Arne Tauber, Bernd Zwattendorfer, Thomas Zefferer: "Elektronisches Einschreiben im D-A-CH-Raum",
D-A-CH Security 2011, 2011, pp. 510-521

Elektronisches Einschreiben im D-A-CH-Raum

Arne Tauber[1], Bernd Zwattendorfer[1], Thomas Zefferer[1]

[1]E-Government Innovationszentrum
{Arne.Tauber, Bernd.Zwattendorfer, Thomas.Zefferer}egiz.gv.at

Zusammenfassung

Begünstigt durch den ständig wachsenden Bedarf an elektronischen Pendants zu traditionellen behördlichen oder privatwirtschaftlichen Prozessen, existieren seit einiger Zeit unter anderem auch unterschiedliche Systeme für eine nachweisliche und zuverlässige Zustellung von elektronischen Dokumenten. Regierungen und Postdienstleister bieten seit Jahren diverse elektronische Mehrwertdienste an, deren Qualität mit jener des klassischen Einschreibens verglichen werden kann. Bis dato gibt es jedoch keine einheitliche Meinung darüber, welche Anforderungen und Eigenschaften in punkto Sicherheit diese Systeme erfüllen bzw. besitzen müssen. Weder von Seiten der Forschung, noch von Seiten der Wirtschaft oder diversen Standardisierungsgremien wurden hier bisher konkrete Richtlinien vorgegeben.
Damit einhergehend findet eine kontinuierliche Heterogenisierung der bestehenden und zukünftigen Zustelllandschaft statt. Jüngste Entwicklungen im IKT-Sektor fordern jedoch eine verstärkte Interoperabilität von Anwendungen, besonders im grenzüberschreitenden Kontext. Pan-europäische IT-Lösungen sind auch ein Schwerpunktthema der Digitalen Agenda der Europäischen Kommission, welches sich unter anderem in der kürzlich wirksam gewordenen EU Dienstleistungsrichtlinie, die eine grenzüberschreitende Nutzbarkeit von E-Government Diensten fordert, manifestiert. Die Interoperabilitätsanforderungen betreffen auch die elektronische Zustellung, die Benutzern die Möglichkeit einer grenzüberschreitenden Zustellung, ähnlich wie bei E-mail, jedoch mit der Qualität des Einschreibens, ermöglichen soll. In diesem Artikel wollen wir die verschiedenen existierenden Zustellsysteme in Deutschland, Österreich und der Schweiz diskutieren und bezüglich ihrer Sicherheitseigenschaften vergleichen, um Interoperabilitätsbestrebungen in diesem Sektor zu erleichtern. Unsere Resultate zeigen, dass sich elektronische Zustellsysteme stark am postalischen Modell des klassichen Einschreibens hinsichtlich Fairness, Nicht-Abstreitbarkeit und Vertrauen orientieren.

1 Einleitung

Wichtige Dokumente, wie z.B. fristgebundene rechtsgeschäftliche Erklärungen, werden sowohl im öffentlichen als auch im privaten Sektor in vielen Fällen auf sichere und verlässliche Weise dem Empfänger übermittelt. Postdienstleister bieten hierfür eine besondere Art des Briefversands, das sogenannte Einschreiben, an. Bei der Versandart Einschreiben erhält der Absender üblicherweise eine Versandbestätigung. Abhängig von der gewählten Versandoption kann ein Einschreiben auch mit „Rückschein“ versendet werden. In diesem Fall erhält der Absender zusätzlich eine vom Empfänger unterzeichnete Empfangsbestätigung (Rückschein), die eine Übermittlung des Zustellstücks rechtssicher dokumentiert.

Herkömmliche elektronische Kommunikationssysteme wie E-mail haben keinerlei Beweiskraft und können vielmehr mit dem Versand einer Postkarte, die keinerlei Sicherheit bietet, verglichen werden. Wenngleich Erweiterungen wie S/MIME (Secure/Multipurpose Internet Mail Extensions) [Rams04] oder PGP (Pretty Good Privacy) [CDF+07] das E-mail Protokoll um Integrität, Authentizität und Vertraulichkeit erweitern, so bleibt die Frage der Nicht-Abstreitbarkeit dennoch offen. Nicht-Abstreitbarkeit bedeutet in diesem Fall, dass Absender nicht abstreiten können, eine E-mail versendet, und Empfänger nicht abstreiten können, eine E-mail empfangen zu haben. Internet Standards wie S/MIME Bestätigungen (RFC 2634) versuchen diese Lücke zu füllen. Diese Ansätze basieren jedoch auf der Annahme fair agierender Empfänger, d.h. dass Empfänger die Übernahme tatsächlich bestätigen.

Aufgrund der verstärkten Nachfrage nach einer rechtssicheren Zustellung im elektronischen Bereich haben Regierungen, Postdienstleister und andere private Anbieter in den letzten Jahren auf Basis sicherer Technologien eine Vielzahl von „qualifizierten“, d.h. rechtssicher mit der Qualität eines Einschreibens, elektronischen Zustellsystemen geschaffen. Dieses Ökosystem umfasst beispielsweise in Deutschland das etablierte Justizsystem *Elektronisches Gerichts- und Verwaltungspostfach* (EGVP), den *E-Postbrief* der deutschen Post oder das demnächst startende *De-Mail* Projekt der deutschen Bundesregierung. Ähnliche Systeme finden sich mit dem Justizsystem *Elektronischer Rechtsverkehr* (ERV) oder dem behördlichen Zustellsystem der öffentlichen Verwaltung auch in Österreich. Mit *IncaMail* bietet die Schweizerische Post ein vergleichbares System für den öffentlichen und privaten Sektor an. Die Eigenschaften und Ausprägungen der angebotenen Dienste sind wie beim klassischen Einschreiben system- bzw. länderabhängig. Dies kann allein schon anhand der Diversität und Heterogenität der bestehenden Systeme beobachtet werden. Solange die Systeme geschlossen bleiben, stellt dies kein Problem dar. Allerdings wünschen sich Benutzer, ähnlich wie bei E-mail, z.B. eine einzige Mailbox, mit welcher global und grenzüberschreitend „qualifiziert“ kommuniziert werden kann. Benutzer sollten nicht mit verschiedenen Systemen, die prinzipiell die gleiche Funktionalität bieten aber zusätzliche Kosten verursachen, konfrontiert werden.

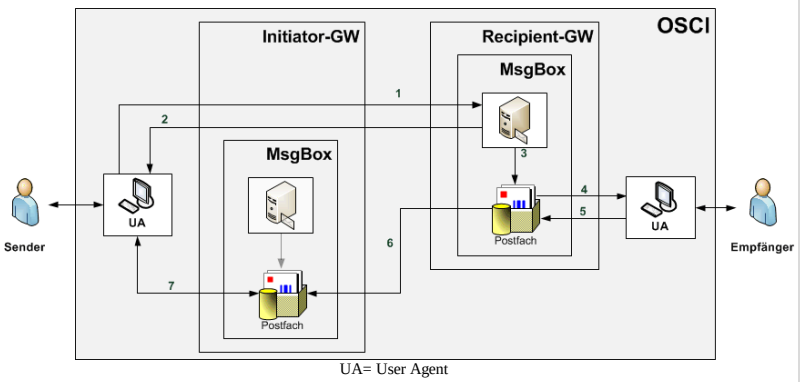
Der Trend in Europa, unterstützt durch die Europäische Kommission mit der Digitalen Agenda [EuKo10a] und dem E-Government Aktionsplan [EuKo10b], geht verstärkt in Richtung eines einheitlichen digitalen Binnenmarkts und fordert interoperable E-Government Lösungen, um die Mobilität von Bürgern innerhalb der EU soweit wie möglich zu vereinfachen. Im Kontext der aktuellen Implementierung der EU Dienstleistungsrichtlinie gilt dies insbesonders auch für die elektronische Zustellung, um Bürgern auch grenzüberschreitend auf sichere und verlässliche Weise behördliche und private Schriftstücke übermitteln zu können. Der Vergleich sowie die Bewertung und Klassifizierung von Zustellsystemen vereinfacht und unterstützt Interoperabilitätsbestrebungen wesentlich. In diesem Artikel vergleichen und evaluieren wir daher die dominanten Zustellsysteme in Deutschland, Österreich und der Schweiz mit dem Fokus auf sicherheitsrelevante Aspekte. In Kapitel 2, 3 und 4 beschreiben wir die Systeme in den einzelnen Ländern. Anschließend vergleichen wir in Kapitel 5 die einzelnen Systeme anhand unterschiedlicher Kriterien und diskutieren die Ergebnisse hinsichtlich bestehender Interoperabilitätsbestrebungen.

2 Deutschland

In Deutschland gibt es derzeit drei dominante Zustellsysteme, die mit der Qualität des klassischen Einschreibens verglichen werden können. Das älteste dieser Systeme ist EGVP, das Elektronische Gerichts- und Verwaltungspostfach, das auf dem OSCI (Online Services Computer Interface) Standard basiert. Das De-Mail Projekt und der E-Postbrief sind jüngste Entwicklungen der deutschen Bundesregierung bzw. der deutschen Post. Diese drei Systeme werden in den nächsten Unterkapiteln eingehender beschrieben.

2.1 OSCI - Online Services Computer Interface

OSCI ist ein Standard für den sicheren und zuverlässigen Versand von Nachrichten und wird hauptsächlich für E-Government Anwendungen in Deutschland eingesetzt, z.B. in der virtuellen Poststelle [PlWe07], um Nachrichten zwischen verschiedenen Verwaltungseinheiten auszutauschen. Das bekannteste Beispiel einer virtuellen Poststelle ist das Elektronische Gerichts- und Verwaltungspostfach (EGVP), das OSCI zur rechtssicheren Kommunikation zwischen Gerichten und Behörden einsetzt. Der Standard wird von der OSCI-Leitstelle [Osci10] gewartet.



(1) Übergabe Zustellstück an MsgBox des Empfänger Gateways

(2) Rückübermittlung einer Zugangsbestätigung

(3) Ablegen der Nachricht im Postfach des Empfängers

(4) Abholen der Nachricht durch Empfänger

(5) Entschlüsselung und Signatur der Empfangsbestätigung

(6) Rückübermittlung der Empfangsbestätigung an das Postfach des Absenders

(7) Abholen der Empfangsbestätigung durch den Absender

Abbildung 1: Architektur und Zustellprozess von OSCI

Architektur und Prozessablauf des OSCI Standards sind in Abbildung 1 dargestellt. OSCI bedient sich des SOAP (Version 1.2) Webservice Standards zur Übermittlung von Nachrichten. Durch eine genauere Spezifikation des SOAP Headers kann OSCI somit als eigenes Webservice-Profil angesehen werden. Im asynchronen Modus definiert der Standard sogenannte Gateways als vertrauenswürdige Stellen, die ein Postfach (MsgBox) für Benutzer zur Verfügung stellen. Der synchrone Modus ist in der Praxis kaum zu realisieren, da dieser eine direkte Kommunikation zwischen Absender und Empfänger voraussetzt. Beide Parteien müssten bei einer derartigen Übertragung somit gleichzeitig online sein.

Die gegenseitige Authentifizierung zwischen den OSCI Gateways erfolgt auf Basis von X.509 Zertifikaten (PKI) und den Standards WS-Trust und WS-Federation. Da OSCI für beliebige Business-Szenarien konzipiert ist, werden Authentisierungsniveaus, Richtlinien und unterstützte Funktionalitäten mittles WSDL (Web Services Description Language) vom jeweiligen Gateway publiziert. Clients können so für das jeweilige Übermittlungsszenario dynamisch konfiguriert werden.

OSCI operiert ausschließlich auf dem SOAP Header und übermittelt, falls gewünscht, dem Absender eine Zugangsbestätigung bei Ankunft der Nachricht im Gateway des Empfängers. Der eigentliche Inhalt der Nachricht ist Ende-zu-Ende verschlüsselt im SOAP Body erhalten. Dieser muss vom Empfänger entschlüsselt, über eine elektronische Signatur bestätigt und anschließend an den Absender als Empfangsbestätigung rückübermittelt werden.

2.2 De-Mail

De-Mail ist ein aktuell noch junges Projekt der deutschen Bundesregierung mit dem Ziel, eine verlässliche und rechtssichere Infrastruktur für die Kommunikation zwischen Bürgern, Unternehmen und der öffentlichen Verwaltung bereitzustellen. Grundlage für De-Mail ist das Bürgerportalegesetz, welches am 24. Februar 2011 im deutschen Bundestag beschlossen wurde. Die Spezifikationen für De-Mail werden vom Bundesamt für Sicherheit in der Informationstechnologie (BSI) [BuSI09] gewartet.

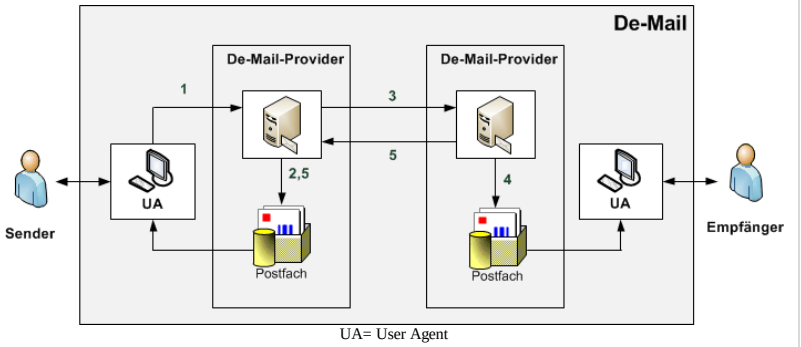


Abbildung 2: Architektur und Zustellprozess von De-Mail (Versandart „De-Mail Einschreiben“)

Abbildung 2 zeigt die Architektur und die Prozessabläufe von De-Mail. Sicherheitsaspekte von De-Mail wurden von [DiKe10] diskutiert. De-Mail Provider garantieren einen fairen Austausch von Nachrichten, indem sie als vertrauenswürdige Vermittler zwischen Absender und Empfänger agieren. Provider müssen daher eine entsprechende Akkreditierung beim BSI durchlaufen. Das technische Konzept von De-Mail unterscheidet zwischen zwei Kommunikationspfaden, die unterschiedliche Sicherheitsanforderungen aufweisen. Die Kommunikation zwischen zwei De-Mail Providern basiert auf dem E-Mail Protokoll SMTP (Simple Mail Transfer Protocol) geschützt durch TLS (Transport Layer Security). Die Kommunikation zwischen User Agents (UA) von Benutzern und ihren Providern kann auf unterschiedliche Arten erfolgen, z.B. über E-Mail oder über einen Webbrowser. In jedem Fall kommt es zwischen UA und De-Mail Provider zu einer temporären Entschlüsselung der Daten (Protokollwechsel), was bereits von mehreren Seiten als Sicherheitsmangel kritisiert wurde [Lapp09]. Eine Ende-zu-Ende Verschlüsselung auf Nachrichtenebene ist dennoch möglich, softern dem Absender das Verschlüsselungszertifikat des Empfängers bekannt ist.

De-Mail unterscheidet zwischen mehreren Authentisierungsniveaus und bietet je nach Niveau unterschiedliche Versandoptionen an. Neben einer Versandbestätigung und Zugangsbestätigung für den Absender können Nachrichten auch „höchstpersönlich“ oder „absenderbestätigt“ versendet werden. Im ersten Fall muss sich der Empfänger mit dem Authentisierungsniveau „hoch“ anmelden, im zweiten Fall gilt dies für den Absender. Hoch bedeutet, dass sich der Benutzer mit einem Zwei-Faktor-Authentifizierungsmechanismus anmelden muss, beispiel-

weise mit Benutzername/Passwort + mobiler TAN (Transaktionsnummer) oder unter Verwendung einer Chipkarte wie dem elektronischen Personalausweis (nPA). De-Mail unterstützt zwei Versandarten. Im Gegensatz zur einfachen Versandart „De-Mail“ bietet ausschließlich die Versandart „De-Mail Einschreiben“ die rechtssichere Zustellung mit einer Versand- und Zugangsbestätigung. In diesem Fall erhält der Absender einen Nachweis, wann die Nachricht verschickt und wann sie in das Postfach des Empfängers zugestellt wurde.

2.3 E-Postbrief

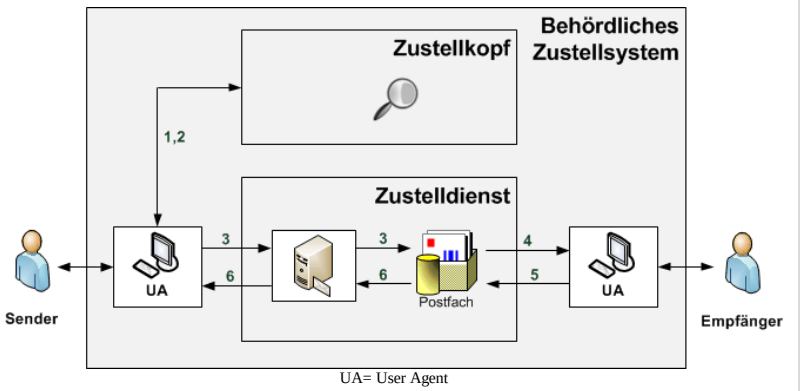
Seit Juli 2010 betreibt die Deutsche Post AG das Zustellservice „E-Postbrief“ [DePo11], welches über standardmäßige Web-browser bedient werden kann. Kunden können sich eine „@epost.de“ Adresse registrieren lassen, Business Kunden eine entsprechende Subdomain. Gleich wie De-mail unterstützt der E-Postbrief zwei unterschiedliche Authentisierungsniveaus. Die standardmäßige Authentifizierung basiert auf Benutzername und Passwort. Eine qualitätsvolle Authentifzierung setzt einen 2-Faktoren Mechanismus voraus und bedarf zusätzlich zu Benutzername und Passwort noch einer mobilen TAN. Sender können zwischen zwei unterschiedlichen Zustellqualitäten wählen. Die Qualität „Einschreiben Einwurf“ übermittelt dem Sender zunächst eine Versandbestätigung. Wurde die Nachricht in das Postfach des Empfängers zugestellt, wird dem Absender zusätzlich eine Zugangsbestätigung übermittelt. Die Qualität „Einschreiben mit Empfangsbestätigung“ baut auf der Qualität „Einschreiben mit Einwurf“ auf, allerdings muss der Empfänger die Zusendung zunächst annehmen (oder ablehnen). Anschließend wird dem Sender eine Empfängsbestätigung übermittelt. Empfänger müssen sich bei dieser Versandoption mit einer hohen Authentifizierungsqualität anmelden. Solle der Empfänger die Zusendung ablehnen, wird diese unmittelbar vom Server gelöscht. Gleich wie be De-Mail ist Ende-zu-Ende Verschlüsselung nicht als integrale Sicherheitsfunktion des Systems vorgesehen. Allerdings können Empfänger ihren öffentlichen Schlüssel in ein Verzeichnis eintragen lassen, sodass Sender nach Bedarf Zusendungen verschlüsseln können. Der Einsatz von qualifizierten Signaturen wird derzeit noch nicht unterstützt, ist allerdings für 2011 vorgesehen. Für Business Kunden stellt die deutsche Post ein Business Client Gateway zur Verfügung, das E-mail Systeme von Organisationen, die auf Outlook Exchange oder Lotus Notes basieren, über ein virtuelles privates Netzwerk an das E-Postbrief System anbindet. Ein Merkmal des E-Postbrief Systems ist die hybride Zustellung. Wird der Empfänger nicht im E-Postbrief System gefunden, so wird die Zusendung über den physischen Zustellkanal an den Empfänger übermittelt.

3 Österreich

In Österreich wurde bereits früh mit der Umsetzung von rechtssicheren Zustellsystemen begonnen. Derzeit gibt es zwei dominante Systeme in der österreichischen Zustelllandschaft. Der Elektronische Rechtsverkehr (ERV) des Justizministeriums ermöglicht die sichere Kommunikation zwischen Gerichten, Anwälten, Notaren, usw. Das behördliche Zustellsystem, welches unter Aufsicht des Bundeskanzleramtes betrieben wird, ermöglicht die rechtssichere Kommunikation zwischen Bürgern, Unternehmen und Behörden. Wir werden diese zwei Systeme in den nächsten Kapiteln eingehender beschreiben.

3.1 Behördliches Zustellsystem

Das behördliche Zustellsystem wurde in Österreich 2004 in Betrieb genommen. So wie De-Mail basiert das System auf einer konkreten rechtlichen Grundlage, dem österreichischen Zustellgesetz, das alle rechtlichen, organisatorischen und technischen Anforderungen regelt. Die technischen Spezifikationen werden vom Bundeskanzleramt gewartet [ReTa08].



(1) Abfrage des Zustelldienstes des Empfängers am Zustellkopf

(2) Antwort des Zustellkopfs

(3) Übergabe des Zustellstücks an den Zustelldienst und Speichern im Postfach des Empfängers

(4) Benachrichtigung des Empfängers via E-Mail/SMS

(5) Abholen des Zustellstücks und Erzeugen der Empfangsbestätigung mittels qualifizierter Signatur

(6) Rückübermittlung der Empfangsbestätigung an den Absender

Abbildung 3: Architektur und Zustellprozess des behördlichen Zustellsystems in Österreich

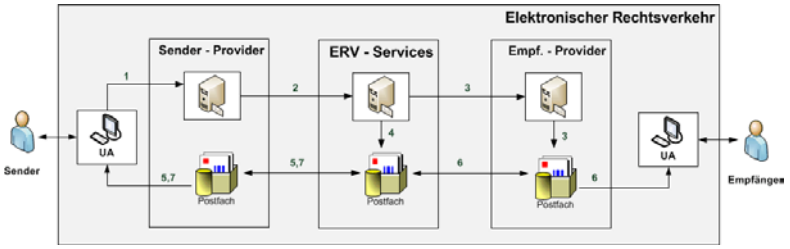
Abbildung 3 zeigt die Architektur und den Zustellprozess des behördlichen Zustellsystems in Österreich, welches im Detail in [Taub09] beschrieben ist. Die Architektur des österreichischen Zustellsystems unterscheidet sich wesentlich von anderen providerbasierten Systemen. Alle Empfänger müssen sich bei einem von derzeit drei zugelassenen Zustelldiensten[1] mit ihrer Bürgerkarte registrieren. Die Bürgerkarte ist der elektronische Ausweis für alle Verwaltungsangelegenheiten in Österreich. Sowohl Chipkarten als auch Mobiltelefone können als Bürgerkarte aktiviert werden und ermöglichen neben der eindeutigen Identifikation auch die Erstellung von qualifizierten elektronischen Signaturen gemäß der EU Signaturrichtlinie [EuSr99]. Da Empfänger in diesem System auch über ihre nationale Identifikationsnummer adressiert werden können, wissen im Gegensatz zu einem E-Mail basierten System die Absender nicht, bei welchem Zustelldienst ein Empfänger registriert ist. Daher müssen Absender in einem ersten Schritt beim sogenannten Zustellkopf, der als zentrales Auskunftsregister dient, den zugehörigen Zustelldienst des Empfängers abfragen. Die Authentifizierung von Absendern am Zustellkopf sowie an Zustelldiensten basiert auf SSL-Client Zertifikaten, die ein besonderes Attribut (Verwaltungseigenschaft [Roes09]) aufweisen müssen. Aus Datenschutzgründen retourniert der Zustellkopf keine persönlichen Daten des Empfängers an den Absender. Es wird ausschließlich die Adresse des Zustelldiensts, bei dem der Empfänger registriert ist, sowie allenfalls ein X.509 Zertifikat für Ende-zu-Ende Verschlüsselung (falls vom Empfänger hinterlegt) übertragen. Die Übermittlung der Zustellstücke vom Absender zum Zustelldienst erfolgt mit dem SwA (SOAP with Attachments) Standard, sodass bei einer Ende-zu-Ende Verschlüsselung die Daten auch in verschlüsselter Form von herkömmlichen E-Mail Clients des Empfängers verarbeitet werden können. Da Sender direkt mit dem Zustelldienst des Empfängers kommunizieren, erhalten Sender keine Versandbestätigung. Dies ist auch vom Gesetz und im behördlichen Postverkehr in Österreich nicht vorgesehen. Bei der

[1] https://www.meinbrief.at, https://www.brz-zustelldienst.at, https://zustellung.telekom.at

Abholung müssen Empfänger mittels Bürgerkarte eine Empfangsbestätigung qualifiziert signieren, welche an den Sender via E-Mail oder Webservice rückübermittelt wird.

3.2 ERV – Elektronischer Rechtsverkehr

Der „Elektronische Rechtsverkehr“ (ERV) ist das österreichische e-Justice System, das eine sichere, zuverlässige und rechtlich-bindende Kommunikationsinfrastruktur für Benutzer (Anwälte, Notare) und Gerichte bzw. Staatsanwaltschaften zur Verfügung stellt. Die technischen Services und die Spezifikation des ERV [Orne07] werden vom Bundesrechenzentrum betrieben bzw. gewartet.



UA= User Agent

(1) Übergabe des Zustellstücks von UA an ERV Provider des Senders

(2) Korrektheitsprüfung und Übergabe an zentrale ERV Services

(3) Übergabe des Zustellstücks and Provider des Empfängers

(4) Generieren der Zugangsbestätigung und Ablegen in Postfach des Sender-Providers

(5) Abrufen der Zugangsbestätigung durch Sender-Provider

(6) Abholen durch Empfänger und generieren der Empfangsbestätigung und Ablegen in Postfach des Sender-Providers bei ERV Services

(7) Abholen der Empfangsbestätigung durch Sender-Provider

Abbildung 4: Architektur und Zustellprozess des elektronischen Rechtsverkehrs

Abbildung 4 zeigt die Architektur und den Zustellprozess des ERV. Die Kernkomponente des ERV bilden die sogenannten „ERV-Services“, die als Web-Services zentral im Bundesrechenzentrum laufen und die Kommunikation zwischen den ERV Providern regeln. ERV Teilnehmer (Gerichte, Anwälte, Notare, etc.) müssen ein Konto bei einem ERV Provider anmelden und erhalten im Anschluss eine ERV Teilnehmernummer. Das konzeptuelle Model ist dem österreichischen Zustellsystem sehr ähnlich. Im Gegensatz zum Zustellsystem, bei dem der Zustellkopf die Verknüpfung Identifikationsdaten ↔ Zustelldienst herstellt, sind im ERV die ERV-Services dafür verantwortlich die Verknüpfung Teilnehmernummer ↔ ERV Provider herzustellen. Im Gegensatz zum Zustellkopf, der ausschließlich als Auskunftsdienst fungiert, müssen ERV-Services allerdings die komplette Nachricht verarbeiten.

Um auch anderen Teilnehmer (z.B. Polizeistationen) den Zugang zum ERV zu ermöglichen, haben die ERV-Services einen internen ERV-Provider implementiert.

4 Schweiz - Incamail

Die Schweizerische Post betreibt das Zustellsystem „IncaMail“ [ScPo11], das ähnlich wie die bereits beschriebenen Systeme die qualitätsvolle Zustellung von Dokumenten zwischen Bür-

gern, Behörden und Organisationen ermöglicht. INCA steht als Abkürzung für Integrity (Integrität), Non-repudiation (Nicht-Abstreitbarkeit), Confidentiality (Vertraulichkeit) und Authenticity (Echtheit). Ähnlich wie E-Postbrief läuft Incamail in einer zentralen Umgebung mit einem einzelnen Provider. Sender müssen sich am IncaMail Zustellsystem registrieren und können dieses dann über einen Web-Browser oder über ein E-mail Client Plugin bedienen. Ist ein Empfänger ein registrierter IncaMail Benutzer, so ist der Prozess der gleiche wie beim E-Postbrief und der Sender erhält sowohl eine Versand- als auch eine Empfangsbestätigung. Im Gegensatz zu den bisher beschriebenen Systemen erlaubt IncaMail aber auch das „eingeschriebene“ Versenden von Nachrichten an herkömmliche E-mail Adressen. In diesem Fall kommt die patentierte SAFE (Secure Attached File Encryption) Technologie zum Einsatz um dem Sender eine Empfangsbestätigung zu retournieren. SAFE verschlüsselt die Nachricht für den Empfänger mit einem geheimen Schlüssel, welcher auf dem IncaMail Server temporär hinterlegt wird. Der Empfänger erhält anschließend eine Benachrichtigung, in welcher die verschlüsselte Originalnachricht bereits als HTML Fragment enthalten ist. Sobald der Empfänger die Benachrichtigung liest und über einen Formularaufruf die verschlüsselte Originalnachricht an den IncaMail Server übermittelt, hat er die Möglichkeit, den Empfang zu bestätigen oder abzulehen. Im Fall der Annahme, wird die Nachricht vom IncaMail Server entschlüsselt und der Empfänger kann sich die Nachricht runterladen. Äquivalent zum E-Postbrief System bietet auch IncaMail seinen Business Kunden einen automatisierten Zugang entweder über Web-Services (SOAP) oder über ein E-mail (SMTP) Gateway.

5 Evaluierung

In diesem Kapitel diskutieren wir die Eigenschaften der beschriebenen Zustellsysteme hinsichtlich Sicherheit sowie mögliche Auswirkungen auf Interoperabilitätsbestrebungen. Tab 1 vergleicht die vorgestellten Zustellsysteme aus dem DACH-Raum anhand fünf festgelegter Kriterien. Nicht-Abstreitbarkeit beschreibt die Eigenschaft, dass sowohl Absender als auch Empfänger nicht abstreiten können, eine Nachricht erhalten zu haben. Beim Kriterium der Vertraulichkeit geht es darum, dass eine Nachricht nur vom Empfänger selbst eingesehen und z.B. nicht abgefangen und von Unbefugten gelesen werden kann (Briefgeheimnis). Über das Unterscheidungskriterium des Transportprotokolls werden die Zustellsysteme dahingehend verglichen, über welchen technischen Kommunikationskanal die Nachrichten elektronisch übertragen werden. Anhand von Authentisierungsniveaus wird unterschieden, mit welcher Qualität bzw. welchem Sicherheitsgrad Zustellstücke übertragen werden können. Elektronische Signaturen garantieren die Authentizität von Bestätigungen. Die Beweiskraft und Auswirkungen auf Interoperabilität hängen wesentlich von der Qualität der elektronischen Signatur ab.

Nicht-Abstreitbarkeit (engl. Non-Repudiation) ist eine der wichtigsten Sicherheitseigenschaften um die rechtssichere Zustellung zu gewährleisten. Allerdings gibt es zwischen den einzelnen Systemen keinen Konsens darüber, welche Bestätigungen bereitgestellt werden müssen. Wenngleich im postalischen Einschreiben Versandbestätigungen in den meisten Ausprägungen ein wichtiges Sicherheitsmerkmal darstellen, werden diese nicht in allen beschriebenen Systemen als notwendig erachtet. Die Bereitstellung einer Versandbestätigung hängt offenbar stark mit der verwendeten Kommunikationstechnologie zusammen. E-Mail basierte Systeme, bei denen die Feststellung eines unmittelbaren Zustellstatus nicht möglich ist (z.B. wenn nicht klar ist ob ein Benutzer mit einer bestimmten Adresse existiert), setzen auf eine Versandbe-

stätigung um dem Absender eine gewisse Sicherheit hinsichtlich des Versands zu geben. In Web-Service basierten Systemen kann der Zustellstatus hingegen unmittelbar ermittelt werden. Somit wird in diesen Systemen eine Versandbestätigung nicht unbedingt als notwendig erachtet. Bei Zugangsbestätigungen gibt es einen höheren Konsens, wobei das behördliche Zustellsystem in Österreich diese Bestätigung rechtlich nicht vorsieht. Systeme, die keine Zugangsbestätigung bereitstellen, verfügen zumindest über eine Empfangsbestätigung, welche eine höhere Qualität, auch aufgrund der (qualifizierten) Unterschrift des Empfängers und der Übernahme und Bestätigung des Inhaltes der Zustellung, aufweist.

Tab. 1: Klassifizierung der Zustellsysteme im D-A-CH Raum

Name	OSCI	De-Mail	E-Postbrief	Öst. Zustellung	ERV	IncaMail
Nicht-Abstreitbarkeit						
Versandbestätigung	-	✓	✓	-	-	✓
Zugangsbestätigung	✓	✓	✓	-	✓	-
Empfangsbestätigung	✓	-	✓	✓	✓	✓
Vertraulichkeit						
Ende-zu-Ende Verschlüsselung	✓(m)	✓(o)	✓(o)	✓(o)	-	✓(o)
Transportprotokoll						
SOAP über HTTP	✓	-	-	✓	✓	-
SMTP	-	✓	-	-	-	✓
Authentisierungsniveaus						
Benutzername/Passwort	✓(i)	✓	✓	-	✓(i)	✓
2-Faktor (z.B. mobile TAN)	✓(i)	✓	✓	-	✓(i)	-
eID (Bürgerkarte / nPA)	✓(i)	✓	-	✓	✓(i)	✓
Elektronische Signaturen						
Fortgeschrittene Signatur	✓(i)	✓	✓	✓	✓(i)	✓
Qualifizierte Signatur	✓(i)	✓	-	✓	✓(i)	✓

Legende: (m) = verpflichtend (mandatory), (o) = optional, (i) = abhängig von der Implementierung des Providers

Eine durchgehende und obligatorische Ende-zu-Ende Verschlüsselung gibt es nur bei OSCI. Systeme wie De-Mail, E-Postbrief, IncaMail und das behördliche Zustellsystem in Österreich bieten eine optionale Verschlüsselung der Nachricht an, sofern das Verschlüsselungs-Zertifikat des Empfängers dem Absender zur Verfügung steht. Dass nicht alle Systeme eine Ende-zu-Ende Verschlüsselung als verpflichtend ansehen, hängt vermutlich mit einer Abwägung zwischen Sicherheit und Komfort auf Benutzerseite zusammen, da die Verwendung und Konfiguration von derartigen Sicherheitstechnologien in der Clientsoftware dem durch-

schnittlichen Benutzer oft nicht zumutbar ist. Die Wahl des dem Zustellsystem zugrundeliegenden Kommunikationsprotokolls, d.h. Webservice Technologie oder SMTP, scheint relativ gleichverteilt. Auch hier scheint eine Abwägung zwischen dem Verbreitungsgrad bzw. Transportkomfort (SMTP) und der Verwendung strukturierter Informationen (Webservices/XML) getroffen worden zu sein. Es muss aber erwähnt werden, dass die meisten Web-basierten Systeme für die Benutzeranbindung aus Komfortgründen trotzdem auch zusätzliche Clientschnittstellen über Mailprotokolle (SMTP/POP/IMAP) bereitstellen.

Bezüglich der Authentisierungsniveaus gibt es bei den beschriebenen Systemen durchgängig unterschiedliche Ansichten. Das österreichische Zustellsystem, De-Mail und IncaMail setzen auf elektronische Identitätskarten, z.B. die Bürgerkarte, den neuen Personalausweis (nPA) oder die Suisse ID. Konsens herrscht jedoch, dass bei Versandoptionen mit Empfangsbestätigung sich der Empfänger qualifiziert authentifizieren muss. Hinsichtlich elektronischer Signaturen gilt dasselbe wie für Authentisierungsniveaus. Wenngleich in allen Systemen fortgeschrittene Signaturen eingesetzt werden, gibt es keinen Konsens über den Einsatz qualifizierter Signaturen. Bei Einsatz der eID mit qualifiziertem Zertifikat werden qualifizierte Signaturen zumeist unterstützt. De-Mail ist das einzige System, bei dem Serversignaturen für Bestätigungen die Qualität einer qualifizierten Signatur aufweisen müssen.

Interoperabilität von Zustellsystemen ist ein relativ junges Forschungsfeld. Die Normierungsorganisation ETSI (European Telecommunications Standards Institute) hat sich bereits vor zwei Jahren dem Thema angenommen und einen Standard für elektronische Zustellsysteme publiziert, den Registered E-Mail (REM) Standard TS 102 640 [Etsi10]. Der Standard wurde bis dato aber noch nicht aufgegriffen, weder von der öffentlichen Verwaltung noch von Seiten der Wirtschaft. Dies hängt nicht zuletzt damit zusammen, dass hinter bestehenden Systemen ein gewisser Investitionsschutz steckt. Interoperabilität kann daher nicht alleine durch einen neuen allgemeingültigen Standard, sondern vielmehr nur durch das Koppeln und Verbinden bestehender Systeme hergestellt werden. Die relativ jungen EU Projekte STORK[2], SPOCS[3] und e-Codex[4] haben sich dem Thema Interoperabilität und Zustellung angenommen. Pilot 4 des EU Projekts STORK entwickelt ein Interoperabilitäts-Framework zur grenzüberschreitenden Zustellung von elektronischen Dokumenten mit der Qualität des klassischen Einschreibens mit Rückschein. Das Framework wird zwischen dem österreichischen behördlichen Zustellsystem und dem benachbarten System des slowenischen Postdienstleisters[5] demonstriert. SPOCS erweitert und optimiert dieses Framework und wird eine Pilotierung zwischen dem österreichischen System, OSCI und dem italienischen Pendant PEC (Posta Elettronica Certificata) [GeMB05] durchführen. Im Gegensatz zu STORK und SPOCS konzentriert sich e-Codex ausschließlich auf Systeme im Justizsektor und entwickelt ein Interoperabilitäts-Framework für den österreichischen ERV, den deutschen EGVP und das niederländischen Pendant, dem sogenannten JUBES (Justitie Berichten Service).

Eine genaue Einschätzung und Bewertung von bestehenden Systemen ist für Interoperabilitätsbestrebungen unerlässlich, um Anforderungen klar definieren und Konzepte optimiert entwerfen zu können. Dabei ist es wichtig, nicht nur Interoperabilität auf technischer Ebene

[2] STORK = Secure idenTity acrOss boRders linKed

[3] SPOCS = Simple Procedures Online for Cross-border Services

[4] e-CODEX = e-Justice Communication via Online Data Exchange

[5] https://moja.posta.si

herzustellen, wie z.B. Webservices mit SMTP zu koppeln bzw. die Protokolle zu transformieren. Eine Harmonisierung muss auch auf semantischer und prozeduraler Ebene erfolgen. Hier ist besonders ein gemeinsames Verständnis von Bestätigungen (Non-Repudiation Services), Authentisierungsniveaus und elektronsicher Signaturen wichtig. Speziell im Rahmen von behördlichen Zustellungen muss der rechtliche Weg mit der Einführung von gemeinsamen Regeln und Gesetzen für eine grenzüberschreitende Zustellung auf europäischer Ebene geebnet werden.

6 Zusammenfassung

Ziel dieses Artikels ist es, einen Überblick über die bestehenden Zustellsysteme mit der Qualität eines elektronischen Einschreibens im D-A-CH Raum zu geben. Wir haben den deutschen OSCI Standard sowie die zwei dominanten Zustellsysteme, De-Mail und den E-Postbrief beschrieben. Neben dem behördlichen Zustellsystem gibt es in Österreich noch das justizielle System „Elektronischer Rechtsverkehr“. Repräsentativ für die Schweiz haben wir IncaMail der Schweizerischen Post beschrieben. Zusammenfassend kann gesagt werden, dass es zwischen den beschriebenen Systemen keinen Konsens über das Bereitstellen von Versandbestätigungen gibt. Bei Zugangsbestätigungen bzw. Empfangsbestätigungen ist hingegen eher ein Konsens zu finden. Dasselbe gilt für eine End-zu-Ende Verschlüsselung. Außer in OSCI wird in keinem System eine solche Verschlüsselung als verpflichtend erachtet. Bei Authentisierungsniveaus gibt es diverse Unterschiede, wobei zumindest eine einhellige Meinung dahingehend besteht, dass die Versandoption Empfangsbestätigung daran gebunden ist, dass der Empfänger sich mit einem hohen Authentisierungsniveau anmeldet (mindestens 2-Faktor). Mit Ausnahme von De-Mail, das qualifizierte Signaturen durchgängig bei allen Bestätigungen einsetzt, sind qualifizierte Signaturen vorwiegend bei Signaturen mittels eID des Senders oder Empfängers zu finden. Nichtsdestotrotz finden wir momentan ein heterogenes Ökosystem an Zustellsystemen vor. Im Sinne der Digitalen Agenda und der EU-Dienstleistungsrichtlinie sollten bestehende Systeme interoperabel gemacht werden, um die grenzüberschreitende Zustellung und somit die Mobilität innerhalb der europäischen Union zu steigern.

Literatur

[BuSI09] BSI (Bundesamt für Sicherheit in der Informationstechnik). De-mail, Technische Richtlinie für Bürgerportale (2009)

[CDF+07] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer. OpenPGP Message Format. In: IETF RFC 4880 (2007)

[DePo11] Deutsche Post. Die Post im Internet. Der E-Postbrief. http://www.epost.de, zuletzt besucht am 23.05.2011.

[DiKe10] J. Dietrich, J. Keller-Herder. De-Mail — verschlüsselt, authentisch, nachweisbar. In: Datenschutz und Datensicherheit – DuD (2010) 299-301

[Etsi0] European Telecommunications Standards Institute (ETSI), “Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM)”, ETSI TS 102 640, v2.1.1 (2010)

[EuKo10a] Europäische Kommission. Eine Digitale Agenda für Europa (2010)

[EuKo10b] Europäische Kommission. Europäischer e-Government Aktionsplan 2011-215 (2010)

[EuSr99] EU Signaturrichtlinie 1999, Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen. In: Amtsblatt der Europäischen Gemeinschaften L13/12 (1999)

[GeMB05] F. Gennai, L. Martusciello, M. Buzzi, A certified email system for the public administration in Italy. In: IADIS International Conference WWW/Internet, (2005) 143-147

[Lapp09] T. Lapp. Brauchen wir De-Mail und Bürgerportale? In: Datenschutz und Datensicherheit – DuD (2009) 651-655

[Orne07] G. Ornetsmüller, webERV – ERVServices – Beschreibung der Webservice-Schnittstelle Teilnehmer <-> Übermittlungsstelle (2007).

[Osci10] OSCI Steering Office, OSCI-Transport – Web Services Profiling and Extensions Specification, Version 2.0. December 2010. Zuletzt abgerufen am 16.03.2010 unter http://www.xoev.de/sixcms/detail.php?gsid=bremen83.c.2316.de

[PlWe07] F. Planitzer, W. Weisweber. In: Virtual Post Office in Practice. ISSE/SECURE 2007 Securing Electronic Business Processes (2007) 427-437

[Rams04] B. Ramsdell, Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification. In: IETF RFC 3851 (2004)

[ReTa08] P. Reichstädter, A. Tauber. Modell und Prozesse der elektronischen Zustellung (zusemod-1.3.0) (2008)

[Roes09] T. Rössler, Object Identifier der öffentlichen Verwaltung (Teil 2 – Taxative Definition) (2009)

[ScPo11] Die Schweizerische Post. IncaMail – vertraulich und nachweislich e-mailen. http://www.incamail.ch. Zuletzt besucht am 23.05.2011.

[Taub09] A. Tauber, Requirements for Electronic Delivery Systems in E-Government, an Austrian Experience. In: Software Services for e-Business and e-Society, IFIP Advances in Information and Communication Technology, vol. 305 (2009) 123-133