Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatikstrategieorgan Bund ISB
Informatiksicherheit SEC

17. November 2010

Kriterienkatalog für die Anerkennung von Zustellplattformen – Version 1.0

Inhalt

1 Zweck ... 2
2 Begriffsbildung ... 2
2.1 Elektronische Nachricht ... 2
2.2 Zustellplattform ... 2
2.3 Eingabeplattform ... 2
2.4 Ausgabeplattform ... 2
3 Anforderungen an Zustellplattformen ... 3
3.1 Anforderungen an die Architektur ... 3
3.2 Technische Sicherheitsanforderungen ... 4
3.2.1 Zugriffsverfahren ... 4
3.2.2 Verschlüsselungsverfahren ... 4
3.2.3 Quittungen ... 5
3.3 Betriebliche Anforderungen ... 6
3.3.1 Informationssicherheit ... 6
3.3.2 IT Service Management ... 6
3.3.3 Information für Benutzer ... 7
3.4 Anforderungen an ein übergreifendes Teilnehmerverzeichnis ... 7
3.5 Anforderungen an die Vermittlungsfunktionen zwischen Zustellplattformen ... 9
3.6 Nutzungskosten ... 10
4 Quellenverzeichnis ... 10
4.1 Relevante ISO Normen ... 10
4.2 Referenzen ... 11

1 Zweck

Dieses Dokument beinhaltet einen detaillierten Katalog von Anforderungen an die Architektur, die technische Sicherheit sowie den Betrieb von Zustellplattformen als Basis für die Regelung des Anerkennungsverfahrens für Zustellplattformen gemäss Artikel 3 der Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen von Zivil- und Strafprozessen sowie von Schuldbetreibungs- und Konkursverfahren (SR 272.1; AS 2010 3105; nachfolgend abgekürzt: VeÜ-ZSSchK).

Anerkannte Zustellplattformen können auch für die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens eingesetzt werden. Anerkennungsentscheide des Eidgenössischen Finanzdepartements EFD gelten stets auch für die Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (SR 172.021.2; AS 2010 3031; abgekürzt: VeÜ-VwV). Für Eingaben an ein Gericht oder eine Bundesbehörde soll möglichst auch die gleiche Infrastruktur benutzt werden können.

Weil aber an einfache Verwaltungsverfahren nicht dieselben Anforderungen gestellt werden wie an Zivil- und Strafprozesse sowie von Schuldbetreibungs- und Konkursverfahren, können Bundesbehörden dafür auch eine andere Übermittlungsart verwenden, wenn diese in geeigneter Weise erlaubt, die Adressatin oder den Adressaten eindeutig zu identifizieren, den Zeitpunkt der Zustellung eindeutig festzustellen und die Verfügung bis zur Zustellung in verschlüsselter Form zu übermitteln.

Dieser Kriterienkatalog wird regelmässig überprüft und bei Bedarf angepasst oder ergänzt.

2 Begriffsbildung

2.1 Elektronische Nachricht

Eine elektronische Nachricht besteht aus einem Kopf- (Header) und einem Rumpfteil (Body), allenfalls ergänzt durch einen oder mehrere Anhänge. Rumpfteil und Anhänge werden als Komponenten bezeichnet.

2.2 Zustellplattform

Eine Zustellplattform ist ein informations- und kommunikationstechnisches System, das der sicheren und nachvollziehbaren Zustellung von elektronischen Nachrichten dient. Die Nachvollziehbarkeit wird über elektronische Quittungen sichergestellt, die zum Zeitpunkt der Eingabe bzw. zum Zeitpunkt der Übergabe der elektronischen Nachricht an die Empfängerin oder den Empfänger ausgestellt werden, einen entsprechenden Zeitstempel enthalten und selbst digital signiert sind.

2.3 Eingabeplattform

Eine Eingabeplattform ist eine Zustellplattform, die nur Eingaben unterstützt und entsprechend nur Quittungen ausgibt, die den Zeitpunkt der Eingabe einer elektronischen Nachricht belegen.

2.4 Ausgabeplattform

Eine Ausgabeplattform ist eine Zustellplattform, die nur Ausgaben unterstützt und entsprechend nur Quittungen ausgibt, die den Zeitpunkt der Übergabe einer elektronischen Nachricht an eine Empfängerin oder einen Empfänger belegen.

3 Anforderungen an Zustellplattformen

3.1 Anforderungen an die Architektur

Die Architektur muss sich am Stand der Technik orientieren sowie vollständig und nachvollziehbar beschrieben sein. Im Sinne eines kontinuierlichen Verbesserungsprozesses muss sie periodisch überprüft und gegebenenfalls angepasst werden. Insbesondere müssen die folgenden Anforderungen an die Architektur mindestens erfüllt sein:

- Das Netzwerk muss gemäss Ergebnis einer Risikobeurteilung segmentiert sein. Die Server für den Betrieb von Zustellplattformen müssen entsprechend ihrem Schutzbedarf über die Netzwerksegmente verteilt werden (siehe Leitfaden zur Implementierung der ISO/IEC 27001:2005 Klausel A.11.4.5, Segregation in networks).
- Server, die vom Internet her erreichbar sind, müssen bedarfsgerecht gehärtet sein (Ergänzung zum Leitfaden zur Implementierung der ISO/IEC 27001:2005 Klausel A.12.1.1, Security requirements analysis and specification). Dazu sollten Best Practices beigezogen werden, wie sie z.B. das Center for Internet Security (CIS) mit den Security Configuration Benchmarks zur Verfügung stellt.
- Entwicklungs-, Test- und Produktionsplattformen müssen voneinander getrennt sein (siehe Leitfaden zur Implementierung der ISO/IEC 27001:2005 Klausel A.10.1.4, Separation of development, test and operational facilities).
- Die bekannten Angriffe gegen Web-Anwendungen, wie sie z.B. vom Open Web Application Security Project (OWASP) dokumentiert werden, müssen erfolgreich abgewehrt werden können (siehe Leitfaden zur Implementierung der ISO/IEC 27001:2005 Klausel A.12.6.1, Control of technical vulnerabilities).
- Elektronische Nachrichten dürfen ausschliesslich in verschlüsselter Form übermittelt und gespeichert werden (siehe Leitfaden zur Implementierung der ISO/IEC 27001:2005 Klauseln A.12.3.1, Policy on the use of cryptographic controls; A.12.3.2, Key management; A.15.1.6, Regulation of cryptographic controls). Eine End-zu-End Verschlüsselung von elektronischen Nachrichten ist nicht erforderlich. Für die Weiterleitung von elektronischen Nachrichten ist es hinreichend, wenn der Kommunikationskanal gesichert ist. Zustellplattformen im Hoheitsbereich einer Behörde dürfen elektronische Nachrichten unverschlüsselt speichern und an interne Systeme weiterleiten. Das aus dieser technischen Schwachstelle resultierende Risiko für eine durchgängige Informationssicherheit muss auf der Basis einer Risikobeurteilung gemäss ISO/IEC 27001:2005 mit angemessenen und wirksamen organisatorischen Massnahmen (Regelung der Verantwortlichkeiten, Arbeitsverfahren, Prozesse) und personellen Massnahmen (Sensibilisierung, Ausbildung und Training der betroffenen Mitarbeitenden) auf ein Restrisiko reduziert werden, das mit den Risikoakzeptanzkriterien der Behörde konsistent ist. Mit Einverständnis des Absenders kann in diesem Fall bei einer Eingabe auf die Verschlüsselung verzichtet werden.
- Bei Verwendung von Passwörtern darf der Betreiber diese nicht auf Dauer speichern oder in Logfiles protokollieren (Ergänzung zum Leitfaden zur Implementierung der ISO/IEC 27001:2005 Klauseln A.11.2.3, User password management; A.10.10.1, Audit logging).

Zur Information der Benutzer müssen zusätzlich die wesentlichen Merkmale der Architektur in einer für technische Laien verständlichen und überzeugenden Form dargestellt werden. Diese Information muss durch den Diensteanbieter auf der Zustellplattform veröffentlicht werden.

3.2 Technische Sicherheitsanforderungen

3.2.1 Zugriffsverfahren

Die Anforderungen an Zugriffsverfahren müssen sich am Stand der Technik sowie der aktuellen Bedrohungslage orientieren und vollständig und nachvollziehbar beschrieben sein. Im Sinne eines kontinuierlichen Verbesserungsprozesses müssen sie periodisch überprüft und gegebenenfalls angepasst werden. Insbesondere müssen die folgenden Anforderungen an Zugriffsverfahren mindestens erfüllt sein:

- Der Zugriff auf elektronische Nachrichten in Übermittlung darf nur über starke Authentifikationsverfahren (z.B. digitale Zertifikate oder persönliche Tokens) erfolgen. Dabei sind starke Authentifikationsverfahren im Sinne der Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB, Anhang 2, Abschnitt 5.3 zu verstehen. Insbesondere darf die Authentifikationsinformation nicht im Klartext übertragen werden, um nicht verwundbar gegenüber Abhorchungs- und Wiedereinspielungsangriffen zu sein (Ergänzung zum Leitfaden zur Implementierung der ISO/IEC 27001:2005 Klausel A.11.4.2, User authentication for external connections).
- Wenn im Authentifikationsverfahren Passwörter eingesetzt werden, müssen diese immer über verschlüsselte Verbindungen übertragen werden (z.B. im Rahmen einer SSL/TLS Session). Werden im Authentifikationsverfahren ausschliesslich Passwörter eingesetzt, müssen diese in Bezug auf die Passwortstärke (ohne Aging) den Anforderungen der Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB, Anhang 1, Abschnitt 2.4, genügen (Ergänzung zum Leitfaden zur Implementierung der ISO/IEC 27001:2005 Klauseln A.11.2.3, User password management; A.11.3.1, Password use).
- Passwörter dürfen nicht auf Dauer gespeichert oder in Logfiles protokolliert werden (Ergänzung zum Leitfaden zur Implementierung der ISO/IEC 27001:2005 Klauseln A.11.2.3, User password management; A.10.10.1, Audit logging).

Zur Information der Benutzer müssen zusätzlich die wesentlichen Merkmale der eingesetzten Zugriffsverfahren in einer für technische Laien verständlichen und überzeugenden Form dargestellt werden. Diese Information muss durch den Diensteanbieter auf der Zustellplattform veröffentlicht werden.

3.2.2 Verschlüsselungsverfahren

Die eingesetzten kryptografischen Verfahren und Systeme müssen dem Stand der Technik entsprechen und sich an der aktuellen Bedrohungslage orientieren. Vorzugsweise sind standardisierte Verfahren und Systeme einzusetzen, wie sie etwa in der Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 6. Januar 2010 der Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen empfohlen werden. Bei proprietären Verfahren und Systemen muss Resistenz gegenüber bekannten kryptanalytischen Angriffen nachgewiesen sein.

Zustellplattformen müssen so konzipiert sein, dass eingesetzte kryptografische Verfahren und Systeme bzw. deren Schlüssellängen mit vertretbarem Aufwand ersetzt werden können.

Für die Übertragung ist eine Verschlüsselung des Inhaltes nur mit Passworten nicht zugelassen, um Offline Password Guessing zu verunmöglichen.

Die Stärke der eingesetzten kryptografischen Verfahren und Systeme muss im Rahmen einer ganzheitlichen Sicherheitsarchitektur vollständig und nachvollziehbar beschrieben werden. Im Sinne eines kontinuierlichen Verbesserungsprozesses müssen die kryptografischen

Verschlüsselungsverfahren periodisch überprüft und gegebenenfalls angepasst werden.

Zur Information der Benutzer müssen zusätzlich die wesentlichen Merkmale der eingesetzten kryptografischen Verfahren und Systeme in einer für technische Laien verständlichen und überzeugenden Form dargestellt werden. Diese Information muss durch den Diensteanbieter auf der Zustellplattform veröffentlicht werden.

3.2.3 Quittungen

Die Eingabeplattform stellt dem Absender den folgenden Typ von Quittung aus:

- Eingabequittung für die Übermittlung durch den Absender auf die Eingabeplattform.

Die Ausgabeplattform stellt dem Absender den folgenden Typ von Quittung aus:

- Ausgabequittung für die Abholung von der Ausgabeplattform durch den Empfänger.

Quittungen müssen mindestens die folgende Information enthalten:

- Information zur elektronische Nachricht selbst
  - Information zum Absender (Name, E-Mail Adresse etc.)
  - Information zum Empfänger (Name, E-Mail Adresse etc.)
  - Betreff (sofern vorhanden)
  - Zeitpunkt der Übermittlung durch den Absender auf die Eingabeplattform, oder Zeitpunkt der Abholung durch den Empfänger von der Ausgabeplattform
- Komponenten selber oder Informationen dazu sowie für jede einzelne Komponente (falls die Nachricht nicht End-zu-End chiffriert ist)
  - Name der Komponente (sofern vorhanden)
  - Format der Komponente
  - Grösse der Komponente in Bytes
  - Hashwert der Komponente, vorzugsweise mit zwei verschiedenen Hashfunktionen berechnet

Die Quittung muss von der Zustellplattform als digital signiertes, strukturiertes Textdokument bereitgestellt werden, welches folgende Eigenschaften aufweist:

- Die Signatur basiert auf einem Zertifikat einer gemäss Bundesgesetz vom 19. Dezember 2003 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Bundesgesetz über die elektronische Signatur, ZertES; SR 943.03) und der dazugehörigen Verordnung vom 3. Dezember 2004 über Zertifizierungsdienste im Bereich der elektronischen Signatur (Verordnung über die elektronische Signatur, VZertES; SR 943.032) anerkannten Anbieterin.
- Die in der Quittung aufgeführten Zeitpunkte stammen von einem synchronisierten Zeitstempeldienst einer gemäss ZertES und VZertES anerkannten Anbieterin.
- Der in der Quittung vom synchronisierten Zeitstempeldienst bestätigte Zeitpunkt des Eingangs einer elektronischen Nachricht auf der Eingabeplattform bzw. der Abholung einer elektronische Nachricht durch den Empfänger (Zeitstempel) darf nicht mehr als eine Minute vom Zeitpunkt des Eingangs bzw. der Abholung der elektronischen Nachricht abweichen.

- Die Quittung muss spätestens eine Minute nach der Erzeugung des Zeitstempels bereitgestellt sein, im Falle von Sammelquittungen eine Minute nach der Erzeugung des Zeitstempels für die letzte Zustellung.

Die oben genannten Zeiten gelten als Regelzeit. Überschreitungen müssen über eine Protokollierung nachgewiesen werden.

3.3 Betriebliche Anforderungen

3.3.1 Informationssicherheit

Die Informationssicherheit ist durch Einrichtung eines Informationssicherheitsmanagementsystems (ISMS) nach ISO/IEC 27001:2005 (Information technology – Security techniques – Information security management systems – Requirements) nachzuweisen. Dieser Nachweis ist wie folgt zu erbringen:

- Bei Betrieb durch Behörden, unabhängig von deren Grösse: Vorlage des Berichts zum formalen internen ISMS Audit gemäss Klausel 6 von ISO/IEC 27001:2005. Der Auditbericht darf keine Befunde enthalten, die eine Zertifzierung ausschliessen. Hinsichtlich der Prinzipien der Auditierung, der Durchführung des Audits und der Kompetenzen des Auditors müssen die Richtlinien von ISO 19011:2002 (Guidelines for quality and/or environmental management systems auditing) eingehalten werden. Der Audit muss mindestens einmal pro Jahr wiederholt werden. Der jeweilige Auditbericht ist unaufgefordert vorzulegen.
- Bei Betrieb durch Privatunternehmen, unabhängig von deren Grösse: Vorlage des durch eine akkreditierte Zertifizierungsstelle ausgestellten Zertifikats, das die Zertifizierung nach ISO/IEC 27001:2005 bescheinigt.

Die in den Anforderungen an Zustellplattformen referenzierten Klauseln in ISO/IEC 27001:2005 dürfen nicht ausgeschlossen werden.

3.3.2 IT Service Management

Beim Betrieb von Zustellplattformen ist von Montag bis Sonntag eine Servicezeit von 00:00 – 24:00 anzubieten. Allfällige Servicefenster müssen im Zeitraum 00:15 - 07:00 der zum Zeitpunkt gültigen Schweizer Zeit terminiert werden.

Die Verfügbarkeit von Zustellplattformen muss protokolliert und über die Zustellplattformen veröffentlicht werden.

Für den zuverlässigen Betrieb von Zustellplattformen muss nachgewiesen werden, dass die folgenden Betriebsprozesse dokumentiert, eingeführt, betrieben, permanent überwacht, periodisch geprüft, unterhalten und verbessert werden:

- Service Lieferprozesse
  - Management von Serviceniveaus
  - Service Berichtswesen
  - Servicekontinuitäts- und -verfügbarkeitsmanagement
  - Budgetierung und Verrechnung von IT Services
  - Kapazitätsmanagement
- Prozesse zum Beziehungsmanagement
  - Pflege der Beziehung zwischen Leistungserbringer und Kunden

  - Lieferantenmanagement
- Prozesse zur Lösung von Störungen und Problemen
  - Behandlung von Störungen (Vorfällen)
  - Behebung von Problemen
- Steuerungs- und Überwachungsprozesse
  - Konfigurationsmanagement
  - Veränderungsmanagement
- Freigabeprozess
  - Management des Freigabeprozesses

Die Betriebsprozesse müssen sich an den internationalen Standards ISO/IEC 20000-1:2005 (Information technology – Service management – Part 1: Specification) und ISO/IEC 20000-2:2005 (Information technology – Service management – Part 2: Code of practice) orientieren.

Zusätzlich muss ein professioneller Service Desk eingeführt, betrieben, permanent überwacht, periodisch geprüft, unterhalten und verbessert werden, der sich z.B. an der IT Infrastructure Library (ITIL) orientiert.

3.3.3 Information für Benutzer

Der Diensteanbieter muss auf der Zustellplattform die folgende Information in einer für technische Laien verständlichen und überzeugenden Form veröffentlichen:

- Die wesentlichen Merkmale der Architektur
- Die wesentlichen Merkmale der Zugriffsverfahren
- Die wesentlichen Merkmale der kryptografischen Verfahren

Zusätzlich muss darauf hingewiesen werden, dass eine End-zu-End Verschlüsselung von elektronischen Nachrichten nicht erforderlich ist. Somit könnten die elektronischen Nachrichten auf der anerkannten Zustellplattform einen kurzen Moment (im Millisekundenbereich) unverschlüsselt sein und vom Betreiber verbotenerweise eingesehen werden. Wenn die Benutzer das Risiko einer solchen Einsichtnahme nicht in Kauf nehmen wollen, müssen sie entweder auf die Benutzung der entsprechenden Zustellplattform verzichten oder die elektronische Nachricht mit dem öffentlichen Chiffrierschlüssel der empfangenden Stelle verschlüsseln (falls ein solcher verfügbar ist).

3.4 Anforderungen an ein übergreifendes Teilnehmerverzeichnis

Im Hinblick auf die plattformübergreifende Vermittlung von elektronischen Nachrichten wird ein übergreifendes Teilnehmerverzeichnis aufgebaut und betrieben. Dieses Verzeichnis ist nicht öffentlich, d.h. es dürfen nur registrierte Behörden und identifizierte Benutzer über ihre Plattform auf das Verzeichnis zugreifen. Insbesondere soll es für sie bei der Erstellung einer Nachricht möglich sein, mittels exakter Suchanfrage bestimmte Teilnehmer zu finden (z.B. über die Bezeichnung einer Behörde oder die E-Mail-Adresse eines identifizierten Benutzers). Die Verwendung von Wildcards ist dabei nicht zulässig.

Das übergreifende Teilnehmerverzeichnis stellt die Teilnehmerverzeichnisse der Zustellplattformen als separate Unterbäume mit Schreibberechtigung zur Verfügung. Der Wurzel dieser Unterbäume liegt eine LDAP Objektklasse mit den folgenden Attributen zugrunde:

Name des Attributs	Bedeutung	Beispiele
Ou	Kanonischer Name der Zustellplattform.	Incamail, ekomm
platformUri	URI, unter welcher die Zustellplattform erreichbar ist.	https://www.bla.ch:8080/
smtpUri	Adresse des für die Interoperabilität bereitgestellten MTA der Zustellplattform.	smtps://smtp.bla.ch:25001/
smimeSignCertificate smimeEncryptionCertificate	Öffentliche Schlüssel der Zustellplattform, die für die S/MIME E-Mail verwendet werden (können auch identisch sein). Format: PKCS#7 SignedData.	
smtpCertificate	Öffentlicher Schlüssel des für die Interoperabilität bereitgestellten MTA der Zustellplattform. Format: PKCS#7 SignedData.	

Den Einträgen in den Unterbäumen des Verzeichnisses ist die Objektklasse inetOrgPerson (gemäss RFC 2798 - Definition of the inetOrgPerson LDAP Object Class) zugrundeliegend. Minimal müssen die folgenden Attribute definiert sein:

- Mail (mail)
- Distinguished name (dn) (aufgebaut unter Verwendung des Attributs Mail)

Zudem kann für jeden Teilnehmer ein Attribut vorgesehen sein, das es erlaubt, zu entscheiden, ob es sich bei diesem Teilnehmer um eine registrierte Behörde oder einen identifizierten Benutzer handelt. Im zweiten Fall kann ein zusätzliches Sichtbarkeitsattribut vorgesehen sein, das es dem Benutzer erlaubt, festzulegen, ob er für andere Benutzer sichtbar sein will (für Behörden sind Verzeichniseinträge allerdings immer sichtbar).

Die Zustellplattformen liefern den Behörden die auf der Zustellplattform verwendete Behördenbezeichnung und den Ort (z.B. Bundesverwaltungsgericht, Bern).

Die Ausgestaltung des übergreifenden Teilnehmerverzeichnisses wird noch im Detail geklärt und die diesbezüglichen Anforderungen werden noch angepasst. Zusätzlich zu den Vorgaben und Richtlinien des Datenschutzes müssen aus heutiger Sicht aber mindestens die folgenden Anforderungen erfüllt sein:

- Jede Zustellplattform muss dem Betreiber des übergreifenden Teilnehmerverzeichnisses ein Verzeichnis der auf ihr registrierten Behörden und identifizierten Benutzern (z.B. gemäss ZertES) zur Verfügung stellen und mindestens einmal pro Tag aktualisieren.
- Der Zugriff des übergreifenden Teilnehmerverzeichnisses auf die Teilnehmerverzeichnisse der Zustellplattformen, sowie der Zugriff der Zustellplattformen auf das übergreifende Teilnehmerverzeichnis müssen gegenseitig authentifiziert sein. Idealerweise wird dabei LDAPS (LDAP over SSL) mit Zertifikaten einer anerkannten Zertifizierungsdiensteanbieterin eingesetzt.

3.5 Anforderungen an die Vermittlungsfunktionen zwischen Zustellplattformen

Es gelten die folgenden Grundannahmen:

- Jeder Benutzer ist auf einer Zustellplattform durch seine E-Mail Adresse identifiziert. Ein Benutzer kann die Rollen Absender oder Empfänger einnehmen.
- Jede Zustellplattform stellt für die Vermittlungsfunktion einen SMTP Mail Transfer Agent (MTA) bereit und publiziert dessen Adresse, zusammen mit einem Public Key (x.509 Zertifikat) in einem übergreifenden Teilnehmerverzeichnis.
- Der Verkehr zwischen den verschiedenen Zustellplattformen erfolgt mit Secure SMTP over TLS gemäss RFC 3207 (verschlüsselter Übermittlungskanal).
- Elektronische Nachrichten werden zwischen den Zustellplattformen als MIME-multipart E-Mails übertragen. Die gesamte Nachricht wird gemäss S/MIME Standard von der absendenden Plattform mit ihrem Private Key signiert und mit dem Public Key der empfangenden Plattform verschlüsselt.
- Jede Plattform verfügt über drei Schlüsselpaare (wobei in der Umsetzung Mehrfachverwendungen derselben Schlüssel erlaubt sind): Ein Paar für Secure SMTP over TLS und zwei weitere Paare für S/MIME.

Die Zustellung einer elektronischen Nachricht eines auf der Zustellplattform Z1 registrierten Benutzers A (Absender A) an den auf der Zustellplattform Z2 registrierten Benutzer B (Empfänger B) geschieht wie folgt:

- Absender A verifiziert unter Verwendung des übergreifenden Teilnehmerverzeichnisses, dass Empfänger B auf Zustellplattform Z2 registriert ist.
- Zustellplattform Z1 verpackt die elektronische Nachricht in eine S/MIME konforme E-Mail mit den folgenden SMTP Headereinträgen:
  - To: Bezeichnet die E-Mail Adresse des Empfängers B auf Zustellplattform Z2.
  - From: Bezeichnet die E-Mail Adresse des Absenders A auf Zustellplattform Z1.
  - Message-ID: Eine von Zustellplattform Z1 vergebene Identifikation für die übermittelte elektronische Nachricht.
  - X-ZP-MsgType: Bezeichnet den Meldungstyp. Im Fall der Übermittlung der elektronische Nachricht ist hier immer der Wert «message» zu verwenden.
- Zustellplattform Z1 signiert die E-Mail mit dem eigenen Private Key und verschlüsselt diese mit dem Public Key von Zustellplattform Z2.
- Die signierte und verschlüsselte E-Mail wird an den MTA von Zustellplattform Z2 übertragen.
- Zustellplattform Z2 entschlüsselt die empfangene E-Mail, überprüft und entfernt die Signatur und legt die elektronische Nachricht im Postfach des Empfängers B ab.
- Zustellplattform Z2 informiert Zustellplattform Z1 über die folgenden Ereignisse:
  - elektronische Nachricht durch Empfänger B abgeholt.
  - Zustellfrist für die elektronische Nachricht ungenutzt abgelaufen.
  - ungültige Signatur der übermittelten elektronischen Nachricht.
- Diese Ereignisse werden wie folgt auf E-Mails abgebildet:
  - Zustellplattform Z2 erstellt eine S/MIME konforme E-Mail mit den folgenden SMTP Headereinträgen:

- To: Bezeichnet die E-Mail Adresse des Absenders A auf Zustellplattform Z1.
- From: Bezeichnet die E-Mail Adresse des Empfängers B auf Zustellplattform Z2.
- Message-ID: Eine von der Zustellplattform Z2 vergebene Identifikation.
- In-Reply-To: Der durch die Zustellplattform Z1 vergebenen Wert im Feld Message-ID.
- X-ZP-MsgType: Bezeichnet den Meldungstyp. Im Fall der Bekanntgabe von Ereignissen sind folgende Werte zu verwenden:
  - receipt-deposited: Elektronische Nachricht im Postfach des Empfängers B abgelegt.
  - receipt-delivered: Elektronische Nachricht durch Empfänger B abgeholt.
  - receipt-timed-out: Zustellfrist für die elektronische Nachricht ungenutzt abgelaufen.
  - receipt-refused: Annahme der elektronischen Nachricht durch Empfänger B wurde verweigert.
  - receipt-invalid-signature: Signatur der übermittelten elektronischen Nachricht ungültig.

  Hat X-ZP-MsgType den Wert receipt-delivered, so enthält der E-Mail Body die Quittung gemäss Abschnitt 3.2.3. In den beiden anderen Fällen ist der E-Mail Body leer.
- Zustellplattform Z2 signiert die E-Mail mit dem eigenen Private Key und verschlüsselt diese mit dem Public Key von Zustellplattform Z1.
- Die signierte und verschlüsselte E-Mail wird an den MTA von Zustellplattform Z1 übertragen.
- Zustellplattform Z1 entschlüsselt die empfangene E-Mail, überprüft und entfernt die Signatur und meldet die Ereignisse an den Absender A in geeigneter Form weiter bzw. stellt diesem die Quittung zu.

3.6 Nutzungskosten

Die Zustellplattformen stellen einander die Interoperabilitätsschnittstelle und die Angaben für das übergreifende Teilnehmerverzeichnis im Sinne einer «Fair Use» kostenlos zur Verfügung.

Verlangt ein Plattform-Betreiber für die Verwendung der Interoperabilitätsschnittstelle oder des übergreifenden Teilnehmerverzeichnisses Kosten (insbesondere für die Abgeltung von Schutzrechten) verliert er seine Zulassung resp. kann keine solche erhalten.

4 Quellenverzeichnis

4.1 Relevante ISO Normen

- ISO/IEC 20000-1:2005 (Information technology – Service management – Part 1: Specification)
- ISO/IEC 20000-2:2005 (Information technology – Service management – Part 2: Code of practice)
- ISO/IEC 27000:2009 (Information technology – Security techniques – Information security management systems – Overview and vocabulary)

- ISO/IEC 27001:2005 (Information technology – Security techniques – Information security management systems – Requirements)
- ISO/IEC 27002:2005 (Information technology – Security techniques – Code of practice for information security management)
- ISO/IEC 27005:2008 (Information technology – Security techniques – Information security risk management)
- ISO/IEC CD 27007 (Information technology – Security techniques – Guidelines for information security management systems auditing); erwartet für 2010
- ISO 19011:2002 (Guidelines for quality and/or environmental management systems auditing)

4.2 Referenzen

- ISO27001 Security home (http://iso27001security.com/)
- International Register of ISMS Certificates (http://www.iso27001certificates.com/)
- Open Web Application Security Project (OWASP) (http://www.owasp.org)
- Center for Internet Security (CIS) (http://www.cisecurity.org/)
- Office of Government Commerce (2001). Service Delivery. IT Infrastructure Library. The Stationery Office. ISBN 0-11-330017-4
- Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB, Anhang 1: Checkliste der minimalen Sicherheitsanforderungen und Verantwortlichkeiten für den generellen Schutzbedarf (www.isb.admin.ch)
- Weisungen über die Informatiksicherheit in der Bundesverwaltung WIsB, Anhang 2: Definitionen und Sicherheitsvorgaben für die Netzwerksicherheit (www.isb.admin.ch)
- Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 6. Januar 2010 (www.bundesnetzagentur.de > Sachgebiete > Qualifizierte elektronische Signatur > Veröffentlichungen > Geeignete Algorithmen)