Policy

Policy E-Mail-Verschlüsselung

IT-Systemhaus

1. Policy

1.1. Unterstützte Standards

(1) Verschlüsselte Nachrichten werden innerhalb des Netzwerks der Bundesagentur für Arbeit über Microsoft Exchange ausgetauscht.

(2) Verschlüsselte E-Mails, welche an externe Kommunikationspartner gesendet werden, entsprechen dem S/MIME-Standard Version 3 nach RFC2633.

(3) Verschlüsselte E-Mails, welche an externe Kommunikationspartner gesendet werden, werden mit AES-256 Bit verschlüsselt.

(4) Es können nur verschlüsselte E-Mails nach dem S/MIME-Standard (RFC2633) empfangen werden. Hierbei muss die Nachricht als EnvelopedData verschickt werden.

(5) Es werden folgende Verschlüsselungsalgorithmen und Schlüssellängen unterstützt:

a. AES mit 256 Bit und 128 Bit Schlüssel

b. 3DES (mit CBC) mit 168 Bit Schlüssel

c. RC2 (mit CBC) mit 128 Bit und 40 Bit Schlüssel

d. RC4 mit 128 Bit mit 40 Bit Schlüssel

e. DES (mit CBC) mit 56 Bit und 40 Bit Schlüssel

(6) Es werden die folgenden Hash-Algorithmen unterstützt:

a. SHA2

b. SHA1

(7) Nachrichten, welche nicht dem Standard entsprechen, werden mit einer Fehlermeldung beantwortet.

(8) Verschlüsselte Nachrichten können nur im Format „Text“ oder „HTML“ versandt werden. BA ausgehende RTF-Nachrichten werden automatisch nach HTML konvertiert.

(9) Softwareprodukte, welche nicht den vorausgehend genannten Standards entsprechen (z.B. PGP, etc.), werden nicht unterstützt und können nicht für den verschlüsselten Austausch von E-Mail-Nachrichten genutzt werden.

1.2. Signieren von E-Mail-Nachrichten

(1) Signierte E-Mail-Nachrichten werden nicht unterstützt.
Eingehende signierte Nachrichten werden dem Empfänger zwar zugestellt, er kann jedoch nicht davon ausgehen, dass die Signatur erfolgreich geprüft werden kann.

(2) Das in der Nachricht enthaltene Signaturzertifikat des externen Kommunikationspartners kann nicht zur Verschlüsselung von Nachrichten genutzt werden. Derartige Nachrichten werden nicht zugestellt.

(3) Für ausgehende Nachrichten ist die Signaturfunktion deaktiviert.

1.3. Voraussetzungen für die Nutzung der E-Mail-Verschlüsselung

(4) Die E-Mail-Verschlüsselung ist nur für Nachrichten nutzbar, welche von oder an eine der folgenden E-Mail-Domänen gesendet werden:

a. arbeitsagentur.de

b. arge-sgb2.de

c. jobcenter-ge.de

d. iab.de

1.4. Zentrale Prüfung auf Schadprogramme

(1) Verschlüsselte E-Mails, welche an externe Kommunikationspartner adressiert sind, werden am zentralen Gateway automatisiert kurzzeitig entschlüsselt, um eine Prüfung auf Schadprogramme zu ermöglichen. Unmittelbar anschließend wird die E-Mail wieder per S/MIME verschlüsselt und an den externen Kommunikationspartner weitergeleitet.

(2) Die Prüfung von verschlüsselten E-Mail-Nachrichten unterliegt der gleichen Policy wie die Prüfung von unverschlüsselten E-Mails.

1.5. Adressbuch für externe Kommunikationspartner

(1) Das Zertifikat des externen Kommunikationspartners muss folgende Voraussetzungen erfüllen, um für die E-Mail-Verschlüsselung verwendbar zu sein:

a. Es muss dem X.509 V3 Standard entsprechen.

b. Es muss bereits gültig sein.

c. Es darf noch nicht abgelaufen sein.

d. Eine der im Zertifikat (SubjectAltName) eingetragenen E-Mail-Adressen muss mit der eingeladenen E-Mail-Adresse übereinstimmen.

e. Die (Erweiterte-)Schlüsselverwendung muss die Attribute „Schlüsselverschlüsselung“ und „Sichere E-Mail“ enthalten.

(2) Aufgrund der Verifikation der, vom externen Kommunikationspartner bereitgestellten Zertifikate, durch einen internen Nutzer, erfolgt keine über die in Punkt (1) dargestellten Voraussetzungen hinausgehende, Prüfung des Zertifikates.

(3) Jeder Eintrag im Adressbuch für externe Kommunikationspartner muss durch einen Nutzer mit korrekt freigeschalteter dDk/Gästekarte freigegeben werden.

(4) Einträge mit abgelaufenem Zertifikat werden automatisch nach 14 Tagen aus dem externen Adressbuch entfernt. Dies gilt auch für Einträge, welche ein Domänenzertifikat nutzen.

(5) Wird eine Einladung oder Änderung nicht innerhalb von 30 Tagen bearbeitet, so wird sie automatisch verworfen.

(6) Es können keine Einladungen an interne E-Mail-Adressen (Liste siehe 1.3 Abs. (4)) verschickt werden.

(7) Einladungen können, sofern es der betriebliche Ablauf erfordert, anonym Versandt werden. Hierbei wird als Absenderadresse noreply@arbeitsagentur.de verwendet.

1.6. Ablauf von Zertifikaten

(1) Interne Nutzer erhalten vor Ablauf ihrer Zertifikate eine neue dDk / Gästekarte.

(2) Externe Kommunikationspartner erhalten rechtzeitig, vor Ablauf der hochgeladenen Zertifikate, eine Benachrichtigung per E-Mail.

1.7. Nutzung von Vorbelegungen

(1) Für dedizierte E-Mail-Domänen können Felder der Eingabemaske vorbelegt werden. Zur Vorbelegung stehen die folgenden Felder zur Auswahl:

a. Firma

b. Organisationseinheit

c. Abteilung

d. Funktion

e. Telefon

f. Mobiltelefon

g. Straße/Hausnummer

h. Postleitzahl

i. Stadt

(2) Vorbelegungen können durch den externen Kommunikationspartner verändert werden, sofern dies nicht explizit deaktiviert wurde. Alle in (1) angegebenen Vorbelegungen können auf Anforderung vor Veränderungen durch den externen Kommunikationspartner geschützt werden.

(3) Vorbelegungen können bei OPS4 formlos über das Postfach „_BA-IT-Systemhaus-Zertifizierungsdienst“ beantragt werden.

a. Domänenname der Gegenstelle (Teil nach dem @-Zeichen der E-Mail-Adresse)

b. Ansprechpartner bei der Gegenstelle

c. Gewünschte Vorbelegung. Diese wird vor der Einrichtung noch mit dem Ansprechpartner der Gegenstelle abgestimmt.

(4) OPS4 prüft Anträge auf Vorbelegungen innerhalb von 10 Arbeitstagen und behält sich vor, diese unter Angabe geeigneter Gründe zurückzuweisen.

1.8. Nutzung von Domänenzertifikaten

(1) Für die verschlüsselte Kommunikation mit bestimmten E-Mail-Domänen können Domänenzertifikate genutzt werden. Diese erlauben es dasselbe Schlüsselmaterial für die gesamte, an diese E-Mail-Domäne gerichtete, Kommunikation zu verwenden.

(2) Es ist prinzipiell möglich, bei aktiviertem Domänenzertifikat, für einzelne E-Mail-Adressen einer Domäne ein vom Domänenzertifikate abweichendes Zertifikat zu nutzen. Ob dies erforderlich bzw. gewünscht ist, wird bei Antragstellung mit der Gegenstelle abgestimmt.

(3) Domänenzertifikate müssen den in Kapitel 1.5 Abschnitt (1) gemachten Vorgaben – mit Ausnahme (1)d – entsprechen.

(4) Die Nutzung eines Domänenzertifikates kann formlos per E-Mail über das Postfach „_BA-IT-Systemhaus-Zertifizierungsdienst“ beantragt werden. Hierbei sind folgende Informationen bereitzustellen:

a. Domänenname der Gegenstelle (Teil nach dem @-Zeichen der E-Mail-Adresse)

b. Technischer Ansprechpartner bei der Gegenstelle mit E-Mail-Adresse und Telefonnummer

c. Kurze Beschreibung der Kooperation

(5) OPS4 kontaktiert innerhalb von 10 Arbeitstagen den Ansprechpartner der Gegenstelle und prüft die technische Machbarkeit sowie die Sicherheitsimplikationen auf Seiten der BA. Der Antrag kann unter Angabe geeigneter Gründe zurückgewiesen werden.

(6) Für den Bereitsteller eines Domänenzertifikates gelten die Festlegungen im Dokument „Nutzung von Domänenzertifikaten“ [7]. Diese werden bei der ersten Kontaktaufnahme durch OPS4 übergeben.

(7) Es ist die Aufgabe der Gegenstelle Änderungen am Domänenzertifikat rechtzeitig (mind. 4 Wochen vorher) anzuzeigen.

(8) OPS4 überwacht das Ablaufen von Domänenzertifikaten und kontaktiert die Gegenstelle rechtzeitig bzgl. eines neuen Domänenzertifikates. Dies kann jedoch nur geschehen, wenn die Kontaktdaten der Gegenstelle noch aktuell sind. Es ist daher die Aufgabe der Gegenstelle oder des Antragstellers Änderungen an den Kontaktdaten laufend/rechtzeitig an OPS4 zu melden.

(9) Läuft ein Domänenzertifikat ab, ohne dass dafür ein Ersatz vorliegt, werden die davon abhängigen Zertifikate gemäß Kapitel 1.5 Abs. (4) gelöscht. Eine Aktualisierung des Domänenzertifikates aktualisiert automatisch alle Adressbucheinträge welche es verwenden. Ein Eingriff durch den externen Kommunikationspartner ist nicht notwendig.

(10) Parallel zu Domänenzertifikaten können auch Vorbelegungen nach Kapitel 1.7 genutzt werden.

1.9. Nutzung des LDAP-Servers für externe Kommunikationspartner

(1) Um externen Kommunikationspatnern das Einbinden der E-Mail-Verschlüsslung in automatisierte Verschlüsselungsgateways zu ermöglichen steht unter cert-download.arbeitsagentur.de ein LDAP-Server zur Verfügung, welcher die Zertifikate der Mitarbeiter und gruppenbezogenen Postfächer der Bundesagentur für Arbeit bereitstellt.

(2) Der Zugriff auf den LDAP-Server kann ausschließlich über LDAP v3 (RFC 2251) erfolgen. Für den Zugriff muss LDAP/s (LDAP über TLS) genutzt werden. Ausnahmen von dieser Regelung sind in begründeten Einzelfällen und nach Abwägung der Risiken möglich.

(3) Der Zugriff auf den LDAP-Server kann formlos per E-Mail über das Postfach „_BA-IT-Systemhaus-Vertrauensdienste“ beantragt werden. Hierbei sind folgende Informationen bereitzustellen:

a. Technischer Ansprechpartner bei der Gegenstelle mit E-Mail-Adresse und Telefonnummer

b. Kurze Beschreibung der Kooperation

(4) Die Nutzungsberechtigung für den LDAP-Server wird über Benutzername und Kennwort vergeben.

(5) OPS4 kontaktiert den Ansprechpartner der Gegenstelle und prüft die technische Machbarkeit sowie die Sicherheitsimplikationen auf Seiten der BA. Der Antrag kann unter Angabe geeigneter Gründe zurückgewiesen werden.

(6) Für den Nutzer des LDAP-Servers gelten die Festlegungen im Dokument „Nutzungsbedingungen LDAP-Verzeichnis E-Mail-Verschlüsselung“ [8]. Diese werden bei der ersten Kontaktaufnahme durch OPS4 übergeben.

(7) Es können beliebige LDAP-Anfragen an den Server gerichtet werden, sofern diese nur die Felder „sn“, „givenName“, „mail“ oder operationale Attribute (sofern verfügbar) abfragen. Andere Filterkriterien sind nicht möglich.

(8) Die Größe des Ergebnissatzes ist auf fünf Einträge begrenzt. Hierbei wird pro Empfänger nur der Eintrag zurückgeliefert, welcher das aktuelle Zertifikat besitzt.

(9) Die Abfrageergebnisse dürfen ausschließlich für die Verschlüsselung von E-Mail-Nachrichten genutzt werden, welche an die Bundesagentur für Arbeit versandt werden.

(10) Die Abfrageergebnisse dürfen nur innerhalb der Organisation genutzt werden, welche die Nutzung des LDAP-Verzeichnisses beantragt hat.