Vertrauensdiensteanbieter der Bundesagentur für Arbeit | 24.04.2020

E-Mail-Verschlüsselung für externe Kommunikationspartner

Version 2.8

IT-Systemhaus

Impressum

OPS4 - IT-Systemhaus
Vertrauensdiensteanbieter der Bundesagentur für Arbeit
Regensburger Straße 104
D-90478 Nürnberg

Inhaltsverzeichnis

1 Allgemeines

1.1 Warum sollte E-Mail-Verschlüsselung eingesetzt werden?

Die Verschlüsselung von E-Mails gewährleistet die Vertraulichkeit der übertragenen Daten. Sie stellt sicher, dass die übertragenen Daten tatsächlich nur von den dafür vorgesehenen Kommunikationspartnern eingesehen und gelesen werden können.

Um die unverschlüsselte E-Mail-Übertragung zu veranschaulichen, wird nachfolgend ein Vergleich mit einer normalen Postbeförderung dargestellt:

Eine unverschlüsselte E-Mail hat in etwa dieselben Sicherheitseigenschaften wie eine Postkarte. Diese ist auf dem Weg vom Absender bis zum Empfänger von jedermann lesbar.

Eine verschlüsselte E-Mail ist wie ein Brief in einer abgeschlossenen Transportbox. Nur wer den Schlüssel zum Öffnen der Transportbox besitzt, kann die Inhalte des Briefes lesen.

2 Voraussetzungen

2.1 Was benötige ich zur E-Mail-Verschlüsselung?

Sie benötigen ein E-Mail-Programm, dass die S/MIME basierte E-Mail-Verschlüsselung unterstützt (z.B. Microsoft Outlook, Mozilla Thunderbird, etc.).

Zur E-Mail-Verschlüsselung benötigen Sie zudem ein Zertifikat sowie den zugehörigen privaten Schlüssel für Ihre eigene E-Mail-Adresse.

2.2 Woher bekomme ich ein Zertifikat für meine E-Mail-Adresse?

Um verschlüsselte Nachrichten senden oder empfangen zu können, benötigen Sie selbst ein Zertifikat sowie das zugehörige Schlüsselmaterial. Dieses kann z. B. von einem Trustcenter (Vertrauensdiensteanbieter) ausgestellt werden.

Seitens der Bundesagentur für Arbeit können hierbei keine Empfehlungen für bestimmte Anbieter gegeben werden. Die Bundesagentur für Arbeit stellt **keine** Zertifikate zur Verschlüsselung für externe E-Mail-Adressen bereit.

3 Austausch verschlüsselter E-Mails

3.1 Wie erhalte ich das Zertifikat meines Ansprechpartners?

Die Zertifikate der E-Mail-Adressen der Bundesagentur für Arbeit können Sie von folgender Internetseite beziehen: https://cert-download.arbeitsagentur.de/

Bitte geben Sie hier in die Suche die **vollständige** E-Mail-Adresse ein, mit der Sie verschlüsselte E-Mails austauschen möchten. Klicken Sie anschließend auf die Schaltfläche **Zertifikat suchen**.

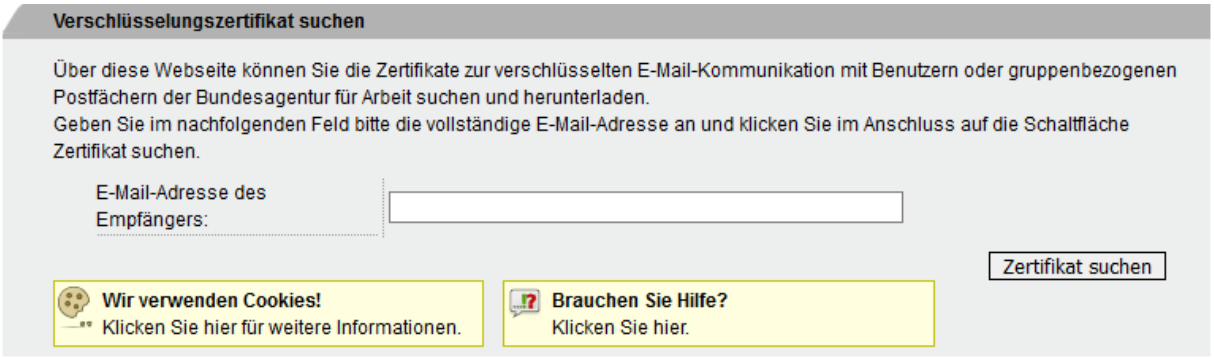

Abbildung 1 - Verschlüsselungszertifikat suchen

> ⚠ Falls Sie für eine bestimmte E-Mail-Adresse kein Ergebnis erhalten, wenden Sie sich bitte an Ihre Ansprechpartner in der Agentur für Arbeit oder dem Jobcenter.

Wenn die E-Mail-Adresse verschlüsselte E-Mails empfangen kann, können Sie im Anschluss das Zertifikat und die entsprechenden Ausstellerzertifikate in verschiedenen Formaten herunterladen:

Abbildung 2 - Ausstellerzertifikate

Hier können Sie das Zertifikat in verschiedenen Dateiformaten beziehen:

- Download des Zertifikats im .cer-Format,
- Download des Zertifikats als PKCS7-Struktur mit Ausstellerzertifikaten,
- Download als vCard-Datei VCF-Format (bspw. für Outlook geeignet),
- Download des Zertifikates und der Ausstellerzertifikate als ZIP-Datei.

3.2 Installation der Zertifikate in Outlook

3.2.1 Herunterladen der benötigten Dateien

Klicken Sie auf **Download der Daten als vCard-Datei** und speichern Sie die Datei ab.

Klicken Sie auf **Download der Ausstellerzertifikate als ZIP-Datei** und speichern Sie die Datei ab.

3.2.2 Importieren der Aussteller-/CA-Zertifikate

Öffnen Sie die ZIP-Datei und den darin befindlichen Eintrag **BA-Class-1-Root-CA-3.cer.**

Wählen Sie **Zertifikat installieren**. Klicken Sie auf **Weiter**, wählen Sie die Option **Alle Zertifikate in folgendem Speicher speichern** und drücken Sie auf **Durchsuchen**. Klicken Sie auf den Eintrag **vertrauenswürdige Stammzertifizierungsstellen** und bestätigen Sie mit OK.

Wählen Sie **Weiter**, **Fertigstellen** und **OK**.

Öffnen Sie nun den in der ZIP-Datei befindlichen Eintrag **BA-VPS-CA-3.cer** und wählen Sie **Zertifikat installieren**. Anschließend klicken Sie zweimal die Schaltfläche **Weiter** und dann **Fertigstellen**.

⚠ Sie benötigen die Zertifikate **BA-VPS-CA-3.cer** und **BA-Class-1-Root-CA-3.cer** auf Ihrem PC! Wenn diese nicht vorhanden sind, führen Sie alle Schritte bitte durch.

3.2.3 Importieren des Kontaktes und Versand einer verschlüsselten E-Mail

Öffnen Sie die heruntergeladene vCard-Datei (.vcf) mit einem Doppelklick. Es werden diverse Felder vorbelegt, wie der Name und die E-Mail-Adresse des Zertifikatsinhabers. Wählen Sie die Schaltfläche **Speichern und Schließen** im Kontakt aus. Nun haben Sie den Kontakt samt seinem Zertifikat angelegt.

Um eine verschlüsselte E-Mail zu versenden, erstellen Sie eine neue E-Mail und wählen Sie als **Empfänger** den soeben gespeicherten **Kontakt** aus. Aktivieren Sie über **Optionen** die Schaltfläche **Nachricht verschlüsseln**. Vervollständigen Sie Ihre E-Mail und senden Sie diese ab.

Falls Sie an andere E-Mail-Adressen der Bundesagentur für Arbeit, des IAB oder der Jobcenter verschlüsselte E-Mails senden möchten, laden Sie die entsprechenden vCard-Dateien - wie ab Kapitel 3.1 beschrieben - herunter und speichern Sie die Kontakte in Outlook ab.

3.3 Empfangen von verschlüsselten E-Mails

Damit Ihnen Ihr Ansprechpartner bei der Bundesagentur für Arbeit verschlüsselte E-Mails senden kann, wird Ihr eigenes Zertifikat benötigt. Bitten Sie Ihren Ansprechpartner Ihnen eine Einladung zur E-Mail-Verschlüsselung zukommen zu lassen. Die Einladung wird Ihnen per E-Mail zugeschickt:

Betreff: Einladung für E-Mail-Verschlüsselung

Guten Tag,

ein Mitarbeiter der Bundesagentur für Arbeit möchte mit Ihnen verschlüsselte E-Mails austauschen. Um dies zu ermöglichen, müssen Sie Ihr Zertifikat, welches Sie für verschlüsselte Emails nutzen, der Bundesagentur für Arbeit zur Verfügung stellen.

Um diesen Vorgang für Sie so einfach wie möglich zu gestalten, steht Ihnen eine Webseite zur Erfassung Ihrer Daten und zum Upload Ihres Zertifikates zur Verfügung. Bitte nutzen Sie den nachfolgenden Link um auf diese Webseite zu gelangen:

<Link zur Erfassung und Änderung der Kontaktdaten>

Bitte speichern Sie diese E-Mail ab. Der Link kann verwendet werden um die von Ihnen eingetragenen Informationen für Ihre E-Mail-Adresse < E-Mail-Adresse> nachträglich zu verändern!

Mit der Nutzung unserer Webseite erklären Sie sich mit unseren Nutzungsbedingungen (https://cert-upload.arbeitsagentur.de/staticpages/page/usage) einverstanden.

Abbildung 3 - E-Mail Benachrichtigung: "Einladung für E-Mail-Verschlüsselung"

Die Einladung enthält einen Link, der Sie zu einer Webseite weiterleitet, auf der Sie Ihre persönlichen Daten eingeben und Ihr eigenes Zertifikat hochladen können. **Bitte bewahren Sie diese E-Mail auf**.

3.4 Kontaktdaten erfassen und Zertifikat hochladen

Mit Klick auf den Link in der Einladungs-E-Mail erhalten Sie auf einer Webseite die Möglichkeit Ihre Kontaktdaten zu erfassen und Ihr eigenes Zertifikat hochzuladen:

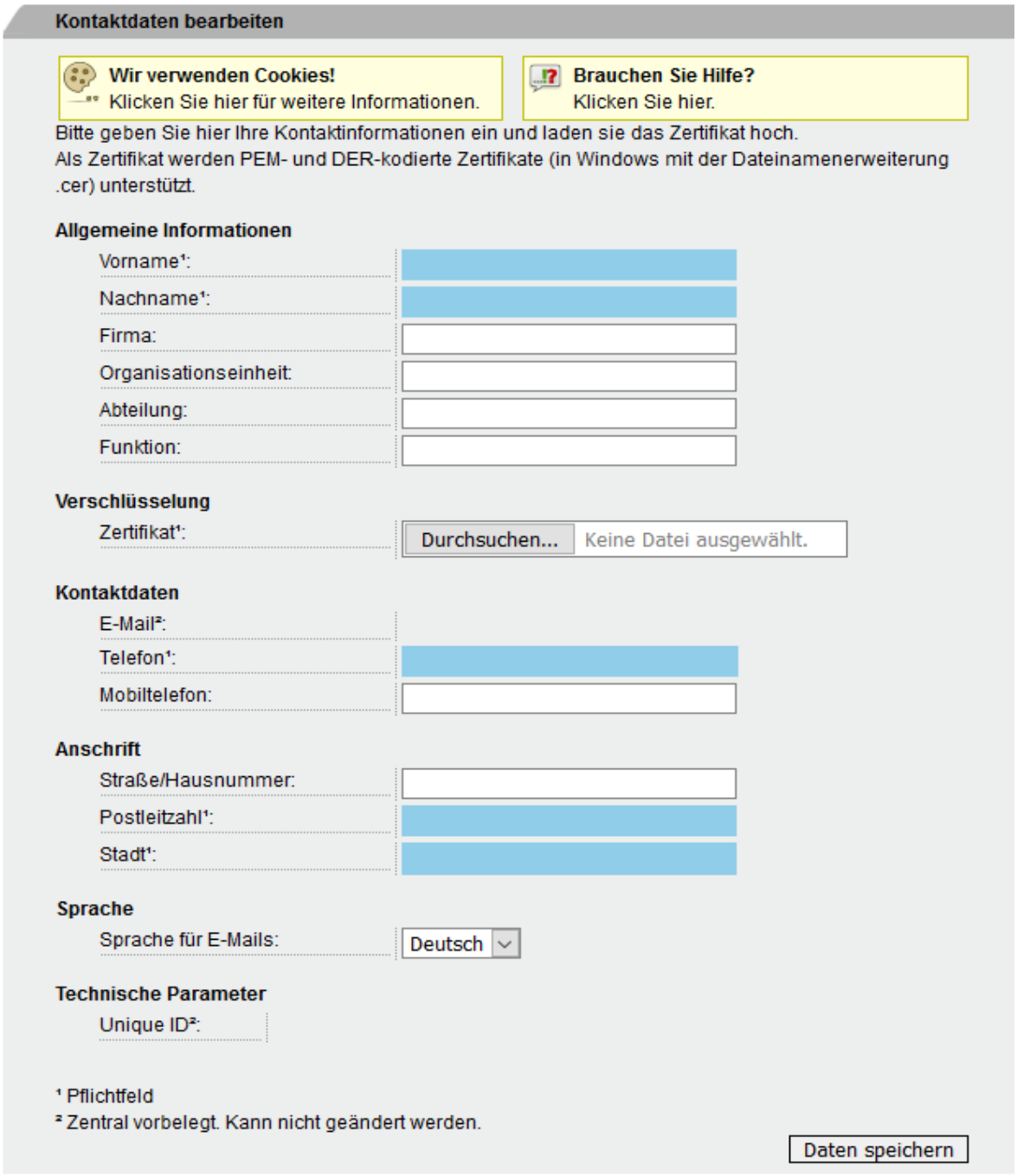

Abbildung 4 - Kontaktdaten bearbeiten

Füllen Sie mindestens die Felder **Vorname**, **Nachname**, **Telefon**, **Postleitzahl** und **Stadt** aus und klicken Sie auf die Schaltfläche **Durchsuchen ...**

Wählen Sie Ihr **Zertifikat** mit der Dateiendung **.cer** aus. Wenn Ihnen dieses Format nicht vorliegt, exportieren Sie Ihr Zertifikat zunächst (siehe Kapitel 4.1, 4.2).

Klicken Sie auf die Schaltfläche **Daten speichern** und im Anschluss **Bestätigen,** um den Einladungsprozess abzuschließen und Ihren Kontakt zur Freigabe einzureichen. Bis die Daten von Ihrem Ansprechpartner freigegeben worden sind, können Sie diese nicht mehr bearbeiten.

Sobald die Freigabe Ihres Kontakts erfolgt ist, können **alle** Mitarbeiterinnen und Mitarbeiter der BA und der Jobcenter **an Sie verschlüsselte E-Mails** senden.

4 Häufig gestellte Fragen & Fehlerbehebung

4.1 Importieren Ihrer .p12- oder .pfx-Datei

Falls Ihnen nur eine .p12 oder .pfx-Datei (Ihr persönliches Schlüsselmaterial) vorliegt, müssen Sie diese zunächst auf Ihrem PC installieren. Folgen Sie dazu bitte dem Zertifikatsimport-Assistent. Der Zertifikatsimportassistent wird gestartet sobald Sie die .p12 oder .pfx Datei öffnen. Geben Sie während des Importvorgangs Ihr Kennwort für diese Datei ein.

4.2 Exportieren Ihres Zertifikats als .cer Datei

Sobald Sie Ihr persönliches Schlüsselmaterial (.p12 oder .pfx-Datei) in Windows importiert haben, müssen Sie Ihr Zertifikat als .cer-Datei exportieren. Öffnen Sie den Internet Explorer und klicken Sie auf **Extras.**

Klicken Sie auf **Internetoptionen** → Wechseln Sie zur Registerkarte **Inhalte** und klicken Sie auf die Schaltfläche **Zertifikate.**

Öffnen Sie unter **Eigene Zertifikate** den bestehenden Eintrag mit einem Doppelklick.

Wechseln Sie zur Registerkarte **Details** → Wählen Sie die Schaltfläche **In Datei kopieren....**

Klicken Sie **Weiter** → **Weiter** → Legen Sie über **Durchsuchen...** den Speicherort für Ihr Zertifikat fest.

> ⚠ Bitte merken Sie sich den Speicherort, dieser wird für die Bearbeitung der Einladung zur E-Mail-Verschlüsselung wieder benötigt.

Klicken Sie **Weiter** und im Anschluss **Fertigstellen**.

4.3 Outlook Fehlermeldung: Verschlüsselungsprobleme

Sie erhalten in Outlook die Fehlermeldung “Verschlüsselungsprobleme“.

Die Fehlermeldung bedeutet, dass Ihr Outlook Probleme mit dem Zertifikat des Empfängers festgestellt hat. Bitte führen Sie die Schritte im Kapitel 3.2 inkl. der Unterkapitel nochmals genau aus. Meistens wird der Schritt 3.2.2 Importieren der CA-Zertifikate falsch durchgeführt.

5 Informationen für technische IT-Services

5.1 Nutzung der eigenen PKI-Infrastruktur

Falls Sie ein eigenes Trustcenter bzw. eine eigene PKI-Infrastruktur betreiben, können diese Zertifikate ebenfalls verwendet werden, wenn Sie die folgenden Voraussetzungen erfüllen:

- Erstellung des Zertifikats gem. X.509 V3 Standard.
- Die im Zertifikat (SubjectAltName) eingetragene E-Mail-Adresse muss mit Ihrer E-Mail-Adresse übereinstimmen (mindestens ein Klasse 1 Zertifikat).
- Die (Erweiterte-)Schlüsselverwendung muss…

  für RSA-Zertifikate mindestens die Attribute „Schlüsselverschlüsselung“ und/oder „Sichere E-Mail“ enthalten.

  für ECC-Zertifikate mindestens die Attribute „Schlüsselvereinbarung“ und „Sichere E-Mail“ enthalten.
- Das Zertifikat muss gültig sein.

5.2 Einsatz von Verschlüsselungsgateways und Sonderkonfigurationen

⚠ Falls Sie ein **Verschlüsselungsgateway (oder auch virtuelle Poststelle genannt) einsetzen, bieten wir Ihnen folgende** technischen Lösungsmöglichkeiten an:

Versand verschlüsselter Nachrichten von der Bundesagentur für Arbeit → zu externen Kommunikationspartnern

Die Bundesagentur für Arbeit nutzt zur Bereitstellung und Verwaltung von Zertifikaten zum Austausch verschlüsselter E-Mails das System **Adressbuch für externe Kontakte**.

Der Prozessablauf gliedert sich in folgende Schritte:

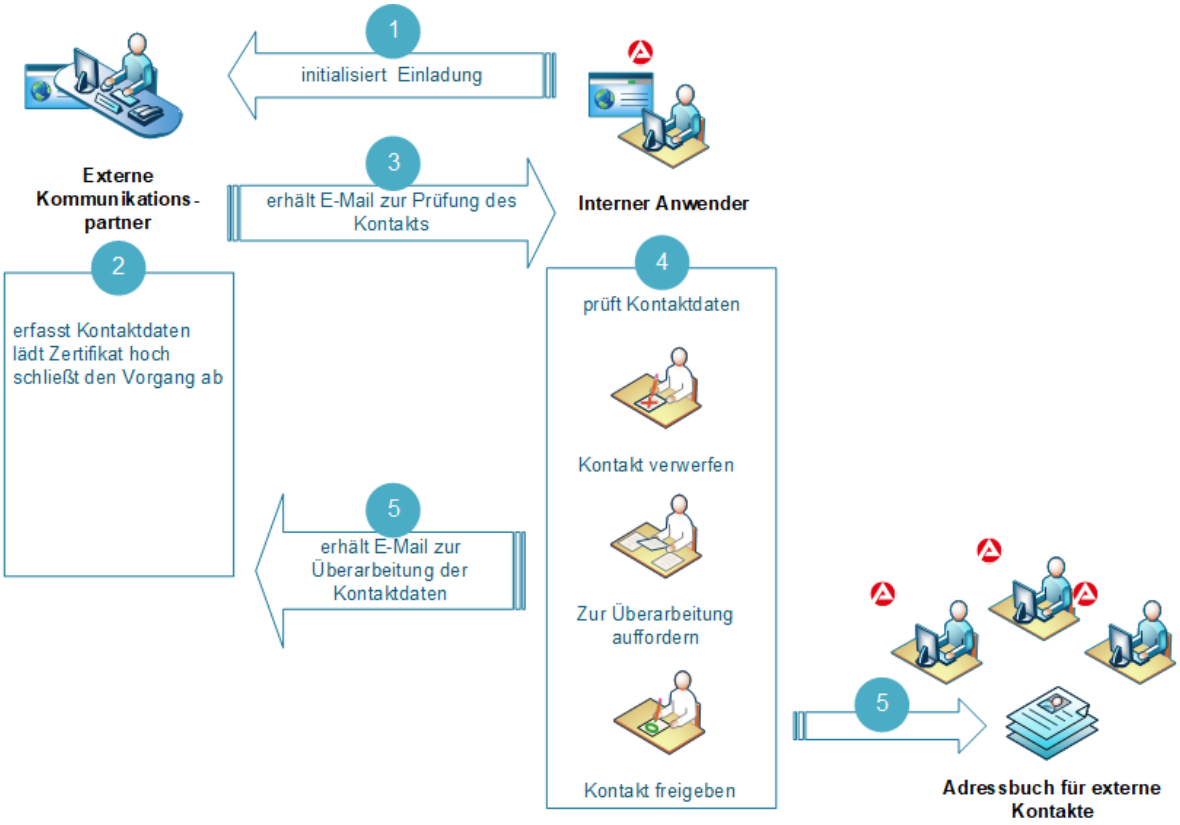

Abbildung 5 - Prozessablauf

1. Interner initialisiert die Einladung
2. Datenerfassung & Upload des Zertifikats

   → **Eigenständig durch den eingeladenen externen Kommunikationspartner**

   Der externe Kommunikationspartner erfasst seine Kontaktdaten, lädt sein *persönliches Zertifikat* zur Verschlüsselung von E-Mails hoch und schließt den Vorgang ab (siehe auch 3.4).

   → **Stellvertretende Bearbeitung aller Einladungen über eine administrative E-Mail-Adresse:**

   Wenn Sie als IT-Dienstleister alle Einladungen für Ihre E-Mail-Domäne erhalten und die Zertifikate und Kontaktdaten pflegen möchten, kann eine von Ihnen benannte E-Mail-Adresse als administrative E-Mail-Adresse eingerichtet werden. Bitte wenden Sie sich dazu an das Postfach IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de

   → **Alternative Domänenzertifikat (Verschlüsselungsgateway):**

   Sollte Ihr Verschlüsselungsgateway ein Domänenzertifikat (Domain-Key) nutzen, ist es ebenfalls möglich dieses für die gesamte E-Mail-Domäne in unserem Adressbuch für externe Kontakte vorzubelegen. Hierdurch ergibt sich der Vorteil, dass nicht alle Nutzer ein persönliches Zertifikat im Rahmen des Einladungsprozesses selbst hochladen müssen. Der Einladungsprozess muss jedoch dennoch durchgeführt werden.

⚠ Die Funktion Domänenzertifikat muss durch Ihr Verschlüsselungsgateway unterstützt werden.

   Gerne senden wir Ihnen die Informationen zur Bereitstellung eines Domänenzertifikats zu. Bitte wenden Sie sich dazu an das Postfach IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de.

   → **Alternative LDAP-Verzeichnis:**

   Es ist ebenfalls möglich, die Zertifikate Ihrer E-Mail-Adressen von Ihrem LDAP-Verzeichnisdienst automatisch abzurufen. Die benötigten Zertifikate werden beim Versand der Einladung abgerufen und im Adressbuch für externe Kontakte hinterlegt.

Bitte senden Sie uns die Verbindungsdaten zu Ihrem LDAP-Verzeichnisdienst an das Postfach IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de.

3. Interner erhält eine E-Mail zur Freigabe des Kontakts
4. Interner prüft die Kontaktdaten
5. Kontaktdaten werden vom Internen freigegeben, zur Überarbeitung zurückgewiesen oder verworfen.

Sobald der externe Kontakt freigegeben wurde, steht er für alle Internen im Adressbuch für externe Kontakte zur Verfügung.

Versand verschlüsselter Nachrichten von externen Kommunikationspartnern → zur Bundesagentur für Arbeit

a) manueller Bezug der Verschlüsselungszertifikate der Bundesagentur für Arbeit

siehe Kapitel 3.1

b) automatisierter Bezug der Verschlüsselungszertifikate der Bundesagentur für Arbeit

Um den Versand von verschlüsselten Nachrichten mit einem Verschlüsselungsgateway (ggf. auch virtuelle Poststelle genannt) zur Bundesagentur für Arbeit zu realisieren, bieten wir Ihnen die Möglichkeit, einen Zugriff zu unserem LDAP-Verzeichnisdienst einzurichten. Häufig bieten Verschlüsselungsgateways die Möglichkeit, Zertifikate für bestimmte E-Mail-Domänen von einem LDAP-Verzeichnisdienst abzurufen, um eine automatisierte Verschlüsselung von E-Mails durchzuführen. Gerne senden wir Ihnen die Informationen zur Beantragung des Zugriffs auf den LDAP-Verzeichnisdienst sowie die Nutzungsbedingungen zu.

Bitte wenden Sie sich dazu an das E-Mail-Postfach

IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de.

Die Bundesagentur für Arbeit stellt für alle E-Mail-Adressen persönliche Zertifikate aus. Ein Domänenzertifikat für die E-Mail-Domänen der Bundesagentur für Arbeit wird **nicht** zur Verfügung gestellt.

Abbildungsverzeichnis