Trust service provider of the Federal Employment Agency | January 27, 2023

Email encryption for external Communication partner

IT-Systemhaus

imprint

OPS4 - IT system house

Trust service provider of the Federal Employment Agency

Regensburger Straße 104

D-90478 Nuremberg

Table of contents

Table of contents 3

1 General..... 5

1.1 Why should email encryption be used?.....5

2 Requirements..... 6

2.1 What do I need for email encryption?..... 6

2.2 Where do I get a certificate for my email address?.....6

3 Exchange of encrypted emails..... 7

3.1 How do I get my contact's certificate? 7

3.2 Installing certificates in Outlook 8th

3.2.1 Downloading the required files..... .....8th

3.2.2 Importing the Issuer/CA Certificates 8th

3.2.3 Importing the contact and sending an encrypted email.....9

3.3 Receiving encrypted emails 9

3.4 Enter contact details and upload certificate..... 9

4 Troubleshooting Help..... 11

4.1 Importing your .p12 or .pfx file..... 11

4.2 Exporting your certificate as a .cer file 11

4.3 Outlook error message: Encryption problems.....11

5 Information for technical IT services 12

5.1 Changing the CA certificate BA-VPS-CA for email encryption.....12

5.2 Use of your own PKI infrastructure..... 12

5.3 Validation of the BA issuer/CA certificates ..... .12

5.4 Supported standards..... 12

5.5 S/MIME signature..... 13

5.6 News for technical contacts..... 13

5.7 Sending encrypted messages from the Federal Employment Agency ÿ to external communication partners 13

5.7.1 Options for providing your certificates and data as part of the invitation process 15

5.7.2 Independently by the invited external communication partner..... 15

5.7.3 Substitute processing of all invitations via an administrative email address 15

5.7.4 Domain certificate (encryption gateway) 16

5.7.5 LDAP directory 17

5.8 Sending encrypted messages from external communication partners ÿ to the Federal Employment Agency 18

5.8.1 Manual retrieval of the encryption certificates from the Federal Employment Agency.... 18

5.8.2 Automated retrieval of the Federal Employment Agency's encryption certificates via LDAP 18

5.8.3 Domain certificate from the Federal Employment Agency 18

List of illustrations 19
List of tables..... 20

1. General

1.1 Why should email encryption be used?

Encrypting emails ensures the confidentiality of the transmitted data. It ensures that the transmitted data can actually only be viewed and read by the designated communication partners. An unencrypted email has roughly the same security properties as a postcard. This can be read by everyone on the way from the sender to the recipient.

2 requirements

2.1 What do I need for email encryption?

- You need an email program that supports S/MIME encryption, e.g Microsoft Outlook, Mozilla Thunderbird, etc.
- To encrypt email you need a certificate and the associated private one Key for your own email address.

2.2 Where do I get a certificate for my email address?

In order to send and receive encrypted emails, you need your email address a certificate and the associated private key. This can e.g. B. be issued by a trust center (trust service provider).

The Federal Employment Agency cannot make any recommendations for specific providers. The Federal Employment Agency **does not** provide certificates for encryption for external email addresses.

Your encryption certificate must meet the following requirements:

- Creation of the certificate according to the X.509 V3

standard. • The email address entered in the certificate (SubjectAltName) must match your email address match (at least a class 1 certificate).

- The (extended) key usage must…
  - for RSA certificates at least the attributes “key encryption” and/or “Secure Email” included.
  - For ECC certificates at least the attributes “Key agreement” and “Secure e-mail” Email” included.
- The certificate must be valid.
- The total term of the certificate must not exceed 5 years. (according to BSI TR-02102-1) • The

key length of RSA keys must be at least 2048 bits.

3 Exchange encrypted emails

3.1 How do I get my certificate?

contact person?

You can get the certificates of the Federal Employment Agency's email addresses from the following website obtain: https://cert-download.arbeitsagentur.de/

Please enter the **full** email address with which you would like to exchange encrypted emails in the search here . Then click the **Find Certificate button.**

Figure 1 - Find encryption certificate

> ⚠ If you do not receive a result for a specific email address, please contact your contact person at the employment agency or the job center. The email address may be incorrect or encryption is not yet activated.

If the email address can receive encrypted emails, you can then do so
Download the certificate and the corresponding issuer certificates in various formats:

Figure 2 - Issuer certificates

Here you can obtain the certificate in various file formats:

- Download the certificate in .cer format,
- Download the certificate as a PKCS7 structure with issuer certificates, • Download as a vCard file in VCF format (e.g. suitable for Outlook),
- Download the certificate and the issuer certificates as a ZIP file.

3.2 Installing certificates in Outlook

3.2.1 Download the files you need

Click on **Download the data as a vCard file** and save the file.

Click on **Download the issuer certificates as a ZIP file** and save the file.

3.2.2 Importing the issuer/CA certificates

Open the ZIP file and the entry **BA-Class-1-Root-CA-3.cer inside.**

Select **Install Certificate.** Click **Next,** select **Save all certificates to the following store** option and press **Browse.** Click on the **Trusted Root Certification Authorities** entry and confirm with OK.

Select **Next, Finish** and **OK.** Now open the **BA-VPS-CA-10.cer** entry in the ZIP file and select **Install Certificate.** Then click the **Next** button twice and then **Finish.**

⚠ You need the **BA-VPS-CA-10.cer** and **BA-Class-1-Root-CA-3.cer** certificates on your PC! If these are not available, please follow all steps.

3.2.3 Import the contact and send an encrypted email

Open the downloaded vCard file (.vcf) with a double click. Various fields are prefilled, such as the name and email address of the certificate holder. Select the **Save and Close** button in the contact. You have now created the contact including its certificate.

To send an encrypted email, create a new email and select the **contact** you just saved as the **recipient .** From **Options ,** enable the **Encrypt Message button.** Complete your email and send it.

If you would like to send encrypted emails to other email addresses of the Federal Employment Agency, the IAB or the job centers, download the corresponding vCard files - as described from Chapter 3.1 - and save the contacts in Outlook.

3.3 Receiving encrypted emails

Your own certificate is required so that your contact at the Federal Employment Agency can send you encrypted emails. Ask your contact person to send you an invitation for email encryption. The invitation will be sent to you by email:

Subject: Invitation for email encryption

Good day,

Your contact at the Federal Employment Agency (BA) or the job center would like to exchange encrypted emails with you. To make this process as easy as possible for you, a website is available to collect your data. Please use the following link to access this website: <Link for recording and changing contact details>

Please save this email. The link can be used to subsequently change the information you entered for your email address <email address> !

A working aid for email encryption can be found at: https://www.arbeitsagentur.de/e-mail- verschluesselung

By using our website you agree to our terms of use https://cert-upload.arbeitsagentur.de/staticpages/page/usage agreed.

Figure 3 - Email Notification: “Email Encryption Invitation”

The invitation contains a link that redirects you to a webpage where you can enter your personal information and upload your own certificate. **Please keep this email.**

3.4 Enter contact details and upload certificate

By clicking on the link in the invitation email you will be given the opportunity to submit yours on a website To collect contact details and upload your own certificate:

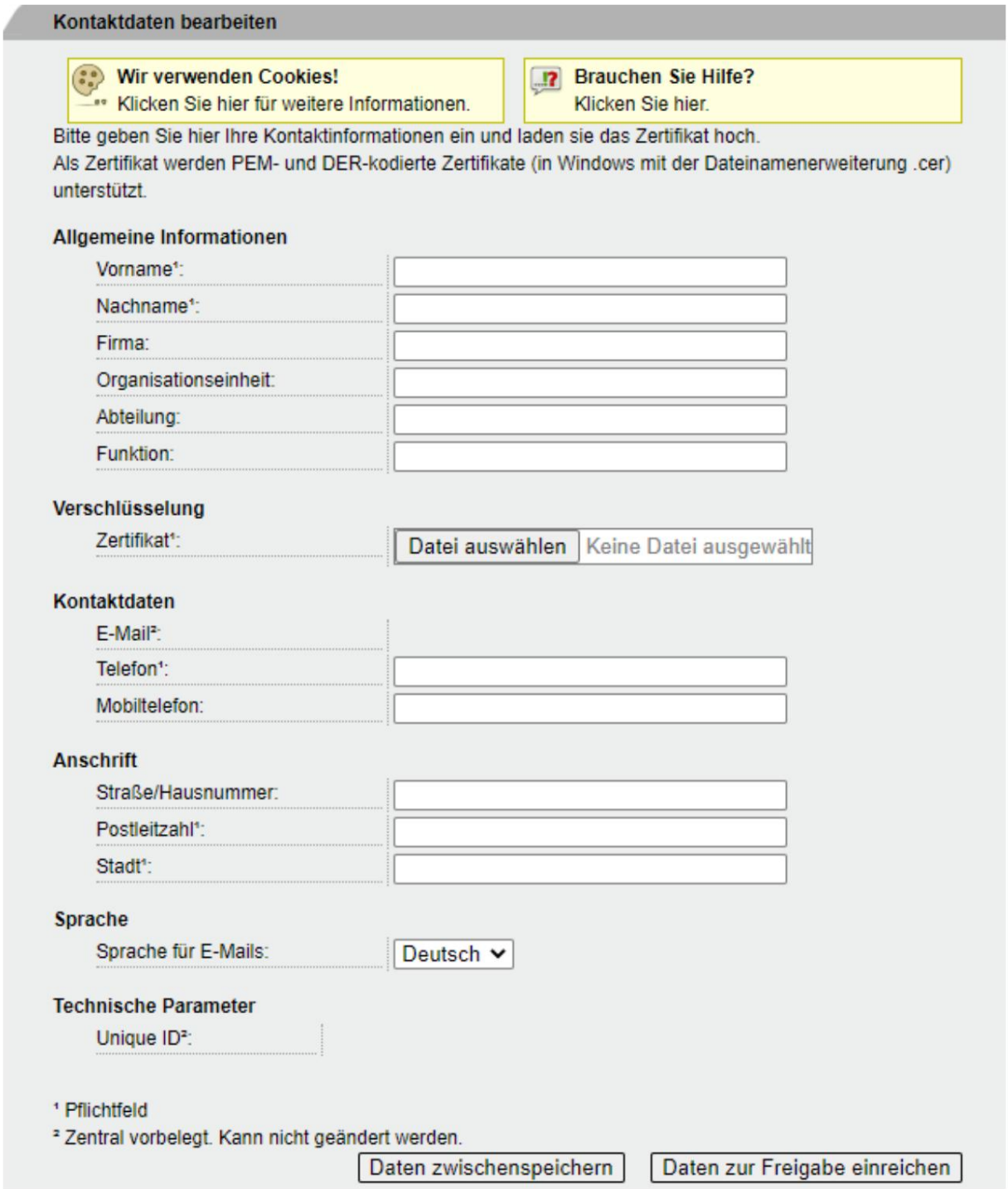

Figure 4 - Edit contact details

Complete at least the **First Name, Last Name, Phone, Zip Code** and **City** fields and click the **Browse...** button.

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

Click the **Submit Details for Sharing** button to complete the invitation process and submit your contact for sharing. Until the data has been approved by your contact person, you can no longer edit it.

As soon as your contact has been approved, **all** employees of the Federal Employment Agency and the job center can send **you encrypted emails .**

4 Troubleshooting Help

4.1 Importing your .p12 or .pfx file

If you only have a .p12 or .pfx file (your personal key material), you must first install it on your PC. To do this, please follow the certificate import wizard. The certificate import wizard will start as soon as you open the .p12 or .pfx file. Enter your password for this file during the import process.

4.2 Export your certificate as a .cer file

Once you have imported your personal key material (.p12 or .pfx file) into Windows, you will need to export your certificate as a .cer file.
Right-click on the Windows Start menu and select **Run.**

Enter **certmgr.msc** here and confirm with Enter.
On the left, under Certificates, expand the **My Certificates ÿ Certificates folder.**
Right-click on your certificate and select **All Tasks ÿ Export :**

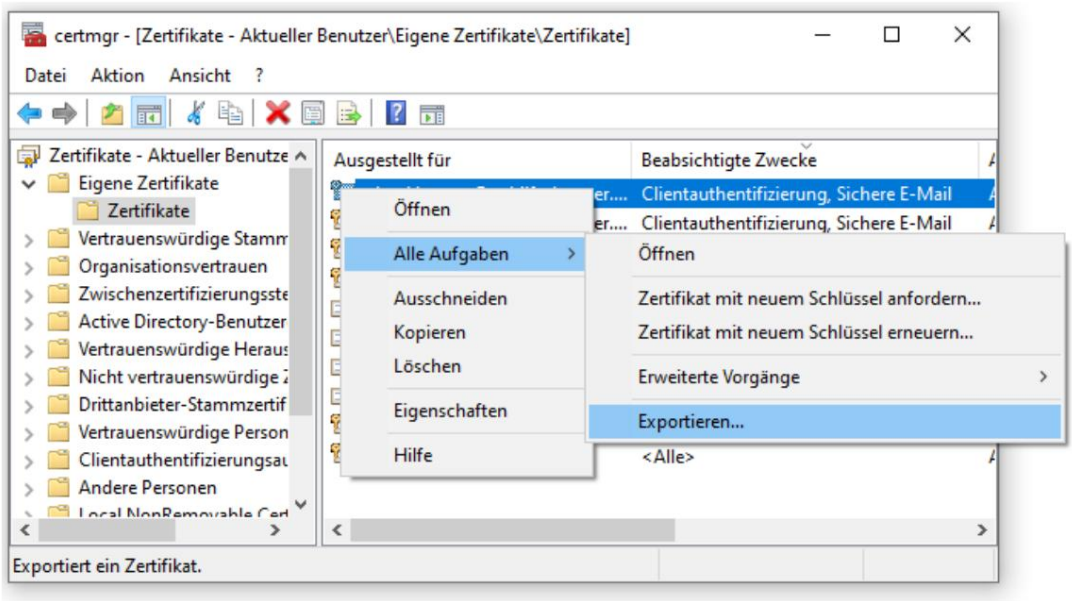

Figure 5 – Certificate Manager certmgr.msc

Click **Next ÿ Next ÿ Next** and use **Browse...** to enter the name and the Specify the location for your certificate.

> ⚠ Please note the storage location; this will be needed again to process the invitation for email encryption.

Click **Save ÿ Next ÿ Finish.**

Finally, confirm the success message with **OK**

4.3 Outlook error message: Encryption problems

You receive the error message **Encryption problems** in Outlook

The error message means that Outlook has detected problems with the recipient's certificate. Please carry out the steps in chapter 3.2 including the subchapters again in detail. Most of the time, step 3.2.2 Importing the CA certificates is performed incorrectly.

5 Information for technical IT services

5.1 Changing the CA certificate BA-VPS-CA to email Encryption

At the end of January 2023, the certificate chain for the email encryption certificates for the Federal Employment Agency (@arbeitsagentur.de), the job center (@jobcenter-ge.de) and the Institute for Labor Market and Vocational Research (@iab. de) changed.

If you have had problems sending encrypted emails to us since then, download this Certificate of **BA-VPS-CA-10** at:

https://www.pki.arbeitsagentur.de/cacerts/emv/ssl-client-smartcard/ Download and install this on your systems.

5.2 Use of your own PKI infrastructure

If you operate your own trust center or PKI infrastructure, these self-signed certificates can also be used if you meet the following requirements:

- Creation of the certificate according to the X.509 V3 standard. • The email address entered in the certificate (SubjectAltName) must match your email address match (at least a class 1 certificate).
- The (extended) key usage must...
  - for RSA certificates at least the attributes “key encryption” and/or “Secure Email” included.
  - For ECC certificates at least the attributes “Key agreement” and “Secure e-mail” Email” included.
- The certificate must be valid.
- The total term of the certificate must not exceed 5 years.
- The key length of RSA keys must be at least 2048 bits.

5.3 Validation of the BA’s issuer/CA certificates

Via the website https://cert-download.arbeitsagentur.de You will receive end user certificates and the appropriate issuer certificates from the BA as a search result. Validation of the fingerprints of the issuer certificates can be done via https://www.pki.arbeitsagentur.de/cacerts/emv/ssl-client-smartcard/ take place.

5.4 Supported Standards

Encrypted emails that are 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 must be sent as EnvelopedData.

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

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

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

⚠ Software products that do not comply with the aforementioned standards (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 emails are delivered to the recipient, but the signature is removed centrally beforehand. The signature certificate of the external communication partner contained in the message cannot be used to encrypt messages. The certificates from external communication partners are stored in the Federal Employment Agency
managed exclusively via the **address book for external contacts .**

Messages sent from the Federal Employment Agency are not signed via S/MIME. As a replacement, all emails from the Federal Employment Agency will be given a DKIM signature.

5.6 News for technical contacts

Would you like to be informed about technical changes to email encryption, for example if you change CA? We would be happy to register you as a technical contact in our system.

To do this, please send the following information to IT-Systemhaus.Vertrautsdienste@arbeitsagentur.de:

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

Information about technical contacts[1]:

- First and Last Name
- Email address (personal)
- Email address of the area/team (if available)
- Telephone number

5.7 Sending encrypted messages from the

Federal Employment Agency ÿ to external communication partners

The Federal Employment Agency uses the address book system for external contacts to provide and manage certificates for exchanging encrypted emails .

The invitation process in the **address book for external contacts** is divided into the following steps:

1. Internal initializes the invitation
2. Data collection & upload of the certificate
3. Internal receives an email to review/approve the contact
4. Internal checks the contact details
5. Contact details are approved internally, rejected for revision or discarded.

ℹ Once the external contact has been released, it will be available to everyone internally in the external contacts address book.

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

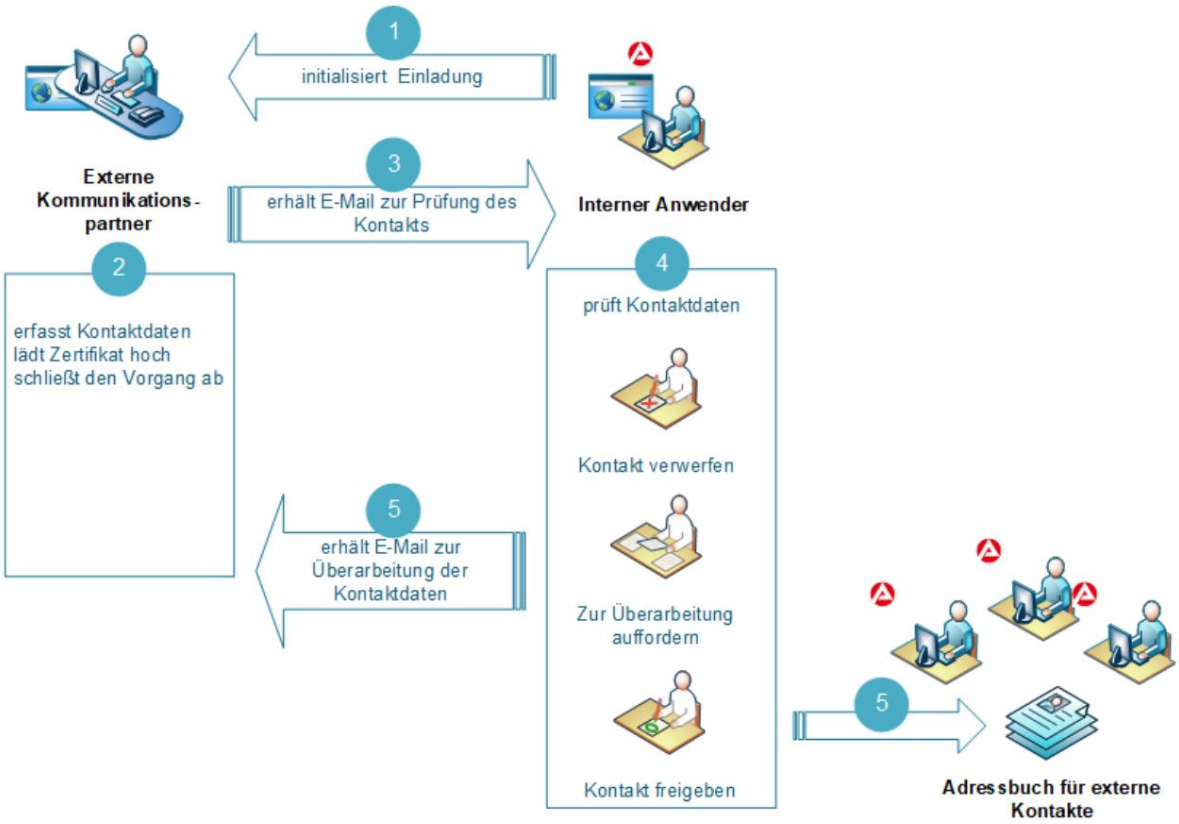

Figure 6 - Invitation Process - Address Book for External Contacts

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 we can set up with you to provide your certificates and data. These settings can also be combined with each other.

5.7.2 Independently by the invited external communication partner

The external communication partner records his contact details, uploads his **personal certificate** for encrypting emails and completes the process (see also 3.4).

5.7.3 Substitute processing of all invitations by an administrative team E-mail address

If you, as the technical contact, receive all invitations for your email domain and want to maintain the certificates and contact information, an email address you specify can be set up as an administrative email address. The actually invited contacts (your users) receive an overview of the stored data (according to GDPR) via email. The stored administrative email address will be communicated to your users.

To set up an administrative email address, please send the following information to: IT-Systemhaus.Vertrautsdienste@arbeitsagentur.de

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

Details of technical contacts2:

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

Field label	Desired value
company	*optional*
Street, house number	*optional*
Postal code	*optional*
City	*optional*

Table 1 - desired defaults for all invitations (administrative email Address)

*The administrative email address specified will receive all invitations for the specified email domain.

2 This information is 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 pre-assign this certificate for the entire email domain in our address book for external contacts. This has the advantage that not all users have to upload a personal certificate. The invitation process must be carried out despite the domain certificate.

⚠ The domain certificate feature must be supported by your encryption gateway.

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

- Your domain certificate in a ZIP archive (without password protection)
- Email domain(s) for which the domain certificate is to be used
- Name of the company/authority for which the certificate is being set up
- Product name of your encryption gateway, if your security policy allows it.

Information about technical contacts:3

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

Field label	Desired value	Changeable by your users (yes/no)?
company	*optional*	
Street, house number	*optional*	
Postal code	*optional*	
City	*optional*	
certificate	Your domain certificate will be pre-populated	

Table 2 - desired defaults for all invitations (domain certificate)

3 This information is used to contact you in case of technical problems, to inform you about the expiration of your domain certificate or to inform you about 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 are regularly updated in the address book for external contacts.

To connect your LDAP directory, please send the following information to: IT-Systemhaus.Vertrautsdienste@arbeitsagentur.de

- Your email 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 3 - technical specifications of the LDAP directory

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

Information about technical contacts:4 –

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

Field label	**Desired value**	**Changeable by your users (yes/ no)?**
company	*optional*	
Street, house number	*optional*	
Postal code	*optional*	
City	*optional*	

Table 4 - desired defaults for all invitations (LDAP directory)

To fully automate the invitation process for your users, your LDAP directory must provide all required mandatory fields. These are: first name, last name, certificate, telephone number, zip code and city

4 This information is 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 parties

Communication partners ÿ to the Federal Agency for Work

5.8.1 Manual retrieval of the encryption certificates from the Federal Agency for Work

see chapter 3.1.

5.8.2 Automated retrieval of encryption certificates Federal Employment Agency via LDAP

In order to send encrypted messages to the Federal Employment Agency using an encryption gateway, we offer you the option of setting up access to our LDAP directory service.

Send us to IT-Systemhaus.Vertrautsdienste@arbeitsagentur.de the following information to order your access:

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

Information about technical contacts:5 –

- First and Last Name
- Email address (personal)
- Email address of the area/team (if available)
- Telephone number.

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

5.8.3 Domain certificate from the Federal Employment Agency

⚠ The Federal Employment Agency only provides personal email addresses for all email addresses certificates. A domain certificate for the email domains of the Federal Employment Agency @arbeitsagentur.de; @jobcenter-ge.de or iab.de is **not** provided.

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

List of illustrations

Figure 1 - Find Encryption Certificate..... ..... 7 Figure 2 - Issuer certificates .... 8 Figure 3 - Email notification: "Invitation for email encryption" .... 9 Figure 4 - Edit contact details .... 10 Figure 5 – Certificate manager certmgr.msc..... ..... 11 Figure 6 - Invitation Process - Address Book for External Contacts..... 14

Table directory

Table 1 - desired defaults for all invitations (administrative email address) ..... 15 Table 2 - desired defaults for all invitations (domain certificate) 16
Table 3 - technical data of the LDAP directory..... 17
Table 4 - desired defaults for all invitations (LDAP directory)..... 17