

Vertrauensdiensteanbieter der Bundesagentur für Arbeit | 05.09.2024

E-Mail-Verschlüsselung für externe Kommunikationspartner



Dokumenteninformation

Autor: Vertrauensdiensteanbieter der Bundesagentur für Arbeit
Regensburger Straße 104
D-90478 Nürnberg

Dokumenten-ID: PKI.810.501.1

Datum: 05.09.2024


Tabelle 1 – Dokumenteninformation

Impressum

Z24 - IT-Systemhaus
Vertrauensdiensteanbieter der Bundesagentur für Arbeit
Regensburger Straße 104
D-90478 Nürnberg

Inhaltsverzeichnis

Dokumenteninformation	2
Inhaltsverzeichnis	3
1	Allgemeines.....5
1.1	Warum sollte E-Mail-Verschlüsselung eingesetzt werden?.....5
2	Voraussetzungen.....6
2.1	Was benötige ich zur E-Mail-Verschlüsselung?.....6
2.2	Woher bekomme ich ein Zertifikat für meine E-Mail-Adresse?.....6
3	Austausch verschlüsselter E-Mails.....7
3.1	Wie erhalte ich das Zertifikat meines Ansprechpartners?.....7
3.2	Einrichtung der Zertifikate in Outlook.....8
3.2.1	Herunterladen der benötigten Dateien.....8
3.2.2	Importieren der CA-Zertifikate.....8
3.2.3	Importieren des Kontaktes und Versand einer verschlüsselten E-Mail.....9
3.3	Empfangen von verschlüsselten E-Mails.....9
3.4	Kontaktdaten erfassen und Zertifikat hochladen.....9
4	Hilfe zur Fehlerbehebung.....11
4.1	Importieren Ihrer P12- oder PFX-Datei.....11
4.2	Exportieren Ihres Zertifikats als CER-Datei.....11
4.3	Outlook Fehlermeldung: Verschlüsselungsprobleme.....11
5	Informationen für technische IT-Services.....12
5.1	Wechsel der Zertifikatskette der E-Mail-Verschlüsselung.....12
5.2	Nutzung der eigenen PKI-Infrastruktur.....12
5.3	Validierung der Aussteller-/CA-Zertifikate der BA.....12
5.4	Unterstützte Standards.....12
5.5	S/MIME Signatur.....13
5.6	News für technische Ansprechpartner.....13
5.7	Versand verschlüsselter Nachrichten von der Bundesagentur für Arbeit → zu externen Kommunikationspartnern.....13
5.7.1	Möglichkeiten zur Bereitstellung Ihrer Zertifikate und Daten im Rahmen des Einladungsprozesses.....15
5.7.2	Eigenständig durch den eingeladenen externen Kommunikationspartner.....15
5.7.3	Stellvertretende Bearbeitung aller Einladungen durch eine administrative E-Mail- Adresse.....15
5.7.4	Domänenzertifikat (Verschlüsselungsgateway).....16
5.7.5	LDAP-Verzeichnis.....17
5.8	Versand verschlüsselter Nachrichten von externen Kommunikationspartnern → zur Bundesagentur für Arbeit.....18
5.8.1	Manueller Abruf der Verschlüsselungszertifikate der Bundesagentur für Arbeit....18
5.8.2	Automatisierter Abruf der Verschlüsselungszertifikate der Bundesagentur für Arbeit per LDAP.....18



5.8.3	Domänenzertifikat der Bundesagentur für Arbeit	18
	Abbildungsverzeichnis	19
	Tabellenverzeichnis.....	20

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. 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.

2 Voraussetzungen

2.1 Was benötige ich zur E-Mail-Verschlüsselung?

- Sie benötigen ein E-Mail-Programm, welches S/MIME Verschlüsselung unterstützt z.B. Microsoft Outlook, Mozilla Thunderbird, etc.
- Zur E-Mail-Verschlüsselung benötigen Sie ein Zertifikat und den zugehörigen privaten Schlüssel für Ihre eigene E-Mail-Adresse.

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

Um verschlüsselte E-Mails senden und empfangen zu können, benötigen Sie für Ihre E-Mail-Adresse ein Zertifikat und den zugehörigen privaten Schlüssel. 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.

Ihr Verschlüsselungszertifikat muss folgende Voraussetzungen erfüllen:

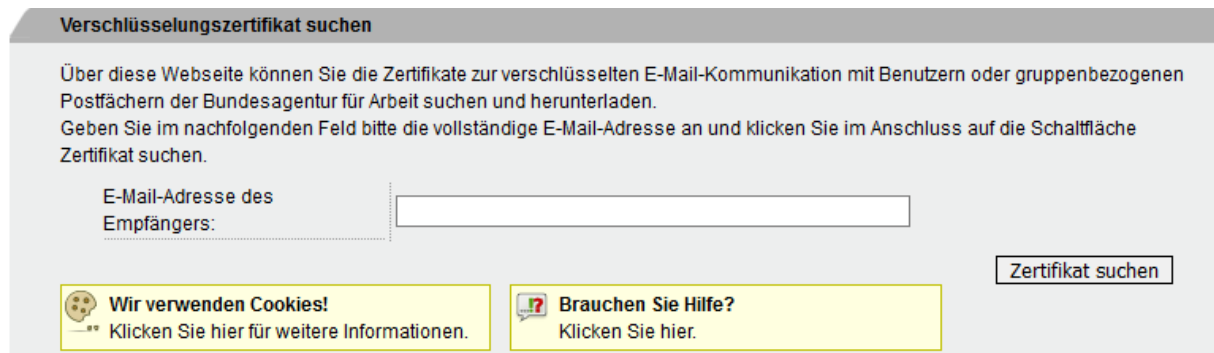
- Erstellung des Zertifikats gem. X.509 V3 Standard.
- Die im Zertifikat (SubjectAltName) eingetragene E-Mail-Adresse muss mit Ihrer E-Mail-Adresse übereinstimmen (mindestens ein Klasse 1 Zertifikat).
- Die (Erweiterte-)Schlüsselverwendung muss...
 - für RSA-Zertifikate mindestens die Attribute „Schlüsselverschlüsselung“ und/oder „Sichere E-Mail“ enthalten.
 - für ECC-Zertifikate mindestens die Attribute „Schlüsselvereinbarung“ und „Sichere E-Mail“ enthalten.
- Das Zertifikat muss gültig sein.
- Die Gesamtlauzeit des Zertifikats darf 5 Jahre nicht übersteigen. (gem. BSI TR-02102-1)
- Die Schlüssellänge von RSA-Schlüsseln muss mindestens 2048 Bit betragen.

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**.

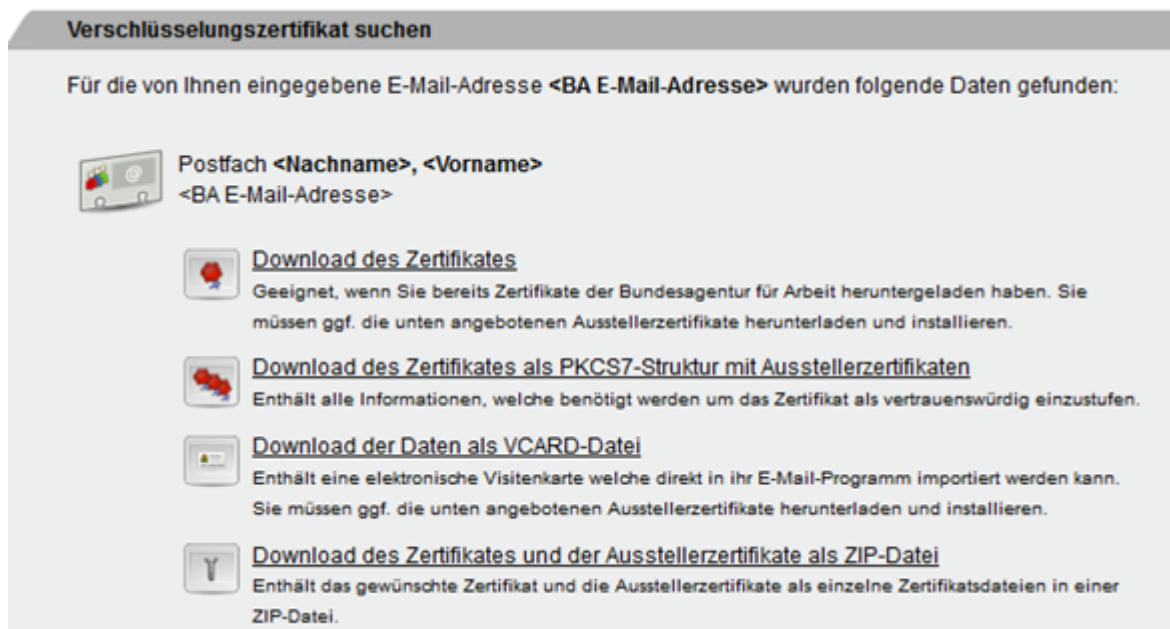


The screenshot shows a search form titled 'Verschlüsselungszertifikat suchen'. It contains a text input field for the email address of the recipient, with the label 'E-Mail-Adresse des Empfängers:'. To the right of the input field is a button labeled 'Zertifikat suchen'. Below the input field, there are two yellow boxes: one with a cookie icon and the text 'Wir verwenden Cookies! Klicken Sie hier für weitere Informationen.', and another with a question mark icon and the text 'Brauchen Sie Hilfe? Klicken Sie hier.'

Abbildung 1 - Verschlüsselungszertifikat suchen

 Falls Sie für eine bestimmte E-Mail-Adresse kein Ergebnis erhalten, wenden Sie sich bitte an Ihren zuständigen Ansprechpartner in der Agentur für Arbeit oder dem Jobcenter. Ggf. ist die E-Mail-Adresse falsch oder die Verschlüsselung ist noch nicht aktiviert.

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



The screenshot shows the search results for a certificate. It starts with the text 'Für die von Ihnen eingegebene E-Mail-Adresse <BA E-Mail-Adresse> wurden folgende Daten gefunden:'. Below this, there is a list of search results for a mailbox. The first result is 'Postfach <Nachname>, <Vorname> <BA E-Mail-Adresse>'. Underneath this, there are four download options, each with a small icon and a description:

- Download des Zertifikates**: Geeignet, wenn Sie bereits Zertifikate der Bundesagentur für Arbeit heruntergeladen haben. Sie müssen ggf. die unten angebotenen Ausstellerzertifikate herunterladen und installieren.
- Download des Zertifikates als PKCS7-Struktur mit Ausstellerzertifikaten**: Enthält alle Informationen, welche benötigt werden um das Zertifikat als vertrauenswürdig einzustufen.
- Download der Daten als VCARD-Datei**: Enthält eine elektronische Visitenkarte welche direkt in ihr E-Mail-Programm importiert werden kann. Sie müssen ggf. die unten angebotenen Ausstellerzertifikate herunterladen und installieren.
- Download des Zertifikates und der Ausstellerzertifikate als ZIP-Datei**: Enthält das gewünschte Zertifikat und die Ausstellerzertifikate als einzelne Zertifikatsdateien in einer ZIP-Datei.

Abbildung 2 – Suchergebnis Zertifikate

Die Zertifikate der Bundesagentur für Arbeit können ebenfalls über <https://openkeys.de/> oder <https://www.globaltrustpoint.com/> sowie deren LDAP-Schnittstellen abgefragt werden. Jedoch können Abfragelimits oder andere Einschränkungen gelten. Bitte informieren Sie sich dazu beim jeweiligen Anbieter.

3.2 Einrichtung 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.

Wechseln Sie auf die Webseite: <https://www.pki.arbeitsagentur.de/cacerts/emv/ssl-client-smartcard/>

Klicken Sie oben links auf **Alle Zertifikate als ZIP-Datei** und speichern Sie die Datei ab.

3.2.2 Importieren der CA-Zertifikate

1. Öffnen Sie die soeben heruntergeladene ZIP-Datei
2. Wechseln Sie in den Ordner **der**
3. Öffnen Sie die Datei

CN_BA-Class-1-Root-CA-3_PN_O_Bundesagentur_fuer_Arbeit_C_DE.crt

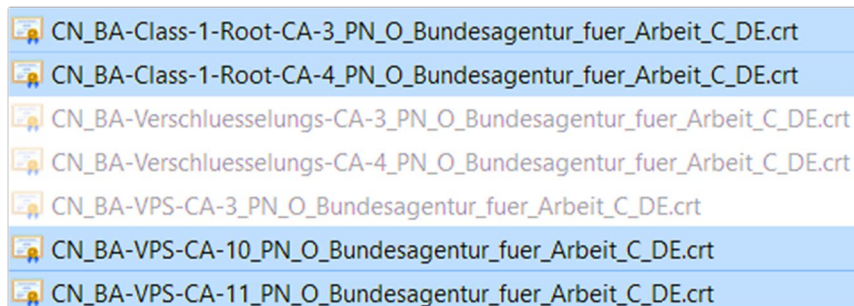


Abbildung 3 – BA-Class-1-Root-CA und BA-VPS-CA Dateien im ZIP-Archiv

4. Klicken Sie **Zertifikat installieren** → **Weiter**
5. Wählen Sie die Option **Alle Zertifikate in folgendem Speicher speichern** und drücken Sie auf **Durchsuchen**.
6. Klicken Sie auf den Eintrag **Vertrauenswürdige Stammzertifizierungsstellen** und bestätigen Sie mit OK.

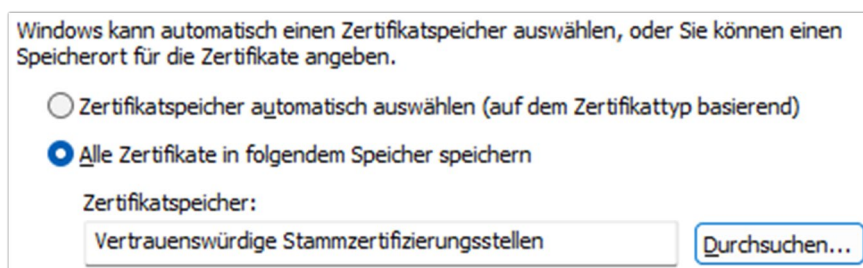


Abbildung 4 – Zertifikatimport-Assistent - Zertifikatsspeicher

7. Wählen Sie **Weiter**, **Fertigstellen** und **OK**.
8. Wiederholen Sie die Schritte 1-7 für die Datei
CN_BA-Class-1-Root-CA-4_PN_O_Bundesagentur_fuer_Arbeit_C_DE.crt
9. Öffnen Sie nun die in der ZIP-Datei enthaltene Datei
CN_BA-VPS-CA-10_PN_O_Bundesagentur_fuer_Arbeit_C_DE.crt
10. Wählen Sie **Zertifikat installieren**
11. Klicken Sie **2x** die Schaltfläche **Weiter** dann **Fertigstellen** und **OK**.
12. Wiederholen Sie die Schritte 9-11 für die Datei
CN_BA-VPS-CA-11_PN_O_Bundesagentur_fuer_Arbeit_C_DE.crt

⚠ Die Zertifikate **BA-Class-1-Root-CA-3.cer** und **BA-Class-1-Root-CA-4.cer** müssen im Zertifikatspeicher für **vertrauenswürdige Stammzertifizierungsstellen** installiert werden damit die Zertifikate der Bundesagentur für Arbeit als vertrauenswürdig eingestuft werden.

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 des Jobcenters 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 oder des Jobcenters 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,

Ihr Ansprechpartner bei der Bundesagentur für Arbeit (BA) oder des Jobcenters möchte mit Ihnen verschlüsselte E-Mails austauschen. Um diesen Vorgang für Sie so einfach wie möglich zu gestalten, steht Ihnen eine Webseite zur Erfassung Ihrer Daten 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!

Eine Arbeitshilfe zur E-Mail-Verschlüsselung finden Sie unter: <https://www.arbeitsagentur.de/e-mail-verschluesselung>

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


Abbildung 5 - 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:

Kontaktdaten bearbeiten

 **Wir verwenden Cookies!**
Klicken Sie hier für weitere Informationen.

 **Brauchen Sie Hilfe?**
Klicken Sie hier.

Bitte geben Sie hier Ihre Kontaktinformationen ein und laden sie das Zertifikat hoch.
Als Zertifikat werden PEM- und DER-kodierte Zertifikate (in Windows mit der Dateinamenerweiterung .cer) unterstützt.

Allgemeine Informationen

Vorname¹:

Nachname¹:

Firma:

Organisationseinheit:

Abteilung:

Funktion:

Verschlüsselung

Zertifikat¹: Keine Datei ausgewählt.

Kontaktdaten

E-Mail²:

Telefon¹:

Mobiltelefon:

Anschrift

Straße/Hausnummer:

Postleitzahl¹:

Stadt¹:

Sprache

Sprache für E-Mails: ▾

Technische Parameter

Unique ID²:

¹ Pflichtfeld
² Zentral vorbelegt. Kann nicht geändert werden.

Abbildung 6 - 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 Dateiondung **.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 zur Freigabe einreichen**, 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 Bundesagentur für Arbeit und der Jobcenter **an Sie verschlüsselte E-Mails** senden.

Falls Sie die eingegebenen Daten speichern aber noch nicht zur Freigabe einreichen wollen, klicken Sie auf die Schaltfläche **Daten zwischenspeichern**.

4 Hilfe zur 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 Computer installieren. Folgen Sie dazu bitte dem Zertifikatsimport-Assistenten. 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.

Klicken Sie mit der rechten Maustaste auf das Startmenü von Windows und wählen **Ausführen**.

Geben Sie hier **certmgr.msc** ein und bestätigen dies mit Enter.

Erweitern Sie links unter Zertifikate den Ordner **Eigene Zertifikate** → **Zertifikate**.

Wählen Sie mit der rechten Maustaste auf ihrem Zertifikat **Alle Aufgaben** → **Exportieren...** aus:

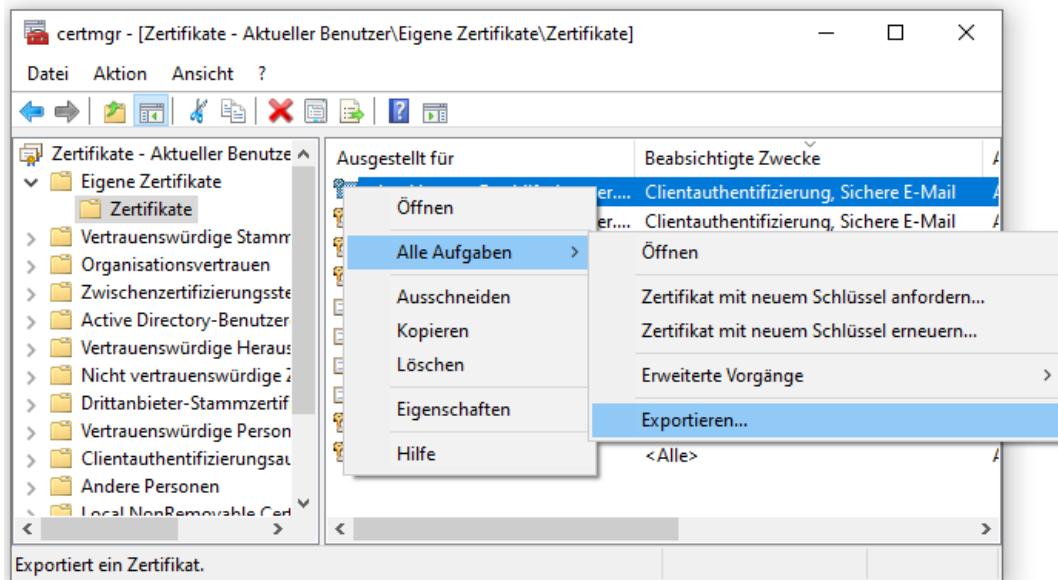


Abbildung 7 - Zertifikatsmanager certmgr.msc

Klicken Sie **Weiter** → **Weiter** → **Weiter** und legen Sie über **Durchsuchen...** den Namen und 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 **Speichern** → **Weiter** → **Fertigstellen**.

Bestätigen Sie zum Abschluss die Erfolgreich-Meldung mit **OK**

4.3 Outlook Fehlermeldung: Verschlüsselungsprobleme

Sie erhalten in Outlook die Fehlermeldung **Verschlüsselungsprobleme**

Die Fehlermeldung bedeutet, dass 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 Wechsel der Zertifikatskette der E-Mail-Verschlüsselung

Ab Mitte Juni 2024 wurde die Zertifikatskette für die Zertifikate der E-Mail-Verschlüsselung der Bundesagentur für Arbeit (@arbeitsagentur.de), der Jobcenter (@jobcenter-ge.de) und des Instituts für Arbeitsmarkt- und Berufsforschung (@iab.de) erweitert.

Die **BA-VPS-CA-11** ist als neue ausstellende CA dazugekommen.

Die **BA-Class-1-Root-CA-4** ist als Root-CA dazugekommen.

Die alten Zertifikate der **BA-VPS-CA-10** und **BA-Class-1-Root-CA-3** bleiben bis zum Ende ihres Lebenszyklus vorhanden.

Falls Sie seit dieser Änderung Probleme beim Versand verschlüsselter E-Mails an uns haben bzw. die neu ausgestellte Zertifikate zur Verschlüsselung nicht als vertrauenswürdig eingestuft werden, laden Sie die Zertifikate der **BA-VPS-CA-10**, **BA-VPS-CA-11**, **BA-Class-1-Root-CA-3** und **BA-Class-1-Root-CA-4** unter: <https://www.pki.arbeitsagentur.de/cacerts/emv/ssl-client-smartcard/> herunter und installieren Sie diese auf Ihren Systemen und/oder Verschlüsselungsgateways.

5.2 Nutzung der eigenen PKI-Infrastruktur

Falls Sie ein eigenes Trustcenter bzw. eine eigene PKI-Infrastruktur betreiben, können diese selbstsignierten 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.
- Die Gesamtlaufzeit des Zertifikats darf 5 Jahre nicht übersteigen.
- Die Schlüssellänge von RSA-Schlüsseln muss mindestens 2048 Bit betragen.

5.3 Validierung der Aussteller-/CA-Zertifikate der BA

Über die Webseite <https://cert-download.arbeitsagentur.de> erhalten Sie als Suchergebnis die Zertifikate und passenden Ausstellerzertifikate zur verschlüsselten E-Mail-Kommunikation mit Benutzern oder gruppenbezogenen Postfächern der Bundesagentur für Arbeit. Eine Validierung der Fingerprints der Ausstellerzertifikate kann über die <https://www.pki.arbeitsagentur.de/cacerts/emv/ssl-client-smartcard/> erfolgen.

5.4 Unterstützte Standards


Verschlüsselte E-Mails, welche an externe Kommunikationspartner gesendet werden, entsprechen dem S/MIME-Standard Version 3 nach RFC 8551. Diese verschlüsselten E-Mails werden mit AES-256 Bit verschlüsselt.

Es können nur verschlüsselte E-Mails nach dem S/MIME-Standard (RFC 8551) empfangen werden. Hierbei muss die Nachricht als EnvelopedException verschickt werden.

Es werden mindestens folgende Verschlüsselungsalgorithmen und Schlüssellängen unterstützt:

- AES mit 256 Bit und 128 Bit Schlüssel
- 3DES (mit CBC) mit 168 Bit Schlüssel

Nachrichten, welche nicht verarbeitet werden können, werden mit einer Fehlermeldung beantwortet und nicht zugestellt.

 Softwareprodukte, welche nicht den vorausgehend genannten Standards entsprechen (z. B. PGP, etc.), werden nicht unterstützt und können nicht für den Austausch von verschlüsselten E-Mails mit der Bundesagentur für Arbeit genutzt werden.

5.5 S/MIME Signatur

Eingehende signierte E-Mails werden dem Empfänger zwar zugestellt, jedoch wird vorab die Signatur zentral entfernt. Das in der Nachricht enthaltene Signaturzertifikat des externen Kommunikationspartners kann **nicht** zur Verschlüsselung von Nachrichten genutzt werden. Die Zertifikate von externen Kommunikationspartnern werden in der Bundesagentur für Arbeit ausschließlich über das **Adressbuch für externe Kontakte** verwaltet.

Von der Bundesagentur für Arbeit ausgehende Nachrichten werden nicht per S/MIME signiert. Als Ersatz werden alle E-Mails der Bundesagentur für Arbeit mit einer DKIM-Signatur versehen.

5.6 News für technische Ansprechpartner

Sie möchten über technische Änderungen zur E-Mail-Verschlüsselung mit uns informiert werden, beispielsweise bei einem CA-Wechsel? Gerne hinterlegen wir Sie dazu als technischen Ansprechpartner in unserem System.

Dazu senden Sie bitte folgende Angaben an IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de:

- E-Mail-Domäne(n), für die Sie der technische Ansprechpartner sind
- Name der Firma/Behörde, für welche die Sie der technische Ansprechpartner sind

Angaben zu technischen Ansprechpartnern¹:

- Vor- und Nachname
- E-Mail-Adresse (persönlich)
- E-Mail-Adresse des Bereichs/Teams (wenn vorhanden)
- Telefonnummer

5.7 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 Einladungsprozess im **Adressbuch für externe Kontakte** gliedert sich in folgende Schritte:

1. Interner initialisiert die Einladung
2. Datenerfassung & Upload des Zertifikats
3. Interner erhält eine E-Mail zur Prüfung/Freigabe des Kontakts
4. Interner prüft die Kontaktdaten
5. Kontaktdaten werden vom Internen freigegeben, zur Überarbeitung zurückgewiesen oder verworfen.

¹ Diese Angaben werden verwendet, um Sie bei technischen Problemen zu kontaktieren oder Sie bei Neuigkeiten wie einem Wechsel unserer Ausstellerzertifikate zu informieren.

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

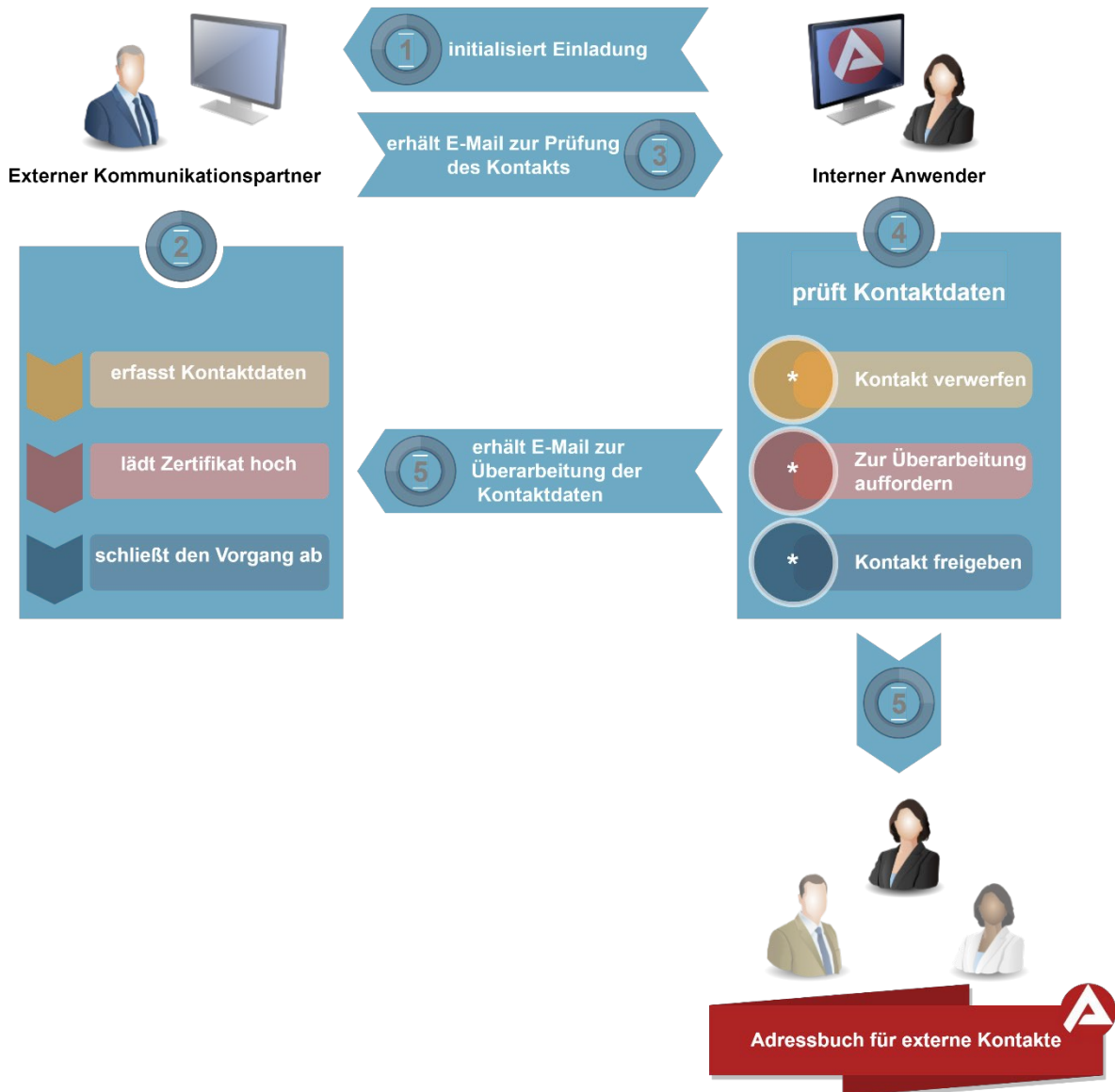


Abbildung 8 - Einladungsprozess - Adressbuch für externe Kontakte

5.7.1 Möglichkeiten zur Bereitstellung Ihrer Zertifikate und Daten im Rahmen des Einladungsprozesses

Nachfolgend finden Sie alle technischen Sonderkonfigurationen, die wir mit Ihnen zur Bereitstellung Ihrer Zertifikate und Daten einrichten können. Diese Einstellungen können auch miteinander kombiniert werden.

5.7.2 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).

5.7.3 Stellvertretende Bearbeitung aller Einladungen durch eine administrative E-Mail-Adresse

Wenn Sie als technischer Ansprechpartner 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. Die tatsächlich eingeladenen Kontakte (Ihre Nutzer) erhalten per E-Mail eine Übersicht der gespeicherten Daten (gemäß DSGVO). Die hinterlegte administrative E-Mail-Adresse wird Ihren Nutzern hierbei mitgeteilt.

Zur Einrichtung einer administrativen E-Mail-Adresse senden Sie bitte folgende Angaben an:

IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de

- E-Mail-Domäne(n) für die die administrative E-Mail-Adresse genutzt werden soll
- Administrative E-Mail-Adresse*:
- Name der Firma/Behörde für welche die administrative E-Mail-Adresse eingerichtet wird

Angaben zu technischen Ansprechpartnern²:

- Vor- und Nachname
- E-Mail-Adresse (persönlich)
- E-Mail-Adresse des Bereichs/Teams (wenn vorhanden)
- Telefonnummer
- gewünschte Vorbelegungen für alle Einladungen:

Feldbezeichnung	Gewünschter Wert
Firma	<i>optional</i>
Straße/Hausnummer	<i>optional</i>
Postleitzahl	<i>optional</i>
Stadt	<i>optional</i>


Tabelle 2 - Gewünschte Vorbelegungen für alle Einladungen (administrative E-Mail-Adresse)

i *Die angegebene administrative E-Mail-Adresse erhält alle Benachrichtigungen (Einladungen, Erinnerungen an ablaufende bzw. abgelaufene Benutzerzertifikate und Mitteilungen zu den eingegebenen Kontaktdaten) für die angegebene E-Mail-Domäne.

² Diese Angaben werden verwendet, um Sie bei technischen Problemen zu kontaktieren oder Sie bei Neuigkeiten wie einem Wechsel unserer Ausstellerzertifikate zu informieren.

5.7.4 Domänenzertifikat (Verschlüsselungsgateway)

Nutzen Sie in Ihrem Verschlüsselungsgateway ein Domänenzertifikat (Domain-Key), ist es ebenfalls möglich dieses Zertifikat für die gesamte E-Mail-Domäne in unserem Adressbuch für externe Kontakte vor zu belegen. Hierdurch ergibt sich der Vorteil, dass nicht alle Nutzer ein persönliches Zertifikat hochladen müssen. Der Einladungsprozess muss trotz des Domänenzertifikats durchgeführt werden.

 Die Funktion Domänenzertifikat muss durch Ihr Verschlüsselungsgateway unterstützt werden.

Zur Einrichtung Ihres Domänenzertifikats senden Sie bitte folgende Angaben an:

IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de

- Ihr Domänenzertifikat in einem ZIP-Archiv (**ohne Passwortschutz**) oder Download-Link auf Ihrer Webseite
- E-Mail-Domäne(n) für die das Domänenzertifikat genutzt werden soll
- Name der Firma/Behörde für welche das Zertifikat eingerichtet wird
- Produktname Ihres Verschlüsselungsgateways, falls es Ihre Sicherheitspolicy zulässt.

Angaben zu technischen Ansprechpartnern:³

- Vor- und Nachname
- E-Mail-Adresse (persönlich)
- E-Mail-Adresse des Bereichs/Teams (wenn vorhanden)
- Telefonnummer
- gewünschte Vorbelegungen für alle Einladungen:

Feldbezeichnung	Gewünschter Wert	Durch Ihre Benutzer änderbar (ja/nein)?
Firma	<i>optional</i>	
Straße/Hausnummer	<i>optional</i>	
Postleitzahl	<i>optional</i>	
Stadt	<i>optional</i>	
Zertifikat	Ihr Domänenzertifikat wird vorbelegt	

Tabelle 3 - Gewünschte Vorbelegungen für alle Einladungen (Domänenzertifikat)

³ Diese Angaben werden verwendet, um Sie bei technischen Problemen zu kontaktieren, Sie über den Ablauf Ihres Domänenzertifikats zu informieren oder Sie bei Neuigkeiten wie einem Wechsel unserer Ausstellerzertifikate zu informieren.

5.7.5 LDAP-Verzeichnis

Es ist ebenfalls möglich, Ihren oder ein öffentlicher LDAP-Verzeichnisdienst (beispielsweise OpenKeys, Global TrustPoint oder Bayern-PKI) an unser System Adressbuch für externen Kontakte anzubinden. Die benötigten Zertifikate und Daten werden beim Versand der Einladung abgerufen und regelmäßig im Adressbuch für externe Kontakte aktualisiert.

Zur Anbindung eines LDAP-Verzeichnisses senden Sie bitte folgende Angaben an:

IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de

- Ihre E-Mail-Domäne(n), für welche das LDAP-Verzeichnis angebunden werden soll

Technische Daten des LDAP-Verzeichnisses	
Hostname / URL:	bspw. ldap.domain.de
Port:	bspw. 389 oder 636
Benutzername (Bind DN):	<i>optional</i>
Passwort (Bind Passwort):	<i>optional</i>
Suchbasis (Base DN):	bspw. ou=certificates

Tabelle 4 - Technische Daten des LDAP-Verzeichnisses

- Weitere Felder die abgefragt werden sollen bspw. givenName, surname, etc.

Angaben zu technischen Ansprechpartnern:⁴

- Vor- und Nachname
- E-Mail-Adresse (persönlich)
- E-Mail-Adresse des Bereichs/Teams (wenn vorhanden)
- Telefonnummer
- gewünschte Vorbelegungen für alle Einladungen:

Feldbezeichnung	Gewünschter Wert	Durch Ihre Benutzer änderbar (ja/nein)?
Firma	<i>optional</i>	
Straße/Hausnummer	<i>optional</i>	
Postleitzahl	<i>optional</i>	
Stadt	<i>optional</i>	

Tabelle 5 - Gewünschte Vorbelegungen für alle Einladungen (LDAP-Verzeichnis)

i Um den Einladungsprozess für Ihre Nutzer vollständig zu automatisieren, müssen alle erforderlichen Pflichtfelder entweder durch Ihr LDAP-Verzeichnis oder Vorbelegungen befüllt werden. Diese lauten: Vorname, Nachname, Zertifikat, Telefonnummer, PLZ und Stadt.

⁴ Diese Angaben werden verwendet, um Sie bei technischen Problemen zu kontaktieren oder Sie bei Neuigkeiten wie einem Wechsel unserer Ausstellerzertifikate zu informieren.

5.8 Versand verschlüsselter Nachrichten von externen Kommunikationspartnern → zur Bundesagentur für Arbeit

5.8.1 Manueller Abruf der Verschlüsselungszertifikate der Bundesagentur für Arbeit

siehe Kapitel 3.1.

5.8.2 Automatisierter Abruf der Verschlüsselungszertifikate der Bundesagentur für Arbeit per LDAP

Um den Versand von verschlüsselten Nachrichten mit einem Verschlüsselungsgateway zur Bundesagentur für Arbeit zu realisieren, bieten wir Ihnen die Möglichkeit, einen Zugriff zu unserem LDAP-Verzeichnisdienst einzurichten.


Um Ihren Zugriff zu beantragen, senden Sie bitte folgende Angaben an:

IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de


- Name der Firma/Behörde, für welche der Zugriff eingerichtet wird
- Produktname Ihres Verschlüsselungsgateways, falls es Ihre Sicherheitspolicy zulässt.
- Ist der LDAP-Zugriff über Netze des Bundes (NdB) oder DOI gewünscht?

Angaben zu technischen Ansprechpartnern:⁵

- Vor- und Nachname
- E-Mail-Adresse (persönlich)
- E-Mail-Adresse des Bereichs/Teams (wenn vorhanden)
- Telefonnummer.

 Die LDAP-Zugangsdaten werden ausschließlich per verschlüsselter E-Mail übermittelt. Sie erhalten dazu eine Einladung zur E-Mail-Verschlüsselung.

5.8.3 Domänenzertifikat der Bundesagentur für Arbeit

 Die Bundesagentur für Arbeit stellt für alle E-Mail-Adressen ausschließlich persönliche Zertifikate aus. Ein Domänenzertifikat für die E-Mail-Domänen der Bundesagentur für Arbeit @arbeitsagentur.de; @jobcenter-ge.de oder iab.de wird **nicht** zur Verfügung gestellt.

⁵ Diese Angaben werden verwendet, um Sie bei technischen Problemen zu kontaktieren oder Sie bei Neuigkeiten wie einem Wechsel unserer Ausstellerzertifikate zu informieren.

Abbildungsverzeichnis

Abbildung 1 - Verschlüsselungszertifikat suchen	7
Abbildung 2 – Suchergebnis Zertifikate.....	7
Abbildung 3 – BA-Class-1-Root-CA und BA-VPS-CA Dateien im ZIP-Archiv	8
Abbildung 4 – Zertifikatimport-Assistent - Zertifikatsspeicher	8
Abbildung 4 - E-Mail Benachrichtigung: "Einladung für E-Mail-Verschlüsselung"	9
Abbildung 5 - Kontaktdaten bearbeiten	10
Abbildung 6 - Zertifikatsmanager certmgr.msc.....	11
Abbildung 7 - Einladungsprozess - Adressbuch für externe Kontakte	14

Tabellenverzeichnis

Tabelle 1 – Dokumenteninformation	2
Tabelle 2 - Gewünschte Vorbelegungen für alle Einladungen (administrative E-Mail-Adresse)	15
Tabelle 3 - Gewünschte Vorbelegungen für alle Einladungen (Domänenzertifikat)	16
Tabelle 4 - Technische Daten des LDAP-Verzeichnisses	17
Tabelle 5 - Gewünschte Vorbelegungen für alle Einladungen (LDAP-Verzeichnis)	17