Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ
Direktionsbereich Zentrale Dienste
Fachbereich Rechtsinformatik

Anforderungen an Plattformen für die sichere Zustellung im Rahmen von rechtlichen Verfahren (Kriterienkatalog Zustellplattformen)

vom 16. September 2014 (Version 2.0)

Anhang zur Verordnung des EJPD vom 16. September 2014 (SR …) über die Anerkennung von Plattformen für die sichere Zustellung im Rahmen von rechtlichen Verfahren (Anerkennungsverordnung Zustellplattformen)

Inhaltsverzeichnis

1 Zweck und Inhalt

[1] Der vorliegende Kriterienkatalog spezifiziert die Anforderungen an Zustellplattformen gemäss Artikel 2 der Anerkennungsverordnung Zustellplattformen.

[2] Anerkannte Zustellplattformen können auch für die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens eingesetzt werden. Anerkennungsentscheide des Eidgenössischen Justiz- und Polizeidepartements (EJPD) gelten somit stets auch für die Verordnung vom 18. Juni 2010 über die elektronische Übermittlung im Rahmen eines Verwaltungsverfahrens (VeÜ-VwV, SR 172.021.2).

2 Grundlegende Bestandteile elektronischer Nachrichten

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

3 Beizug von Dritten

Die Inhaberin der Anerkennung (Dienstanbieterin) kann den technischen Betrieb der Plattform ganz oder teilweise auf Dritte übertragen. Sie behält dabei die technische, administrative, rechtliche und Führungsverantwortung.

4 Anforderungen an die Informationssicherheit

4.1 Grundanforderungen für Privatunternehmen

[1] Ist die Dienstanbieterin ein Privatunternehmen, ist die Informationssicherheit durch Einrichtung, Implementierung, Betrieb, Überwachung, Überprüfung, Instandhaltung und Verbesserung eines Informationssicherheitsmanagementsystems (ISMS) nach SN EN ISO/IEC 27001, 2013, Information technology – Security techniques – Information security management systems – Requirements[1] zu gewährleisten.

[1] Die aufgeführte Norm kann eingesehen und bezogen werden bei der Schweizerischen Normen-Vereinigung (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

[2] Die Wirksamkeit und Angemessenheit des ISMS ist durch Vorlage eines Zertifikats nach SN EN ISO/IEC 27001, 2013, nachzuweisen, das durch eine von der Schweizerischen Akkreditierungsstelle (SAS) akkreditierte Zertifizierungsstelle ausgestellt wurde. Das Dienstangebot der Zustellplattform muss im Geltungsbereich des zertifizierten ISMS liegen. Bis zum Ablauf der durch die SAS verabschiedeten Übergangsfrist wird auch ein nach SN EN ISO/IEC 27001, 2005, Information technology – Security techniques – Information security management systems – Requirements[2] ausgestelltes Zertifikat anerkannt.

[3] Wird eine neue Ausgabe der Norm ISO/IEC 27001 publiziert, muss spätestens nach Ablauf der Übergangsfrist eine gültige Zertifizierung des ISMS nach dieser neuen Ausgabe nachgewiesen werden. Das Dienstangebot der Zustellplattform muss aber weiterhin im Geltungsbereich des zertifizierten ISMS liegen.

4.2 Grundanforderungen für Behörden

[1] Ist die Dienstanbieterin eine Behörde, kann in begründeten Ausnahmefällen zwar nicht auf ein ISMS nach SN EN ISO/IEC 27001, 2013, aber auf eine formale Zertifizierung durch eine akkreditierte Zertifizierungsstelle verzichtet werden. In einem solchen Fall ist die Wirksamkeit und Angemessenheit des ISMS durch Vorlage eines Auditberichts zum formalen internen ISMS Audit gemäss Klausel 9.2 von SN EN ISO/IEC 27001, 2013, nachzuweisen. Der Auditbericht darf keine Befunde enthalten, die eine Zertifizierung ausschliessen. Bis zum Ablauf der durch die SAS verabschiedeten Übergangsfrist wird auch ein Auditbericht zum formalen internen ISMS Audit gemäss Klausel 6 von SN EN ISO/IEC 27001, 2005, anerkannt.

[2] Hinsichtlich der Prinzipien der Auditierung, der Durchführung des Audits sowie der Kompetenzen und Erfahrung der Auditorinnen und Auditoren gelten die Normen SN EN ISO/IEC 19011, 2011, Guidelines for auditing management systems[3] und SN EN ISO/IEC 27007, 2011, Information technology – Security techniques – Guidelines for information security management systems auditing[4]. Das Audit muss mindestens einmal pro Jahr wiederholt werden und die entsprechenden Auditberichte müssen dem BJ vorgelegt werden.

[3] Wird eine neue Ausgabe der Norm ISO/IEC 27001 publiziert, muss spätestens nach Ablauf der Übergangsfrist die Konformität des ISMS mit dieser neuen Ausgabe über den internen Auditbericht nachgewiesen werden. Das Dienstangebot der Zustellplattform muss aber weiterhin im Geltungsbereich dieses ISMS liegen.

4.3 Zusatzanforderungen für Privatunternehmen und Behörden

Die in den nachfolgenden Ziffern 4.3.1 bis 4.3.3 beschriebenen Anforderungen müssen bei der Risikobehandlung gemäss SN EN ISO/IEC 27005, 2011, berücksichtigt werden.

---

2 Die aufgeführte Norm kann eingesehen und bezogen werden bei der Schweizerischen Normen-Vereinigung (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

3 Die aufgeführte Norm kann eingesehen und bezogen werden bei der Schweizerischen Normen-Vereinigung (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

4 Die aufgeführte Norm kann eingesehen und bezogen werden bei der Schweizerischen Normen-Vereinigung (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

4.3.1 Management des Betriebs und der Kommunikation

[1] Das Management von Betrieb und Kommunikation der Zustellplattform hat sich am Stand der Technik zu orientieren, muss vollständig und nachvollziehbar beschrieben sein und ist periodisch zu überprüfen und anzupassen.

[2] Insbesondere müssen die folgenden Anforderungen erfüllt sein:

a. Entwicklungs-, Test- und Produktionsplattformen sind voneinander getrennt.

b. Das Netzwerk ist gemäss dem Ergebnis einer Risikobeurteilung segmentiert. Die Server für den Betrieb der Zustellplattform sind entsprechend ihrem Schutzbedarf über die Netzwerksegmente verteilt.

c. Elektronische Nachrichten werden ausschliesslich in verschlüsselter Form übermittelt und gespeichert. Eine End-zu-End Verschlüsselung ist nicht erforderlich.

d. Passwörter sind nicht unverschlüsselt gespeichert oder in Logfiles protokolliert.

e. Die eingesetzten kryptografischen Verfahren und Systeme haben dem Stand der Technik zu entsprechen und sich an der aktuellen Bedrohungslage zu orientieren. Es sind standardisierte Verfahren und Systeme einzusetzen, wie sie z.B. in der Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) der deutschen Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen[5] oder in vergleichbaren Standards aufgeführt sind. Abweichungen müssen sachlich begründet und in Bezug auf ihre Angemessenheit und Wirksamkeit geprüft sein. Bei proprietären Verfahren und Systemen ist Resistenz gegenüber bekannten kryptoanalytischen Angriffen nachzuweisen.

f. Die Zustellplattform ist so konzipiert, dass die eingesetzten kryptografischen Verfahren und Systeme und deren Schlüssellängen mit vertretbarem Aufwand ersetzt werden können.

g. Bei der Übertragung ist zur Verhinderung von offline „Password Guessing“-Angriffen eine Nachrichtenverschlüsselung mit nur von Passwörtern abgeleiteten Schlüsseln unzulässig.

h. Die Stärke der eingesetzten kryptografischen Verfahren und Systeme ist im Rahmen einer ganzheitlichen Sicherheitsarchitektur vollständig und nachvollziehbar beschrieben. Im Sinne eines fortlaufenden Verbesserungsprozesses müssen die kryptografischen Verfahren und Systeme periodisch überprüft und gegebenenfalls auch angepasst werden.

4.3.2 Zugriffssteuerung

[1] Die von der Zustellplattform verwendeten Massnahmen zur Zugriffssteuerung haben sich am Stand der Technik und an der aktuellen Bedrohungslage zu orientieren, müssen vollständig und nachvollziehbar beschrieben sein sowie periodisch überprüft und gegebenenfalls angepasst werden.

[2] Insbesondere müssen die folgenden Anforderungen erfüllt sein:

a. Der Zugriff auf elektronische Nachrichten in Übermittlung erfolgt über starke Authentifikationsverfahren (z.B. digitale Zertifikate oder persönliche Tokens). Die Authentifikationsinformation wird zum Schutz vor Abhorchungs- und Wiedereinspielungsangriffen nicht im Klartext übertragen.

b. Werden für die Authentifikation Passwörter eingesetzt, sind diese über verschlüsselte Verbindungen zu übertragen (z.B. im Rahmen einer Secure Sockets Layer [SSL] / Trans-

[5] Die Auflistung geeigneter Algorithmen und Parameter ist publiziert unter: www.bundesnetzagentur.de > Die Bundesnetzagentur > Qualifizierte elektronische Signatur > Aufgaben der Bundesnetzagentur / Veröffentlichungen > Festlegung geeigneter Algorithmen.

port Layer Security [TLS] Verbindung). Auf eine zeitliche Beschränkung der Gültigkeitsdauer von Passwörtern kann verzichtet werden. Sie haben in Bezug auf die Passwortstärke den gebräuchlichen und aktuellen Anforderungen zu entsprechen.

c. Passwort-Guessing und Trivialpasswörter sind mit geeigneten Massnahmen zu unterbinden. Zudem sind die Benutzerinnen und Benutzer auf die Stärke ihres Passworts hinzuweisen (Passwort-Meter; ein starkes Passwort umfasst mindestens 8 Stellen und ist zusammengesetzt aus mindestens drei der Elemente Grossbuchstaben, Kleinbuchstaben, Zahlen oder Sonderzeichen) sowie auf die Tatsache, dass das Passwort persönlich ist und nicht weitergegeben werden darf.

4.3.3 Beschaffung, Entwicklung und Instandhaltung von Plattformkomponenten

a. Server, die über das Internet erreichbar sind, sind bedarfsgerecht gehärtet. Best Practices, wie sie zum Beispiel das Center for Internet Security[6] mit den Security Configuration Benchmarks zur Verfügung stellt, sind berücksichtigt.

b. Bekannte Angriffe gegen Web-Anwendungen, wie sie zum Beispiel im Rahmen des Open Web Application Security Project[7] dokumentiert sind, werden erfolgreich abgewehrt.

4.4 Ausnahme für Behörden

Zustellplattformen, die unter der alleinigen Kontrolle einer Behörde stehen, dürfen elektronische Nachrichten unverschlüsselt speichern und an interne Systeme weiterleiten. Die Behörde hat das aus dieser technischen Schwachstelle resultierende Risiko für eine durchgängige Informationssicherheit auf der Basis einer Risikobeurteilung gemäss SN EN ISO/IEC 27001, 2013, mit angemessenen und wirksamen administrativen oder Führungsmassnahmen oder aber anderen technischen Massnahmen auf ein Restrisiko zu reduzieren, das mit den Risikoakzeptanzkriterien der Behörde konsistent ist.

6 www.cisecurity.org
7 www.owasp.org

5 Anforderungen an die Quittungen

5.1 Quittungsinhalt

Eine Quittung muss enthalten:

a. Informationen zur Quittung
   1. Name der die Quittung ausstellenden Zustellplattform,
   2. Angabe, ob es sich um eine Abgabe-, Abhol-, Verfall- oder Annahmeverweigerungsquittung handelt;

b. Informationen zur elektronischen Nachricht
   1. Information zur Absenderin oder zum Absender der Nachricht (Name, E-Mail-Adresse),
   2. Information zur Empfängerin oder zum Empfänger der Nachricht (Name, E-Mail-Adresse),
   3. Betreff-Feld (falls vorhanden),
   4. Zeitstempel;

c. Komponenten oder Informationen zu den einzelnen Komponenten der Nachricht (wenn die Nachricht nicht End-zu-End verschlüsselt ist)
   1. Name der Komponente (falls vorhanden),
   2. Typ und Format der Komponente,
   3. Grösse der Komponente in Bytes,
   4. Hashwert(e) der Komponente, wenn möglich gebildet mit zwei verschiedenen kryptografischen Hashfunktionen;

d. den Quittungszeitpunkt;

e. eine fortgeschrittene elektronische Signatur gemäss Bundesgesetz vom 19. Dezember 2003 über die elektronische Signatur (ZertES, SR 943.03).

5.2 Zeitquellen

a. Die elektronische Signatur der Quittung basiert auf einem Zertifikat einer gemäss ZertES anerkannten Anbieterin und ist mit einem entsprechenden Zeitstempel verbunden.

b. Der in der Quittung aufgeführte Zeitpunkt stammt von der Systemzeit der Zustellplattform derjenigen Dienstanbieterin, die abgabe- oder abholseitig an der Übermittlung beteiligt sind.

5.3 Definition der Zeitpunkte

Die Zeitpunkte werden wie folgt definiert:

a. Bei einer Eingabe an ein Gericht oder eine Behörde
   1. *Abgabezeitpunkt:* Zeitpunkt, in welchem die von der Absenderin oder dem Absender benutzte Zustellplattform bestätigt, dass der Uploadprozess für die Eingabe abgeschlossen wurde;

2. *Abholzeitpunkt:* Zeitpunkt, in welchem die von einem Gericht oder von der Behörde benutzte Zustellplattform bestätigt, dass der Abholprozess für die Eingabe abgeschlossen wurde.

b. Beim Versand von Vorladungen, Verfügungen, Entscheiden oder anderen Mitteilungen (Mitteilungen) durch ein Gericht oder eine Behörde
   1. *Abgabezeitpunkt:* Zeitpunkt, in welchem die vom Gericht oder von der Behörde benutzte Zustellplattform bestätigt, dass der Uploadprozess für die Mitteilung abgeschlossen wurde;
   2. *Übergabezeitpunkt:* Zeitpunkt, in welchem die von der Empfängerin oder vom Empfänger benutzte Plattform die Nachricht für den Versand aufbereitet und dem Versandprozess übergeben oder im Postfach des Empfängers oder der Empfängerin auf der Plattform für den Download zur Verfügung gestellt hat;
   3. *Abholzeitpunkt:* Wenn die Mitteilung bis spätestens am Ende der anwendbaren gesetzlichen Abholfrist abgeholt wird, beschreibt dies den Zeitpunkt, in welchem die von der Adressatin oder dem Adressaten benutzte Zustellplattform bestätigt, dass der Abholprozess für die Mitteilung abgeschlossen wurde;
   4. *Verfallen-Zeitpunkt:* Wenn die Mitteilung bis spätestens am Ende der anwendbaren gesetzlichen Abholfrist nicht abgeholt wird, gilt das Ende der Frist als Verfallen-Zeitpunkt;
   5. *Ablehnen-Zeitpunkt:* Zeitpunkt, in dem die Annahme der Mitteilung bis spätestens am Ende der anwendbaren gesetzlichen Frist verweigert wird.

5.4 Auszustellende Quittungen

[1] Die Zustellplattformen stellen folgende Quittungen aus:

a. Bei einer Eingabe an ein Gericht oder eine Behörde:
   1. Quittung mit dem Abgabezeitpunkt (Abgabequittung);
   2. Quittung mit dem Abholzeitpunkt (Abholquittung).

b. Bei der Zustellung von Mitteilungen durch ein Gericht oder eine Behörde:
   1. Quittung mit dem Abgabezeitpunkt (Abgabequittung);
   2. Quittung mit
      - dem Abholzeitpunkt, wenn die Mitteilung von der Adressatin oder dem Adressaten innerhalb der gesetzlichen Frist abgeholt wird (Abholquittung);
      - dem Verfallen-Zeitpunkt, wenn die Mitteilung von der Adressatin oder dem Adressaten innerhalb der gesetzlichen Frist nicht abgeholt wird (Verfallquittung); resp.
      - dem Ablehnen-Zeitpunkt, wenn die Annahme der Mitteilung von der Adressatin oder dem Adressaten innerhalb der gesetzlichen Frist verweigert wird (Annahmeverweigerungsquittung).

[2] Soll eine Plattform nur für die Übermittlung von Eingaben an Behörden anerkannt werden (Abgabeplattform), so braucht sie abweichend von Absatz 1 Buchstabe a nur die Abgabequittung auszustellen.

5.5 Herstellung und Versand der Quittungen

a. Die Quittung wird von der Zustellplattform als elektronisch signierte Datei im Format PDF hergestellt.

b. Der Zeitstempel in der Signatur der Quittung weicht nicht mehr als eine Minute von dem in der Quittung aufgeführten Zeitpunkt ab. Die Quittung wird spätestens eine Minute nach der Signaturanbringung bereitgestellt.
Diese Fristen bilden die Regel. Werden sie nicht eingehalten, sind die Abweichungen zu protokollieren, Abweichungen von mehr als 5 Minuten sind der Zulassungsbehörde am nächsten Werktag schriftlich zu melden.

c. Bei einer Eingabe an ein Gericht oder eine Behörde erhalten die Absenderin oder der Absender sowie das Gericht resp. die Behörde je die gleiche der in Ziffer 5.4 Absatz 1 Buchstabe a genannten Quittungen.
Die Absenderin oder der Absender kann gegenüber der von ihm resp. ihr benutzten Zustellplattform erklären, dass sie bei der Einreichung von Eingaben auf die Zusendung der Abholquittung resp. bei der Zustellung von Mitteilungen auf die Zusendung der Abgabequittung verzichtet.

d. Beim Versand von Mitteilungen durch ein Gericht oder eine Behörde erhalten das Gericht resp. die Behörde sowie die Adressatin oder der Adressat je die gleiche der in Ziffer 5.4 Absatz 1 Buchstabe b genannten Quittungen.
Ein Gericht oder eine Behörde kann gegenüber der von ihm resp. ihr benutzten Zustellplattform erklären, dass sie beim Empfang von Eingaben auf die Zusendung der Abholquittung resp. beim Versand von Mitteilungen auf die Zusendung der Abgabequittung verzichtet. Bei "Autoaccept" kann der Empfang ohne Zeitangabe bestätigt werden.

e. Richtet sich eine elektronische Nachricht gleichzeitig an mehrere Adressatinnen oder Adressaten, können mehrere Quittungszeitpunkte in einer Sammelquittung zusammengefasst sein. Der in der Sammelquittung aufgeführte Zeitpunkt ist identisch mit dem Abschluss der Zusammenfassung der Quittungszeitpunkte.

f. Die Quittungen werden den Empfängerinnen oder den Empfängern über die von ihnen benutzte Zustellplattform zugänglich gemacht.

g. Quittungen können unverschlüsselt übermittelt werden, sofern sie neben dem Quittungsinhalt gemäss Ziffer 5.1 keine weiteren Details des Inhalts der Eingabe resp. Mitteilung nennen.

h. Die Zustellplattformen dürfen die Quittungen auf Wunsch der an der Zustellung Beteiligten an jede von diesen bezeichnete Mailadresse versenden.

i. Der Dateiname der Quittung muss eine eindeutige Identifizierung der Quittung ermöglichen und kann im folgenden Format bezeichnet werden:
[YYMMDD]_[Message Identifier]_[Zustellplattform]_[Quittungsart].

6 Anforderungen an das IT Service Management

6.1 Grundanforderungen

[1] Für den zuverlässigen Betrieb der Zustellplattform muss nachgewiesen sein, dass die folgenden Betriebsprozesse dokumentiert, eingeführt, betrieben, permanent überwacht, periodisch geprüft, unterhalten und verbessert sind:

a. Servicebereitstellungsprozesse
   1. Management von Serviceniveaus,
   2. Service Berichtswesen,
   3. Servicekontinuitäts- und -verfügbarkeitsmanagement,
   4. Budgetierung und Verrechnung von IT Services,
   5. Kapazitätsmanagement,
   6. Informationssicherheitsmanagement;
b. Prozesse zum Beziehungsmanagement
   1. Pflege der Beziehung zwischen Leistungserbringer und Kunden,
   2. Lieferantenmanagement;
c. Lösungsprozesse
   1. Management von Vorfällen und Serviceanfragen,
   2. Management von Problemen;
d. Steuerungsprozesse
   1. Konfigurationsmanagement,
   2. Änderungsmanagement,
   3. Freigabe- und Bereitstellungsmanagement.

[2] Die Prozesse haben sich an den Normen SN EN ISO/IEC 20000-1, 2011, Information technology – Service management – Part 1: Service management system requirements[8] und SN EN ISO/IEC 20000-2, 2012, Information technology – Service management – Part 2: Guidance on the application of service management systems[9] oder an vergleichbaren Normen zu orientieren. Eine entsprechende Zertifizierung ist erwünscht, aber nicht erforderlich.

[3] Zusätzlich muss ein professioneller Service Desk eingeführt, betrieben, permanent überwacht, periodisch geprüft, unterhalten und verbessert sein.

6.2 Verfügbarkeit

[1] Grundsätzlich muss eine Zustellplattform an allen Tagen rund um die Uhr zur Verfügung stehen. Allfällige Servicefenster sind zwischen 00:15 Uhr und 07:00 Uhr nach Schweizer Zeit oder an Wochenenden zu planen. Sie sind auf der Zustellplattform mindestens 72 Stunden im Voraus zu veröffentlichen.

---

8 Die aufgeführte Norm kann eingesehen und bezogen werden bei der Schweizerischen Normen-Vereinigung (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

9 Die aufgeführte Norm kann eingesehen und bezogen werden bei der Schweizerischen Normen-Vereinigung (SNV), Bürglistrasse 29, 8400 Winterthur, www.snv.ch.

[2] Die Verfügbarkeit der Zustellplattform wird protokolliert und das Protokoll auf der Zustellplattform veröffentlicht.

6.3 Synchronisation der Systemzeit

Die Systemzeit der Zustellplattform ist mit einem Referenzzeitserver so zu synchronisieren, dass zu keinem Zeitpunkt die Systemzeit mehr als 5 Sekunden von der Zeit des Referenzzeitservers abweicht. Der Synchronisierungsmechanismus und die festgestellten Zeitdifferenzen sind zu protokollieren.

6.4 Grössen für elektronische Nachrichten

Die Zustellplattform muss elektronische Nachrichten mit einer Nutzgrösse von 15 MB und einer Transport-/Zustellgrösse von 25 MB verarbeiten können.

6.5 Informationen für Benutzerinnen und Benutzer

[1] Die Dienstanbieterin muss auf der Zustellplattform in einer für den technischen Laien verständlichen Form die wesentlichen Merkmale veröffentlichen:

a. der Architektur;
b. der Zugriffskontrollen;
c. der kryptografischen Verfahren und Systeme.

[2] Darüber hinaus ist darauf hinzuweisen, dass eine End-zu-End Verschlüsselung von elektronischen Nachrichten nicht zwingend erforderlich ist. Dazu ist gleichzeitig der folgende Hinweis zu veröffentlichen:
Eine unverschlüsselte Nachricht kann auf der Zustellplattform unverschlüsselt vorliegen und damit von der Dienstanbieterin oder von durch sie beauftragten Dritten eingesehen werden, selbst wenn dies untersagt ist. Benutzerinnen und Benutzer, die das Risiko einer Einsichtnahme nicht in Kauf nehmen können, müssen auf die Benutzung der Zustellplattform verzichten oder die Nachricht zusätzlich verschlüsseln (z.B. mit dem öffentlichen Signaturschlüssel der Empfängerin oder des Empfängers).

[3] Die Benutzerinnen und Benutzer der Zustellplattform sind über ihre Sorgfalts- und Mitwirkungspflichten sowie über die Tatsache aufzuklären, dass ihre Einträge im übergeordneten Teilnehmerverzeichnis (vgl. nachfolgend Ziffer 7) sichtbar sind. Sie sind auch auf die Stärke ihres Passworts hinzuweisen (vgl. Ziffer 4.3.2 Absatz 2 Buchstabe c) und auf die Tatsache, dass der Betreff der Nachricht sowie die Dateinamen allfälliger Anhänge nicht verschlüsselt übermittelt werden.

7 Anforderungen an das übergeordnete Teilnehmerverzeichnis

[1] Für die Vermittlung von elektronischen Nachrichten zwischen Zustellplattformen führt das BJ ein übergeordnetes, nicht öffentliches Teilnehmerverzeichnis. Auf das Verzeichnis darf nur über anerkannte Plattformen zugegriffen werden. Die Verwendung von Einträgen für Werbe- oder andere Marketingzwecke ist nicht zulässig.

[2] Das übergeordnete Teilnehmerverzeichnis muss die Teilnehmerverzeichnisse der Zustellplattformen als separate Unterbäume mit Schreibberechtigung zur Verfügung stellen. Der Wurzel dieser Unterbäume liegt eine Lightweight Directory Access Protocol (LDAP) Objektklasse mit folgenden Attributen zugrunde (weitere Attribute sind möglich, wie z.B. die Koordinaten eines Service Desks, allfällige Sicht- und Suchbarkeitspräferenzen, Grössenbeschränkungen für Nachrichten und Kommentare):

Name des Attributs	Bedeutung	Beispiele
Ou	Kanonischer Name der Zustellplattform.	ekomm, Incamail, Kanton Bern, PrivaSphere
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	X.509-Zertifikate für die öffentlichen Schlüssel, die von der Zustellplattform für S/MIME zur Signierung bzw. Ver- und Entschlüsselung verwendet werden (können auch identisch sein). Format: PKCS#7 SignedData	
smtpCertificate	X.509-Zertifikat für den öffentlichen Schlüssel, der vom MTA der Zustellplattform für die gesicherte Übertragung von Nachrichten an andere Zustellplattformen verwendet wird. Format: PKCS#7 Signed-Data.	

[3] Den Einträgen in den Unterbäumen des Verzeichnisses liegt die Objektklasse inet-OrgPerson gemäss RFC 2798 zugrunde. Die folgenden zwei Attribute sind zwingend erforderlich:

a. Mail (mail);
b. Distinguished Name (dn).

[4] Jede Teilnehmerin und jeder Teilnehmer muss über das Attribut Mail eindeutig identifizierbar sein. Typischerweise ist der Distinguished Name unter Verwendung des Attributs Mail aufgebaut.

[5] Jede Zustellplattform hat im übergeordneten Teilnehmerverzeichnis die Einträge der auf ihr registrierten Teilnehmerinnen und Teilnehmer zur Verfügung zu stellen und mindestens einmal pro Tag zu aktualisieren.

[6] Die Teilnehmerinnen und Teilnehmer sind von den Plattformbetreibern zu identifizieren. Dabei können insbesondere folgende Verfahren angewendet werden:

a. Persönliche Identifikation gemäss den Anforderungen von Artikel 5 der Verordnung vom 3. Dezember 2004 über die elektronische Signatur (VZertES, SR 943.032);
b. Identifikation mittels SuisseID;
c. Validierung der Wohnadresse mittels Brief;
d. Bestehende schriftliche Vertragsbeziehung zwischen der Teilnehmerin oder dem Teilnehmer und dem Plattformbetreiber;
e. Gruppenregistrierung (Bestätigung von Identitäten durch kantonale Anwaltsverbände oder registrierte und identifizierte Anwältinnen und Anwälte).

[7] Der Zugriff des übergeordneten Teilnehmerverzeichnisses auf die Teilnehmerverzeichnisse der Zustellplattformen, sowie der Zugriff der Zustellplattformen auf das übergeordnete Teilnehmerverzeichnis müssen gegenseitig stark authentifiziert sein. Idealerweise wird dazu LDAPS (LDAP over SSL) mit Zertifikaten einer gemäss ZertES anerkannten Zertifizierungsdienstanbieterin eingesetzt.

[8] Sofern eine Behörde ein Formular für an sie gerichtete Eingaben im Internet zur Verfügung stellt, ist im übergeordneten Teilnehmerverzeichnis auch die entsprechende URL für Formulareingaben aufzuführen.

8 Anforderungen an die Vermittlungsfunktionen zwischen Zustellplattformen

[1] Sind die Absenderin oder der Absender und die Empfängerin oder der Empfänger einer elektronischen Nachricht auf der gleichen Zustellplattform registriert, erfolgt die Übermittlung der Nachricht über diese Zustellplattform. Sind sie nicht auf der gleichen Zustellplattform registriert, muss die Nachricht zwischen Zustellplattformen vermittelt werden. In der Regel wird dabei eine Nachricht über zwei Plattformen vermittelt, eine Vermittlung über mehr als zwei Plattformen kann aber nicht ausgeschlossen werden.

[2] Im Folgenden bezeichnet A die Absenderin oder den Absender einer Nachricht, Z_A die Zustellplattform, auf der A registriert ist bzw. über die die Nachricht versandt wird, B bezeichnet die Empfängerin oder den Empfänger und Z_B die Zustellplattform, auf der B registriert ist ($Z_A \neq Z_B$). In der Regel sind Z_A und Z_B miteinander verbunden und können Nachrichten austauschen. Sind sie nicht verbunden, sind weitere Zustellplattformen in die Nachrichtenvermittlung einzubinden.

8.1 Grundlegende Anforderungen

[1] Die Vermittlungsfunktion zwischen Zustellplattformen muss kryptografisch abgesichert sein. Dabei erfolgt diese Absicherung auf zwei Schichten:

1. Auf der Transportschicht erfolgt eine Datenverschlüsselung gemäss RFC 3207 (Secure Simple Mail Transfer Protocol [SMTP] over TLS). Dazu muss jede Zustellplattform einen SMTP Mail Transfer Agent (MTA) betreiben, der Secure SMTP over TLS unterstützt. Die Adresse dieses MTA muss – zusammen mit einem X.509-Zertifikat smtpCertificate – im übergeordneten Teilnehmerverzeichnis veröffentlicht sein. Mit Hilfe der X.509-Zertifikate authentifizieren sich die MTA gegenseitig.
2. Auf der Anwendungsschicht erfolgt eine Nachrichtenverschlüsselung gemäss dem Secure Multipurpose Internet Mail Extensions (MIME) Standard (S/MIME), d.h. eine elektronische Nachricht wird von der absendenden Plattform mit dem privaten Signaturschlüssel signiert und mit dem öffentlichen Verschlüsselungsschlüssel der empfangenden Plattform verschlüsselt. Die entsprechenden X.509-Zertifikate smimeSignCertificate und smimeEncryptionCertificate müssen im übergeordneten Teilnehmerverzeichnis veröffentlicht sein.

[2] Demzufolge muss jede Plattform über drei Schlüsselpaare verfügen: Ein Schlüsselpaar für die Datenverschlüsselung auf der Transportschicht und zwei Schlüsselpaare für die Nachrichtensignierung und -verschlüsselung auf der Anwendungsschicht (in der Tabelle in Abschnitt 7 sind die entsprechenden Zertifikate als smtpCertificate, smimeSignCertificate und smimeEncryptionCertificate aufgeführt). In einer konkreten Implementierung kann ein Zertifikat auch für mehrere Zwecke eingesetzt werden.

[3] Die Datenverschlüsselung auf der Transportschicht wird im Folgenden nicht weiter betrachtet. Sie bedingt im Wesentlichen eine Konfiguration der MTA's zur Unterstützung von STARTTLS (Secure SMTP over TLS). Für die Nachrichtenverschlüsselung auf der Anwendungsschicht muss das im Folgenden beschriebene Vermittlungsprotokoll eingesetzt werden.

8.2 Vermittlungsprotokoll

[1] Nachfolgend wird der Fall einer Nachrichtenvermittlung über zwei Zustellplattformen Z_A und Z_B skizziert. Z_B muss eine Abholquittung ausgeben und den Übergabezeitpunkt protokollieren, Z_A eine Abgabequittung.

a. Die plattformübergreifende Nachrichtenvermittlung zwischen Z_A und Z_B wird folgendermassen abgewickelt:

   1. Z_A erhält die zu vermittelnde elektronische Nachricht, bestätigt sie mit einer Abgabequittung und verpackt sie in eine S/MIME-konforme Nachricht mit folgenden SMTP Headereinträgen:
      - To: Mail-Adresse von B;
      - From: Mail-Adresse von A;
      - Message-ID: Ein von Z_A bestimmter, plattformübergreifend eindeutiger Bezeichner (Identifier) für die Nachricht;
      - X-ZP-MsgType: Meldungstyp, wobei im Fall der Übermittlung einer elektronischen Nachricht «message» zu verwenden ist;
      - Abgabezeitpunkt resp. Abholzeitpunkt oder Verfallen-Zeitpunkt oder der Ablehnen-Zeitpunkt (vgl. dazu oben Ziffer 5.3; mit Angabe von Datum, Stunde und Minute) in Millisekunden seit 1.1.1970 ("X-ZP-IntakeTimeStampMillis", "X-ZP-ReceiveTimeStampMillis")[10], damit die Zeiten auch bei plattformübergreifenden Meldungen konsistent dargestellt werden[11];
      - Sender Platformname ("X-ZP-FromPlatform") enthaltend den eindeutigen „OU“ Eintrag der Plattform im übergeordneten Teilnehmerverzeichnis.

      Zusätzliche optionale Headereinträge sind möglich (z.B. für die lokale Zeit von Z_A oder ob es sich um eine Eingabe oder eine Mitteilung handelt[12]). Die eigentlich zu vermittelnde elektronische Nachricht stellt den Rumpfteil der S/MIME-konformen Nachricht dar.
   2. Z_A signiert die S/MIME-konforme Nachricht mit ihrem privaten Signierschlüssel und verschlüsselt das Resultat mit dem öffentlichen Verschlüsselungsschlüssel von Z_B.
   3. Die signierte und verschlüsselte Nachricht wird vom MTA von Z_A an den MTA von Z_B übertragen. Dazu wird die Datenverschlüsselung auf der Transportschicht (START-TLS bzw. Secure SMTP over TLS) genutzt. Allfällige Signaturen, die der Absicherung auf der Transportschicht dienen, müssen nicht weiter berücksichtigt werden. Anderenfalls – d.h. wenn die Nachricht nicht entgegengenommen werden oder nicht an den Empfänger ausgeliefert werden kann – muss A möglichst zeitnah darüber orientiert werden.
   4. Z_B entschlüsselt die so empfangene Nachricht, überprüft und entfernt die Signatur, protokolliert den Übergabezeitpunkt und übergibt diese Z_A. Gleichzeitig wird die Nachricht im Postfach von B abgelegt und kann von B abgerufen oder bei explizitem Einverständnis direkt empfangen werden.

---

10 Zur Vereinfachung des Handlings sollten dieselben Zeitpunkte in einem weiteren X-Header in menschenlesbarer Form angegeben werden.

11 Abgabe- oder Weitergabezeitpunkte der lokalen Plattform können insbes. auf dem WEB-GUI der Plattform (z.B. mit „mouseover“ oder „more info“-pop-up) dargestellt werden. Auf den ersten Blick für den Laien sind aber nur die plattformübergreifend koordinierten Zeitpunkte sichtbar.

12 Wenn beispielsweise Absenderin und Empfängerin je Behörden sind, ist es nicht automatisch klar, ob es sich um eine Eingabe oder ein Urteil bzw. eine Verfügung handelt. Um ein korrektes Funktionieren von „receipt-auto-delivered“ zu gewährleisten ist in diesem Fall der optionale Header "X ZP TypeOfCommunication" mit den Werten „ENQUIRY“ und „AUTHORITY_RESPONSE“ nützlich.

5. Die empfangende Plattform Z_B stellt sicher, dass von der Absenderin oder vom Absender signierte Meldungen gelesen werden können, wenn sie via Web-Schnittstellen empfangen werden.
6. Z_B akzeptiert die Meldung unabhängig vom Status des Absenders im übergeordneten Teilnehmerverzeichnis.

b. Nach Vermittlung an Z_B liegt die Nachricht im Zuständigkeitsbereich von Z_B. Wenn mit der Nachricht in der Folge etwas geschieht, obliegt es Z_B, Z_A darüber zu informieren. Dazu kann Z_B eine S/MIME-konforme Nachricht mit folgenden SMTP Headereinträgen konstruieren und an Z_A zurücksenden:
   1. To: Mail-Adresse von A.
   2. From: Mail-Adresse von B.
   3. Message-ID: Ein von Z_B bestimmter (wiederum plattformübergreifend eindeutiger) Bezeichner für die Nachricht.
   4. In-Reply-To: Der von Z_A vergebene Wert im Feld Message-ID.
   5. X-ZP-MsgType: einer der folgenden Meldungstypen:
      - receipt-deposited: Nachricht ist im Postfach von B abgelegt;
      - receipt-delivered: Nachricht ist von B abgeholt worden;
      - receipt-auto-delivered: Nachricht ist automatisch an B – z.B. eine Behörde – weitergeleitet worden. Z_B kann auf die Ausgabe einer Abholquittung verzichten;
      - receipt-timed-out: Die Zustellfrist für die Nachricht ist ungenutzt abgelaufen;
      - receipt-refused: Die Entgegennahme der Nachricht ist von B verweigert worden;
      - receipt-invalid-signature: Die Signatur der Nachricht ist ungültig;
      - receipt-error: Signatur-unabhängige generische Fehlermeldung;
      - confidential: Dieser Nachrichtentyp wird z.B. für die Abgabequittung verwendet, sofern diese über die andere Zustellplattform übermittelt wird.
        Um das Ziel grösstmöglicher Robustheit zu verfolgen, werden diese interoperablen Meldungen ohne den Einsatz des smimeEncryptionCertificate nur auf der Transportschicht zwingend geschützt (mandatory TLS).

c. Hat X-ZP-MsgType den Wert «receipt-delivered», muss der Rumpfteil der Nachricht die entsprechende Zustellquittung und allenfalls zusätzliche Informationen (z.B. in Form von zusätzlichen SMTP-Headereinträgen) enthalten. Hat X-ZP-MsgType den Wert «receipt-error», kann der Rumpfteil der Nachricht weiterführende Informationen zum aufgetretenen Fehler enthalten. Wurde der Header X-Zp-ERROR-To-User verwendet, wird dieser dem betroffenen Benutzer gezeigt. In diesem und allen anderen Fällen kann der Rumpfteil auch leer sein.

d. In jedem Fall signiert Z_B die Nachricht mit ihrem privaten Signierschlüssel und verschlüsselt das Resultat mit dem öffentlichen Verschlüsselungsschlüssel von Z_A. Die signierte und verschlüsselte Nachricht wird vom MTA von Z_B an den MTA von Z_A übertragen (wiederum über einen auf der Transportschicht mit Hilfe von Secure SMTP over TLS kryptografisch abgesicherten Kanal). Schliesslich entschlüsselt Z_A die Nachricht, überprüft und entfernt die Signatur und meldet die Ereignisse an A in geeigneter Form zurück bzw. übergibt diesem die Quittung.

[2] Support beim Versand an Behörden: Wenn die Absenderplattform nach 2 (Werk)Tagen feststellt, dass eine empfangende Behörde eine Eingabe noch nicht abgeholt hat, kann sie bei der Empfangsplattform ein Alert-Ticket eröffnen. Die Empfangsplattform stellt sicher, dass innerhalb der verbleibenden Frist bei der Support-Organisation der bei ihr unter Vertrag

stehenden Behörde ein Ticket eröffnet wird. Die Absenderplattform wird vor Ablauf der Frist von der Empfangsplattform über den Status informiert.

8.3 Nutzung von Vermittlungsfunktionen und Teilnehmerverzeichnissen

[1] Die Plattformen stellen einander die Vermittlungsfunktionen gemäss obigem Protokoll und die Angaben für das übergeordnete Teilnehmerverzeichnis kostenlos zur Verfügung.

[2] Für die Endbenutzerin und den Endbenutzer sind Wildcard-Suchen auf dem übergeordneten Verzeichnis erlaubt.