
Unterschrift des Betreuers

MAGISTERARBEIT

Konzepte zur Bereitstellung der elektronischen Zustellung für das außerbehördliche Umfeld

zur Erlangung des akademischen Grades
Diplomingenieur (Dipl.-Ing.)

ausgeführt am
Institut für Rechnergestützte Automation
Forschungsgruppe Industrial Software

der Technischen Universität Wien

unter der Anleitung von
Univ.-Prof. Dipl.-Ing. Dr. techn. Thomas Grechenig
und Dipl.-Ing. Gerald Fischer als verantwortlich mitwirkenden Assistenten

durch
Christoph Markaritzer, bakk.rer.soc.oec.
Eduard-Richter-Gasse 21
8010 Graz

Graz, am 15. August 2007

Unterschrift (Student)

Eidesstattliche Erklärung

Ich erkläre an Eides statt, daß ich die vorliegende Arbeit selbständig und ohne fremde Hilfe verfaßt, andere als die angegebenen Quellen nicht benützt und die den benutzten Quellen wörtlich oder inhaltlich entnommenen Stellen als solche kenntlich gemacht habe.

Graz, am 15. August 2007 ----------

Christoph Markaritzer

Vorwort und Danksagung

Ein Studium ist eine große psychische Belastung, die nicht leicht zu bewältigen ist und mich durch Licht und Schatten geführt hat.
Allerdings trägt die universitäre Ausbildung auch zur Reifung der eigenen Persönlichkeit bei und lehrt in vielen Dingen für das weitere Leben.
Nachfolgend möchte ich mich bei folgenden Personen bedanken, die mir im Allgemeinen bei der Bewältigung meines Studiums und im Speziellen bei der Entstehung dieser Arbeit behilflich waren:

Zu Beginn danke ich Herrn DI Günter Rauchegger für seine Hilfe in Mathematik und Statistik, wodurch ein frühes Scheitern meines Studiums abgewendet werden konnte.
Herrn Edgar Kadlec, bakk., ein ständiger Wegbegleiter im Studium, möchte ich für die gute und oftmals erheiternde Zusammenarbeit danken.
Meiner Tante Frau Dr. Waltraud Markaritzer und Herrn Dr. Helmut Haselwander gilt spezieller Dank für die moralische Unterstützung im und um mein Studium.
Außerdem möchte ich Herrn Mag. Mathias Knafl für juristische Hilfestellung und interessante Diskussionen im Themengebiet der elektronischen Zustellung danken.
Nicht zuletzt möchte ich meinen Eltern Dank für die Ermöglichung des Studiums und die dabei aufgebrachte Geduld aussprechen.
Abschließend möchte ich Herrn Prof. Thomas Grechenig, Herrn DI Gerald Fischer und Herrn DI Peter Reichstädter für die Betreuung und die Ermöglichung der schnellen Abwicklung dieser Arbeit danken.

Kurzfassung

Die vorliegende Magisterarbeit beschäftigt sich damit, wie die elektronische Zustellung, die heute zur gesicherten Übermittlung von behördlichen Dokumenten an Bürger angewandt wird, für die Kommunikation zwischen natürlichen bzw. nicht natürlichen Personen erweitert werden kann.

Nach Erläuterung der Ausgangssituation und Klärung der rechtlichen und technischen Grundlagen, wird das System der behördlichen elektronischen Zustellung genauer beschrieben. Die Erkenntnis daraus ist, daß das behördliche elektronische Zustellsystem durch sein offenes Design Potentiale bietet, die im außerbehördlichen Umfeld genutzt werden können.
In weiterer Folge werden die Anforderungen an die elektronische Zustellung im außerbehördlichen Umfeld analysiert, sowie notwendige Erweiterungen der behördlichen elektronischen Zustellung dokumentiert.
Darauf aufbauend und bezugnehmend auf das parallel in der Praxis laufende Projekt „kommerzielle e-Zustellung“ der Wirtschaftskammer Österreich, wird eine Konzeption eines Zustellsystems für das außerbehördliche Umfeld vorgestellt. Eines der Hauptprobleme der Konzeption ist, daß das zukünftige System für viele Benutzer verfügbar sein soll und dabei auch rechtliche und technische Sicherheit bieten muß. Als Lösung dieser Probleme wird eine modulare Bauweise des Systems in Form einer serviceorientierten Architektur gewählt, die bei Bedarf an die jeweiligen Bedürfnisse der unterschiedlichen Benutzer angepasst werden kann.
Zum besseren Verständnis wird der Ablauf der elektronischen Zustellung im außerbehördlichen Umfeld aus der Sicht des Absenders, des Empfängers und der Systemkomponenten modelliert.
Als Abschluß der Arbeit werden mögliche Anwendungsszenarien vorgestellt.

Abstract

This thesis analyses the issue of how to extend the electronic delivery, which is already in use, for secured transmission of documents from the administration to citizens. The focus of the current thesis is to find a solution to enable secure communication between natural and/or legal persons.

After explaining the initial situation and clarifying the legal and technical basics, the existing system of the official electronic delivery is described in detail. The conclusion of this analysis is that the official electronic delivery system offers, due its open system architecture, potentials which can be used in the external environment.

Furthermore, the requirements for the electronic delivery in the external environment were analysed and necessary extensions revealed. Based on these investigations and, moreover, on the case study “kommerzielle e-Zustellung” (“commercial e-delivery”) by the Austrian chamber of commerce (WKO), a concept of an electronic delivery system for an external environment is presented. The main problem of this concept is that the prospective system must be available for many potential users and should also offer legal and technical security. The solution for these problems is to build the system in a modular way, in the form of a service-oriented architecture, which can be adapted to the respective needs of different users if necessary.
For a better understanding of the electronic delivery system in the external environment, the process flow from the view of the sender, the receiver and the system components is modelled. As a conclusion of the thesis possible business case are introduced.

Inhaltsverzeichnis

Inhaltsverzeichnis I

Abbildungsverzeichnis IV

Tabellenverzeichnis V

1 Einleitung 1
1.1 Motivation und Zielsetzung 2
1.2 Aufbau der Arbeit 3

2 Grundlagen der Zustellsysteme 4
2.1 Das konventionelle Zustellsystem 4
2.1.1 Die private Briefsendung 4
2.1.2 Die rechtsichere behördliche Zustellung 5
2.2 Die elektronische Zustellung im behördlichen Umfeld 6
2.2.1 Die Bausteine 7
2.2.2 Aktuelle Entwicklung 8
2.3 Die elektronische Zustellung im außerbehördlichen Umfeld 9
2.3.1 Ziele 9
2.3.2 Aktuelle Entwicklung 10

3 Rechtliche Grundlagen 12
3.1 Für die behördliche elektronische Zustellung 12
3.1.1 Zustellgesetz 12
3.1.2 E-Government-Gesetz 12
3.2 Für die kommerzielle elektronische Zustellung 13
3.2.1 Relevante Bestimmungen im Zustellgesetz 13
3.2.2 Relevante Bestimmungen im E-Government-Gesetz 14
3.3 Für die elektronische Signatur 15
3.4 Beweiskraft elektronisch zugestellter Dokumente 17
3.4.1 Unterschiede in der Beweiskraft 17
3.4.2 Vergleich der Beweiskraft 18
3.4.3 Beweiskraft von Ausdrucken 19

4 Technische Grundlagen 20
4.1 Serviceorientierte Architekturen und Webservices 20
4.2 Asymmetrische Kryptoverfahren 21
4.3 Digitale Signaturen 22
4.3.1 XML-Signaturen 24
4.3.2 Zeitstempel 25
4.4 Die Bürgerkarte 26
4.4.1 Das Modell 26
4.4.2 Die Funktionen 27
4.5 Module für Online Applikationen 29

5 Beschreibung der behördlichen elektronischen Zustellung 30
5.1 Beschreibung der Softwarearchitektur 30
5.1.1 Die Applikation 31
5.1.2 Das Modul für Online Applikationen Zustellung 32
5.1.3 Der Zustelldienst 33
5.1.4 Der Zustellkopf 33
5.1.5 Die Benutzerschnittstelle für den Empfänger 34
5.2 Der Ablauf anhand rechtlicher und technischer Gesichtspunkte 34
5.2.1 Anmeldung bei einem elektronischen Zustelldienst 34
5.2.2 Erstellung des Dokuments 36
5.2.3 Ermittlung des Zustelldients 37
5.2.4 Abfertigung des Dokuments durch MOA-ZS 38
5.2.5 Übergabe des Dokuments an den Zustelldienst 39
5.2.6 Verständigung des Empfängers 40
5.2.7 Abholung des Dokuments 41
5.2.8 Versenden des Zusellnachweises 42

6 Anforderungen an die kommerzielle elektronische Zustellung 43
6.1.1 Anforderungen an das ursprüngliche System 43
6.2 Anforderungen an das zukünftige System 44
6.2.1 Technische Anforderungen 44
6.2.2 Organisatorische Anforderungen 45
6.3 Notwendige Erweiterungen des behördlichen Modells 46
6.3.1 Identifikation bzw. Authentifizierung 46
6.3.2 Klassifizierung der Dokumenttypen 50
6.3.3 Einzel- und Massensendungen 50
6.3.4 Art der Benutzerschnittstelle 51
6.3.5 Zustellqualitäten und -varianten 53
6.3.6 Vertretungsregelung 54
6.3.7 Verrechnung und Preisgestaltung 55

7 Konzeption des kommerziellen elektronischen Zustellsystems 57
7.1 Systembeschreibung 57
7.1.1 Die Systemkomponenten 58
7.1.2 Die Schnittstellen 61
7.1.3 Das Modell bei Anwendung der reinen elektronischen Zustellung 62
7.1.4 Das Modell bei Anwendung der dualen Zustellung 63
7.2 Spezifikation der Anwendungsfälle 65
7.2.1 Anwendungsfälle des Absendedienst 65
7.2.2 Anwendungsfälle des Zustelldiensts 72
7.2.3 Gemeinsame Anwendungsfälle mit dem behördlichen Modell 82
7.3 Entwurf der Softwarearchitektur 83
7.3.1 Benötigte Datenbanken 83
7.3.2 Attribute der Komponenten 86
7.3.3 Methoden der Komponenten 88

7.4 Beschreibung der Formate für den Datenaustausch 98
7.4.1 Benutzerschnittstelle Absender – Absendedienst 98
7.4.2 Absendedienst – Zustellkopf 99
7.4.3 Zustellkopf – Zustelldienst 103
7.4.4 Absendedienst – Zustelldienst 104
7.4.5 Zustelldienst – Benutzerschnittstelle Empfänger 112
7.5 Ablauf der kommerziellen elektronischen Zustellung 113
7.5.1 Aus der Sicht des Absenders 113
7.5.2 Aus der Sicht des Empfängers 118
7.5.3 Aus der Sicht der Systemkomponenten 122

8 Anwendungsszenarien für die kommerzielle elektronische Zustellung 129
8.1 Allgemeines Anwendungsszenario 129
8.2 Spezielle Anwendungsszenarien 130
8.2.1 Ausschreibungsmanagement 130
8.2.2 e-Zustellung „Ultra Light“ 130
8.2.3 Elektronische Rechnung und elektronischer Zahlschein 131
8.2.4 Elektronischer Rechtsverkehr 132

9 Conclusio 133
9.1 Zusammenfassung der Ergebnisse 133
9.2 Perspektiven 134

10 Literaturverzeichnis 136

Glossar i

Abbildungsverzeichnis

Abbildung 1: Der Ablauf der behördlichen elektronischen Zustellung 7
Abbildung 2: Aussehen und Komponenten der Amtssignatur 16
Abbildung 3: Serviceoriente Architektur 20
Abbildung 4: Bildung einer digitalen Signatur 22
Abbildung 5: Verifikation einer digitalen Signatur 23
Abbildung 6: Das Modell der Bürgerkarte 26
Abbildung 7: Ableitung der Stammzahl und des Personenkennzeichens 28
Abbildung 8: Das Komponentenmodell der behördlichen e-Zustellung 30
Abbildung 9: MOA-ZS als Middleware 32
Abbildung 10: MIME-Container der Sendung 36
Abbildung 11: Verschlüsselter Container der Sendung 39
Abbildung 12: Modell der reinen kommerziellen elektronischen Zustellung 62
Abbildung 13: Modell der dualen Zustellung 63
Abbildung 14: Anwendungsfalldiagramm des Absendienstes 65
Abbildung 15: Anwendungsfalldiagramm des Zustelldiensts 72
Abbildung 16: XML Schema „SucessErrorCode“ 98
Abbildung 17: XML Schema “Invoice“ 98
Abbildung 18: XML Schema "StdQuery" 99
Abbildung 19: XML Schema "StdAnswer" 100
Abbildung 20: XML Schema "BQuery" 101
Abbildung 21: XML Schema "BAnswer" 102
Abbildung 22: XML Schema "ComDelReq" 105
Abbildung 23: XML Schema Unterelement "Receiver" 106
Abbildung 24: XML Schema Unterelement "Sender" 107
Abbildung 25: XML Schema „ComDelStat“ 108
Abbildung 26: XML Schema „ComDelNot“ im Erfolgsfall 110
Abbildung 27: XML Schema „ComDelNot“ bei fehlgeschlagener Zustellung 111
Abbildung 28: XML Schema "DocumentList" 112
Abbildung 29: EPK aus Absendersicht 114
Abbildung 30: EPK Subprozeß „Zustellanfrage“ 115
Abbildung 31: EPK Subprozeß „Abfertigung des Dokuments" 116
Abbildung 32: EPK Subprozeß „Versand des Dokuments“ 117
Abbildung 33: EPK aus Empfängersicht 118
Abbildung 34: EPK Subprozess „Anmelden Empfänger“ 119
Abbildung 35: EPK Subprozess „Annahme bzw. Ablehnung des Dokuments“ 120
Abbildung 36: EPK Subprozess „Abholung des Dokuments“ 121
Abbildung 37: Ablaufdiagramm Anmeldevorgang Absender 122
Abbildung 38: Ablaufdiagramm Zustellanfrage 123
Abbildung 39: Ablaufdiagramm Abfertigung des Dokuments 124
Abbildung 40: Ablaufdiagramm Versand des Dokuments 125
Abbildung 41: Ablaufdiagramm Benachrichtigung, Anmeldung Empfänger 126
Abbildung 42: Ablaufdiagramm Ablehnung eines Dokuments 127
Abbildung 43: Ablaufdiagramm Abholung, Erstellung und Versand der Zustellbestätigung 128
Abbildung 44: Kommunikationswege der elektronischen Zustellung 129
Abbildung 45: Vereinte Zustellsysteme 135

Tabellenverzeichnis

Tabelle 1: Anwedungsfälle Absendedienst behördlich und kommerziell 82
Tabelle 2: Anwedungsfälle Zustelldienst behördlich und kommerziell 82
Tabelle 3: Datenbank „SenderData“ 83
Tabelle 4: Datenbank „DispatchData“ 83
Tabelle 5: Datenbank „Documents“ 84
Tabelle 6: Datenbank „ReceiverData“ 84
Tabelle 7: Datenbank „LogData“ 85
Tabelle 8: Datenbank „PostOfficeBox“ 85
Tabelle 9: LDAP Parameter 103
Tabelle 10: EPK Notation 113

1 Einleitung

In der heutigen Zeit wird die Nutzung von Informationstechnologie als alltäglich und selbstverständlich angesehen. Vor allem in den letzten Jahren wurde speziell durch die Verbreitung des Internets die Vernetzung von Informationssystemen vorangetrieben.
Die Kommunikation findet sowohl im geschäftlichen als auch im privaten Umfeld mehr und mehr elektronisch statt.

Als Kommunikationsmittel dient in den meisten Fällen die E-Mail, die eine kostengünstige und schnelle Kommunikation ermöglicht. Beim Einsatz von E-Mails treten jedoch auch potentielle Sicherheitsrisiken, in Form von Viren und sonstiger Malware in den Vordergrund.
Bei näherer Betrachtung treten weitere Unsicherheiten auf:
Da E-Mail Adressen im Grunde frei wählbar sind, kann in vielen Fällen nur über die IP-Adresse feststellt werden, ob es sich bei der in der E-Mail Adresse angegebenen Person wirklich um dieselbe handelt.
Des Weiteren ist ohne den Einsatz von spezieller, meist proprietärer E-Mail Sicherheitssoftware unsicher, ob der Inhalt nicht während der Übertragung von Dritten gelesen oder gar verändert wurde.
Am Ende der Übertragung ist außerdem ungewiß, ob die Nachricht auch wirklich beim (richtigen) Empfänger angekommen ist.

Alle diese Aspekte scheinen die E-Mail für die Übertragung sensibler Daten und Dokumente auszuschließen.
Als Lösung bietet sich die Entwicklung eines gesicherten, standardisierten und für jedermann offenen elektronischen Zustellsystems an, bei dem die oben genannten Probleme der E-Mail nicht auftreten.

In Österreich spielt die Behörde hierfür eine Vorreiterrolle. Im Zuge der Einführung des E-Governments, das die Durchführung von Verwaltungsaufgaben über den elektronischen Weg ermöglichen soll, wurde bereits ein System für die elektronische Zustellung entwickelt. Das Ziel der behördlichen elektronischen Zustellung ist es, dem Bürger auf elektronischem Weg Informationen genauso rechtsicher wie auf Papier zukommen zu lassen, wofür auch das Zustellrecht novelliert wurde.

Die elektronische Zustellung im behördlichen Umfeld ist vollständig implementiert. Für das außerbehördliche Umfeld, d.h. für die Kommunikation zwischen den Bürgern untereinander existiert nach heutigem Stand der Dinge noch kein gleichwertig verfügbares System.

1.1 Motivation und Zielsetzung

Das Ziel der vorliegenden Magisterarbeit ist es, Konzepte zu analysieren bzw. zu entwickeln, mit deren Hilfe die elektronische Zustellung im außerbehördlichen Umfeld eingeführt werden kann.
Die behördliche elektronische Zustellung besitzt Potentiale die auch im außerbehördlichen Umfeld nützlich sein können. Zu diesem Zweck und um Synergien ziehen zu können, ist ein detailliertes Verständnis des behördlichen Modells notwendig.
Im Rahmen dieser Arbeit soll analysiert werden, welche Komponenten der behördlichen elektronischen Zustellung auch im außerbehördlichen Umfeld verwendet werden können und welche Komponenten angepaßt bzw. erweitert werden müssen.
Neben den technischen Details ist es auch vorteilhaft die rechtlichen Rahmenbedingungen der elektronischen Zustellung zu kennen.
Ein weiteres Ziel dieser Arbeit ist es, das gesamte System der elektronischen Zustellung anhand einer rechtlichen, organisatorischen und technischen Beschreibung für die Allgemeinheit verständlicher zu machen.
Abschließend soll durch die Beschreibung von etwaigen Anwendungsszenarien hypothetisch festgestellt werden, wie und in welchen außerbehördlichen Bereichen die elektronische Zustellung verwendet werden kann.
Diese Arbeit leistet einen Beitrag dazu, die Bemühungen der Wirtschaft bei der Etablierung der elektronischen Zustellung für das außerbehördliche Umfeld zu unterstützen.

1.2 Aufbau der Arbeit

Kapitel 1 Einleitung

Kapitel 2 erläutert die unterschiedlichen Zustellsysteme.

Kapitel 3 beschreibt die aktuellen rechtlichen Grundlagen.

Kapitel 4 beschreibt die relevanten technischen Grundlagen.

Kapitel 5 beschreibt das System und den Ablauf der behördlichen elektronischen Zustellung aus rechtlichen und technischen Gesichtspunkten.

Kapitel 6 führt eine Anforderungsanalyse für die elektronische Zustellung im außerbehördlichen Umfeld durch.

Kapitel 7 stellt eine Konzeption für ein elektronisches Zustellsystem für das außerbehördliche Umfeld vor. Aufbauend auf der momentanen Entwicklung in der Wirtschaft, werden, ein mögliches Systemdesign und eine Beschreibung des Ablaufs durchgeführt.

Kapitel 8 gibt einen Überblick über die möglichen Anwendungsszenarien der elektronischen Zustellung im außerbehördlichen Umfeld.

Kapitel 9 bietet eine Zusammenfassung der Arbeit und soll einen Ausblick über zukünftige Entwicklungen geben.

2 Grundlagen der Zustellsysteme

In diesem Kapitel wird zu Beginn das System der konventionellen Zustellung beschrieben, um erstens einen Überblick über die konventionellen Zustellverfahren und um zweitens ein Verständnis aufzubauen, wie die elektronische Zustellung darauf aufbaut.
In weiterer Folge werden das Konzept der behördlichen elektronischen Zustellung, sowie das der sich in Entwicklung befindlichen außerbehördlichen elektronischen Zustellung, vorgestellt.

2.1 Das konventionelle Zustellsystem

2.1.1 Die private Briefsendung

In Österreich können natürliche und nicht natürliche Personen verschiedenartige Briefe versenden.

Die österreichische Post [WWW10] bietet hierfür folgende Zustellqualitäten an:

- Standard
  Die normal übliche Briefsendung, die ohne Bestätigung bzw. Bescheinigung an den Empfänger zugestellt wird.

  Um mehr Sicherheit beim Versand zu erhalten, kann gemäß der Definition im Postgesetz [PostG06], eine Postsendung auch auf folgende spezielle Arten aufgegeben werden:

- Eingeschrieben
  Der Versand des Briefes wird hierbei von der Post schriftlich bestätigt. Der Empfang des Briefes ist durch den Empfänger bzw. durch einen Übernahmeberechtigten zu bestätigten.
  Bei etwaig auftretenden Problemen kann der Zustellvorgang im Nachhinein nachverfolgt werden.

- Eigenhändig
  Ein als „Eigenhändig“ aufgegebener Brief, wird nur an die als Empfänger bestimmte Person ausgegeben.

- Rückschein
  Beim Rückscheinbrief wird die Zustellung des Briefes genau bestätigt. Dies geschieht mittels eines Rückscheins, der vom Empfänger zu unterschreiben ist und anschließend an den Absender zurückgesendet wird.

2.1.2 Die rechtsichere behördliche Zustellung

Die Zustellung von behördlichen Dokumenten ist in Österreich durch das Zustellgesetz [ZusG04] geregelt. Gemäß Zustellgesetz gibt es für behördliche Mitteilungen und Bescheide einen speziellen Brieftyp, den behördlichen Rückscheinbrief.

Es existieren zwei verschiedene Qualitäten des Rückscheinbriefes:

- RSa-Brief
  Der RSa-Brief, der auch Rückscheinbrief blau bzw. als blauer Brief [Feil06] bezeichnet wird, darf nur dem ausgewiesenen Empfänger selbst ausgefolgt werden. Die offizielle Bezeichnung dafür heißt „Eigenhändige Zustellung“ [ZusG04]. Als RSa-Brief werden nur besonders wichtige behördliche Dokumente versendet. Die genaue Regelung wann ein Dokument als RSa-Brief zugestellt werden muß, wird im betreffenden Verwaltungsgesetz festgelegt.
  Wenn der Empfänger beim ersten Zustellversuch nicht anzutreffen ist, wird ein zweiter Zustellversuch durchgeführt. Bleibt der zweite Zustellversuch erfolglos, wird der Brief beim Postamt zur Abholung hinterlegt.

- RSb-Brief
  Der RSb-Brief, der auch Rückscheinbrief weiß bzw. als weißer Brief [Feil06] bezeichnet wird, muß im Gegensatz zum RSa-Brief nicht zwingend an den ausgewiesenen Empfänger zugestellt werden, sondern kann auch an Personen, im gleichen Haushalt bzw. am selben Arbeitsplatz, ausgefolgt werden. Die offizielle Bezeichnung dafür heißt: „Zustellung auch an Ersatzempfänger“ [ZusG04.]
  Wenn beim ersten Zustellversuch des RSb-Briefs, weder der Empfänger selbst, noch ein Ersatzempfänger anzutreffen ist, wird der Brief am Postamt zur Abholung hinterlegt.

2.2 Die elektronische Zustellung im behördlichen Umfeld

Im Zuge der Einführung von E-Government wurde es Behörden und Bürgern ermöglicht Verwaltungsaufgaben auf elektronischem Weg, vom Antrag über die Erledigung bis hin zur Zustellung, durchzuführen [WWW08].

Die behördliche elektronische Zustellung ist dabei ein zentraler Baustein des E-Governments und ermöglicht der Behörde das Versenden von Dokumenten ohne und mit Zustellnachweis (in Analogie zum konventionellen RSa-Brief. Anmerkung: RSb wird aufgrund der nicht fertig implementierten elektronischen Vollmachtsregelung noch nicht unterstützt) [Posc06].

In Österreich versenden Behörden jährlich mehrere Millionen Schriftstücke [Hof03]. Das Ziel der elektronischen Zustellung ist es, den Behörden eine Vereinfachung des Zustellprozesses zu ermöglichen, sowie die Anzahl der konventionell versendeten Dokumente auf ein Minimum zu reduzieren [HoRe04]. Dadurch können einerseits Medienbrüche vermieden und andererseits Kosten für Druck, Kuvertierung und Porto eingespart werden [Kast05].
Für den Bürger entsteht eine Reihe von Vorteilen, wie der zeit- und ortsunabhängige Zugang zu behördlichen Dokumenten.

Bei der behördlichen elektronischen Zustellung liegt die Zustellqualität und -sicherheit auf gleich hohem Niveau wie bei der konventionellen Zustellung. Für die Durchführung gibt es eine genaue gesetzliche Regelung im Zustellgesetz [ZusG04].

Der in Abbildung 1 dargestellte Prozeß läuft recht einfach ab, da das Modell für Verwaltung und Bürger gleichsam verständlich sein soll [Reic04].

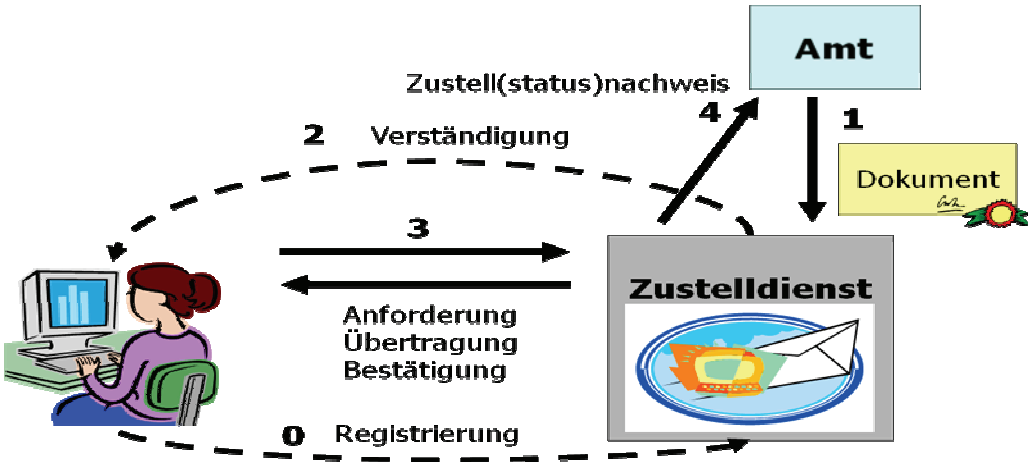

Abbildung 1: Der Ablauf der behördlichen elektronischen Zustellung

Quelle: [Reic04]

0. Der Bürger registriert sich mit der Bürgerkarte (siehe Abschnitt 4.4) bei einem behördlichen Zustelldienst
1. Die Behörde stellt fest, ob an den Bürger elektronisch zugestellt werden kann, und leitet daraufhin das Dokument an den Zustelldienst des Bürgers weiter.
2. Der Bürger erhält eine elektronische Verständigung vom Zustelldienst
3. Der Bürger signiert den elektronischen Zustellnachweis und erhält daraufhin Zugriff auf die Dokumente
4. Der Zustelldienst übermittelt den Zustellnachweis an die Behörde

Eine detaillierte Beschreibung des Ablaufs findet sich in Abschnitt 5.2 dieser Arbeit.

2.2.1 Die Bausteine

Der Prozeß der behördlichen elektronischen Zustellung besteht aus mehreren Bausteinen [HoRe04]:

- Ein Zustellkopf, der dazu dient, einer Behörde auf Anfrage mitzuteilen, ob und bei welchem Zustelldienst ein Bürger registriert ist.
- Der Zustelldienst, der dazu dient das Zustellstück von der Behörde anzunehmen und bis zur Abholung vom Bürger aufzubewahren.
  Es können mehrere behördliche sowie auch private Zustelldienste vorkommen [WWW01].
- Ein Verständigungssystem, das den Empfänger über die Hinterlegung eines Dokuments informiert. Die Verständigung kann elektronisch über E-Mail, SMS, Telefax oder Voicemail oder auch postalisch erfolgen [Feil06].

- Die Benutzerschnittstelle für die Abholung des Dokuments durch den Empfänger
- Dokumentation für spätere Nachforschungen über die erfolgten Zustellungen und Unzustellbarkeit

Eine genauere Beschreibung der Bausteine findet sich in Abschnitt 5.1 dieser Arbeit.

2.2.2 Aktuelle Entwicklung

Nach heutigem Stand (Frühjahr 2007), steht ein behördlicher Zustelldienst zur Verfügung. Dieser wird vom Bundeskanzleramt betrieben und ist unter der Adresse www.zustellung.gv.at erreichbar.
In weiterer Folge ist geplant, daß behördliche Zustelldienste vor allem von privaten Institutionen betrieben werden können [Posc06].

Obwohl die elektronische Zustellung schon seit dem Jahr 2005 möglich ist, hat sich das System in der Praxis noch nicht richtig durchgesetzt.
Folgende Gründe scheinen dafür verantwortlich:
Einerseits sind wenige Bürger für die elektronische Zustellung registriert, da die Anschaffung und Nutzung der dafür notwendigen Bürgerkarte als kompliziert und aufwendig angesehen wird [Baum06].
Andererseits bieten Behörden ein relativ spärliches Angebot und stellen derzeit beispielsweise nur Meldebestätigungen und Strafregisterauszüge elektronisch zu.

Als Ausweg wird die Einführung der **dualen Zustellung** angesehen. Die duale Zustellung ermöglicht die Vereinigung der elektronischen und konventionellen Zustellung unter einer Schnittstelle [WWW01]. Die Behörde kann unabhängig davon, ob an die Empfänger elektronisch zugestellt werden kann, Dokumente elektronisch absenden [Posc06]. Die Zustellung selbst erfolgt, gänzlich von der Behörde ausgelagert, durch den Zustelldienst, der, wenn möglich elektronisch, oder anderenfalls konventionell, in Papierform zustellt.
Die genaue Beschreibung des Konzepts der dualen Zustellung kann in [CeRo06] nachgelesen werden.

2.3 Die elektronische Zustellung im außerbehördlichen Umfeld

Nach heutigem Stand der Dinge existiert, wie bereits erwähnt, noch kein elektronisches Zustellsystem für das außerbehördliche Umfeld [Baum07a]. Als außerbehördliches Umfeld wird dabei das Kommunikationsumfeld zwischen natürlichen bzw. nicht natürlichen Personen untereinander bezeichnet.

Das behördliche System kann, aufgrund von rechtlichen (nur Behörden dürfen zustellen) und technischen (keine Antwort- bzw. Verrechnungsmöglichkeit, etc.) Einschränkungen, nicht im außerbehördlichen Umfeld eingesetzt werden [LaHe06].
Aus diesem Grund existieren seitens der Wirtschaft Pläne die elektronische Zustellung im außerbehördlichen Umfeld einzuführen [WWW12].

Um das System der elektronischen Zustellung im außerbehördlichen von dem im behördlichen Umfeld abzugrenzen, soll dafür eine eigene Bezeichnung etabliert werden, wobei Begriffe wie „elektronische Zusendung“ oder „elektronischer Einschreibbrief“ zur Auswahl stehen. In diversen projektinternen Dokumenten, wie z.B. in [Baum06], wird die Bezeichnung „kommerzielle elektronische Zustellung“ verwendet.

In dieser Arbeit werden fortfahrend die Begriffe „elektronische Zustellung im außerbehördlichen Umfeld“ und „kommerzielle elektronische Zustellung“ äquivalent verwendet.

2.3.1 Ziele

Um ein ausgereiftes Zustellsystem für das außerbehördliche Umfeld zur Verfügung zu haben werden folgende teilweise sich mit dem behördlichen Modell deckende Ziele bei der Entwicklung verfolgt [Tisc06]:

- Offenes System
  Das System soll zur Nachvollziehbarkeit der Vorgänge offen gestaltet werden. Spezifikationen sollen offen gelegt und es sollen keine proprietären Schnittstellen verwendet werden.

- Offener Anwenderkreis
  Die Nutzung des Systems soll für jedermann, d.h. für natürliche bzw. nicht natürliche Personen und des Weiteren auch für Behörden, offen sein..

- Zeit- und Ortsunabhängiger Zugang
  Absender bzw. Empfänger sollen Dokumente zu jeder Zeit und an jedem Ort versenden bzw. abholen können.

- Rechtliche und technische Sicherheit
  Die Zustellung, sowie die Authentizität und Integrität von Dokumenten soll eindeutig nachweisbar sein.
  Technisch erreicht man dies durch den Einsatz von digitalen Signaturen und durch Datenverschlüsselung. Rechtliche Sicherheit wird durch Einhaltung der gesetzlichen Regelung, insbesondere der Bestimmungen im Signaturgesetz [SigG99] gewährt.

- Optimierung des Workflows
  Der Workflow in Unternehmen soll verbessert und Medienbrüche vermieden werden [Baum07a].
  Der Absender kann ein elektronisch verfaßtes Dokument sofort gesichert abschicken. Das Dokument ist schnell für den Empfänger verfügbar und kann elektronisch weiterverarbeitet werden. Weiters besteht die Möglichkeit einer elektronischen Antwort an den Absender.

- Kosteneinsparung
  Die kommerzielle elektronische Zustellung soll zwar nicht gratis angeboten werden, aber zu einem wesentlich günstigeren Preis als die konventionelle Zustellung [Baum07a].

2.3.2 Aktuelle Entwicklung

In der Praxis läuft momentan (Frühjahr 2007) das Projekt „kommerzielle e-Zustellung“, das vom Verein „e-Zustellung Austria“ und „AUSTRIAPRO“ in Zusammenarbeit mit der Wirtschaftskammer Österreich gestartet wurde. Das Ziel des Projekts ist die Standardisierung und anschließende Umsetzung der kommerziellen elektronischen Zustellung [Baum07a].
Der aktuelle Stand des Projekts kann unter [WWW12] nachgelesen werden.

Durch die Einführung der kommerziellen elektronischen Zustellung wird erwartet, daß sich etliche Bürger bzw. Unternehmen für die behördliche elektronische Zustellung registrieren.

Synergien können vor allem dadurch auftreten, daß es Bürgern bzw. Unternehmen ermöglicht wird Dokumente an Behörden zu senden bzw. auf behördliche Zustellungen elektronisch zu antworten.

Eine weitaus größere Zielgruppe könnte durch die Bereitstellung der dualen Zustellung im außerbehördlichen Umfeld angesprochen werden. In absehbarer Zeit wird es dadurch zu einer Öffnung und Liberalisierung des Postmarktes kommen [LaHe06].
Das Konzept, das im Rahmen dieser Arbeit für die kommerzielle elektronische Zustellung entwickelt wird, lehnt sich an aktuelle Entwicklungen in der Praxis an.

3 Rechtliche Grundlagen

3.1 Für die behördliche elektronische Zustellung

Für die behördliche elektronische Zustellung gibt es eine fixe gesetzliche Regelung.
Der Grund dafür ist, daß die behördliche elektronische Zustellung von der staatlichen Verwaltung durchgeführt wird und die Verwaltung gemäß des Legalitätsprinzips in Artikel 18 des Bundesverfassungsgesetzes [BVG07], nur aufgrund von Gesetzen aktiv werden darf.

3.1.1 Zustellgesetz

In Österreich wurde durch die Novellierung des Zustellgesetzes [ZusG04] im Jahr 2004 die elektronische Zustellung von behördlichen Dokumenten an natürliche und nicht natürliche Personen ermöglicht.

Das Zustellgesetz wurde soweit geändert, daß heute die behördliche elektronische Zustellung gesetzlich der konventionellen Zustellung gleichwertig ist.
Im neu geschaffenen Abschnitt III des Gesetzes wird unter Anderem folgendes definiert:

- Die Aufgaben, die ein elektronischer Zustelldienst erfüllen muß. (siehe Abschnitt 5.1.3)
- Der Ablauf der behördlichen elektronischen Zustellung im Detail. (siehe Abschnitt 5.2)

3.1.2 E-Government-Gesetz

Das E-Government-Gesetz [EGovG04] ist am 1. März 2004 in Kraft getreten. Mittels E-Government-Gesetz wurde eine Grundlage geschaffen, die den elektronischen Verkehr zwischen Bürger und Behörde regelt. Das Szenario sieht vor, daß es Bürgern ermöglicht wird, Eingaben an Behörden auf elektronischem Weg durchzuführen und daß die Behörde im Gegenzug Dokumente elektronisch an den Bürger zustellen kann [DPW04.]
Das E-Government-Gesetz [EGovG04] befaßt sich nicht explizit mit der elektronischen Zustellung, sondern überwiegend mit der „eindeutigen Identifikation von Bürgern in Datenanwendungen“ mittels Bürgerkarte (Eine genaue Beschreibung der Bürgerkarte findet sich in Abschnitt 4.4).

Zur Identifikation wird laut § 6 des E-Government Gesetzes [EGovG04] die Stammzahl der betroffenen Person verwendet. Bei der Stammzahl handelt es sich bei natürlichen Personen um eine Ableitung aus der Zentralen Melderegister-Zahl, sowie bei nicht natürlichen Personen um die Firmenbuchnummer.

Das Verwenden der gleichen Stammzahl für alle behördlichen Verwaltungsbereiche rief bei der Datenschutzkommission Bedenken hervor [Krie05]. Aus diesem Grund wurde die Einführung eines für jeden Verwaltungsbereich eigenen bereichspezifischen Personenkennzeichens, kurz bPK, beschlossen, das aus der Stammzahl des Bürgers für jeden Verwaltungsbereich separat berechnet wird. Die Stammzahl des Bürgers bleibt dabei der Behörde verborgen [WWW11].

Bei der behördlichen elektronischen Zustellung werden Empfänger systemweit mittels Zustell-bPKs (bPK für den Bereich Zustellung) identifiziert.

3.2 Für die kommerzielle elektronische Zustellung

Für die kommerzielle elektronische Zustellung gibt es keine vorgegebene gesetzliche Regelung. Der Grund dafür ist, daß die kommerzielle elektronische Zustellung im Privatrechtsbereich angesiedelt ist und das Privatrecht auf dem Grundsatz der Privatautonomie basiert [Kuns06]. Dies bedeutet, daß Vereinbarungen zwischen natürlichen bzw. nicht natürlichen Personen frei innerhalb gesetzlicher Grenzen getroffen werden können. Die Normen des Privatrechts geben dazu nur einen gewissen Rahmen vor.

Im Speziellen existieren im Zustell- sowie im E-Government-Gesetz jedoch Bestimmungen, die explizit auf die kommerzielle elektronische Zustellung hinweisen.

3.2.1 Relevante Bestimmungen im Zustellgesetz

§ 28 (2) des Zustellgesetzes [ZusG04] erwähnt folgendes:

„Weitere Dienstleistungen, wie insbesondere die nachweisbare Zusendung von Dokumenten im Auftrag von Privaten, können in den Geschäftsbedingungen als fakultativer Vertragsinhalt angeboten werden. Für die nachweisbare Zusendung von Dokumenten im Auftrag von Privaten darf die Verteilerleistung (§ 30 Abs. 2 Z. 2) zu denselben Bedingungen wie für die Verteilung von behördlichen Dokumenten in Anspruch genommen werden“ [ZusG04].

Eine Begründung, warum sich § 28 (2) so im Gesetz wiederfindet, kann ein mögliches Entgegenkommen an die Wirtschaftstreibenden sein, die sich schon seit längerer Zeit eine Möglichkeit der nachweisbaren elektronischen Zustellung wünschen und somit eventuell behördliche Zustelldienste mitnutzen könnten [Kuns06].

Eine weitere Begründung dafür wird speziell im Satz „*Für die nachweisbare Zusendung von Dokumenten im Auftrag von Privaten darf die Verteilerleistung (§ 30 Abs. 2 Z. 2) zu denselben Bedingungen wie für die Verteilung von behördlichen Dokumenten in Anspruch genommen werden.“* [ZusG04] gesucht.
Dies bedeutet, daß durch das Gesetz die explizite Erlaubnis zur Abfrage des behördlichen Zustellkopfes gegeben wird.
Bei genauer Betrachtung ergibt sich daraus aber ein Nachteil für Personen, die nur für die Zustellung von privaten Dokumenten bei einem kommerziellen Zustelldienst registriert sind. Der Grund hierfür ist, daß im behördlichen Verzeichnis nur Personen aufscheinen, die sich zur Zustellung von behördlichen Dokumenten angemeldet haben [Kuns06].
Für die kommerzielle Zustellung soll entweder ein eigener Zustellkopf geschaffen werden oder mit der Behörde vereinbart werden, daß auch rein kommerzielle Zustelldienste vom behördlichen Zustellkopf referenziert werden können.

3.2.2 Relevante Bestimmungen im E-Government-Gesetz

Das E-Government-Gesetz [EGovG04] ermöglicht auch den Einsatz der Bürgerkarte zur Identifikation bzw. Authentifizierung im außerbehördlichen Umfeld. Der Gesetzgeber erwartet, daß durch den vermehrten Einsatz der Bürgerkarte Synergieeffekte entstehen [Kuns06].

Für den privatrechtlichen Bereich wird deshalb laut § 14 des E-Government-Gesetzes [EGovG04] ein zum bPK analoges wirtschaftsbereichspezifisches Personenkennzeichen, kurz wbPK eingeführt, das aus der Stammzahl des Bürgers abgeleitet wird [WWW11].

Das wbPK kann zur Identifikation bzw. Authentifizierung bei der kommerziellen elektronischen Zustellung verwendet werden.

3.3 Für die elektronische Signatur

Die elektronische Signatur bietet eine rechtlich sichere Möglichkeit elektronische Dokumente mit einer Unterschrift zu versehen [WWW01].

Beim Begriff „elektronische Signatur“ handelt es sich um einen juristischen Fachausdruck. Die technische Realisierung erfolgt mittels digitaler Signaturen. (siehe Abschnitt 4.3)
Den rechtlichen Rahmen von elektronischen Signaturen bildet das Signaturgesetz [SigG99] und die Signaturverordnung [SigV04]. Das Signaturgesetz beruht dabei auf einer EU-Richtlinie für elektronische Signaturen [SigR99]. Österreich war einer der ersten EU-Staaten, der diese Richtlinie in einem Gesetz implementiert hat. In der Praxis unterscheidet man, je nach Anwendungsbereich, folgende Kategorien von elektronischen Signaturen [WWW01]:

- Die sichere elektronische Signatur
  Einer sicheren elektronischen Signatur ist die höchste Qualitätsstufe zuzuordnen und ist, bis auf wenige Ausnahmen, wie z.B. im Erb- und Familienrecht, der eigenhändigen Unterschrift gleichzusetzen [SigG99].
  Laut § 2 (3) des Signaturgesetzes [SigG99] dient die sichere elektronische Signatur zur persönlichen Identifikation und darf ausschließlich dem Signator zugeordnet sein.
  Die sichere elektronische Signatur muß auf einem qualifizierten Zertifikat beruhen und mittels sicherer Hardware, wie z.B. Chipkarten erstellt werden.
  Eine nachträgliche Veränderung der signierten Daten muß ebenfalls feststellbar sein.

- Die fortgeschrittene elektronische Signatur
  Der Begriff der fortgeschrittenen elektronischen Signatur ist nicht im Signaturgesetz angeführt, sondern wird in der Richtlinie der Europäischen Union über elektronische Signaturen [SigR99] angeführt.
  Die fortgeschrittene elektronische Signatur kann mittels eines einfachen Zertifikats erstellt werden und die technischen Anforderungen zur Erstellung sind geringer als bei der sicheren elektronischen Signatur [WWW01].

- Die Verwaltungssignatur

  Bei der Verwaltungssignatur handelt es sich um eine elektronische Signatur, die bei E-Government Anwendungen der sicheren elektronischen Signatur gleichgestellt ist. Laut Definition im E-Goverment-Gesetz [EGovG04] soll der Zugang zum E-Government dadurch erleichtert werden. Der Einsatz der Verwaltungssignatur ist derzeit bis Ende 2007 befristet, wird aber vorrausichtlich verlängert werden. Der Unterschied zur sicheren elektronischen Signatur ist nur gering. So können beispielsweise private Schlüssel auch auf sicheren Servern abgelegt werden, wodurch die Handy-Signatur ermöglicht wird [WWW01].

- Die Amtssignatur

  Die Amtssignatur ist eine spezielle elektronische Signatur im Sinne des Signaturgesetzes [SigG99], die von Seiten der Behörde auf ein elektronisch zuzustellendes Dokument angebracht wird. Ein Merkmal ist die unverkennbare Bildmarke, die als Kennzeichnung eines amtlichen Dokuments dient.

  Das Aussehen der Amtssignatur wird in Abbildung 2 dargestellt:

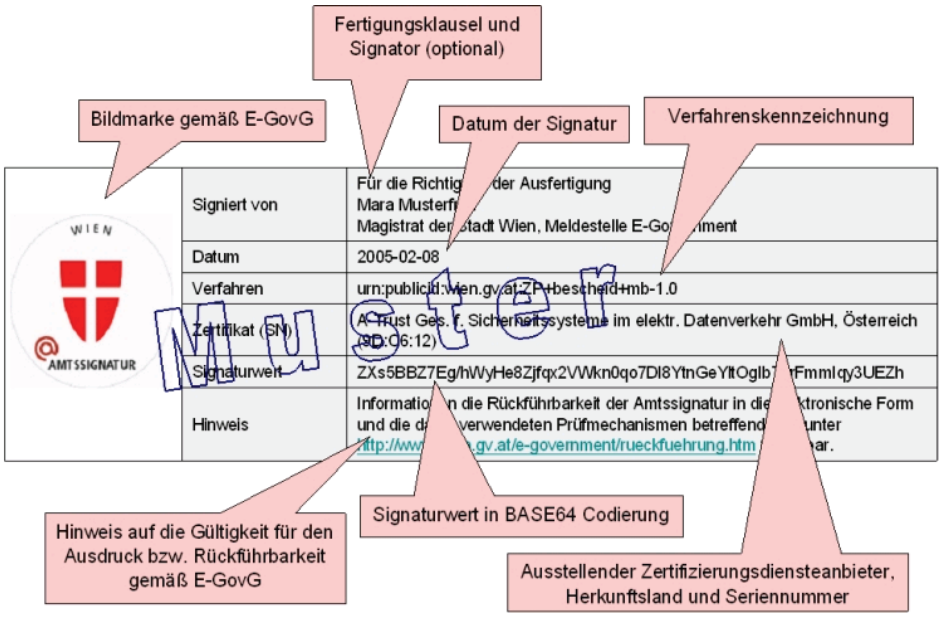

Abbildung 2: Aussehen und Komponenten der Amtssignatur

Quelle: [Wimm05]

Wenn auf einem elektronisch zugestellten Dokument eine Amtssignatur angebracht wurde, gilt für das ausgedruckte Dokument die Vermutung der Echtheit. [Wimm05]. (siehe Abschnitt 3.4.3)

- Die Stapelsignatur
  Bei einer Stapelsignatur handelt es um das Signieren eines „Stapels von Dokumenten“ in einem einzigen Signaturvorgang. Das bedeutet, daß bei Stapelsignaturen die Autorisierung nur einmalig durchgeführt werden muß, aber mehrere Dokumente gleichzeitig signiert werden. Dabei wird aber für jedes Dokument eine eigene Signatur erstellt [WWW01].
  Wenn man mittels des Stapelsignaturverfahrens sichere elektronische Signaturen automatisiert erstellen will, tritt ein rechtliches Problem auf:

  Laut § 4 (2) der Signaturverordnung [SigV04] müssen alle zu signierenden Dokumente vor Auslösen des Signaturvorgangs dem Signator vorliegen und bekannt sein.
  Außerdem müssen laut § 18 (2) des Signaturgesetzes [SigG99] die zu signierende Dokumente vor dem Auslösen des Signaturvorgangs angezeigt werden.
  Dies bedeutet, daß es gemäß gesetzlicher Regelung derzeit in Österreich nicht möglich ist automatisiert für eine unbestimmte Anzahl an Dokumenten sichere elektronische Signaturen zu erstellen.

  Die gesetzliche Regelung bezieht sich aber nur auf sichere elektronische Signaturen. Alle anderen Formen von elektronischen Signaturen können im Stapelverfahren erstellt werden [WWW01].

3.4 Beweiskraft elektronisch zugestellter Dokumente

Aus juristischer Sicht ist es besonders interessant abzuschätzen, wie groß die Beweiskraft elektronisch zugestellter Dokumente in einem etwaigen gerichtlichen Beweisverfahren ist und welche Folgen daraus für die Betroffenen entstehen [Kuns06].

3.4.1 Unterschiede in der Beweiskraft

Einem behördlich elektronisch zugestellten Dokument kommt nach der Novelle des Zustellgesetzes [ZusG04] die gleiche Beweiskraft wie einem herkömmlichen RSa- oder RSb-Brief zu.
Die Beweiskraft eines kommerziell elektronisch zugestellten Dokuments ist gesetzlich nicht festgelegt und obliegt daher der freien Beweiswürdigung. Unter freier Beweiswürdigung versteht man, daß ein Gericht im Beweisverfahren die zu beweisende Tatsache nach freier Überzeugung für wahr oder falsch halten kann [Rech03].

3.4.2 Vergleich der Beweiskraft

Da es sich bei der kommerziellen Variante der elektronischen Zustellung, um eine neue Entwicklung handelt, sind noch keine Erfahrungswerte vorhanden, wie ein Gericht in der Praxis kommerziell elektronisch zugestellte Dokumente als Beweismittel beurteilt. Deshalb stellt Kunst [Kuns06] einen hypothetischen Vergleich der Beweiskraft elektronisch zugestellter Dokumente mit der von herkömmlichen schriftlichen Formen auf. Der Vergleich baut dabei auf die zwei wesentlichen Sachverhalte auf, die im Zusammenhang mit Sendungen zu Streitigkeiten führen können. Diese sind der Zugang des Dokuments und die Unverfälschtheit des Dokumenteninhalts.

- Der Brief
  Bei einem herkömmlichen Brief liegt die Beweislast, ob der Brief beim Empfänger angekommen ist, beim Absender. Damit der Absender die Zustellung des Briefes auch wirklich beweisen kann, ist der Brief eingeschrieben aufzugeben.
  Der Inhalt des Briefes wird in der Regel nicht angezweifelt wenn dieser mit einer nachweisbar eigenhändigen Unterschrift versehen wurde.

- Das Telefax
  Bei einem Telefax kann die Sendung und der Empfang eines Dokuments bestätigt werden. Es wird jedoch nicht näher beschrieben wie stark die Beweiskraft der Bestätigung ist.
  Der Inhalt des Faxes besitzt nur eine geringe Beweiskraft. da selbst, wenn das Originaldokument mit einer eigenhändigen Unterschrift versehen wurde, die Unterschrift auf der Faxkopie, laut Urteil des obersten Gerichtshofes (OGH, 27.3.1995, 1 Ob 515/95), als nicht eigenhändig anzusehen ist.

- Die E-Mail
  E-Mails unterliegen im Regelfall bezüglich des Empfangs und des Inhalts der freien Beweiswürdigung.
  In vielerlei Hinsicht wird deshalb E-Mails keine allzu große Beweiskraft zugeordnet. Der Inhalt von E-Mails läßt sich sehr leicht verfälschen und ebenso ist es nicht einfach festzustellen, ob eine E-Mail wirklich empfangen wurde. Als einzige Ausnahme bezüglich des Inhalts sind die mit einer digitalen Signatur versehenen E-Mails anzusehen.

Aufgrund der Erkenntnisse aus dem Schriftformenvergleich schließt Kunst [Kuns06] auf die Beweiskraft des elektronisch zugestellten Dokuments folgendermaßen:

Elektronisch zugestellte Dokumente unterliegen, wie bereits beschrieben, der freien Beweiswürdigung. Die Beweiskraft erhöht sich aber, da die Absendung und der Empfang eines Dokumentes, sowie die Authentizität und Integrität des Inhalts nachgeprüft werden kann.
Die Schlußfolgerung daraus ist, daß elektronisch zugestellten Dokumenten aufgrund der erwähnten Tatsachen, trotz fehlender gesetzlicher Beweisvorschriften eine hohe Beweiskraft bei Gericht zugeordnet werden wird.

3.4.3 Beweiskraft von Ausdrucken

Laut § 20 des E-Government Gesetzes [EGovG04] besitzt ein Ausdruck eines behördlich elektronisch zugestellten Dokuments nur dann Beweiskraft, wenn das ausgedruckte Dokument mit einer Amtssignatur versehen wurde und elektronisch rückführbar ist. Konkret bedeutet dies, daß die elektronische Signatur nachrechenbar sein muß [Kast05].
Von der zustellenden Behörde muß ein Internetdienst angeboten werden, der es erlaubt ein ausgedrucktes Dokument wieder elektronisch zu erfassen.

Um die elektronische Signatur korrekt nachrechnen zu können, muß die händische Eingabe des Dokuments jedoch gänzlich fehlerlos geschehen. Wenn bei der Eingabe auch nur ein Fehler passiert (z.B. a statt ä), ist das Dokument nicht mehr authentisch und die Prüfung der elektronischen Signatur wird fehlschlagen [Kast05].
Die Prüfung der elektronischen Signatur ist deshalb so strikt geregelt, weil sie maschinell durchgeführt wird und eine Maschine dabei jedes Zeichen genau verifiziert.

Kastner [Kast05] kritisiert die fehlende Benutzerfreundlichkeit bei der Verifikation eines gedruckten Dokuments, besonders deswegen, weil bei der Eingabe keine Fehler gemacht werden dürfen. Des Weiteren wird die Eingabe von längeren Dokumenten als langwierig und die Rückführung von Bildern als unmöglich angesehen.

Es ist anzunehmen, daß Ausdrucken von kommerziell zugestellten Dokumenten ebenfalls Beweiskraft zugeordnet werden wird, wenn ebenfalls die Möglichkeit der Rückführung und die Validierung der elektronischen Signatur ermöglicht wird.

4 Technische Grundlagen

4.1 Serviceorientierte Architekturen und Webservices

Bei serviceorientierten Architekturen (SOA) [SOA06] handelt es sich um ein spezielles Softwarearchitekturkonzept. Eine SOA zeichnet sich dadurch aus, daß sie modular aus einzelnen voneinander unabhängigen Services aufgebaut ist und erst zur Laufzeit ermittelt wird, welche Services benötigt und von wem diese angeboten werden [DGH03].

In der Praxis werden SOA meist in Form von Webservice Architekturen [WSA04] implementiert [Haus04].
Ein Webservice ist per Definition eine Software-Komponente, die über das Internet erreichbar ist und für die Kommunikation mit anderen Maschinen, Schnittstellen in einem standardisierten und maschinenlesbaren Format zur Verfügung stellt [WSA04].

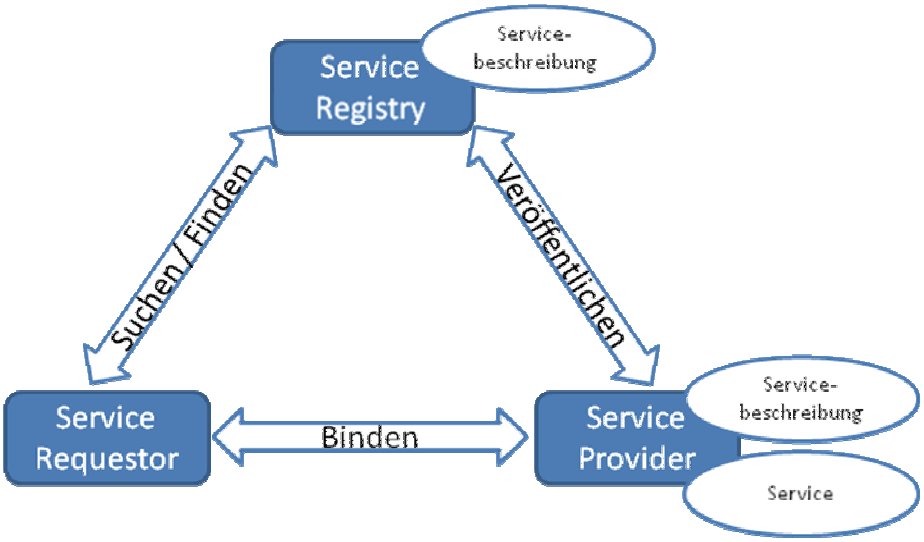

Abbildung 3: Serviceoriente Architektur
Quelle: [Kreg01]

Grundsätzlich besteht eine SOA aus folgenden drei Komponenten [Kreg01]:

- Service Provider
  Der Service Provider stellt verschiedene Services zur Verfügung. Die dazugehörige Beschreibung erfolgt im Regelfall XML [XML06] basiert mittels der Webservices Description Language (WSDL) [WSDL07].

- Service Requestor
  Der Service Requestor benötigt ein bestimmtes Service zur Erfüllung einer Aufgabe und nimmt dafür die Services des Service Providers in Anspruch.

- Service Registry
  Die Service Registry ist ein Verzeichnisdienst, dessen Spezifikation in vielen Fällen dem UDDI-Standard [UDDI04] entspricht, indem die vom Service Provider angebotenen Services veröffentlicht werden. Der Service Requestor kann durch Abfrage des Verzeichnisses das gewünschte Service finden.

Für die Kommunikation zwischen den einzelnen Komponenten wird das Simple Object Access Protocol (SOAP) [SOAP00] verwendet [Kreg01]. Das Datenformat einer SOAP Nachricht wird mittels eines XML Schemas [XSD04] definiert. Die Übertragung der Nachrichten erfolgt in den meisten Fällen über HTTP [HTTP99].
Außerdem können Dokumente verschiedener MIME-Typen [MIME96] als Anhang einer SOAP Message mittels SOAP with Attachments (SwA) [SwA06] mitgesendet werden.

4.2 Asymmetrische Kryptoverfahren

Asymmetrische Kryptoverfahren werden zur Ver- und Entschlüsselung von Daten und zur Bildung von digitalen Signaturen (siehe Abschnitt 4.3) angewandt.
Es kommt dabei ein Schlüsselpaar bestehend aus einem öffentlichen Schlüssel (Public Key), der zum Verschlüsseln der Daten und einem privaten Schlüssel (Private Key), der zum Entschlüsseln verwendet wird, zum Einsatz.
Details können in [Schn96] nachgelesen werden.

Die Anwendung asymmetrischer Kryptoverfahren wurde von den RSA Laboratories [WWW14] in den Public-Key Cryptography Standards (PKCS) spezifiziert.

Für die elektronische Zustellung sind davon folgende relevant:

- PKCS #1: RSA Cryptography [PKCS1]
  Spezifiziert die Ver- und Entschlüsselung von Daten unter Zuhilfenahme des RSA-Verfahrens [RSA78].

- PKCS #7: Cryptographic Message Syntax (CMS) [PKCS7]
  Spezifiziert eine Syntax für das Verschlüsseln und Signieren einer Nachricht innerhalb einer Public-Key-Infrastruktur (für Details siehe [Weis01]). Außerdem bildet PKCS #7 die Basis für den S/MIME [SMIM99] Standard.

4.3 Digitale Signaturen

Mittels digitaler Signaturen kann die Echtheit (Integrität) und Unverfälschtheit (Authentizität) von Dokumenten sichergestellt werden [Bert03].
Digitale Signaturen basieren in der Regel auf asymmetrischen Kryptoverfahren [Schw05].

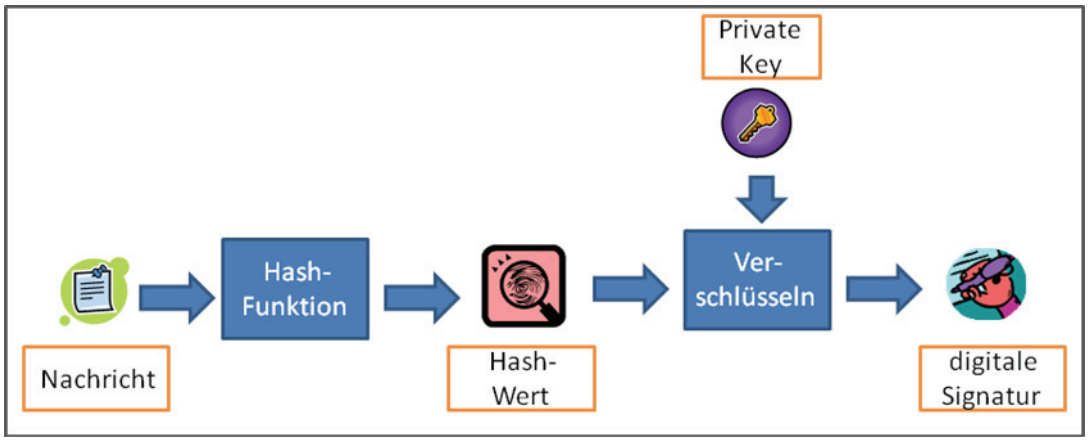

Abbildung 4: Bildung einer digitalen Signatur

Die Bildung einer digitalen Signatur, die in Abbildung 4 illustriert wird, läuft folgendermaßen ab:

1. Berechnung des Hash-Wertes, des sogenannte elektronischen Fingerabdrucks der Nachricht.
2. Verschlüsselung des Hash-Wertes der Nachricht mit dem privaten Schlüssel des Signators.

Das Resultat des Verfahrens ist die digitale Signatur, die zusammen mit der ursprünglichen Nachricht die signierte Nachricht bildet [Bert03].

Der Hash-Wert kann mittels des öffentlichen Schlüssels des Signators (der meistens mit dem Dokument mitgeschickt wird oder Online abrufbar ist) entschlüsselt werden.

Der Signator kann dadurch beweisen, daß die Signatur von ihm stammt, da nur er in der Lage war die Nachricht mit seinem privaten Schlüssel zu verschlüsseln [Bert03].

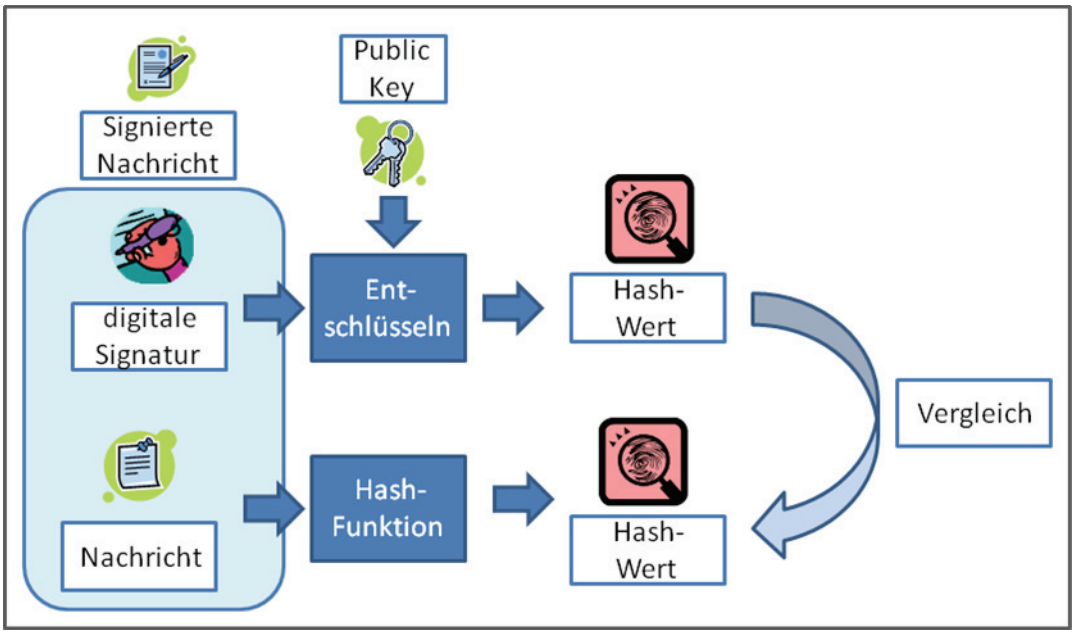

Abbildung 5: Verifikation einer digitalen Signatur

Die Verifikation einer digitalen Signatur, die in Abbildung 5 veranschaulicht wird, läuft folgendermaßen ab:

1. Die digitale Signatur wird mit dem öffentlichen Schlüssel entschlüsselt, um den vorher verschlüsselten Hash-Wert wieder im Klartext vorliegen zu haben.
2. Der Hash-Wert wird aus der Nachricht selbst neu berechnet.
3. Zur Gültigkeitsprüfung werden die beiden Hash-Werte miteinander verglichen.

Stimmen beide Hash-Werte überein, ist die Signatur gültig und man kann annehmen, daß das Dokument unverfälscht ist.
Ergeben sich zwei unterschiedliche Hash-Werte ist anzunehmen, daß der Inhalt des Dokuments verändert wurde. Schon die Veränderung von nur einem Zeichen ergibt einen anderen Hash-Wert [Schw05].

Durch das soeben vorgestellte Verfahren kann die Integrität des Dokuments bewiesen werden. Um auch die Authentizität zu gewährleisten benötigt man ein sogenanntes Zertifikat.

Zertifikate dienen dazu den öffentlichen Schlüssel an eine bestimmte Person zu binden und gelten bei der Verwendung im Internet als Äquivalenz zu einem amtlichen Lichtbildausweis [Schw05].
Die Ausstellung eines Zertifikats geschieht in der Regel durch eine staatlich anerkannte Zertifizierungsstelle. Der Antragsteller muß in der Regel dort selbst vorsprechen und sich mit einem Ausweis identifizieren. Die Zertifizierungsstelle bestätigt mit ihrer eigenen digitalen Signatur, daß der vergebene öffentliche Schlüssel genau einer Person zugeordnet ist [Bert03].
Als Standard wird der ITU-Standard X.509 [X509] angesehen. Dabei handelt es sich quasi um einen Verzeichnisdienst für Zertifikate, dessen Struktur weltweit einheitlich vorgegeben ist [Schw05].

4.3.1 XML-Signaturen

XML Dokumente können ebenfalls mit einer digitalen Signatur versehen werden.
Dafür wurde vom World Wide Web Consortium (W3C) die Empfehlung „XML-Signature Syntax and Processing“ [DSIG02] herausgegeben, die die Anwendung und Interpretation von digitalen Signaturen auf XML Dokumente [XML06] beschreibt.

Das Anbringen einer digitalen Signatur auf ein XML Dokument funktioniert im Grunde gleich wie auf ein normales Dokument, allerdings tritt bei der Berechnung des Hash-Wertes folgendes Problem auf:
Eine unterschiedliche Anzahl von Leerzeichen hat keinen Einfluss auf die Gültigkeit von XML Dokumenten, jedoch sehr wohl Einfluss auf die zu berechnenden Hash-Werte. Da die Verifikation einer digitalen Signatur über das Vergleichen der Hash-Werte geschieht, dürfen sich die Hash-Werte keinesfalls unterscheiden.
Als Ausweg dafür wurde ein eigenes Verfahren, das Kanonisierung („Gleichmachen“) [CAN01] genannt wird, entwickelt. Hierbei werden überflüssige Leerzeichen entfernt, wodurch sichergestellt ist, daß für dasselbe Dokument immer der gleiche Hash-Wert berechnet wird.
Man unterscheidet drei Arten von XML-Signaturen [DSIG02]:

- Die Enveloping Signature
  Dabei umschließt der Signature Tag die signierten Daten quasi wie eine Klammer.

- Die Enveloped Signature
  Dabei ist der Signature Tag ein Teil der signierten Daten, wird aber nicht zur Berechnung des Hashwertes herangezogen

- Die Detached Signature
  Dabei enthält der Signature Tag Referenzen auf die signierten Daten.

4.3.2 Zeitstempel

Bei einem Zeitstempel handelt es sich um einen Wert, der einem bestimmten Ereignis, wie beispielsweise dem Absenden oder dem Empfangen eines Dokuments, einen Zeitpunkt zuordnet [TSP01].
Damit objektiv die Erzeugung eines Zeitstempels möglich ist, ist eine Timestamp-Authority, kurz TSA, erforderlich.
Die Erstellung eines Zeitstempels geschieht wie folgt:

1. Die TSA empfängt den Hash-Wert der Daten.
2. Die TSA signiert den Hash-Wert digital mit einem nur für diesen Zweck verwendeten privaten Schlüssel.
3. Die TSA erstellt ein Dokument auf dem der digital signierte Hash-Wert, mitsamt dem genauen Signaturzeitpunkt abgebildet ist.

Durch die Signierung des Hash-Werts durch die TSA wird die Authentizität des Hash-Wertes bestätigt [Kast05].

4.4 Die Bürgerkarte

Bei der Bürgerkarte handelt es sich im Grunde nicht um eine reale physische Karte, sondern um ein Modell, das dem Bürger unterschiedliche Funktionen für den E-Government und E-Commerce Bereich bereitstellt [WWW02].
In der Praxis wird meistens eine Chipkarte, wie z.B. eine dezidierte Signaturkarte, eine maestro-Bankomatkarte oder die e-card der Sozialversicherung als Bürgerkarte verwendet. Zur Nutzung der Bürgerkarte wird ein Chipkartelesegerät und eine spezielle Software, die Bürgerkartenumgebung genannt wird, benötigt.
Andererseits ist es heute bereits möglich, das Handy als Bürgerkarte zu verwenden. Dafür wird von der „Mobilkom Austria“ der Dienst „A1 Signatur“ angeboten [WWW13].

4.4.1 Das Modell

Das Modell der Bürgerkarte besteht, wie in Abbildung 6 dargestellt, aus fünf Komponenten [HoKa04]:

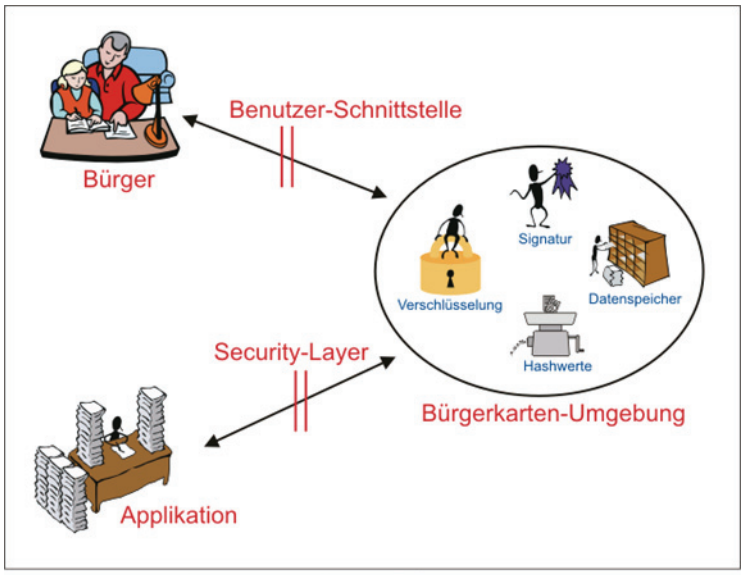

Abbildung 6: Das Modell der Bürgerkarte
Quelle: [HoKa04]

- Die Applikation
  Bei der Applikation handelt es sich entweder um eine E-Government Anwendung, wie z.B. die elektronische Zustellung oder um eine E-Commerce Anwendung, wie z.B. Online-Banking.

- Die Bürgerkarten-Umgebung
  Die Bürgerkarten Umgebung ist eine Anwendung, die entweder lokal am eigenen Rechner ausgeführt wird (lokale Bürgerkarten-Umgebung), oder als serverseitiger Dienst (serverbasierte Bürgerkarten-Umgebung), der z.B. über das Internet erreichbar ist.
  Dabei handelt es sich um einen Container, in dem die, in Abschnitt 4.4.2 beschriebenen, Funktionen der Bürgerkarte zusammengefaßt sind

- Der Security-Layer
  Der Security-Layer ist jene Schnittstelle, über die die Kommunikation zwischen der Applikation und der Bürgerkarten-Umgebung stattfindet.

- Die Benutzerschnittstelle
  Die Benutzerschnittstelle ermöglicht die Kommunikation zwischen Bürger und Bürgerkarten-Umgebung.

- Der Bürger
  Der Bürger ist jene Person, die die Funktionen der Applikation und der Bürgerkarten-Umgebung anwendet. In der Regel handelt es sich dabei nicht um den Bürger selbst, sondern um eine spezifische E-Government oder E-Commerce Anwendung.

4.4.2 Die Funktionen

Die drei Kernfunktionen der Bürgerkarte stellen sich wie folgt dar [Posc02]:

- Erstellen einer elektronischen Signatur
  Das Erstellen einer elektronischen Signatur wird als Schlüsselfunktion der Bürgerkarte bezeichnet [Posc02]. Auf der Bürgerkarte wird dazu ein qualifiziertes Zertifikat gespeichert, wodurch einem breiten Spektrum an Bürgern ermöglicht wird rechtsgültige elektronische Signaturen zu erstellen.

- Personenbindung
  Da das auf der Bürgerkarte vorhandene Signaturzertifikat nur den Namen des Bürgers beinhaltet, wurde für die sogenannte Personenbindung als zusätzliche Identifikationsfunktion implementiert.

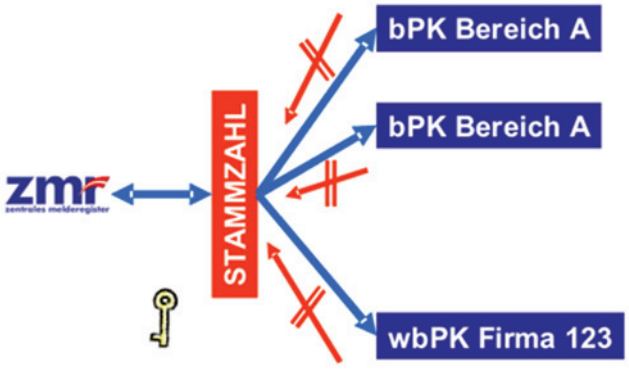

Abbildung 7: Ableitung der Stammzahl und des Personenkennzeichens

Quelle: [WWW01]

In der Personenbindung wird die aus der Zahl des Eintrags im zentralen Melderegister (ZMR-Zahl) mittels starker Verschlüsselung abgeleitete Stammzahl der betroffenen Person gespeichert [WWW02].

In einem Verwaltungsverfahren bzw. bei einer E-Commerce Anwendung wird nicht die Stammzahl direkt verwendet, sondern das bereichspezifische Personenkennzeichen (bPK) (siehe Abschnitt 3.1.2) bzw. das wirtschaftsbereichspezifische Personenkennzeichen (wbPK) (siehe Abschnitt 3.2.2).
Die Berechnung des bPKs bzw. des wbPKs erfolgt mittels Einwegableitungen aus der Stammzahl. Die genauen Berechnungsverfahren sind in [HoHo04] spezifiziert.

- Datenspeicher
  Die Bürgerkarte kann auch als Datenspeicher verwendet werden. Technisch gesehen wird der Speicherplatz in mehrere logische Datenbereiche, sogenannte Infoboxen, unterteilt. Jeder Anwendung wird im Regelfall eine dezidierte Infobox zur Verwendung zugewiesen. Der Zugriff auf die Infoboxen kann entweder paßwortgeschützt sein oder frei vonstatten gehen. Weiters können die Daten in der Infobox auch verschlüsselt vorliegen.

4.5 Module für Online Applikationen

Die Module für Online Applikationen, die Dienste im Bereich der elektronischen Signatur anbieten, wurden vom Bundeskanzleramt und vom Bundesministerium für Finanzen entwickelt, um ein sicheres Online-Verwaltungsverfahren durchführen zu können. Diese Module bilden das Gegenstück auf der Seite der Verwaltung zur sogenannten Bürgerkartenumgebung des Bürgers [WWW09].
Die Module können sowohl im behördlichen, als auch im außerbehördlichen Umfeld lizenzkostenfrei eingesetzt werden.

Bei der elektronischen Zustellung finden folgende Basismodule Anwendung:

- MOA-ID [ScMo06] für die Identifikation und Authentifizierung
  Das Modul MOA-ID, kurz für MOA-Identifikation, dient dazu um den Bürger, zu authentifizieren. Mit Hilfe des MOA-ID Moduls wird auch das bereichsspezifische Personenkennzeichen (kurz bPK) des Bürgers für einen bestimmten Behördenbereich berechnet [WWW09].
  Im außerbehördlichen Umfeld kann das Modul in einem eigenen MOA-WID Modus betrieben werden.

- MOA-SS [MSSSP04] zur Signaturerstellung
  Das Modul MOA-SS, kurz für MOA-Serversignatur, erzeugt elektronische Signaturen für Dokumente. Bei den Signaturen handelt es sich um elektronische Signaturen, die den Vorgaben des Signaturgesetzes [SigG99] entsprechen [WWW09].

- MOA-SP [MSSSP04] für die Signaturprüfung
  Das Modul MOA-SP, kurz für MOA-Signaturprüfung, dient zur Verifikation digitaler Signaturen.

Außerdem wurde für die behördliche elektronische Zustellung ein eigenes MOA-ZS [NaLi04] Basismodul entwickelt. Eine genaue Beschreibung dazu findet sich in Abschnitt 5.1.2 dieser Arbeit.

5 Beschreibung der behördlichen elektronischen Zustellung

5.1 Beschreibung der Softwarearchitektur

Der Aufbau des behördlichen Zustellsystems ist komponentenbasiert und entspricht im Grunde dem einer serviceorientierten Architektur.

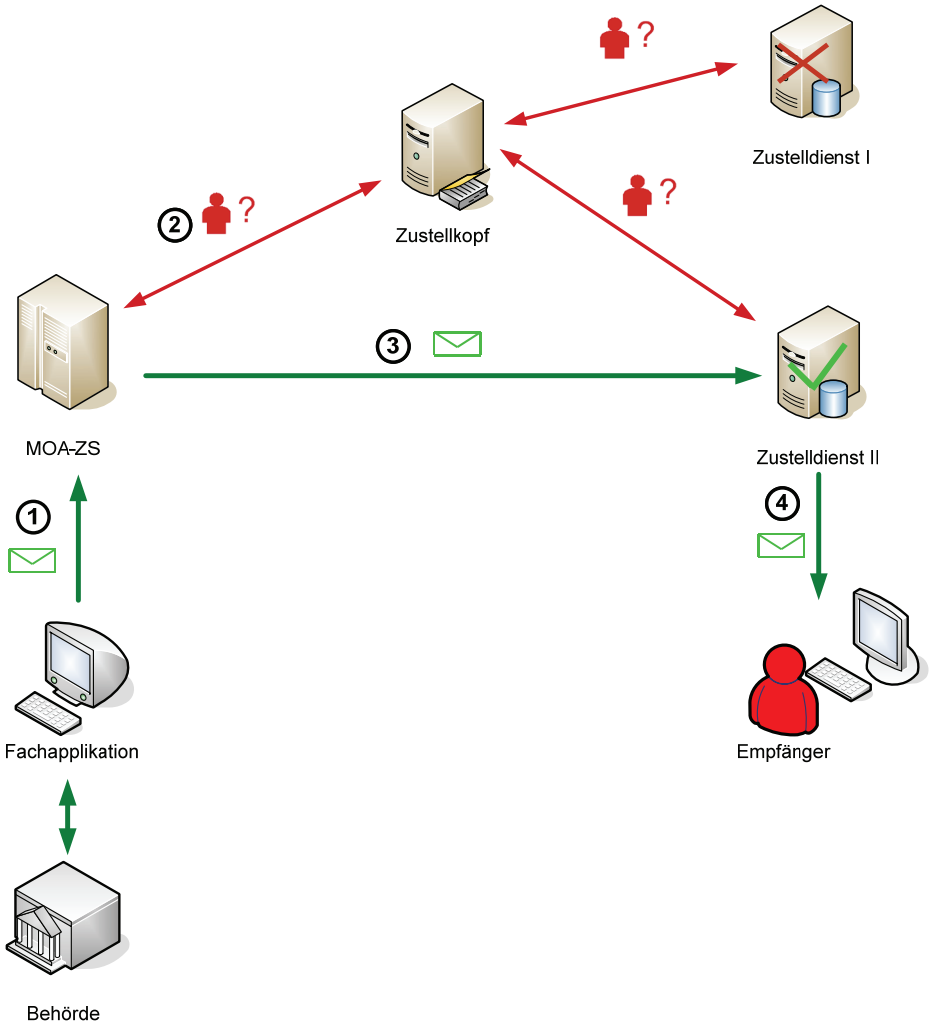

Abbildung 8: Das Komponentenmodell der behördlichen e-Zustellung

Im Modell übernehmen das MOA-ZS Basismodul die Rolle des Service Requesters und der Zustelldienst die des Service Providers. Der Zustellkopf fungiert als Service Register.

Die behördliche elektronische Zustellung ist bisweilen die erste SOA, die in der öffentlichen Verwaltung implementiert wurde.

5.1.1 Die Applikation

Die Applikation dient der Behörde als Werkzeug zur Durchführung der elektronischen Zustellung und erledigt dabei folgende Aufgaben:

- Verfassen von Dokumenten
- Anbringen der Amtssignatur mittels des Behördenzertifikats (Object Identifier der öffentlichen Verwaltung) [Holl06]
- Anfrage beim Zustellkopf ob an den gewünschten Empfänger elektronisch zugestellt werden kann.
- Verschlüsselung des Dokuments wenn der Public Key des Empfängers bekannt ist
- Auswahl des Zustelldiensts über den das Dokument zugestellt werden soll
- Übergabe des Dokuments an den Zustelldienst
- Übernahme von Statusmeldungen und Zustellnachweisen

In der Praxis wurden unter Anderem folgende Applikationen entwickelt:

- Sichere Signatur aus Office 2007
  Dabei handelt es um ein Plug-In für Microsoft Word 2007, das die Erstellung von sicheren elektronischen Signaturen aus Microsoft Word heraus ermöglicht. Darüber hinaus unterstützt es das Versenden von Dokumenten mittels elektronischer Zustellung [WWW04].

- Fabasoft XZS
  Fabasoft, ein Hersteller von E-Government Software in Österreich, bietet mit Fabasoft XZS, als Zusatzprodukt zur eGov-Suite, eine für die elektronische Zustellung spezifizierte Anwendung an [WWW06].

5.1.2 Das Modul für Online Applikationen Zustellung

Das MOA-ZS Basismodul [NaLi04] dient dazu, um Applikationen den Zugang zur elektronischen Zustellung zu erleichtern, in dem es Schnittstellen zur Interaktion mit dem Stammzahlenregister, dem Zustellkopf, dem MOA-SS Basismodul und dem Zustellserver zur Verfügung stellt.
Die Applikation muß folglich nur mehr die eine Schnittstelle zum MOA-ZS implementieren.

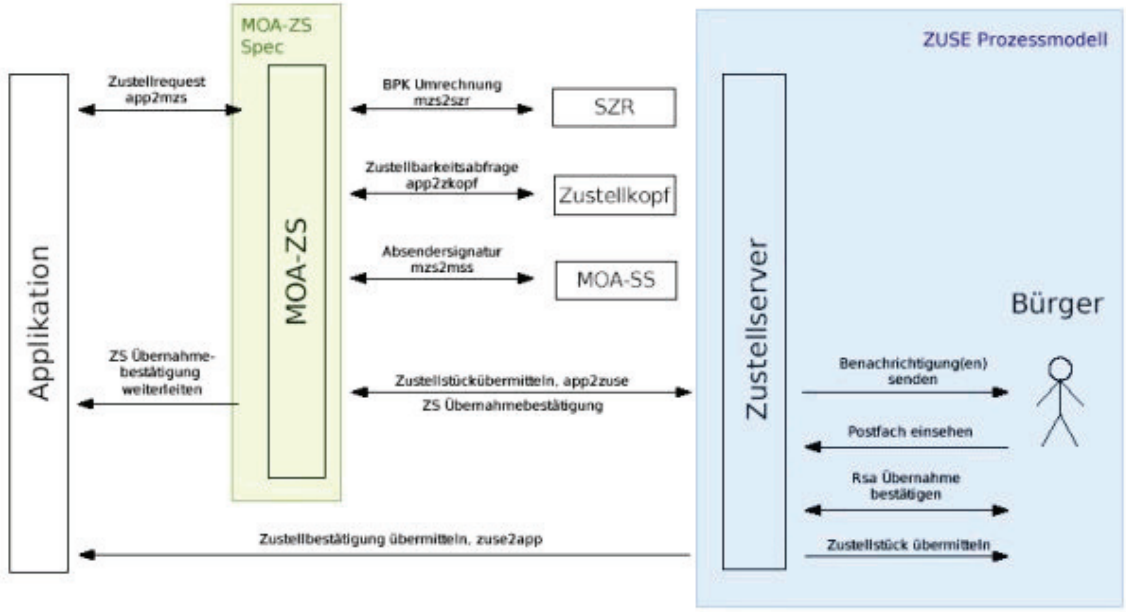

Abbildung 9: MOA-ZS als Middleware
Quelle: [WWW09]

In Abbildung 9 wird der Prozeß der elektronischen Zustellung unter Verwendung des MOA-ZS Moduls als Middleware illustriert.
Das MOA-ZS stellt folgende Funktionalität, in den meisten Fällen durch Aufruf von externen Anwendungen, zur Verfügung [NaLi04]:

- Annahme der Dokumente von der Applikation
- Berechnung des verschlüsselten Zustell-bPKs aus dem bPK beim Stammzahlregister
- Durchführung von Einfach- und Mehrfachanfragen beim Zustellkopf
- Anbringen der Amtssignatur mittels MOA-SS
- Verschlüsselung des Dokuments wenn Public Key des Empfängers bekannt ist
- Übergabe des Dokuments an den Zustelldienst

5.1.3 Der Zustelldienst

Beim Zustelldienst handelt es sich um einen Server, der folgende Aufgaben übernimmt [NaRe04]:

- Verwaltung von elektronischen Postfächern
- Entgegennahme von Dokumenten von der absendenden Applikation
- Verständigung des Empfängers
- Senden von Statusmeldungen und Zustellnachweisen an die Applikation
- Protokollierung der Vorgänge
- Führen eines Verzeichnisdienstes (gemäß § 28 (1) des Zustellgesetzes [ZusG04]) mit Daten der registrierten Personen, der vom Zustellkopf abgefragt werden kann.
  Der Verzeichnisdienst muß gemäß dem in [LHHM04], S. 5-11 vorgegebenen LDAP–Modell [LDAP06] implementiert werden.
- Anbieten von optionalen Zusatzdiensten, wie z.B. den Ausdruck von Dokumenten oder das Anbieten eines Dokumentenarchivs.

5.1.4 Der Zustellkopf

Der Zustellkopf ist ein Webservice, das als zentraler virtueller Verzeichnisdienst fungiert.
Der Zustellkopf übernimmt folgende Aufgaben [HoRe04]:

- Entgegennahme von Zustellanfragen
  - Einzelanfragen für genau einen Empfänger mittels LDAP [LDAP06]
  - Bulkanfragen (Mehrfachabfragen) für mehrere Empfänger gleichzeitig mittels SOAP Nachricht
- Abfrage der Verzeichnisdienste aller bekannten Zustelldienste, ob der Empfänger dort registriert ist
- Senden einer Antwort auf die Zustellanfrage, sowie weiterer Informationen (siehe Abschnitt 5.2.3)

5.1.5 Die Benutzerschnittstelle für den Empfänger

Die Benutzerschnittstelle dient zur Kommunikation zwischen Zustelldienst und Empfänger.
Die Implementierung der Benutzerschnittstelle kann im Grunde nach Vorstellungen des Zustelldienstanbieters erfolgen, muß allerdings dabei folgende technische Anforderungen erfüllen [HoRe04]:

- Die Signatur zur Identifikation des Empfängers bzw. für den Zustellnachweis soll über die Security Layer Schnittstelle der Bürgerkarte gebildet werden
- Aufbau der Verbindung zum Zustelldienst mittels starker SSL Verschlüsselung, bevorzugt über HTTPS [TLS00]
- Die Implementierung wird als Webinterface empfohlen, kann jedoch auch in Form eines Mail-Clients erfolgen
- Die Anforderungen an die Client-Infrastruktur sind möglichst gering zu halten

5.2 Der Ablauf anhand rechtlicher und technischer Gesichtspunkte

Anmerkung: Es wird dabei angenommen, daß für die Kommunikation zwischen der Applikation und dem Zustelldienst, das MOA-ZS als Middleware verwendet wird.

5.2.1 Anmeldung bei einem elektronischen Zustelldienst

In § 32 des Zustellgesetzes wird geregelt, wie die Einrichtung eines elektronischen Postfachs abläuft:

1. Identifikation des Benutzers:
   Vor dem Anlegen eines elektronischen Postfachs muß eine „qualitätsvolle Identifikation“ des Benutzers stattfinden.
   Eine natürliche Person muß sich mittels Bürgerkarte identifizieren. Die Stammzahl wird mittels Security Layer aus der Bürgerkarte ausgelesen und das Zustell-bPK daraus berechnet.
   Für eine nicht natürliche Person muß die Identifikation von einer zeichnungsberechtigten natürlichen Person mittels Bürgerkarte durchgeführt werden. Dem Zustelldienst muß, z.B. mittels Vollmacht bzw. durch eine Firmenbuchabfrage bewiesen werden, daß die natürliche Person für die nicht natürliche Person wirklich zeichnungsberechtigt ist.

2. Angabe der Verständigungsadressen:
   Der Benutzer muß mindestens eine elektronische Verständigungsadresse bekanntgeben, die vom Zustelldienst auf Gültigkeit überprüft wird (z.B. durch Versenden eines Bestätigungscodes an die E-Mail Adresse und anschließender Eingabe in einem Webformular [HoRe04])
   Neben der elektronischen Verständigungsadresse muß auch eine postalische Verständigungadresse angeben werden, die vom Zustelldienst optional durch Anfrage beim zentralen Melderegister bzw. beim Firmenbuch validiert werden kann.
3. Angabe eines Verschlüsselungszertifikats:
   Damit der Benutzer Dokumente verschlüsselt zugestellt bekommt, hat er die Möglichkeit seinen öffentlichen Schlüssel in Form eines X.509 Verschlüsselungszertifikats dem Zustelldienst bekannt zu geben. Wird ein Dokument mit der Bürgerkarte verschlüsselt, so kann dieses bei Verlust oder bei der Beschädigung der Karte nicht mehr entschlüsselt werden. Daher wird für die Verschlüsselung die Verwendung eines eigenen Verschlüsselungszertifikats empfohlen [WWW01]. Dabei kann ein Softwarezertifikat eingesetzt werden, das entweder in einer paßwort-geschützten Datei gespeicher oder bei einem „Trusted Center“ hinterlegt wird.
4. Angabe der gewünschten Dateiformate:
   Der Benutzer hat die Möglichkeit aus einer Liste von MIME-Typen zu wählen in welchem Dateiformat er Dokumente elektronisch zugestellt bekommen möchte.
5. Datenkontrolle und Zustimmung zur elektronischen Zustellung:
   Bevor das elektronische Postfach endgültig angelegt wird, werden dem Benutzer nochmals die gesammelten Anmeldedaten aufgelistet. Mittels Signierung der Daten wird der Anmeldvorgang beendet.

Nach dem Anlegen eines Postfachs ist es dem Benutzer jederzeit möglich sein seine Daten zu ändern. Ebenfalls steht es dem Benutzer frei sich wieder vom Zustelldienst abzumelden.
Der Empfänger kann dem Zustelldienst seine Abwesenheit melden. Während dieser Zeit werden Dokumente, die mit einer Rechtsmittelfrist verbunden sind, nicht elektronisch, sondern konventionell auf Papier zugestellt.

Für die administrativen Vorgänge ist wie beim Anlegen des Postfachs eine Identifikation mittels Bürgerkarte notwendig.

5.2.2 Erstellung des Dokuments

Da das Dokument für die Durchführung des Zustellprozesses selbst keine relevanten Daten enthält, kann es die Behörde im Grunde in jedem beliebigen Dateiformat, wie PDF, ZIP, etc., erstellen [HoRe04].
Im Hinblick auf die Einführung der dualen Zustellung ist, zur Vereinfachung des Drucks und Kuvertierungsprozesses auf ein einheitliches Format zu achten. Als bevorzugtes Datenformat wird XML angesehen, weil das Dokument damit strukturiert aufgebaut und automatisch verarbeitet werden kann. Weiters bringt XML selbst Standards zu Signierung und Verschlüsselung mit [HoRe04].

Das Dokument wird unabhängig vom Format, vor dem Absenden in einem MIME-Container verpackt.

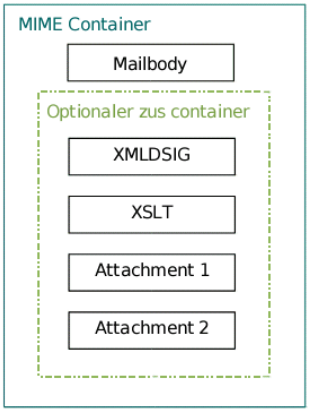

Abbildung 10: MIME-Container der Sendung
Quelle: [NHRL04]

Der MIME-Container, der in Abbildung 10 illustriert wird, beinhaltet folgendes:

- Einen zweiten MIME-Container in dem das eigentliche Dokument und der Mailbody enthalten sind. Im Mailbody steht eine Textnachricht mit der dem Empfänger mitteilt wird, daß das eigentliche Dokument als Attachment beiliegt [NHRL04].

- Einen optionalen ZUS Container.
  Dabei handelt es sich einen ZIP-Container, dem der MIME-Typ (application/zus) zugeordnet ist, um von einem speziellen Tool automatisch geöffnet werden zu können [NHRL04].

5.2.3 Ermittlung des Zustelldients

Die Ermittlung des zuständigen Zustelldients wird gemäß § 33 des Zustellgesetzes [ZusG04] durch Anfrage beim Zustellkopf durchgeführt.
Die Behörde muß sich dafür beim Zustellkopf mittels des Behördenzertifikats (OID) [Holl06] identifizieren.

Die Anfrage kann mittels folgender Parameter gestellt werden [LiHo04]:

- Für natürliche Personen:
    - Mittels unverschlüsselter oder verschlüsselter Zustell-bPK
    - Mittels Namen des Empfängers und der elektronischen bzw. postalischen Verständigungsadresse (und Geburtsdatum bei RSa-Qualität)

- Für nicht natürliche Personen:
    - Direkt über die Stammzahl
    - Mittels Bezeichnung und der elektronischen bzw. postalischen Verständigungsadresse

Der Zustellkopf sendet als Antwort eine SOAP Nachricht, die bei einer Einfachantwort gemäß dem „StdAnswer“ Schema ([LiHo04], S. 10) und bei einer Bulkantwort gemäß dem „BulkAnswer“ Schema ([LiHo04], S. 20) aufgebaut ist.

Ist die angefragte Person bei einem Zustelldienst registriert, sind folgende Daten enthalten:

- Das Zustell-bPK
- Die URI des oder der Zustelldienste(s)
- Die vom Empfänger akzeptierten MIME-Typen
- Das optionale X.509 Zertifikat des Empfängers

Ist die angefragte Person entweder bei keinem Zustelldienst registriert oder als abwesend gemeldet, wird eine Fehlermeldung an die Applikation gesendet und in weiterer Folge der elektronische Zustellvorgang abgebrochen.

Sollte der Empfänger bei mehreren Zustelldiensten registriert sein ist es, gemäß § 33 (3) des Zustellgesetzes [ZusG04] der Behörde erlaubt den Zustelldienst frei auszuwählen.

In § 33 (2) des Zustellgesetzes [ZusG04] wird ausdrücklich erwähnt, daß eine Anfrage beim Zustellkopf nur dann erlaubt ist, wenn die Versendung eines Dokuments beabsichtigt wird. Anfragen, die aus anderen Gründen durchgeführt werden, sind verboten.

5.2.4 Abfertigung des Dokuments durch MOA-ZS

Zu Beginn wird das Dokument in einem SOAP Container, der gemäß dem XML Schema „DeliveryRequest“ ([NaLi04], S. 9) aufgebaut ist, von der Applikation zum MOA-ZS gesendet [NaLi04].

Dabei werden folgende vier Informationen an das MOA-ZS übermittelt:

- Die Applikation (Sender)
- Der Empfänger (Receiver)
- Die Zustell-Metainformationen (MetaData)
- Das Zustellstück (Payload)

Im ersten Schritt erfolgt das Anbringen der Amtssignatur mit Hilfe des externen MOA-SS Moduls gemäß dem XMLDSIG Format [DSIG02] als Enveloped Signature [NaLi04]. Es wird unterschieden in welchem Datenformat das zuzustellende Dokument vorliegt:

- XML Dokumente
  Jedes zuzustellende XML Dokument verfügt über zwei XSLT Stylesheets [XSLT07], das Signatur Stylesheet zur Ausgabe im Secure Viewer und das Vorschau Style Sheet für die Ausgabe im Webbrowser.
  Das XML Dokument wird mit dem Signatur Stylesheet signiert. Das Vorschau Stylesheet wird mit keiner Signatur versehen.

- Nicht-XML Dokumente
  Bei Nicht-XML Dokument, muß ein eigenes XML „Zustelldeckblatt“ [NaLi04], das Information über den Absender, den Empfänger und die Attachments beinhaltet, erstellt werden. Die Signatur wird anschließend an diesem Deckblatt angebracht.

- Kombination von XML und Nicht-XML Dokumenten
  Die Signatur wird am ersten XML Dokument angebracht. Alle anderen Dokumente gelten dann als ebenfalls signiert [NaLi04].

Hat der Bürger dem Zustelldienst seinen Public Key bekannt gegeben, wird das Dokument unter Zuhilfenahme des RSA – Verfahrens verschlüsselt.
Die aus der Verschlüsselung resultierende CMS-Datei [PKCS7] wird anschließend in einen S/MIME [SMIM99] Container, der in Abbildung 11 illustriert wird, verpackt [NHRL04.]

Schlägt die Verschlüsselung aus irgendeinem Grund fehl, wird der gesamte Zustellvorgang abgebrochen und eine Fehlermeldung an die Applikation gesendet.

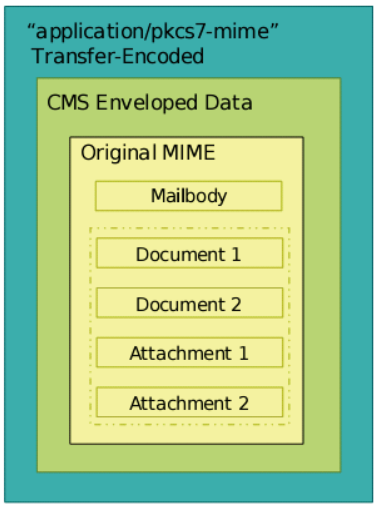

Abbildung 11: Verschlüsselter Container der Sendung
Quelle: [NaLi04]

5.2.5 Übergabe des Dokuments an den Zustelldienst

Die Übergabe des Dokuments erfolgt mittels einer SOAP Nachricht, in der Metainformationen über die Zustellung übertragen werden.
Das eigentliche Dokument wird entweder als MIME Anhang mittels SOAP with Attachments übertragen oder per Callback-URL mittels HTTP(S)-Get [HTTP99] referenziert [NHRL04].

Die Metainformationen müssen gemäß dem XML Schema „DeliveryRequest“ ([NHRL04], S. 10) aufbereitet werden und folgende Angaben enthalten:

- Das Zustell-bPK, das durch die vorherige Anfrage beim Zustellkopf ermittelt wurde.
- Eine Benachrichtigungsadresse, wohin später die Zustellbestätigung verschickt werden soll.
- Die Daten des Absenders bzw. des Empfängers.
- Weitere Metadaten, wie die Zustellqualität und der späteste Zeitpunkt zum Versenden der ersten Verständigung.
- Eine optionale Referenz auf das Dokument, mit deren Hilfe es später möglich ist das Dokument über HTTP(S)-Get vom Zustelldienst abholen zu lassen.
- Ein von der absendenden Behörde speziell definiertes Benachrichtigungsintervall für Nicht-RSa Sendungen.

Wurde das Dokument am Ende vom Zustelldienst angenommen, sendet er eine SOAP - Nachricht, deren Struktur im Schema „DeliveryRequestStatus“ ([NHRL04], S. 17) beschrieben wird, an die Applikation.

5.2.6 Verständigung des Empfängers

Hat der Zustelldienst das Dokument angenommen, muß gemäß § 34 (1) des Zustellgesetzes [ZusG04] der Empfänger verständigt werden. Die Verständigung läuft gemäß § 34 (3) des Zustellgesetzes folgendermaßen ab:

- Erste elektronische Verständigung
- Zweite elektronische Verständigung bei Nachabholung des Dokuments innerhalb von 2 Tagen
- Postalische Verständigung wenn wiederum keine Abholung innerhalb von 24 Stunden erfolgt

Elektronische Verständigungen über E-Mail sind mit einer digitalen Signatur gemäß dem S/MIME [SMIM99] Standard zu versehen und wenn der Empfänger seinen Public-Key bekanntgegeben hat, damit zu verschlüsseln [NaRe04].

Die postalische Verständigung erfolgt mittels Postkarte, die gemäß dem XML Schema „RecipientNotification“ [NHRL04] aufgebaut sein kann

5.2.7 Abholung des Dokuments

1. Der Empfänger loggt sich gemäß § 35 (1) des Zustellgesetzes [ZusG04] mittels „qualitätsvoller“ Identifikation beim Zustelldienst ein.
   Bei Vorliegen von Dokumenten in RSa-Qualität muß zur Vereinfachung des Abholverfahrens nicht jedes Dokument einzeln signiert werden, sondern nur der Erhalt neuer Dokumente direkt beim Login mittels digitaler Signatur des Empfängers bestätigt werden. Der Empfänger signiert dabei den sogenannten Authblock [NaRe04], in dem der Name, das Geburtsdatum des Empfängers, sowie das aktuelle Datum und die Uhrzeit, die URL des Zustelldients, und das Zustell-bPK enthalten sind.
2. Die Dokumente werden anschließend mitsamt der Bezeichnung des Absenders und der Zustellqualität aufgelistet.
3. Der Empfänger kann ein Dokument an eine E-Mail Adresse weiterleiten, auf den lokalen Rechner herunterladen oder, wenn es unverschlüsselt ist, direkt im Webinterface anzeigen.

Ein abgeholtes RSa-Dokument ist, laut § 34 (5) des Zustellgesetzes [ZusG04], aus Sicherheitsgründen, wie z.B. bei Fehlern während der Abholung, für zwei weitere Wochen beim Zustelldienst zu speichern.

Ein Dokument darf nicht gelöscht werden, bevor es angezeigt wurde. Es besteht allerdings die Möglichkeit Nicht-RSa Dokumente abzulehnen. In diesem Fall wird eine Verständigung an die Applikation gesendet und das Dokument vom Zustelldienst gelöscht [NaRe04].

Fristen, die mit dem zugestellten Dokument in Verbindung stehen, beginnen laut § 34 (4) des Zustellgesetzes [ZusG04] frühestens mit dem Zeitpunkt der Abholung und spätestens eine Woche, nachdem die erste Verständigung versendet wurde, zu laufen. Im Nachhinein kann eine nachweisbare Abwesenheit des Empfängers die Frist verlängern.
Treffen während einer Sitzung neue Dokumente ein, wird der Empfänger verständigt, darf aber erst nach neuerlichem Login Zugriff darauf erhalten.

5.2.8 Versenden des Zusellnachweises

Ein Zustellnachweis wird gemäß § 35 (2) und (3) des Zustellgesetzes [ZusG04] in folgenden Fällen versendet:

- Bei erfolgreicher RSa-Sendung
- Bei nicht Abholung einer RSa-Sendung
- Bei Annahmeverweigerung einer Nicht-RSa-Sendung

Dabei wird eine SOAP Nachricht, die nach dem XML Schema „DeliveryNotification“ ([NHRL04], S. 19) aufgebaut ist, an die Applikation übertragen bzw. per E-Mail an die Behörde versendet.

Bei erfolgreicher Zustellung werden in der SOAP Nachricht der vorher signierte Authblock und ein Zeitstempel über den Zustellzeitpunkt gesendet.

Bei nicht erfolgreicher Zustellung werden in der SOAP Nachricht der Fehlercode und der Grund des Fehlers in Textform übertragen [NHRL04].

6 Anforderungen an die kommerzielle elektronische Zustellung

Zu Beginn werden die Anforderungen an die behördliche elektronische Zustellung zusammengefaßt und daraus die Anforderungen an die kommerzielle elektronische Zustellung abgeleitet. In weiterer Folge wird erörtert in welchen Bereichen das behördliche System erweitert werden muß.

6.1.1 Anforderungen an das ursprüngliche System

Die Anforderungen an das behördliche System sind gemäß der Definitionen im Zustellgesetz [ZusG04] und nach Reichstädter [Reic04] folgende:

- Zur Registrierung bei einem Zustelldienst über das Internet ist eine qualitative Authentifizierung des Bürgers mittels Bürgerkarte notwendig.
- Zuzustellende Dokumente müssen zur Nachweisbarkeit der Authentizität und der Integrität mit der Amtssignatur versehen werden. Dem Bürger und der Behörde müssen ermöglicht werden die Amtssignatur auf Richtigkeit zu prüfen.
- Der Bürger muß über das Eintreffen neuer Dokumente verständigt werden.
- Für das Abholen eines Dokuments ist eine qualitative Authentifizierung des Bürgers mittels Bürgerkarte notwendig.
- Es müssen authentische Zustellnachweise, d.h. vom Bürger digital signiert, im Fall der erfolgreichen Zustellung und Unzustellbarkeitsmeldungen im Fall der nicht erfolgreichen Zustellung, an die Behörde gesendet werden.
- Es muß Bürgern möglich sein auf zugestellte Dokumente zeit- und ortsunabhängigen Zugriff zu erhalten.
- Verfahrenslaufzeiten, insbesondere für den Druck, das Kuvertieren und den Versand durch die Post, sollen verkürzt und des weiteren Kosten gesenkt werden.
- Die elektronische Zustellung soll zur Vermeidung von Medienbrüchen beitragen.
- Es muß sichergestellt sein, daß Daten, die über das Internet übertragen werden, verschlüsselt sind. Die zuzustellende Dokumente sollten zusätzlich mit dem Public Key des Empfängers verschlüsselt werden.
- Der Prozeß der elektronischen Zustellung soll einfach gestaltet werden, um gleichsam für Bürger und Behörden und soll von verschiedenen Zustelldienstanbietern leicht implementierbar sein.

6.2 Anforderungen an das zukünftige System

Anmerkung: Die Anforderungsanalyse wird gemäß den Vorgaben in [Wint05] durchgeführt und unterscheidet dabei in technische und organisatorische Anforderungen.

6.2.1 Technische Anforderungen

- Funktionale Anforderungen:
    - Der Absender muß sich vor dem Absenden eindeutig identifizieren.
    - Der Absender muß überprüfen können, ob an einen oder mehrere Empfänger elektronisch zugestellt werden kann.
    - Der Absender muß die Dokumente vor dem Absenden elektronisch signieren können.
    - Der Absender muß die Dokumente vor dem Absenden verschlüsseln können.
    - Die Absender muß die Zustellqualität auswählen können.
    - Der Absender muß den Zustelldienst auswählen können.
    - Der Absender muß ein oder mehrere Dokumente an einen oder mehrere Empfänger versenden können.
    - Das Absenden von Dokumenten muß automatisiert möglich sein.
    - Dem Absender muß eine signierte Zustellbestätigung zurückgesendet werden.
    - Der Absender muß sich die Rechnung für die Zustellung vom System anzeigen lassen und online bezahlen können.
    - Der Empfänger muß über das Eintreffen neuer Dokumente verständigt werden.
    - Der Empfänger muß sich vor dem Abholen der Zustellstücke eindeutig identifizieren.
    - Der Empfänger muß vor dem Zugriff auf die Dokumente eine Zustellbestätigung signieren.
    - Der Empfänger muß sich die Dokumente anzeigen lassen, downloaden oder an eine E-Mail Adresse weiterleiten können.
    - Das Abholen der Dokumente muß automatisiert möglich sein.
    - Der Empfänger muß die digitalen Signaturen überprüfen können.
    - Der Empfänger muß die Möglichkeit haben, seine vorübergehende Abwesenheit beim Zustelldienst zu melden.
    - Der Empfänger muß die Annahme eines Dokuments verweigern können

Der Empfänger muß die Möglichkeit haben ein Dokument zu löschen.

- Daten müssen bei der Übertragung über das Internet verschlüsselt werden, um Dritten keine Einsicht in Dokument zu gewähren.
- Daten müssen vom System in ausreichender Weise archiviert bzw. gesichert werden.

- Nichtfunktionale Anforderungen:

  Neben den üblichen Anforderungen an Performance, Skalierbarkeit, Verfügbarkeit und Wartbarkeit sind für die kommerzielle elektronische Zustellung folgende speziellen Anforderungen zu beachten:

  - Der Registrierungsprozeß bei einem Absende- bzw. Zustelldienst muß über das Internet durchführbar sein.
  - Das Design von Systemschnittstellen für die Kommunikation zwischen unterschiedlichen Komponenten muß offen sein.
  - Die Benutzerschnittstelle muß als Web-Interface realisiert werden oder in bestehende Anwendungen als Erweiterung eingebaut werden.
  - Die Identifikation bzw. die Authentifizierung muß mit derzeit gängigen Hilfsmitteln möglich sein, um vielen Benutzern den Zugang zum System zu ermöglichen.
  - Das System muß soweit erweiterbar sein, daß neue technische Entwicklungen, wie beispielsweise für die Identifikation bzw. Authentifizierung, schnell nutzbar sind.
  - Die Vorgänge müssen während der Zustellung protokolliert werden, um den Zustellvorgang nachvollziehbar zu machen. Benutzerdaten und Dokumente selbst dürfen nur in codierter Form protokolliert werden.

6.2.2 Organisatorische Anforderungen

- Es müssen in Analogie zur konventionellen Zustellung mehrere auswählbare Zustellqualitäten angeboten werden.
- Es muß ein geeignetes Schema für die Abrechnung von Zustellungen bereit gestellt werden.
- Es muß ein Vollmachtregelung zur Vertretung nicht natürlicher Personen durch natürliche Personen bereitgestellt werden.
- Das Konzept der dualen Zustellung muß angewendet werden können.

6.3 Notwendige Erweiterungen des behördlichen Modells

Aufgrund der im vorherigen Abschnitt spezifizierten Anforderungen muß das behördliche Modell für die kommerzielle elektronische Zustellung in einigen Punkten angepaßt bzw. erweitert werden.

6.3.1 Identifikation bzw. Authentifizierung

Nachfolgend werden die Vor- und Nachteile unterschiedlicher Varianten zur Identifikation bzw. Authentifizierung diskutiert:

Bürgerkarte

- Vorteile:
  - Absolute Rechtssicherheit durch sichere elektronische Signatur
  - Die Bürgerkarten-Umgebung ist frei verfügbar
  - Die Module für Online Applikationen können ebenfalls im außerbehördlichen Umfeld genutzt werden
  - Die Definitionen der Schnittstellen des Security-Layers sind offengelegt
  - Die Authentifizierung des Absenders und des Empfängers kann mit Hilfe der Personenbindung erfolgen
  - Das qualifizierte Zertifikat kann für die Erstellung der Absendersignatur und die Verschlüsselung des Dokumenteninhalts verwendet werden

- Nachteile:
  - Es besitzen nur wenige Bürger eine aktivierte Bürgerkarte
  - Der Registrierungsprozeß wird als aufwendig angesehen
  - Es muß ein eigenes Chipkartenlesegerät angeschafft werden
    (Anmerkung: Dies ist in Unternehmen meistens bereits vorhanden)
  - Die Verwendung eines Zustell-wbPKs über mehrere Absende- bzw. Zustelldienste hinweg ist nach derzeitiger Gesetzeslage nicht zulässig [Kuns06]. Als Ausweg könnte die Berechnung des Zustell-wbPKs nicht aus der Stammzahl des Benutzers, sondern aus einem beliebig generierten String erfolgen [Baum06]
  - Bei Verwendung von wbPKs wird die Signatur der Personenbindung gebrochen und kann daher nicht mehr geprüft werden [Baum06]

Handy-Signatur

- Vorteile:
  - Das Verfahren ist mobil überall einsetzbar
  - Keine Anforderungen an Vorhandensein einer speziellen Software- oder Hardwareinfrastruktur, nur Handy notwendig
  - Obwohl die Handy-Signatur momentan nur von A1 angeboten wird, können dieses Service Kunden aller anderen Netze mitverwenden [Tisc07]

- Nachteile:
  - Der Registrierungsprozeß wird als aufwendig angesehen
  - Es sind nur wenige Benutzer registriert
  - Die dabei verwendete Verwaltungssignatur besitzt im Allgemeinen nur bis Ende 2007 Gültigkeit

Einfache bzw. fortgeschrittene Signatur

- Vorteile
  - Der Registrierungsprozeß ist einfach
  - Das Zertifikat kann auf alternativer Hardware gespeichert werden (wie z.B. USB-Sticks) [WWW07] oder als reines Softwarezertifikat vorliegen)

- Nachteile
  - Geringere Rechtssicherheit als die Bürgerkarte
  - Das Verfahren kann nur bedingt mobil eingesetzt werden
  - Elektronische Signaturen haben allgemein den Ruf kompliziert zu sein [Tisc07]

Username und Paßwort

- Vorteile
  - Die einfachste und seit Jahren meist verwendete Identifizierungsmethode
  - Der Registrierungsprozeß ist einfach
  - Man kann ohne zusätzliche Hard- und Software von überall Zugang bekommen [Tisc07]

- Nachteile
  - Das Verfahren ist allgemein unsicher und die Gefahr von Mißbrauch dementsprechend hoch

    (Anmerkung: Die Abfrage der Adresse des Benutzers kann im Zentralen Melderegister und durch Zusendung der Zugriffsdaten mittels eigenhändiger Briefsendung geprüft werden.

    Um das Ausforschen der Benutzerdaten zu erschweren, kann zur Bestätigung einer Tätigkeit die zusätzliche Eingabe von Transaktionsnummern, sogenannten TANs, gefordert werden.)
  - Das Verfahren bietet keine Rechtssicherheit

Kreditkarte

- Vorteile
  - Das Verfahren ist einfach zu realisieren, setzt aber den Besitz einer Kreditkarte voraus
  - Die Authentifizierung des Benutzers kann über die Kreditkartennummer und den dazugehörigen Sicherheitscode oder mit PIN erfolgen
  - Es kann relativ leicht mit Hilfe des Luhn-Algorithmus [Luhn60] geprüft werden, ob die Kreditkartennummer gültig ist

- Nachteile

    Es kann nicht errechnet werden, ob die Kreditkartennummer auch dem angegebenen Benutzer zuzuordnen ist. Dafür muß eine Abfrage bei der Kreditkartengesellschaft gemacht werden
  - Mißbrauch kann durch Phishing-Attacken betrieben werden
  - Das Verfahren bietet eine sehr geringe Rechtssicherheit

Ausgelagerte Identifikation

Hierbei wird die Authentifizierung von Benutzern an externe Stellen, bei denen sich der Benutzer schon vorher eindeutig identifiziert hat abgegeben. Es würden z.B. Banken, Mobilfunkanbieter, das Portal der Wirtschaftskammer [Baum06] oder ein eigenes Trust-Center [Tisc07] in Frage kommen.
Das Verfahren könnte so ablaufen, daß der Benutzer beispielsweise aus einem Net-banking-System, bei dem er angemeldet ist, zu einem elektronischen Zustelldienst weitergeleitet wird.

- Vorteil
  - Es muß keine eigene Implementierung erfolgen

Zusammenfassend ist anzumerken, daß die Identifikation bzw. Authentifizierung als ein kritischer Faktor anzusehen ist.
Zur Lösung könnte man mehrere Identifikationsvarianten im System implementieren, wodurch man zwar nicht immer absolute Rechtssicherheit gewährt würde, aber eine größere Benutzergruppe angesprochen würde.

6.3.2 Klassifizierung der Dokumenttypen

Dokumente sollen neben dem MIME-Typ, vom Absender anhand folgender Typen klassifiziert werden können:

- Rechnung
- Mahnung
- Vertrag
- Ausschreibung
- Sonstige

Empfänger können angeben, welche Dokumenttypen sie empfangen wollen.
Bei nicht natürlichen Personen könnte beispielweise jedem Vertreter eine bestimmte Klasse von Dokumenten zugeordnet werden. [Baum06]

6.3.3 Einzel- und Massensendungen

Im kommerziellen Modell sollen folgende Versandvarianten angeboten werden:

- Einzelversand
  Der Absender versendet, beispielsweise über ein Webinterface, ein oder mehrere Dokumente an einen Empfänger.

- Einzelempfang
  Der Empfänger holt ein einzelnes Dokument, beispielsweise über ein Webinterface ab

- (Automatisierter) Massenversand
  Ein oder mehrere Dokumenten werden an mehrere Empfänger versendet. Um den Massenversand zu automatisieren, eignet sich am besten eine eigene Applikation.

  Das Anbringen der Absendersignatur kann im Stapelverfahren durchgeführt werden. Dafür kann eine sichere elektronische Signatur gewählt werden, da das Dokument, wie in §4 (2) der Signaturverordnung [SigV04] gefordert, vor dem Auslösen des Signaturvorgangs in der Regel als bekannt anzusehen ist.

- (Automatisierter) Massenempfang
  Hierbei werden mehrere Dokumente durch einen Empfänger gleichzeitig empfangen. Der automatisierte Massenempfang kann am Besten mittels einer eigenen Applikation erfolgen.

  Wenn Dokumente der Zustellqualität „Eigenhändig“ vorliegen, ist der automatisierte Empfang als problematisch anzusehen. Die Zustellbestätigung, muß in diesem Fall vom Empfänger mit einer sicheren elektronischen Signatur versehen werden. Eine sichere elektronische Signatur darf aber laut § 4 (2) Zeile 5 der Signaturverordnung [SigV04] nicht automatisch auf unbekannte Daten, wie es die Zustellbetätigung wäre, angebracht werden [WWW01].

  Das Zustellgesetz [ZusG04] enthält aber für das automatisierte Signieren des behördlichen Zustellnachweises in § 35 (2) eine Ausnahmeregelung.
  Diese lautet: *„…An die Stelle der sicheren elektronischen Signatur darf aufgrund besonderer Vereinbarung mit dem Zustelldienst eine an die Verwendung sicherer Technik gebundene automatisiert ausgelöste Signatur treten.“*

  Aufgrund dieser Bestimmung ist anzunehmen, daß auch eine außerbehördliche Zustellbestätigung, die mit gesicherter Technik automatisiert signiert wurde, Rechtsgültigkeit besitzt

6.3.4 Art der Benutzerschnittstelle

Nachfolgend werden die Vor- und Nachteile verschiedener Implementierungsarten der Benutzerschnittstelle diskutiert:

Eigene Applikation

- Vorteile:
  - Anpassbarkeit an die Bedürfnisse des jeweiligen Benutzers
  - Gute Umsetzbarkeit der Konzepte, wie z.B. für den Massenversand bzw. –empfang

- Nachteile:
  - Installation einer zusätzlichen Software muß durchgeführt werden
  - Software muß separat gewartet werden

Integration in Standardapplikation mittels Plug-In

- Vorteile:
  - Die Benutzerschnittstelle kann gut in Standardapplikationen integriert werden
  - Der Versand eines Dokuments kann beispielsweise über ein Office bzw. E-Mail Programm erfolgen
  - Der Empfang von Dokumenten kann ebenfalls über ein normales E-Mail Programm erfolgen
  - Gute Umsetzbarkeit der Konzepte für den Massenversand bzw. -empfang

- Nachteile:
  - Extra Installation des Plug-Ins
  - Eventuell schwer in proprietäre Lösungen integrierbar

Dynamisch erzeugtes Webinterface

- Vorteile:
  - Mobil verfügbar, vergleichbar wie ein Webmail-Client
  - Plattformunabhängige Lösung
  - Keine lokale Installation notwendig

- Nachteile:
  - Extra Installation des Plug-Ins
  - Schlechte Bedienbarkeit bei großen Mengen von Dokumenten [Kapp06]
  - Schwer umsetzbare Automatisierung von Versand und Empfang

6.3.5 Zustellqualitäten und -varianten

Bei der der kommerziellen elektronischen Zustellung sollen folgende drei Zustellqualitäten implementiert werden:

- Standard
  Hierbei wird nach der Zustellung eine einfache Empfangsbestätigung an den Absender übermittelt. Der Empfänger signiert diese nicht digital, wodurch der Empfänger kein qualifiziertes Zertifikat besitzen muß.
  Allerdings besteht keine absolute Sicherheit, ob das Dokument wirklich vom gewünschten Empfänger abgeholt wurde.

- Rückschein
  Hier wird bei der Abholung die Empfangsbestätigung vom Zustelldienst digital signiert. Der Zustelldienst übernimmt durch die Signierung der Empfangsbestätigung die Rolle des Annahmeberechtigten, wodurch der Empfänger ebenfalls kein qualifiziertes Zertifikat benötigt. Es ist allerdings ebenso unsicher, ob das Dokument vom gewünschten Empfänger abgeholt wurde.

- Eigenhändig
  Hierbei muß die Empfangsbestätigung vom Empfänger selbst digital signiert werden, wodurch der Empfänger auf jeden Fall ein qualifiziertes Zertifikat benötigt.
  Diese Variante würde, bei Verwendung einer sicheren elektronischen Signatur, rechtlich der konventionellen Sendung „Eigenhändig mit Rückschein“ entsprechen.

Bei der kommerziellen elektronischen Zustellung müssen auch verschiedene Varianten zur Absicherung des Inhalts angeboten werden:

- Durch (optionale) Inhaltsverschlüsselung kann das Dokument während der Übertragung nicht von Dritten gelesen werden.

- Durch (optionale) elektronische Signierung, kann die Integrität und Authentizität festgestellt werden. Der Absender sollte die Qualität der elektronischen Signatur wählen können.

6.3.6 Vertretungsregelung

Da die kommerzielle elektronische Zustellung vor allem im B2B Bereich eingesetzt werden wird, muß genau spezifiziert werden, wie eine nicht natürliche Person von einer natürlichen Person vertreten werden kann.

Zur Realisierung der Vertretungsregelung können drei Varianten herangezogen werden:

- Zentrale Verwaltung
  Hierbei muß für die Vertretungsregelung eine eigene Stelle geschaffen werden, die die Informationen in einem zentralen Verzeichnis speichert. Das System „Firmen A-Z“ der Wirtschaftskammer, in dem alle Betriebe Österreichs aufgelistet sind, könnte dafür angepaßt werden [Baum06].
  Alternativ kann das Vollmacht und Vertretungsregelungsbasismodul, MOA-VV, verwendet werden.
  Das Verzeichnis ist mit einem Zugriffsschutz zu versehen, um nicht jedermann die Einsicht in die Vollmachtsregelung von Unternehmen zu ermöglichen.

- Verteilte Verwaltung
  Hierbei kann im Grunde jeder Zustelldienst ein eigenes Modell implementieren und als „eine digitale Posteingangsstelle mit Verteilungsfunktion“ [Baum06] agieren.
  Das Verfahren könnte folgendermaßen realisiert werden:
  Die Vertretung der nicht natürlichen Person (z.B. der Prokurist) gibt dem Zustelldienst alle annahmeberechtigten natürlichen Personen bekannt. Weiters kann definiert werden, welche speziellen Dokumenttypen an die annahmeberechtigte Person geleitet werden.
  Der Vorteil einer verteilten Verwaltung ist, daß hierfür keine Schnittstelle zu einem externen System spezifiziert werden muß.

- Mischform von beiden
  Hierbei wird ein Teil der Regeln zentral, der andere verteilt gespeichert. Diese Art der Verwaltung scheint nicht besonders sinnvoll, insbesondere da es dabei zu Redundanzen und etwaigen Widersprüchen bei der Abfrage kommen kann.

6.3.7 Verrechnung und Preisgestaltung

Da es sich bei der kommerziellen elektronischen Zustellung um eine Dienstleistung handelt, wird für die Durchführung eine Gebühr eingehoben werden. Folglich muß ein spezielles Verrechnungssystem spezifiziert werden.

Generell kann man zwischen zwei Verrechnungsmodellen unterscheiden:

- Inter-Billing:
  Der Absender muß hierbei, analog zur konventionellen Zustellung, Porto bezahlen [Baum06].
  Die Verrechnung könnte hierbei folgendermaßen ablaufen:
  Der Absender muß direkt vor dem Absenden eines Dokuments die Zustellung bezahlen. Dies könnte z.B. durch Angabe einer Kreditkartennummer erfolgen.
  Komfortabler wäre es jedoch, wenn der Absendedienst die Anzahl der versendeten Dokumente protokolliert und dem jeweiligen Absender in regelmäßigen Abständen Rechnungen zukommen läßt.

- Intra-Billing:
  Dieses Modell kann auf mehrere Arten realisiert werden:

  - Bilaterale Variante:
    Hierbei werden alle Leistungen bilateral verrechnet. Dafür sind aber eine Vielzahl von spezifischen Abkommen zwischen den einzelnen Absende- und Zustelldiensten notwendig.

  - Zentrale Abrechnung:
    Hierbei erfolgt die Abrechnung über eine zentrale Stelle, der so genanten Clearingstelle. Der Zustellkopf könnte beispielsweise als Clearingstelle fungieren. Vorrausgesetzt ist allerdings, daß bei jeder Zustellung der Zustellkopf miteinbezogen wird.
    Bei der zentralen Variante sind nur Abkommen zwischen den Absende- bzw. Zustelldiensten mit der Clearingstelle notwendig.
    Die Verrechnung könnte in die Spezifikation des Zustellkopf aufgenommen werden.

- Elektronische Briefmarke
  Das System könnte vergleichbar zur konventionellen Briefmarke aufgebaut werden. Dabei verkauft eine zentrale Stelle Briefmarken an potentielle Absender. Die Briefmarke könnte als ein Zeichencode mitsamt Prüfnummer, ähnlich einer Handy-Wertkarte, realisiert werden [Baum06]. Bei der Durchführung einer Zustellung löst der Absender die Briefmarken durch Eingabe des Zeichencodes beim Absendedienst ein.

Für die Tarifgestaltung gibt es folgende Ideen:

- Unterschiedliche Preisstaffelung für unterschiedliche Zustellqualitäten
- Zusätzliche Preisstaffelung anhand des Datenvolumens
- Bonussystem um Leute zur Nutzung der kommerziellen elektronischen Zustellung anzulocken [LaHe06]
- Rabattsystem bei häufiger Nutzung

Laut einer Umfrage beim e-day 2006 der Wirtschaftskammer wurde von den Anwesenden Preisvorstellungen von 10 Cent über 1 € bis hin zu 3 € genannt, wobei im Durchschnitt 30 Cent vorgeschlagen wurden. Dabei ist anzumerken, daß die Preise weit unter denen für die konventionelle Zustellung liegen [Baum06].

7 Konzeption des kommerziellen elektronischen Zustellsystems

Im folgenden Kapitel wird eine auf dem behördlichen Modell aufbauende und den Anforderungen der Wirtschaft entsprechende Konzeption eines kommerziellen elektronischen Zustellsystems vorgestellt. Im Rahmen dieser Konzeption werden der Entwurf der Softwarearchitektur, die Spezifikation der Anwendungsfälle, sowie die Funktionalität der beteiligten Komponenten und Schnittstellen beschrieben. Den Abschluß bildet eine Modellierung des Ablaufs aus verschiedenen Sichtweisen.

7.1 Systembeschreibung

Aufgrund der durchgeführten Anforderungsanalyse soll das das System der kommerziellen elektronischen Zustellung zusammenfassend folgende Funktionalität zur Verfügung stellen:

- Technisch und rechtlich gesichertes Absenden von Dokumenten durch einen Absender
- Technisch und rechtlich gesichertes Empfangen von Dokumenten durch einen Empfänger
- Wahl von unterschiedlichen Zustellqualitäten
- Automatisierter Massenversand und –empfang
- Klassifizierung von Dokumenttypen
- Verwaltung von elektronischen Postfächern
- Erstellung und Versendung von Zustellbestätigungen
- Möglichkeit zur Prüfung der Authentizität von Dokumenten
- Protokollierung zur Nachvollziehbarkeit des Zustellvorgangs
- Vollmachtsregelung zur Vertretung von nicht natürlichen Personen durch natürliche Personen
- Bereitstellung eines Verrechnungsschemas

Die Sicherheit des Zustellvorgangs wird durch digitales Signieren des Dokuments und der Zustellbestätigung, sowie durch Protokollierung der Vorgänge gewährleistet.

7.1.1 Die Systemkomponenten

Das System der kommerziellen elektronischen Zustellung wird analog zum behördlichen System in modularer Bauweise in Form einer serviceorientierten Architektur aufgebaut werden und dabei aus folgenden Komponenten bestehen:

Absendedienst

Dabei handelt es sich um eine für die kommerzielle elektronische Zustellung neu entworfene Komponente, die das Absenden von Dokumenten ermöglicht.
Der Aufbau orientiert sich am behördlichen MOA-ZS [NaLi04] Basismodul, wobei die Funktionalität dabei in folgenden Bereichen erweitert wird:

- Verpflichtende Registrierung für neue Absender
- Wahl der Zustellqualitäten: Standard, Eingeschrieben mit Rückschein, Eigenhändig mit Rückschein
- (Automatisierter) Versand von Einzel- und Massensendungen
- Verrechnung der Zustellungen anhand der bilaterale Methode
- Protokollierung der Absendungen
- Übernahme von Zustellbestätigungen vom Zustelldienst

Es können im System beliebig viele Absendedienste vorkommen.

Zustelldienst

Der Zustelldienst stellt elektronische Postfächer zur Verfügung und übernimmt Dokumente vom Absendedienst.
Die Spezifikation basiert auf dem behördlichen Zustelldienst (siehe Abschnitt 5.1.3 bzw. [NeRe04]), wobei folgende Erweiterungen implementiert werden:

- Vertretungsregelung für nicht natürliche Personen anhand der verteilten Verwaltung
- Erweiterte Klassifizierung der Dokumente
- (Automatisierter) Empfang von Einzel- und Massensendungen
- Versenden der Zustellbestätigung an den Absendedienst

Anmerkungen zum Absende- bzw. Zustelldienst:
In der Praxis wird es öfters vorkommen, daß der Absende- und der Zustelldienst als eine Komponente realisiert werden [Baum06]. Für die hier durchgeführte Konzeption, ist es zur Bewahrung der Modularität vorteilhafter, zwei voneinander unabhängige Komponenten zu spezifizieren.
Weiters ist zu beachten, daß bei einer Realisierung als eine gemeinsame Komponente, der Registrierungsprozeß für Absender bzw. Empfänger nur einmal durchlaufen werden muß.

Zustellkopf

Dabei handelt es sich um den zentralen virtuellen Verzeichnisdienst.
Es kommt nur ein Zustellkopf im System vor, der als Webservice implementiert wird.

Es wäre möglich den behördlichen Zustellkopf im kommerziellen Modell mitzuverwenden, wofür die Spezifikation folgendermaßen erweitertet werden müßte:

- Zustelldienste, die keine Postfächer für behördliche Dokumente zur Verfügung stellen, müssen referenziert werden.
- Empfänger, die sich nur für die kommerzielle und nicht für die behördliche elektronische Zustellung registriert haben, müssen ebenfalls referenziert werden.

Anmerkungen zum Zustellkopf:
Da alle Zustellanfragen über den Zustellkopf laufen, kann bei Ausfall des Zustellkopfs überhaupt keine elektronische Zustellung mehr durchgeführt werden.
Aus diesem Grund muß das Ausfalls- bzw. Überlastungsrisiko, beispielsweise durch Clustering bzw. Load-Balancing [Baum06] minimiert werden.
Der Zustellkopf kann auch in einer hierarchischen Struktur, ähnlich dem Domain-Name-System aufgebaut werden [Baum06].

Identifikations –bzw. Authentifizierungsmodul

Aufgrund verschiedener Identifikations- bzw. Authentifizierungsmethoden wird eine eigene Komponente, in Form eines Moduls geschaffen. Bei Bedarf kann dieses einfach ausgetauscht werden, um dem Absender bzw. dem Empfänger wahlweise mehrere Varianten zur Verfügung zu stellen.

Zur Identifikation könnte das behördliche MOA-(W)ID [ScMo06] verwendet werden.

Anmerkung zur Identifikation bzw. Authentifizierung:
In der hier vorgestellten Konzeption wird, aufgrund rechtlicher Einschränkungen (siehe Abschnitt 6.3.1) kein zentral im System vergebenes Zustell-wbPK, sondern jeweils eine eigene eindeutige ID beim Absende- bzw. beim Zustelldienst verwendet.

Signaturerstellungs- und –Prüfungsmodul

Zur Erstellung und zur Prüfung von digitalen Signaturen wird ein eigenes Modul implementiert. Da verschiedene Arten von Signaturen eingesetzt werden können, soll dieses Modul ebenso problemlos austauschbar sein.

Für die Erstellung bzw. die Prüfung der digitalen Signatur können die Basismodule MOA-SS bzw. MOA-SP [MSSSP04] verwendet werden.

Anmerkung zur Datensicherheit:
Der Austausch der Daten zwischen den Komponenten soll generell verschlüsselt erfolgen. Dies kann am besten mit der Bereitstellung einer Public-Key-Infrastruktur ermöglicht werden.

7.1.2 Die Schnittstellen

Für die Kommunikation zwischen den Komponenten untereinander und zur Interaktion zwischen dem Absendedienst mit dem Absender bzw. zwischen dem Zustelldienst und dem Empfänger, werden Schnittstellen benötigt. Diese sind folgend:

- Systemschnittstelle Absendedienst – Zustellkopf
  (siehe Abschnitt 7.4.2)
- Systemschnittstelle Zustellkopf – Zustelldienst
  (siehe Abschnitt 7.4.3)
- Systemschnittstelle Absendedienst – Zustelldienst
  (siehe Abschnitt 7.4.4)
- Benutzerschnittstelle Absender
- Benutzerschnittstelle Empfänger

Anmerkung zu den Benutzerschnittstellen:
In der Praxis wird es ebenfalls vorkommen, daß die Benutzerschnittstelle für den Absender und für den Empfänger als eine gemeinsame realisiert wird. In der hier durchgeführten Konzeption werden aufgrund der unterschiedlichen Funktionalität beide Benutzerschnittstellen getrennt beschrieben.

7.1.3 Das Modell bei Anwendung der reinen elektronischen Zustellung

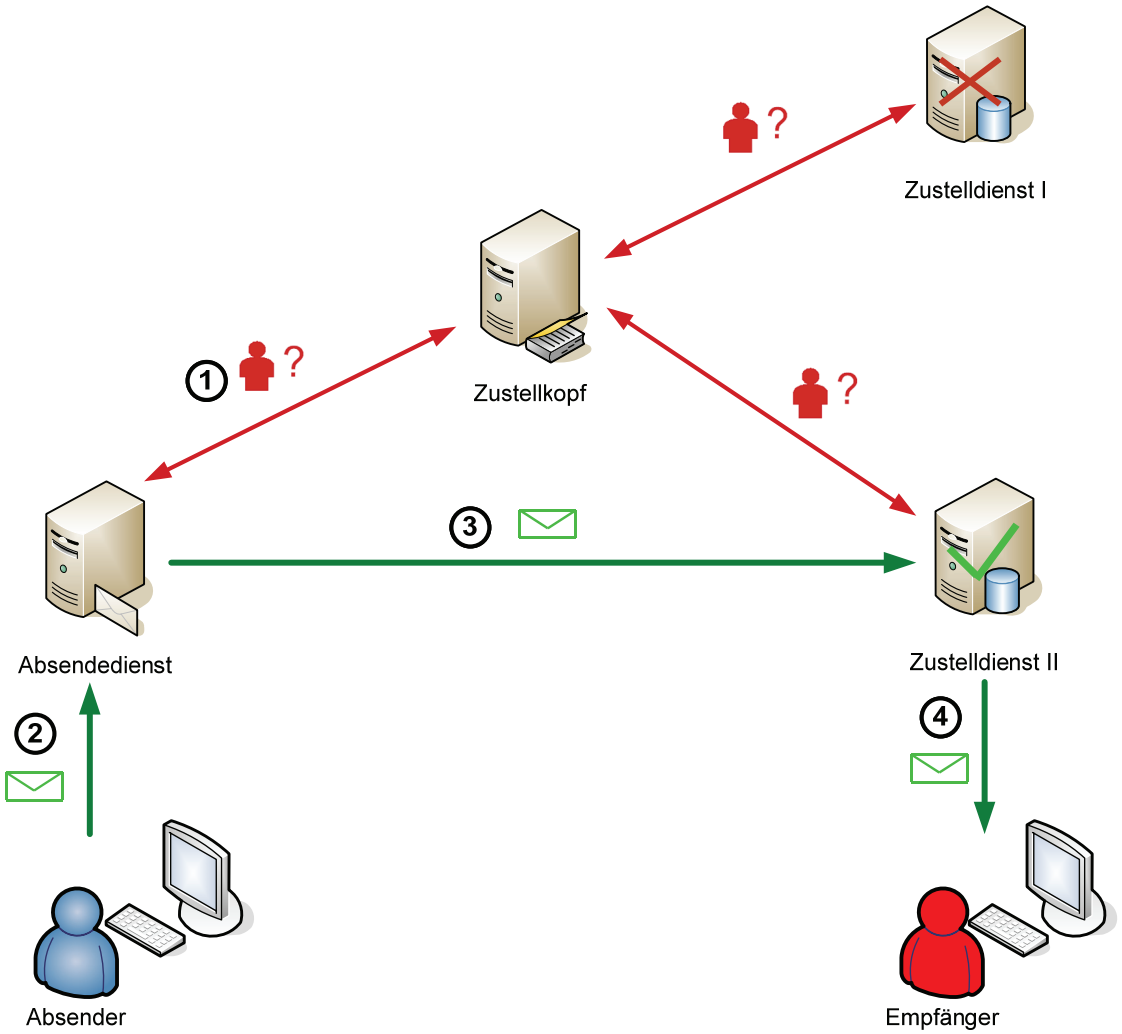

Abbildung 12: Modell der reinen kommerziellen elektronischen Zustellung

Die reine elektronische Zustellung, die in Abbildung 12 vereinfacht veranschaulicht wird, läuft folgendermaßen ab:

1. Der Absender leitet eine Zustellanfrage über den Absendedienst an den Zustelldienst um zu überprüfen, ob den gewünschten Empfänger elektronisch zugestellt werden kann
2. Der Absender fertig das Dokument für den Versand ab (Signierung, optionale Verschlüsselung, Wahl der Zustellqualität)

3. Das Dokument wird an den Zustelldienst des Empfängers übergeben.
4. Der Empfänger erhält eine Verständigung, meldet sich beim Zustelldienst an, signiert die Zustellbestätigung und erhält Zugriff auf das Dokument.

Eine detaillierte Modellierung des Ablaufs findet sich in Abschnitt 7.5.

7.1.4 Das Modell bei Anwendung der dualen Zustellung

Das sich zurzeit in Entwicklung befindliche behördliche Modell der dualen Zustellung [CeRo06] ist auch für den Einsatz im außerbehördlichen Umfeld geeignet.

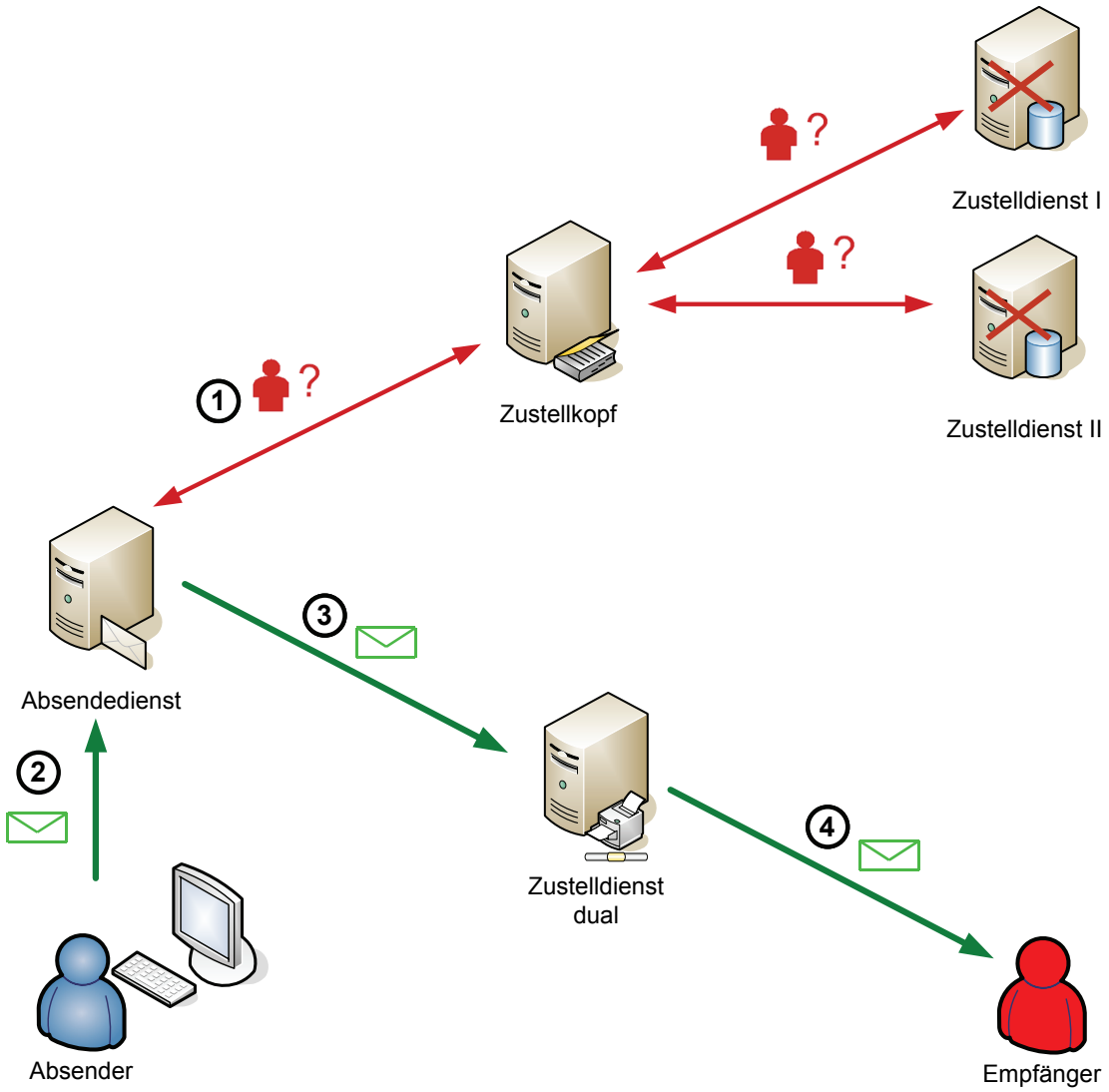

Abbildung 13: Modell der dualen Zustellung

Bei der dualen Zustellung kann der Absender das Dokument selbst dann, wenn der Empfänger bei keinem Zustelldienst registriert ist, elektronisch absenden.
In diesem Fall wird das Dokument in Schritt 3 an einen speziellen Zustelldienst übergeben, der das Dokument ausdruckt und konventionell an den Empfänger versendet [CeRo06].
Für den korrekten Druck des Dokuments und die Kuvertierung müssen vom Absender spezielle Parameter an den Zustelldienst übergeben werden.

Die Empfangsbestätigung wird in diesem Fall vom Empfänger händisch signiert und konventionell an den Zustelldienst zurückgeschickt.
Bei erfolgreicher Zustellung scannt der Zustelldienst die Zustellbestätigung und leitet sie in digitaler Form an den Absender weiter.

Bei Anwendung der dualen Zustellung treten jedoch auch Datenschutzbedenken auf:
Wird ein Dokument auf Papier ausgedruckt, ist eine vorherige Verschlüsselung des Dokumenteninhalts nicht möglich. In diesem Fall könnte das Dokument nicht nur während der Übertragung über das Internet, sondern auch durch das Personal beim Zustelldienst während des Drucks bzw. der Kuvertierung gelesen werden.
Ein Zustelldienst, der die duale Zustellung anbietet, muß deshalb besonders vertrauenswürdiges Personal beschäftigen. Trotz alledem scheint das Versenden von höchstvertraulichen Informationen mittels dualer Zustellung bedenklich.

7.2 Spezifikation der Anwendungsfälle

7.2.1 Anwendungsfälle des Absendedienst

Anmerkung:

Die für das kommerzielle Modell neu definierten Anwendungsfälle sind färbig hervorgehoben.

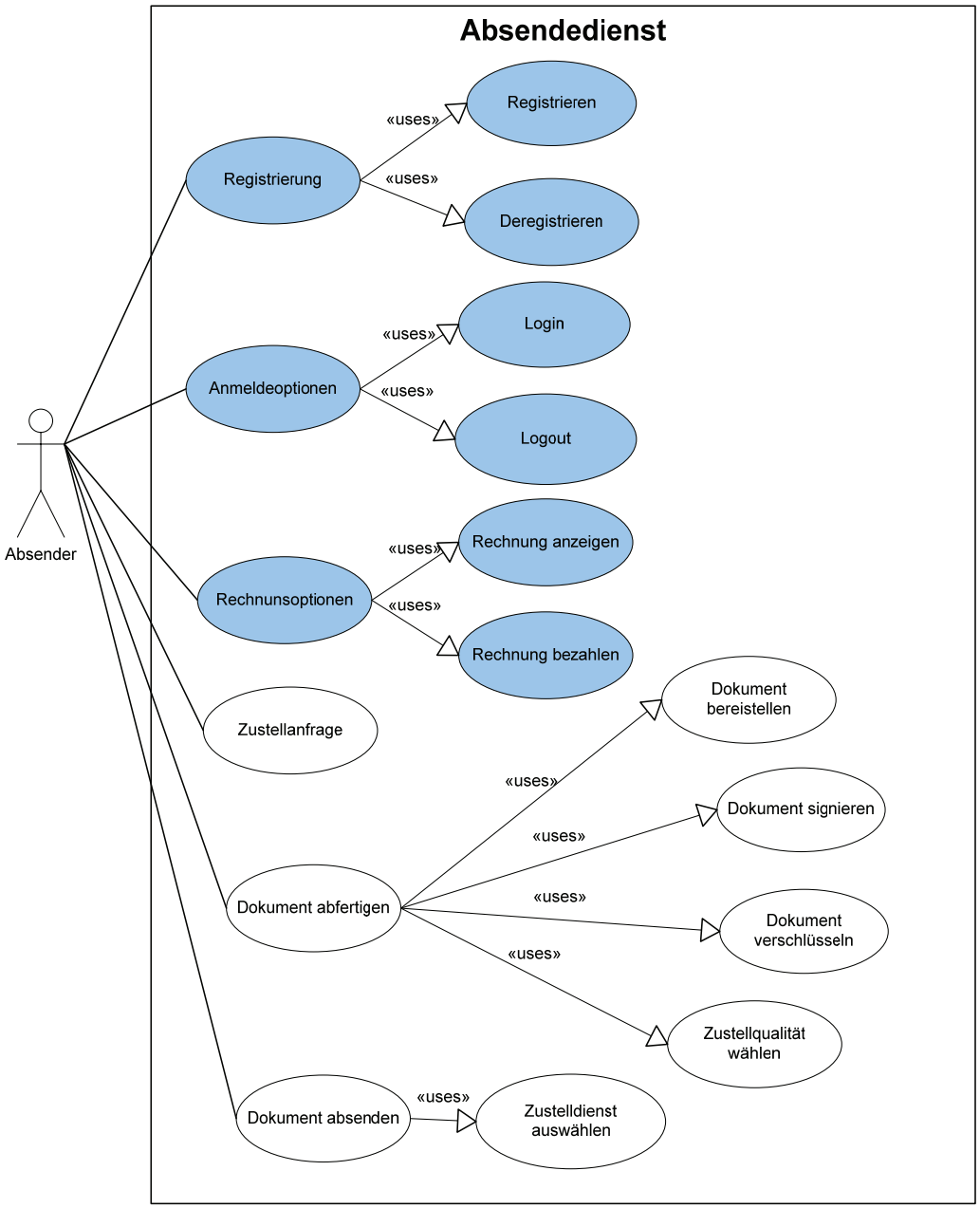

Abbildung 14: Anwendungsfalldiagramm des Absendienstes

Anmerkung:
Die Notation der Anwendungsfallbeschreibung wurde aus [ZGK03] entnommen.

Registrierung

A1. Registrieren	
Aktor	Absender
Kurzbeschreibung	Der Absender registriert sich bei einem Zustelldienst
Vorbedingungen	Identifikationsmittel (Bürgerkarte, etc.) im Besitz des Absenders
Beschreibung des Ablaufs	1. Der Absender ruft die Benutzerschnittstelle des Absendedienstes auf und wählt die Option „Registrieren“ 2. Das System öffnet den Registrierungsdialog 3. Der Absender gibt alle notwendigen Daten ein (Name, Adresse) und speichert die Eingabe 4. Das System listet dem Absender die Anmeldedaten auf 5. Der Absender bestätigt die Richtigkeit der Daten 6. Das System zeigt daraufhin die AGB des Absendedienstes an 7. Am Ende akzeptiert der Absender die AGB
Alternativer Ablauf	5. Ist der Absender im Besitz eines Zertifikats bestätigt er die Richtigkeit der Daten mittels digitaler Signatur
Auswirkungen	Der Absender kann Dokumente gesichert versenden
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst, Identifikationsmodul

A2. Deregistrieren	
Aktor	Absender
Kurzbeschreibung	Der Absender deregistriert sich vom Absendedienst
Vorbedingungen	Der Absender ist bei einem Absendedienst registriert
Beschreibung des Ablaufs	1. Der Absender ist über die Benutzerschnittstelle beim Absendedienst angemeldet und wählt die Option „Deregistrierung“ aus 2. Das System fordert den Absender zur Bestätigung auf 3. Der Absender bestätigt und ist fortan vom Absendedienst deregistriert
Auswirkungen	Der Absender kann keine Dokumente mehr versenden
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst

Anmeldung am Absendedienst für registrierte Benutzer

A3. Login	
Aktor	Absender
Kurzbeschreibung	Der Absender meldet sich beim Absendedienst an
Vorbedingungen	Der Absender ist beim Absendedienst registriert
Beschreibung des Ablaufs	1. Der Absender ruft die Benutzerschnittstelle auf und wählt die Option „anmelden“. In Folge dessen gibt der Empfänger seine Benutzerdaten ein 2. Das System überprüft die Benutzerdaten. Wenn die Daten korrekt sind, wird der Absender angemeldet. Bei einer falschen Angabe wird der Absender zur nochmaligen Eingabe aufgefordert
Auswirkungen	Der Absender ist angemeldet
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst, Identifikationsmodul

A4 Logout	
Aktor	Absender
Kurzbeschreibung	Der Absender meldet sich vom Absendedienst ab.
Vorbedingungen	Der Absender ist beim Absendedienst angemeldet.
Beschreibung des Ablaufs	1. Der Absender wählt die Option „abmelden“ 2. Das System schließt die Sitzung und meldet den Absender ab
Auswirkungen	Der Absender ist abgemeldet
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst

Rechnungsoptionen

A5. Rechnung anzeigen	
Aktor	Absender
Kurzbeschreibung	Der Absender läßt sich die aktuelle Rechnung für die Sendungen anzeigen
Vorbedingungen	Der Absender ist beim Absendedienst angemeldet
Beschreibung des Ablaufs	1. Der Absender wählt die Option „Rechnung anzeigen“ 2. Das System zeigt dem Absender die Rechnung an
Auswirkungen	Der Absender kennt den aktuellen Rechnungsstand
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst

A6. Rechnung bezahlen	
Aktor	Absender
Kurzbeschreibung	Der Absender bezahlt die aktuelle Rechnung
Vorbedingungen	Der Absender ist beim Absendedienst angemeldet
Beschreibung des Ablaufs	1. Der Absender wählt die Option „Rechnung bezahlen“ 2. Das System zeigt dem Absender die Rechnung an 3. Der Absender gibt dem System die Kontodaten für die Bezahlung an und bestätigt den Vorgang 4. Das System bucht den Rechnungsbetrag vom Konto des Absenders ab
Auswirkungen	Der Absender hat die aktuelle Rechnung bezahlt
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst

A7. Zustellanfrage	
Aktor	Absender
Kurzbeschreibung	Anfrage ob an einen oder mehrere bestimmte(n) Empfänger elektronisch zugestellt werden kann
Vorbedingungen	Der Absender ist beim Absendedienst angemeldet
Beschreibung des Ablaufs	1. Der Absender wählt die Option „Zustellanfrage“ und gibt die Daten des Empfängers (Namen, Adresse bzw. Verständigungsadresse) an 2. Der Absendedienst führt mit den Daten des Empfängers eine Anfrage beim Zustellkopf durch 3. Der Zustellkopf teilt dem Absendedienst mit, ob an den oder die Empfänger elektronisch zugestellt werden kann. Wenn ja, wird auch eine Liste mit den akzeptierten Dokumenttypen und der optionale Public-Key des Empfängers mitgesendet. 4. Der Absendedienst leitet die Antwort des Zustellkopfs an den Absender weiter
Auswirkungen	Der Absender weiß, ob die Zustellung möglich ist
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst, Zustellkopf

Abfertigung des Dokuments

A8. Dokument bereitstellen	
Aktor	Absender
Kurzbeschreibung	Der Absender stellt das oder die Dokumente dem Absendedienst bereit
Vorbedingungen	Zustellanfrage durchgeführt
Beschreibung des Ablaufs	1. Der Absender wählt die Option „Dokument bereitstellen“, und gibt dem Absendedienst dem Pfad zum Dokument bekannt 2. Der Absendedienst lädt das Dokument auf dem Server und bestätigt dem Absender die Übernahme des Dokuments
Auswirkungen	Das Dokument ist auf dem Server des Absendedienst geladen
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst

A9. Zustellqualität wählen	
Aktor	Absender
Kurzbeschreibung	Der Absender wählt die Zustellqualität
Vorbedingungen	Zustellanfrage durchgeführt
Beschreibung des Ablaufs	1. Der Absendedienst fordert den Absender zur Angabe der Zustellqualität auf 2. Der Absender gibt mit welcher Zustellqualität die Dokumente versendet werden sollen 3. Der Absendedienst bestätigt dem Absender die Wahl der Zustellqualität
Auswirkungen	Dem Absendedienst ist bekannt mit welcher Qualität die Zustellung erfolgen soll
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst

A10. Dokument signieren	
Aktor	Absender
Kurzbeschreibung	Der Absender sendet ein Dokument ab
Vorbedingungen	Zustellanfrage durchgeführt
Beschreibung des Ablaufs	1. Der Absendedienst bereitet das Signieren des oder der Dokumente vor, zeigt dem Absender das oder die zu signierende(n) Dokumente an und fordert zum Auslösen des Signaturvorgangs auf 2. Der Absender bestätigt den Signiervorgang 3. Der Absendedienst versieht das oder die Dokument(e) mit der digitalen Signatur des Absenders
Alternativer Ablauf	1. Der Absendedienst signiert das Dokument automatisch.
Auswirkungen	Ein (oder mehrere) Dokument(e) wurde(n) an mit der digitalen Signatur des Absenders versehen
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst, Signaturmodul

A11. Dokument verschlüsseln	
Aktor	Absender
Kurzbeschreibung	Der Absender sendet ein Dokument ab.
Vorbedingungen	Zustellanfrage durchgeführt
Beschreibung des Ablaufs	1. Der Absender wählt die Option „Dokument verschlüsseln“ 2. Der Absendedienst verschlüsselt, wenn der öffentliche Schlüssel des Empfängers bekannt ist, das oder die Dokument(e) und teilt dem Absender das Resultat mit
Alternativer Ablauf	1. Der Absendedienst verschlüsselt das Dokument automatisch
Auswirkungen	Ein (oder mehrere) Dokument(e) wurde(n) verschlüsselt
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst
Anmerkungen	Wenn ein öffentlicher Schlüssel des Empfängers bekannt ist, kann der Verschlüsselungsvorgang in der Regel vom Absendedienst automatisch durchgeführt werden

A12. Dokument absenden	
Aktor	Absender
Kurzbeschreibung	Der Absender sendet ein Dokument ab
Vorbedingungen	Zustellanfrage durchgeführt und Dokument abgefertigt
Beschreibung des Ablaufs	1. Der Absender wählt die Option „Dokument absenden“ und gibt an über welchen Zustelldienst das oder die Dokument(e) an den Empfänger zugestellt werden sollen 2. Der Absendedienst übermittelt daraufhin das oder die Dokument(e) an den Zustelldienst des oder der Empfänger 3. Der Zustelldienst bestätigt dem Absendedienst die Übernahme 4. Der Absendedienst teilt dem Empfänger mit, daß das oder die Dokument(e) erfolgreich an den Zustelldienst übergeben wurde(n)
Auswirkungen	Ein (oder mehrere) Dokument(e) wurde(n) an den oder die Absender versandt
Technologien	Benutzerschnittstelle Absendedienst, Absendedienst, Zustelldienst

7.2.2 Anwendungsfälle des Zustelldiensts

Abbildung 15: Anwendungsfalldiagramm des Zustelldiensts

Registrierung

Z1. Registrieren	
Aktor	Empfänger
Kurzbeschreibung	Registrieren bei einem Zustelldienstanbieter und Anlegen eines elektronischen Postfachs
Vorbedingungen	Identifikationsmittel (Bürgerkarte, etc.) im Besitz des Empfängers
Beschreibung des Ablaufs	1. Der Empfänger wählt die Option „Registrieren“ 2. Das System öffnet den Registrierungsdialog 3. Der Empfänger gibt alle notwendigen Daten ein (Name, Adresse, Benachrichtigungsadresse) 4. Das System listet dem Empfänger die Anmeldedaten auf 5. Der Empfänger bestätigt die Korrektheit der Daten 6. Das System verifiziert die Benachrichtigungsadresse des Empfängers. Wenn die Adresse nicht korrekt ist, muß der Absender bzw. der Empfänger diese korrigieren 7. Der Empfänger kann seinen Public-Key zur Verschlüsselung mitteilen 8. Das System zeigt daraufhin die AGB des Zustelldients an 9. Am Ende akzeptiert der Empfänger die AGB
Alternativer Ablauf	5. Ist der Absender im Besitz eines Zertifikats bestätigt er die Richtigkeit der Daten mittels digitaler Signatur
Auswirkungen	Der Empfänger kann Dokumente empfangen
Technologien	Benutzerschnittstelle Zustelldienst, Zustelldienst, Identifikationsmodul

Z2. Deregistrieren	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger deregistriert sich vom Zustelldienst
Vorbedingungen	Z1, Z3
Beschreibung des Ablaufs	1. Der Empfänger wählt die Option „Deregistrierung“ aus 2. Das System fordert den Empfänger zur Bestätigung auf 3. Der Empfänger bestätigt und ist fortan vom Zustelldienst deregistriert
Auswirkungen	Das elektronische Postfach ist gelöscht
Technologien	Benutzerschnittstelle Zustelldienst, Zustelldienst

Anmeldung am Zustelldienst für registrierte Benutzer

Z3. Login	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger meldet sich beim Zustelldienst an
Vorbedingungen	Z1
Beschreibung des Ablaufs	1. Der Empfänger ruft die Benutzerschnittstelle auf und wählt die Option „anmelden“. In Folge dessen gibt der Empfänger seine Benutzerdaten ein 2. Der Zustelldienst überprüft die Benutzerdaten. Wenn die Daten korrekt sind, wird der Empfänger angemeldet. Bei einer falschen Angabe wird der Empfänger zur nochmaligen Eingabe aufgefordert
Auswirkungen	Der Empfänger ist angemeldet
Technologien	Benutzerschnittstelle Zustelldienst, Zustelldienst, Identifikationsmodul

Z4. Logout	
Aktor	Empfänger
Kurzbeschreibung	Z3
Vorbedingungen	Der Empfänger ist beim Zustelldienst angemeldet
Beschreibung des Ablaufs	1. Der Empfänger wählt die Option „abmelden“ 2. Das System schließt die Sitzung und meldet den Empfänger ab
Auswirkungen	Der Empfänger ist abgemeldet
Technologien	Benutzerschnittstelle Zustelldienst, Zustelldienst, Identifikationsmodul

Verwaltung des elektronischen Postfachs

Z5. Dokumenttypen angeben	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger meldet dem Zustelldienst welche Dokumenttypen er zugestellt bekommen möchte
Vorbedingungen	Z3
Beschreibung des Ablaufs	1. Der Empfänger wählt die Option „Dokumenttypen angeben“ aus. In Folge dessen wählt der Empfänger aus einer Liste die Dokumenttypen, die er zugestellt bekommen möchte 2. Der Zustelldienst speichert die gewählten Dokumenttypen im Profil des Empfängers ab
Auswirkungen	Der Empfänger hat die gewünschten Dokumenttypen angegeben
Technologien	Benutzerschnittstelle Zustelldienst, Zustelldienst

Z6. Vollmacht vergeben	
Aktor	Empfänger
Kurzbeschreibung	Es werden die für eine nicht natürliche Person annahmeberechtigten natürlichen Personen angegeben
Vorbedingungen	Z3
Beschreibung des Ablaufs	1. Der Empfänger, in diesem Fall eine, für die nicht natürliche Person zeichnungsberechtigte natürliche Person wählt die Option „Vollmacht vergeben“ aus. In weiterer Folge gibt der Empfänger die Daten der anderen bevollmächtigten Personen bekannt 2. Der Absendedienst speichert die Daten
Auswirkungen	Dem Zustelldienst sind die für die nicht natürliche Person bevollmächtigte(n) Persone(n) bekannt
Technologien	Benutzerschnittstelle Zustelldienst, Zustelldienst
Anmerkungen	Die Angabe von anderen annahmeberechtigten Personen ist nur bei nicht natürlichenn Personen möglich

Z7. Abwesenheit melden	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger meldet dem Zustelldienst seine Abwesenheit
Vorbedingungen	Z3
Beschreibung des Ablaufs	1. Der Empfänger wählt die Option „Abwesenheit melden“ aus und gibt die Zeitdauer der Abwesenheit an 2. Der Absender erhält bei versuchter Zustellung in der Abwesenheitszeit des Empfängers eine Meldung darüber
Auswirkungen	Der Empfänger wird im Zeitraum der Abwesenheit nicht über das eintreffen neuer Dokumente verständigt. Der Absender erhält bei der Zustellanfrage die Abwesenheitsmeldung des Empfängers
Technologien	Benutzerschnittstelle Zustelldienst, Zustelldienst
Anmerkungen	Da bei der kommerziellen elektronischen Zustellung durch die Zustellung eines Dokuments keine Rechtsfrist zu laufen beginnt, können Dokumente auch in Abwesenheit des Empfängers zugestellt werden. Die Abwesenheitsmeldung gibt dem Absender in erster Linie zu erkennen, daß der Empfänger das Dokument erst nach seiner Rückkehr abholen wird.

Annahme des Dokuments

Z8. Dokumente auflisten	
Aktor	Empfänger
Kurzbeschreibung	Die abholbereiten Dokumente werden dem Empfänger in einer Liste angezeigt
Vorbedingungen	Mindestens ein Dokument im Postfach, Z3
Beschreibung des Ablaufs	1. Der Empfänger wählt die Option „Dokumente auflisten“ 2. Das System zeigt eine Liste mit den abholbereiten Dokumenten an. Wenn keine Dokumente vorliegen, wird eine leere Liste mit einer entsprechenden Meldung angezeigt
Alternativer Ablauf	1. Das System listet die Dokumente nach dem Anmelden des Empfängers automatisch auf
Auswirkungen	Der Empfänger weiß, welche Dokumente für ihn bereit liegen
Technologien	Benutzerschnittstelle Zustelldienst, Zustelldienst

Z9. Empfangsbestätigung signieren	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger versieht die Empfangsbestätigung (bzw. den Authblock) mit einer digitalen Signatur
Vorbedingungen	Neue „eigenhändige Dokumente vorliegend, Z3
Beschreibung des Ablaufs	1. Das System meldet dem Empfänger, daß neue „eigenhändige“ Dokumente vorliegen und zeigt ihm den Authblock an. 2. Der Empfänger versieht den Authblock mit einer digitalen Signatur 3. Das System erstellt aus dem Authblock die Empfangsbestätigung und sendet diese an den Absender
Auswirkungen	Der Absender hat die Sicherheit, daß der Empfänger die Dokumente empfangen hat
Technologien	Benutzerschnittstelle Zustelldienst, Zustelldienst, Signaturmodul
Anmerkungen	Damit insbesondere bei sehr vielen neuen Dokumenten, nicht jeder einzelne Rückschein signiert werden muß, genügt es, analog zur behördlichen elektronischen Zustellung, daß der Empfänger nach dem Anmelden einen Authblock (siehe [HoRe04], S. 15), signiert.

Abholen des Dokuments

Z10. Dokument entschlüsseln	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger entschlüsselt mit seinem Private-Key ein verschlüsseltes Dokument
Vorbedingungen	Mindestens ein mit dem Public Key des Empfängers verschlüsseltes Dokument im Postfach, Z3
Beschreibung des Ablaufs	1. Der Empfänger wählt ein verschlüsseltes Dokument aus der Liste aus und wählt anschließend die Option „entschlüsseln“ 2. Das System entschlüsselt mit Hilfe des Private-Keys des Empfängers das Dokument
Auswirkungen	Das Dokument ist entschlüsselt.
Technologien	Benutzerschnittstelle Zustelldienst oder nach Download des Dokuments am lokalen Rechner

Z11. Dokument anzeigen	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger läßt sich ein Dokument anzeigen
Vorbedingungen	Mindestens ein Dokument im Postfach, Z3 und Z10 bei einem verschlüsselten Dokument
Beschreibung des Ablaufs	1. Der Empfänger wählt ein Dokument aus der Liste aus und wählt anschließend die Option „anzeigen“ 2. Das System zeigt das Dokument in einem Vorschaufenster an
Auswirkungen	Der Empfänger kann den Inhalt des Dokuments lesen
Technologien	Benutzerschnittstelle Zustelldienst
Anmerkungen	Ein verschlüsseltes Dokument kann erst nach der Entschlüsselung angezeigt werden

Z12. Dokument downloaden	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger downloadet ein Dokument auf seinen lokalen Rechner
Vorbedingungen	Mindestens ein Dokument im Postfach, Z3
Beschreibung des Ablaufs	1. Der Empfänger wählt ein Dokument aus der Liste aus und wählt anschließend die Option „downloaden“ 2. Das System öffnet einen „Speichern unter“ Dialog. 3. Der Empfänger wählt den genauen Speicherort des Dokument 4. Das System übertragt über das Internet das Dokument auf den Rechner des Empfängers
Auswirkungen	Ein Dokument liegt lokal am Rechner des Empfängers
Technologien	Benutzerschnittstelle Zustelldienst

Z13. Dokument per E-Mail weiterleiten	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger leitet ein oder mehrere Dokumente an eine E-Mail Adresse weiter.
Vorbedingungen	Mindestens ein Dokument im Postfach, E-Mail Adresse auf Gültigkeit validiert, Z3
Beschreibung des Ablaufs	1. Der Empfänger wählt ein Dokument aus der Liste aus und wählt anschließend die Option „per E-Mail weiterleiten“ 2. Das System zeigt dem Empfänger eine Liste mit E-Mail Adressen an, die für die Weiterleitung des Dokuments angegeben wurden 3. Der Empfänger wählt entweder eine dieser E-Mail Adressen aus oder gibt eine neue E-Mail Adresse ein 4. Wenn der Empfänger eine neue E-Mail Adresse angibt, muß diese vom System erst geprüft werden. Wenn die E-Mail dem System bereits bekannt ist, wird das Dokument dorthin weitergeleitet
Auswirkungen	Ein oder mehrere Dokumente sind an eine E-Mail Adresse weitergeleitet worden
Technologien	Benutzerschnittstelle Zustelldienst

Z14. Absendersignatur prüfen	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger überprüft die Korrektheit der Absendersignatur.
Vorbedingungen	Mindestens ein Dokument im Postfach, Z3 und Z11 oder Z12 oder Z13
Beschreibung des Ablaufs	1. Der Empfänger hat ein Dokument ausgewählt und wählt die Option „Absendersignatur prüfen“ aus 2. Das System prüft die auf dem Dokument vorhandene Absendersignatur und teilt dem Empfänger das Resultat mit
Auswirkungen	Der Empfänger weiß, ob die Absendersignatur korrekt ist
Technologien	Benutzerschnittstelle Zustelldienst, Signaturmodul

Sonstiges

Z15. Verständigung erhalten	
Aktor	Empfänger
Kurzbeschreibung	Der Zustelldienst verständigt dem Empfänger über das Eintreffen von neuen Dokumenten
Vorbedingungen	Mindestens ein neues Dokument vorliegend
Beschreibung des Ablaufs	1. Der Zustelldienst sendet elektronisch per E-Mail, SMS oder Telefax eine Verständigung an den Empfänger
Auswirkungen	Der Empfänger weiß, daß ein neues Dokument für ihn bereit liegt
Technologien	per E-Mail, SMS oder Telefax

Z16. Dokumentannahme verweigern	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger verweigert die Annahme eines Dokuments.
Vorbedingungen	Mindestens ein Dokument im Postfach, Z3
Beschreibung des Ablaufs	1. Der Empfänger wählt ein neu eingetroffenes Dokument aus der Liste und aus und wählt anschließend die Option „Annahme verweigern“ 2. Das System warnt den Empfänger, daß das Dokument gelöscht bei Annahmeverweigerung automatisch gelöscht wird 3. Der Benutzer bestätigt dem System die Verweigerung der Annahme 4. Das System löscht das verweigerte Dokument aus dem Postfach und sendet eine Mitteilung an den Absender
Auswirkungen	Der Absender ist über die Verweigerung der Dokumentenannahme informiert
Technologien	Benutzerschnittstelle Zustelldienst
Anmerkungen	Dokumente werden bei Annahmeverweigerung automatisch gelöscht und können vom Empfänger nicht geöffnet werden

Z17. Dokument löschen	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger löscht ein Dokument aus dem Postfach
Vorbedingungen	Mindestens ein Dokument im Postfach, Z3 und Z11 oder Z12 oder Z13
Beschreibung des Ablaufs	1. Der Empfänger wählt ein oder mehrere Dokument(e) aus einer Liste aus und markiert diese(s) zum Löschen 2. Das System löscht das oder die Dokument(e) aus dem Postfach des Empfängers
Alternativer Ablauf	1. Der Empfänger gibt ein Zeitintervall (z.B. 14 Tage) bekannt nach dem alle abgeholten Dokumente gelöscht werden sollen 2. Das System löscht nach Ablauf des Intervalls alle abgeholten Dokumente
Auswirkungen	Eine oder mehrere Dokument(e) sind aus dem Postfach gelöscht
Technologien	Benutzerschnittstelle Zustelldienst
Anmerkungen	Der Empfänger kann nur abgeholte Dokumente löschen

Z18. Antwort senden	
Aktor	Empfänger
Kurzbeschreibung	Der Empfänger sendet eine Antwort an den Absender
Vorbedingungen	Zustelldienst implementiert Absendefunktion, Absendedienst bietet ein elektronisches Postfach an, Dokument im Postfach des Empfängers, Z3 und Z11 oder Z12 oder Z13
Beschreibung des Ablaufs	1. Der Absender wählt die Option „Antworten“. 2. Der Zustelldienst führt eine Zustellanfrage mit den Daten des Absenders beim Zustellkopf 3. Der Empfänger lädt das Antwortdokumet auf den Server und wählt die gewünschte Zustellqualität. 4. Der Zustelldienst signiert das Dokument, verschlüsselt es gegebenenfalls und sendet das Dokument an den Absendedienst 5. Der Absender wird verständigt und holt das Dokument ab. 6. Der Empfänger erhält die Zustellbestätigung
Auswirkungen	Der Absender hat auf seine Zustellung eine Antwort erhalten
Technologien	Benutzerschnittstelle Zustelldienst, Zustelldienst, Absendedienst
Anmerkungen	Die Rollen des Absenders und Empfängers bzw. des Absende- Zustelldiensts sind vertauscht

7.2.3 Gemeinsame Anwendungsfälle mit dem behördlichen Modell

Absendedienst
Zustellanfrage
Dokument bereitstellen
Dokument signieren
Dokument verschlüsseln
Zustellqualität wählen
Zustelldienst wählen
Dokument absenden

Tabelle 1: Anwedungsfälle Absendedienst behördlich und kommerziell

Zustelldienst
Registrieren
Degistriereren
Login
Logout
Abwesenheit melden
Dokumenttypen angeben
Verständigung erhalten
Empfangsbestäitung signieren
Dokumente auflisten
Dokumentannahme verweigern
Dokument löschen
Dokument entschlüsseln
Dokument anzeigen
Dokument per E-Mail weiterleiten
Dokument downloaden
Absendersignatur prüfen
Absendersignatur prüfen

Tabelle 2: Anwedungsfälle Zustelldienst behördlich und kommerziell

7.3 Entwurf der Softwarearchitektur

7.3.1 Benötigte Datenbanken

Datenbanken des Absendedienstes

Die Datenbank „SenderData“ speichert die Daten der registrierten Absender.

Datenbank *SenderData*	
SenderID	ID des Absenders
SenderNotation	Bezeichnung des Absenders
SenderName	Name
SenderGivenName	Vorname
SenderAdress	Adresse
SenderTelephone	Telefonnummer
SenderMail	E-Mail
CorporateBody/PhysicalPerson	Hinweis ob natürliche oder nicht natürliche Person
SenderPublicKey	Public-Key des Absenders
Invoice	Rechnungsstand für durchgeführte Absendungen

Tabelle 3: Datenbank „SenderData“

In der Datenbank „DispatchLogData“ werden die durchgeführten Absendungen protokolliert.

Datenbank *DispatchLogData*	
DispatchID	ID der Absendung
SenderID	ID des Absenders beim Absendedienst
ReceiverID	ID des Empfängers beim Zustelldienst
ReceiverName	Name des Empfängers
ReceiverAdress	Adresse des Empfängers
CorporateBody/PhysicalPerson	Hinweis ob Empfänger natürliche oder nicht natürliche Person
DeliveryServiceURL	Webadresse des Zustelldiensts des Empfängers
DocumentID	ID des Dokuments
DispatchTimestamp	Zeitstempel des Absendens
DispatchCosts	Kosten für die Absendung

Tabelle 4: Datenbank „DispatchData“

In der Datenbank „Documents“ werden die versendeten Dokumente archiviert. Es erscheint sinnvoll die Dokumente bis zum Ablauf der kleinen Verjährungsfrist [WWW08] von 3 Jahren aufzubewahren

Datenbank *Documents*	
DocumentID	ID des Dokuments
DispatchID	ID der Absendung
Document	Dokument (in verschlüsselter Form)
HashValue	Hash-Wert des Dokuments

Tabelle 5: Datenbank „Documents“

Datenbanken des Zustelldiensts

In der Datenbank „ReceiverData“ sind die Profile der beim Zustelldienst registrierten Empfänger gespeichert.
Diese Datenbank dient als Basis für den LDAP-Verzeichnisdienst, dessen Spezifikation auf dem behördlichen Modell übernommen werden kann. (Siehe [LHHM04] S. 5-11)

Datenbank ReceiverData	
ReceiverID	ID des Empfängers
CorporateBody/Physical Person	Hinweis ob natürliche oder nicht natürliche Person
ReceiverNotation	Bezeichnung
ReceiverName	Name
ReceiverGivenName	Vorname
ReceiverAdress	Adresse
ReceiverMail	E-Mail
ReceiverPhone	Telefonnummer
ReceiverBirthdate	Geburtsdatum
PreferedNotification	Bevorzugte Verständigungsart
NotificationAdress	Verständigungsadresse(n)
cpRepresentative	Für die nicht natürliche Person bevollmächtige natürliche Personen
ReceiverPublicKey	(Optionaler) Public-Key des Empfängers
DocumentTypes	Gewünschte Dokumenttypen
Absence	Hinweis über Abwesenheit

Tabelle 6: Datenbank „ReceiverData“

Die Datenbank „DeliveryLogData“ speichert die Protokollierung der Vorgänge.

Datenbank *DeliveryLogData*	
DeliveryID	ID der Zustellung
ReceiverID	ID des Empfängers beim Zustelldienst
ZSDocumentID	ID des Dokuments beim Zustelldienst (in Datenbank *PostOfficeBox)*
ADDocumentID	ID des Dokuments beim Absendedienst
DispatchServiceURL	Internetadresse des Absendediensts
SenderID	ID des Absenders
SenderName	Name des Absenders
DeliveryTimeStamp	Zeitstempel der Übergabe an den Zustelldienst
NotificationTimeStamp	Zeitstempel der Verständigung
PickupTimeStamp	Zeitstempel der Abholung

Tabelle 7: Datenbank „LogData“

Die Datenbank „PostOfficeBox“ ist das eigentliche elektronische Postfach, in dem die vom Zustelldienst übernommenen Dokumente aufbewahrt werden.

Datenbank *PostOfficeBox*	
DocumentID	ID des Dokuments
Document	Dokument (in verschlüsselter Form)
HashValue	Hash-Wert des Dokuments
DeliveryID	ID der Zustellung
ReceiverID	ID des Empfängers beim Zustelldienst

Tabelle 8: Datenbank „PostOfficeBox“

7.3.2 Attribute der Komponenten

Absendedienst

DispatchData : DispatchID, SenderID, ReceiverID, DocumentID, DeliveryServiceList
Die für die Absendung notwendigen Daten: Vorgangsnummer, ID des Absenders, ID des Empfängers, ID der Dokumente, Liste der Zustelldienste bei denen der oder die Empfänger registriert (ist) sind

ReceiverData : ReceiverID, Name, Adress, DocumentTypes, Public
Die Daten des Empfängers: ID des Empfängers, Name, Adresse, akzeptierte Dokumenttypen, optionaler Public Key

DocumentList: DocumentID, Document, Hash value
Die Liste der abzusendenden Dokumente: ID des Dokuments, das Document selbst, der Hash-Wert des Dokuments

Zustelldienst

DispatchData : DispatchID, SenderID, ReceiverID, DocumentID, DeliveryServiceList
Die für die Absendung notwendigen Daten: Vorgangsnummer, ID des Absenders, ID des Empfängers, ID der Dokumente, Liste der Zustelldienste bei denen der oder die Empfänger registriert (ist) sind

ReceiverData : ReceiverID, Name, Adress, DocumentTypes, Public
Die Daten des Empfängers: ID des Empfängers, Name, Adresse, akzeptierte Dokumenttypen, optionaler Public Key

DocumentList: DocumentID, Document, Hash value
Die Liste der abzusendenden Dokumente: ID des Dokuments, das Document selbst, der Hash-Wert des Dokuments

Signaturerstellungs- prüfungsmodul

UserID
Die ID des Benutzers

UserPrivateKey
Der Private-Key des Benutzers zur Erstellung der elektronischen Signatur

Benutzerschnittstelle Absender

SenderID
Die ID des momentan angemeldeten Absenders

DispatchID
Die ID der aktuellen Absendung (Vorgangsnummer)

Benutzerschnittstelle Empfänger

ReceiverID
Die ID des momentan angemeldeten Empfängers

DocumentList
Liste der Dokumente im Postfach des Empfängers

DocumentID
Die ID des momentan ausgewählten Dokuments

Authblock
Der Authblock bei vorliegen von neuen „eigenhändigen“ Dokumenten

7.3.3 Methoden der Komponenten

Anmerkung: Um die Übersichtlichkeit zu bewahren wurden die Methoden anhand der Anwendungsbereiche kategorisiert, und dabei jeweils mit der Kurzbezeichnung des Bereichs (Z.B. RE für Registrierungsoptionen) und einer Nummer versehen.

Absendedienst

Registrierungsoptionen (RE)

RE1. registrateSender(RegistrationData):Sucess oder Errorcode
Diese Methode registriert einen neuen Absender beim Absendedienst

*RE2. deregistrateSender(SenderID):*Sucess oder Errorcode
Diese Methode deregistriert den angegebenen Absender vom Zustelldienst

Anmeldeoptionen (AN)

AN1. loginSender():Sucess oder Errorcode
Diese Methode meldet den Absender beim Absendedienst an

AN2. logoutSender(SenderID):Sucess oder Errorcode
Diese Methode meldet den Absender vom Absendedienst ab

Durchführung von Zustellanfragen (ZA)

ZA1. searchReceiver(ReceiverData):DispatchID, DeliveryServiceList oder Errorcode
Diese Methode fragt mit den Empfängerdaten über die Schnittstelle Absendedienst – Zustellkopf beim Zustellkopf an, ob und bei welchen Zustelldiensten der (oder die) Empfänger registriert ist (sind)

Abfertigung des Dokuments (AF)

AF1. retrieveDocument(Document, DispatchID):DocumentID oder Errorcode
Diese Methode stellt per HTTP Get das Dokument dem Absendedienst bereit

AF2. setDeliveryQuality(DeliveryQuality, DispatchID):Sucess oder Errorcode
Diese Methode stellt die gewünschte Zustellqualität für die aktuelle Sendung ein

AF3. signDocument(DispatchID):Sucess oder Errorcode
Diese Methode bringt eine digitale Signatur auf dem oder den Dokument(en) an

AF4. encryptDocument(DispatchID):Sucess oder Errorcode
Diese Methode verschlüsselt das Dokument mit dem Public-Key des Empfängers

Versenden des Dokuments (SE)

SE1. setDeliveryService(DeliveryServiceID, DispatchID):Sucess oder Errorcode
Diese Methode legt den Zustelldienst fest

SE2. sendDocument(DispatchID): Success- oder Errorcode
Diese Methode bereitet das Dokument gemäß dem „DeliveryRequest“ auf und übergibt es anschließend an den Zustelldienst

Entgegennahme der Zustellbestätigung (ZB)

ZB1. takeoverDeliveryNotication(ComDelNot):ACK
Diese Methode übernimmt über die Schnittstelle Absendedienst – Zustelldienst die (signierte) Empfangsbestätigung vom Zustelldienst

Verrechnungsoptionen (VR)

VR1. getInvoice():Invoice
Diese Methode liefert den aktuellen Rechnungsstand

VR2. payInvoice(Invoice)
Diese Methode führt den Bezahlvorgang einer Rechnung aus

Zustellkopf

Abfrage der Verzeichnisdienste der Zustelldienste und Antwort (ZK)

ZK1. enquireOneReceiver(StdQuery):StdAnswer
Diese Methode fragt mittels der Daten aus der Zustellanfrage des Absendedienstes die LDAP-Verzeichnisdienste aller bekannten Zustelldienste ab, ob der Empfänger dort registriert ist. Die Ergebnisse werden in einer „StdAnswer“ zusammengefaßt

ZK2. enquireMultipleReceivers(BQuery):BAnswer
Diese Methode fragt mittels der Daten aus der Zustellanfrage des Absendedienstes die LDAP-Verzeichnisdienste aller bekannten Zustelldienste ab, ob die Empfänger dort registriert sind. Die Ergebnisse werden in einer „BAnswer“ zusammengefaßt

Zustelldienst

Registrierungsoptionen (RE)

RE1. registrateReceiver(RegistrationData):Success oder Errorcode
Diese Methode registriert einen neuen Empfänger und legt für ihn ein elektronisches Postfach beim Zustelldienst an

RE2. deregistrateReceiver(ReceiverID)
Diese Methode deregistriert den angegebenen Empfänger vom Zustelldienst

Anmeldeoptionen (AN)

AN1. loginReceiver():Success oder Errorcode
Diese Methode meldet den Empfänger beim Zustelldienst an

AN2. logoutReceiver(ReceiverID):Success oder Errorcode
Diese Methode meldet den Empfänger vom Zustelldienst ab

Verwaltung des elektronischen Postfachs (VP):

VP1. setRepresentative(ReceiverID, RepresentData):Success oder Errorcode
Diese Methode fügt einen neuen Annahmeberechtigten für eine nicht natürliche Person hinzu

VP2. setDocumentTypes(ReceiverID, DocumentTypes):Success oder Errorcode
Diese Methode speichert die gewünschten Dokumenttypen im Profil des Empfängers ab

VP3. setAbsence(ReceiverID, true/false):Success oder Errorcode
Diese Methode speichert den Abwesenheitsstatus des Empfängers ab

Abfrage des Verzeichnisdienstes (VD)

*VD1. getReceiversID(*StdQuery oder BQuery):ReceiverData
Diese Methode führt eine LDAP Abfrage des Verzeichnisdienstes des Zustelldients durch

Übernahme des Dokuments (UD)

UD1. takeoverDocument(ComDelReq):ComDelStat
Diese Methode übernimmt über die Schnittstelle Absendedienst – Zustelldienst Dokumente vom Absendedienst. Im Anschluß daran wird eine Statusmeldung an den Absendedienst gesende.

UD2. notifyReceiver(ReceiverID)
Diese Methode verständigt den Empfänger über das Eintreffen von neuen Dokumenten

Erstellung und Signierung der Zustellbestätigung oder Annahmeverweigerung (ZB)

ZB1. createAuthblock(ReceiverID):Authblock
Diese Methode erstellt den Authblock

ZB2. signAuthblock(Authblock, ReceiverID):Authblock
Diese Methode versieht den Authblock mit der digitalen Signatur des Empfängers

ZB3. createDeliveryNotification(DocumentID, Authblock oder 0): Success oder Errorcode
Diese Methode erstellt die Zustellbestätigung, versieht sie mit der digitalen Signatur des Zustelldients und baut entweder den Authblock oder eine Fehlermeldung ein

ZB4. deleteDocument(DocumentID):Success oder Errorcode
Diese Methode löscht das Dokument mit der angegebenen ID

ZB5. refuseDocument(DocumentID):Success oder Errorcode
Diese Methode sendet eine Nachricht über die verweigerte Annahme des Dokuments an den Absendedienst und löscht anschließend das Dokument aus dem Postfach

Abholung des Dokuments (AD)

AD1. getDocumentList(ReceiverID):DocumentList
Die Methode erstellt eine Liste mit den Dokumenten des angegebenen Empfängers

AD2. getDocument(DocumentID):Document
Diese Methode stellt das Dokument mit der angegebenen ID zum Download zur Verfügung

AD3. emailDocument(DocumentID):Success oder Errorcode
Diese Methode leitet das Dokument mit der angegebenen ID per E-Mail an den Empfänger weiter

AD4. checkSignature(DocumentID): Success oder Errorcode
Diese Methode prüft die Signatur des Dokuments

Identifikationsmodul

Einlesen und Überprüfen der Identifikationsdaten (ID)

ID1. readOutIdentificationdata():IdentificationData
Diese Methode liest die Identifikationsdaten des Absenders bzw. des Empfängers aus.

ID2. checkUserdata(IdentificationData):Success oder Errorcode
Diese Methode überprüft die Identifikationsdaten auf Richtigkeit

Signaturerstellungs- prüfungsmodul

Erstellen der Signatur (ES)

ES1. createSignature(Document):SignedDocument
Diese Methode versieht ein Dokument mit einer digitalen Signatur

Prüfen der Signatur (PS)

PS1. checkSignature(Signature, Document, PublicKey):Success oder Errorcode
Diese Methode prüft bei Übergabe einer digitalen Signatur eines Dokuments und des Public-Keys des Signators, ob die übergebene Signatur korrekt ist

Benutzerschnittstelle Absender

Anmerkung:

Die Benutzerschnittstelle Absender implementiert selbst nur Funktionen zum Einlesen des Dokuments und von Eingaben des Empfängers. Die restliche Funktionalität kommt durch Aufruf der korrespondierenden Methoden beim Absendedienst zu Stande.

Einlesen von Daten (ME)

ME1. readInSenderData()
Diese Methode liest die Absenderdaten ein

ME2. readInReceiverData():ReceiverData
Diese Methode liest die Empfängerdaten ein

ME3. readInDocument():Document
Diese Methode liest das Dokument ein

Anzeigen von Daten (MA)

MA1. displayDeliveryNotification()
Diese Methode zeigt die Zustellbestätigung an

MA2. displayInvoice()
Diese Methode zeigt den aktuellen Rechnungsstand an

Delegationsmethoden (DM)

DM1. registrateSender()
Diese Methode ruft die korrespondierende Methode zur Registrierung beim Absendedienst auf

DM2. deregistrateSender()
Diese Methode ruft die korrespondierende Methode zur Deregistrierung beim Absendedienst au.

DM3. loginSender()
Diese Methode ruft die korrespondierende Methode zur Anmeldung beim Absendedienst auf

DM4. logoutSender()
Diese Methode ruft die korrespondierende Methode zur Abmeldung beim Absendedienst auf

DM5. checkDeliverability()
Diese Methode ruft die korrespondierende Methode zur Zustellanfrage beim Absendedienst auf

DM6. chooseDeliveryQuality()
Diese Methode liest die gewünschte Zustellqualität ein

DM7. signDocument()
Diese Methode ruft die korrespondierende Methode zum Signieren des Dokuments beim Absendedienst auf

DM8. chooseDeliveryService()
Diese Methode liest ein über welchen Zustelldienst das Dokument versendet werden soll

DM9. sendDocument()
Diese Methode ruft die korrespondierende Methode zum Versenden des Dokuments beim Absendedienst auf

DM10. payInvoice()
Diese Methode ruft die korrespondierende Methode zum Bezahlen einer Rechnung beim Absendedienst auf

Benutzerschnittstelle Empfänger

Anmerkung:

Die Benutzerschnittstelle Empfänger implementiert selbst nur Funktionen zum Anzeigen der Dokumentenliste des Dokuments und der Zustellbestätigung, zur Auswahl eines Dokuments und zur Entschlüsselung eines chiffrierten Dokuments.

Die restliche Funktionalität kommt durch Aufruf der korrespondierenden Methoden beim Zustelldienst zu Stande.

Einlesen von Daten (ME)

ME1. readInReceiverData()
Diese Methode liest die Empfängerdaten ein

Anzeigen von Daten (MA)

MA1. displayDocumentList()
Diese Methode zeigt dem Empfänger die Liste der Dokumente in seinem Postfach an.

MA2. displayDeliveryAuthentification()
Diese Methode zeigt dem Empfänger die abzusendende Zustellbestätigung an

MA3. displayDocument()
Diese Methode holt das ausgewählte unverschlüsselte Dokument vom Zustelldienst und zeigt es dem Empfänger am Bildschirm an

Delegationsmethoden (DM)

DM1. registrateReceiver()
Diese Methode ruft die korrespondierende Methode zur Registrierung beim Zustelldienst auf

DM2. deregistrateReceiver()
Diese Methode ruft die korrespondierende Methode zur Deregistrierung beim Zustelldienst auf

DM3. loginReceiver()
Diese Methode ruft die korrespondierende Methode zur Anmeldung beim Zustelldienst auf

DM4. logoutReceiver()
Diese Methode ruft die korrespondierende Methode zur Abmeldung beim Zustelldienst auf

DM5. downloadDocument()
Diese Methode holt das ausgewählte unverschlüsselte Dokument vom Zustelldienst und speichert es lokal beim Empfänger

DM6. emailDocument()
Diese Methode ruft die korrespondierende Methode beim Zustelldienst zum Weiterleiten des Dokuments per E-Mail auf

DM7. signDeliveryNotification()
Diese Methode ruft die korrespondierende Methode beim Zustelldienst zur Signierung der Zustellbestätigung auf

DM8. refuseDocument()
Diese Methode ruft die korrespondierende Methode beim Zustelldienst zur Ablehnung des Dokuments auf

DM9. checkSignature()
Diese Methode ruft die korrespondierende Methode beim Zustelldienst zur Prüfung der Signatur des Dokuments auf

Allgemeine Hilfsmethoden (HF)

HF1. selectDocument()
Diese Methode speichert die ID des aus der Liste gewählten Dokuments

HF2. decryptDocument()
Diese Methode entschlüsselt ein verschlüsseltes Dokument

7.4 Beschreibung der Formate für den Datenaustausch

Die Kommunikation zwischen den einzelnen Systemkomponenten erfolgt, bis auf wenige Ausnahmen, mittels SOAP Nachrichten, deren Aufbau in weiterer Folge beschrieben wird.

7.4.1 Benutzerschnittstelle Absender – Absendedienst

Erfolgs- oder Fehlernachricht (SuccessErrorcode)

Die Erfolgs- oder Fehlermeldung ist nach folgendem Schema aufgebaut:

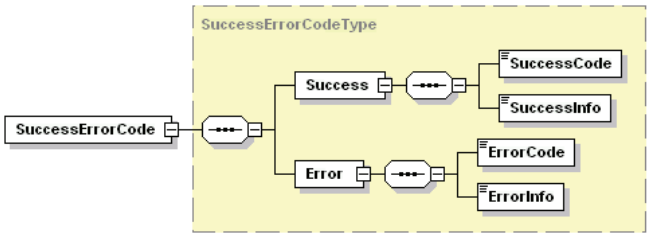

Abbildung 16: XML Schema „SucessErrorCode“

Datenformat für Rechnung (Invoice)

Die Rechnung für Absendungen wird nach dem, in Abbildung 17 dargestellten Schema „Invoice“, aufgebaut.

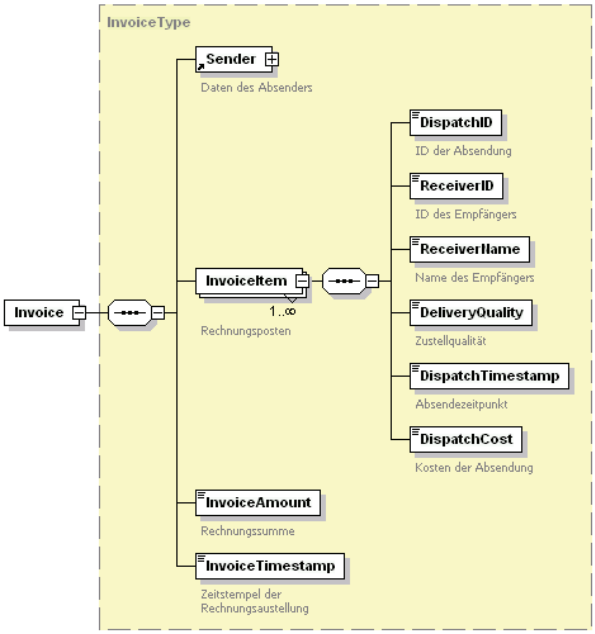

Abbildung 17: XML Schema “Invoice“

Sonstige Nachrichten

Des Weiteren werden noch triviale SOAP - Nachrichten zur Angabe der Empfängerdaten für die Zustellanfrage (ReceiverData), der Zustellqualität (DeliveryQuality) und zur Wahl des Zustelldients (DeliveryService) gesendet, deren Datenformat nicht spezifiziert wird.

7.4.2 Absendedienst – Zustellkopf

Einzelanfrage beim Zustellkopf (StdQuery)

Eine Einzelanfrage muß gemäß des in Abbildung 18 illustrierten „StdQuery“ Schemas aufgebaut sein:

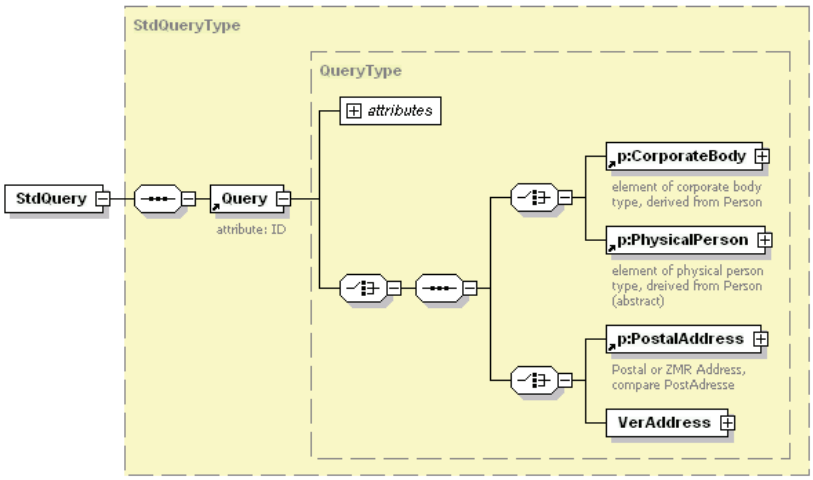

Abbildung 18: XML Schema "StdQuery"

Es wird zwischen Anfragen für natürliche und nicht natürliche Personen unterschieden. Bei natürlichen Personen kann die Anfrage auf drei Arten erfolgen:

- Mittels Namen (p:PhysicalPerson) und Adresse (p:PostalAdress) und optionalen Geburtsdatum bei eigenhändigen Zustellungen
- Mittels Namen (p:PhysicalPerson) und Verständigungsadresse (VerAdress) und optionalen Geburtsdatum bei eigenhändigen Zustellungen

Bei nicht natürlichenn Personen kann die Anfrage auf analog erfolgen:

- Mittels Bezeichnung (p:CorporateBody) und Adresse (p:PostalAdress)
- Mittels Bezeichnung (p:CorporateBody) und Verständigungsadresse (VerAdress)

Zusätzlich zu den Daten muß bei der Anfrage eine ID zur eindeutigen Identifikation mitübergeben werden, die später mit der Antwort wieder zurückgesendet wird.

Einzelantwort des Zustellkopfs (StdAnswer)

Der Zustellkopf antwortet auf eine Einzelanfrage durch eine SOAP Nachricht, die auf dem Schema „StdAnswer“ ([LiHo04], S. 10) des behördlichen Modells basiert.

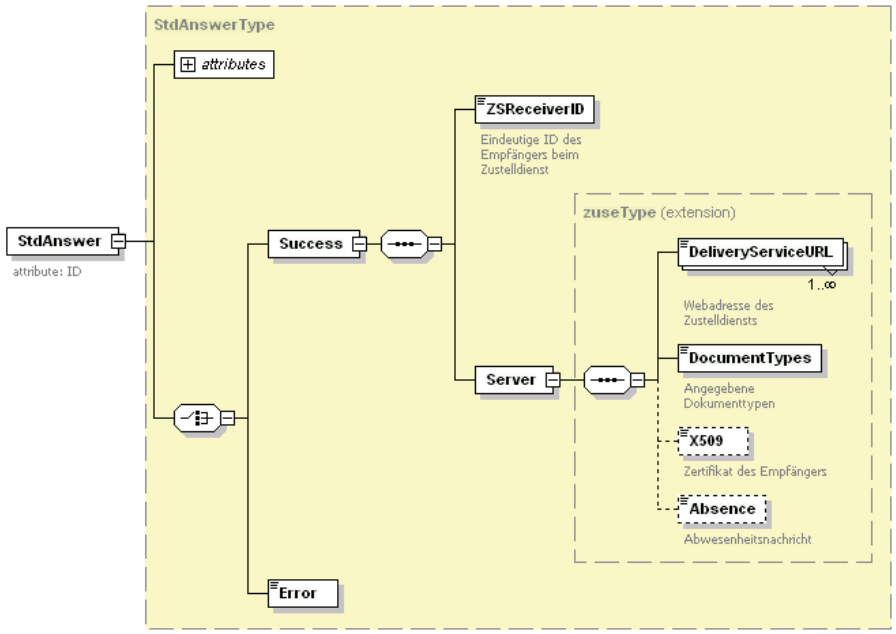

Abbildung 19: XML Schema "StdAnswer"

Ist der Empfänger bei keinem Zustelldienst registriert, wird eine Fehlermeldung (Error) gesendet.

Wenn an dem Empfänger elektronisch zugestellt werden kann, so sind in den Unterelementen von „Success“ folgende Daten enthalten:

- Die eindeutige ID des Empfängers beim Zustelldienst (ZSReceiverID)
- Die Internetadresse der Zustelldienste, bei denen der Empfänger registriert ist. (DeliveryServiceURL)
- Die Dokumenttypen, die dem Empfänger zugestellt werden können. (DocumentTypes)
- Das optionale Verschlüsselungszertifikat des Empfänges (X509)
- Die optionale Abwesenheitsmeldung des Empfängers (Absence)

Bulkanfrage an den Zustellkopf (BQuery)

Bei der Bulkanfrage an den Zustellkopf kann in einem Schritt für beliebig viele Empfänger angefragt werden.
Die Anfrage muß gemäß des aus dem behördlichen Modell entnommenen und adaptierten „BQuery“ ([LiHo04], S. 12) Schemas aufgebaut sein
Gemäß des „BQuery“ Schemas können im Gegensatz zum „StdQuery“ Schema beliebig viele „Query“ Elemente enthalten sein.

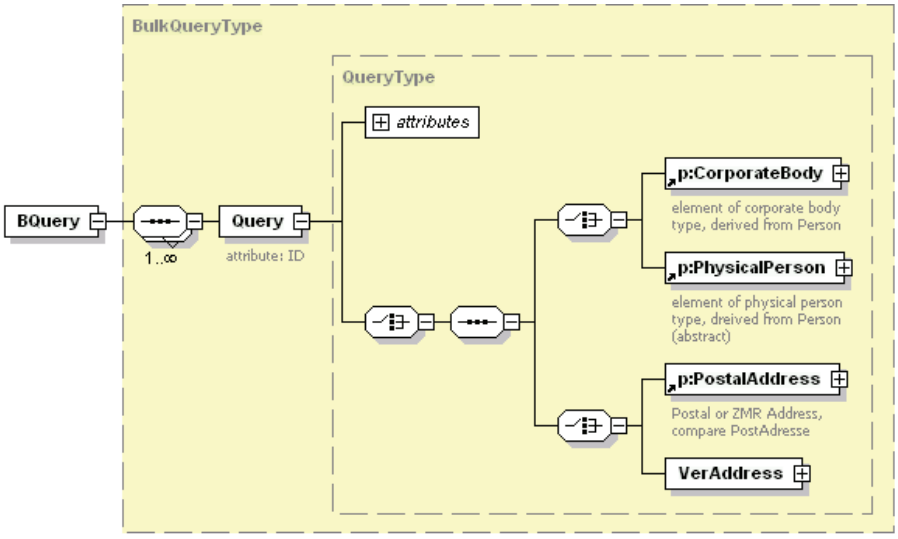

Abbildung 20: XML Schema "BQuery"

Bulkantwort des Zustellkopf (BAnswer)

Die Antwort des Zustellkopfs auf Mehrfachanfragen ist gemäß des „BAnswer“ Schema aufgebaut und basiert auf dem behördlichen „BulkAnswer“ ([LiHo04], S. 20) Schema

Dabei können beliebig viele Unterelemente „Answer“ vorkommen, die alle die gleiche Bedeutung wie im „StdAnswer“ Schema haben.
Neu sind beim „BulkAnswer“ Schema allerdings das Element „ZUSEUrl“, das zusammengefaßt die Adressen aller gefundenen Zustelldienste enthält, und das Element „DocumentTypes“, das analog alle akzeptierten Dokumenttypen enthält.

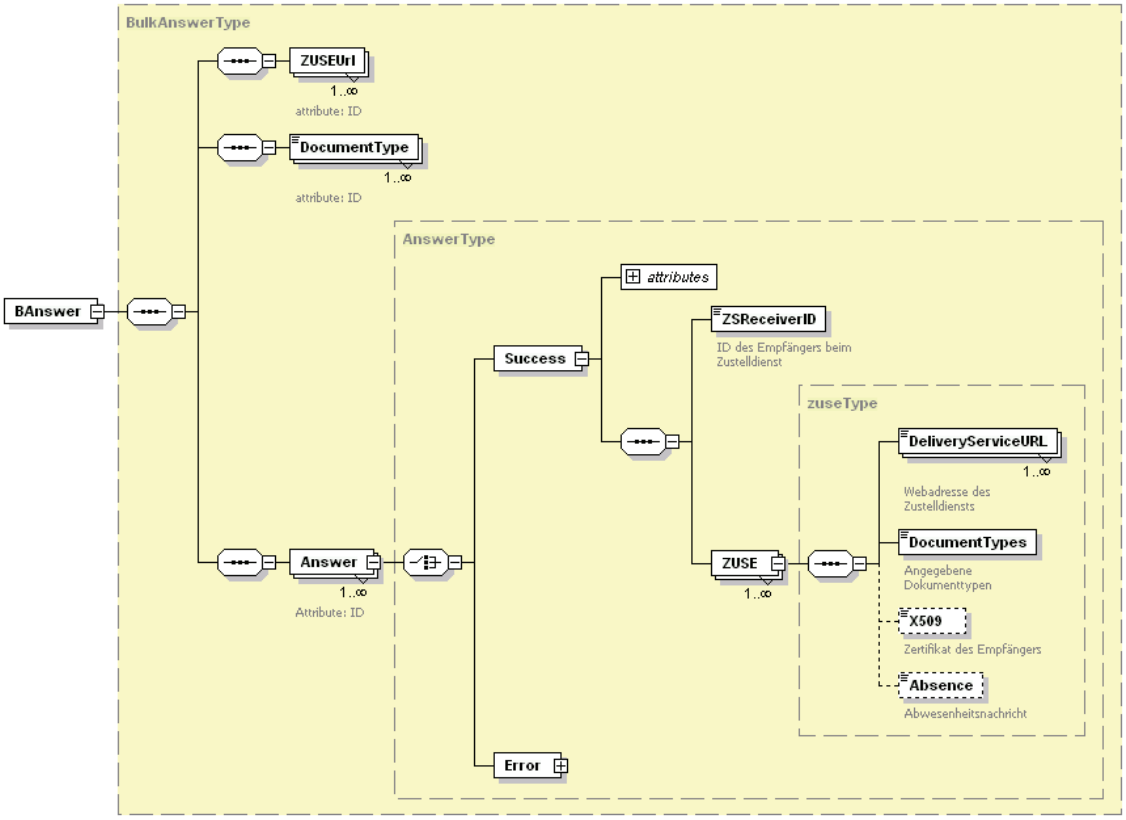

Abbildung 21: XML Schema "BAnswer"

7.4.3 Zustellkopf – Zustelldienst

Die Definition der Schnittstelle zwischen dem Zustellkopf und dem Zustelldienst basiert auf der behördlichen Spezifikation in [LHHM04].

Anfrage beim Verzeichnisdienst des Zustelldients (LDAPQuery)

Der Zustellkopf führt mittels der Parameter der Anfrage des Absendiedienstes eine LDAP-Abfrage über HTTP Get bei den Verzeichnisdiensten aller bekannten Zustelldienste durch.

PARAMETER	BESCHREIBUNG
cn	Bezeichnung der nicht natürlichenn Person
sn	Nachname
givenName	Vorname
tel	Telefonnummer
mail	E-Mail
gvBirthdate	Geburtsdatum
street	Straße
postCode	Postleitzahl
municipilaty	Ort
countryCode	Land
notAdress	Verständigungsadresse

Tabelle 9: LDAP Parameter

Bei natürlichen Personen kann die Abfrage Parameter enthalten;

- Nachname (sn), Vorname (givenName) und Adresse (street, postCode, municipilaty) und optionalem Geburtsdatum (gvBirthdate) bei eigenhändigen Zustellungen
- Nachname(sn), Vorname (givenName) und Verständigungsadresse (notAdress) und optionales Geburtsdatum (gvBirthdate) bei eigenhändigen Zustellungen.

Bei nicht natürlichenn Personen erfolgt die Anfrage analog:

- Bezeichnung (cn) und Adresse (street, postCode, municipilaty)
- Bezeichnung (cn) und Verständigungsadresse (notAdress)

Antwort des Verzeichnisdienstes des Zustelldients (LDAPAnswer)

Die Antwort des Verzeichnisdienstes „LDAPAnswer“ erfolgt unabhängig davon, ob es sich bei der Person um eine natürliche oder nicht natürliche handelt. Die Antwort kann folgendermaßen aussehen:

- Keine Übereinstimmung
  Die Person ist nicht beim betreffenden Zustelldienst registriert.

- Übereinstimmung
  Die Person ist beim betreffenden Zustelldienst registriert.
  Folgende Daten werden dabei übermittelt:

  - ID des Empfängers beim Zustelldienst (ReceiverID)
  - Akzeptierte Dokumenttypen (DocumentTypes)
  - Optionaler Public-Key zur Verschlüsselung (ReceiverPublicKey)
  - Optionale Abwesenheitsnachricht (Absence)

7.4.4 Absendedienst – Zustelldienst

Übertragung des Dokuments vom Absende- zum Zustelldienst (ComDelReq)

In der SOAP Nachricht selbst werden Metainformationen zur Zustellung gespeichert und das eigentliche Dokument entweder als Attachment mitübertragen oder als Callback Attachment URL referenziert.

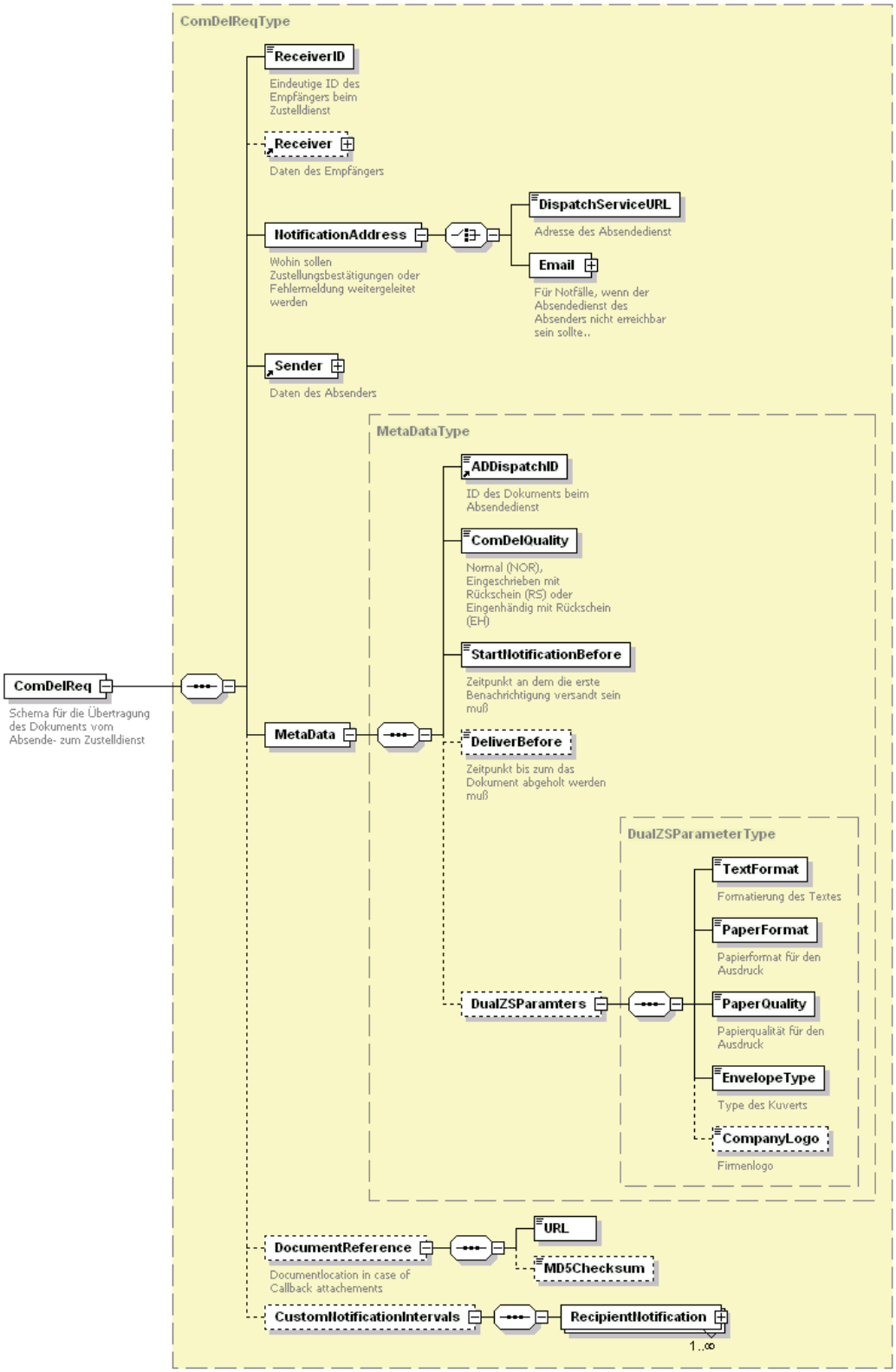

Abbildung 22: XML Schema "ComDelReq"

Die Nachricht muß gemäß dem Schema „ComDelReq“ (Abbildung 22), das auf dem behördlichen „DeliveryRequest“ ([NHRL04], S. 11) basiert, aufgebaut sein und enthält folgende Daten:

- Die eindeutige ID des Empfängers beim Zustelldienst (ReceiverID)
- (Optional) Genaue Daten des Empfängers (Receiver in Abbildung 23)
    - Eine natürliche (p:PhysicalPerson) bzw. eine nicht natürliche (p:CorporateBody) Person
    - Die Adresse des Empfänger (p:PostalAdress)

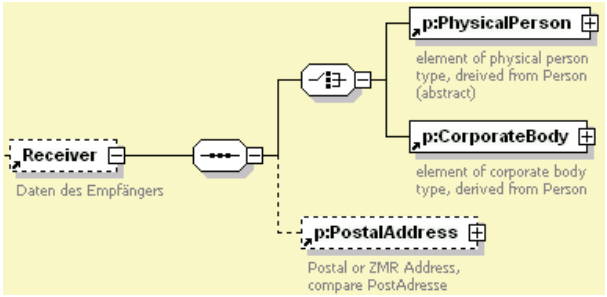

Abbildung 23: XML Schema Unterelement "Receiver"

- Adresse an die die Zustellbestätigung gesendet wird (NotificationAdress)
    - Die Internetadresse des Absendedienst (DispatchServiceURL)
    - E-Mail Adresse des Absenders für Fälle in denen der Absendedienst nicht erreichbar ist (Email)

Anmerkung:
Im hier vorgestellten Modell wird die Zustellbetätigung im Regelfall vom Zustelldienst an den Absendedienst, der sie dann an Absender weiterleitet, gesendet. Der Vorteil davon ist, daß der Absender flexibler mit dem Absendedienst vereinbaren kann, wie er die Zustellbestätigung erhalten möchte (z.B. per E-Mail oder über das Webinterface, etc.). Man erspart sich dadurch auch eine direkte Schnittstelle zwischen Zustelldienst und Absender zu implementieren.

- Genaue Daten des Absenders (Sender in Abbildung 24
    - Die eindeutige ID des Absenders beim Absendedienst (SenderID)
    - Der Public-Key zur Verifikation der Absendersignatur (PublicKey)
    - Weitere Daten des Absenders (p:PhysicalPerson bzw. p:CorporateBody)

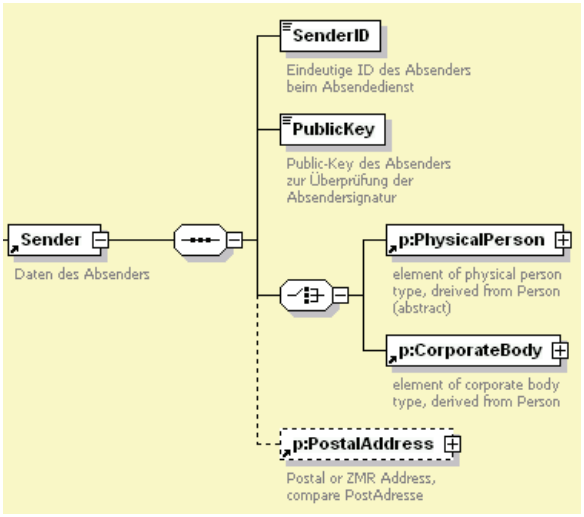

Abbildung 24: XML Schema Unterelement "Sender"

- Die für die Zustellung notwendigen Metadaten (MetaData)
  - ID des Dokuments beim Absendedienst (ADDispatchID)
  - Die Zustellqualität (ComDelQuality)
  - Spätester Zeitpunkt der ersten Verständigung (StartNotificationBefore)
  - Spätester Zeitpunkt zum Abholen des Dokuments (DeliverBefore)
  - Paramter für den Druck bei Anwendung der dualen Zustellung (DualZSParamters)

- Die URL des Dokuments, wenn dieses als Callback – Attachment abgeholt wird (DocumentReference)
- Intervalle für die Benachrichtigung des Empfängers (CustomNotificationIntervall)

Erfolgs- oder Fehlermeldung bei Annahme des Dokuments (ComDelStat)

Der Zustelldienst sendet nach Erhalt des Dokuments eine Bestätigung an den Absendedienst. Das dafür verwendete Schema „ComDelStat“ .basiert auf dem behördlichen „DeliveryRequestStatus“ ([NHRL04], S. 17)

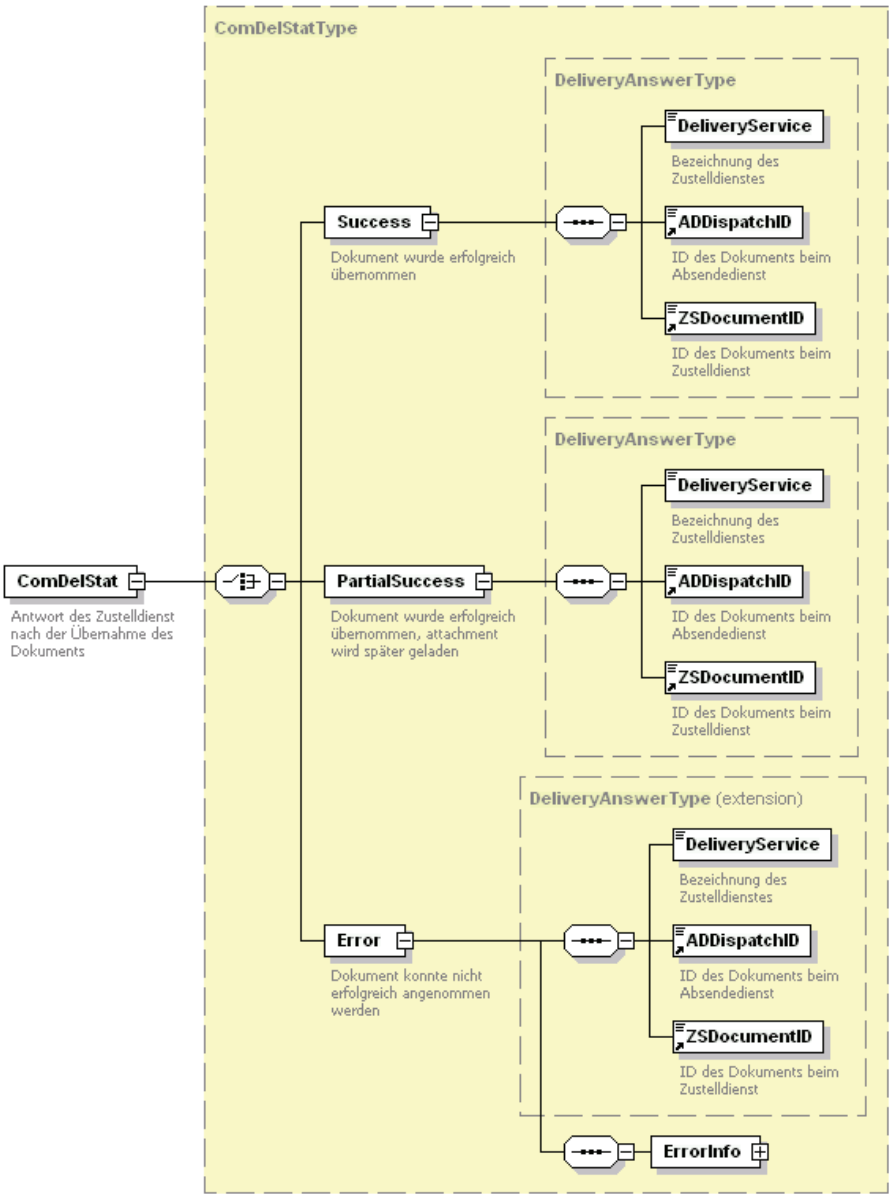

Abbildung 25: XML Schema „ComDelStat“

Die Nachricht enthält den jeweiligen Status der Dokumentenannahme:

- Erfolgreiche Annahme des Dokuments (Success)
- Teilweise Erfolgreiche Annahme, wenn das Dokument per Callback – URL über HTTP-Get nachgeladen wird (PartialSuccess)
- Fehler bei der Annahme des Dokuments (Error)
  Die Fehlermeldung erhält einen Fehlercode und einen Fehlertext. Fehler treten auf, wenn der Empfänger nicht beim Zustelldienst registriert ist oder die gesendeten Dokumenttypen nicht empfangen will.

Folgende Daten sind dazu im jeweiligen Statuselement enthalten:

- Die Bezeichnung des Zustelldienst (DeliveryService)
- Die ID des Dokuments beim Absendedienst (ADDispatchID)
- Die ID des Dokuments beim Zustelldienst (ZSDocumentID)

Datenformat der Zustellbestätigung (ComDelNot)

Das Datenformat der Zustellbestätigung „ComDelNot“ basiert auf dem behördlichen XML Schema „DeliveryNotification“ ([NHRL04], S. 19)
Dabei sind in jedem Fall folgende Daten enthalten:

- Die Bezeichnung des Zustelldients (DeliveryService)
- Die ID des Dokuments beim Absendedienst (ADDispatchID)
- Die ID des Dokuments beim Zustelldienst (ZSDocumentID)
- Informationen über erfolgte Verständigungen

In Abbildung 26 wird der Aufbau der Zustellbestätigung bei erfolgreicher Zustellung dargestellt, wobei folgende Daten hinzugefügt werden:

- Genaue Daten des Absenders (Sender)
- Genaue Daten des Empfängers (Receiver)
- Zeitstempel der Signaturerstellung des Empfänger (ConfirmationTimestamp)
- Der Authblock (AuthBlock)
  Dieser enthält die persönlichen Daten des Empfängers und einen Zeitstempel der Anmeldung.
- Signatur des Empfängers (dsig:Signature)

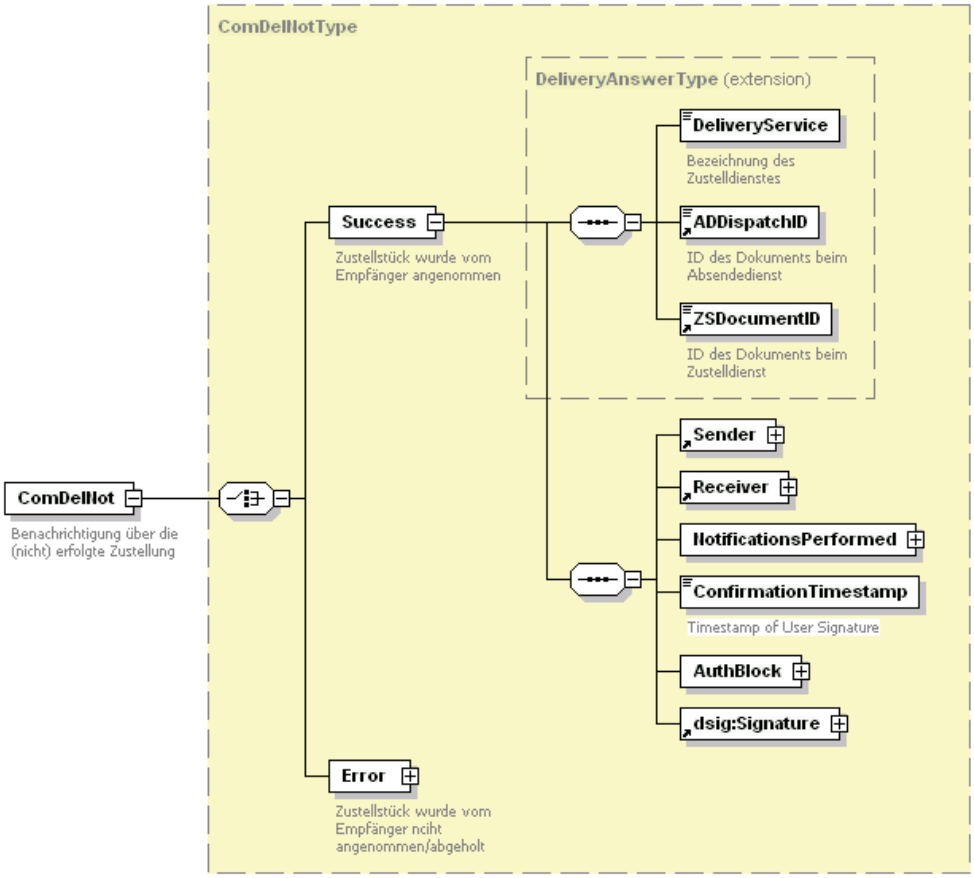

Abbildung 26: XML Schema „ComDelNot“ im Erfolgsfall

In Abbildung 27 wird die Zustellbestätigung bei nicht erfolgreicher Zustellung dargestellt. Dabei werden folgende Daten hinzugefügt:

- Fehlermeldung (ErrorInfo)
  Die Fehlermeldung enthält einen Fehlercode und einen Fehlertext. Mögliche Fehler sind die Nichtabholung bzw. die Annahmeverweigerung eines Dokuments oder das Fehlschlagen der elektronischen Verständigung des Empfängers
- Digitale Signatur des Zustelldients (ZUSESignature)

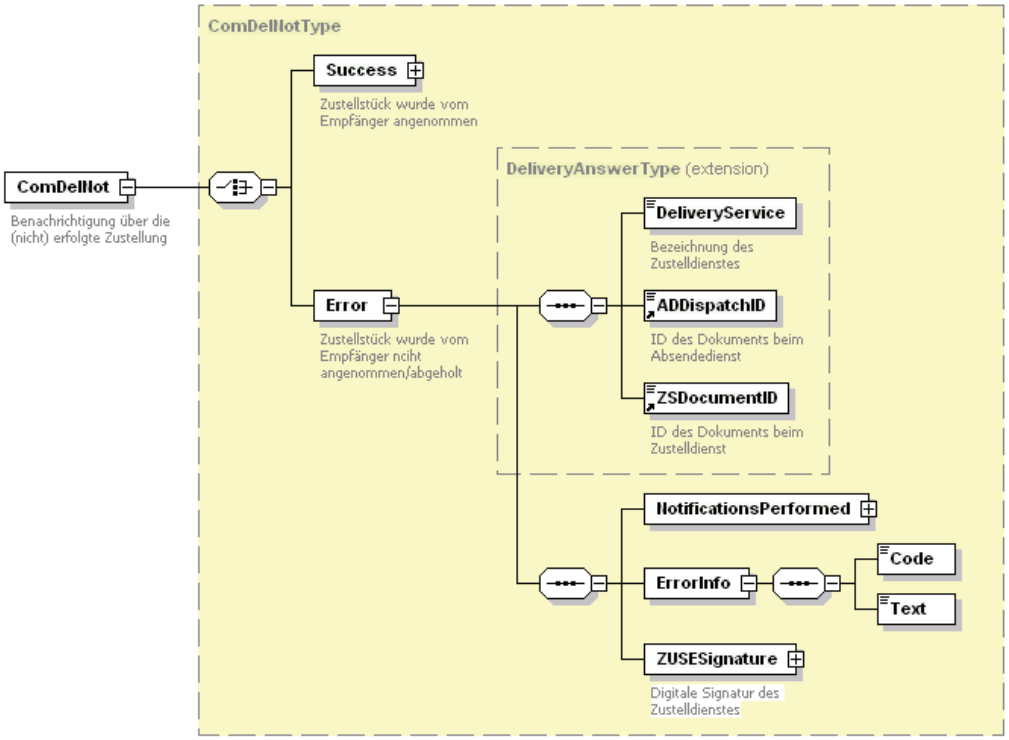

Abbildung 27: XML Schema „ComDelNot“ bei fehlgeschlagener Zustellung

Weitere Fehler bei der Kommunikation können bei Störungen in der Übertragung oder bei Nicht-Erreichbarkeit oder Überlastung des Absende- bzw. Zustelldients auftreten.

7.4.5 Zustelldienst – Benutzerschnittstelle Empfänger

Erfolgs- oder Fehlernachricht (SuccessErrorcode)

Das Datenformat entspricht dem in Abschitt 7.4.1 beschriebenen.

Datenformat für die Dokumentliste (DocumentList)

Die Liste der Dokumente wird dem Schema „DocumenList“ entsprechend vom Zustelldienst an die Benutzerschnittstelle Empfänger gesendet.

In Abbildung 28 wird das „DocumentList“ Schema dargestellt:

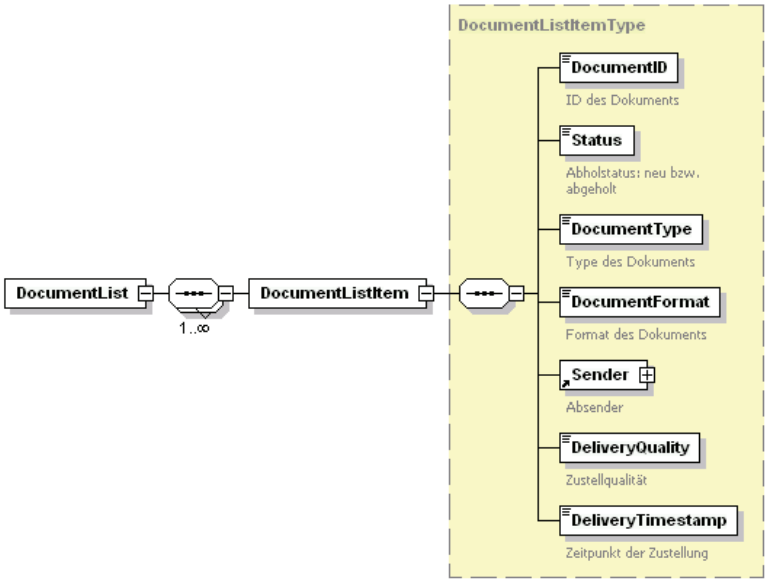

Abbildung 28: XML Schema "DocumentList"

Sonstige Nachrichten

Weitere triviale SOAP-Nachrichten, wie beispielsweise zum Übermitteln der Registrierungsdaten des Empfängers und zur Übergabe der Dokumenten ID, werden hier nicht näher spezifiziert.

7.5 Ablauf der kommerziellen elektronischen Zustellung

Nachdem im Laufe dieses Kapitels die Softwarearchitektur und die einzelnen Systemkomponenten beschrieben und für den Absender bzw. Empfänger spezifische Konzepte diskutiert wurden, soll nun ein detaillierter Überblick über den Ablauf der kommerziellen elektronischen Zustellung gegeben werden.
Grundlage für die Modellierung des Ablaufs ist ebenfalls der behördliche elektronische Zustellprozeß, der hier in einigen Punkten abgewandelt, angewandt wird.

7.5.1 Aus der Sicht des Absenders

Nachfolgend wird der Prozeß der kommerziellen elektronischen Zustellung aus der Sicht des Absenders in Form von ereignisgesteuerten Prozeßketten, kurz EPK, modelliert.
Zur Bewahrung der Übersichtlichkeit wurde der Kernprozeß in mehrere Subprozesse unterteilt. Die Unterteilung orientiert sich an den wichtigsten Use-Cases des Absenders: Anmelden, Zustellanfrage, Abfertigung des Dokuments, Absenden des Dokuments.

EPK Notation

	Ein Ereignis stellt das Eintreten eines bestimmten Zustands dar.		Nachricht, die einer Funktion zugeordnet ist.
	Eine Funktion stellt eine Aktivität dar.		Verknüpfungsoperatoren: UND, ODER, EXKLUSIV ODER
	Systemkomponente, die an der Ausführung einer Funktion beteiligt ist.		Verweis auf einen Unterprozeß

Tabelle 10: EPK Notation

Die EPK Notation wurde aus [KNS92] entnommen.

Kernprozeß aus Absendersicht

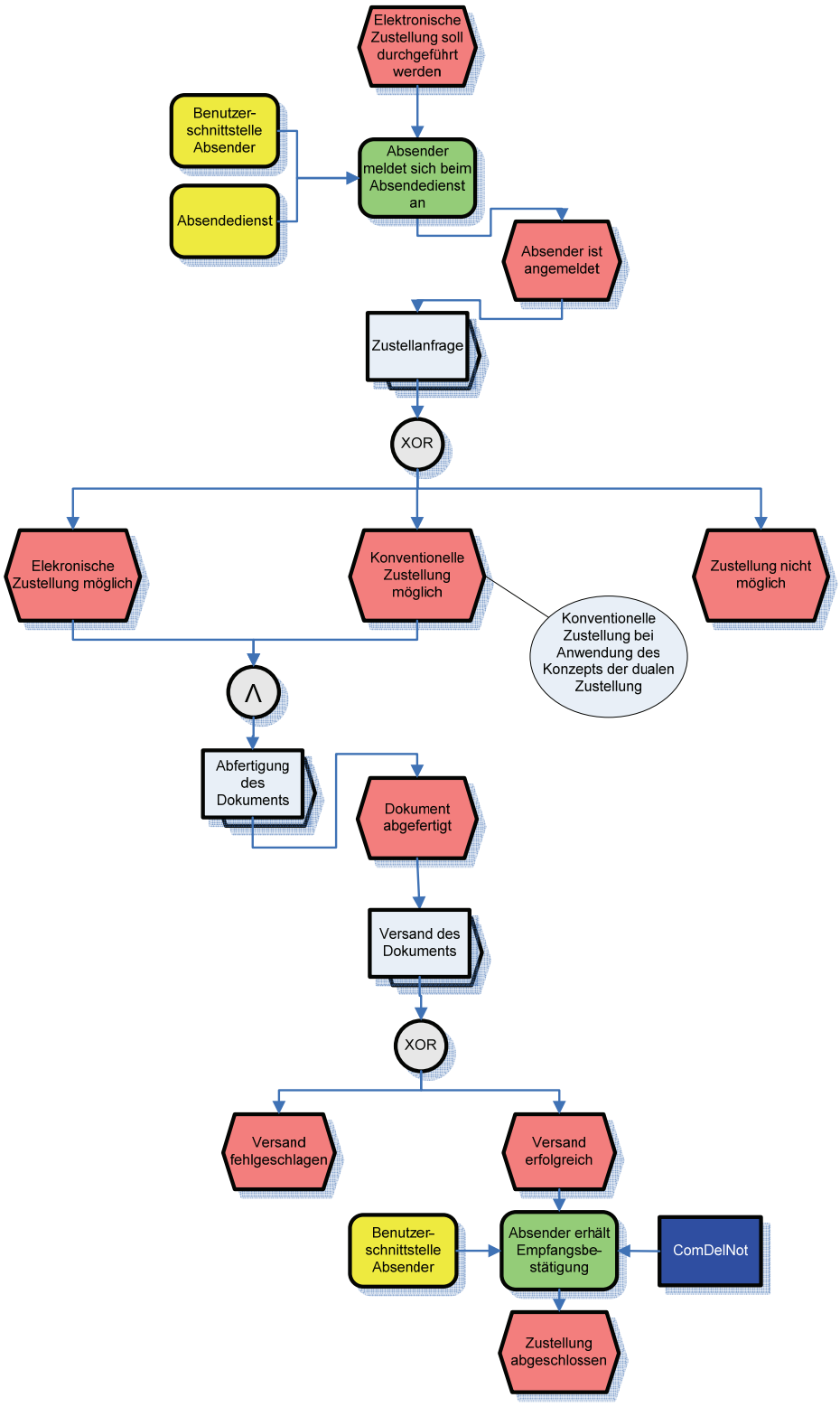

Abbildung 29: EPK aus Absendersicht

Zustellanfrage

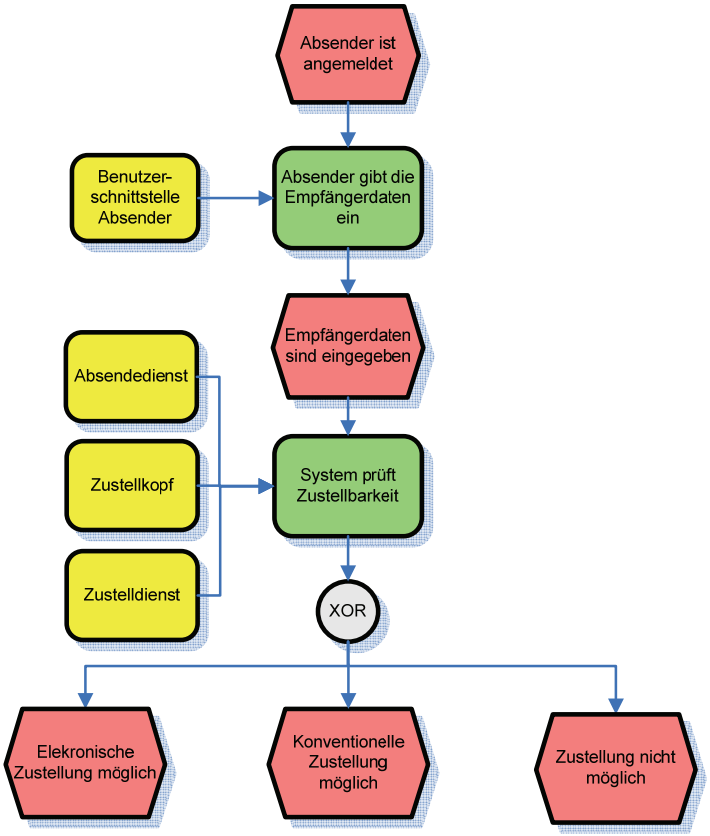

Abbildung 30: EPK Subprozeß „Zustellanfrage“

Abfertigung des Dokuments

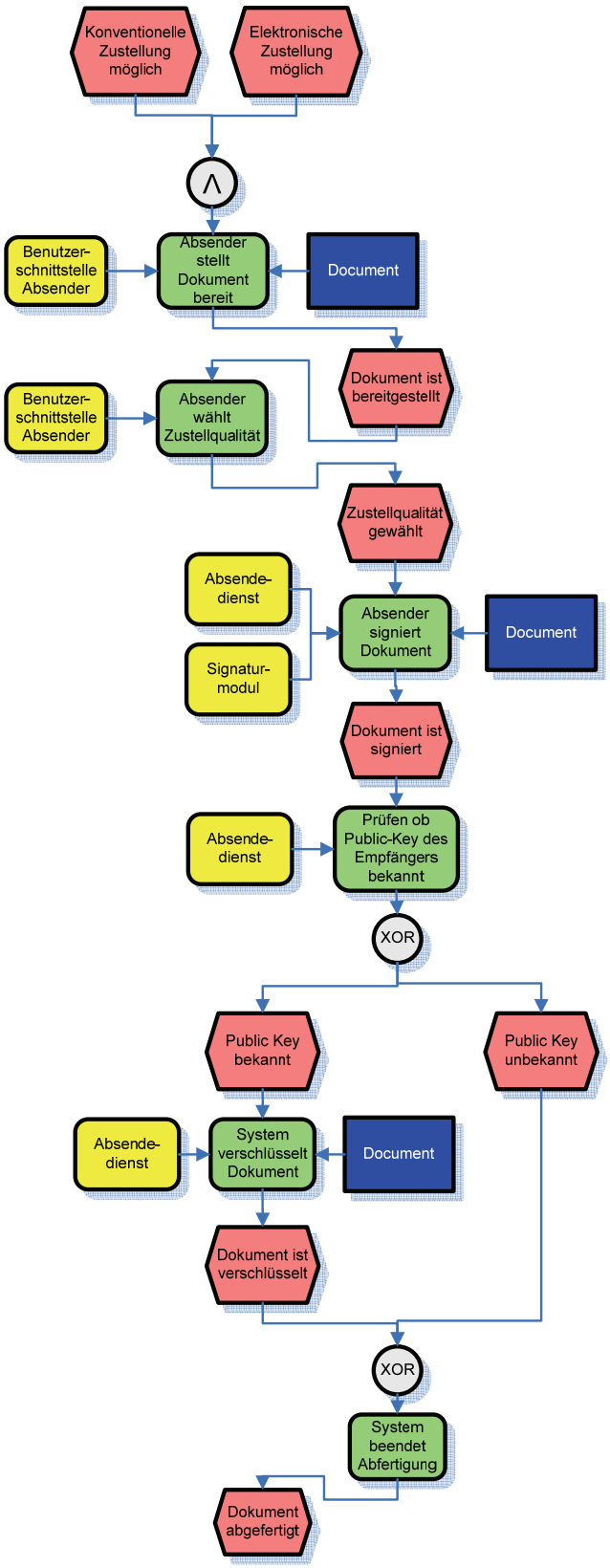

Abbildung 31: EPK Subprozeß „Abfertigung des Dokuments"

Versand des Dokuments

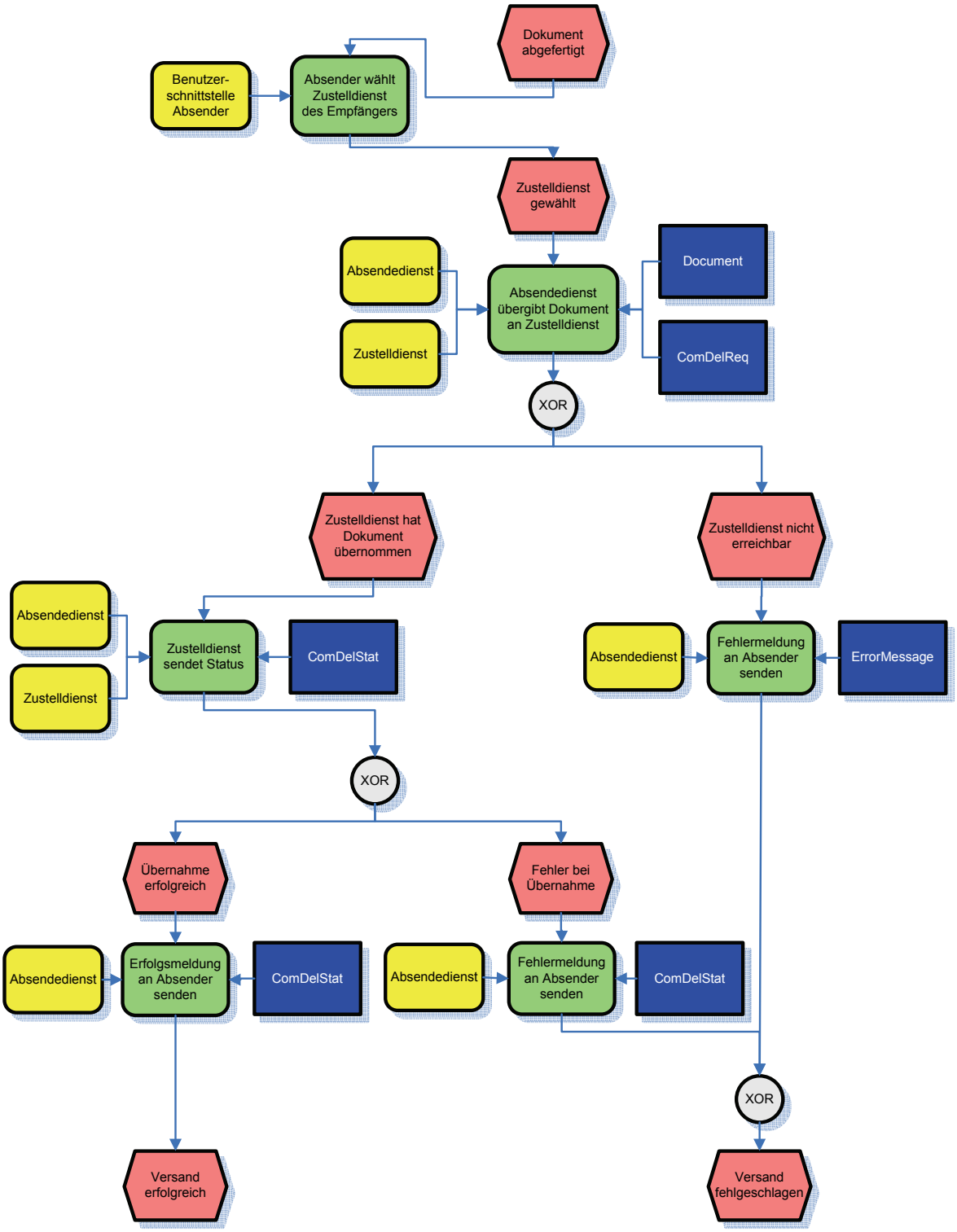

Abbildung 32: EPK Subprozeß „Versand des Dokuments“

7.5.2 Aus der Sicht des Empfängers

Der Kernprozeß wurde ebenfalls in mehrere Subprozesse unterteilt. Die Unterteilung erfolgt anhand der Use-Cases: Verständigung erhalten, Signierung der Zustellbestätigung bzw. Ablehnung der Annahme und Abholung des Dokuments.

Kernprozeß aus Empfängersicht

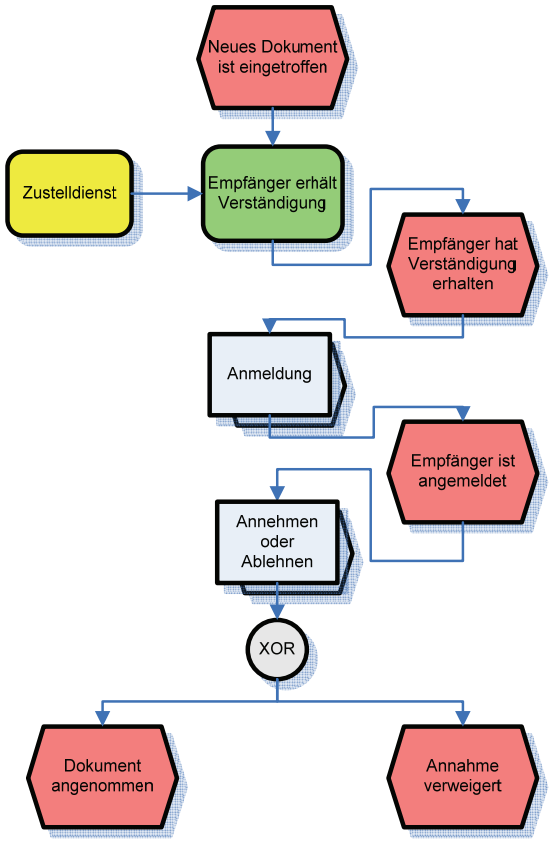

Abbildung 33: EPK aus Empfängersicht

Anmeldung des Empfängers und Signierung des Authblocks

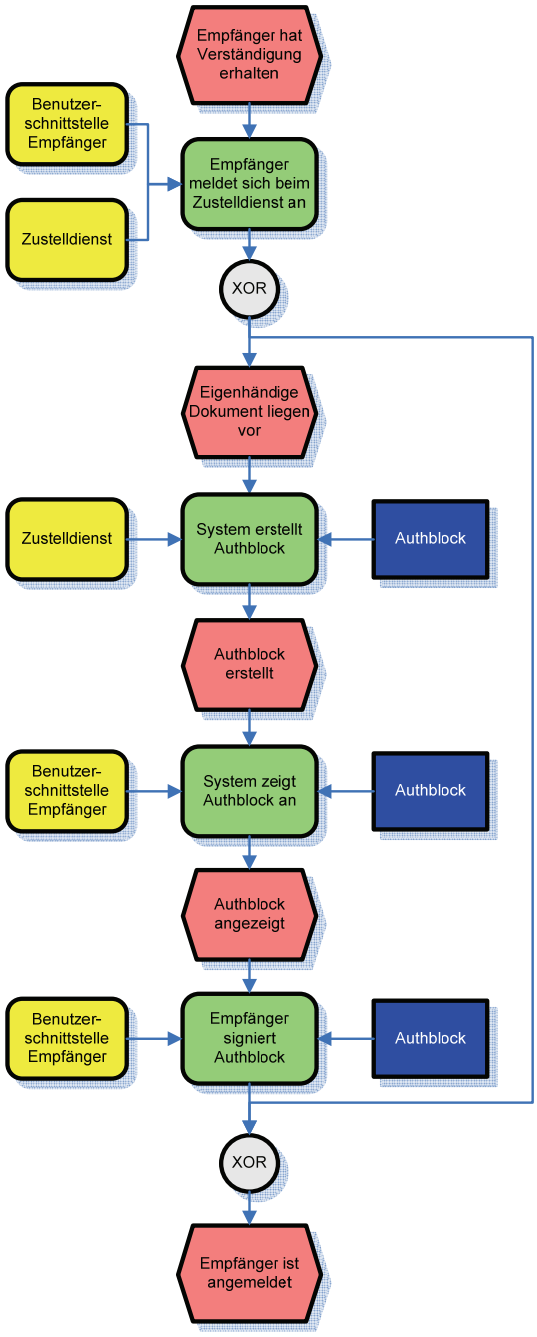

Abbildung 34: EPK Subprozess „Anmelden Empfänger“

Annahme bzw. Ablehnung des Dokuments

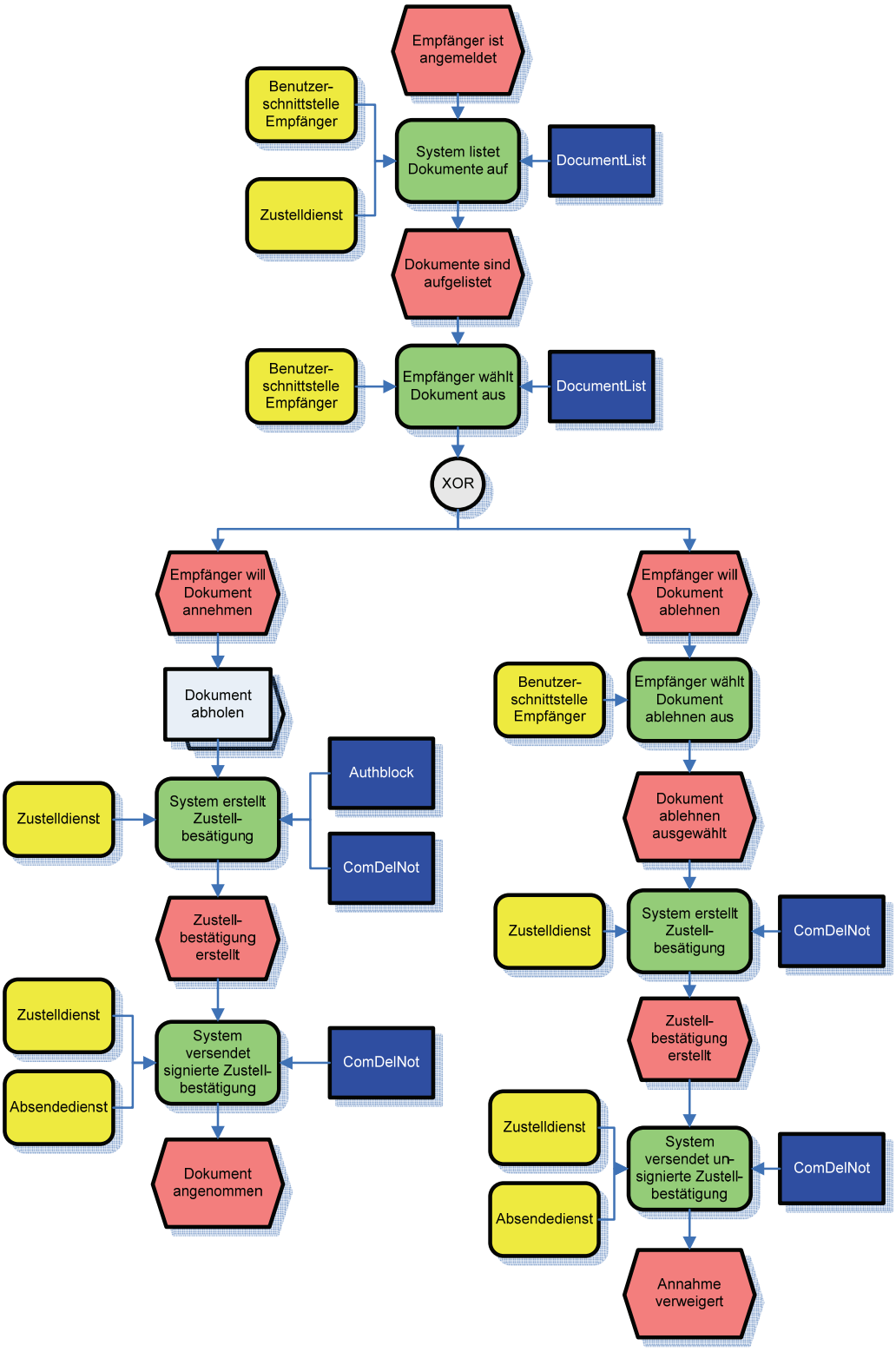

Abbildung 35: EPK Subprozess „Annahme bzw. Ablehnung des Dokuments“

Abholung des Dokuments

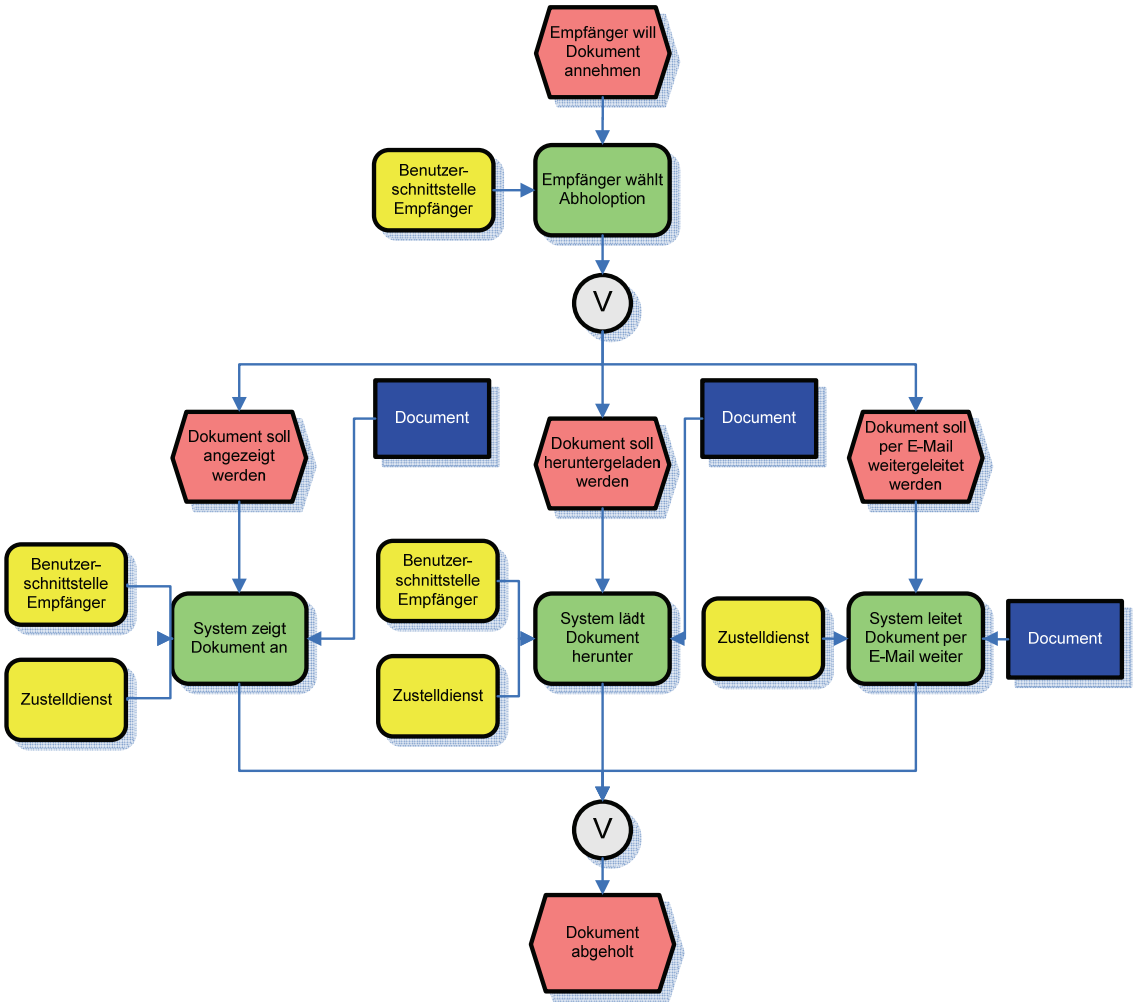

Abbildung 36: EPK Subprozess „Abholung des Dokuments“

7.5.3 Aus der Sicht der Systemkomponenten

Im Weiteren wird der Ablauf der kommerziellen elektronischen Zustellung aus der Sicht der beteiligten Systemkomponenten beschrieben. Ziel dabei ist es, den zeitlichen Kontrollfluß der Komponenten sowie den Nachrichtenaustausch zwischen den Komponenten darzustellen. Es soll ebenfalls gezeigt werden, wann während des Ablaufs ein Eingreifen des Absenders bzw. Empfängers notwendig ist.

Anmeldung des Absenders

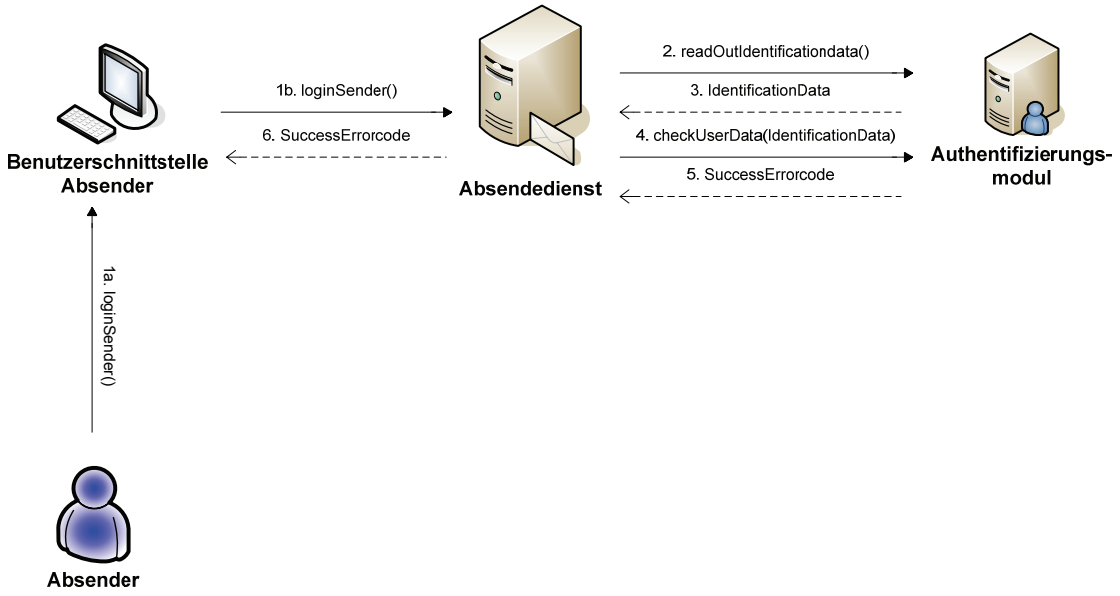

Abbildung 37: Ablaufdiagramm Anmeldevorgang Absender

Der Absender startet in Schritt 1 den Anmeldevorgang. In den Schritten 2-5 werden vom Authentifizierungsmodul die Identifikationsdaten des Absenders eingelesen und überprüft.

Wie dies in der Realität tatsächlich abläuft, hängt von der eingesetzten Authentifizierungsmethode ab.

Zustellanfrage

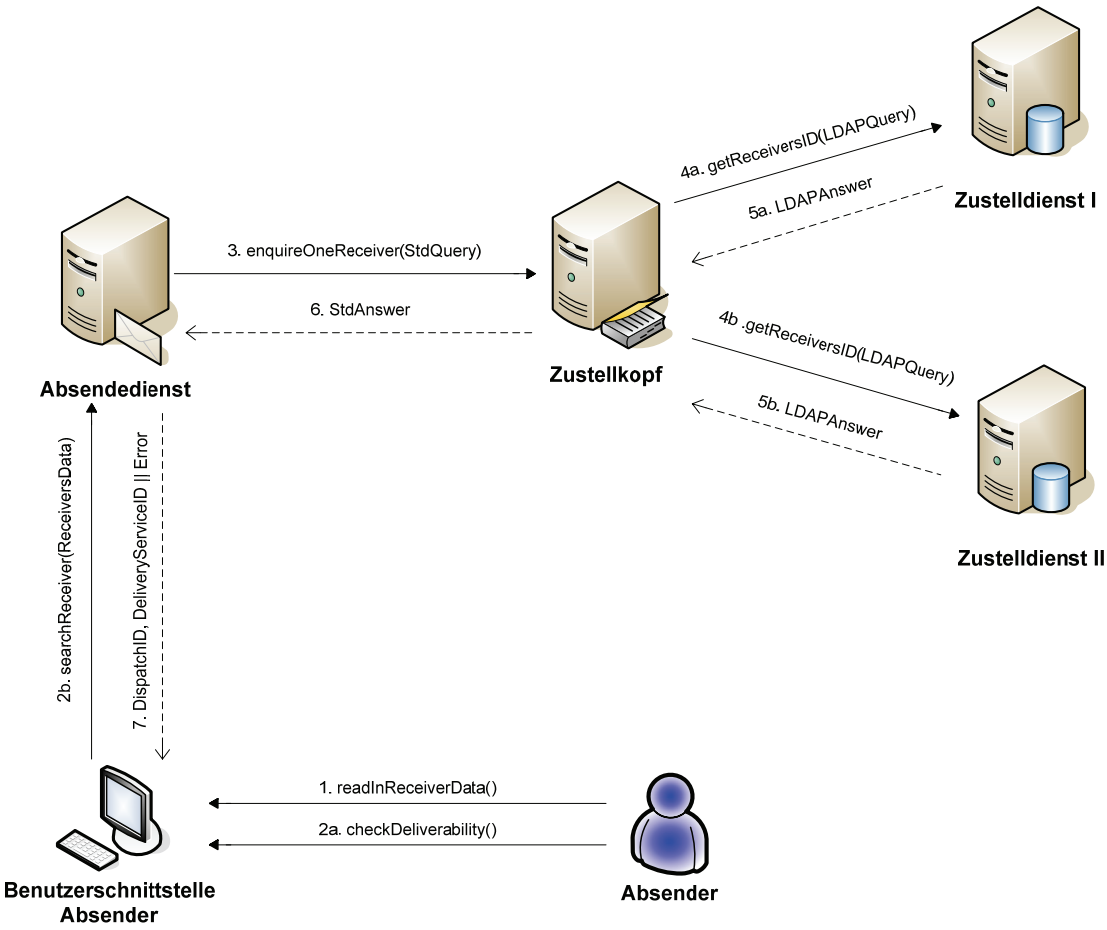

Abbildung 38: Ablaufdiagramm Zustellanfrage

Im dargestellten Fall wird die Anfrage für genau einen Empfänger durchgeführt.

Nach erfolgtem Anmeldevorgang gibt der Absender die Daten des Empfängers über die Benutzerschnittstelle Absender ein (Schritt 1). Der Absendedienst führt eine Zustellanfrage beim Zustellkopf durch.

In Schritt 3 wird die Methode „equireOneReceiver“ für eine Einfachabfrage beim Zustellkopf aufgerufen.

(Bei einer Mehrfachanfrage, müßten die Anfragedaten gemäß dem Schema „BQuery“ strukturiert werden und der Methode „enquireMultipleReceivers“ übergeben werden.)

Weiters werden vom Zustellkopf an die Verzeichnisdienste aller bekannten Zustelldienste LDAP Abfragen gesendet. In diesem Modell hier, wird die Anfrage in den Schritten 4a bzw. 4b vereinfacht nur für zwei Zustelldienste dargestellt.

Abfertigung des Dokuments

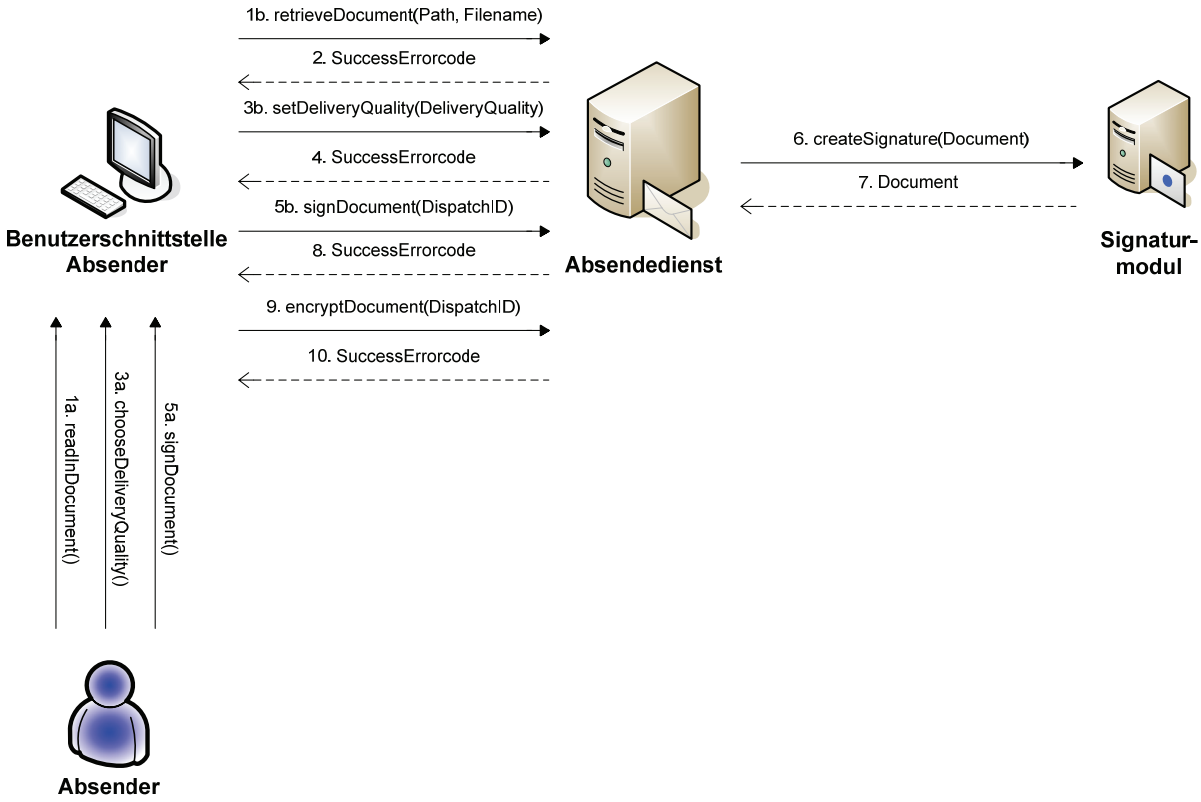

Abbildung 39: Ablaufdiagramm Abfertigung des Dokuments

In diesem Modell wird nur die Abfertigung eines einzelnen Dokuments beschrieben. Wenn mehrere Dokumente abgesendet werden sollen, wiederholen sich die Schritte 1-10 dementsprechend oft.

Zur Erstellung der digitalen Signatur auf dem Dokument, in den Schritten 5a bis 7, kommt das externe Signaturmodul zum Einsatz. Bei der Erstellung einer sicheren elektronischen Signatur wird das Dokument dem Absender vor dem Auslösen des Signaturvorgangs noch einmal angezeigt.

Die Auslösung des Signaturvorgangs könnte bei der Verwendung einer niedrigeren Signaturqualität automatisiert werden.

Die Verschlüsselung des Dokuments in Schritt 10 kann nur durchgeführt werden, wenn der Public-Key des Empfängers bekannt ist.

Versand des Dokuments

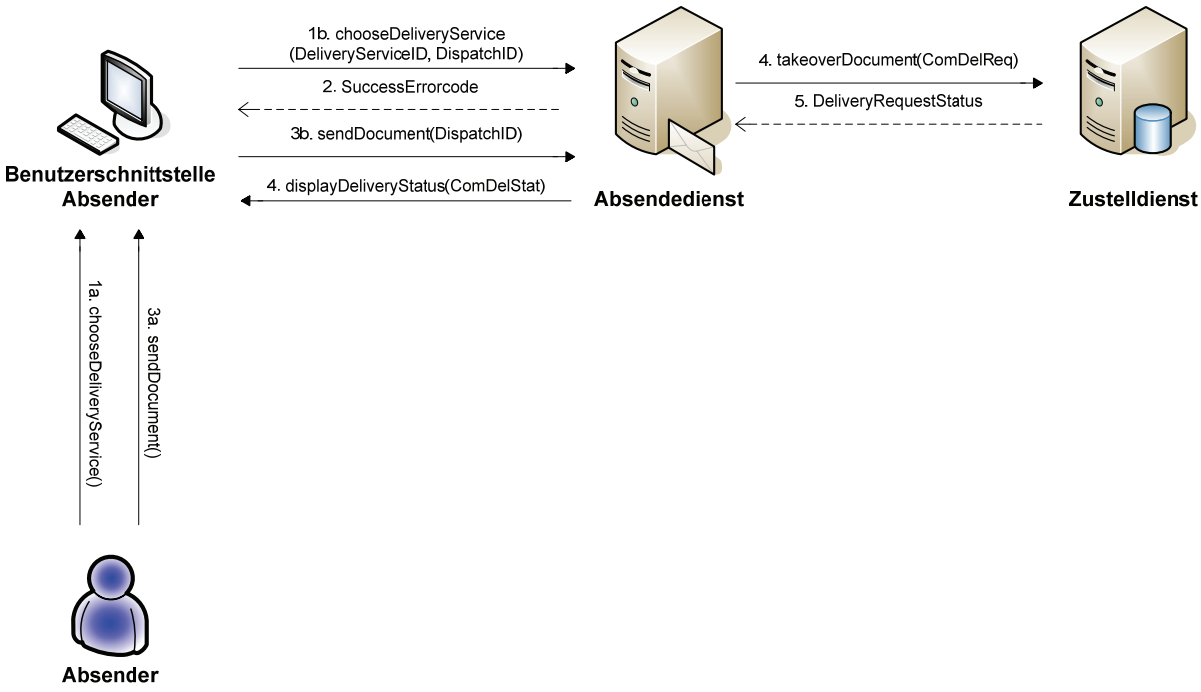

Abbildung 40: Ablaufdiagramm Versand des Dokuments

Der Absender wählt den Zustelldienst (Schritt 1a) und sendet anschließend das Dokument über die Benutzerschnittstelle Absender (Schritt 3a) ab. In Schritt 4 übergibt der Absendedienst das Dokument an den Zustelldienst. Ist in Schritt 4 der Zustelldienst trotz wiederholten Versuchs aus irgendeinem Grund nicht erreichbar, sendet der Absendedienst eine Fehlermeldung an den Absender und bricht den Absendevorgang ab.

Benachrichtigung, Anmeldung des Empfängers und Signierung des Authblocks

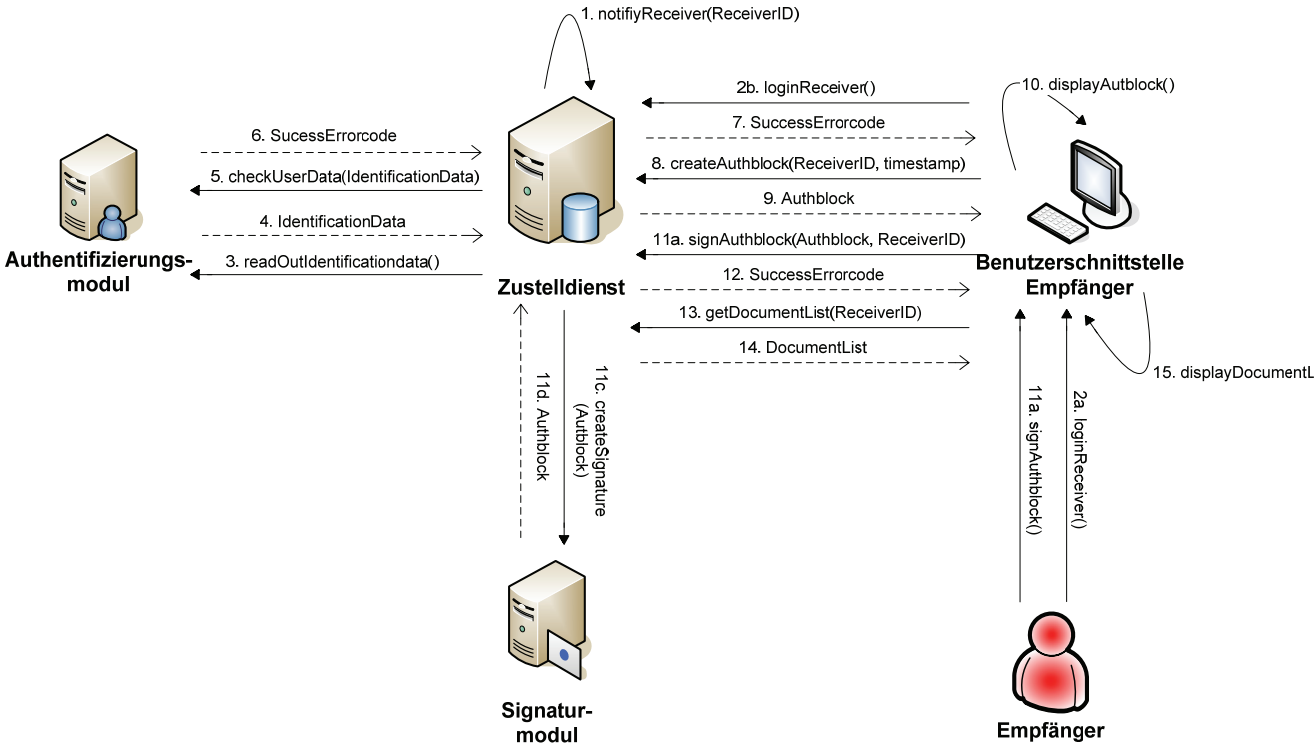

Abbildung 41: Ablaufdiagramm Benachrichtigung, Anmeldung Empfänger

Sobald der Zustelldienst neue Dokumente übernommen hat, verständigt er automatisch den Empfänger. (Schritt 1)

Der Anmeldevorgang des Empfängers (Schritt 2a bis 7) findet analog zu dem des Absenders statt.

Nach dem erfolgreichen Anmelden wird, wie in diesem Fall dargestellt, bei Vorliegen von eigenhändig anzunehmenden Zustellstücken der Authblock vom Zustelldienst erstellt. (Schritt 8 bis 9)

Im Anschluß daran wird der Autblock in den Schritten 11a – 12 vom Absender mit Hilfe des Signaturmoduls signiert.

Nach dem Signieren des Authblocks werden dem Empfänger die Dokumente aufgelistet (Schritt 13 – 15).

Ablehnung eines Dokuments

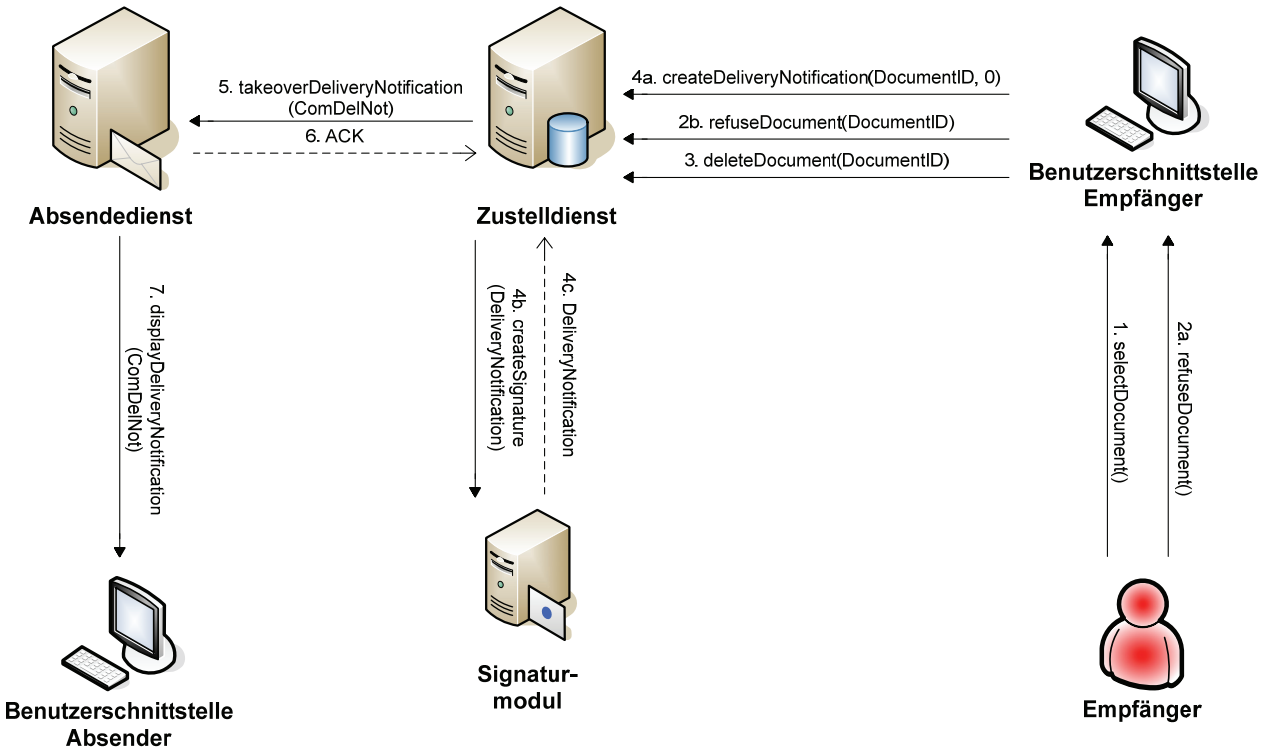

Abbildung 42: Ablaufdiagramm Ablehnung eines Dokuments

Der Empfänger wählt ein Dokument aus der Liste (Schritt 1) und anschließend die Option „Annahme verweigern“. (Schritt 2a) Der Zustelldienst löscht darauf das Dokument vom Server (Schritt 2b bis 3), und erzeugt eine Zustellbestätigung über die nicht erfolgreiche Zustellung, die mit der digitalen Signatur des Zustelldients versehen wird (Schritt 4).

Die Zustellbestätigung wird in Schritt 5 an den Absendedienst gesendet, der sie dann an den Absender weiterleitet. Sollte der Absendedienst im Ausnahmefall nicht erreichbar sein, sendet der Zustelldienst die Zustellbestätigung per E-Mail an den Absender.

Abholung des Dokuments, Erstellung und Versand der Zustellbestätigung

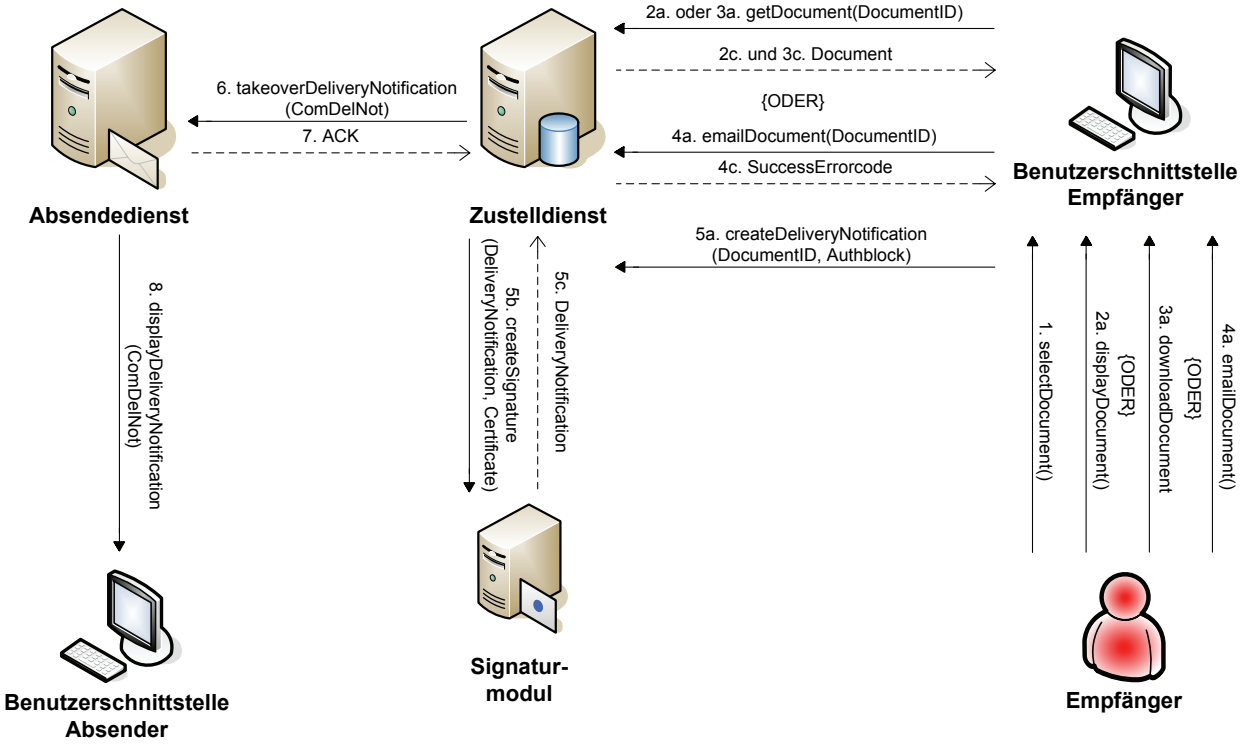

Abbildung 43: Ablaufdiagramm Abholung, Erstellung und Versand der Zustellbestätigung

Anmerkung zum Abholvorgang:

Der Empfänger wählt ein Dokument aus der Liste (Schritt 1). Das Dokument kann nun auf drei verschiedene Arten abgeholt werden:

Wenn das Dokument nicht verschlüsselt ist, kann das Dokument direkt von der Benutzerschnittstelle Empfänger angezeigt werden. (siehe Schritt 2a bis 2c.)

Weiters besteht die Möglichkeit das Dokument auf dem lokalen Rechner zu speichern (Schritt 3a bis 2c) oder an eine E-Mail Adresse (Schritt 4a bis 4c) weiterzuleiten.

Der Zustelldienst erstellt daraufhin eine signierte Zustellbestätigung über die erfolgreiche Zustellung, in der der Authblock mit der digitalen Signatur des Empfängers eingebaut wird. (Schritt 5a bis 5c). Die Zustellbestätigung wird am Ende an den Absendedienst gesendet. (Schritt 6)

8 Anwendungsszenarien für die kommerzielle elektronische Zustellung

8.1 Allgemeines Anwendungsszenario

Mit der Einführung der kommerziellen elektronischen Zustellung wird erstmals die Möglichkeit einer durchgängig gesicherten elektronischen Kommunikation zwischen Bürgern, Unternehmen und Behörden (jeweils auch untereinander) ermöglicht [Baum07b].

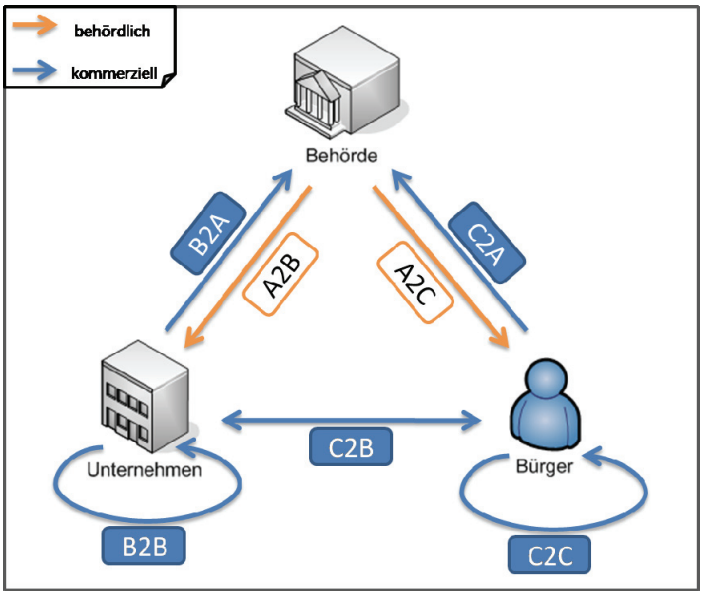

Abbildung 44: Kommunikationswege der elektronischen Zustellung

Die kommerzielle elektronische Zustellung erweitert dabei die behördliche um folgende Kommunikationswege:

- Bürger an Bürger (C2C)
- Unternehmen an Unternehmen (B2B)
- Unternehmen an Bürger (B2C)
- Bürger an Behörden (C2A)
- Unternehmen an Behörden (B2A)

Durch die neue Möglichkeit für Bürger und Unternehmen an Behörden elektronisch zuzustellen, entstehen neue Synergien.

Im speziellen kann ein Bürger bzw. ein Unternehmen auf eine behördliche Zustellung,. antworten. Voraussetzung dabei ist nur, daß die Behörde ebenfalls ein elektronisches Postfach bei einem Zustelldienst besitzt Der Vorgang würde folgendermaßen ablaufen:

1. Der Bürger bzw. ein Unternehmen hat ein Dokument von der Behörde zugestellt bekommen und wählt die Option „Antworten“
2. Der Absendedienst des Bürgers bzw. Unternehmens führt mit den Daten der Behörde eine Zustellanfrage beim Zustellkopf durch und übergibt anschließend das Dokument an den Zustelldienst der Behörde
3. Der Zustelldienst verständigt den zuständigen Sachbearbeiter, der daraufhin das Dokument abholt

8.2 Spezielle Anwendungsszenarien

8.2.1 Ausschreibungsmanagement

Bei Ausschreibungen ist es im Regelfall wichtig, daß die von den Teilnehmern erstellten Unterlagen, nicht vor einem bestimmten Zeitpunkt vom Ausschreiber geöffnet werden können [Baum06].
Mittels elektronischer Zustellung könnte dies folgendermaßen realisiert werden:

1. Die Dokumente der Teilnehmer werden mittels elektronischer Zustellung eingereicht.
2. Der Teilnehmer hat durch den Zeitstempel der Absendung den Beweis für das termingerechte Einreichen.
3. Der Ausschreiber erhält die Verständigung über das Vorliegen der Unterlagen und bestätigt den Empfang, kann aber die Unterlagen noch nicht öffen.
4. Der Teilnehmer erhält die Bestätigung über die erfolgreiche Zustellung.
5. Die Unterlagen können vom Ausschreiber zu einem speziell festgelegten Zeitpunkt geöffnet werden.

8.2.2 e-Zustellung „Ultra Light“

Bei e-Zustellung „Ultra Light“ handelt es sich um ein Konzept des Projekts „kommerzielle e-Zustellung“ [WWW12], das vorsieht, an nicht registrierte Empfänger, deren E-Mail Adresse aber bekannt ist, elektronisch zustellen zu können [Baum06].

Dies würde folgendermaßen ablaufen:

1. Der Absender gibt die E-Mail Adresse des Empfängers dem Absendedienst bekannt.
2. Der Absender lädt das Dokument auf dem Absendeserver.
3. Der Absendedienst sendet eine Verständigungsnachricht per E-Mail an den Empfänger. In der E-Mail ist ein eindeutiger Link zum Dokument vorhanden.
4. Der Empfänger holt das Dokument über Aufruf des Links ab.
5. Der Absendedienst registriert den Download und leitet eine Zustellbestätigung an den Absender weiter.

Die e-Zustellung „Ultra-Light“ bietet zwar nur geringe Rechtssicherheit, jedoch ist diese höher als bei einer normalen E-Mail anzusehen [Baum06].

8.2.3 Elektronische Rechnung und elektronischer Zahlschein

In Österreich existiert seit kurzer Zeit ein ebInterface [WWW03] genannter Standard für elektronische Rechnungen. Dabei handelt es sich um XML – basierte Rechnungen, die mit einer digitalen Signatur versehen sind. Es existieren auch Schnittstellen zum Einbinden der elektronischen Rechnung in ERP-Systeme.

Des Weiteren wird in Zukunft ein elektronischer Zahlschein [Mart05] eingeführt werden. Der elektronische Zahlschein wird insbesondere zum asynchronen Bezahlen, wie z.B. nach Abschluß eines E-Government Verfahrens, verwendet werden.

In der Spezifikation zum elektronischen Zahlschein wird für die Übermittlung der Einsatz der elektronischen Zustellung vorgeschlagen.
Für die Übermittlung der elektronischen Rechnung bietet sich ebenfalls die elektronische Zustellung als Alternative zur Übermittlung über E-Mail oder zur Abholung am Internetportal des jeweiligen Unternehmens an [Baum06].

8.2.4 Elektronischer Rechtsverkehr

Die elektronische Übermittlung von Klagen und Schriftsätzen an Gerichte ist an und für sich nichts Neues. Laut gesetzlicher Regelung im Gerichtsorganisationsgesetz [GOG06] ist die Teilnahme am elektronischen Rechtsverkehr (ERV) schon seit Ende Jänner 1998 für alle Rechtsanwälte und Notare verpflichtend.

Das heute eingesetzte System für den ERV wurde im Jahr 2001 von Seiten der Telekom Austria entwickelt [WWW05].
Die Schnittstellen dieses System sind, wie bei der elektronischen Zustellung offengelegt. Der Datenaustausch findet unter Verwendung des international gebräuchlichen ebXML Formats [ebXML01] über das Internet statt.

Die Praxis zeigt allerdings, daß im Kanzleialltag der ERV nicht besonders gut angenommen wird. Gründe dafür sind unter Anderem:

- Umständlichkeit, da Klagen und Schriftsätze doppelt verfaßt werden müssen und nur auf konventionelle Weise verbessert werden können.
- Unsicherheit da der ERV nur in ausgewählten Gebieten angewendet werden kann.
- Der eigene Klient bzw. der gegnerische Anwalt kann nicht in den ERV einbezogen werden, sondern muß gesondert angeschrieben werden.

Die elektronische Zustellung könnte folgendermaßen zur Optimierung des ERVs beitragen:

- Rechtsanwälte übermitteln Klagen und ergänzende Schriftsätzen aller Art elektronisch an Gerichte, insbesondere auch wenn diese eine eigenhändige Zustellung erfordern und daher nicht mit dem ERV übertragen werden dürfen [Schn05]
- Gerichte können Schriftsätze und Ladungen an Rechtsanwälte und sonstige Parteien übermitteln
- Zur besseren Kommunikation mit dem eigenen Klienten und dem gegnerischen Anwalt

9 Conclusio

9.1 Zusammenfassung der Ergebnisse

Die sichere elektronische Zustellung von Dokumenten zwischen Bürgern untereinander ist trotz technischer Kommunikationslösungen wie z.B. E-Mail heute noch nicht möglich.

Aus diesem Grund wurde im Rahmen dieser Magisterarbeit eine auf technischen und rechtlichen Gesichtspunkten basierende Anforderungsanalyse zur Einführung der kommerziellen elektronischen Zustellung durchgeführt. In weiterer Folge wurde eine Konzeption eines kommerziellen Zustellsystems vorgestellt. Dieses System ist als Erweiterung des behördlichen Zustellstellsystems konzipiert, wobei versucht wurde die vorher definierten speziellen Anforderungen darin einzubauen.

Im Zuge der Arbeit stellte sich heraus, daß die Entwicklung und Implementierung eines elektronischen Zustellsystems aus technischer Sicht, als relativ einfach einzustufen ist. Die notwendigen Internettechnologien, sowie Verschlüsselungsverfahren und digitale Signaturen sind allesamt technisch ausgereift und weltweit anerkannt.

Das eigentliche Problem bei der Konzeption besteht darin, daß es keine gesetzliche Regelung für die Zustellung von Dokumenten zwischen Bürgern untereinander gibt, sondern diese der freien Vertragsvereinbarung unterliegt [Kuns06].

Bis jetzt kann man nur Mutmaßungen anstellen, wie das kommerzielle Zustellsystem absolut rechtsicher gestaltet werden kann.

Insbesondere der Einsatz von sicheren elektronischen Signaturen für die Bewahrung der Authentizität und Integrität von zugestellten Dokumenten und Zustellbestätigungen ist für die Rechtssicherheit des kommerziellen Zustellsystems unabdingbar.

Wie sich in Zukunft das kommerzielle elektronische Zustellsystem in der Praxis etablieren wird und welche Beweiskraft elektronisch zugestellten Dokumenten wirklich zugeordnet werden wird, bleibt derzeit offen. Um die Zweifel darin zu beseitigen, läuft deshalb von Seiten der Wirtschaftskammer ein Standardisierungsprozeß, in dem geprüft wird, wie Rechtssicherheit erlangt werden kann. Die vorliegende Arbeit versucht einen Beitrag zur Entwicklung dieses Standards zu leisten.

9.2 Perspektiven

Aus den ursprünglich getrennten behördlichen und privaten elektronischen Zustellsystemen kann in naher Zukunft ein vereintes Modell entstehen.
Das Szenario sieht vor, daß behördliche und kommerzielle Zustellungen von einem gemeinsamen Zustelldienst abgeholt werden können.
Das bereits bestehende Absendeverfahren, im behördlichen Umfeld mittels Fachapplikation bzw. MOA-ZS und im außerbehördlichen Umfeld mittels Absendedienst, bleibt dabei unverändert bestehen.
Der Zustelldienst muß von technischer Seite aus sicherstellen, daß sowohl die Schnittstellen zur Kommunikation mit der Behörde als auch zum außerbehördlichen Absendedienst implementiert werden.
Bei Vereinigung der beiden Zustellmodelle muß sich der Empfänger nur bei einem Zustelldienst registrieren und hat danach ein elektronisches Postfach für behördliche und private Dokumente zur Verfügung. Besonders hervorzuheben ist dabei auch die neu geschaffene Möglichkeit der elektronischen Antwort an die Behörde.
In Folge dessen kann damit gerechnet werden, daß durch immer mehr registrierte Personen bei elektronischen Zustelldiensten Netzwerksynergieeffekte zum Tragen kommen.
Zur weiteren Optimierung des Verfahrens, insbesondere für den Absender, bietet ein Zustelldienst auch die duale Zustellung an, wodurch es möglich wäre, daß behördliche und private Dokumente konventionell auf Papier an Empfänger, die bei keinem Zustelldienst registriert sind, gesendet werden.

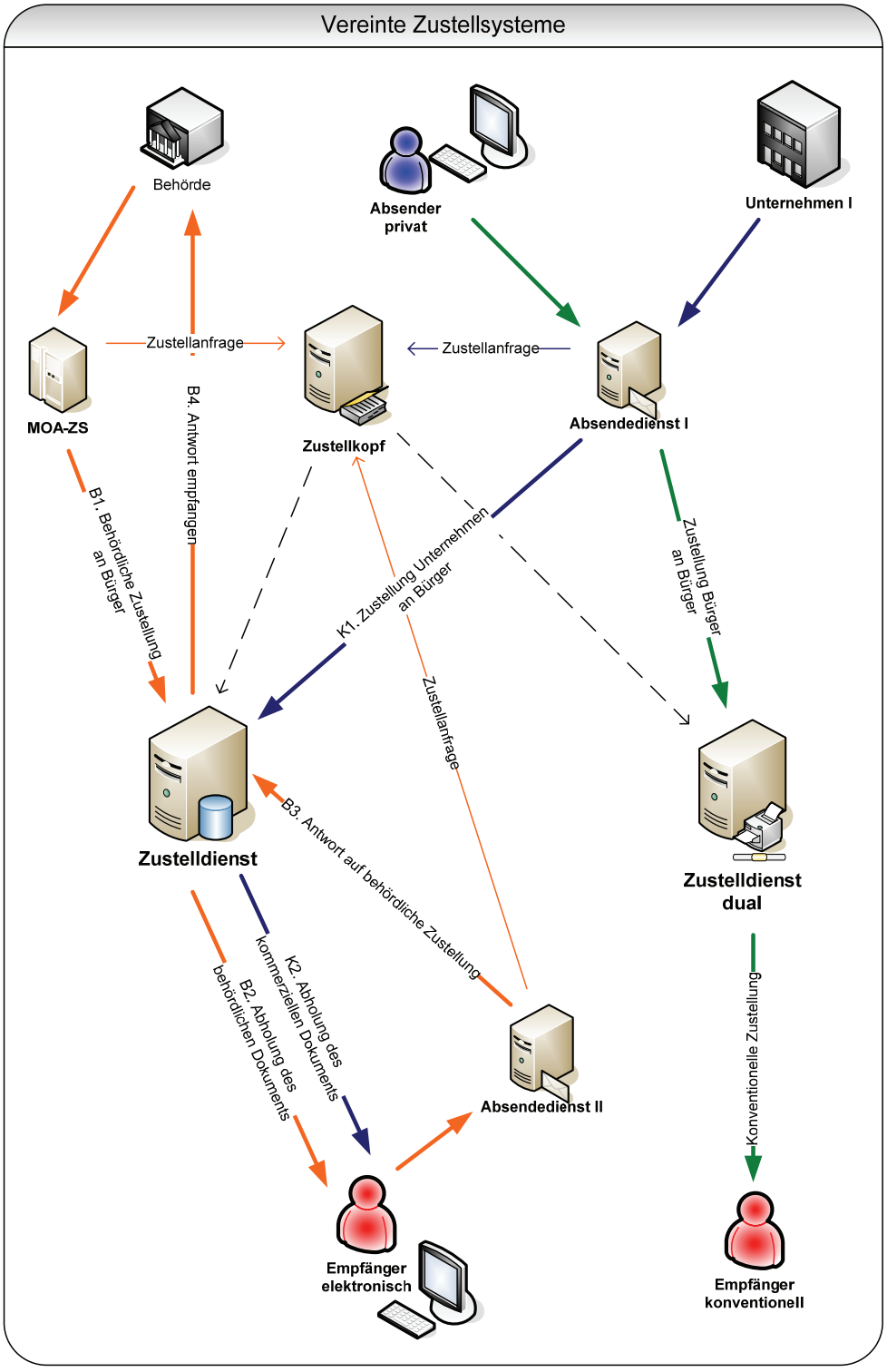

Abbildung 45: Vereinte Zustellsysteme

Besonderes Augenmerk ist in Zukunft, wie in Abbildung 45 zusammenfassend dargestellt, auf die durch Vereinigung von behördlicher, kommerzieller und dualer Zustellung auftretenden Synergien, zu richten.

10 Literaturverzeichnis

[Baum06] C. Baumann:
Kommerzielle elektronische Zustellung,
Pflichtenheft – V 1.0. Wien, Austria Pro, 2006

[Baum07a] C. Baumann: Der elektronische Einschreibbrief.
http://wko.at/ebusiness/eday_2007/vortraege/
baumann_eday2007.pdf
(3. April 2007)

[Baum07b] C. Baumann:
Elektronische Zustellung in der Wirtschaft, 2007
http://www.austriapro.at/arbeitskreise/e_zustellung/
2007_02_15_baumann.pdf (30. März 2007)

[Bert03] A. Bertsch: Digitale Signaturen im E-Commerce. In A. Meier, E-Government (S. 97-109). Dpunkt, 2003

[BVG07] Bundesverfassungsgesetz - B-VG - BGBl. I Nr. 5/2007.

[CAN01] Canonical XML Version 1.0, W3C Recommendation, 2001
http://www.w3.org/TR/2001/REC-xml-c14n-20010315 (20. Juni 2007)

[CeRo06] M. Center, T. Rössler: Duale Zustellung Konzept.
https://demo.egiz.gv.at/plain/content/download/131/555/file/
DualeZustellung.pdf (3. April 2007)

[DGH03] S. Dustdar, H. Gall, M. Hauswirth: Software-Architekturen für Verteilte Systeme, Springer, 2003

[DPW04] W. Dohr, H.J. Pollirer E. Weiss: E-Government-Gesetz
samt Änderungen in AVG, ZustellG, MeldeG, Manz, 2004

[DSIG02] XML-Signature Syntax and Processing, W3C Recommendation, 2002
http://www.w3.org/TR/xmldsig-core/ (25. Mai 2007)

[ebXML01] OASIS ebXML Technical Architecture Specification v1.0.4, 2001
http://www.ebxml.org/specs/ebTA.pdf (23. Juni 2007)

[EGovG04] Bundesgesetz über Regelungen zur Erleichterung des elektronischen Verkehrs mit öffentlichen Stellen - (E-Government-Gesetz – EgovG) - BGBl. I Nr. 10/2004.

[Feil06] E. Feil: Zustellwesen. Linde, 2006

[GOG06] Gerichtsorganisationsgesetz - GOG - BGBl. I Nr. 92/2006

[Haus04] T. Hauser: Web Services: die Standards. Bonn: Galileo Press, 2004

[Hof05] S. Hof: Alternative security approaches in E-government. Linz, Univ., Diss.: Trauner, 2005

[HoHo04] A. Hollosi, R. Hörbe: Bildung von Stammzahl und bereichsspezifischen Personenkennzeichen (bPK), 2004.
http://www.cio.gv.at/it-infrastructure/sz-bpk/Stammzahl-bPK-Algorithmen.1-0-2.20040603.pdf (29. Mai 2007)

[HoKa04] A. Hollosi, G. Karlinger:
Einführung in die österreichische Bürgerkarte.
http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/introduction/Introduction.html (23. Februar 2007)

[Holl06] A. Hollosi: Object Identifier der öffentlichen Verwaltung, 2006
http://www.cio.gv.at/it-infrastructure/oid/OID-1_0_6-20060227.pdf
(22. Juni 2007)

[HoRe04] A. Hollosi, P. Reichstädter:
Modell und Prozesse der elektronischen Zustellung, 2004
http://www.cio.gv.at/it-infrastructure/delivery/spec/zusemod.pdf
(8. Jänner 2007)

[HTTP99] Hypertext Transfer Protocol -- HTTP/1.1, 1999
http://tools.ietf.org/html/rfc2616 (25. Mai 2007)

[TLS00] HTTP Over TLS, 2000
http://tools.ietf.org/html/rfc2818 (25. Mai 2007)

[Kapp06] G. Kappel: Web Engineering. John Wiley & Sons Ltd, 2006

[Kast05] C. Kastner: Elektronische Zustellung mit Fabasoft.
Faba International Services, 2005

[KNS92] G. Keller, N. Nütgens, A.W. Scheer:
Semantische Prozeßmodellierung auf der Grundlage
Ereignisgesteuerter Prozeßketten (EPK), 1992
http://www.iwi.uni-sb.de/Download/iwihefte/heft89.pdf
(28. April 2007)

[Kreg01] H. Kreger: Web Services Conceptual Architecture, WSCA 1.0, IBM Software Group, 2001,
http://www.cs.uoi.gr/~zarras/mdw-ws/
WebServicesConceptualArchitectu2.pdf (21. Juni 2007)

[Krie05] F. Krieger: Der elektronische Rechts- und Zahlungsverkehr zwischen Gemeinde und BürgerInnen im E-Government. Graz: Univ.,
Dipl.-Arb, 2005

[Kuns06] H. Kunst: Rechtliche Rahmenbedingungen der kommerziellen elektronischen Zustellung. Wien: Univ., Diss, 2006

[LaHe06] G. Laga, A. Heinrich:
Sichere elektronische Zustellung im täglichen Leben, 2006.
http://e-government.adv.at/2006/pdf/
Laga_Heinrich_Zustellung_20060602.pdf (14. März 2007)

[LDAP06] Lightweight Directory Access Protocol (LDAP): The Protocol, 2006
http://www.ietf.org/rfc/rfc4511.txt (25. Mai 2007)

[LHHM04] M. Liehmann, A. Hollosi, R. Hörbe, J. Mariel:
Elektronische Zustellung – LDAP-Schemabeschreibung, 2004
http://www.cio.gv.at/it-infrastructure/delivery/spec/zuseldap.pdf
(8. Jänner 2007)

[LiHo04] M. Liehmann, A. Hollosi:
Elektronische Zustellung – Zustellkopf-Schnittstellenspezifikation, 2004
http://www.cio.gv.at/it-infrastructure/delivery/spec/zusekopf.pdf
(8. Jänner 2007)

[Luhn60] H.P. Luhn: Computer for Verifying Numbers, U.S. Patent 2.950.048, 1960
http://patft.uspto.gov/netacgi/nph-Parser?patentnumber=2950048
(20. Juni 2007)

[Mart05] B. Martin: Elektronischer Zahlschein - Spezifikation des Verfahrens EZ-1.0.0, 2005
http://www.cio.gv.at/it-infrastructure/payment/ez/
ElektronischerZahlschein.pdf (23. Juni 2007)

[MIME96] Multipurpose Internet Mail Extensions, 1996
http://tools.ietf.org/html/rfc2045 (25. Mai 2007)

[SPSS04] Spezifikation Module für Online Anwendungen – SP und SS
http://www.cio.gv.at/onlineservices/basicmodules/
moa-spss/handbook/handbook/spec/MOA-SPSS-1.2.pdf
(30. April 2007)

[NaLi04] L. Naber, M. Liehmann:
MOA-ZS - Technische Spezifikation, 2004.
http://labs.cio.gv.at/delivery/mzsspec.pdf (17. März 2007)

[NaRe04] L. Naber, P. Reichstädter:
ZUSE, Technische Spezifikation, 2004.
http://www.cio.gv.at/it-infrastructure/delivery/spec/zusespec.pdf
(8. Jänner 2007)

[NHRL04] L. Naber, A. Hollosi, P. Reichstädter, M. Liehmann:
ZUSE Interface Spezifikation– Aufbau, 2004
http://www.cio.gv.at/it-infrastructure/delivery/spec/zusemsg.pdf
(8. Jänner 2007)

[PKCS1] Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography, Specifications Version 2.1, 2003
http://tools.ietf.org/html/rfc3447 (25. Mai 2007)

[PKCS7] PKCS #7: Cryptographic Message Syntax, Version 1.5, 1998
http://tools.ietf.org/html/rfc2315 (25. Mai 2007)

[Posc02] R. Posch et al.: Weißbuch Bürgerkarte, 2002
http://www.buergerkarte.at/weissbuch/20020515/
WeissbuchBuergerkarte.20020515.pdf
(23. Februar 2007)

[Posc06] R. Posch et al.: Behörden im Netz – Das österreichische E-Government ABC, Österreichische Computer Gesellschaft, 2006

[PostG06] Bundesgesetz über das Postwesen - (Postgesetznovelle 2005) - BGBl. I Nr. 2/2006

[Rech03] W. Rechberger:Grundriss des österreichischen Zivilprozessrechts - Erkenntnisverfahren, Manz, 6. Auflage, 2003

[Reic04] P. Reichstädter: Elektronische Zustellung Overview, 2004
https://labs.cio.gv.at/delivery/zustellung.ppt (16. März 2007)

[RSA78] R. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21 (2), S.120–126, 1978
http://theory.lcs.mit.edu/~rivest/rsapaper.pdf (23. Juni 2007)

[Schn05] M. Schneider: Jüngste Entwicklungen zum IT-Einsatz.
http://www.univie.ac.at/RI/IRIS2005/Arbeitspapierln/Schneider.pdf
(30. April 2007)

[Schn96] B. Schneier: Applied Cryptography, John Wiley & Sons, Second Edition, 1996

[Schw05] J. Schwenk: Sicherheit und Kryptographie im Internet. Wiesbaden, Vieweg, 2005

[ScMo06] R. Schamberger, L. Moser:
Spezifikation Module für Online Applikationen -– ID, MOA-ID, 2006.
http://www.cio.gv.at/onlineservices/basicmodules/
moa-id/specification/MOA_ID_1.3_20060315.pdf (16. April 2007)

[SigG99] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG) - BGBl. I Nr. 190/1999.

[SigR99] Richtlinie des europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen - 1999/93/EG

[SigV04] Verordnung über elektronische Signaturen (Signaturverordnung – SigV) - BGBl.II Nr. 527/2004

[SMIM99] S/MIME Version 3 Message Specification, 1999
http://www.ietf.org/rfc/rfc2633.txt (27. Mai 2007)

[SOA06] OASIS Reference Model for Service Oriented Architecture 1.0, 2006
http://www.oasis-open.org/committees/download.php/19679/
soa-rm-cs.pdf (22. Juni 2007)

[SOAP00] Simple Object Access Protocol (SOAP) 1.1, W3C Note, 2000
http://www.w3.org/TR/2000/NOTE-SOAP-20000508 (25. Mai 2007)

[SwA00] SOAP Messages with Attachments (SwA), W3C Note, 2000
http://www.w3.org/TR/SOAP-attachments (25. Mai 2007)

[Tisc06] H., Tischler: Nutzen der elektronischen Zustellung für Behörden und Unternehmen, 2006.
http://wko.at/ebusiness/eday_2006/pdf/tischler.pdf (4. April 2007)

[Tisc07] H., Tischler: Elektronische Zustellung: Identifikation/ Authentifizierung, 2007. http://www.austriapro.at/arbeitskreise/e_zustellung/ eZustellung_apro_TISCHLER_20070329.ppt (11. April 2007)

[TSP01] Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP), 2001 http://www.ietf.org/rfc/rfc3161.txt (25. Mai 2007)

[UDDI04] UDDI Version 3.0.2, UDDI Spec Technical Committee Draft, 2004 http://uddi.org/pubs/uddi-v3.0.2-20041019.pdf (23. Juni 2007)

[VSig04] Regelung der sicherheitstechnischen und organisationsrelevanten Voraussetzungen für Verwaltungssignaturen (Verwaltungssignaturverordnung - VerwSigV) – BGBl. II Nr. 159/2004

[Weis01] J. Weise: Public Key Infrastructure Overview, SunPS GlobalSecurity Practice, SunBluePrints™OnLine, 2001 http://www.sun.com/blueprints/0801/publickey.pdf (23. Juni 2007)

[Wimm05] M. Wimmer, M: . (2005). FAQ zur Amtssignatur, 2005. http://www.cio.gv.at/faq/Amtssignatur/ faq-as-1-0-2-20050222.pdf (10. März 2007)

[Wint05] M.Winter: Methodische objektorientierte Softwareentwicklung. dpunkt.Verlag, 2005

[WSA04] Web Services Architecture, W3C Working Group Note, 2004 http://www.w3.org/TR/ws-arch/ (23. Juni 2007)

[WSDL07] Web Services Description Language (WSDL) Version 2.0 Part 1: Core Language, W3C Proposed Recommendation, 2007 http://www.w3.org/TR/wsdl20/ (23. Juni 2007)

[WWW01] A-Sit - Zentrum für sichere Informationstechnologie - Austria http://www.a-sit.at/ (27. Februar 2007)

[WWW02] Die österreichische Bürgerkarte.
http://www.buergerkarte.at (11. April 2007)

[WWW03] ebInterface: der österreichische XML Rechnungsstandard
http://www.ebinterface.at/index.html (30. April 2007)

[WWW04] EGIZ. E-Government Innovationszentrum:
http://demo.egiz.gv.at (16. März 2007)

[WWW05] ERV - Elektronischer Rechtsverkehr
http://kmu.telekom.at/Loesungen/Branchenloesungen/erv/index.php
(30. April 2007)

[WWW06] Fabasoft.
http://www.fabasoft.at (23. März 2007)

[WWW07] heise online
http://www.heise.de (10. April 2007)

[WWW08] HELP.gv.at - Ihr offizieller Amtshelfer für Österreich
http://www.help.gv.at (16. März 2007)

[WWW09] Bundeskanzleramt Östereich - IKT Strategie des Bundes
http://www.cio.gv.at (15. März 2007)

[WWW10] Die österreichische Post AG
http://www.post.at (16. März 2007)

[WWW11] Österreichische Datenschutzkommission –
Stammzahlenregisterbehörde
http://www.stammzahlenregister.gv.at (25. Mai 2007)

[WWW12] Wirtschaftskammer Österreich – AustriaPRO:
- Arbeitskreis E-Zustellung
http://portal.wko.at/wk/format_detail.wk?angid=1&stid=299150
&dstid=1637&opennavid=0 (29. Mai 2007)

[WWW13] A1.net - A1 Signatur
http://www.a1.net/privat/a1signatur (30. Mai 2007)

[WWW14] RSA Laboratories
http://www.rsa.com/rsalabs/default.asp (30. Mai 2007)

[X509] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2002
http://tools.ietf.org/html/rfc3280 (24. Mai 2007)

[XML06] Extensible Markup Language (XML) 1.0 (Fourth Edition),
W3C Recommendation, 2006
http://www.w3.org/TR/2006/REC-xml-20060816 (25. Mai 2007)

[XSD04] XML Schema, W3C Recommendation, 2004
http://www.w3.org/TR/2004/REC-xmlschema-0-20041028 (20. Juni 2007)/

[XSLT07] XSL Transformations (XSLT) Version 2.0, W3C Recommendation, 2007
http://www.w3.org/TR/xslt20/ (23. Juni 2007)

[ZGK04] W. Zuser, T. Grechenig, M. Köhle: Software Engineering mit UML und dem Unified Process, Pearson Studium, 2., überarbeitete Auflage, 2004

[ZusG04] Bundesgesetz über die Zustellung behördlicher Dokumente
(Zustellgesetz – ZustG) - BGBl. I Nr. 10/2004.

Glossar

Außerbehördliches Umfeld	Kommunikationsumfeld zwischen Bürgern bzw. Unternehmen
bPK	Bereichspezifisches Personenkennzeichen
Elektronische Signatur	Elektronisches Äquivalent zur eigenhändigen Unterschrift
ID	Eindeutige Identifikationsnummer
LDAP	Lightweight Directory Access Protocol. Ein Protokoll zum Zugriff auf einen Verzeichnisdienst
Natürliche Personen	Jeder Mensch gemäß 16 § des Allgemeinen Bürgerlichen Gesetzbuches
Nicht natürliche Personen	Unternehmen, Verein oder Körperschaften öffentlichen Rechts
Private Key	Der private Schlüssel, der nur dem Eigentümer bekannt ist und bei asymmetrischen Kryptoverfahren zur Entschlüsselung oder Signierung von Nachrichten dient
Public Key	Der öffentliche Schlüssel, der bei asymmetrischen Kryptoverfahren zur Verschlüsselung oder Prüfung der Signatur von Nachrichten dient
RSA	Kryptoverfahren nach Rivest, Shamir und Adleman
RSa-Brief	Behördlicher eigenhändiger Rückscheinbrief
RSb-Brief	Behördlicher Rückscheinbrief, der auch an Ersatzempfänger zugestellt werden kann
SOAP	Simple Object Access Protocol. Ein XML-basiertes einfaches Protokoll zum Austausch von Daten
wbPK	Wirtschaftsbereichsspezifisches Personenkennzeichen
XML	Extensible Markup Language. Auszeichnissprache zur Darstellung strukturierter Daten in Textform
ZMR	Zentrales Melderegister
Zustell-bPK	Bereichsspezifisches Personenkennzeichen für den Bereich „Zustellung“
Zustellqualität	Art der Durchführung einer Zustellung, z.B. Normal oder Eingeschrieben mit Rückschein