zwischen Lesegerät und

Datenträger erfolgt unter Verwendung elektromagnetischer Felder (Finkenzeller, 2008) welche von der Sende-Empfangs-Einheit erzeugt werden. Dieses elektromagnetische Feld wird von der Antenne des RFID-Transponders empfangen, woraufhin der Transponder seinen Nummerncode an das Lesegerät sendet. Je nach Sendestärke und Frequenzbereich des Lesegerätes und der verwendeten Antenne kann die Reichweite von wenigen Zentimetern bis hin zu zehn Metern variieren. Das Lesegerät leitet die Zahlenkombination an die Datenbank weiter und das System verknüpft den Code mit Informationen aus der Datenbank (Informationsforum RFID, 2009).

Ein RFID System beinhaltet die beiden Komponenten Transponder und Lesegerät und wird in Abbildung 11: Komponenten eines RFID Systems grafisch veranschaulicht (Finkenzeller, 2008).

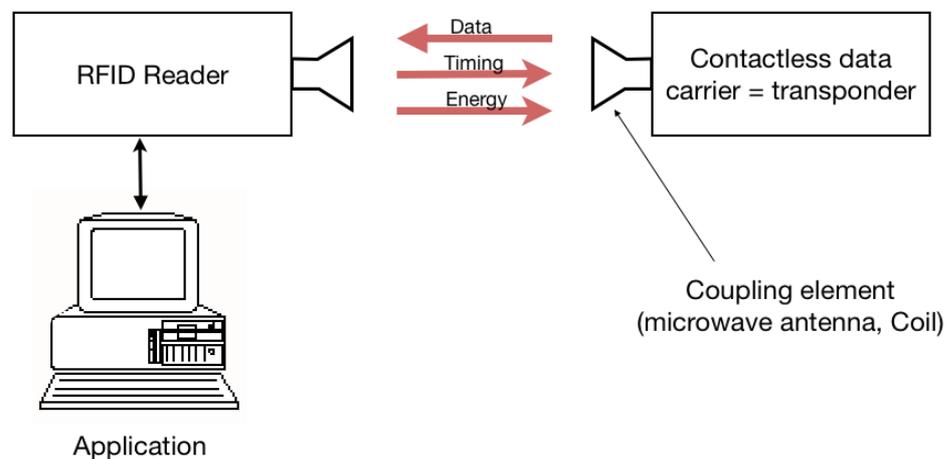


Abbildung 11: Komponenten eines RFID Systems (Finkenzeller, 2008)

3.3.5.4 USB Token

Oft werden die Funktionen einer Smart Card zur Verschlüsselung und zur Signierung von Nachrichten auf einem USB (Universal Serial Bus) Token angeboten. Dieser benötigt keine speziellen Lesegeräte, da fast jeder Personal Computer über eine USB-Schnittstelle verfügt.

Die Token unterscheiden sich nur äußerlich von Smart Cards, bestehen aber aus denselben Elementen und verfügen ebenso über integrierte Rechenleistung für die Ausführung der Funktionen (Schweitzer, 2004).

3.3.5.5 Mobiltelefon und PDA

Auch Mobiltelefone können Träger für digitale Identitäten sein. Des Weiteren verfügen sie über große Speicherkapazitäten sowie Rechenleistungen und unterstützen gängige Programmiersprachen, wie Java (Schweitzer, 2004).

Die Identifikation und Authentifikation findet mit der SIM Card statt, einer Smart Card, welche in das mobile Gerät gesteckt wird. Die Verwaltung von Identitätsinformationen kann über diese SIM Card, einer zweiten Smart Card in Form des Speichers oder über den internen Speicher des Gerätes erfolgen. Bildschirm und Tastatur werden als Ein- und Ausgabegerät genutzt (Schweitzer, 2004).

Personal Digital Assistants (PDAs) sind mit leistungsfähigeren Prozessoren und größerem Speicherplatz als Mobiltelefone ausgestattet, funktionieren jedoch gleich wie Mobiltelefone in Bezug auf Identifikation und Authentifikation (Schweitzer, 2004).

In den letzten Jahren gab es starke technologische Entwicklungen bei den Mobiltelefonen, welche um neue Funktionalitäten erweitert wurden und somit PDAs überflüssig machten. Diese Smart Phones eignen sich besonders gut als Träger digitaler Identitäten zum Aufruf von eDienstleistungen, da sie meist über große Rechenleistungen sowie große Displays verfügen (Schweitzer, 2004).

3.4 Realisierung

Identifikation bezeichnet den Vorgang der Ermittlung der Identitätsdaten des Benutzers. In der digitalen Welt erfolgt der Identitätsnachweis schrittweise durch Authentifizierung, Autorisierung und Identifikation. Weiters dient Kryptografie hierbei zum Schutz ausgetauschter Daten vor unberechtigtem Zugriff Dritter. Wie der digitale Identitätsnachweis realisiert werden kann, wird in den folgenden Kapiteln beschrieben (Hoye, 2008).

3.4.1 Elektronische Signatur

Die digitale Signatur findet ihren Einsatz auch innerhalb von eGovernment, da viele eServices eine Identifikation der BürgerInnen Voraussetzung um uneingeschränkten Zugang und Nutzung von öffentlichen eServices zu erlangen. Dadurch können die Authentizität des Absenders sowie die Unverfälschtheit der gesandten und empfangenen Daten festgestellt werden (Dridi & Pernul, 2002).

„Elektronische Signatur“ ist kein Synonym für den Begriff „digitale Signatur“, obwohl diese zwei Termini nur schwer voneinander unterscheidbar sind.

Digitale Signatur ist ein Unterbegriff von elektronischer Signatur, es ist ein präziserer Typ. Im Gegensatz zur elektronischen Signatur, ist die digitale Signatur eine spezielle Technologie, die auf asymmetrischer Verschlüsselung beruht. Die digitale Signatur ist ein einzigartiger numerischer Wert, der auf dem gesamten gezeichneten Dokument beruht mit dem Ziel, die Herkunft und die Integrität der Daten zu sichern. Die elektronische Signatur ist der rechtliche Begriff der sich auch alle Arten von Datenauthentifizierung

bezieht und kann auch den gedruckten Namen, die eMail-Adresse oder eine gescannte Signatur umfassen.

Zusammenfassend bedeutet dies: Digitale Signatur ist die Technologie, elektronische Signatur ist das legale Konzept dahinter. Elektronische Signatur wird durch digitale Signatur-Technologie erzeugt (Dumortier, 2004).

Die Beziehung zwischen den beiden Begriffen ist in Abbildung 12: Beziehung zwischen „digitalen“ und „elektronischen“ Signaturen dargestellt.

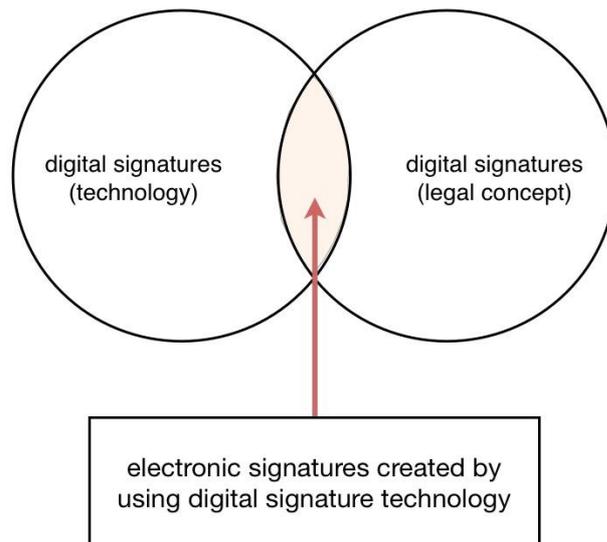


Abbildung 12: Beziehung zwischen „digitalen“ und „elektronischen“ Signaturen (Dumortier, 2004)

Elektronische Signatur kann unterschiedlich ausgeprägt sein und je nach Typ unterschiedliche Funktionen und juristische Wirkung besitzen.

Die Unterschiede werden in der EU-Richtlinie 1999/93/EG festgehalten:

- Einfache elektronische Signatur
Die einfache elektronische Signatur bezeichnet „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen.“ (Europäisches Parlament und Rat, 1999)
- Fortgeschrittene elektronische Signatur (sichere elektronische Signatur)
Die "fortgeschrittene elektronische Signatur" ist eine elektronische Signatur, die folgende Anforderungen erfüllt (Europäisches Parlament und Rat, 1999):
 - a) Sie ist ausschließlich dem Unterzeichner zugeordnet.
 - b) Sie ermöglicht die Identifikation des Unterzeichners.
 - c) Sie wird mit Mitteln erstellt, die der Unterzeichner unter seiner alleinigen Kontrolle halten kann.
 - d) Sie ist so mit den Daten, auf die sie sich bezieht, verknüpft, dass eine nachträgliche Veränderung der Daten erkannt werden kann.

Um Dokumente zu unterzeichnen wird ein asymmetrischer Verschlüsselungsalgorithmus⁵⁸ verwendet.

- Fortgeschrittene elektronische Signatur (qualifizierte elektronische Signatur): Die fortgeschrittene elektronische Signatur beruht auf qualifizierten Zertifikaten und wird durch ein sicheres Signaturerzeugungsgerät erstellt.

Viele eGovernment-Dienste sind nur durch qualifizierte elektronische Signatur erreichbar, da sie die Authentizität des Absenders sowie die Unverfälschtheit der gesandten und empfangenen Daten gewährleistet (Dridi & Pernul, 2002). Die qualifizierte elektronische Signatur beruht auf der Verschlüsselung von Botschaften. Mittels Hash-Verfahrens⁵⁹ wird der Hash-Wert des Dokumentes ermittelt, dieser anschließend mit dem Private Key des Senders verschlüsselt und als Signatur angehängt.

Die Signaturerstellung mit allen beschriebenen Komponenten wird in Abbildung 13: Signaturerstellung dargestellt.

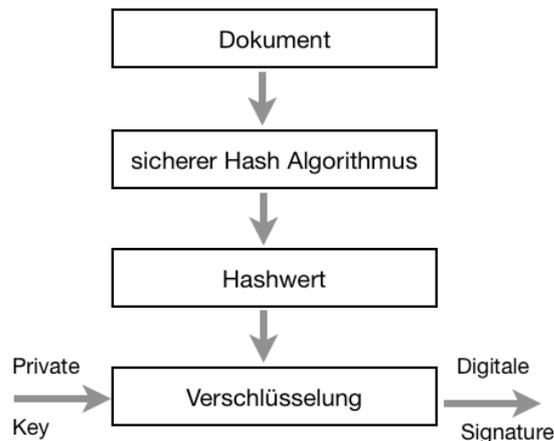


Abbildung 13: Signaturerstellung (Signature Perfect KG, 2008)

Der Empfänger des Dokuments bildet ebenso einen Hash-Wert des Dokuments und entschlüsselt die Nachricht mit dem Public Key des Senders. Die beiden Hash-Werte werden verglichen. Stimmen sie überein wurde die Botschaft genau so verschickt. Diese Signatur des Senders dient dem Empfänger der Nachricht als Bestätigung für die Echtheit des Dokuments (Hühnlein & Korte, 2006).

Das Verfahren zur Prüfung des Hash-Wertes wird in Abbildung 14: Signaturprüfung mittels Hash-Wert dargestellt. Das gesamtheitliche System der digitalen Signatur wird in Abbildung 15: Digitale Signatursysteme dargestellt.

⁵⁸ siehe Kapitel 3.3.2 Verschlüsselung, Seite 47

⁵⁹ Für die Beschreibung von Hash-Verfahren siehe Kapitel 3.3.1 Hash-Verfahren, Seite 46

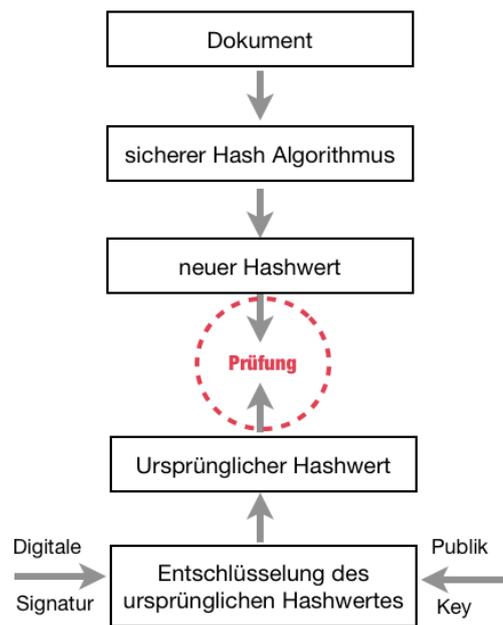


Abbildung 14: Signaturprüfung mittels Hash-Wert (Signature Perfect KG, 2008)

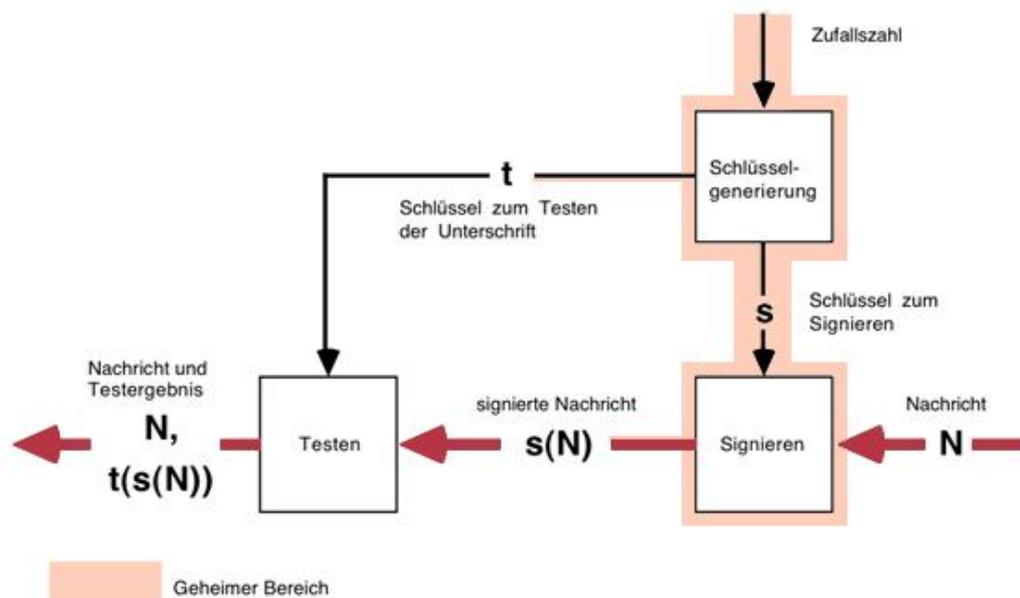


Abbildung 15: Digitale Signatursysteme (Pfitzmann, Waidner, & Pfitzmann, 1990)

Die praktische Erstellung elektronischer Signaturen erfolgt über eine sichere Signaturerzeugungseinheit (SSEE). Diese kann in unterschiedlichen Medien integriert sein, wie beispielsweise in Smart Cards oder USB Token⁶⁰ (Signature Perfect KG, 2008).

⁶⁰ siehe Kapitel 3.3.5 Hardware, Seite 57

3.4.2 Zeitstempel

Ein Zeitstempel wird eingesetzt, um den Inhalt eines digitalen Dokumentes zu einem bestimmten Zeitpunkt zu bestätigen. Zeitstempel werden online von Zeitstempeldiensten oder Servern erstellt. Ein Zeitstempel wird wie eine elektronische Signatur erzeugt, ist jedoch nicht personengebunden.

Die Datenstruktur beinhaltet:

- Erstellungsdatum und Uhrzeit des Stempels
- Hash-Wert des Dokumenteninhaltes

Qualifizierte Zeitstempel werden durch zertifizierte Unternehmen wie Trust Center oder durch zertifizierte Geräte erstellt (Signature Perfect KG, 2008).

Zeitstempel können als Ergänzung zu qualifizierten elektronischen Signaturen eingesetzt werden, um die Signaturerstellungszeit festzuhalten. Damit lässt sich ein Zeitpunkt festhalten, an dem ein Zertifikat noch Gültigkeit hat und somit eine Signatur zu Recht erfolgt (Signature Perfect KG, 2008).

3.4.3 Digitale Zertifikate

Um ein Dokument qualifiziert zu signieren, ist ein entsprechendes Zertifikat von Nöten.⁶¹ Ein Zertifikat entspricht einem digitalen Personalausweis. Bei einem solchen Ausweis garantiert die zuständige Vertrauensstelle, dass die angeführte Unterschrift tatsächlich vom Besitzer stammt. In der digitalen Welt ist dies gleich zu setzen wie die elektronische Signatur. Hier dient der Public Key zur Verschlüsselung und zur Prüfung einer Signatur. Um die Echtheit einer Signatur zu überprüfen, wird die Zugehörigkeit eines Public Keys zu einer Person überprüft und durch ein Zertifikat bestätigt.

Die vertrauenswürdige Instanz wird hierbei als Zertifizierungsdiensteanbieter (Certification Authority CA oder Certification Service Provider CSP) bezeichnet. Die CA überprüft die Zugehörigkeit des Public Keys zu einer Person und stellt zur Bestätigung ein sogenanntes Public Key Zertifikates aus. Die Authentizität dieses Zertifikates wird durch die Signatur des Zertifizierungsdiensteanbieters sichergestellt (Schweitzer, 2004).

Der Zertifizierungsdiensteanbieter ist für die Korrektheit des ausgestellten Zertifikates sowie für die Einhaltung der Richtlinien verantwortlich.

Die Richtlinien für Zertifikate sind in der Zertifikationspolicy (Certificate Policy CP) enthalten, welche durch das Signaturgesetz und die Verordnung festgelegt werden.

⁶¹ siehe Kapitel 3.4.1 Elektronische Signatur, Seite 68

Eine Certificate Policy enthält Regelungen, was ein Zertifikat beinhalten muss und unter welchen Bedingungen ein Zertifikat sicher benutzt werden kann. Somit kann der Empfänger mit Hilfe der Certificate Policy die Qualität der Signatur überprüfen.

Zertifikate müssen der Certificate Policy entsprechen und enthalten Informationen über den Namen des Benutzers, den öffentlichen Schlüssel (Public Key) des Benutzers, die Gültigkeitsdauer des Zertifikates sowie den Namen der Zertifizierungsstelle und deren elektronische Signatur.

Ein verbreitetes Format für Zertifikate ist X.509. Da es eine große Anzahl an verschiedenen Verschlüsselungsverfahren, Zertifizierungsdiensteanbietern und Zertifikatinhabern gibt, ist es notwendig, einen einheitlichen Standard für Zertifikate zu etablieren, um eine Interoperabilität zu gewährleisten. Daher entstand 1988 der X.509 Standard, welcher mittlerweile in Version 3 den Aufbau von Zertifikaten beschreibt. X.509 beinhaltet eine Reihe an erforderlichen und optionalen Feldern und wird in Abbildung 16: Format des X.509 v3 Zertifikats dargestellt (Dietrich, 2004).

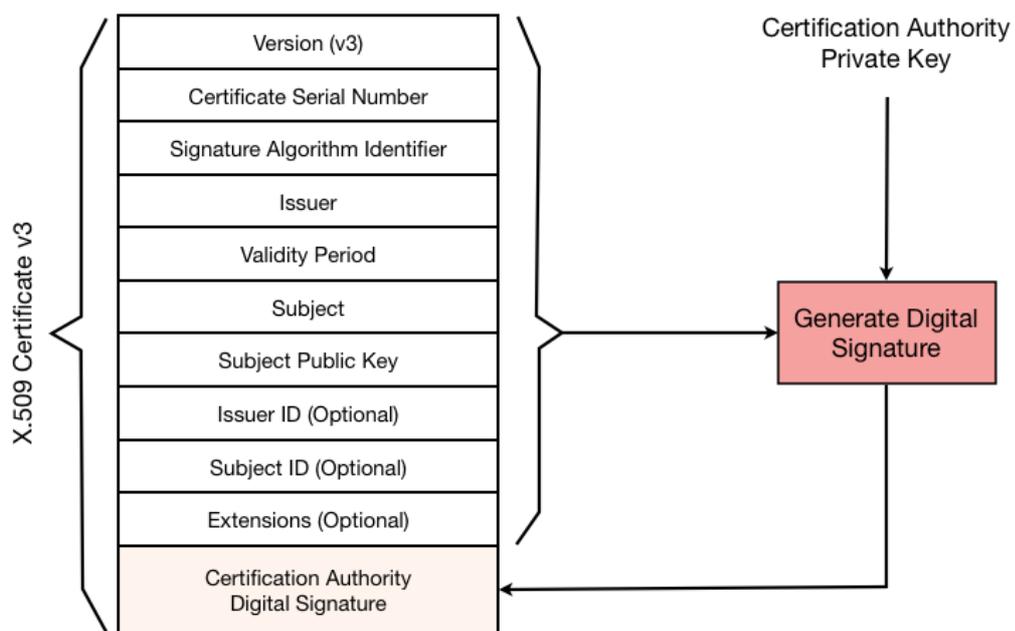


Abbildung 16: Format des X.509 v3 Zertifikats (Dietrich, 2004)

Einige Datenfelder des X.509 Zertifikates und deren Aussage werden in Tabelle 4: Aufbau eines X.509 v3 Zertifikats beschrieben⁶².

⁶² Eine genau Beschreibung der einzelnen Felder unter: <http://www.faqs.org/rfcs/rfc2459.html> (Zugriff am 01.10.2011)

Tabelle 4: Aufbau eines X.509 v3 Zertifikats (The Internet Society, 1999)

Inhalt	Erläuterung
Versionsnummer	beschreibt die Versionsnummer [0-2], derzeit 2 für V3
Seriennummer	eindeutiger Identifikator innerhalb der CA
Signatur	Verwendete kryptografische Algorithmen
Aussteller	Name der CA
Gültigkeitsdauer	Zeitpunkte für Beginn und Ende der Gültigkeit des Zertifikats
Benutzername	Name des Benutzers
Schlüssel	Public Key des Benutzers und verwendeter Algorithmus
Aussteller ID	optionale ID zur eindeutigen Identifikation
Benutzer ID	optionale ID zur eindeutigen Identifikation
Signatur	Signatur des Zertifikats unterschrieben mit dem Private Key

Abbildung 17: Zertifikat von Swisskey AG zeigt anhand eines Beispiels, wie ein Zertifikat der Swisskey AG im Netscape Communicator aussieht (Schlauri, 2002).

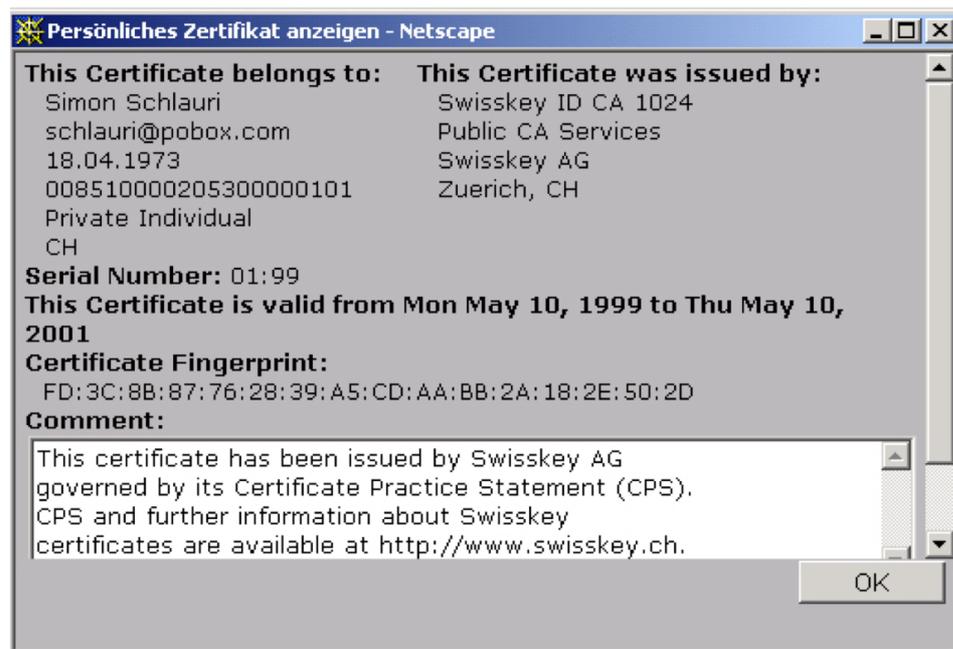


Abbildung 17: Zertifikat von Swisskey AG (Schlauri, 2002)

Ein Zertifikat hat nur eine beschränkte Gültigkeit und kann für maximal fünf Jahre ausgestellt werden. Nach Ablauf dieser Zeit wird das Zertifikat im Trust Center gesperrt.

Ein Zertifikat kann gestohlen oder beeinträchtigt werden, ablaufen oder inkorrekt ausgestellt werden. Für diese Probleme stellt die Behörde eine Widerrufsliste (The Zertifikate Revocation List CRL) und ein online abrufbares Statusprotokoll für Zertifikate

zur Verfügung. Die Widerrufsliste enthält alle widerrufenen Zertifikate zusammen mit dem Grund des Widerrufs. Wenn jemand Zutritt zu einem Server erlangen möchte wird das Zertifikat mit Hilfe der Widerrufsliste auf seine Gültigkeit überprüft und der Zutritt gewährt oder verweigert, je nach Status des Zertifikates. Um am aktuellen Stand zu bleiben, muss die Liste regelmäßig heruntergeladen werden. Eine Alternative zu CRL stellt das Online Certificate Status Protocol (OCSP) dar. Dieses muss nicht aktuell gehalten werden, sondern wird in Echtzeit überprüft.

Digitale Signaturen werden eingesetzt um Nachrichten oder Daten zu signieren, als auch zu Authentifikationszwecken um Kommunikationspartner zu authentifizieren. Eine Signatur kann die Benutzerkennung und das Passwort bei einer Anmeldung ersetzen als auch zur Authentifizierung von Webservern und Webclients eingesetzt werden.

3.4.4 Authentisierung und Autorisierung

Der Vorgang der Authentisierung und Autorisierung wird im englischen allgemein als „authentication“ zusammengefasst. Auch im Deutschen werden diese Ausdrücke vielfach und fälschlicherweise synonym verwendet.

3.4.4.1 Authentisierung

Zur Authentisierung bedarf es einiger Schritte, von der Authentisierung des Kartenlesegerätes gegenüber der Karte bis hin zu endgültigen Authentisierung des Users gegenüber der Dienstleistung.

Für die Zugriffskontrolle des Smart Card Chips und des Terminals werden kryptografische Protokolle benutzt, mit welchen der Zugriff auf die Daten der Karte möglich werden. Die entsprechenden Protokolle werden in Kapitel 3.3.4 Protokolle, Seite 48 beschrieben, die Authentisierungsverfahren werden im Folgenden erläutert.

Terminalauthentisierung

Für einen Zugriff auf die Singnaturfunktion der Karte muss sich das Kartenlesegerät gegenüber der Karte ausweisen. Dies geschieht über eine Terminalauthentisierung auf der Karte (Bundesamt für Sicherheit in der Informationstechnik, 2011). Die Smart Card kann dadurch überprüfen, ob die Kommunikation über eine autorisierte Gegenstelle erfolgt. Das Kartenlesegerät wird als „trusted“ oder „untrusted“ authentifiziert.

Weiters dient die Terminalauthentisierung dem Nachweis der Zugriffsrechte durch ein Terminal oder eines Dienstanbieters (Bundesamt für Sicherheit in der Informationstechnik, 2011). Es können die Berechtigungen der Gegenstelle abgefragt werden (Bundesamt für Sicherheit in der Informationstechnik, 2009).

Diese Rechte werden an die Sitzungsschlüssel gebunden, welche in der Chipauthentisierung ausgehandelt wurden. Damit können die Rechte nur innerhalb dieses Kommunikationskanals ausgeübt werden⁶³ (Bundesamt für Sicherheit in der Informationstechnik, 2011).

Die Rechte werden über die Zertifikate vergeben, welche von der Berechtigungs-PKI festgelegt wird. Die PKI übermittelt Zertifikate an den Chip, in welcher der Typ als auch die Rechte des Terminals festgelegt werden. Diese Zertifikate werden durch sogenannte Berechtigungs-Certification Authorities ausgegeben.

Die Terminalauthentisierung ist nur erfolgreich, wenn der Terminaltyp mit dem Typ der über PACE angekündigt wurde übereinstimmt und das Passwort für diesen Terminaltyp zulässig ist. Nur dadurch kann eine Terminalauthentisierung nachgewiesen werden (Bundesamt für Sicherheit in der Informationstechnik, 2011).

Nach erfolgreicher Authentisierung des Kartenlesegeräts mittels Terminalauthentisierung kann davon ausgegangen werden, dass das Lesegerät ein autorisiertes Kommunikationsgerät ist (Bundesamt für Sicherheit in der Informationstechnik, 2011).

Passive Authentisierung

Die passive Authentisierung dient dem Echtheitsnachweis der Daten, die auf dem Chip gespeichert werden. Dazu werden die Daten und der öffentliche Schlüssel der Smart Card signiert (Bundesamt für Sicherheit in der Informationstechnik, 2011). Die entsprechenden Zertifikate sind auf dem Smart Card Chip gespeichert und werden vom Terminal überprüft. Das Zertifikat wird manipulationssicher auf dem Kartenlesegerät gespeichert. Alle weiteren notwendigen Daten sind auf der Smart Card selbst gespeichert (Bundesamt für Sicherheit in der Informationstechnik, 2011).

Mittels passiver Authentisierung werden nur die gespeicherten Daten auf ihre Echtheit geprüft, die Echtheit des Chips wird mittels Chipkartenauthentisierung festgestellt (Bundesamt für Sicherheit in der Informationstechnik, 2011).

Chipauthentisierung

Die Chipauthentisierung prüft die Authentizität des Smart Card Chips und weist nach, dass sich der Chip im Besitz des privaten Schlüssels (Private Key) befindet, der zum öffentlichen Schlüssel (Public Key) gehört. Damit wird es für die Gegenstelle der Smart Card möglich zu überprüfen, ob die Kommunikation über einen authentisierten Chip erfolgt (Bundesamt für Sicherheit in der Informationstechnik, 2011).

⁶³ siehe Unterkapitel Chipauthentisierung, Seite 77

Weiters wird durch die Chipauthentisierung eine sichere Kommunikation zwischen Smart Card und Terminal ermöglicht. Es werden Schlüssel vereinbart und ein sicherer Kanal (Secure Messaging) zwischen Kartenlesegerät und Ausweis aufgebaut. Dafür wird das PACE Protokoll eingesetzt⁶⁴ (Bundesamt für Sicherheit in der Informationstechnik, 2011).

Sichere Kommunikation

Die Kommunikation zwischen Smart Card und Gegenstelle muss verschlüsselt und integritätssicher ablaufen. Dies kann durch Schlüsselmanagement basierend auf dem PACE Protokoll und der Chipauthentisierung erfolgen. Die Verschlüsselung der Kommunikation gewährleistet die Vertraulichkeit der übertragenen Daten (Bundesamt für Sicherheit in der Informationstechnik, 2011).

Authentisierung des Users gegenüber der Smart Card

Der Benutzer einer Smart Card muss sich gegenüber der Smart Card als berechtigter Benutzer authentisieren um bestimmte Dienste nutzen zu können. Dafür kann der Nutzer Authentisierungsdaten verwalten und diese auf der Smart Card speichern. Diese Autorisierungsdaten werden von den Kartenlesegeräten an die prüfende Smart Card weitergeleitet. Die Autorisierung kann beispielsweise über einen PIN erfolgen (Bundesamt für Sicherheit in der Informationstechnik, 2011).

Online Authentisierung

Am Online ePortal muss eine komplette Authentisierung durchgeführt werden. Im Browser wird die Seite der Dienstleistung aufgerufen und die Anmeldung gestartet. Die Anmeldeprozedur muss authentisiert werden (Bundesamt für Sicherheit in der Informationstechnik, 2011). Dafür werden Anmeldeinformationen, wie beispielsweise Benutzername und Kennwort, mit einer Liste bekannter Daten abgeglichen. Sind diese Informationen korrekt, wird der Benutzer authentifiziert (Lhotka, Rockford, 2004).

Der Beweis der Identität, die Authentisierung, kann auf drei Arten passieren (Fegghi, & Williams, 1998):

- Wissen, kognitive Identifikation: aufgrund von Passwort oder PIN
- Besitz, possessive Identifikation: basierend auf einer Smart Card, einem USB-Token etc.
- Sein, existenzielle Identifikation: mittels Fingerprint, Stimme etc.

⁶⁴ siehe Kapitel 3.3.4.1 Datenübertragungsprotokolle für Kartenlese, Seite 53

3.4.4.2 Autorisierung

Die Autorisierung findet nach einer Authentisierung des Users statt und entscheidet welche Funktionen genutzt werden können und welche Berechtigungen dieser innerhalb der Anwendung hat, wie beispielsweise Zugriffsberechtigungen (Lhotka, Rockford, 2004).

Um eine Aktion auf einer Ressource, wie beispielsweise einer Smart Card, erfolgreich zu autorisieren, muss sich die Entität vorab gegenüber einem Policy Enforcement Point (PEP) identifizieren (Lutters, 2009). Dies bedeutet, die Entität muss beweisen, dass sie berechtigt ist, die angegebene Identität zu führen (Lutters, 2009).

Nachdem PEP die Nachweise über die Identität erhalten hat, beauftragt dieser einen Authentifikationsserver, die Korrektheit der Daten zu prüfen und damit die Person zu authentifizieren. Wurde dies positiv bestätigt, wird die bestätigte Identität inklusive der Sicherheitsrichtlinien an einen Policy Decision Point (PDP) weitergereicht.

Anhand der Sicherheitsrichtlinie und der Identität bestimmt PDP die Erlaubnisse und Berechtigungen, welche die anfragende Entität mit der bestimmten Ressource hat. Berechtigungen beschreiben Dienste, welche die Entität nutzen darf, während Erlaubnisse Aktionen beschreiben, die die Entität mit der Ressource ausführen darf. Dazu zählen beispielsweise Dateizugriff oder Speicherquota. Das Ergebnis dieser Untersuchung wird über eine Authorization Decision Assertion (ADA) an den PEP zurückgeschickt. PEP erlaubt oder verweigert anhand der ADA der Entität die beantragte Aktion für diese Ressource. Dieser Prozess wird in Abbildung 18: Autorisierung und Authentisierung dargestellt.

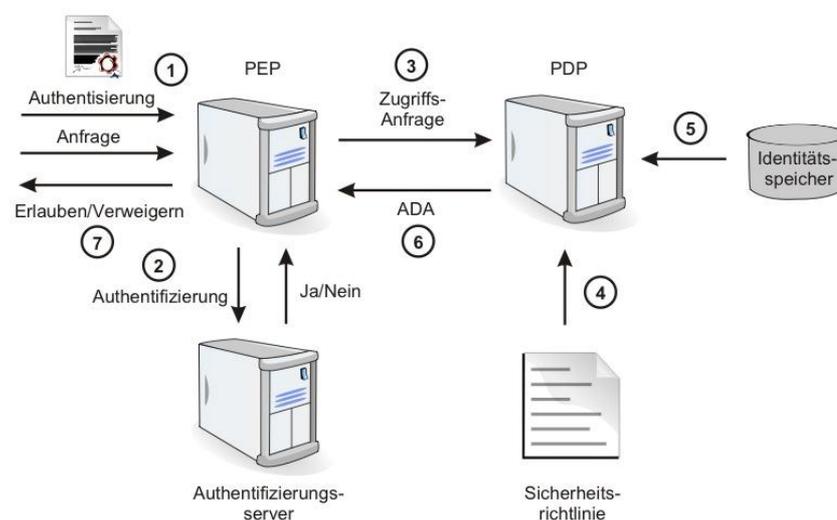


Abbildung 18: Autorisierung und Authentisierung (Lutters, 2009)

3.4.4.3 eID-Anwendung

Mit Hilfe der eID-Anwendung, welche auf einer Smart Card gespeichert wird, ist es dem Inhaber möglich, sich zu authentisieren und zu identifizieren. Diese eID-Funktion umfasst folgende Datenfelder (Lutters, 2009):

- Vorname, Familienname
- Titel
- Geburtsdatum, Geburtsort
- Flags für die Kennzeichnung unterschiedlicher Mindestalter
- Anschrift
- Dokumentenart
- Ausstellendes Land
- Abfragemöglichkeit der Dokumentengültigkeit

Nach einer erfolgreichen Authentisierung erhalten Terminals Zugriff auf die Identitätsdaten, die auf der Smart Card gespeichert sind. Der Vorgang der Ermittlung der Identitätsdaten des Benutzers wird als Identifikation bezeichnet (Bundesamt für Sicherheit in der Informationstechnik, 2011).

Ein Zugriff auf die Daten der eID-Funktion ist nur durch autorisierte Stellen mittels Zertifikate möglich. Bei jeder Transaktion kann sich der Benutzer alle Daten anzeigen lassen, die von einer Funktion angefordert werden und diese bei Bedarf selektiv einschränken. Eine Übertragung ausgewählter Daten muss vom Benutzer mittels PIN bestätigt werden (Lutters, 2009).

Die Authentizität und Integrität der Daten wird durch den verschlüsselten Kanal gesichert, welcher durch die Chipauthentisierung aufgebaut wurde (Bundesamt für Sicherheit in der Informationstechnik, 2011).

3.4.5 Implementation

Es gibt bereits eine Reihe von Implementationen, welche sich mit unterschiedlichen Aspekten und Problemen von digitalen Identitäten beschäftigen.

3.4.5.1 Kerberos

Kerberos ist ein Authentifikationsdienst, welcher vollständig auf symmetrischen Verschlüsselungsverfahren basiert. Der Schlüsselaustausch findet hier über ein Key Distribution Center statt. Kerberos besteht aus dem Authentication Server (AS) und dem Ticket Granting Server (TGS).

Für eine sichere Kommunikation erfragt der Web-Client vom Authentication Server ein Ticket. Dieses wird mit einem Schlüssel des Web-Clients verschlüsselt. Das Ticket kann damit nur vom Web-Client entschlüsselt werden und kann beim Ticket Granting Server eingelöst werden. Somit wurde der Web-Client authentifiziert.

Für eine Kommunikation sendet der Ticket Granting Server dem Web-Client einen Schlüssel sowie die Bestätigung der Authentifikation. Gegen Vorweis dieser beiden Informationen kann der Web-Client die Kommunikation mit dem System starten (Massachusetts Institute of Technology, 2011).

3.4.5.2 Public Key Infrastruktur PKI

Die Public Key Infrastruktur (PKI) ist ein Framework für asymmetrische Verschlüsselungen und digitale Signaturen innerhalb von Netzwerken mittels Public Key Zertifikaten⁶⁵.

Eine PKI wird verwendet, um die Echtheit der Verschlüsselung und der digitalen Signatur bewerten zu können (Dridi & Pernul, 2002).

Dieses Framework besteht aus vielen Instanzen und Komponenten, wie Zertifizierungsdienstanbieter, Benutzer, Zertifikate und Verzeichnisse. Die Aufgabe der Infrastruktur ist es, diese einzelnen Komponenten zu organisieren und verwendete Protokolle und Dokumente zu standardisieren (Bundesamt für Sicherheit in der Informationstechnik, 2006).

Die folgende Abbildung 19: PKI Umgebung gibt einen Überblick dieser Komponenten innerhalb einer PKI.

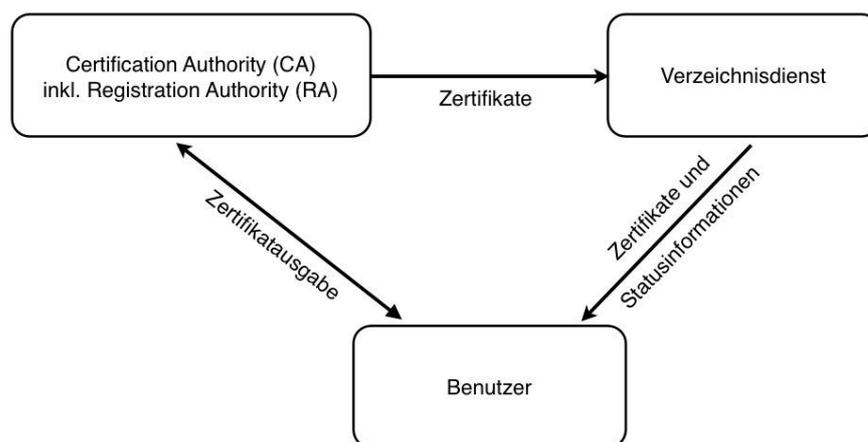


Abbildung 19: PKI Umgebung (Schweitzer, 2004)

Stellt eine Person einen Antrag auf ein Zertifikat, so übernimmt die Authentifikation des Antragstellers die Registration Authority (RA). Weiters treten Zertifizierungsdienstleister (CAs) innerhalb einer PKI als Trust Center auf und bürgen für die Zugehörigkeit eines öffentlichen Schlüssels (Public Key) zur Identität eines Zertifikatinhabers.

Der Verzeichnisdienst (DIR) des Zertifizierungsdienstleisters stellt ein Verzeichnis für öffentliche Schlüssel und Zertifikate dar.

⁶⁵ siehe Kapitel 3.4.3 Digitale Zertifikate, Seite 72

Alle Dienste stehen in dem Personal Security Environment (PSE) innerhalb der PKI-Anwendung zur Verfügung. Das PSE bezeichnet den Ort, an welchem die privaten Schlüssel (Private Key) verwahrt werden, wie beispielsweise einer Smart Card (Lutters, 2009).

3.4.5.3 PKI mit X.509 Zertifikaten

Ein weit verbreitetes Format für Public Key Zertifikate ist das X.509 Format. X.509 basiert auf einem hierarchisch aufgebauten Vertrauensmodell, dargestellt in Abbildung 20: Hierarchische PKI, und umfasst mehrere vertrauenswürdige Instanzen, von welchen Vertrauensbeziehungen abgeleitet werden (Schweitzer, 2004).

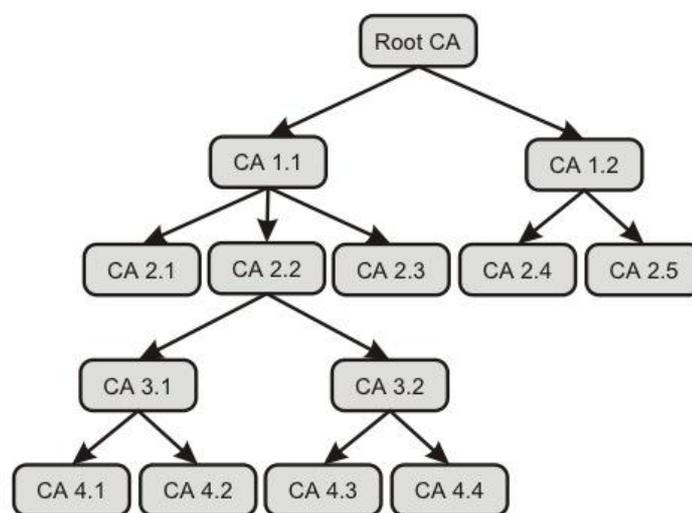


Abbildung 20: Hierarchische PKI (Lutters, 2009)

Die höchste Instanz wird als Root Certification Authority (Root Certification Authority) bezeichnet. Die Root Certification Authority besitzt ein selbstsigniertes Zertifikat des Public Keys, das so genannte Root-Zertifikat. Alle Certification Authorities innerhalb der PKI können nun entweder X.509 Endbenutzerzertifikate ausstellen oder weitere untergeordnete CAs zertifizieren. Dabei besitzen die Certification Authorities 1.1 und 1.2 nur Zertifikate, welche von der Root Certification Authority ausgestellt wurden. Certification Authority 2.1 bis 2.3 besitzen Zertifikate der Certification Authority 1.1 und so weiter. Jedes Zertifikat in einer PKI kann schlussendlich auf das Root-Zertifikat der Root Certification Authority zurückgeführt werden.

Diese Kette an Zertifikaten wird als Vertrauenskette (chain of trust) bezeichnet (Lutters, 2009).

3.4.5.4 PKI mit PGP

Eine weitere PKI-Lösung stellt die Pretty Good Privacy (PGP) dar. PGP ist frei verfügbar für den Privatgebrauch und wird zur Verschlüsselung sowie Signierung von eMails verwendet. Die Nachrichten werden mittels eines symmetrischen Verfahrens verschlüsselt und der Schlüssel mit einem asymmetrischen Verfahren daraufhin ausgetauscht. Das Format des Public Key Zertifikates unterscheidet sich vom X.509 Standard. Auch wird keine zentrale Instanz eingesetzt, sondern Benutzer sind in einem Key Ring organisiert und akzeptieren gegenseitig ihre öffentlichen Schlüssel (Public Key). Man spricht hier von einem „Web of Trust“. Zur Verschlüsselung der Nachricht wird beispielsweise ein IDEA- oder CAST-Algorithmus (symmetrisch), für den Schlüsselaustausch zum Beispiel ein RSA Algorithmus (asymmetrisch) verwendet (Zimmermann, 2002).

Der Ablauf der Verschlüsselung von Pretty Good Privacy wird in Abbildung 21: PGP Verschlüsselung dargestellt.

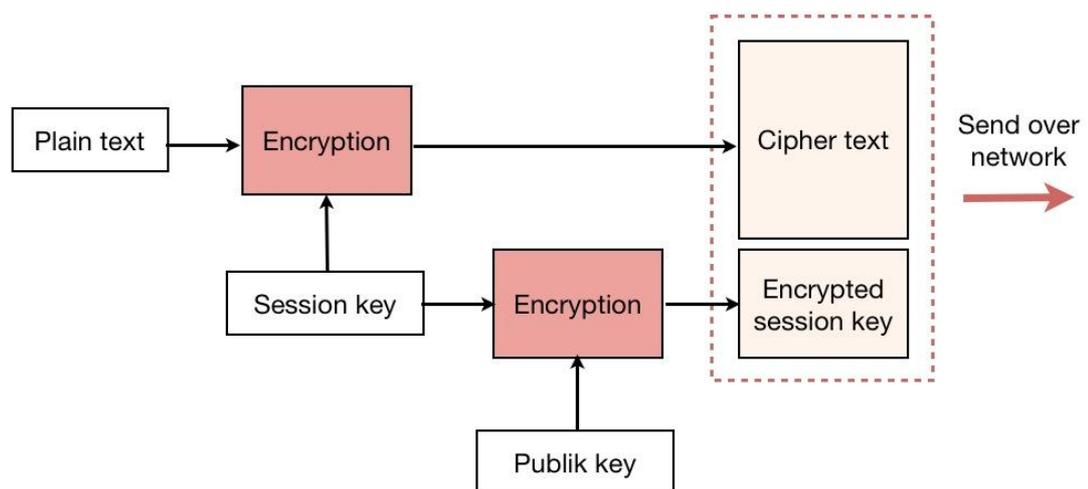


Abbildung 21: PGP Verschlüsselung (Zimmermann, 2002)

4 eID im Einsatz

Immer mehr Länder haben die Vorteile neuer Informations- und Kommunikationstechnologien erkannt und haben sich zum Ziel gemacht, eine zentrale virtuelle Anlaufstelle für BürgerInnen und Unternehmen zu schaffen. Um sichere Kommunikation und Datenaustausch zwischen BürgerInnen und Unternehmen entwickelten Länder unterschiedliche eID Lösungen.

Im folgenden Kapitel werden einige eID-Lösungen sowie eGovernment Dienstleistungen unter Einbindung von digitaler Identität präsentiert. Bei der Auswahl der dargestellten Länderbeispiele wurde versucht, unterschiedliche Lösungen anzubieten, um Unterschiede in Strategie, Implementierungen und Anwendung von elektronischer Identität zu verdeutlichen.

4.1 eID-Lösungen

Auf europäischer Ebene existiert bereits eine Unzahl an eID Konzepten, welche vor allem für die Verwendung von eGovernment Diensten im öffentlichen Sektor gebraucht werden. Mit der steigenden Bedeutung von eGovernment, wo Transaktionen elektronisch durchgeführt werden, ist es wichtig, die eigene Identität ohne persönlichen Kontakt zu bezeugen. Auch wird oft der Einsatz von elektronischen Signaturen in diesem Kontext gebraucht, um legal bindende Verträge und Formulare zu unterzeichnen (A-SIT, 2004).

4.1.1 Username/Passwort Systeme

Einige Länder benutzen Systeme außerhalb einer PKI um Personen zu authentifizieren. So verwenden einige Länder ein Benutzernamen/Passwort System um Zugriff zu diversen Applikationen zu ermöglichen (European Communities, 2009).

In manchen Ländern bedarf es dafür vorab einer persönlichen Identifikation bei der Behörde oder online Registrierung bei der Applikation. In Zypern müssen sich User zuerst persönlich bei der Behörde ausweisen, um danach einen Zugang zur Applikation TAXISnet mittels Benutzernamen/Passwort zu erhalten. In Tschechien bedarf es zuerst einer Anmeldung bei der Applikation mittels qualifiziertem Zertifikat, dache ist eine Authentifizierung mittels Username/Passwort möglich (European Communities, 2009).

4.1.1.1 Länderbeispiel Norwegen

Eines der bekanntesten Beispiele für ein Username/Passwort System ist die Implementierung von MinID in Norwegen im Oktober 2009. MinID ermöglicht den Zugang zu vielen öffentlichen Dienstleistungen über das Internet. Es handelt sich hierbei um einen eine PinCode Karte, welche zur Anmeldung bei der Steuerbehörde oder anderen Institutionen dient, wie beispielsweise Zugang zum ePortal MyPage (European Communities, 2009).

Je nach Applikation ist eine single factor Identifikation mittels Benutzername/Passwort oder eine two-factor Identifikation mittels SMS Authentifizierung erforderlich (European Communities, 2009).

Bereits 1.5 Millionen Norweger nutzen bereits MinID. In Zukunft soll es auch möglich sein, sich mittels einer eID-Karte einzuloggen, was einer der wichtigsten Meilensteine für die digitale Entwicklung in Norwegen darstellen wird.

4.1.2 Soft Identity Token

Token sind nicht immer auf Smart Cards reduziert, und können auch PKI Zertifikate in Soft-Format oder Zertifikate auf einem anderen physischen Träger, wie beispielsweise USB, umfassen.

4.1.2.1 Länderbeispiel Dänemark

Um die BürgerInnen zu einer Nutzung anzuregen, entwickelte Dänemark 2003 ein offizielles elektronisches Signaturschema, welches allen BürgerInnen kostenlose elektronische Signatur bereitstellte. Diese konnte für die meisten öffentlichen und privaten Kontakte genutzt werden (Nielsen & Meinertz, 2003).

Im Jänner 2010 wurde daher eine Roadmap entworfen, welche eine „neue digitale Signatur NemID“ einführen soll.

NemID (im Deutschen „Einfache ID“) ist eine elektronische Signatur, die auf softwarebasierten Signatur-Zertifikaten beruht (European Communities, 2009).

Diese ermöglicht damit einen Zugang zu öffentlichen elektronischen Diensten durch sichere Identifikation (Europäische Union, 2011).

NemID wurde Mitte 2010 in enger Zusammenarbeit mit dem Bankensektor eingeführt, um zu ermöglichen, NemID sowohl in öffentlichen als auch privaten Sektor sowie für Net-Banking für eine sichere Authentifizierung einsetzen zu können. Ziel der Einführung war, die Qualität von öffentlichen Services für BürgerInnen und Unternehmen zu erhöhen und die Bereitstellung öffentlicher Services so effizient und effektiv wie möglich zu gestalten (Wang, 2011).

4.1.3 Hard Identity Token

4.1.3.1 Smart Cards

Eine Studie der Europäischen Gemeinschaften⁶⁶ zeigte, dass Identitätskarten die dominante Lösung für digitale Identifikation darstellen (European Communities, 2009).

⁶⁶ Quelle der Studie (European Communities, 2009)

Eine eID-Karte gewährleistet eine eindeutige Identifikation und Authentifizierung und ermöglicht dadurch einen sicheren Zugang zu online Dienstleistungen. Viele Dienstleistungen sind daher nur mehr mittels eID-Karte zugänglich (Dumortier, 2004).

Von zweiunddreißig Ländern haben bereits dreizehn Länder eID-Karten an die BürgerInnen ausgegeben, wie beispielsweise Belgien, Italien oder Litauen. Siebzehn Länder planen eine eID-Karte einzuführen und haben teilweise bereits Pilotprojekte gestartet. Nur fünf Länder geben derzeit keine ID Karten aus: Dänemark, Irland, Lettland, Norwegen und UK. Bis auf Dänemark existieren bereits Pläne zur Implementierung einer eID-Karte (European Communities, 2009).

Länderbeispiel Finnland

Ein Pionier in der Implementierung eines eID Konzeptes war Finnland. Als erstes Land der Welt schuf Finnland einen rechtlichen Rahmen für den Einsatz von eID-Karten. Im Juli 1999 wurde der Electronic Identity Cards Act verabschiedet und im Dezember 1999 wirksam (A-SIT, 2004). Die ersten eID-Karten (FINEID) wurden daraufhin bereits im Dezember 1999 ausgegeben.

Die eID-Karte ist mit einem Chip ausgestattet, welcher ein sogenanntes „Citizen Certificat“ enthält. Dieses Citizen Certificat enthält Informationen über den/die BürgerIn und einen elektronischen Identifikator. Es zertifiziert dass der öffentliche Schlüssel dem Besitzer der eID-Karte zugeordnet werden kann⁶⁷ (Finnish Population Registration Centre, 2006).

Die elektronische Identität wird generiert, indem der/die BürgerIn diese mit der Eingabe eines persönlichen Identifikationscode bestätigt. Der elektronische Identifikator identifiziert daraufhin den Nutzer in einer sicheren Online-Transaktion (Finnish Population Register Centre, 2011).

Die Zertifikate werden für die Verschlüsselung von eMails, Daten oder Dokumenten verwendet und ermöglichen die Erzeugung elektronischer Signaturen (Finnish Population Register Centre, 2006). Durch die Funktion der elektronischen Identifikation ermöglicht die eID ebenso die Nutzung von elektronischen Services der öffentlichen Verwaltung, Versicherungen sowie diversen Einrichtungen. Weiters gilt es als offizielles Reisedokument innerhalb von neunzehn Europäischen Ländern (A-SIT, 2004).

Die Citizen Certificates werden von dem Finish Population Register Centre ausgegeben und können auf Smart Cards der Visa Electronic Card, die von der Finnischen OP Bank Group ausgegeben werden, oder auf einer mobilen SIM Card gespeichert werden (Finnish Population Register Centre, 2011).

⁶⁷ mehr zu Zertifikate in Kapitel 3.4.3 Digitale Zertifikate, Seite 72

Eine Smart Card kostet 48€ und wird von polizeilichen Behörden ausgegeben (Finnish Population Register Centre, 2011).

Die Erwartungen an die Karte übertragen jedoch das Ergebnis. Bis März 2004 erwarben nur 26.000 FinnInnen eine FINEID (A-SIT, 2004).

Im Oktober 2006 konnte bereits eine Ausstellung von 123.000 eID-Karten erreicht werden. Die Nummer der aktivierten Citizen Certificates lag 2006 bei 104.000 und steigt jährlich um 35.000 Stück an (Finnish Population Register Centre, 2006).

Ende Juli 2007 wurden insgesamt rund 153.600 Citizen Certificates ausgestellt. 38.600 BürgerInnen haben die eID-Karten mit der Krankenversicherungskarte kombiniert⁶⁸ (Finnish Population Register Centre, 2007). Mit November 2010 wurden insgesamt 341.800 Zertifikate ausgestellt, davon integrierten 159.000 Personen die Krankenversicherungskarte (Finnish Populaton Register Centre, 2010).

Länderbeispiel Belgien

Belgien war Pionier für eine breit gefächerte Distribution von eID-Karten.

Im Jahr 2000 startete die belgische Regierung das eID Projekt BelpIC (Belgian Personal Identity Card) (Europäische Union, 2009). Das Projekt hatte zum Ziel, die bestehenden Identitätskarten um Funktionen zur Identifikation und Authentifizierung zu erweitern. Dafür wurden digitale Zertifikate auf der Identitätskarte gespeichert. Dies ermöglicht den BürgerInnen den Zugang zu verschiedenen elektronischen Dienstleistungen der öffentlichen Einrichtungen (Steria, 2011). Weiters wird durch die Karte der Zugriff auf das Regierungsportal Begium.be⁶⁹ möglich (Europäische Union, 2010).

Im März 2003 wurde die elektronische Identitätskarte offiziell in elf Gemeinden für eine Probezeit von drei Monaten eingeführt (Europäische Union, 2010) und ungefähr 70.000 eID-Karten verteilt (Europäische Union, 2009).

Bereits im April 2003 wurde es ermöglicht, erste Dienstleistungen online zu nutzen, wie beispielsweise Tax-on-Web, eine Applikation zur online Abgabe von Steuererklärungen (eTax)⁷⁰ (Europäische Union, 2010).

Nachdem das eID Projekt erfolgreich startete wurde im September 2004 eine weit angelegte Distribution der eID-Karten gestartet, mit dem Ziel alle BürgerInnen bis Ende 2009 mit einer eID-Karte zu versorgen und somit acht Millionen Karten in Umlauf zu bringen (Europäische Union, 2009).

⁶⁸ Seit Juni 2004 kann die eID-Karte mit der nationalen Krankenversicherungskarte kombiniert werden.

⁶⁹ siehe Kapitel 4.3.1.1 Belgium.be - Belgien, Seite 113

⁷⁰ Details zum eDienst Steuererklärungen siehe Kapitel 4.2.2.1 eTax, Seite 102

Um auch die nicht-elektronische Identitätskarte der im Ausland lebenden Belgier durch die neue eID-Karte zu ersetzen wurden eID-Karten an alle belgischen Konsulate und Botschaften gesandt (Europäische Union, 2010).

Im Juli 2008 wurden für ausländische Staatsangehörige, sowohl für EU und Nicht-EU Mitglieder, elektronische ID Karten ausgegeben um auch diesen eine elektronische Kommunikation mit den Behörden zu ermöglichen (Europäische Union, 2010).

Ende 2006 wurden über vier Millionen eID-Karten ausgestellt, bis 2009 waren es über neun Millionen. BelpIC ist damit eines der größten Projekte in Europa (Federal Public Service for Information and Communication Technology, 2006).

Im Oktober 2007 wurde ein Pilotprojekt gestartet, welches den Entwurf einer eID-Karte für Kinder unter zwölf Jahren (Kids-ID⁷¹) umfasste. Das Projekt wurde im März 2009 erfolgreich umgesetzt und Kids-ID Karten ausgegeben. Im Juli 2009 war bereits die Hälfte aller Kinder in Belgien unter zwölf Jahre im Besitz der Kids-ID, was bedeutet, dass zu diesem Zeitpunkt bereits 115.100 Karten im Umlauf waren (Europäische Union, 2010).

Länderbeispiel Estland

Estland fasste im Jahr 2000 den Beschluss, eine eID-Karte einzuführen. Diese Karten wurden zum ersten Mal im Jänner 2002 aufgegeben. Im ersten Jahr wurden 130.000 Karten ausgestellt. Mit Ende Mai 2005 waren es bereits 765.000 ausgestellte Karten. Weiter 158.000 eID-Karten wurden an ausländische StaatsbürgerInnen ausgegeben. Estland war damit Vorreiter unter den europäischen Ländern in Bezug auf eine breit gefächerte Distribution (Europäische Kommission, 2005).

Die Karten werden in einem Standard-Format ausgegeben, BürgerInnen können nicht über die Funktionalitäten entscheiden. Einzig die Gültigkeit des Zertifikates kann aufgelöst werden (Europäische Kommission, 2005).

Äußerlich enthält die Karte Vorname, Nachname, Geschlecht, Staatsbürgerschaft, Geburtsdatum, Geburtsort, persönliche Identitätsnummer, Fotos, Signatur, Ausstellungsraum, Ablaufdatum und eine Dokumentennummer (Martens T. , Electronic Identity management in Estonia between market and state governance, 2010).

Die Karte ist mit einem Chip ausgestattet, welcher zwei Zertifikate und den privaten Schlüssel (Private Key) speichert, welcher durch einen PIN Code geschützt wird. Die Zertifikate beinhalten den Namen des Besitzers und eine persönliche (nationale) ID Nummer. Mittels der Zertifikate kann eine Authentifizierung vorgenommen sowie eine elektronische Signatur erzeugt werden (Europäische Kommission, 2005).

⁷¹ Details zu Kids-ID unter <http://www.ibz.rrn.fgov.be/index.php?id=1503&L=0> (Zugriff am 01.10.2011)

Ein interessantes Merkmal der eID-Karte ist, dass das Authentifizierungszertifikat auch eine eindeutige eMail-Adresse enthält welche dem Benutzer zugeordnet ist. Das Format der eMail-Adresse ist Vorname.Nachname_NNNN@eesti.ee, wobei NNNN eine Zufallszahl darstellt. Die email Adresse ist nicht mit einem email Service verbunden sondern dient vielmehr als Weiterleitungsadresse. Sie gilt als lebenslange Adresse, welche zur Kommunikation mit Behörden dient, und wird im Estonian National Registry der Zertifizierungsdienstanbieter öffentlich gemacht (Europäische Kommission, 2005).

Die Karten sind verpflichtend für jede/n BürgerIn. Ebenso ist die eID-Karte Voraussetzung für alle eServices welche einer sicheren Authentifizierung bedürfen (Martens T. , eGovernment in Estonia, 2011). Derzeit besitzen 1.1 Mio. BürgerInnen eine eID-Karte (von 1.35 Mio. Bevölkerung), die Hälfte davon verwendet die ID Karte regelmäßig (Martens T. , eGovernment in Estonia, 2011).

4.1.3.2 Biometrische Daten

Als zusätzliches Identitätsmerkmal können biometrische Daten auf eID-Karten gespeichert werden. Eine Studie der Europäischen Gemeinschaften zeigt, dass bereits fünf von zweiunddreißig untersuchten Ländern biometrische Daten verwenden, basierend auf Fingerabdrücken (Italien Litauen, Niederlande, Portugal, Spanien). Vier weitere Länder planen die Einführung biometrischer Daten in Form von Fingerabdrücken (Frankreich, Estland, Türkei, UK), drei Länder denken an, biometrische Daten in einer zukünftigen eID zu inkludieren (Deutschland, Polen, Rumänien) (European Communities, 2009).

In Litauen werden ID-Karten eingesetzt, um die Person in der virtuellen Welt zu identifizieren und ihr zu ermöglichen, elektronische Dokumente mittels elektronischer Signatur basierend auf qualifizierten Zertifikaten zu unterzeichnen. Die neue ID Karte beinhaltet sowohl einen Kontakt- als auch kontaktlosen Chip. Der Kontakt-Chip beinhaltet das Identifikations-Zertifikat und qualifiziertes Zertifikat für die elektronische Signatur. Um noch mehr Sicherheit bei der Identifikation zu gewährleisten beinhaltet der kontaktlose Chip beinhaltet auch biometrische Daten in Form von Fingerabdrücken. Diese Karten werden seit Jänner 2009 ausgegeben (European Communities, 2009).

In Italien muss der Fingerabdrucke seit Jänner 2010 zwingend auf der eID-Karte gespeichert werden. Die Daten werden in einer ge-hash-ten⁷² Form auf dem Chip gespeichert. Auch Portugal, Niederlande und Spanien werden biometrische Daten in Form von Fingerabdruck auf den eID Karten abgespeichert (European Communities, 2009).

⁷² Details zu Hash-Verfahren siehe Kapitel 3.3.1 Hash-Verfahren, Seite 46

Länder wie Estland, Frankreich oder UK planen einen Einsatz von biometrischen Daten zur Identifikation. Frankreich werden Fingerabdrücke bereits abgenommen, wenn eine nicht elektronische ID Karte beantragt wird, diese Daten werden jedoch bis dato nicht weiter verarbeitet. Die zukünftige eID-Karte soll diese biometrischen Daten miteinschließen. Estland sowie UK plant die Einbindung von biometrischen Daten für die nächste Generation der eID-Karte (European Communities, 2009).

4.1.3.3 Mobile Token

Auch mobile Token werden im Rahmen von eGovernment Applikationen eingesetzt. Diese Systeme beinhalten einen Zertifikats-basierenden Zugang zu Applikationen kombiniert mit einem einmaligen SMS Nachrichtensystem. Zusätzliche Software oder Hardware Installationen werden nicht benötigt. In einigen Fällen dient das Mobile Endgerät gleichzeitig als Träger der Identität, Kartenlesegerät und Middleware Applikation⁷³ (European Communities, 2009).

Länderbeispiel Estland

In Estland ist zusätzlich zur eID-Karte auch eine mobile eID erhältlich. Diese Mobile-ID im Mai 2007 eingeführt und durch EMT, ELisa und Tele2 angeboten. Um eine Mobile-ID zu erlangen, muss die SIM Card des mobilen Endgerätes durch eine PKI-fähige ausgetauscht werden. Der Registrierungsprozess für Zertifikate wird durch den Mobilfunkbetreiber durchgeführt. Danach muss der Benutzer die Mobile-ID über ein Web-Interface aktivieren (European Communities, 2009).

Der Vorteil der mobilen ID besteht darin, dass weder ein Kartenlesegerät noch spezielle Software für eine Identifikation benötigt wird (Martens T. , Electronic Identity management in Estonia between market and state governance, 2010).

Länderbeispiel Niederlande

In den Niederlanden existiert das System DigiD, welches eine Identifikation und Authentifizierung für BürgerInnen für eServices bereitstellt⁷⁴. Registrierte Nutzer des DigiD Systems können sich auch mittels mobiler ID anmelden, und erhalten einen SMS Code über Ihr mobiles Endgerät (European Communities, 2009).

4.1.4 eID-Systeme

4.1.4.1 Länderbeispiel Niederlande

Für sichere Identifikation und Authentifizierung von BürgerInnen innerhalb von eGovernment Dienstleistungen implementierte die niederländische Regierung ein

⁷³ Details zu IDs auf Mobiltelefonen siehe Kapitel 3.3.5.5 Mobiltelefon und PDA, Seite 67

⁷⁴ siehe Kapitel 4.1.4 eID-Systeme, Seite 92

ganzheitliches eID-System. DigiD⁷⁵ (dieser Name steht für Digitale Identität) wird von verschiedenen staatlichen Behörden geteilt um eine Authentifizierung der Identität einer Person zu ermöglichen, die Transaktionen über das Internet macht (Mühlberger, 2007). Dieser digitale Pass für Behörden wird von der Verwaltungsorganisation Logius verwaltet und ist an die sogenannte „Bürgerservicenummer“ (sozial-fiskale Identitätsnummer) gekoppelt (Malek, 2011).

Der Anwender der Services, die von den staatlichen Behörden angeboten werden, loggt sich zuerst mittels Login-Code (Name und Passwort) in das System ein, es wird eine sichere Verbindung mittels Secure Socket Layer (SSL) hergestellt und dann kann der Anwender in Kontakt mit einer Reihe an staatlichen Institutionen treten (Mühlberger, 2007).

Die Anzahl der öffentlichen Behörden die dieses DigiD-System implementieren steigt von Tag zu Tag⁷⁶ (Mühlberger, 2007). Zwischenzeitlich ist der größte Teil der niederländischen Gemeinden, wie auch die Steuerbehörde, die Sozialversicherungsbank SVB und das „Uitvoeringsinstituut Werknemersverzekering“⁷⁷ an DigiD angeschlossen (Malek, 2011). Auch die Anzahl der Anfragen über DigiD steigt konstant. Über DigiD ist es möglich, elektronische Anfragen zu senden, beispielsweise bezüglich der Kinderbeihilfe oder Pensionszahlungen an die Versicherungsbehörde. Auch Steuererklärungen können elektronisch eingereicht werden (eTax) (Mühlberger, 2007).

In den Niederlande wurde auch eine PKI entwickelt: PKI Overheid. Es wurde entworfen um sichere elektronische Kommunikation mit der Regierung zu ermöglichen. GBO.Overheid⁷⁸ unterstützt das Management und die Kontrolle dieses Systems (Europäische Union, 2011).

⁷⁵ DigiD wurde durch GBO.Overheid (Gemeenschappelijke Beheerorganisatie) in Kooperation mit den Dutch Tax Authorities entwickelt , Siehe <http://www.digid.nl>

⁷⁶ Eine Liste der teilnehmenden Behörden kann auf <http://www.digid.nl/burger/over-digid/wie-doen-mee> eingesehen werden (Zugriff am 01.10.2011)

⁷⁷ Sozialversicherungsbank SVB ist zuständig für die Leistungen aus der allgemeinen Pensionsversicherung, das „Uitvoeringsinstituut Werknemersverzekering“ ist zuständig für alle Leistungen aus den Sozialversicherungen (Malek, 2011)

⁷⁸ GBO.Overheid (Gemeenschappelijke Beheerorganisatie) ist eine Serviceorganisation die gegründet wurde um eGovernment Services zu Verwalten, wie beispielsweise DigiD. GBO.Overheid ist zuständig für das allgemeine Management des eGovernments

4.1.5 Initiativen zur Förderung von eID

Wie im vorherigen Kapitel präsentiert, konnten viele Länder eine Implementierung von eID erfolgreich realisieren. Dazu bedurfte es in einigen Ländern vieler Initiativen und Aktionspläne. Einige Beispiele, wie Länder die Implementierung von eID vorantrieben oder deren Nutzung förderten, werden in diesem Kapitel aufgezeigt.

4.1.5.1 Länderbeispiel Belgien

Um die nationale eID-Karte zu bewerben wurde 2009 eine Kampagne mit dem Slogan „Your eID as easy as can be“. Die Kampagne zielte darauf ab, bestehende und zukünftige eGovernment Applikationen vorzustellen und auf die verschiedenen Einsatzmöglichkeiten der eID-Karte aufmerksam zu machen (Europäische Union, 2010).

Es wurde eine geführte Tour auf der „Welcome to e-Belgium“⁷⁹ Website angeboten, weiters wurden Informationspakete sowie Kartenlesegerät ausgeteilt (Europäische Union, 2009).

4.1.5.2 Länderbeispiel Estland

Estland war ein Vorreiter unter den europäischen Ländern in Bezug auf eine breit gefächerte Distribution von eID-Karten.

Die ersten Karten wurden im Jänner 2002 ausgegeben. Die Basissoftware für eine Authentifizierung wurde öffentlich zugänglich für alle Entwickler gemacht. Damit können Organisation Applikationen und Prozesse entwickelt, denen eID-Karte als zentrales Identifikationselement zugrunde liegt. Dadurch wurde eine weit verbreitete Annahme und Einsatz der eID-Funktionalitäten erreicht, welches in eine große Anzahl an Applikationen resultierte, beispielsweise online Steuererklärungen (eTax), online Verträge, etc.

Damit kommt Estland dem Ziel immer näher, ein „online Staat“ zu werden, deren Schlüssel zum Erfolg in der digitalen Identifikation einer Person liegt (Europäische Kommission, 2005).

4.1.5.3 Länderbeispiel Norwegen

Norwegen ist sehr bemüht die öffentliche Verwaltung effizienter und Serviceorientierter zu gestalten. Darum wurde im Juni 2005 das eNorway 2009-Projekt gestartet. Als Ziel soll eine PKI entwickelt werden, um eine sichere Kommunikation innerhalb der Regierung und mit den BürgerInnen und Unternehmen über elektronische im Internet angebotene öffentliche Dienste zu ermöglichen. Die wichtigste Entwicklung in Norwegen war die Schaffung einer Elektronischen Identität. Weiters Ein wurde ein ePortal entwickelt und einige eServices gestartet Um auf diese Dienstleistungen zuzugreifen unterstützt die

⁷⁹ siehe <http://www.welcome-to-e-belgium.be/> (Zugriff am 01.10.2011)

norwegische öffentliche Verwaltung den Gebrauch von Smart Cards. Um die Entwicklung von eID Lösungen voran zutreiben wurden Investitionen von ungefähr sieben Millionen Euro getätigt (European Communities, 2005).

4.1.6 Schwierigkeiten bei eID Implementierung

Während einige Länder eine Implementierung von eID rasch realisieren konnten, standen manche Länder vor großen Hindernissen. Einigen gelang es durch Initiativen eID erfolgreich umzusetzen, manche Länder verfügen nach wie vor über keine eID-Lösung.

4.1.6.1 Länderbeispiel Spanien

Bevor Spanien ein eID-Karte implementierte, gab es dreizehn Anbieter für Identifikations- und Zertifikatsdienste. Besonders wichtig waren die digitalen Zertifikate, welche durch Royal Spanish Mint innerhalb des Programmes CERES ausgestellt wurden. Diese CERES Zertifikate wurden bereits seit 1996 ausgestellt, sind softwarebasiert und bedürfen daher keiner weiteren Hardware, wie beispielsweise einem Kartenlesegerät. Jede/r BürgerIn kann ein solches Zertifikat kostenfrei beantragen. 2008 waren circa 1.727.990 Zertifikate in Verwendung. Des Weiteren haben einige autonome Gemeinden eigene digitale Zertifikate ausgegeben (Heichlinger & Gallego, 2010).

Im November 2002 startete Spanien das Electronic National Identity Document Projekt und erweiterte die bestehenden Identitätskarten um Funktionen zur Identifikation und Authentifizierung um die Nutzung von elektronischen Dienstleistungen sicher zu gestalten (Heichlinger & Gallego, 2010).

Besonders hervorzuheben ist Spanien, da die Ausgabe der Karten dezentral passierte und durch die Polizeibehörde durch 256 Polizeidienststellen erfolgte. Im Jahr 2006 wurde die eID-Karte als Teil eines Pilotprojektes zuerst nur in Burgos ausgegeben und umfassten 7.000 eID-Karten. Danach folgten territoriale Implementierungen und die eID-Karten wurden offiziell ausgegeben. Im Februar 2008 wurden 23.000 eID-Karten pro Tag ausgestellt. Ende 2009 besaßen es bereits 13.000.000 BürgerInnen eine eID-Karte (Heichlinger & Gallego, 2010).

Obwohl die Ausgabe der eID-Karten erfolgreich ausgeteilt wurden, war die Nutzung sehr gering. Hier zeigte sich eine Dominanz der CERES Zertifikate, welche nach wie vor zunehmen, obwohl eID eine sichere Alternative für Authentifikation darstellt (Heichlinger & Gallego, 2010).

Die Legislative schreibt vor, bis Ende 2009 alle Services online anzubieten. Die e Services sind nur durch sichere Authentifikation der BürgerInnen nutzbar. Dieses ausgeweitete Angebot sollte auch zu einem vermehrten Nutzen der eID-Karte führen. Empirische

Studien zeigten jedoch, dass die Einführung der Voraussetzung zur Authentifikation darin resultierte, dass weniger spanische BürgerInnen die eServices in Anspruch nahmen. Daher setzen die meisten Services keine Authentifikation mittels eID voraus.

Einer der Hauptgründe, weshalb sich eID noch nicht durchsetzen konnte ist die Akzeptanz bei den BürgerInnen. Wesentlicher Faktoren spielen das benötigte technische Equipment, wie Kartenlesegerät, Software etc., kombiniert mit einem unterdurchschnittlichen Niveau von technischem Fachkönnen der Spanischen Bevölkerung. Umfragen zeigen, dass die Karte zwar als sicher eingestuft, jedoch nicht als „user-friendly“ und aufwändig sowie teuer in der Anschaffung gesehen wird (Heichlinger & Gallego, 2010).

4.1.6.2 Länderbeispiel Vereinigtes Königreich

Das Vereinigte Königreich steht vor großen Hindernissen bei der Einführung von elektronischer Identität. Da die Öffentlichkeit der Idee einer Identitätskarte sehr feindlich gegenüber steht, konnte ein Identitätsdokument noch nicht realisiert werden. Die Regierung plant eine Implementierung bis 2013 und schuf im Jahr 2000 rechtliche Rahmenbedingungen durch die Verabschiedung des Electronic Communications Act 2000 (A-SIT, 2004).

4.1.6.3 Länderbeispiel Dänemark

eIDs und die Verwendung einer gemeinsamen digitalen Signatur für den öffentlichen Bereich um eine sichere Infrastruktur für den Zugang zu eGovernment Diensten aufzubauen war eines der Grundsteile der dänischen eGovernment Strategie (Wang, 2011).

Dänemark begann bereits im Jahr 2000, Initiativen zu starten, um die Verwendung von elektronischen Signaturen anzuregen. Bereits 2001 folgte ein eGovernment Projekt, welches zum Ziel hatte, den öffentlichen Sektor zu „digitalisieren“ (Europäische Union, 2011). Digitale Signatur sollte mit ausreichend hohem Sicherheitslevel BürgerInnen und Unternehmen zur Verfügung stehen um eine hohe Nutzung zu fördern und eine Basis für weitere Entwicklungen für personalisierte und transaktionsbasierte eGovernment Dienstleistungen zu schaffen (Wang, 2011). Die entsprechende eGovernment Strategie folgte im Jänner 2002 mit der Vision, digitale Technologien einzuführen um Organisationen und Arbeitsprozesse zu modernisieren und die Qualität der Services zu erhöhen (Europäische Union, 2011).

Im Februar 2003 wurde die Basistechnologie geschaffen für den Einsatz von digitalen Signaturen im öffentlichen also auch verwaltungsinternen Bereich. Ein Jahr später wurde eine neue eGovernment Strategie für 2004-2006⁸⁰ veröffentlicht, mit dem Ziel, effektive,

⁸⁰ Dokument verfügbar unter http://www.epractice.eu/files/media/media_275.pdf (Zugriff am 01.10.2011)

kundenspezifische Services für BürgerInnen und Unternehmen zu schaffen (Europäische Union, 2011).

Dänemark begann eine Reihe an Services elektronisch verfügbar zu machen und damit den BürgerInnen alle Geschäfte mit öffentlichen Behörden auch online zu ermöglichen. Weiters veröffentlichte die dänische Regierung ein Bürgerwebportal borger.dk, welches einen Überblick über persönliche Dienste in Beziehung zur öffentlichen Verwaltung schafft (Europäische Union, 2011).

Um die BürgerInnen zu einer Nutzung anzuregen, entwickelte Dänemark 2003 ein offizielles elektronisches Signaturschema (Nielsen & Meinertz, 2003) und führte NemID ein, welche den Zugang zu öffentlichen elektronischen Diensten durch sichere Identifikation ermöglichte (Europäische Union, 2011). Ziel der Einführung war, die Qualität von öffentlichen eServices für BürgerInnen und Unternehmen zu erhöhen und die Bereitstellung öffentlicher eServices so effizient und effektiv wie möglich zu gestalten (Wang, 2011).

Doch die Implementierung und der Einsatz der digitalen Signatur schritten nur langsam voran, da weder Nachfrage noch Angebot besteht. Die Regierung ist mit vielen Hindernissen konfrontiert (Nielsen & Meinertz, 2003). Eine der Hauptbarrieren war, dass Leute nur dann Vertrauen finden, wenn sie Geschäftspartner persönlich sehen und deren Identität verifizieren können. Weiters haben BürgerInnen keine Motivation, digitale Signatur nachzufragen, da diese mit einer Investition in Hardware (Smart Cards, Kartenlesegerätes) verbunden ist (Nielsen & Meinertz, 2003).

Dänemark startet weitere Initiativen um die Nutzung von eGovernment Dienstleistungen und NemID zu fördern, beispielsweise die „Digital Government Strategy for 2011-2015“. Diese sollte dazu beitragen, den öffentlichen Sektor zu digitalisieren. Um eine sichere Nutzung von eGovernment Services zu gewährleisten beschloss die Regierung am 1. November 2010, dass eGovernment Services nur mehr unter Einsatz von NemID genutzt werden können (Europäische Union, 2011).

Letzte Statistiken aus Juli 2011 zeigten, dass mittlerweile mehr als 2.9 Millionen digitale Signaturen für BürgerInnen ausgestellt wurden bei einer Gesamtbevölkerung von 5.3 Millionen BürgerInnen. Insgesamt wurden 209 Millionen Transaktionen ausgeführt (Wang, 2011).

Die Einführung der digitalen Signatur dient als Basis für Dienste, welche einer sicheren Identifikation und Authentifikation bedürfen. Dänemark ist jedoch bemüht, eine eID

einzuführen und sieht diese als Grundstein einer fortgeschrittenen Implementierung von eGovernment, in welchem der öffentliche Sektor voll integrierte und individual erreichbare Lösungen bieten kann (Wang, 2011).

Da die Nutzung der NemID nur gering ist, konnte eine eID noch nicht realisiert werden, noch wurden Pläne oder Projekte diesbezüglich angedacht (A-SIT, 2004).

4.1.6.4 Länderbeispiel Slowakei

Die slowakische Regierung ist bemüht um die Einführung von eID, steht jedoch vor einigen Hindernissen. Bereits im Mai 2002 trat ein Gesetz betreffend elektronischer Signaturen in Kraft, staatliche Behörden und Institutionen haben jedoch nach wie vor Schwierigkeiten, elektronische Signaturen zu erkennen und auszulesen. Eines der Haupthindernisse für eine vollständige Implementierung von elektronischen Signaturen liegt in der Knappheit an Software Applikationen (A-SIT, 2004).

Seit 2009 arbeitet die slowakische Regierung an einem eID Projekt, welches zum Ziel hat, eID-Karten zur Identifikation und Authentifikation innerhalb von eGovernment zu ermöglichen. Es müssen Voraussetzungen für eine Personalisierung der eID-Karten geschaffen werden und die notwendige Hardware und Software Infrastruktur geschaffen werden. Weiters gilt es, die Ausgabe der Karte zu planen, und diese an alle BürgerInnen auszugeben. Für die Verwendung von eID muss sichergestellt werden, dass elektronische Dienste für alle BürgerInnen erreichbar werden. Die Implementierung der eID soll bis 2012 abgeschlossen werden (Europäische Union, 2001).

4.1.7 Grenzüberschreitender Einsatz von eID

Von CEN/TC 224 wurde eine technische Spezifikationen erarbeitet, welche definiert, welche Anforderungen an eine europäische Bürgerkarte gestellt werden.

Die Europäische Bürgerkarte (European Citizen Card, ECC) ist eine Chipkarte, welche von einer nationalen Behörde ausgegeben wird und einen Berechtigungsnachweis enthält um folgende Leistungen zu ermöglichenden (CEN Europäisches Komitee für Normung, 2007):

- Identitätsprüfung
- Einsatz als EU-weites Reisedokument,
- Erleichterung des Zugangs zu eGovernment Dienstleistungen

Diese technische Spezifikation legt die Merkmale einer Europäischen Bürgerkarte fest.

Die Karte muss zur Überprüfung der Identität des Inhabers dienen. Dies geschieht aufgrund der Identitätsnachweise, welche auf der Karte gespeichert werden. Durch diese Karte soll ein leichter Zugang auf Informationen und Dienstleistungen öffentlicher Stellen erreicht werden, weiters es kann eine sichere Übertragung von Informationen an

öffentliche Stellen erfolgen. Dabei muss die Karte sicherheitsrechtlichen Aspekten gerecht werden, wie Schutz vor unerlaubtem Zugriff oder Missbrauch der Daten⁸¹. Die Kontaktschnittstelle⁸² kann kontaktlos oder kontaktbehaftet sein, muss jedoch den entsprechenden ISO-Normen⁸³ gerecht werden (CEN Europäisches Komitee für Normung, 2007).

So stellte beispielsweise Giesecke&Devrient auf der CeBit 2007 einen Entwurf der europäischen Bürgerkarte vor. Diese Karte ist mit einer Reisefunktion und einer eID ausgestattet und ermöglicht unterschiedlichste Formen des Einsatzes, angefangen von Interaktion mit Behörden über Transaktionen bis hin zu Online-Einkäufen. Die elektronische Bürgerkarte besitzt einen Chip, auf welchem persönliche Daten (Name, Geburtsdatum etc.) sowie ein elektronisches Foto und Fingerabdrücke gespeichert werden. Die Karte dient hierbei als Sicherheitselement und übermittelt nur notwendige Daten. Bei einem Einkauf werden die benötigten Kundendaten automatisch gesandt, bei Besuchen eines Chatrooms werden das Alter und damit die Berechtigung des Zugriffs verifiziert. So können beispielsweise Kinder und Jugendliche im Internet geschützt werden. Weiters dient die Karte als Ausweisdokument für EGovernment Dienstleistungen und kann um Funktionen wie digitale Signatur erweitert werden (Giesecke&Devrient, 2010).

4.2 eServices

Mit Hilfe einer eID kann auf eine Anzahl von Applikationen in unterschiedlichsten Bereichen in sicherem Umfeld zugegriffen werden. So wird es möglich, BürgerInnen und Unternehmen sicher in Prozesse einzubinden.

Das Dienstleistungsangebot ist breit gefächert und wird im folgenden Kapitel anhand unterschiedlicher Länderbeispiele aufgezeigt. Fokus liegt hierbei auf eGovernment Services welche einer sicheren Identifikation und Authentifizierung des Benutzers bedürfen.

Viele Länder sind bereits auf den „eGovernment-Zug“ aufgesprungen und bieten Informationen, Kommunikationsmöglichkeiten und Dienstleistungen für Ihre BürgerInnen, Unternehmen oder eigenen Institutionen an. Sieht man sich nun die Situation in unterschiedlichen Ländern an, so kann bemerkt werden, dass bereits alle Regierungen zumindest über ein Informationsportal für BürgerInnen bieten mit Informationen zur Regierung, den Ministerien und der Verwaltung.

⁸¹ siehe Kapitel 3.2.1 Sicherheit, Seite 37

⁸² siehe Kapitel 3.3.5.2 Kartenlesegerät, Seite 61

⁸³ Kontaktbehaftete Schnittstellen siehe ISO/IEC 7816, kontaktlose Schnittstellen siehe ISO/IEC 14443

4.2.1 Good-Practice

Im Folgenden werden zwei Länderbeispiele präsentiert, welche als Good-Practice⁸⁴ herangezogen werden können.

4.2.1.1 Länderbeispiel Island

Island war das erste Land, das weltweit digitalisiert wurde. Bereits im Jahr 1996 wurde die erste Strategie für die Entwicklung eines eGovernments veröffentlicht. Bis heute konnte Island eine Reihe von Dienstleistungen elektronisch realisieren und zählt heute zu den Ländern in Europa, welche die höchste Nutzung von elektronischen Dienstleistungen hat (Europäische Union, 2011). Zolldeklarationen werden in Island beispielsweise ausschließlich elektronisch angenommen. Die Website der Zollbehörde ist sehr userfreundlich gestaltet und bietet die Möglichkeit, die Schrittgröße oder Farben zu ändern (Capgemini, 2007).

4.2.1.2 Länderbeispiel Finnland

Laut einer Studie der Europäischen Kommission (Veröffentlichung November 2009) über eGovernment Angebote in den EU-Mitgliedsstaaten liegt Finnland an der Spitze der Länder beim Angebot guter eGovernment Dienstleistungen. Mit einem gesamtheitliche Angebot und Online- Verfügbarkeit von eServices steht Finnland an siebenter Stelle unter allen Europäischen Ländern (Capgemini, 2010).

In Finnland gibt es bereits seit 2002 eine Reihe an eServices und verschiedene Ministerien bieten Online-Informationen und –Dienstleistungen an.

So bieten beispielsweise die nationale Sozialversicherung, verschiedene Ministerien, oder die Steuerbehörde eine große Anzahl an Applikationen und elektronischer Formulare (eFormulare) (European Communities, 2007).

Im Jänner 2010 veröffentlichte das Public Management Department des Finanzministeriums den „SADe Services and Project Report 2009⁸⁵“, eine Studie welche 282 webbasierte Dienstleistungen analysierte. Die Studie zeigt, dass die Nutzung von Dienstleistungen seit der Studie 2008 zugenommen hat. Eine Ausnahme bilden Dienstleistungen, welche die Verwendung von ePayment erfordern. Die Verwendung von elektronischer Bezahlung bleibt gering. Die Verwendung der Dienste der

⁸⁴ Good-Practice Beispiele zeigen praktisch erfolgreiche Verfahren oder Lösungen in einer Gesamtschau. Diese müssen nicht Best-Practice sein, sind jedoch erfolgreiche und anerkannte Lösungen welche bestehenden Leitbildern, Zielen und anerkannten Werten entsprechen (Krems, 2011).

⁸⁵ Dokument verfügbar unter

http://www.vm.fi/vm/en/04_publications_and_documents/01_publications/04_public_management/2010_0107SADeSe/name.jsp (Zugriff am 01.10.2011)

Sozialversicherung und Steuerbehörde nehmen jedoch zu (Denmark Ministry of Finance, 2010). Finnland machte sich zum Ziel, alle wichtigen öffentlichen Dienstleistungen für BürgerInnen und Unternehmen bis 2013 ganzheitlich elektronisch zur Verfügung zu stellen.

4.2.2 Die gebräuchlichsten eServices

Cap Gemini hat im Auftrag der Europäischen Kommission die zwanzig am meist gebräuchlichen eGovernment Dienstleistungen herausgefiltert und an Hand der Entwicklungsstufen⁸⁶ treisirogetak (Capgemini, 2007). Die Ergebnisse werden in Tabelle 5: Die 20 am meist gebräuchlichen eGovernment Dienstleistungen präsentiert.

Tabelle 5: Die 20 am meist gebräuchlichen eGovernment Dienstleistungen (Capgemini, 2007)

Public Service	Max. Maturity Level Found
Income Tax Declaration	5
Social Security Benefits	5
ID Documents (passports, driver's license etc.)	5
Public Libraries	5
Data Submission To Statistical Offices	5
Environment-Related Permits	5
Car Registration	4
Buliding Permit	4
Certificates	4
Job Search Services	4
Enrolment In Higher Education	4
Announcement of Moving	4
Health-Related Services	4
Social Contirbutions For Employees	4
Corporate Tax Declaration	4
Value Added Tax Declaration	4
Registration Of A New Company	4
Customs Declaration	4
Public Procurement	4
Declaration to Police	3

Im Folgenden werden exemplarisch einige dieser eServices anhand unterschiedlicher Länderbeispiele vorgestellt.

⁸⁶ siehe Kapitel 2.1.2 Grundlagen und Charakteristika, Seite 8

4.2.2.1 eTax

Das am meist genutzte eService ist die elektronische Einreichung der Steuererklärungen (eTax).

Länderbeispiel Estland

Auch in Estland ist die meist genutzte elektronische Dienstleistung die eTax Applikation. Die Authentifizierung findet über die ID Karte oder die mobile eID statt. Weiters gibt es die Möglichkeit, sich über PKI Zertifikate von Banken einzuloggen.

Die Verwendung von eID in Zusammenhang mit der Dienstleistung der Steuerbehörde ist in Abbildung 22: Nutzung von eID-Karten und mobiler eID für eTax Services sichtbar. Hier wird deutlich, dass der Einsatz von eID und die Nutzung von eServices kontinuierlich steigen (Martens T. , Electronic Identity management in Estonia between market and state governance, 2010).

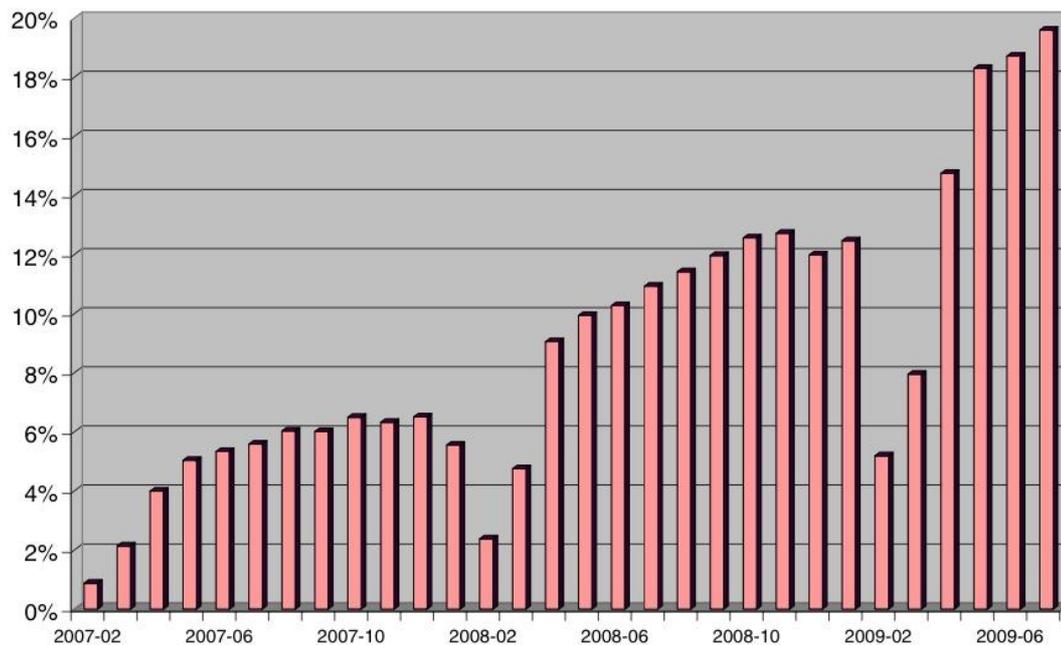


Abbildung 22: Nutzung von eID-Karten und mobiler eID für eTax Services (Martens T. , Electronic Identity management in Estonia between market and state governance, 2010)

Länderbeispiel Belgien

Bereits im April 2003 wurde es ermöglicht, erste Dienstleistungen online zu nutzen, wie beispielsweise Tax-on-Web, eine Applikation zur online Abgabe von Steuererklärungen (eTax).

Das Angebot von Dienstleistungen auf Tax-on-Web⁸⁷ wurde 2007 erweitert, um die BürgerInnen in der Abgabe der Steuererklärung zu unterstützen (Europäische Union, 2010). Es umfasst eine Berechnung der Einkommenssteuer, eine Abzeichnung und Sicherung der Daten online, eine elektronische Übermittlung der Formulare sowie den Erhalt einer Übermittlungsbestätigung seitens der Steuerbehörde. Benutzer können weiters die Historie der gesandten Steuerbescheide einsehen und den Verlauf der Rückzahlungen betrachten.

Im Juli 2009 füllten bereits über 1.7 Millionen Belgier ihre Steuererklärung über Tax-on-Web aus. Im Vergleich zum Vorjahr bedeutet dies einen Anstieg von 700.000 mehr Online-Anträgen (Europäische Union, 2009).

Länderbeispiel Island

In Island füllen bereits 90 Prozent der BürgerInnen die Einkommenssteuererklärung elektronisch über die Seite www.skattur.is aus (eTax). Dafür erhalten Steuerzahler/innen eine ID und Passwort für die Anmeldung. Ein Pilotprojekt für den Einsatz von digitalen Identitäten wurde bereits gestartet (Capgemini, 2007).

Länderbeispiel Finnland

Das Service der Steuerbehörde bietet BürgerInnen und Unternehmen die Möglichkeit, Steuerinformationen elektronisch zu versenden. Dieses Service ist das am meist verwendetest in Finnland und breites 120.000 Nutzer machen Gebrauch davon (European Communities, 2007).

Länderbeispiel Niederlande

Im September 2009 kündigte die Europäische Kommission die Auszeichnung von eGovernment Dienstleistungen an, welche als Good Practice Beispiel präsentiert werden. Als besonders gut hervorgehoben wurde „IR Service On-Line“, eine Plattform, welche es SteuerzahlerInnen und –beraterInnen eine große Anzahl an Services bietet.

Länderbeispiel Tschechien

Alle Arten von Steuererklärungen können über das Portal <http://adis.mfcr.cz/adis/jepo> gesandt werden. Dieses Service wurde 2003 eingeführt und wurde zuerst nur für bestimmte Steuererklärungen entwickelt. Mittlerweile wurde der Service auf alle Sparten ausgedehnt. Insgesamt wurden bereits 138.558 eFormulare mit elektronischer Signatur übermittelt (Europäische Kommission, 2011).

⁸⁷ Tax-on-Web unter <http://ccff02.minfin.fgov.be/taxonweb/app/citizen/public/taxbox/home.do> (Zugriff am 01.10.2011)

4.2.2.2 eVoting

In einigen Ländern ist es bereits möglich, elektronisch an Wahlen teilzunehmen.

Länderbeispiel Schweiz

Ein sehr positives Beispiel ist die Schweiz, welche die ersten Prototypen in Genf im Jänner 2003 testete, gefolgt von Cologny im November 2003, Carouge im April 2004 und Meyrin im Juni 2004. Die Beteiligung an den elektronischen Wahlen (eVoting) übertraf alle Erwartungen. Im November 2004 wählen acht Gemeinden in Geneva zum zweiten Mal über das Internet. Es wurden keine sicherheitsrelevanten oder technischen Probleme verzeichnet. Die Wähler erhielten eine Karte mit einem einmaligen ID-Schlüssel sowie einer PIN, welche eine sichere Anmeldung in einer virtuellen Stimmzettel-Box möglich machten. Insgesamt wählten 22 Prozent der Teilnehmer über das Internet (Treasury Board of Canada Secretariat, 2004).

Länderbeispiel Belgien

Im Mai 2003 war es erstmalig möglich, an Wahlen auch in elektronischer Form teilzunehmen. Bereits 3.2 Millionen BürgerInnen und damit 44 Prozent der Wahlberechtigten, gaben ihre Stimme elektronisch ab (Europäische Union, 2011).

Länderbeispiel Portugal

Auch Portugal startete eine große Anzahl an Projekten für elektronische Wahlen (eVoting). Das erste Projekt wurde 2004 während der Europäischen Wahlen ins Leben gerufen und beinhaltete das Testen drei verschiedener Technologien, eingeschlossen 150.000 Wähler, angewandt in neun Gemeinden. Im Jahr 2005 wurden diese Wahl-Plattformen verbessert, um sie für Parlamentswahlen einsetzen zu können. Auch BürgerInnen, welche sich im Ausland aufhielten, war es möglich, an diesen Wahlen teilzunehmen. Insgesamt nahmen 4.500 Personen von 38 Ländern an den Wahlen teil. Beide dieser Projekte waren nicht bindend sondern wurden für Studien eingesetzt, welche als sehr positiv bewertet wurden (Dias & Menéndez, 2007).

Länderbeispiel Estland

Während der Gemeindewahlen in Estland im Oktober 2005 war es möglich, auch online seine Stimme abzugeben. Um dies zu ermöglichen, wurde der legislative Rahmen bereits 2002 geschaffen, 2003 folgte dann der Startschuss für die Entwicklung eines eVoting Systems. Das elektronische Wählen wurde durch den Einsatz der eID-Karten möglich. Genau 9.317 Wähler machten Gebrauch von diesem System (insgesamt besaßen 850.000 Wahlteilnehmer zu diesem Zeitpunkt bereits die ID-Karte) und wählten elektronisch, 9287 Stimmen waren gültig (Martens T. , Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications - National Profile Estonia, 2007). Seit der Einführung im Oktober 2005 stieg die Anzahl der „eVoter“ gradual an, im Oktober 2009

betrug der Anteil an elektronischen Wähler 15 Prozent - über 100.000 BürgerInnen entscheiden sich für eine elektronische Stimmabgabe (Europäische Kommission, 2009).

4.2.3 Neue eServices

4.2.3.1 Antrag auf Pensionsförderungen

Ein neues eService in Belgien seit März 2011 ist „Demand de Pension“⁸⁸, über welches Angestellte online eine Pensionsförderung anmelden können. Dieses Service bedarf dem Einsatz einer eID-Karte mit entsprechendem Kartenlesegerät (Europäische Union, 2011).

4.2.3.2 Online Jobsuche

Seit April 2007 ist es für junge Arbeitssuchende in Belgien möglich, sich mittels eID-Karte online für eine „first job card“ des nationalen Arbeitsamtes zu registrieren. Der Besitz einer solchen „first job card“ berechtigt zu einem „initial employment contract“ (CPE),⁸⁹ welcher den Arbeitssuchenden ermöglicht, leichter einen Job zu finden (Europäische Union, 2011).

4.2.3.3 Meldung von Polizeidelikten

Im Juni 2007 wurde das Police-on-Web⁹⁰ Service online genommen, welches belgischen BürgerInnen ermöglicht, Verbrechen online der Polizei zu melden. Um ein Delikt anzuzeigen, ist eine Authentifikation mittels eID erforderlich (Belgischer föderaler öffentlicher Dienst Informations- und Kommunikationstechnologie, 2011).

Auch Italien bietet dieses Service „Denuncia vi@ Web“ (Reprot a crime via the Web“ und ermöglicht den BürgerInnen, verlorene oder gestohlene Güter online einzumelden. Dieses eService soll dazu dienen, den Prozess des Ausfüllens von Delikt-Anzeigen zu vereinfachen und dieses Service rund um die Uhr anzubieten (Capgemini, 2007).

4.2.3.4 Online Bahnticket

Seit Juni 2009 ist es in Belgien möglich, die eID-Karte als gültiges Bahnticket zu nutzen. Dieses eService war das erste seiner Art in Europa. Der User kauft online ein Zugticket des nationalen Eisenbahnunternehmens SNCB⁹¹ und das Ticket wird elektronisch auf der ID-Karte gespeichert. Im Zug zeigt der/die Reisende dem/der Schaffner/in seine/ihre eID-Karte, diese wird gescannt wird das Ticket über das Lesegerät angezeigt (Europäische Union, 2011).

⁸⁸ siehe <http://www.demanddepension.be> (Zugriff am 01.10.2011)

⁸⁹ Mehr Informationen unter <http://www.epractice.eu/node/281985> (Zugriff am 01.10.2011)

⁹⁰ Siehe <https://policeonweb.belgium.be/eloket/selectComplaintTypeAndAuthentication.action> (Zugriff am 01.10.2011)

⁹¹ siehe <http://www.b-rail.be/main/D/> (Zugriff am 01.10.2011)

4.2.3.5 Online Football Tickets

Im Jänner 2010 wurde eine weitere Dienstleistung in Belgien elektronisch angeboten: Online-Kauf von Football Karten. Dieses Service vereinfacht den elektronischen Kauf von Tickets für ein Football-Match und reduziert die Papierlast. Ein weiterer Vorteil liegt in der besseren Kontrolle von Fälschungen und illegalen Weiterverkäufen (Europäische Union, 2011).

4.2.3.6 DATEN BOX

Im Oktober 2009 wurde in Tschechien die Daten Box⁹² etabliert, ein Service, welches es Personen ermöglicht, die elektronische Kommunikation mit öffentlichen Behörden zu registrieren und aufzuzeichnen. Jede Daten Box ist Passwort-geschützt und nur durch eine zertifizierte elektronische Signatur zugänglich. Das System ist schnell, sicher und einfach zu bedienen und garantiert eine Authentifizierung von Sender und Empfänger von Nachrichten.

Seit 1. November 2009 ist jede Behörde und legale Person zur Aktivierung einer Daten Box verpflichtet. Im Oktober 2009 waren bereits mehr als 350.000 Daten Boxen registriert, darunter 8.000 von öffentlichen Einrichtungen und ungefähr 340.000 von legalen Personen. Auch 14.600 BürgerInnen haben sich freiwillig angemeldet. Zusammengerechnet wurden bereits 54.700 Daten Boxen aktiviert (Europäische Union, 2011).

4.2.4 Initiativen zur Förderung der Entwicklung und des Nutzens von eServices

Viele Länder konnten eine Reihe von eGovernment Dienstleistungen realisieren. Dies bedurfte jedoch der Schaffung einiger Grundlagen sowie oftmals Initiativen zur Förderung der Entwicklung.

4.2.4.1 Länderbeispiel Belgien

Belgien führte in den letzten Jahren einige Initiativen durch, um eGovernment näher an die BürgerInnen und Unternehmen zu bringen, den Zugang zu neuen Technologien zu vereinfachen, den Gebrauch zu erhöhen und interne Prozesse zu vereinfachen.

Die Federal eSociety Policy (2007-2010) hatte zum Ziel, eGovernment Dienstleistungen für alle erreichbar zu machen. So wurde 2007 das eGovernment Portal Belgium.be inhaltlich und funktionell überarbeitet und eine neue Version im Mai 2008 online gebracht (Europäische Union, 2011).

⁹² siehe <http://www.datoveschranky.info> (Zugriff am 01.10.2011)

Im Jahr 2008 führte die belgische Telecommunications Agency der Region Wallonien eine Umfrage⁹³ zu dem Nutzen von Informations- und Kommunikationstechnologien durch. Diese brachte zum Ergebnis, dass beinahe ein Drittel der Bevölkerung von Wallonien keinen Gebrauch von Internet macht. Die Ursachen darin liegen einerseits an einem fehlenden physikalischen Zugang sowie Schwierigkeiten im Umgang mit den neuen Technologien (Agence Wallonne des Télécommunication, 2009).

Als Antwort startete die belgische Regierung im Februar 2010 die Initiative „Start2surf@home“, welche zum Ziel hatte, Infrastruktur für den Zugang zu elektronischen Informationen und Dienstleistungen zu schaffen. Es wurden Computer mit Internetzugang für 100.000 Belgier zu einem reduzierten Preis bereitgestellt. Das „Star2suft@home“-Paket wird individuell an den Nutzer und seine Bedürfnisse angepasst und umfasst einen Computer, Internet, Antivirus Software sowie eine Einführung in die Welt des Computers und des Internets (Europäische Union, 2011).

Die Initiative zeigte Erfolge, während 2009 nur 64 Prozent der Haushalte über Internet Anschluss verfügte (Europäische Union, 2009), stieg die Zahl im Jahr 2010 auf 73 Prozent, 70 Prozent davon verfügten über eine Breitband-Verbindung. Auch die Anzahl der Personen, welche online mit öffentlichen Stellen interagieren verdoppelte sich seit dem Jahr 2007: Die Abfrage von Informationen führten 2010 27,8 Prozent der Personen durch, 13,8 Prozent luden Formulare herunter und 13,1 Prozent sandten ausgefüllte Formulare elektronisch an die Behörden (Europäische Union, 2011).

Um administrative Prozesse zu vereinfachen wurde im November 2009 ein neuer Strategie-Plan „Administrativ Simplification and eGovernment Plan (2010-2014)“⁹⁴ für 2010 bis 2014 verabschiedet. Dieser Plan sieht vor, bis 2012 ungefähr 25 Prozent der administrativen Belastung zu reduzieren, mit gleichzeitiger Minimierung der Kosten. Die Prozesse sollen durch eine Einführung von neuen technologischen Mitteln vereinfacht, harmonisiert und optimiert werden und dadurch eine einfache Verarbeitung der eFormulare erreicht werden. Dienstleistungen sollten kundenspezifischer gestaltet werden um eine Personalisierung der eFormulare zu ermöglichen (Europäische Union, 2011).

⁹³ Mehr Informationen unter <http://www.awt.be/web/dem/index.aspx?page=dem,fr,men,000,000> (Zugriff am 01.10.2011)

⁹⁴ Dokument zum Strategie-Plan verfügbar unter http://easi.wallonie.be/servlet/Repository/Strategie_du_Gouvernement_wal.PDF?IDR=9755 (Zugriff am 01.10.2011)

Im Juli 2010 wurde festgesetzt, wie die Ziele des Strategie-Planes bestmöglich bis 2014 realisierbar sind. Folgende Ziele gibt es bis 2014 zu erreichen (Europäische Union, 2011):

- Vereinfachung und Verbesserung der Rechtsvorschriften
- Vereinfachung und Verbesserung der Prozesse
- Dematerialisierung der Prozesse
- Verwaltung administrativer Dokumente durch elektronische Mittel
- Vereinfachung und Dematerialisierung von Datensammlung und –verteilung
- Verbesserung der Information und Kommunikation bezüglich öffentlicher Dienstleistungen

4.2.4.2 Länderbeispiel Malta

Malta war ebenso bemüht eine erstklassige Informationsgesellschaft zu errichten. Daher versucht die Regierung ein eGovernment in Malta einzurichten und startete eine Initiative. Die Regierung baute Beziehungen mit dem lokalen ICT Sektor auf um elektronische Dienstleistungen zu entwickeln und zu implementieren. Die IT Agency MITTS Ltd. Der Regierung wird eine Plattform zur Verfügung stellen um alle eServices einzuführen. Unterstützt durch CIMU, die Central Information Management Unit, will Malta eine eGovernment Anwendung schaffen, die weltweit unvergleichlich ist (Europäische Union, 2011).

Im Juli 2009 startete die Regierung eine Umfrage⁹⁵, welche die Zufriedenheit der BürgerInnen mit den eGovernment Angeboten evaluieren sollte. Diese Umfrage ermöglichte es BürgerInnen und Unternehmen, ihre Erfahrungen mit eGovernment zu bewerten (Europäische Union, 2011).

Die Studie ergab, dass bereits 64 Prozent der Online-User bereits Gebrauch von eGovernment Services gemacht haben. Die am meist präferierte Interaktion mit der Regierung sind Internet und eMail, gefolgt von persönlichen Besuchen. Die am meist genutzte Servicekategorie ist die Steuererklärung (eTax). Bei der Befragung nach dem Nutzen von eGovernment sehen die meisten User den Vorteil der Kosten- und Zeitersparnis (MITA, 2009).

Die Regierung sieht dieses Input als besonders wichtig um das eGovernment optimal an die Bedürfnisse der Nutzer anzupassen (Europäische Union, 2011).

⁹⁵ Studie zum Download unter <https://mygov.mt/notify/Mita%20eGov%20Online%20Surveys.pdf> (Zugriff November 2007)

Im September 2009 kündigte die Europäische Kommission die Auszeichnung von zwei eGovernment Dienstleistungen an, welche als Good Practice Beispiel präsentiert werden. Diese zwei ausgezeichneten Services sind das System für Kundenbetreuung und das viel genutzte Registrierungssystem für Fahrzeuge. Weiters als besonders gut hervorgehoben wurde „IR Service On-Line“, eine Plattform, welche es SteuerzahlerInnen und –beraterInnen eine große Anzahl an Services bietet (Europäische Union, 2011).

4.2.4.3 Länderbeispiel Island

Island war das erste Land, das weltweit digitalisiert wurde und ist seit dem stetig bemüht, das Angebot an eGovernment Informationen und Dienstleistungen zu verbessern.

Im Oktober 1996 wurde die Strategie „The Icelandic Government’s Vision of the Information Society“⁹⁶ veröffentlicht. Ziel war es, jedem/r BürgerIn zu ermöglichen, elektronische Dienste zu nutzen und Daten und Informationen mittels digitaler Signatur zu verschlüsseln.

Im Jahr 2000 wurde ein Arbeitsplan vorgestellt um eGovernment einzuführen, vermehrt Services über die Webseite der Ministerien anzubieten und Gesetze anzupassen. Ein Bericht über die Notwendigkeit der Einführung einer PKI Technologie folgte im Mai 2001. In den folgenden Jahren wurden Politische Strategien formuliert, Gesetze angepasst und Richtlinien vorgegeben, um die Entwicklung von eGovernment voranzutreiben.

Im März 2007 ging das ePortal island.is online. Island.is war eines der größten Projekte der eGovernment Strategien. Das ePortal hatte zum Ziel, einen besseren Zugang zu Informationen und Dienstleistungen zu schaffen, Kosteneinsparungen in Bezug auf den Zugang und das Angebot von Dienstleistungen zu realisieren und die Qualität der Dienstleistungen zu verbessern.

Im Bericht „i2010 Annual Information Society Report 2007“⁹⁷ der Europäischen Kommission war Island im Vergleich mit anderen Europäischen Ländern weit vorne in den untersuchten Indikatoren „connectivity“ und „citizen use“ (Europäische Union, 2011). Die Verwendung von eGovernment Dienstleistungen stieg die letzten Jahre kontinuierlich an und zählt nun zu eine der höchsten in Europa. Island hat laut Studie von Capgemini die höchste Nutzungsrate an öffentlichen eServices (Capgemini, 2010).

⁹⁶ Strategie verfügbar unter <http://www2.stjr.is/framt/vision00.htm> (Zugriff am 01.10.2011)

⁹⁷ Bericht verfügbar unter http://www.epractice.eu/files/media/media_458.pdf (Zugriff am 01.10.2011)

4.2.5 Schwierigkeiten bei der Entwicklung von eServices

4.2.5.1 Länderbeispiel Lettland

Auch Lettland war bemüht, eGovernment zu implementieren. Bereits 2000 wurden Richtlinien „Socio-Economic Programme eLatvia – Strategic Guidelines“⁹⁸ verfasst, welche darauf abzielten, die Effektivität und Wettbewerbsfähigkeit von Lettland in der globalen Wirtschaft zu verbessern (Europäische Union, 2011).

Darauf folgend adoptierte das Ministerkabinett im September 2001 eine Verordnung über die Bürgeridentitätskarte, die die Integration elektronischer Chips in die eID-Karte unterstützt. Dieser Chip soll den Namen des Inhabers, dessen Geschlecht, ein digitales Bild, eine persönliche Identifikationsnummer sowie eine elektronische Signatur enthalten. Im August 2002 wurde die Konzeption „eGovernment Conception“⁹⁹ seitens des Ministerkabinetts adoptiert, welches Strategien für eine Implementierung von eGovernment festlegte. Hauptziel war, eine bürgerorientierte, demokratische und effektive Administration zu schaffen (Europäische Union, 2011).

Im September 2004 wurde ein nationales Programm „Development and Improvement of eGovernment Infrastructure Base for 2004-2006“ gestartet, im September 2005 folgte das Programm „Latvian eGovernment Development Programme 2005-2009“¹⁰⁰ (Europäische Union, 2011).

Lettland strebte als Grundstein zur Implementierung eines eGovernments die Schaffung einer digitalen elektronischen Signaturinfrastruktur an (Palfinger, 2007).

Im Juni 2005 wurde daher eine Vereinbarung für die Einführung einer qualifizierten elektronischen Signatur getroffen (Europäische Union, 2011). Ende September 2006 wurde die elektronische Signatur durch die Latvian Post CSP implementiert (Palfinger, 2007), welche von einer Verwendung von qualifizierten Zertifikaten zur Unbestreitbarkeit ausgeht (Smite, 2007). Mit Hilfe der elektronischen Signatur wurde es BürgerInnen möglich, eServices zu nutzen.

Doch die Nutzung digitaler Signatur seitens der BürgerInnen war gering. Lettland stand vor folgenden Problemen, welche eine Einführung von eGovernment erschwerte (eUser, 2009):

- geringe Verbreitung des Internets durch hohe Zugangskosten
- Fehlen von fixen Telefonleitungen in den meisten ländlichen Gebieten

⁹⁸ Dokument verfügbar unter http://www.epractice.eu/files/media/media_384.pdf (Zugriff am 01.10.2011)

⁹⁹ Dokument verfügbar unter http://www.epractice.eu/files/media/media_346.pdf (Zugriff am 01.10.2011)

¹⁰⁰ Dokument verfügbar unter http://www.rapl.gov.lv/uploads/filedir/Angliska_versijaElectronic%20Government%20Development%20Programme%20for%202005-2009_EN.doc (Zugriff am 01.10.2011)

- Fehlen von Anwendungen von elektronischer Signatur
- kein öffentlich bekannter Access-Point, der alle existierenden öffentlichen eServices und Informationen darüber auflistet

In den letzten Jahren nahmen die Ausgaben im Bereich der Informations- und Kommunikationstechnologie zu, sowohl im öffentlichen Sektor als auch bei den privaten Unternehmungen. Weiters wurde eine Informationsgesellschaft aufgebaut und drei staatliche Projekte implementiert (Unified Information System of Municipalities, National Unified Library Information System, Education Information System). Diese Fakten unterstützen die Entwicklung des eGovernments (eUser, 2009).

Die Dienstleistungen, welche über das nationale ePortal Latvija.lv zur Verfügung stehen, werden immer häufiger genutzt, wie Verifizierung von Dokumenten oder Aufenthaltsorte von BürgerInnen. Zwischen Dezember 2008 und März 2009 ist die Anfrage für diese Services um das Vierfache gestiegen.

Auch die Anzahl der elektronischen Transaktionen nimmt jährlich zu. Im August 2009 wurden bereits 45.000 Dokumente in staatlichen Institutionen elektronisch ausgetauscht. Weiters zeigen Studien, dass immer mehr Institutionen elektronische Mittel dafür verwenden, Informationen von BürgerInnen zu gewinnen und Informationen und Daten zwischen Regierungsinstitutionen auszutauschen (eUser, 2009).

Erst im Februar 2010 wurde ein das „eID Card Concept“¹⁰¹ für die Einführungen einer nationale eID-Karte entworfen. Eine Implementierung von eID-Karten soll die Verwendung von elektronischen Signaturen und damit die Nutzung von eGovernment Dienstleistungen fördern (Europäische Union, 2011).

Mit dieser Karte können BürgerInnen identifiziert und authentifiziert werden wenn sie eServices nutzen. Sie ermöglicht eine elektronische Signierung von Dokumenten und den Zugang zu eServices. Weiters können BürgerInnen, Unternehmen und Staatsbeamte Smart Cards verwenden um Zugang zu allen staatlichen und kommerzielle elektronischen Services zu erhalten. Auch Staatsbeamte werden identifiziert wenn sie sich in Applikationen der Abteilungen einloggen. Mithilfe dieser Karte kann eine digitale Signatur an Dokumente oder Daten geknüpft werden und das Dokument dadurch gesperrt werden.

¹⁰¹ Dokument verfügbar unter <http://polsis.mk.gov.lv/view.do?id=3286> (Zugriff am 01.10.2011)

Seit Juni 2010 ist es für BenutzerInnen einer mobilen ID möglich, eGovernment Services in Anspruch zu nehmen. Auch diese Entwicklung soll dazu beitragen, die Nutzung von eGovernment Services zu verstärken (Europäische Union, 2011).

4.3 ePortale

Viele Länder bieten Ihre Dienstleistungen gebündelt über ein ePortal an. Das folgende Kapitel stellt zwei ausgewählte nationale ePortale vor, welche als plakative Beispiele für Good Practice herangezogen werden können.

4.3.1.1 *Belgium.be - Belgien*

Im November 2002 wurde das ePortal Belgium.be¹⁰² veröffentlicht, welches als neuer Eintrittspunkt für öffentliche Dienstleistungen für BürgerInnen und Unternehmen dient. Im Mai 2008 wurde eine erneuerte Version des ePortals veröffentlicht um eine höhere Qualität betreffend Inhalt und Dienstleistungen anbieten zu können (Belgischer föderaler öffentlicher Dienst, 2009).

Ein Bereich des ePortals führt zu allen vorhandenen öffentlichen Dienstleistungen, die online verfügbar sind¹⁰³. Diese eServices setzen für die sichere Kommunikation eine Benutzerauthentifikation des Users voraus. Daher muss sich der/die BürgerIn vorab registrieren¹⁰⁴. Der/die NutzerIn registriert sich mittels eID-Karte über das ePortal um seine/ihre Identität zu prüfen. Danach kann der User einen Benutzernamen und ein Passwort festlegen, weiters eine eMail-Adresse und die bevorzugte Sprache des ePortals bekanntgeben (Belgischer föderaler öffentlicher Dienst, 2009).

Das ePortal wurde im September 2009 um das ePortal My.belgium.be¹⁰⁵ ergänzt, welches registrierten Benutzern einen online Zugang zu persönlichen Dokumenten sowie verschiedenen Services der Bundesregierung ermöglicht. Auch die Registrierung für my.belgium.be erfolgt über die Funktionalitäten der eID-Karte (Europäische Union, 2011).

4.3.1.2 *IRISbox - Belgien*

Im Februar 2008 veröffentlichten sieben Gemeinden der belgischen Region Brussels-Capital die IRISbox¹⁰⁶ eService Plattform, welche den BürgerInnen ermöglicht

¹⁰² siehe <http://www.belgium.be/> (Zugriff am 01.10.2011)

¹⁰³ siehe http://www.belgium.be/fr/services_en_ligne/ (Zugriff am 01.10.2011)

¹⁰⁴ Registrierung für Online-Dienste des Portals unter <https://www.belgium.be/usermgmt/eGovUserMgmtwebapp/public/RegistrationIntro.do> (Zugriff am 01.10.2011)

¹⁰⁵ siehe <http://my.belgium.be/> (Zugriff am 01.10.2011)

¹⁰⁶ siehe http://irisbox.irisnet.be/vip/portal/intro_fr.htm (Zugriff am 01.10.2011)

elektronische Dokument und Dienstleistungen online zu beanspruchen. Für den Zugriff ist eine elektronische ID Karte und ein Kartenlesegerät kombiniert mit einer PIN-Eingabe notwendig. Die Plattform bietet eine steigende Anzahl an Services für Unternehmen und öffentliche Angestellte (Europäische Union, 2011).

4.3.1.3 Help.gv - Österreich

Das österreichische ePortal help.gv.at gilt innerhalb Europas als Vorzeigemodell und wurde mit dem eEurope-Award 2003¹⁰⁷ in der Kategorie „A better life for European Citizen“ ausgezeichnet. 2007 erhält das ePortal den zweiten Hauptpreis des „Amtsmanager 2007“¹⁰⁸ in der Kategorie „eGovernment“.

Das ePortal Help.gv.at wurde 2008 vom Bundeskanzleramt entwickelt und bietet behördenübergreifend Informationen und Dienstleistungen. Dabei geht Help.gv von unterschiedlichen Lebenssituationen aus, wie Heirat, Wohnen oder Schwangerschaft und bietet für die über 150 Themen Informationen zu Amtswegen, erforderliche Dokumente, Gebühren, Fristen sowie fertige Formulare oder Vorlagen. Zudem können unterschiedliche Verwaltungsverfahren direkt online abgewickelt werden (Bundeskanzleramt Österreich, 2011).

Das Hauptaugenmerk liegt dabei auf Übersichtlichkeit, Verständlichkeit, Konzentration auf das Wesentliche und Transparenz.

Seit Jänner 2009 besteht eine personalisierte Version von Help.gv – MyHelp.gv. Benutzer, welche eine Bürgerkarte besitzen können ihr persönliches Profil übersenden. Persönliche Daten werden sicher gespeichert und sind nur dem authentifiziertem Nutzer zugänglich. Diese Seite soll es dem/r BürgerIn einfacher machen, für ihn relevante Informationen zu finden und zu speichern. Dies geschieht beispielsweise automatisch bei Eingabe des Wohnsitzes, durch welche alle für diese Region relevanten eFormulare und Behörden aufgelistet. Weitere eServices sind eine automatische Erinnerungsfunktion, zum Beispiel wenn der Pass bald abläuft, oder die Nutzung eines eigenen Web- Mail-Dienstes (Europäische Union, 2011).

Der Zugang zu MyHelp.gv ist nur durch die eID-Karte (Bürgerkarte) möglich (Bundeskanzleramt Österreich, 2011).

¹⁰⁷ Der eEurope-Award wird von dem Europäischen Institut für öffentliche Verwaltung mit Unterstützung durch die Europäische Kommission durchgeführt, Siehe http://www.eipa.eu/eEurope_Awards/index.htm (Zugriff am 01.10.2011)

¹⁰⁸ Amtsmanager 2007 ist ein von der WKÖ, dem ORF und Kurier veranstalteter Wettbewerb, mehr Informationen siehe http://portal.wko.at/wk/format_detail.wk?AngID=1&StID=292012&DstID=0 (Zugriff am 01.10.2011)

5 Herausforderungen

Durch einen Einsatz von elektronischer Identität bei eGovernment Applikationen können viele Vorteile genutzt und Potentiale ausgeschöpft werden. Bei der Umsetzung von eID Lösungen stehen Länder jedoch vor unterschiedlichen Herausforderungen, welche es zu überwinden gibt. Das folgende Kapitel soll einen Überblick über mögliche Hindernisse bei der Einführung und Umsetzung von eID-Lösungen geben.

5.1 Rechtmäßigkeit

Eine der wichtigsten Rahmen für die Einführung digitaler Identitäten ist die Schaffung rechtlicher Grundlagen. Es müssen Änderungen an bestehenden Rechtsvorschriften vorgenommen werden. Diese Grundlagen müssen abgeändert werden, um eine Neustrukturierung überhaupt erst erschließen zu können (Schmidt, 2003).

Doch besonders im rechtlichen Bereich müssen erst Erfahrung im Umgang mit digitalen Identitäten gesammelt werden (Schweitzer, 2004). Die Schaffung einer geeigneten rechtlichen Grundlage wird zusätzlich erschwert durch das Fehlen von Präzedenzfällen, an denen sich die Rechtsprechung orientieren kann (Sallmann & Prorok, 2001).

Offene Fragen hinsichtlich der rechtlichen Rahmenbedingungen und ungeklärte juristische Aspekte können eine Implementierung von eGovernment verzögern und stellen damit ein Haupthindernis für eine Einführung dar (Mies, 2000).

5.2 Organisation, Projekt- und Veränderungsmanagement

5.2.1 Kooperation, Kommunikation und Koordination

Grundlage jeder Verwaltungsreform ist eine umfassende Kommunikation, Koordination, Kooperation¹⁰⁹ (Dridi, Pernul, & Sabol, 2001).

Bei komplexen Aufgaben ist eine regelmäßige Kommunikation zwischen und innerhalb beteiligter Institutionen unabdingbar. Durch Abstimmungen kommt es später zu geringeren Reibungsverlusten (Bertelsmann Stiftung, in Kooperation mit Booz, Allen, Hamilton, 2002).

Der Abstimmungsbedarf bei der Einführung von neuen Technologien stellt sich in einigen Bereichen als Problem dar. Möchte eine Behörde eine Dienstleistung online bereit stellen, so bedarf dies der Abstimmung mit dem behördlichen Umfeld. Diese kann eine

¹⁰⁹ siehe Kapitel 3.2.4.3 Koordination und Kooperation, Seite 45

Modernisierung verzögern oder im kritischsten Falle blockieren, beispielsweise wenn gerade andere neue Systeme eingeführt werden (Haldenwang, 2002).

In vielen Regierungen herrschen zentralistische Strukturen in welchen die Kooperationskultur zwischen Behörden und Ministerien nur schwach entwickelt sind. Auf der Reformagenda muss daher eine Dezentralisierung stehen. Reformen müssen daher auf der lokalen Ebene erfolgen, erforderlich ist jedoch eine zentralstaatliche Steuerung des Prozesses (Haldenwang, 2002).

Umstrukturierungen¹¹⁰ bestehender traditioneller Verfahrensabläufe und Kommunikationswege sind ohne Planung nicht zu bewältigen (Bundeskanzleramt, 2011). Es ist ein Projekt- und Veränderungsmanagement¹¹¹ notwendig, welches die operative Planung mit dem Personalmanagement verknüpft. Hier ist es besonders wichtig, Verantwortlichkeiten klar festzulegen und die Personalführung als zentrales Thema zu betrachten (Haldenwang, 2002).

5.2.2 Kompetenzen, Qualifizierung und Motivation

Neben der Bereitstellung der notwendigen Infrastruktur bedarf eGovernment kompetentem Personal, die Anforderungen an Qualifikation und Motivation der Mitarbeiter des öffentlichen Dienstes durch den Einsatz von neuen Technologien ansteigen werden (Haldenwang, 2002). Weiters kann durch eGovernment kann die Komplexität von Arbeitsabläufen zunehmen (Bertelsmann Stiftung, 2002).

Bei einer Reorganisation der Verwaltung und Infrastruktur wird von den Mitarbeitern hohe Flexibilität im Umgang und der Anwendung dieser neuen Technologien verlangt (Bundeskanzleramt, 2011). Dies kann zu Widerstand bei den Mitarbeitern führen (Bertelsmann Stiftung, 2002).

Um neues Fachpersonal zu werben und die Motivation bestehender Mitarbeiter zu steigern kann die Mitwirkung attraktiv gestaltet werden, beispielsweise durch Personalentwicklungskonzepte, flexible Arbeitszeiten (Haldenwang, 2002). Um Anreize zu schaffen können weiters auch Prämierungen für engagierte Mitarbeiter ausgeschrieben werden, wie Belobigungen, Vorstellung auf Webseiten oder Eigenverantwortlichkeit für Teilprojekte (Bertelsmann Stiftung, 2002).

Ebenso wichtig ist, dass Mitarbeiter sich mit den neuen Technologien und Prozessen mit entwickeln können (Kubiec, 2008). Dies kann durch entsprechenden Bildungs- und

¹¹⁰ siehe Kapitel 3.2.4.1 Umstrukturierung, Seite 44

¹¹¹ siehe Kapitel 3.2.4.2 Projekt- und Veränderungsmanagement, Seite 45

Schulungsangeboten gefördert werden (Haldenwang, 2002). Durch umfassende Qualifizierungsmaßnahmen können Mitarbeiter in der Bewältigung des Transformationsprozessen unterstützt werden (Bertelsmann Stiftung, 2002).

5.2.3 Einbindung der Politik

eGovernment erfordert Investitionen in eine technische Infrastruktur, besonders im verwaltungsinternen Bereich und betrifft die Energieversorgung, Telekommunikation und bestehende staatliche EDV-Systeme (Haldenwang, 2002).

Die Umsetzung von BundOnline2005, dem deutschen eGovernment Projekt, bedurfte einem Gesamtbudget von € 1,65 Milliarden. Neun Prozent davon wurden für Schulungen der Mitarbeiter aufgewandt. Die Ressourcen für dieses Projekt wurde von den Behörden selbst aufgebracht, da es kein Investitionsprogramm gab (Haldenwang, 2002).

Bei der Einführung von eGovernment spielt der politische Rahmen eine wichtige Rolle. Zentral hierbei ist die Einbindung der politischen Seite und der Einsatz einer starken einflussreichen Exekutive (Schedler & Proeller, New Public Management, 2006). Gelingt es, hohe Aufmerksamkeit auf eGovernment innerhalb der Politik zu lenken, kann dies einen Motor für Initiativen (OECD, 2001) oder Unterstützung in Form von Subventionen oder Förderungen bedeuten (Schedler, Summermatter, & Schmidt, Electronic Government einführen und entwickeln – Von der Idee zur Praxis, 2003).

Die Verankerung von eGovernment im politischen Prozess kann daher als weiterer kritischer Faktor gesehen werden, welcher die Entwicklung von eGovernment beschleunigen kann (Schmidt, 2003).

5.3 Infrastruktur, Technologien und Technikeinsatz

eGovernment bedeutet elektronische Kommunikation und Transaktion zwischen BürgerInnen und Verwaltung. Ziel ist es, ein „True eGovernment“¹¹² zu schaffen, welches als durchgängiges eGovernment medienbruchfreie Dienste bietet (Prorok & Sallmann, 2001). Um dies zu ermöglichen, bedarf es Infrastruktur sowohl auf Anwenderseite als auch Anbieterseite¹¹³.

Verwaltungsintern bedarf es der Einrichtung von EDV-Systemen, IKT-gestützten Arbeitsplätzen und einer Vernetzung innerhalb der Behörden und Ämter (Haldenwang, 2002). Um die Ziele einer Effizienzsteigerung und Kostenreduktion zu realisieren, müssen

¹¹² „true eGovernment“ Begriff siehe Kapitel 2.1.2.3 Interaktionsniveau, Seite 10

¹¹³ siehe Kapitel 3.2.3 Technische Entwicklung, Seite 42

Medienbrüche verhindert werden. So muss es einem Sachbearbeiter eines Dokumentes möglich sein, die rein elektronisch zu bearbeiten (Dridi & Pernul, 2002).

Um dem User zu ermöglichen, auf Informationen und Dienstleistungen zuzugreifen ist die notwendige Voraussetzung eine Verfügbarkeit der Systeme. Hier werden vor allem Herausforderungen an die Netzwerkinfrastruktur gestellt. Bei der Schaffung einer eGovernment Lösung muss darauf geachtet werden, dass die Belastung der Netzwerke möglichst gering ausfällt, da manche Regionen nur über geringe Netzwerkkapazitäten verfügen (Schweitzer, 2004).

Mängel in der der Ausstattung und staatlicher Infrastruktur stellen eine kritische Barriere für den Einsatz neuer Technologien dar. Es stellt sich die Frage nach der Ressourcenverwendung und der Ressourcenausstattung. Oft liest ein Großteil der Gelder in Personalausgaben, an Sachausgaben wird gespart. Das Ergebnis ist ein personell gut ausgestatteter Staatsapparat mit unzureichender Sachausstattung (Haldenwang, 2002).

Bei der Einbindung neuer Technologien muss darauf geachtet werden, keine Insellösungen zu schaffen. Vielmehr sollte eine Architektur entworfen werden, welche eine modulartige Erweiterbarkeit und Interoperabilität zwischen unterschiedlichen Anwendungen ermöglicht (Dridi & Pernul, 2002). Die Architektur sollte modulartig gestaltet werden, damit sie erweiterbar wird. Eine Interoperabilität ist notwendig, damit verschiedene Implementierungen bestehender oder neuer Systeme möglich sind. Dadurch kann eine Standardisierung erreicht werden (Schweitzer, 2004).

Ein gutes Beispiel für Modularität ist die digitale Signaturinfrastruktur¹¹⁴ von Lettland. Diese Infrastruktur ist konform mit EU – Standards und erweiterbar (Palfinger, 2007).

Die Entwicklung von Standards kann auch von Seiten der Regierung gefördert werden, wie am Beispiel von Belgien erkennbar ist¹¹⁵.

Um eine Verbreitung von Applikationen für den Einsatz von eID zu fördern, machte Estland die Basissoftware, welche für den Einsatz von eID notwendig ist, öffentlich zugänglich für alle Entwickler und bat diese kostenlos zum Download an (Europäische Kommission, 2005).¹¹⁶

¹¹⁴ siehe Kapitel 4.2.5.1 Länderbeispiel Lettland, Seite 111

¹¹⁵ siehe Kapitel 4.2.4.1 Länderbeispiel Belgien, Seite 107

¹¹⁶ siehe Kapitel 4.1.5.2 Länderbeispiel Estland, Seite 94

5.4 Digitale Spaltung

Für die Nutzung des eGovernment Angebotes bedarf es auch auf Nachfragerseite entsprechender Infrastruktur, wie einem Computer oder Internetzugang (Prorok & Sallmann, 2001). Neben diesen Mindestanforderungen ist für den Einsatz von eID zusätzliche Hardware oder Software notwendig, wie beispielsweise ein Träger der elektronischen Identität oder einem Kartenlesegerätes. Doch gerade im Bereich der Infrastruktur auf Nachfragerseite kommt es zu vielen Herausforderungen.

eGovernment richtet sich an alle BürgerInnen gleichermaßen, unabhängig von sozialer oder wirtschaftlicher Stellung innerhalb der Gesellschaft, Herkunft oder Eigenschaften (Nägeli, 2004). Um eine aktive Nutzung seitens der BürgerInnen zu gewährleisten, muss daher ein Zugang auf allen Ebenen zu erschwinglichen Preisen, unabhängig von Zeit und Ort möglich sein. Nur so kann der Bildung einer Zweiklassengesellschaft und somit einer „digitale Spaltung“ entgegengewirkt werden (Gisler, Einführung in die Begriffswelt des E-Governments, 2001). Dieses Ziel wird stark durch Initiativen der EU gefördert.

Der Zugang zu neuen Technologien stellt daher einen kritischen Faktor von eGovernment dar (Haldenwang, 2002). Dies umfasst sowohl soziale Hürden wie beispielsweise Analphabetismus, als auch Personen, welche Schwierigkeiten im Umgang mit neuen Technologien haben.

Daneben ist zu beachten, dass nicht alle Personen über benötigte Geräte verfügen (Dridi & Pernul, 2002). Bevölkerungsgruppen, welchen keinen Zugang zu Infrastruktur und Internet haben dürfen hier nicht außer Acht gelassen werden. eGovernment darf nicht nur besser gestellte Bevölkerungsgruppen und modernen Unternehmenssektoren zur Verfügung gestellt werden. Der individuelle Zugang zu eGovernment über heimische Computer darf nicht als Standardfall gesehen werden (Haldenwang, 2002).

Um jedoch alle Gesellschaftsschichten einzubinden, können Regierungen öffentliche Zugangsmöglichkeiten zu elektronischen Diensten schaffen, wie beispielsweise freier Internetzugang in Bibliotheken oder öffentlichen Stellen (Dridi & Pernul, 2002).

Eine weitere Möglichkeit stellte die Förderung durch die Regierung dar. In Belgien wurde die Kampagne „Start2surf@home“ zur Förderung des Einsatzes von eID im eGovernment gestartet und notwendige Hardware an die BürgerInnen ausgegeben¹¹⁷ (Europäische Union, 2011).

¹¹⁷ siehe Kapitel 4.2.4.1 Länderbeispiel Belgien, Seite 107

Damit kann der Bildung einer Zweiklassengesellschaft entgegengewirkt werden (Gisler, Einführung in die Begriffswelt des E-Governments, 2001).

Neben der Ermöglichung des Zugangs zu Informations- und Kommunikationstechnologien bedarf es auch einem entsprechenden Umgang mit diesen. In Spanien erlagen der Einsatz von eID keine Akzeptanz, da die BürgerInnen zu wenig Skills bezüglich neuer Technologien besaßen und daher keine Gebrauch von eDiensten machten¹¹⁸.

Eine ständige Aus- und Weiterbildung gilt daher als einer der Grundpfeiler der Informationsgesellschaft (Gisler, Einführung in die Begriffswelt des E-Governments, 2001). Hier kann der Staat durch Bildungs- und Schulungsmaßnahmen unterstützend wirken und entsprechende Angebote für BürgerInnen und Unternehmen zur Verfügung stellen (Haldenwang, 2002).

5.5 Akzeptanz

Die Entwicklung und der Erfolg von eGovernment hängen im Besonderen von der Akzeptanz und der Nutzung der Bevölkerung ab. In der Slowakei beispielsweise stehen die BürgerInnen einer Einführung von eID sehr feindseelig gegenüber¹¹⁹.

Die Akzeptanz von eGovernment wird durch viele Faktoren beeinflusst. Um Vertrauen zu gewinnen muss an vielen Fronten gearbeitet werden, wie technische Lösungen, Verfügbarkeit sowie Information und Schulungen. Die tatsächliche Nutzung hängt im Besonderen von der Vorhandenen Infrastruktur sowie dem Wissensstand der BürgerInnen über die Arte der Verwendung ab (Schmidt, 2003).

5.5.1 eServices

5.5.1.1 Verfügbarkeit

eGovernment Dienstleistungen werden nur in Anspruch genommen, wenn eine ständige Verfügbarkeit der Systeme gewährleistet ist (Schweitzer, 2004).

Die Verfügbarkeit umfasst jedoch auch das Vorhandensein eines breiten Dienstleistungsangebotes. Eine Studie der Mementum Research Group im Jahr 2000 ergab, dass sich BürgerInnen eine erhöhte Einbindung von traditionellen Services in elektronische Services (Momentum Research Group, 2000).

¹¹⁸ siehe Kapitel 4.1.6.1 Länderbeispiel Spanien, Seite 95

¹¹⁹ siehe Kapitel 4.1.6.4 Länderbeispiel Slowakei, Seite 98

5.5.1.2 Rasche Abwicklung

Um die Nutzung von eServices zu fördern bedarf es neben der Verfügbarkeit der Systeme ebenso kurzer Antwortzeiten auf Anfragen. Besonders rasch können Transaktionen gestaltet werden, wenn diese ohne Medienbrüche ablaufen und auf allen Stufen elektronisch erfolgen (Dridi & Pernul, 2002). Dies bedarf wiederum entsprechender Infrastruktur (Dridi & Pernul, 2002).

5.5.1.3 Bedienungsfreundlichkeit

Damit eGovernment genutzt wird, muss Bedienungsfreundlichkeit gewährleistet werden. Ein effizientes und effektives Design sowie Benutzerführung müssen bei dem Entwurf von Dienstleistungen beachtet werden. Dies lässt sich unter dem Begriff der Usability zusammenfassen, und beinhaltet folgende Aspekte (Nägeli, 2004):

- Lernbarkeit: Können Benutzer das Angebot beim ersten Versuch ohne Probleme nutzen?
- Einprägsamkeit: Können Benutzer sich bei weiteren Besuchen an die Funktionen und deren Benutzung erinnern?
- Effektivität: Können Benutzer intuitiv navigieren und Prozesse ausführen? Wird der Inhalt der einzelnen Seiten versanden? Ist das Design einheitlich und vorhersehbar?
- Effizienz: Findet der Benutzer was gesucht wird, kann das Ziel in einer vernünftigen Zeit erreicht werden?
- Zufriedenstellung: Hat der Benutzer ein gutes Gefühl wenn er diesen Dienst elektronisch nutzt? Kehrt der Benutzer zurück, um das Angebot erneut in Anspruch zu nehmen?

Das Informations- und Dienstleistungsangebot von eGovernment sollte diesen Aspekten gerecht werden (Nägeli, 2004). Spanien scheiterte im Punkt der Benutzerfreundlichkeit, da die BürgerInnen die Bedienung von eServices für zu aufwendig halten.¹²⁰

In manchen Ländern herrscht eine beinahe unhandbare Vielfalt von technischen Standards und Applikationen. Oft wird jedoch das Angebot von Information vernachlässigt. Interaktive Dienstleistungen werden ohne Erklärung oder Hilfe zur Verfügung gestellt. Höhere Qualität bei neuen Internetangeboten könnte durch höheren Informationsgehalt, eindeutige Navigation, mehr Kundenorientierung und neue Funktionalitäten wie Thesaurus oder Beschwerdemanagement erreicht werden (Elanet, 2003).

¹²⁰ siehe Kapitel 4.1.6.1 Länderbeispiel Spanien, Seite 95

Als Basis für eine kontinuierliche Verbesserung können regelmäßige Nutzerbefragung zu angebotenen Dienstleistungen, dem Design oder der Nutzerfreundlichkeit durchgeführt werden. Dies erhöht auch die Akzeptanz des Angebotes bei den BürgerInnen (Bertelsmann Stiftung, in Kooperation mit Booz, Allen, Hamilton, 2002).

Eine Studie der Mementum Research Group im Jahr 2000 zeigte auf, dass nur mehr dreizehn Prozent der BürgerInnen den persönlichen Kontakt bei Verwaltungsdienstleistungen als wichtig erachten. Dies schließt darauf zurück, dass mehr BürgerInnen Online-Dienstleistungen nutzen würden, wenn der Zugang dazu einfach und verständlich gestaltet wird (Momentum Research Group, 2000).

5.5.1.4 Vollständigkeit des Angebots

Um BürgerInnen zu einem aktiven Nutzen von eGovernment anzuregen bedarf es auch einem umfassenden Leistungsangebot, welches alle Bedürfnisse erfasst. Das Repertoire an Dienstleistungen sollte möglichst breit gefächert und groß sein, sodass Nutzer sämtliche Arbeitsschritte online durchführen können. Damit gilt ein hohes Maß an Vollständigkeit von Informationen und Dienstleistungen als kritischer Faktor für eine aktive Nutzung (Bertelsmann Stiftung, in Kooperation mit Booz, Allen, Hamilton, 2002).

Um das Prinzip des „One-Stop-Shops“ umzusetzen, sollten Plattformen alle Dienstleistungen für die häufigsten Anliegen zusammenführen (Bertelsmann Stiftung, in Kooperation mit Booz, Allen, Hamilton, 2002).

Um BürgerInnen die Vorteile von eGovernment aufzuzeigen und Ihn mit dem Angebot an Informationen und Dienstleistungen vertraut zu mache können Regierungen Kampagnen starten, wie beispielsweise Belgien¹²¹ mit dem Projekt „Welcome to e-Belgium“¹²² (Europäische Union, 2009).

5.5.1.5 Gebündeltes Angebot

Die Schaffung einer zentralen Anlaufstelle bietet Vorteile für die Verwaltung als auch den/die BürgerIn. Mit einem zentralen eGovernment Service Center kann eine ständige Neuentwicklung von bereits existierenden Lösungen verhindert werden. Dadurch wird die Zusammenarbeit zwischen Behörden enger und verbessert.

Der Nutzer profitiert von einer einheitlichen Benutzeroberfläche. Beispiel einer solchen „Service-Institution“ ist das Österreichische Help.gv¹²³ (Bertelsmann Stiftung, in Kooperation mit Booz, Allen, Hamilton, 2002).

¹²¹ siehe Kapitel 4.2.4.1 Länderbeispiel Belgien, Seite 107

¹²² siehe <http://www.welcome-to-e-belgium.be/> (Zugriff am 01.10.2011)

¹²³ siehe Kapitel 4.3.1.3 Help.gv - Österreich, Seite 114

5.5.2 Sicherheit

5.5.2.1 Vertrauen

Ein wesentlicher Faktor ist Vertrauen. Die Mementum Research Group führte im Jahr 2000 eine Studie über kritischer Faktoren hinsichtlich des Vertrauens seitens der BürgerInnen in die Regierung durch. Unter anderen kam die Studie zum Ergebnis, dass Sicherheit hier eine zentrale und kritische Variable darstellt. Durch den Beweis der Sicherheit würden mehr BürgerInnen eGovernment Dienstleistungen nutzen (Momentum Research Group, 2000).

5.5.2.2 Datenschutz und Datensicherheit

Es ist unabdingbar, dass Datenschutz und Datensicherheit gewährleistet wird (Daum & Eichhorn, 2005).

Wichtig ist, eine sichere Übertragung, Speicherung und Bearbeitung von Daten innerhalb des Transaktionsprozesses zwischen BürgerInnen und Behörden zu gewährleisten.

Die Wahrung der Datensicherheit beginnt bereits bei der Identifikation für eServices, da der Sicherheitsaspekt auch Angriffe auf Daten während des Datenaustauschs zwischen dem Träger der Identität und dem Kartenlesegerät betrifft.

Bei kontaktbehafteten Kartenlesegeräten sind Angriffe auf die Schnittstelle schwieriger, insbesondere bei Geräten mit hohem Sicherheitsstandard¹²⁴. Daher können Identifikationsdaten unverschlüsselt an die Karte übertragen werden. Bei einer kontaktlosen Schnittstelle ist dies nicht möglich, da die Daten durch die Luft übertragen und dabei missbräuchlich mitgeschnitten werden können (Rankl & Effing, 1998).

Zur Datenübertragung stehen verschiedene Verschlüsselungs- und Sicherheitstechniken zur Verfügung¹²⁵, diese müssen jedoch in ihrem Einsatz in Bezug auf das gesamtheitliche eGovernment hinterfragt werden. Nicht in jedem Fall ist die höchste und aufwändigste Sicherheitsstufe notwendig. Es muss erforscht werden, in welchem Umfeld die BürgerInnen hohe Sicherheit erwarten und welche Bereiche Daten einem hohen Schutz bedürfen (Bertelsmann Stiftung, 2002).

5.5.2.3 Security und Privacy Policies

Damit Benutzer Vertrauen in die Kommunikation mit Behörden gewinnen, muss auf ein Vorhandensein von Sicherheitstechnologien hingewiesen werden (Zumsteg, 2004).

Dafür sollten verständliche und leicht zugängliche Security und Privacy Policies formuliert werden, welche Bedenken der BürgerInnen über Datenmissbrauch auszuräumen. Dies gilt

¹²⁴ siehe Klassifikation von Kartenlesegeräten, Kapitel 3.3.5.2 Kartenlesegerät, Seite 61

¹²⁵ siehe Kapitel 3.3.2 Verschlüsselung, Seite 47

hauptsächlich für den Datenmissbrauch seitens der Behörde, wie beispielsweise Steuerfahndung oder Strafverfolgung (Bertelsmann Stiftung, 2002).

5.5.3 Beispiel eVoting

Ein interessantes Beispiel für die Herausforderungen bei der Implementierung von eGovernment Dienstleistungen bietet die Abgabe von elektronischen Stimmen bei Wahlen. Hier kommt es zu einer kritischen Situation: Einerseits müssen Teilnehmer eindeutig identifiziert und seine Wahlberechtigung überprüft werden, andererseits muss die Stimmabgabe anonym erfolgen und geheim gehalten werden.

Damit der/die BürgerIn an Wahlen elektronisch teilnimmt, muss Vertrauen in den Wahlvorgang geschaffen werden. Dies kann durch Transparenz und Überprüfbarkeit des Wahlverfahrens gewährleistet werden.

Wichtig ist ebenso die Verfügbarkeit des Wahlsystems. Ein Ausfall würde zur Folge haben, dass alle Bestrebungen bezüglich der vermehrten Nutzung zu Nichte gemacht werden.

Gerade in diesem heiklen Bereich ist es von großer Bedeutung, das Vertrauen der BürgerInnen beim eVoting nicht zu enttäuschen (Karger & Rüss, 2003).

6 Zusammenfassung und Ausblick

Der Begriff eGovernment bezeichnet den elektronischen Austausch von Informationen, das elektronische Angebot von Dienstleistungen sowie die elektronische Transaktion zwischen Regierung, BürgerInnen und Organisationen (Bundeskanzleramt, 2011). eGovernment versucht mit Hilfe von neuen Innovations- und Kommunikationstechnologien einen papierlosen elektronischen Verkehr zwischen BürgerInnen und Behörde umzusetzen (Kahl & Weber, 2008).

Neue Medien bieten eine Chance für vielschichtige Weiterentwicklung der Demokratie. Zahlreiche Akteure nutzen das Internet zur Kommunikation, Koordination und Vernetzung, als Plattform für Öffentlichkeitsarbeit, Mitgliederwerbung oder Fundraising. Unter dem Dach der eDemokratie entsteht dadurch eine neue Möglichkeit der Teilnahme an Prozessen (Bertelsmann Stiftung, 2002).

Durch eGovernment wird es möglich, Dienstleistungen näher an die BürgerInnen zu bringen. Informationen, Produkte und Dienstleistungen können einer breiten Öffentlichkeit zugänglich gemacht und überall und zu jeder Zeit erbracht werden.

Transaktionen werden durch online-Einbindung effizienter und die Interaktion wird transparenter, komfortabler und kostengünstiger.

Sieht man sich nun die Situation in unterschiedlichen Ländern an, so kann festgehalten werden, dass bereits alle Regierungen zumindest über ein Informationsportal verfügen, bei dem sich die BürgerInnen über Regierung, Ministerien und Verwaltung informieren können. Viele Länder bieten jedoch auch schon Interaktionsmöglichkeiten mit einzelnen Behörden oder Institutionen, beispielsweise der Steuerbehörde oder der Sozialversicherung an.

Um eine Nutzung von eGovernment Dienstleistungen anzuregen, bedarf es der Akzeptanz auf der Anwenderseite. Ein wesentlicher Faktor ist Vertrauen.

Eine Studie von TNS Emnid zeigte auf, dass BürgerInnen das Internet für zu unsicher halten, um damit online Dienstleistungen durch zu führen: Das Haupthindernis stellt die oft notwendige Übermittlung von persönlichen Daten dar.

Bedingung für die Bildung von Vertrauen ist die Schaffung und Durchsetzung rechtlicher Rahmenbedingungen. Auch die Sicherheit der Netze sowie die Gewährleistung von Datensicherheit und Datenschutz sind von besonderer Bedeutung für die Akzeptanz (Gisler, Einführung in die Begriffswelt des E-Governments, 2001).

Integrität, Authentizität, Verbindlichkeit und Vertraulichkeit spielen eine wichtige Rolle und die Erreichung dieser Ziele ist unverzichtbar für den Erfolg von eGovernment (Zumsteg, 2004).

In diesem Bereich bildet das Konzept der elektronischen Identität das Herzstück von eGovernment. Durch eID ist ein sicherer und eindeutiger Nachweis der Identität gewährleistet (Krüger, 2009). Weiters kann durch eindeutige Identifikation und Authentifizierung ein sicherer Zugang zu Dienstleistungen und Informationen gewährleistet werden. Durch die Ergänzung einer elektronischen Signatur ist es auch möglich, Daten verschlüsselt zu übertragen und Dokumente digital zu signieren. eID schafft damit Authentizität, Vertraulichkeit und Integrität und kann somit als Enabler für sichere und damit erfolgreiche eGovernment Applikationen gesehen werden.

Eine erfolgreiche Implementierung von eID bedarf weiters einem engen Zusammenspiel von Technik, Recht, Organisation und Gesellschaft. Vorab muss eine rechtliche Grundlage geschaffen werden sowie der Einsatz neuer Systeme durch verwaltungsinterne Umstrukturierungen ermöglicht werden. Das Projekt muss gut koordiniert sein und kann nur durch Kommunikation und Kooperation zwischen Behörden ermöglicht werden.

Weiters bedarf der Einbindung von eID-Lösungen in eGovernment hoher Investitionen in Infrastruktur, sowohl auf Anbieterseite als auch auf der Anwenderseite. Eine mögliche Lösung wäre die Einbindung der Politik, da diese oft Initiator von Förderprogrammen oder Subventionen ist.

Doch die Schaffung von Rahmenbedingungen und eine Implementierung einer eID-Lösung ist noch kein Garant für eine intensive Nutzung des Angebots.

Um den Einsatz von eID im Rahmen von eGovernment zu fördern startete die EU eine Reihe von Initiativen. Es wurden Richtlinien festgesetzt, um die Schaffung von Rahmenbedingungen für einen erfolgreichen Einsatz voranzutreiben und die Länder in der Etablierung von eID-Lösungen zu unterstützen. Die Verwendung von eServices wird beworben und der private und öffentliche Bereich dazu angeregt die Vorteile des eGovernments in Anspruch zu nehmen und zu nutzen.

Auch auf Anwenderseite bedarf es eines Zugangs und entsprechender Infrastruktur um eServices nutzen zu können. Diese ist oft nicht verfügbar. Hier gilt es darauf zu achten, dass die Schaffung von eGovernment keine digitale Spaltung erzeugt, sondern alle Bevölkerungsschichten unabhängig von Zeit und Ort, auf allen Ebenen und zu erschwinglichen Preisen mit einzubinden.

eGovernment muss als partizipativer Prozess angesehen werden. Um den Erfolg von eGovernment zu fördern, bedarf es einer engen Partnerschaft von Regierung, BürgerInnen und dem Privatsektor. eGovernment sollte sich an den Wünschen und Bedürfnissen der BürgerInnen orientieren und diese in den Mittelpunkt rücken. Um eGovernment jedoch erfolgreich zu verwirklichen, darf nicht vergessen werden, auch Politik und Verwaltungsspitzen mit einzubinden. Hindernisse, wie Widerstände durch Führungskräfte und Mitarbeiterinnen, sollten durch Aufklärungsarbeit vermieden werden.

Länder starteten Initiativen und entwickelten Strategien für eine Förderung des Einsatzes von eServices unter Verwendung elektronischer Ausweise.

Viele Länder haben bereits Gesetze und Richtlinien adaptiert, jedoch fehlen in einigen nach wie vor die gesetzlichen Grundlagen wie etwa elektronische Kommunikation oder die Anerkennung digitaler Signaturen. In weiteren Ländern sind entsprechende Gesetze in Bearbeitung jedoch noch nicht verabschiedet worden (Martens & Felder, 2003).

Die Vision ist ein grenzüberschreitender Einsatz der elektronischen Identität sowie die internationale Nutzung von elektronischen Dienstleistungen. Um eine national und grenzüberschreitende Interoperabilität von Anwendungen zu ermöglichen und zu unterstützen, ist die Europäische Kommission bemüht, Standardisierungsmaßnahmen voranzutreiben. So wurden beispielsweise EU Initiativen gestartet, um die Aktivität der Standardisierung und Harmonisierung auf technischer Seite voranzutreiben.

Finnland adoptierte als erstes europäisches Land ein Gesetz und gab bereits 1999 die ersten eID-Karten aus. Belgien startete eine Kampagne, um den BürgerInnen die Vorteile von eGovernment aufzuzeigen und gab während eines Aktionstages eine geführte Tour durch das virtuelle Belgien. Zugleich gab Belgien ein verbilligtes Startpaket an die BürgerInnen aus, um sie mit der notwendigen Infrastruktur wie einem Computer oder einem Kartenlesegerät auszustatten. Dänemark entwickelte ein elektronisches Signaturschema und gibt Zertifikate frei an BürgerInnen aus.

Viele Länder haben mittlerweile Konzepte entwickelt, um durch den Einsatz elektronischer Identitäten einen höheren Sicherheitsstandard gewährleisten zu können. Auf europäischer Ebene existiert bereits eine Unzahl an eID Konzepten, von der Verwendung von Username und Passwort über rein softwarebasierter Zertifikate bis hin zu Smart Cards oder mobiler Lösungen.

EU Mitgliedsstaaten wie Belgien, Italien, Estland oder Spanien haben bereits eID-Karten ausgegeben, andere Länder planen die Einführung der Karten.

Aufgrund der immer mehr zunehmenden Verbreitung von elektronischen Ausweisen und der Adoption elektronischer Signaturen in der Administration kann angenommen werden, dass die Nachfrage nach elektronischen Services zunehmen wird.

Letztendlich hängt der Erfolg von eGovernment vom Vertrauen der BürgerInnen in die Dienstleistungen ab. Es gilt daher, entsprechende Rahmen zu schaffen, Hindernisse zu überwinden und eine Distribution und Nutzung von Dienstleistungen unter Einsatz von eID zu fördern. Nur wenn die Kommunikation und Transaktion von Daten zwischen BürgerInnen und Behörden schnell, einfach und sicher abläuft, werden BürgerInnen die Abwicklung über elektronische Medien der traditionellen Methode bevorzugen. eID kann dafür einen wesentlichen Beitrag leisten.

ANHANG

Anhang A: Literaturverzeichnis

Agence Wallonne des Télécommunication. (2009). *Usages TIC 2008 des citoyens wallons*. Wallons.

Alighierei, G. (2002). *Global E-Government Web-Services*. Zürich: Diplomarbeit, angefertigt am Insitut für Informatik der Universität Zürich.

Andersson, H., Bylund, M., Olsson, A. R., Olsson, O., Seipel, P., & Sjödin, G. (kein Datum). *Dept of IT, MES College of Engineering, Kuttippuram*. Abgerufen am 15. September 2011 von <http://220.227.128.112/downloads/CriticalPerspectives/Reading%20Material%20CPT-S7/Survey%20of%20Privacy%20and%20Information%20Technology.pdf>

A-SIT. (2004). *Survey on EU's Electronic-ID Solutions* (1.0 Ausg.). Graz.

Basu, S. (März 2004). E-Government and Developing Countries: An Overview. *International Review of Law Computers & Technology* (Volume 18, No 1), S. 109-132.

Belgischer föderaler öffentlicher Dienst Informations- und Kommunikationstechnologie. (2011). *Police-on-Web*. Abgerufen am 02. Oktober 2011 von <https://policeonweb.belgium.be/eloket/selectComplaintTypeAndAuthentication.action>

Belgischer föderaler öffentlicher Dienst. (2009). *Registrierung auf dem Portal*. Abgerufen am 01. Oktober 2011 von Portal Belgium.be: <https://www.belgium.be/usermgmt/eGovUserMgmtwebapp/public/RegistrationIntro.do>

Bernold, R. (Januar 2011). Digitale Identitäten als Grundstein des Vertrauens im Internet. (R. Riedl, Hrsg.) *Fachzeitschrift eGov Präsenz* (Digitale Identitäten), S. 6.

Bernold, R. (Januar 2011). eGov Fokus SuisseID in der öffentlichen Verwaltung -Fazit und Ausblick zur SuisseID. *Fachzeitschrift "eGov Präsenz"* (1), S. 34-35.

Bertelsmann Stiftung. (2002). *Balanced E-Government*. Gütersloh: Verlag Bertelsmann Stiftung.

Bertelsmann Stiftung, in Kooperation mit Booz, Allen, Hamilton. (2002). *Balanced E-Government*. Gütersloh: Verlag Bertelsmann Stiftung.

Biham, E., Dunkelman, O., Keller, N., & Shamir, A. (2011). *New Data-Efficient Attacks on 6-Round IDEA* (2011/417 Ausg.).

Buchsbaum, T. M. (20. Oktober 2004). *Bundesministerium für Inneres*. Abgerufen am 15. September 2011 von http://www.bmi.gv.at/cms/BMI_wahlen/wahlrecht/files/Bericht_UAG_3_Internationales.pdf

Bundesamt für Sicherheit in der Informationstechnik. (2011). *Anforderungen an Chipkartenleser mit nPA Unterstützung* (1.2 Ausg.). Bonn.

Bundesamt für Sicherheit in der Informationstechnik. (2006). *Das E-Government-Glossar*. In *E-Government-Handbuch*. Bonn: Bundesanzeiger Verlag.

Bundesamt für Sicherheit in der Informationstechnik. (2009). *eCards mit kontaktloser Schnittstelle als sichere Signaturerstellungseinheit* (1.0 Ausg.). Bonn.

Bundesamt für Sicherheit in der Informationstechnik. (2006). *Grundlagen der elektronischen Signatur*. Bonn.

Bundesamt für Sicherheit in der Informationstechnik. (2011). *Technische Richtlinie TR-03127 - Architektur elektronischer Personalausweis und elektronischer Aufenthaltstitel* (1.14 Ausg.). Bonn.

Bundeskanzleramt. (2011). *Digitales Österreich*. (Bundeskanzleramt, Herausgeber) Abgerufen am 10. September 2011 von <http://www.digitales.oesterreich.gv.at/site/5226/default.aspx>

Bundeskanzleramt Österreich. (01. Jänner 2011). *Was ist HELP?* (Bundeskanzleramt, Herausgeber) Abgerufen am 05. Oktober 2011 von help.gv.at:https://www.help.gv.at/Portal.Node/hlpd/public/content/impressum/Seite.732000.html

Bundesministerium für Inneres. (01. April 2010). *Die Beauftragte der Bundesregierung für Informationstechnik*. (B. d. Innern, Herausgeber) Abgerufen am 2011 von Die Beauftragte der Bundesregierung für Informationstechnik: http://www.cio.bund.de/DE/E-Government/e-government_node.html

Bürge, U. (2002). *Digitale Identität und eID-Karte ,Das Projekt einer schweizerischen elektronischen Identitätskarte*. Bundesamt für Justiz, Bern.

Capgemini. (2010). *Digitizing Public Services in Europe: Putting ambition into action*. 9th Benchmark Measurement.

Capgemini. (2007). *The User Challenge Benchmarking the Supply of Online Public Services - 7th Measurement*.

CEN Europäisches Komitee für Normung. (2007). *Identifikationskartensysteme - Europäische Bürgerkarte*. Brüssel.

Commission of the European Communities. (2006). *i2010 eGovernment Action Plan: Accelerating eGovernment in Europe for the Benefit of All*. Brüssel.

Cryptas it-Security GmbH. (2011). *Cryptoshop*. Abgerufen am 29. September 2011 von <http://www.cryptoshop.com/index.php>

DATAKOM. (2011). *Wissens-Portal ITwissen.info*. (DATAKOM-BuchverlagGmbH, Herausgeber) Abgerufen am 15. September 2011 von ITwissen.info: <http://www.itwissen.info/>

Daum, R., & Eichhorn, P. (2005). Neue Formen der Kooperation durch Electronic Government. In S. Klewitz-Hommelsen, & B. Hinrich, *Die Zeit nach dem E-Government* (1. Ausg.). Münster: LIT Verlag.

Denmark Ministry of Finance. (2010). *SADe Services and Project Report 2009* (Bd. Ministry of Finance publications 3/2010). Ministry of Finance.

Dietrich, D. (2004). *Securing Web Services in a User-To-Application Model based on Certificate Private Extensions and Smartcard Technology*. März.

Donath, B. (März 2009). Mehr Sicherheit in der elektronischen Welt - Was bedeuten elektronische Identitäten für die Alltagsorganisation des Bürgers? *Science Allemagne*, S. 7-9.

Dridi, F., & Pernul, G. (2002). Electronic Government. *Essener Unikate* (18), S. 33-43.

Dridi, F., Pernul, G., & Sabol, T. (2001). The Webocracy Project: Overview and Security Aspects. *Tagungsband der Arbeitskonferenz Professionelles Wissensmanagement, Erfahrungen und Visionen*. Baden-Baden.

Dumortier, J. (2004). Legal Status of Qualified Electronic Signatures in Europe. In S. Paulus, N. Pohlmann, & H. Reimer, *ISSE 2004 - Securing Electronic Business Processes* (S. 281-289). Vieweg.

Eifert, M., Schreiber, L., & Stapel-Schulz, C. (Dezember 2000). *MEDIAKomm*. (D. I. Urbanisik, Herausgeber) Abgerufen am 10. September 2011 von http://mediakomm.difu.de/index.phtml?text_id=82&language=de

Elanet. (2003). *KEeLAN - Key Elements for electronic Local Authorities' Networks*.

Europäische Kommission. (November 2008). Aktionsplan für elektronische Signaturen und die elektronische Identifizierung zur Förderung grenzübergreifender öffentlicher Dienste im Binnenmarkt.

Europäische Kommission. (2006). *E- Government-Aktionsplan im Rahmen der i 2010-Initiative: Beschleunigte Einführung elektronischer Behördendienste in Europa zum Nutzen aller*. Europäische Kommission, Brüssel.

Europäische Kommission. (22. Oktober 2004). *eEPOCH*. Abgerufen am 19. September 2011 von www.eepoch.net

Europäische Kommission. (1999). *eEurope - An Information Society for All*. Communication, European Commission, Brüssel.

Europäische Kommission. (2001). *eEurope 2002 - Auswirkungen und Prioritäten*. Brüssel.

Europäische Kommission. (2002). *eEurope 2005: Eine Informationsgesellschaft für alle - Aktionsplan*. Aktionsplan, Europäische Kommission, Brüssel.

Europäische Kommission. (2009). *eGovernment Factsheets - eGovernment in Estonia*. Europäische Kommission.

Europäische Kommission. (Juli 2005). *eID in action: Estonia*. *Synergy* (Issue 03), S. 8.

Europäische Kommission. (2007). *EUCLID : European initiative for a Citizen digital ID solution*. Abgerufen am 01. Oktober 2011 von Cordis: http://cordis.europa.eu/fetch?CALLER=PROJ_ICT_TEMP&ACTION=D&CAT=PROJ&RCN=61482

Europäische Kommission. (2010). *EUROPA 2020 - Eine Strategie für intelligentes , nachhaltiges und integratives Wachstum*. Brüssel.

Europäische Kommission. (1994). *Europe's Way to the Information Society - An Action Plan*. Brüssel.

Europäische Kommission. (14. März 2007). *FASME : Facilitating Administrative Services for Mobile Europeans*. Abgerufen am 19. September 2011 von Cordis: http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&CAT=PROJ&RCN=57450

Europäische Kommission. (2007). *Government User IDentity for Europe - creating an European standard for interoperable and secure identity management architecture for eGovernment*. Abgerufen am 01. Oktober 2011 von Cordis: http://cordis.europa.eu/search/index.cfm?fuseaction=proj.document&PJ_RCN=6526790

Europäische Kommission. (11. August 2011). *IDABC Programme*. Abgerufen am 19. September 2011 von IDABC: <http://ec.europa.eu/idabc/en/chapter/3.html>

Europäische Kommission. (2008). *Preparing Europe's digital future - i2010 Mid-Term*. Luxemburg: European Commissions Publicatios Office.

Europäische Union. (2011). *eGovernment in Austria*. eGovernment Practice Editorial Team, EUROPEAN DYNAMICS S.A.

Europäische Union. (2009). *eGovernment in Belgium*. eGovernment Practice Editorial Team, EUROPEAN DYNAMICS S.A.

Europäische Union. (2011). *eGovernment in Belgien* (14.0 Ausg.). eGovernment Practice Editorial Team, EUROPEAN DYNAMICS S.A.

Europäische Union. (2011). *eGovernment in Denmark* (14.0 Ausg.). eGovernment Practice Editorial Team, EUROPEAN DYNAMICS S.A.

Europäische Union. (2011). *eGovernment in Iceland* (9.0 Ausg.). eGovernment Practice Editorial Team, EUROPEAN DYNAMICS S.A.

Europäische Union. (2011). *eGovernment in Latvia* (14.0 Ausg.). eGovernment Practice Editorial Team, EUROPEAN DYNAMICS S.A.

Europäische Union. (2011). *eGovernment in Malta*. eGovernment Practice Editorial Team, EUROPEAN DYNAMICS S.A.

Europäische Union. (2011). *eGovernment in Netherlands* (14.0 Ausg.). eGovernment Practice Editorial Team, EUROPEAN DYNAMICS S.A.

Europäische Union. (2001). *eGovernment in Slovakia* (14 Ausg.). eGovernment Practice Editorial Team, EUROPEAN DYNAMICS S.A.

Europäische Union. (2011). *eGovernment in the Czech Republic*. eGovernment Practice Editorial Team, EUROPEAN DYNAMICS S.A.

Europäische Union. (30. Mai 2008). Electronic Identity: easy access to public services across the EU. *Pressemitteilung* . Brüssel.

Europäische Union. (09. April 2009). *ePractice - BE: Launch of awareness-raising campaign on the use of the eID card*. Abgerufen am 01. Oktober 2011 von ePractice: <http://www.epractice.eu/en/news/289408>

Europäische Union. (2010). *ePractice - eGovernment Factsheet Belgium - History*. Abgerufen am 01. Oktober 2011 von ePractice: <http://www.epractice.eu/en/document/288178>

Europäisches Parlament und Rat. (12. Juli 2002). Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation.

Europäisches Parlament und Rat. (24. Oktober 1995). Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.

Europäisches Parlament und Rat. (13. Dezember 1999). Richtlinie 1999/93/EG über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen.

European Commission. (11. Jänner 2011). *eTEN Programme*. Abgerufen am 19. September 2011 von eTEN: http://ec.europa.eu/information_society/activities/eten/index_en.htm

European Committee for Standardization. (2009). *European Committee for Standardization*. Abgerufen am 19. September 2011 von <http://www.cen.eu/cen/pages/default.aspx>

European Communities. (31. Oktober 2005). *ID documents become mandatory in the Netherlands*. Abgerufen am 02. Oktober 2011 von Liberty Security: <http://www.libertysecurity.org/article520.html>

European Communities. (2007). *Preliminary Study on Mutual Recognition of eSignatures for eGovernment applications - National Profile Finland*.

European Communities. (2009). *Study on eID Interoperability for PEGS: Update of Country Profiles*.

eUser. (2009). *The context of supply and demand of public online services in Latvia*. Abgerufen am 22. Dezember 2009 von eUser: http://www.euser-eu.org/eUSER_E-GovernmentCountryBrief.asp?CasEID=2208&CaseTitleID=1%20032

Federal Public Service for Information and Communication Technology. (2006). *E-ID Hierarchy and Certificate Profiles* (3.1 Ausg.).

Feghhi, J., Feghhi, J., & Williams, P. (1998). *Digital Certificates: Applied Internet Security*. Addison-Wesley Professional.

Finkenzeller, K. (2008). *RFID-Handbuch: Grundlagen und praktische Anwendungen von Transpondern, kontaktlosen Chipkarten und NFC* (5 Ausg.). München: Carl Hanser Verlag GmbH & CO. KG.

Finnish Population Register Centre. (01. August 2007). *By the end of July, Citizen Certificates had been issued to a total of 153,600 people*. Abgerufen am 02. Oktober 2011 von FINEID: <http://fineid.fi/default.aspx?docid=2884&site=10&id=0>

Finnish Population Register Centre. (2006). *Electronic Identity and Certificates*. Abgerufen am 02. Oktober 2011 von Population Register Centre: <http://www.vrk.fi/default.aspx?id=21>

Finnish Population Register Centre. (2011). *FAQs*. Abgerufen am 02. Oktober 2011 von fineid: <http://www.intermin.fi/vrk/fineid/home.nsf/pages/A39152E72875131CC2257054002C5BE5>

Finnish Population Register Centre. (02. November 2006). *Porvoo 10 Conference: European nations, USA and Asia meet in the Porvoo 10 Conference in Finland to discuss the future of e-services*. Abgerufen am 02. Oktober 2011 von <http://www.vrk.fi/default.aspx?site=4&docid=2935>

Finnish Population Registration Centre. (2006). *Certificates*. Abgerufen am 02. Oktober 2011 von Certificates: <http://www.vrk.fi/default.aspx?id=24>

Finnish Population Register Centre. (01. Dezember 2010). *By the end of November, Citizen Certificates had been issued to a total of 341,800 people*. Abgerufen am 02. Oktober 2011 von FINEID: <http://www.fineid.fi/default.aspx?site=10&docid=4033>

Französische Botschaft in Deutschland. (März 2009). *Die sichere digitale Identität. Science Allemagne*.

Friedrichs, S., Hart, T., & Schmidt, O. (2002). *Balanced E-Government": Visionen und Prozesse zwischen Bürgernähe und Verwaltungsmodernisierung. Das Parlament*, 39-40 (Aus Politik und Zeitgeschichte).

Friedrichs, S., Hart, T., & Weizel, C. (2002). *10-Punkte-Plan für gutes E-Government*.

Giesecke&Devrient,. (2010). *Die Europäische Bürgerkarte - mehr als ein Ausweis*. Abgerufen am 21. Februar 2010 von Giesecke&Devrient: http://www.gi-de.com/portal/page?_pageid=45,133567&_dad=portal&_schema=PORTAL

Gisler, M. (2001). Einführung in die Begriffswelt des E-Governments. In M. Gisler, & D. Spahni, *E-Government - Eine Standortbestimmung* (2 ed., pp. 13-30). Bern, Stuttgart, Wien: Haupt.

Gisler, M., & Spahni, D. (2000). *Electronic Government – Ein Überblick* (1. Ausg.). Bern: Hochschule f. Wirtschaft u. Verwaltung Bern.

Güngöz, Ö., & Seel, C. (November 2003). Die neue E-Government Generation. *Government Computing*, S. 9.

Haldenwang, C. (2002). *Electronic Government (e-government) und Entwicklung: Ansätze zur Modernisierung der öffentlichen Politik und Verwaltung*. Bonn.

Haneberg, D. (2006). *Sicherheit von Smart Card-Anwendungen*. Augsburg.

Heichlinger, A., & Gallego, P. (Dezember 2010). A new e-ID card and online authentication in Spain. *Identity in the information society* (Volume 3, Number 1), S. 43-64.

Hochschule Luzern. (2011). *eBanking - aber sicher!* Abgerufen am 29. September 2011 von https://www.ebankingabersicher.ch/index.php?option=com_content&view=article&id=134&lang=de

Hoye, N. (2008). *Digitale Identitäten im Kontext von E-Government-Anwendungen*. Hamburg: Diplomica Verlag.

Hughes, M., Imamura, T., & Maruyama, H. (2002). *Decryption Transform for XML Signature*. w3c.

Hühnlein, D., & Korte, U. (2006). *Grundlagen der elektronischen Signatur: Recht - Technik - Anwendung* (1. Ausg.). SecuMedia.

Imamura, T., Dillaway, B., & Simon, E. (2002). *W3C. W3C Recommendation, W3C*.

Informationsforum RFID. (2009). *Informationsforum RFID*. Abgerufen am 29. September 2011 von http://www.info-rfid.de/technologie/was_ist_rfid/index_ger.html

ISO. (2006). *ISO/IEC FCD 14443-4 - Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 4: Transmission protocol* (Draft International Standard Ausg.). London.

Joswig, M., & Stember, J. (2002). *E-Government und Qualitätsmanagement: Innovationen durch das Internet und Beispiele für Qualitätsoffensiven in der öffentlichen Verwaltung* (1. Ausg., Bd. Management der öffentlichen Verwaltung). Kronach, München, Bonn, Potsdam: Link/Dt. Kommunal-Verl.

Kahl, A., & Weber, K. (2008). *Allgemeines Verwaltungsrecht* (2. ed.). Wien: Facultas Universitätsverlag.

Karger, P., & Rüss, O. (2003). Sicherheit ist conditio sine qua non : Erfahrungsgeleiteter Ansatz für Online-Wahlen in Deutschland. In E. Schweighofer, T. Menzel, G. Kreuzbauer, & D. (. Liebwald, „Zwischen Rechtstheorie und e-Government: Aktuelle Fragen der Rechtsinformatik 2003 (S. 255-262). Wien: Verlag Österreich.

Knie, F. j. (Januar 2001). Ohne gegenseitiges Vertrauen würden die Zusammenarbeit und das Zusammenleben nicht möglich sein. *Fachzeitschrift "eGov Präsenz"* (1/2011), S. 24-27.

KPMG Consulting AG. (Mai 2000). *Universität St. Gallen*. (KPMG, Hrsg.) Abgerufen am 10. September 2011 von [http://www.idt.unisg.ch/org/idt/ceegov.nsf/8656d8c1c7597e52c1256c8a003aba10/1c30cd5b8649428dc1256c8c00517e85/\\$FILE/Verwaltung%20der%20Zukunft.pdf](http://www.idt.unisg.ch/org/idt/ceegov.nsf/8656d8c1c7597e52c1256c8a003aba10/1c30cd5b8649428dc1256c8c00517e85/$FILE/Verwaltung%20der%20Zukunft.pdf)

Krems, B. (20. Jänner 2011). *Gute Praxis-Beispiele ("Good Practice")*, 1.42. Abgerufen am 29. September 2011 von Online-Verwaltungslexikon: http://www.olev.de/g/good_practice.htm

Krüger, J. (März 2009). Fraunhofer-Innovationscluster "Sichere Identität - Eindeutigkeit und Unverfälschtheit in der realen und digitalen Welt". *Science Allemagne* , S. 10-11.

Kubiec, M. (2008). *Schweden als Musterland des E-Government*. Wien.

Lalive d'Epinay, M. (2002). Im Fadenkreuz von eGovernment und eGovernance: Staat und Gesellschaft vor neuen Herausforderungen. In D. Spahni, *eGovernment 2: Perspektiven und Prognosen* (S. 3-62). Bern, Stuttgart, Wien: Haupt.

Langer, J., & Roland, M. (2010). *Anwendungen und Technik von Near Field Communications (NFC)* (1. Ausg.). Berlin, Heidelberg: Springer.

Lhotka, Rockford. (29. Juni 2004). *Microsoft Developer Network*. (Microsoft Deutschland GmbH) Abgerufen am 25. September 2011 von <http://msdn.microsoft.com/de-de/library/bb978972.aspx>

Limacher, R., & Schickel, M. (2002). *Public Key Infrastructure und das Management digitaler Zertifikate*. Basel.

Liu, R. (2002). *Smart Card Betriebssysteme*. München.

Lutters, S. (2009). *Digital Identity*. Universität Paderborn.

Malek, W. (23. August 2011). Dkfm. (C. Freudenthaler, Interviewer)

Martens, M., & Felder, B. (2003). *Elektronische Signaturen im E-Government, Ausgangssituation und Handlungsmodelle für Kommunen*. Mummert Consulting AG, Hamburg.

Martens, T. (11. August 2011). eGovernment in Estonia. (C. Freudenthaler, Interviewer)

Martens, T. (2010). Electronic Identity management in Estonia between market and state governance. *Identity in the information society* (Volume 3, Number 1), S. 213-233.

Martens, T. (April 2007). *IDABC European eGovernment Services*. Abgerufen am 15. September 2011 von <http://ec.europa.eu/idabc/servlets/Doc0bb7.pdf?id=29079>

Massachusetts Institute of Technology. (24. Mai 2011). *Massachusetts Institute of Technology*. Abgerufen am 25. September 2011 von <http://web.mit.edu/kerberos/www/>

Mehlich, H. (2002). *Electronic Government. Die elektronische Verwaltungsreform. Grundlagen, Entwicklungsstand, Zukunftsperspektiven*. Wiesbaden: Gabler.

Mies, H. (2000). *e-Government: Eine Modeerscheinung oder "digitale Revolution" und Zukunft der Städte?* Chemnitz: Price Waterhouse Coopers.

MITA. (2009). *eGov Online Surveys*. Abgerufen am 05. Oktober 2011 von Mygov.mt: <https://mygov.mt/notify/Mita%20eGov%20Online%20Surveys.pdf>

Momentum Research Group. (2000). *Benchmarking the eGovernment Revolution*.

Mühlberger, G. (November 2007). eGovernment in Netherlands. (C. Freudenthaler, Interviewer)

Nägeli, T. (2004). *Design von nachhaltigen, multilingualen E-Government Portalen für alle*. Locarno.

National Institute of Standards and Technology. (1994). Digital Signature Standard (DSS). *Information Processing Standards Publications*.

Network Sorcery inc. (2011). *Network Sorcery*. Abgerufen am 29. September 2011 von <http://www.networksorcery.com>

Nielsen, J., & Meinertz, U. (März 2003). *Denmark Launches Nationwide Digital Signatures*. Abgerufen am 21. 02 2010 von Center of digital Government: <http://www.centerdigitalgov.com/international/story.php?docid=43522>

OASIS Open. (15. März 2004). *Web Services Security*. Abgerufen am 29. September 2011 von OASIS Open: <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf>

OECD. (2001). *Government of the Future*. OECD Publishing.

Organization for the Advancement of Structured Information Standards. (17. Juni 2008). *OASIS*. Von <http://www.oasis-open.org/committees/security/> abgerufen

Palfinger, H. (November 2007). eGovernment in Latvia. (C. Freudenthaler, Interviewer)

Panayiotou, A. (2004). *Electronic Governance for the Lands and Surveys Department in Cyprus*. Athen, Griechenland.

Pfitzmann, B., Waidner, M., & Pfitzmann, A. (1990). *Rechtssicherheit trotz Anonymität in offenen digitalen Systemen*.

Pohlmann, N., & Hesse, M. (März 2007). Kryptographie: Von der Geheimwissenschaft zur alltäglichen Nutzenanwendung (V) – Prüfsummen, Zertifikate und die sichere elektronische Signatur. *IT-Sicherheit & Datenschutz* (Volume 31, Nummer 3), S. 218-221.

PRIME. (2011). *PRIME*. Abgerufen am 19. September 2011 von PRIME: <https://www.prime-project.eu/>

Prorok, T., & Sallmann, R. (2001). *e-Government – Revolution der öffentlichen Verwaltung?* Wien.

Prorok, T., & Sallmann, R. (Februar 2002). E-Government; Leitfaden für Österreichs Städte und Gemeinden. 37. KDZ Managementberatungs- und WeiterbildungsGmbH.

Prosser, A., & Müller-Török, R. (2002). E-Democracy: Eine neue Qualität im demokratischen Entscheidungsprozess. *Wirtschaftsinformatik* (44. Jahrgang - Heft 6), S. 545-556.

Quade, M., & Wölfle, R. (2010). *SuisseID in der Praxis*. Basel, Schweiz: gesowip.

Rankl, W., & Effing, W. (1998). *Handbuch der Chipkarten* (3. Ausg.). München: Carl Hanser Verlag.

Riedl, R. (Januar 2011). Mehr Vertrauen tut not! *Fachzeitschrift "eGov Präsenz"*, 1/2011, S. Leitartikel.

Rivest, R. L., Shamir, A., & Adleman, L. (February 1977). A method for obtaining digital signatures and public-key cryptosystems. *Magazine Communications of the AMC* (Volume 21 Issue 2).

Sallmann, R., & Prorok, T. (23. Mai 2001). *KDZ Zentrum für Verwaltungsforschung*. (KDZ, Hrsg.) Abgerufen am 10. September 2001 von http://www.kdz.eu/de/webfm_send/348

Sánchez, S., Pérez, E., Gómez, A., & Carracedo, J. (2010). *Social and Legal Implications of Digital Identity in a Multi-national Environment*.

SATW ICT-Kommission. (2007). *Democracy vs e-democracy?*

- Schaffry, A. (22. Dezember 2004). *SAP info*. Abgerufen am 29. September 2011 von <http://de.sap.info/e-government-beschleunigt-verwaltungsprozesse/2037>
- Schallbruch, M. (März 2009). Sicherer gegenseitiger Identitätsnachweis mit dem elektronischen Personalausweis in Deutschland ab 2010. *Science Allemagne* , S. 5-6.
- Schedler, K., & Proeller, I. (2006). *New Public Management* (3. Aufl. Ausg.). Bern/Stuttgart/Wien: Haupt.
- Schedler, K., Summermatter, L., & Schmidt, B. (2003). *Electronic Government einführen und entwickeln – Von der Idee zur Praxis* (1 Ausg.). Bern, Stuttgart, Wien: Haupt Verlag.
- Schlauri, S. (2002). *Elektronische Signaturen*. Zürich: Schulthess Juristische Medien AG , Zürich.
- Schmidt, B. (2003). *e-Government und Servicequalität – Analysen zur Perspektive von IT - Anbietern und Verwaltungsführung* (1 Ausg.). Bern,Stuttgart,Wien: Haupt Verlag.
- Schüssel, W. (6. März 2000). (Bundespressdienst, Hrsg.) Abgerufen am 10. September 2011 von <http://www.bs13.goed.at/archiv/regierungserklaerung.pdf>
- Schweitzer, R. (01. Oktober 2004). Globale digitale Identitäten - Ein Realisierungskonzept für digitale Vollmachten. *Diplomarbeit* . Zürich, Schweiz.
- Signature Perfect KG. (2008). *Leitfaden Elektronische Signatur* (5 Ausg.). Frankfurt am Main.
- Smite, I. (November 2007). eGovernment in Latvia. (C. Freudenthaler, Interviewer)
- Steinebach, M. (März 2009). Watermarking- Schutz digitaler Medien. *Science Allemagne* , S. 28-30.
- Steria. (2011). *Case study BelPic*. Abgerufen am 02. Oktober 2011 von Steria: <http://www.steria.be/documents/File/casestudyBELPIC-EN.pdf>
- The Internet Society. (Jänner 1999). Abgerufen am 25. September 2011 von <http://www.faqs.org/rfcs/rfc2459.html>

The World Bank. (2011). *The World Bank*. (T. W. Group, Herausgeber) Abgerufen am 10. September 2011 von <http://go.worldbank.org/M1JHE0Z280>

Tino, S. (2004). E-Government: von der „Portalisierung“ zur umfassenden Neugestaltung öffentlicher Leistungserbringung. In C. (. Reichard, M. (. Scheske, & S. T. (Hrsg.), *Das Reformkonzept E-Government* (1. Ausg., S. 13-25). Münster: LIT Verlag.

TNS Emnid. (08. Dezember 2003). *Government Online - A National Perspective 2003 - Germany*. (TNS, Hrsg.) Abgerufen am 10. September 2011 von TNS Emnid: http://www.tns-emnid.com/presse/pdf/presseinformationen/GO_2003_Germany.pdf

TNS Global. (27. November 2003). *TNS Global*. (T. Global, Hrsg.) Abgerufen am 10. September 2011 von <http://www.legermarketing.com/documents/tenint/031219ENG.pdf>

Trauner, G. (2006). E-Government als Element einer neuen Verwaltung. In G. Holzinger, P. Oberndorfer, & B. Rauschauer, *Österreichische Verwaltungslehre* (2. Ausg.). Wien: Verlag Österreich.

Treasury Board of Canada Secretariat. (Dezember 2004). *Treasury Board of Canada Secretariat*. Abgerufen am 26. Juni 2007 von http://www.tbs-sct.gc.ca/pki-icp/pki-in-practice/efforts/2004/12/scan-analyse06_e.asp

U.S. General Services Administration Office of Governmentwide Policy. (2004). *Government Smart Card Handbook*.

Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein. (2007). *Verkettung digitaler Identitäten* (1.0 Ausg.). Kiel, Deutschland.

van Arkel, J., & Martiny, L. (04. Februar 2002). *SBS - Salzburger Banken Software*. Abgerufen am 02. Oktober 2011 von <http://www.sbs.co.at/sbs/home.nsf/open/52227EE4037E77F3C1256B560051A907>

von Lucke, J. (1999). *Internet-Technologien in der gesetzlichen Rentenversicherung* (Bd. 21). Heidelberg: R.V. Decker Verlag.

von Lücke, J. (2004). Portale als zentraler Zugang zu E-Government-Diensten. In C. (. Reichard, M. (. Scheske, & S. T. (Hrsg.), *Das Reformkonzept E-Government* (1. Ausg.). Münster: LIT-Verlag.

von Lucke, J., & Reiner mann, H. (2000). *Speyerer Definition von Electronic Government*.

Walloschke, T. (2008). Infrastructures and Middleware for the Application of eID Cards in eGovernment. In N. Pohlmann, H. Reimer, & W. Schneider, *Securing Electronic Business Processes, Highlights of the Information Security Solutions Europe 2008 Conferenc (ISSE 2008: 406-417 Ausg., S. 406-417)*. Madrid, Spanien: Vieweg+Teubner 2009.

Wang, Y.-J. (27. September 2011). eID and eGovernment in Denmark. (C. Freudenthaler, Interviewer)

Weber, R. H. (März 1997). Kryptographie – Schlagwort im Spannungsfeld von Geheimnisschutz und Sicherheitserwartungen. *Zeitschrift für Datenschutz des Kantons Zürich* , S. 36.

Yoon, J. (18. Juni 2007). *The World Bank*. Abgerufen am 10. September 2011 von <http://info.worldbank.org/etools/docs/library/240850/KoreaseGovernmentStrategy.pdf>

Zimmermann, P. (03. Dezember 2002). *The International PGP Home Page*. Abgerufen am 25. September 2011 von <http://www.pgpi.org/>

Zumsteg, F. (2004). *Die Bedeutung von Vertrauen für den Erfolg von E-Government*. Zürich: Diplomarbeit, angefertigt am Institut für Informatik der Universität Zürich.

Anhang B: Abbildungsverzeichnis

Abbildung 1: Übergang von Information über Kommunikation zu Transaktion (Mehlich, 2002)	10
Abbildung 2: Generationen des eGovernment	
Abbildung 3: Identität, digitale Identität und digitale Teilidentität (Unabhängiges Landeszentrum für Datenschutz Schleswig Holstein, 2007)	22
Abbildung 4: eGovernment	
Abbildung 5: Hashwert im hexadezimalen Zahlensystem (Schlauri, 2002)	43
Abbildung 6: Symmetrische Verschlüsselung (Pfitzmann, Waidner, & Pfitzmann, 1990)	44
Abbildung 7: Asymmetrische Verschlüsselung (Pfitzmann, Waidner, & Pfitzmann, 1990)	45
Abbildung 8: SHA mit DSA (National Institute of Standards and Technology, 1994).....	48
Abbildung 9: Klassifizierung von Speicherkarten nach Funktionsumfang (Langer & Roland, 2010).....	53
Abbildung 10: Klassifizierung der Eigenschaften von Terminals (Rankl & Effing, 1998)	57
Abbildung 11: Komponenten eines RFID Systems (Finkenzeller, 2008)	60
Abbildung 12: Beziehung zwischen „digitalen“ und „elektronischen“ Signaturen (Dumortier, 2004)	62
Abbildung 13: Signaturerstellung (Signature Perfect KG, 2008)	63
Abbildung 14: Signaturprüfung mittels Hash-Wert (Signature Perfect KG, 2008)	64
Abbildung 15: Digitale Signatursysteme (Pfitzmann, Waidner, & Pfitzmann, 1990)	64
Abbildung 16: Format des X.509 v3 Zertifikats (Dietrich, 2004).....	66
Abbildung 17: Zertifikat	
Abbildung 18: Autorisierung und Authentifizierung (Lutters, 2009).....	72
Abbildung 19: PKI Umgebung (Schweitzer, 2004)	74
Abbildung 20: Hierarchische PKI (Lutters, 2009)	75
Abbildung 21: PGP Verschlüsselung (Zimmermann, 2002).....	76
Abbildung 22: Nutzung von eID-Karten und mobiler eID für eTax Services (Martens T. , Electronic Identity management in Estonia between market and state governance, 2010)	93

Anhang C: Tabellenverzeichnis

Tabelle 1: Dienstleistungsangebot seitens der Behörde (Zumsteg, 2004)	15
Tabelle 2: Standards für kontaktlose Smartcards (Langer & Roland, 2010)	55
Tabelle 3: Klassifikation von Kartenlesegeräten (DATACOM, 2011)	58
Tabelle 4: Aufbau eines X.509 v3 Zertifikats (The Internet Society, 1999)	67
Tabelle 5: Die 20 am meist gebräuchlichen eGovernment Dienstleistungen (Capgemini, 2007).....	92

Stich- und Fachwörterverzeichnis

2-Wege-Kommunikation	13
Adressat	9
Advanced Encryption Standard	50, 55
Aktionsplan	29, 31, 32, 42
Akzeptanz	38, 44, 96, 121, 123, 127, 128
Algorithmus	47, 48, 50, 51, 52, 55, 74, 84
Alphabetismus	120
Anonymität	18, 21, 26, 27
Asymmetrische Verschlüsselung	47, 49, 51, 52, 55, 68, 69, 81, 83, 84
Ausprägungsgrad	12, 63
Authentication Server	81
Authentication Header Protocol	55
Authentifikation	2, 25, 34, 39, 47, 55, 56, 57, 67, 76, 81, 82, 96, 98, 106, 113
Authentifikationsdienst	81
Authentifikationsschlüssel	61
Authentifikationsserver	79
Authentifizierung	2, 18, 24, 25, 26, 27, 31, 32, 59, 67, 68, 69, 76, 85, 86, 87, 88, 90, 92, 94, 95, 100, 102, 107, 128
Authentisierung	2, 19, 39, 55, 56, 76, 77, 78, 79, 80
Authentizität	19, 27, 68, 70, 73, 77, 81, 128
Authorization Decision Assertion	79
Automatisierung	1, 2, 10, 28, 100
Autorisierung	2, 39, 54, 56, 67, 76, 78, 79
Back-Office	13, 36
BePIC	88, 89
Benutzerfreundlichkeit	123
Benutzerführung	122
Beschwerdemanagement	123
Beziehungsebenen	8, 9, 15
Biometrische Daten	61, 91
Browser-Zertifikate	55
Bürgernähe	21
Byte	53, 57, 61
Carlisle Adamns und Stafford Tavares Algorithmus	50, 84
CEN	34
CERES Zertifikat	95
Certificate Policy	73
Charakteristika	5, 14
Chipauthentisierung	76, 77, 78, 81
Chipkartenauthentisierung	77
Citizen Certificate	87, 88

Client Authentifizierung	54
Close-Coupling	60
Coprozessor	59
Data Encryption Standard	50, 55
Daten Box	107
Datenbanken	8, 10, 43, 65, 66
Datenbankmanagementsystem	9
Datenbanksystem	36
Datenschutz	2, 38, 39, 40, 41, 125, 128
Datenschutzverstoß	38
Datensicherheit	38, 39, 41, 125, 128
Denuncia vi@ Web	106
Dezentralisierung	117
DigiD	92, 93
Digital Signature Algorithm	51
Digitale Identität	2, 22, 23, 24, 25, 27, 28, 36, 42, 45, 55, 57, 67, 81, 85, 92, 104, 116
Digitale Signatur	24, 25, 31, 40, 41, 42, 44, 51, 52, 59, 68, 76, 81, 96, 97, 98, 100, 113, 129
Digitale Spaltung	120, 129
Digitalisierung	6
Dokumentenmanagementsystem	36, 43
Dual-Interface-Karten	61
eAdministration	9, 10
eDemokratie	9, 10, 127
eEPOCH	36
eEurope	29, 30, 32
Effektivität	1, 2, 3, 4, 6, 8, 31, 32, 86, 97, 111, 122, 123
Effizienz	3, 4, 6, 8, 14, 20, 32, 35, 37, 45, 86, 94, 97, 119, 122, 123, 127
eFormular	11, 101, 104, 108, 109, 115
eGovernment	1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15, 16, 17, 18, 20, 21, 22, 24, 26, 27, 28, 29, 31, 32, 34, 35, 36, 37, 38, 39, 41, 42, 43, 44, 45, 54, 57, 61, 68, 70, 85, 91, 92, 93, 94, 96, 97, 98, 99, 100, 101, 104, 107, 108, 109, 110, 111, 112, 113, 114, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130
eID	2, 3, 4, 5, 6, 23, 24, 25, 26, 28, 31, 33, 34, 36, 37, 39, 80, 85, 87, 88, 89, 91, 93, 95, 96, 98, 99, 100, 102, 106, 116, 120, 121, 122, 128, 130
eID Card Concept	112

eID-Funktion	25, 34, 80, 94
eID-Karte	5, 86, 87, 88, 89, 90, 91, 92, 94, 95, 96, 98, 105, 106, 111, 112, 113, 114, 115, 130
eID-System	33, 92
Einplatinencomputer	62
Einprägsamkeit	123
Ein-Weg-Interaktion	12
Elektronische Bürgerkarte	99
Elektronische Signatur	21, 40, 49, 59, 68, 69, 70, 71, 72, 85, 86, 88, 90, 91, 96, 98, 104, 107, 111, 112, 113, 128, 130
Elektronische Signatur-Funktion	25
Elektronischer Ausweis	24, 129
Elektronisches Regieren	1, 7
Elektronisches Signaturschema	86, 97, 130
Encapsulating Security Payload	55
Entschlüsselungsalgorithmus	48
ePartizipation	10
ePayment	101
ePortal	18, 19, 20, 34, 78, 86, 94, 97, 107, 110, 112, 113, 114
Erreichbarkeit	20, 21, 44
Erweiterbarkeit	44, 119, 120
eService	3, 7, 15, 16, 19, 20, 27, 30, 31, 33, 34, 35, 68, 90, 92, 94, 96, 97, 101, 102, 103, 105, 106, 109, 111, 112, 113, 114, 115, 122, 123, 125, 129
eTax	16, 26, 89, 93, 94, 102, 103, 104, 109
eTEN	35
eTransaktion	11
EUCLID	35
Europäische Bürgerkarte	99
Europäische Gemeinschaften	35, 41, 87, 90
Europäische Komitee für Standardisierung	34
Europäische Kommission	6, 14, 29, 35, 36, 42, 101, 104, 110, 129
Europäische Union	3, 4, 6, 29, 34, 35, 39, 40
Europäischer Rat	29, 41
Europäisches Parlament	41
eVoting	10, 17, 20, 26, 104, 105, 126
FASME	36
FINEID	87, 88
Fingerabdruck	18, 24, 26, 46, 61, 91, 99
Finish Population Register Centre	88
first job card	106

Fortgeschrittene elektronische Signatur	42, 69
Generationen des eGovernments	12, 13, 14
Giesecke&Devrient	99
Government-to-Business	8
Government-to-Citizen	8
Government-to-Employee	9
Government-to-Government	9
GUIDE	36
Halbduplex Protokoll	53
Handshaking Protocol	55
Hardware	43, 92, 95, 97, 98, 120, 121
Harmonisierung	108, 129
Hash-Verfahren	46, 47, 70
Hash-Wert	46, 47, 70, 71, 72
Help.gv	114, 115, 124
Hostrechner	61, 63
Hostschnittstelle	62
Hybridkarte	61
IDABC	35
Identifikation	2, 18, 19, 22, 24, 25, 26, 27, 28, 32, 33, 39, 42, 67, 68, 69, 79, 80, 85, 86, 87, 88, 91, 92, 94, 95, 97, 98, 100, 125, 128
Identifikationscode	87
Identifikator	87
Identität	23, 24, 26
Identitätsdaten	24, 26, 27, 66, 67, 80
Identitätsdokument	24
Identitätskarte	25, 26, 32, 87, 88, 89, 95, 96, 111
Identitätsmanagement	32
Identitätsnachweis	2, 22, 24, 25, 26, 27, 33, 39, 67, 68, 79, 99, 128
Information	1, 9, 10, 11, 12, 14, 15, 16, 17, 18, 20, 21, 24, 25, 30, 38, 43, 44
Informations- und Kommunikationstechniken	7
Informations- und Kommunikationstechnologien	1, 7, 8, 9, 10, 15, 18, 26, 30, 44, 85, 108, 112, 121
Initial employment contract	106
Initiative	3, 29, 31, 32, 33, 34, 35, 93, 95, 96, 98, 107, 108, 109, 118, 120, 128, 129
Innovations- und Kommunikationstechnologien	30, 127
Insellösung	44, 119
Integrität	19, 27, 68, 78, 81, 128
Interaktion	1, 7, 8, 10, 11, 14, 15, 16, 20, 21, 26, 27, 99, 109, 127
Interaktionsgrad	12, 43

Interaktionsniveau	10, 11
Interaktionsstufe	10, 12
International Data Encryption Algorithmus	51, 84
Internet	1, 3, 10, 11, 17, 20, 21, 23, 25, 27, 28, 30, 31, 33, 38, 52, 54, 86, 93, 94, 100, 104, 105, 108, 109, 112, 121, 127
Interoperabilität	33, 36, 42, 44, 56, 73, 119, 129
IPSec	55
IR Service On-Line	110
IRISbox	114
Java	59, 62
Kartenlesegerät	43, 52, 53, 57, 61, 62, 63, 64, 65, 76, 77, 78, 92, 94, 95, 96, 97, 106, 114, 120, 125, 130
Kartenschnittstelle	62
Kerberos	56, 81
Key Distribution Center	48, 81
Kids-ID	89
Kommunikation	9, 12, 14, 16, 21, 27, 34, 41, 45, 50, 78, 85, 100, 113, 127, 128, 129, 130
Kommunikationsplattform	7, 10, 20
Kommunikationsschnittstelle	60
Kontaktbehaftete Schnittstellen	53
Kontaktschnittstelle	99
Kooperation	45, 128
Koordination	45, 127
Kryptografie	46, 47, 50, 54, 58, 59, 67, 74, 76
Lernbarkeit	122
Linux	59
Luftschnittstelle	63
Manipulation	27, 77
Medienbruch	3, 12, 17, 28, 42, 43, 119, 122
Memory Management Unit	59
Micro Controller	57, 58, 59, 61, 62
Mikrochip	57, 59, 65
Missbrauch	2, 38, 41, 99, 125
Mobile eID	92, 102, 130
Mobile Token	91
Mobilität	34
MyHelp.gv	115
NemID	86, 97, 98
Netzwerkinfrastruktur	44, 119
Netzwerkkapazität	119
One face to the costumer	19
One-Stop-Shop	20, 124
Online Certificate Status Protocol	75

Online Reifegrad	14
Open Smart Card Infrastruktur	34
Optimierung	2, 45, 108
PACE Protokoll	53, 54, 77, 78
Passive Authentisierung	77
Personal Digital Assistant	57, 67
Personal Security Environment	82
PIN	58, 64, 78, 79, 80, 90, 104, 114
PKI	94
PKI Overheid	93
Police-on-Web	106
Policy Decision Point	79
Policy Enforcement Point	79
Pretty Good Privacy	51, 83, 84
PRIME	35
Private Key	48, 49, 51, 59, 70, 75, 77, 82, 90
Produktivität	31, 33
Prozesskarte	57, 58, 59
Prüfsumme	46, 47
Prüfsummenverfahren	46
Public Key	48, 49, 51, 54, 59, 70, 72, 73, 74, 78, 82, 83, 84
Public Key Infrastruktur	39, 51, 77, 81, 82, 83, 85, 92, 93, 110
Public Key Infrastruktur Zertifikat	86, 102
Public Key Zertifikat	56, 73, 81, 82, 83
Qualifizierte elektronische Signatur	70, 72, 111
Radio-Frequency Identification-Technology	65, 66
Radio-Frequenz Identification	65
Record Protocol	55
Root Certification Authority	83
Root-Zertifikat	83
RSA Algorithmus	51, 52, 55, 84
SAML	56
Schaufensterfunktion	20
Schlüsselpaar	51, 59
Schlüsselverteilzentrale	48
Schriftformerfordernis	28
Secure Messaging	78
Secure Socket Layer	93
Secure Socket Layer Protokoll	55
Security Controller	59
Server Authentifizierung	54
Sichere elektronische Signatur	69
Sichere Signaturerstellungseinheit	59
Sichere Signaturerzeugungseinheit	71

Sicherheit	1, 5, 19, 22, 27, 28, 35, 40, 43, 47, 50, 61, 64, 91, 96, 124, 125, 127
Sicherheitsdienst	39
Sicherheitsfunktion	63
Sicherheitsinfrastruktur	37, 38, 39, 43
Sicherheitsklasse	64
Sicherheitsstandard	2, 38, 125, 130
Sicherheitstechnologie	125
Signaturfunktion	59
Signaturgesetz	40, 59, 73
Signaturinfrastruktur	111, 120
SIM Card	67, 88, 92
Smart Card	18, 24, 26, 30, 31, 34, 36, 52, 53, 54, 57, 58, 59, 60, 61, 63, 67, 72, 76, 77, 78, 79, 80, 82, 86, 87, 88, 95, 113, 130
Smart Phone	67
SOAP	56, 57
Software	27, 43, 92, 96, 98, 120
Speicherkarte	57, 58, 60
Standardisierung	18, 44, 119, 129
Start2surf@home	108
Symmetrische Verschlüsselung	47, 48, 50, 51, 55, 81, 83, 84
Tags	60
Tax-on-Web	89, 103
Terminal	53, 54, 61, 62, 63, 64, 76, 77, 78, 80
Terminalauthentisierung	76
Ticket Granting Server	81
Token	57, 67, 72, 79, 86
Transaktion	1, 7, 8, 9, 11, 13, 25, 27, 64, 80, 85, 87, 93, 98, 99, 112, 118, 122, 125, 127, 130
Transparenz	1, 8, 19, 20, 30, 32, 115, 126, 127
Transponder	65, 66
Triple Data Encryption Standard	50
True eGovernment	11, 17, 42, 119
Trust Center	72, 75, 82
über Tax-on-Web	103
Übertragungsprotokoll	53, 60, 63
Umstrukturierung	44, 45, 117, 128
Universal Serial Bus	62, 64, 67, 86
Universal Serial Bus Token	67, 72, 79
Usability	122
Veränderungsmanagement	45, 117
Verbindlichkeit	21, 22, 128
Verfügbarkeit	14, 26, 101, 119, 122, 126

Verifikation	52
Verifizierung	112
Verschlüsselung	39, 47, 48, 49, 50, 51, 52, 55, 56, 65, 67, 68, 70, 72, 73, 78, 81, 83, 84, 87, 125
Verschlüsselungsalgorithmus	48, 50, 51, 69
Vertrauen	21, 22, 27, 28, 33, 35, 38, 47, 97, 122, 124, 125, 126, 127, 130
Vertraulichkeit	19, 22, 27, 55, 78, 128
Verwaltungsprozess	2, 10, 22, 25, 26, 40, 41, 45
Verwaltungsreform	45, 116
Virtuelle Verwaltung	21
Vollduplex Protokoll	53
Vollständigkeit	124
Web of Trust	84
Web Service Security	56
Welcome to e-Belgium	94, 124
Wettbewerbsfähigkeit	29, 30, 111
Windows	59
Workflow-Managementsystem	9, 36, 43
X.509	73, 82, 83
X.509 Zertifikat	73, 74, 83
XML Signatur	56
XML Verschlüsselung	56
Zeitstempel	72
Zentraler Kreditausschuss	64
Zertifikat	40, 54, 65, 72, 73, 74, 75, 77, 80, 82, 83, 85, 87, 88, 90, 91, 92, 95, 112, 130
Zertifikate Revocation List	75
Zertifizierungsdiensteanbieter	72, 73, 81, 90
Zuverlässigkeit	28
Zweiklassengesellschaft	120, 121
Zwei-Weg-Interaktion	13