Trust service provider of the Federal Employment Agency | 12.09.2024

E-mail encryption for external communication partners

IT-Systemhaus

Document information

Author:	Trust service provider of the Federal Employment Agency Regensburger Straße 104 D-90478 Nürnberg
Document ID:	PKI.810.501.1 EN
Date:	12.09.2024

Table 1 - Document information

Impressum

Z24 - IT-Systemhaus
Trust service provider of the Federal Employment Agency
Regensburger Str. 104
D-90478 Nürnberg

Contents

1 General

1.1 Why should e-mail encryption be used?

The encryption of e-mails guarantees the confidentiality of the data transmitted. It ensures that the data transmitted can really only be looked at and read by the intended communication partners.

In order to illustrate an unencrypted e-mail transmission, consider this comparison with the use of the common postal service: an e-mail has roughly the same security characteristics as a postcard. Anyone can read it on its journey from the sender to the recipient.

An encrypted e-mail is like a letter in a locked transport box. Only the owner of the key to open the transport box can read the contents of the letter.

2 Requirements

2.1 What do I need for e-mail encryption?

- You are going to need an e-mail program that supports S/MIME-based e-mail encryption such as Microsoft Outlook, Mozilla Thunderbird etc.
- You also need a certificate and a private key for your own e-mail address.

2.2 Where can I get a certificate for my e-mail address?

You will need a certificate and the associated key material to be able to send or receive encrypted messages. This can be issued by a regular Trust Center (Trust Service Provider).

The Federal Employment Agency will not recommend providers due to legal reasons and **does not** provide encryption certificates for external e-mail addresses.

Your encryption certificate has to satisfy the following requirements:

- Certificate creation in adherence with the X.509 V3 standard.
- The e-mail address entered in the certificate (SubjectAltName) must match your e-mail address (at least a class 1 certificate).
- The (Extended) Key Usage must contain
    - for RSA certificates the attributes "keyEncipherment" and/or "emailProtection".
    - for ECC certificates the attributes "keyAgreement" and/or "emailProtection".
- The certificate must be valid.
- The maximum accepted validity period of the certificate is 5 years.
- The key length of RSA keys must be at least 2048 bits.

3 Exchanging encrypted e-mails

3.1 How can I obtain my correspondent's certificate?

The certificates of the Federal Employment Agency's e-mail addresses can be obtained at the following website: https://cert-download.arbeitsagentur.de/

Please enter the **full** e-mail address with which you wish to exchange encrypted e-mails and click the **Get certificate** button.

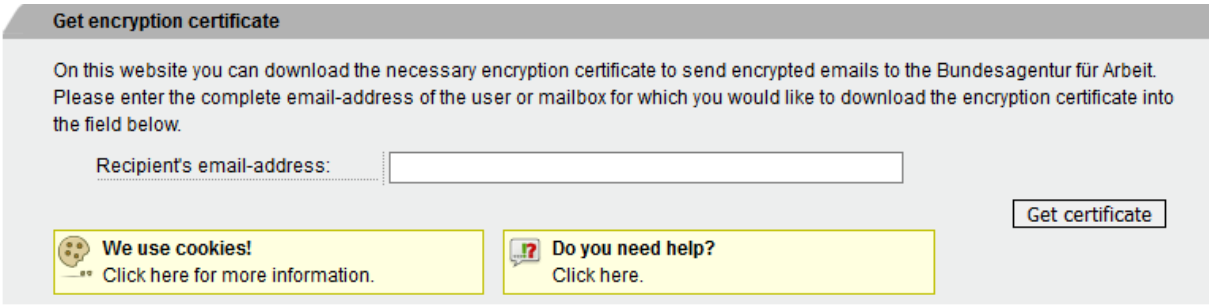

Figure 1 - Searching for an encryption certificate

> ⚠ If you do not receive a result for a specific e-mail address, please contact your contact person in the employment agency or job center. Possibly the e-mail address is incorrect or the encryption is not yet activated.

If the e-mail address can receive encrypted e-mails, you will then be able to download the certificate and the corresponding issuer certificates in various formats:

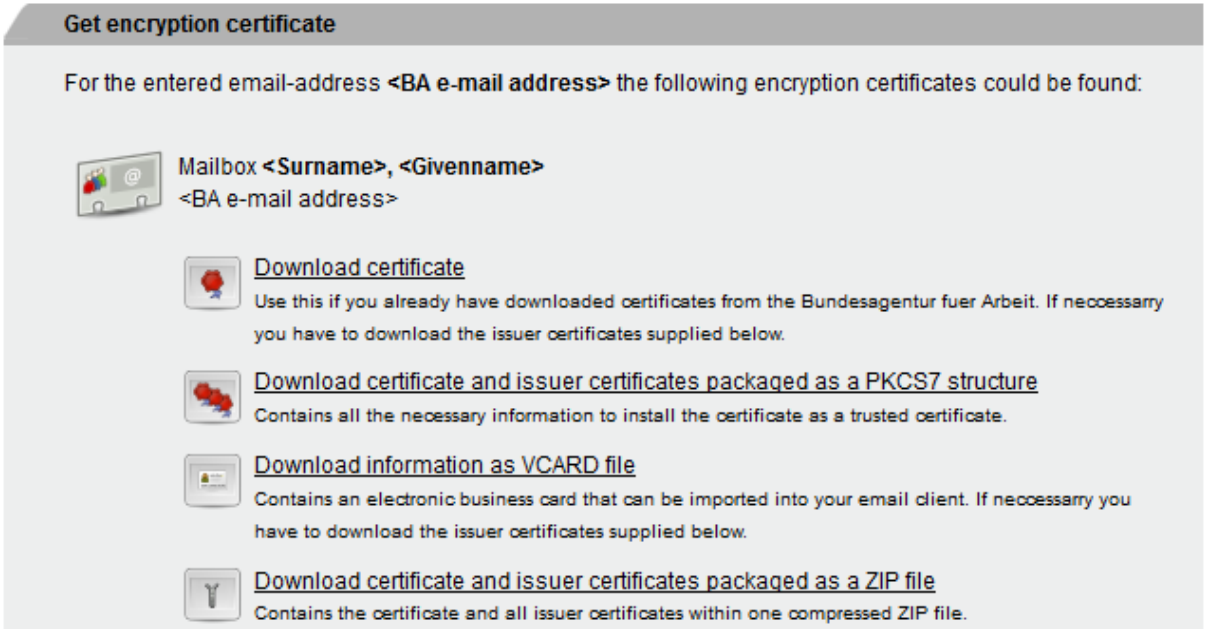

Figure 2 - Encryption and issuer certificates

The certificates of the Federal Employment Agency can also be queried via https://openkeys.de/ or https://www.globaltrustpoint.com/ and their LDAP interfaces. However, query limits or other restrictions may apply. Please contact the respective provider for more information.

3.2 Installing the certificates in Outlook

3.2.1 Downloading the required files

Click on **Download information as VCARD file** and save the file.

Go to the website: https://www.pki.arbeitsagentur.de/cacerts/emv/ssl-client-smartcard/. Click on **Alle Zertifikate als ZIP-Datei** at the top left and save the file.

3.2.2 Importing issuer /CA certificates

1. Unpack the ZIP file you have just downloaded
2. Go to the directory **der**
3. Open the file
   CN_**BA-Class-1-Root-CA-3**_PN_O_Bundesagentur_fuer_Arbeit_C_DE.crt

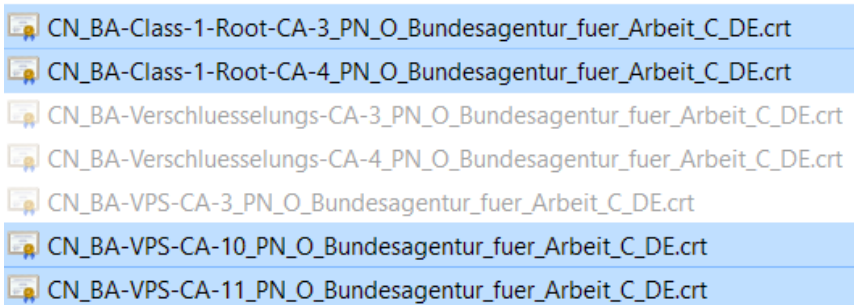

Figure 3 - BA-Class-1-Root-CA and BA-VPS-CA files in the ZIP archive

4. Click **Install certificate** → **Next**
5. Select the option **Place all certificates in the following store** and click **Browse**.
6. Click on the **Trusted Root Certification Authorities** item and confirm with **OK**.

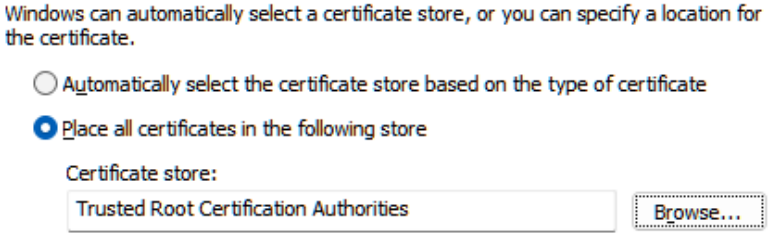

Figure 4 - Certificate Import Wizard - Certificate store

7. Select **Next**, **Finish** and **OK.**
8. Repeat the steps 1-7 for the file
   CN_**BA-Class-1-Root-CA-4**_PN_O_Bundesagentur_fuer_Arbeit_C_DE.crt
9. Open the file contained in the ZIP archive
   CN_**BA-VPS-CA-10**_PN_O_Bundesagentur_fuer_Arbeit_C_DE.crt
10. Select **Install certificate**.
11. Click twice on **Next**, **Finish** and then **OK**.
12. Repeat steps 9-11 for the file
    CN_**BA-VPS-CA-11**_PN_O_Bundesagentur_fuer_Arbeit_C_DE.crt

⚠ The certificates **BA-Class-1-Root-CA-3.crt** and **BA-Class-1-Root-CA-4.crt** must be installed in the certificate store for **Trusted Root Certification Authorities** in order for the certificates of the Federal Employment Agency to be classified as trusted.

3.2.3 Importing the contact and sending an encrypted e-mail

Double-click on the downloaded vCard file (.vcf) to open it. Various fields are already preset, such as the name and the e-mail address of the certificate holder. Select the **Save & Close** button in the contact. Now you have created the contact and its certificate.

To send an encrypted e-mail, create a new e-mail, select the **contact** you just saved as the **recipient**. Activate the **Encrypt** button in **Options**. Complete your e-mail and send it.

If you wish to send encrypted e-mails to other e-mail addresses of the Federal Employment Agency, the Institute for Employment Research or job centers, you should download the corresponding vCard files as described in chapter 3.1 and save the contacts in Outlook.

3.3 Receiving encrypted e-mails

In order for your contact person at the Federal Employment Agency or job center to send you encrypted e-mails, your own certificate is required. Ask your contact person to send you an invitation for email encryption. The invitation will be sent to you via email:

Subject: Invitation for email encryption

Dear Madam,
Dear Sir,

your contact at the Federal Employment Agency (Bundesagentur für Arbeit) or the Jobcenter would like to exchange encrypted emails with you. To make this process as easy as possible for you, a website is available for you to enter your data. Please use the following link to access this website:
<Link to entering and modifying contact details>

Please save this email. The link can be used to edit the information you provided for your e-mail address <e-mail address> at any time.

For more information on email encryption, see: https://www.arbeitsagentur.de/en/e-mail-encryption

By using our website, you agree to our Terms of Use (https://cert-upload.arbeitsagentur.de/staticpages/page/usage).

Figure 5 - E-mail notification: "Invitation for email encryption"

The invitation contains a link to a website where you can enter your personal data and upload your certificate. **Please save this e-mail**.

3.4 Entering contact data and uploading your certificate

Clicking on the link in the invitation e-mail takes you to a website where you can enter your contact information and upload your certificate:

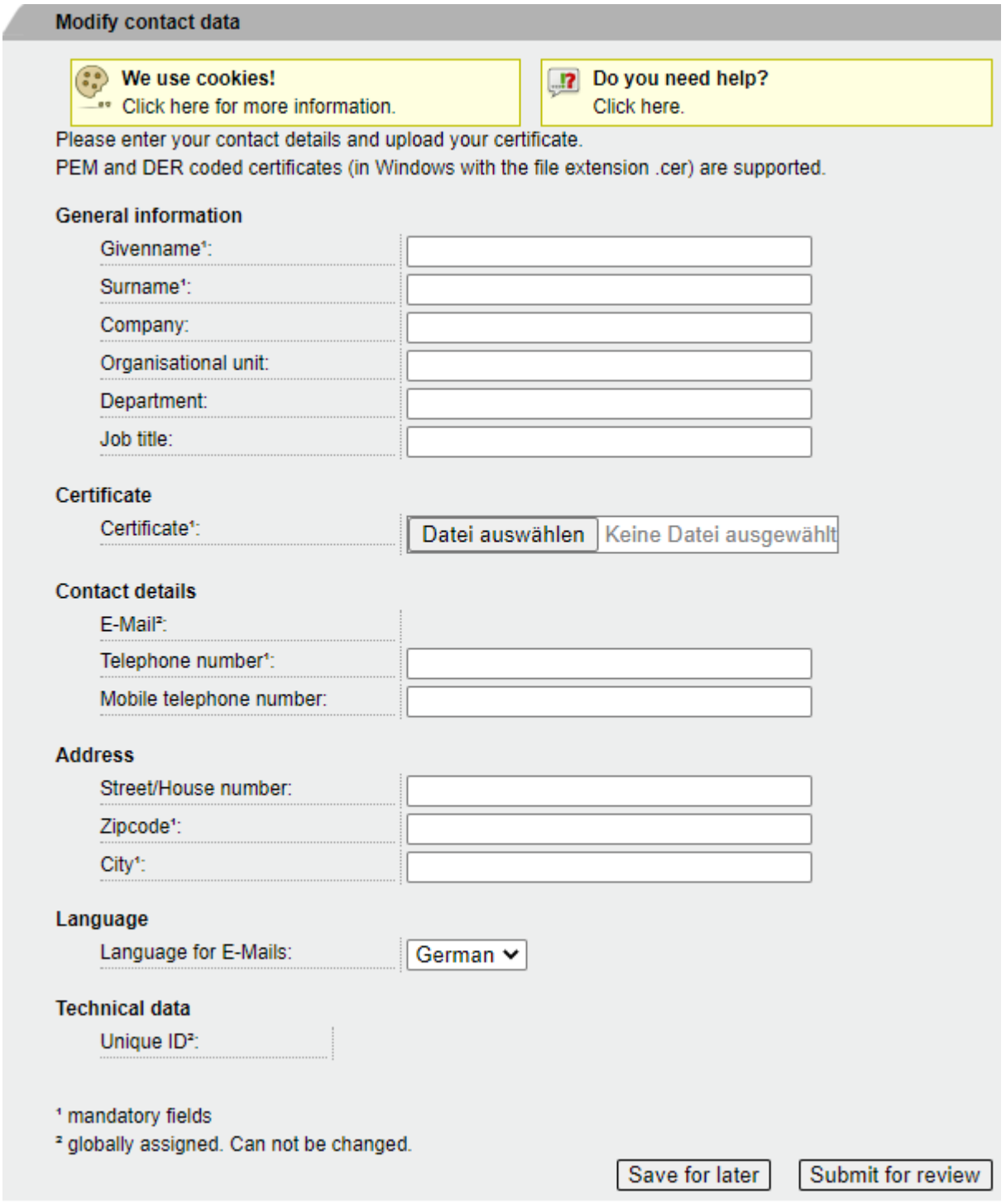

Figure 6 - Editing contact information

Fill out at least the mandatory fields **Givenname**, **Surname**, **Telephone number**, **Zipcode** and **City** and click the **Browse** button.

Select your **certificate** with the file extension **.cer**. If you do not have this format, first export your certificate (see chapter 4.1, 4.2).

Click the **Submit for review** button. This completes the invitation process and submits your contact data for approval. You can no longer edit your data until it has been approved by your contact person.

Once your contact data has been approved, **all** Federal Employment Agency and job center employees can send you **encrypted e-mails**.

If you want to save the entered data without submitting it yet for review, click the **Save for later** button.

4 Help for Troubleshooting

4.1 Importing your P12 or PFX file

If you only have a P12 or PFX file (your personal key material), this must first be installed on your Computer. Please follow the Certificate Import Wizard. The Certificate Import Wizard is launched as soon as you open (‘double-klick’) the P12 or PFX file. You will have to enter your personal password during the import process.

4.2 Exporting your certificate as a CER file

Once you have imported your personal key material (P12 or PFX file), you must export your certificate as a CER file.
Right-click on the Windows Start menu and select **Run**.
Type **certmgr.msc** and confirm with Enter.
Expand the folder **Certificates** → **Personal** → **Certificates** and select yours.
Right-click your certificate and select **All Tasks** → **Export…**.

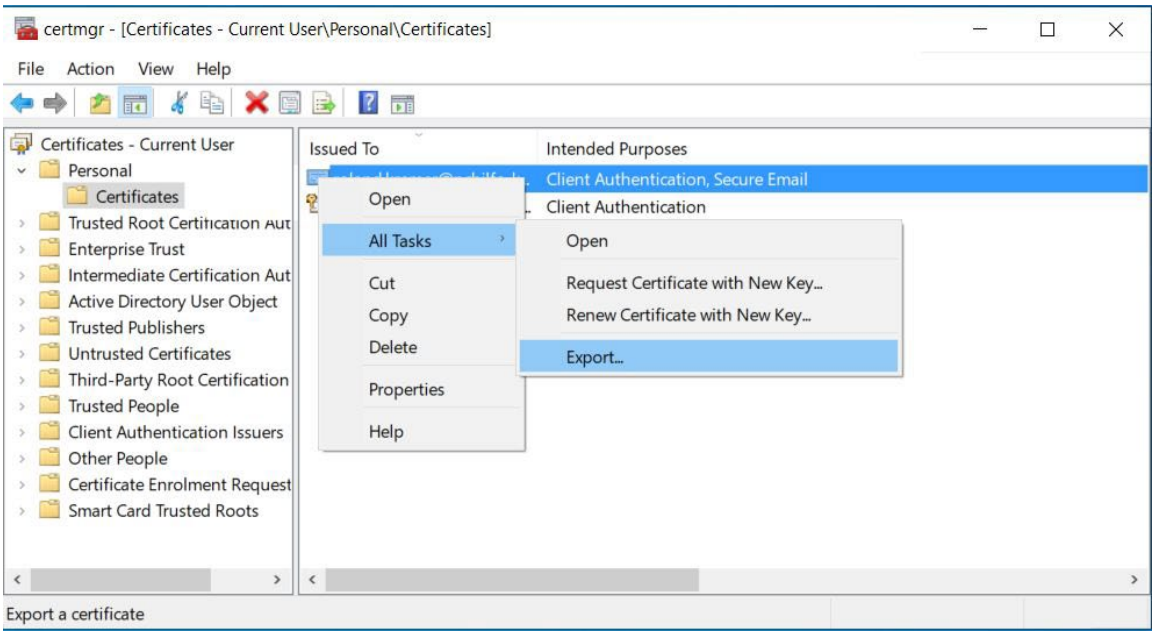

Figure 7 - Certificate Manager certmgr.msc

Click on **Next -> Next -> Next ->** use **Browse...** to specify the name and storage location for your certificate.

> ⚠ You should make a note of this location because it will be needed again to process your invitation to e-mail encryption.

Click on **Save -> Next -> Finish**.
Finally, confirm the successful message with **OK**.

4.3 Outlook error message: encryption problems

You receive the error message “encryption problems” in Outlook.

The error message means that your Outlook has encountered problems with the recipient's certificate. Please repeat the steps in chapter 3.2 including the subchapters exactly. In most cases, step 3.2.2 Importing CA certificates was performed incorrectly.

5 Information for technical IT services

5.1 Change of the certificate chain for email encryption

As of mid-June 2024, the certificate chain for the email encryption certificates of the Federal Employment Agency (@arbeitsagentur.de), the job centers (@jobcenter-ge.de), and the Institute for Employment Research (@iab.de) was extended.

The **BA-VPS-CA-11** has been added as a new issuing CA.

The **BA-Class-1-Root-CA-4** has been added as root CA.

The old certificates of **BA-VPS-CA-10** and **BA-Class-1-Root-CA-3** will remain until the end of their lifecycle.

If you have had problems sending encrypted emails to us since this change or the newly issued certificates for encryption are not classified as trustworthy, download the **BA-VPS-CA-10**, **BA-VPS-CA-11**, **BA-Class-1-Root-CA-3** and **BA-Class-1-Root-CA-4** certificates from: https://www.pki.arbeitsagentur.de/cacerts/emv/ssl-client-smartcard/ and install them on your systems and/or encryption gateways.

5.2 Use of your own PKI infrastructure

If your company operates its own Trust Center or PKI infrastructure, these self-signed certificates can be used if they satisfy the following requirements:

- Certificate creation in adherence with the X.509 V3 standard.
- The e-mail address entered in the certificate (SubjectAltName) must match your e-mail address (at least a class 1 certificate).
- The (Extended) Key Usage must contain
    - for RSA certificates the attributes "keyEncipherment" and/or "emailProtection".
    - for ECC certificates the attributes "keyAgreement" and/or "emailProtection".
- The certificate must be valid.
- The maximum accepted validity period of the certificate is 5 years.
- The key length of RSA keys must be at least 2048 bits.

5.3 Validation of the BA issuer certificates

The certificates and appropriate issuer certificates for encrypted email communication with users or shared mailboxes of the Federal Employment Agency can be obtained at the following website https://cert-download.arbeitsagentur.de.

The fingerprints of the issuer certificates can be validated at the following website https://www.pki.arbeitsagentur.de/cacerts/emv/ssl-client-smartcard/.

5.4 Supported standards

Encrypted e-mails sent to external communication partners comply with the S/MIME standard version 3 according to RFC 8551. These encrypted emails are encrypted with AES-256 bit.

Only encrypted emails according to the S/MIME standard (RFC 8551) can be received. The message has to be sent as EnvelopedData.

At least the following encryption algorithms and key lengths are supported:

- AES with 256 bit and 128 bits key
- 3DES (with CBC) with 168 bits key

Messages that cannot be processed are answered with an error message and will not be delivered.

⚠ Software products that do not meet the standards mentioned above (e.g. PGP, etc.) are not supported and cannot be used to exchange encrypted emails with the Federal Employment Agency.

5.5 S/MIME signature

Incoming signed e-mails are delivered to the recipient, but the signature will be removed at the e-mail-gateway beforehand. The signature certificate of the external communication partner contained in the message **cannot** be used to encrypt messages. The certificates of external communication partners are only managed in the Federal Employment Agency via the **address book for external contacts**.

Messages from the Federal Employment Agency are not signed by S/MIME. As a substitute all Federal Employment Agency's e-mails are provided a DKIM signature.

5.6 News for technical contact persons

Would you like to be informed about technical changes to e-mail encryption with us, for example in the event of a CA change? We would be happy to register you as a technical contact in our system.

Please send us the following information to IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de:

- E-mail domain(s) for which you are the technical contact person
- Name of the company/authority for which you are the technical contact person

Technical contact person's information[1]:

- First and Last Name
- E-Mail address (personal)
- E-mail address of the department / team (if available)
- Telephone number

5.7 Sending encrypted messages from the Federal Employment Agency → to external communication partners

The Federal Employment Agency uses the **Address book for external contacts** system to provision and administer certificates for the exchange of encrypted e-mails.

The process flow consists of the following steps:

1. Internal user initializes the invitation
2. Data collection & upload of the certificate
3. Internal user receives an e-mail to check the contact data
4. Internal user checks the contact data
5. Contact data is approved by the internal user, rejected for revision or discarded.

ℹ As soon as the external contact has been approved, it is available for all internal users in the address book for external contacts.

[1] This information will be used to contact you in the event of technical problems or to inform you of news such as a change in our issuer certificates.

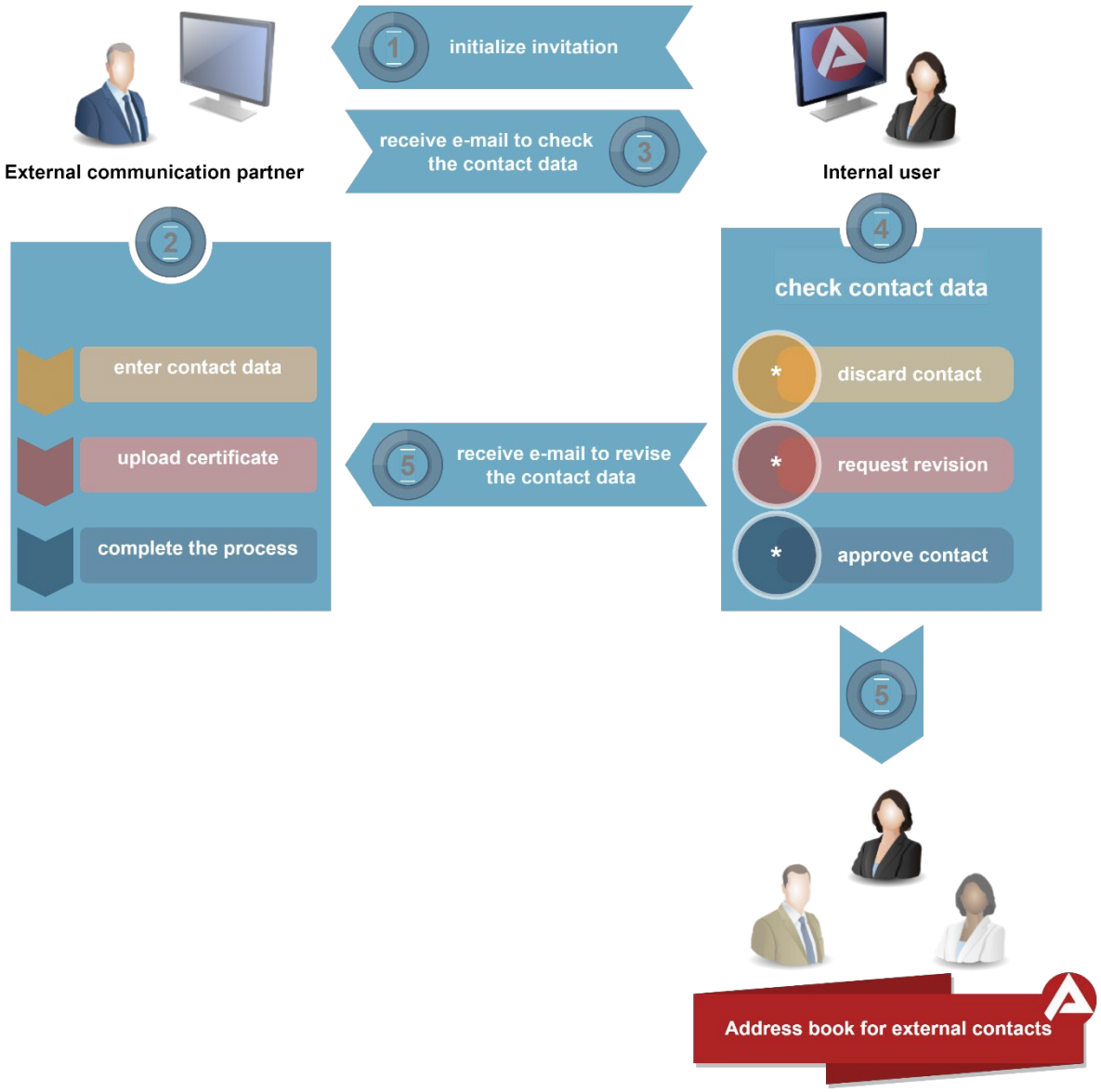

Figure 8 - Invitation process – address book for external contacts

5.7.1 Options for providing your certificates and data as part of the invitation process

Below you will find all the special technical configurations that can be set up with you to provide your certificates and data. It is possible to combine these settings with one another.

5.7.2 Independent processing by the invited external communication partner

The external communication partner enters his contact data, uploads his **personal certificate** for the encryption of e-mails and completes the process (see chapter 3.4).

5.7.3 Representative processing of all invitations via an administrative e-mail address

If you would like, as a technical contact person, to receive all the invitations for your e-mail domain as well as maintain the certificates and contact details, an e-mail address you specify can be set up as an administrative e-mail address. The actually invited contacts (your users) receive an overview of the stored data by email (in accordance with GDPR). The stored administrative email address will be communicated to your users.

To set up an administrative e-mail address, please send the following information to:

IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de.

- E-mail domain(s) for which the administrative e-mail address should be used
- Administrative e-mail address*:
- Name of the company/authority for which the administrative email address will be set up

Technical contact person's information[2]:

- First and Last Name
- E-Mail address (personal)
- E-mail address of the department / team (if available)
- Telephone number
- Desired defaults for all invitations:

Field name	Desired value
Company	*optional*
Street/House number	*optional*
Zip code	*optional*
City	*optional*

Table 2 - Desired defaults for an administrative e-mail address

*The specified administrative email address will receive all notifications (invitations, reminders on expiring or expired user certificates and communications concerning the entered contact data) for the specified email domain.

[2] This information will be used to contact you in the event of technical problems or to inform you of news such as a change in our issuer certificates.

5.7.4 Domain certificate (encryption gateway)

If you use a domain certificate (domain key) in your encryption gateway, it is also possible to preset this certificate for the entire e-mail domain in our address book for external contacts, which has the advantage of not having to upload a personal certificate for all users. The invitation process must be carried out despite the domain certificate.

⚠ The Domain Certificate feature has to be supported by your encryption gateway.

To set up your domain certificate, please send the following information to:
IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de.

- Your domain certificate in a ZIP archive **(without password protection)** or download link on your website
- E-mail domain(s) for which the domain certificate should be used
- Name of the company/authority for which the domain certificate will be set up
- Product name of your encryption gateway, if your security policy allows it.

Technical contact person's information:[3]

- First and Last Name
- E-mail address (personal)
- E-mail address of the department / team (if available)
- Telephone number
- Desired defaults for all invitations:

Field name	Desired value	Can be changed by your users (yes/no)?
Company	*optional*	
Street/House number	*optional*	
Zip code	*optional*	
City	*optional*	
Certificate	Your domain certificate will be preset	

Table 3 - Desired defaults for domain certificates

[3] This information will be used to contact you in the event of technical problems, to inform you about the expiry of your domain certificate or to inform you of news such as a change in our issuer certificates.

5.7.5 LDAP directory

It is also possible to connect your LDAP directory service to our system address book for external contacts. The required certificates and data are retrieved when the invitation is sent and regularly updated in the address book for external contacts.

To connect your LDAP directory to our system, please send the following information to IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de.

- Your e-mail domain(s) for which the LDAP directory should be connected

Technical data of the LDAP directory	
Hostname / URL:	e.g. ldap.domain.de
Port:	e.g. 389 or 636
Username (bind DN):	*optional*
Password (bind password):	*optional*
Search base (base DN):	e.g. ou=certificates

Table 4 - Technical data of the LDAP directory

- Other fields to be queried e.g. givenName, surname, etc.

Technical contact person's information:[4]

- First and Last Name
- E-mail address (personal)
- E-mail address of the department / team (if available)
- Telephone number
- Desired defaults for all invitations:

Field name	**Desired value**	**Can be changed by your users (yes/no)?**
Company	*optional*	
Street/House number	*optional*	
Zip code	*optional*	
City	*optional*	

Table 5 - Desired defaults for the LDAP directory

In order to fully automate the invitation process for your users, all required mandatory fields must be filled either by your LDAP directory or defaults. These are: givenname, surname, certificate, telephone number, zipcode and city.

[4] This information will be used to contact you in the event of technical problems or to inform you of news such as a change in our issuer certificates.

5.8 Sending encrypted messages from external communication partners → to the Federal Employment Agency

5.8.1 Obtaining the Federal Employment Agency's encryption certificates manually

see chapter 3.1

5.8.2 Obtaining the Federal Employment Agency's encryption certificates automatically via LDAP

In order to enable the sending of encrypted messages with an encryption gateway to the Federal Employment Agency, we offer you the option to set up access to our LDAP directory service.

To get your access, please send the following information to

IT-Systemhaus.Vertrauensdienste@arbeitsagentur.de

- Name of the company/authority for which access will be set up
- Product name of your encryption gateway, if your security policy allows it.
- Is LDAP access via federal networks (NdB) or DOI required?

Technical contact person's information:[5]

- First and Last Name
- E-mail address (personal)
- E-mail address of the department / team (if available)
- Telephone number

⚠ The LDAP access data will only be transmitted via encrypted email. You will receive an invitation to email encryption.

5.8.3 Federal Employment Agency's domain certificate

⚠ The Federal Employment Agency only issues personal certificates for all e-mail addresses. A domain certificate for the e-mail domains of the Federal Employment Agency @arbeitsagentur.de, @ jobcenter-ge.de or iab.de will **not** be provided.

[5] This information will be used to contact you in the event of technical problems or to inform you of news such as a change in our issuer certificates.

Index of figures

Index of tables