

Trust service provider of the Federal Employment Agency | 25.02.2022

E-mail encryption for external communication partners





Impressum

OPS4 - IT-Systemhaus

Trust service provider of the Federal Employment Agency

Regensburger Str. 104

D-90478 Nürnberg

Contents

Contents	3
1 General	4
1.1 Why should e-mail encryption be used?	4
2 Requirements	5
2.1 What do I need for e-mail encryption?	5
2.2 Where can I get a certificate for my e-mail address?	5
3 Exchanging encrypted e-mails	6
3.1 How can I obtain my correspondent's certificate?	6
3.2 Installing the certificates in Outlook	7
3.2.1 Downloading the required files	7
3.2.2 Importing issuer /CA certificates	7
3.2.3 Importing the contact and sending an encrypted e-mail	8
3.3 Receiving encrypted e-mails	8
3.4 Entering contact data and uploading your certificate	8
4 Help for Troubleshooting	10
4.1 Importing your .p12- or .pfx file	10
4.2 Exporting your certificate as a .cer file	10
4.3 Outlook error message: encryption problems	10
5 Information for technical IT services	11
5.1 Use of your own PKI infrastructure	11
5.2 Validation of the BA issuer certificates	11
5.3 Supported standards	11
5.4 S/MIME signature	11
5.5 Sending encrypted messages from the Federal Employment Agency → to external communication partners	12
5.5.1 Options for providing your certificates and data as part of the invitation process.	13
5.5.2 Independent processing by the invited external communication partner	13
5.5.3 Representative processing of all invitations via an administrative e-mail address	13
5.5.4 Domain certificate (encryption gateway)	14
5.5.5 LDAP directory	15
5.6 Sending encrypted messages from external communication partners → to the Federal Employment Agency	16
5.6.1 Obtaining the Federal Employment Agency's encryption certificates manually	16
5.6.2 Obtaining the Federal Employment Agency's encryption certificates automatically via LDAP	16
5.6.3 Federal Employment Agency's domain certificate	16
Index of figures	17
Index of tables	18

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:

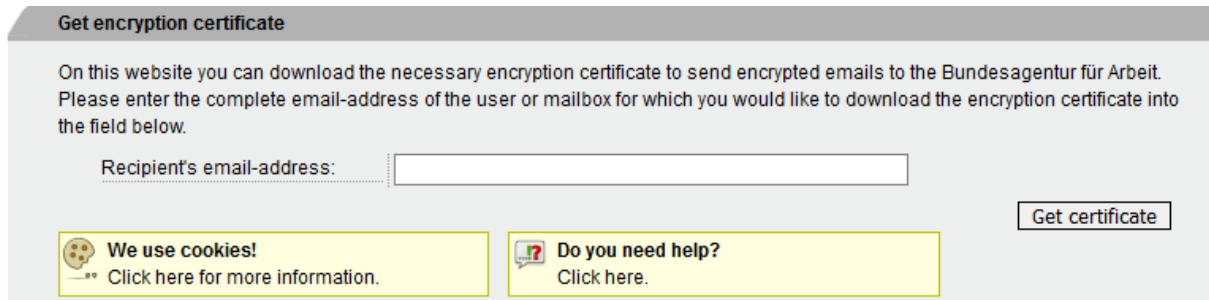
- Certificate creation in adherence with the X.509 V3 standard.
- The e-mail address entered in the certificate (SubjectAltName) must match your e-mail address (at least a class 1 certificate).
- The (Extended) Key Usage must contain
 - for RSA certificates the attributes "keyEncipherment" and/or "emailProtection".
 - 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.



The screenshot shows a web form titled "Get encryption certificate". The form contains the following elements:

- A header bar with the text "Get encryption certificate".
- Introductory text: "On this website you can download the necessary encryption certificate to send encrypted emails to the Bundesagentur für Arbeit. Please enter the complete email-address of the user or mailbox for which you would like to download the encryption certificate into the field below."
- A text input field labeled "Recipient's email-address:".
- A "Get certificate" button.
- Two yellow informational boxes at the bottom:
 - "We use cookies! Click here for more information."
 - "Do you need help? Click here."

Figure 1 - searching for an encryption certificate

 If you do not receive a result for a specific email address, please contact your contact person in the Employment Agency or Job Center. Possibly the email 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:

Get encryption certificate

For the entered email-address <BA e-mail address> the following encryption certificates could be found:



Mailbox <Surname>, <Givenname>
<BA e-mail address>



[Download certificate](#)

Use this if you already have downloaded certificates from the Bundesagentur fuer Arbeit. If necessary you have to download the issuer certificates supplied below.



[Download certificate and issuer certificates packaged as a PKCS7 structure](#)

Contains all the necessary information to install the certificate as a trusted certificate.



[Download information as VCARD file](#)

Contains an electronic business card that can be imported into your email client. If necessary you have to download the issuer certificates supplied below.



[Download certificate and issuer certificates packaged as a ZIP file](#)

Contains the certificate and all issuer certificates within one compressed ZIP file.

Issuer certificates

This download contains the issuer certificates used by the Bundesagentur fuer Arbeit. If you have not used the PKCS7 or ZIP download option and have not communicated with the Bundesagentur fuer Arbeit before you should download and install this certificates.



[Download issuer certificates packaged as a PKCS7 structure](#)

Contains all the necessary information to install the issuers and make the downloaded certificates trustworthy.



[Download issuer certificates packaged as a ZIP file](#)

Contains all the necessary information to install the issuers and make the downloaded certificates trustworthy.

Figure 2 - issuer certificates

You can obtain the certificate in various file formats:

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

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.

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


3.2.2 Importing issuer /CA certificates

Unpack the ZIP file and the item **BA-Class-1-Root-CA-3.cer** that it contains.

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

Select **Next**, **Finish** and **OK**.

Open the **BA-VPS-CA-3.cer** item and select **Install Certificate**. Then click twice on **Next** and then **Finish**.

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

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 IAB 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 to send you encrypted e-mails, your own certificate is required. Ask your contact person to send you an invitation to e-mail encryption. The invitation will be sent to you via e-mail:

Subject: Invitation for email encryption

Dear Madam,

Dear Sir,

an employee of the Federal Employment Agency (Bundesagentur für Arbeit) would like to exchange encrypted emails with you. In order to do so we need your e-mail encryption certificate.

To make this as easy as possible for you, there is a website where you can enter your contact information and upload your certificate. Please use the link below to start:

[<Link to Entering and modifying contact data>](#)

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

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

Figure 3 - 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:

Modify contact data

We use cookies!
Click here for more information.

Do you need help?
Click here.

Please enter your contact details and upload your certificate.
 PEM and DER coded certificates (in Windows with the file extension .cer) are supported.

General information

Givenname¹:

Surname¹:

Company:

Organisational unit:

Department:

Job title:

Certificate

Certificate¹: Keine Datei ausgewählt

Contact details

E-Mail²:

Telephone number¹:

Mobile telephone number:

Address

Street/House number:

Zipcode¹:

City¹:

Language

Language for E-Mails:

Technical data

Unique ID²:

¹ mandatory fields
² globally assigned. Can not be changed.

Figure 4 - editing contact information

Complete at least the mandatory fields like **Givenname**, **Surname**, **Telephone number**, **Zipcode** and **City** and click on 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 on 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**.

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 PC. 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 importation 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** → **Certificates** and select yours.

Right-click your certificate and select **All Tasks** → **Export**.

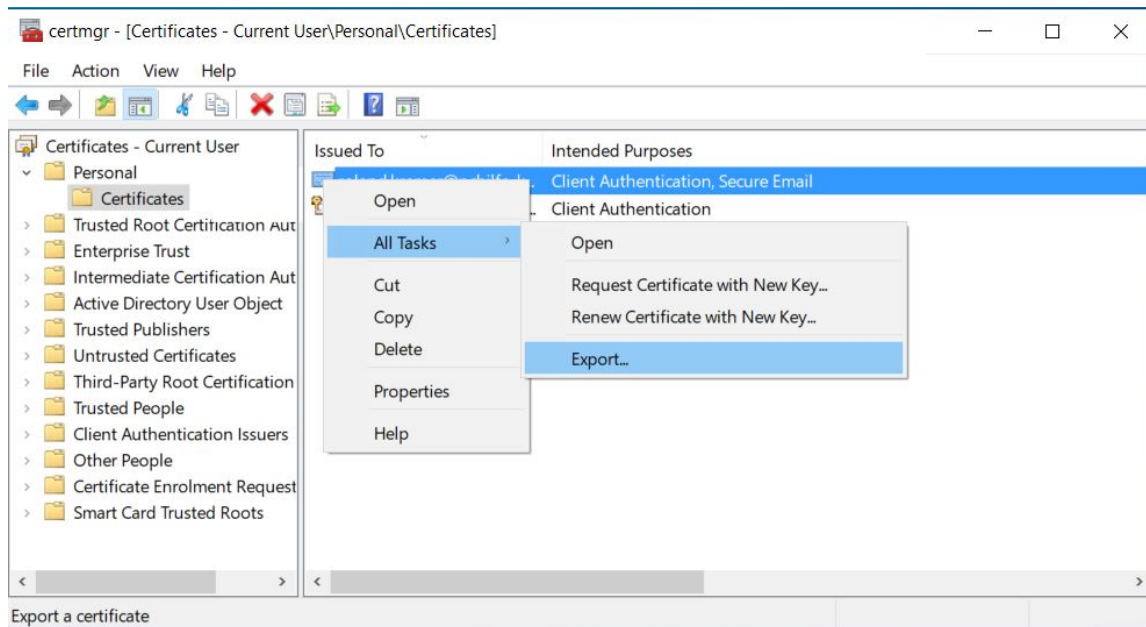



Figure 5 – Certmanager certmgr.msc

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 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.

5.2 Validation of the BA issuer certificates

The end user certificates and the appropriate issuer certificates 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 <http://www.pki.arbeitsagentur.de/CertList>.

5.3 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.

The following encryption algorithms and key lengths are at least supported:

AES with 256 bit and 128 bit key

3DES (with CBC) with 168 bit 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.

5.4 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 emails are provided a DKIM signature.

5.5 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.

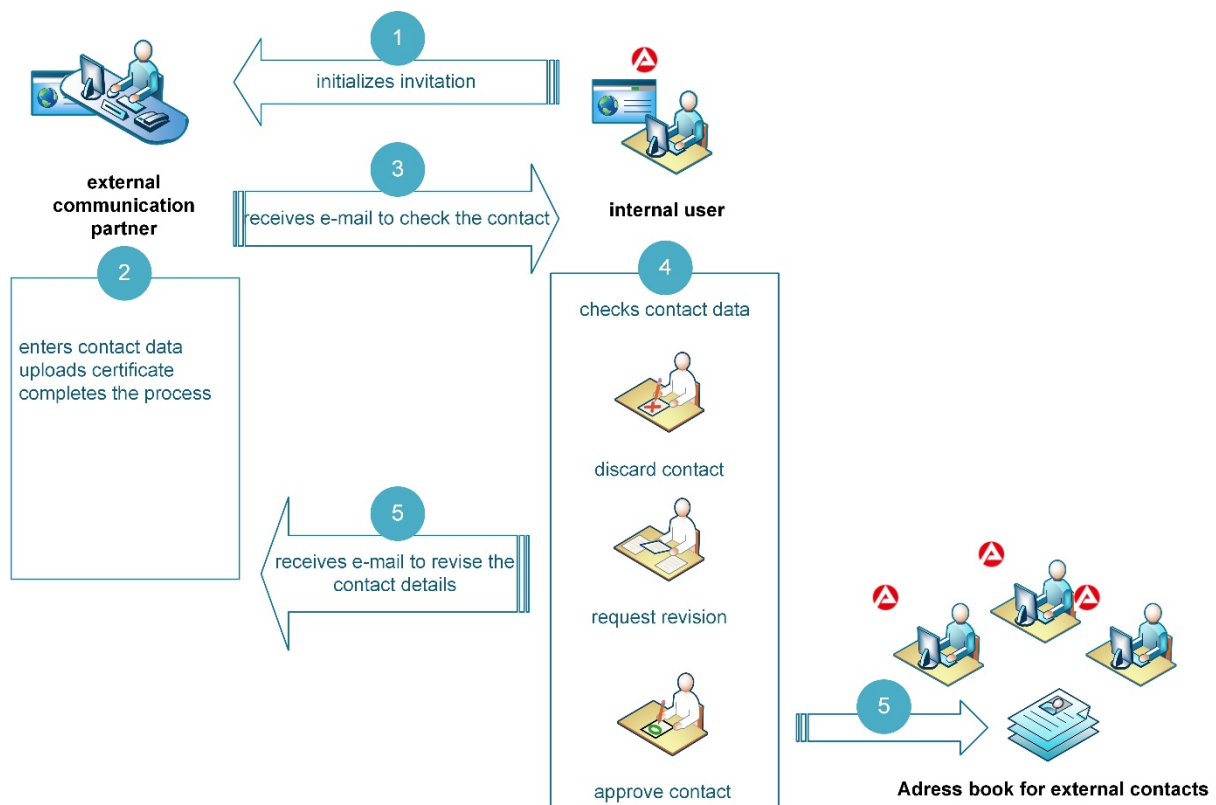


Figure 6 - Invitation process – address book for external contacts

5.5.1 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.

5.5.2 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).

5.5.3 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 information¹:

- 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	<i>optional</i>
Street/House number	<i>optional</i>
Zip code	<i>optional</i>
City	<i>optional</i>


Table 1 - desired defaults for an administrative e-mail address

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

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.

5.5.4 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)
- 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: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	Can be changed by your users (yes/no)?
Company	<i>optional</i>	
Street/House number	<i>optional</i>	
Zip code	<i>optional</i>	
City	<i>optional</i>	
Certificate	Your domain certificate will be preset	

Table 2 - desired defaults for domain certificates

² 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.

5.5.5 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):	<i>optional</i>
Password (bind password):	<i>optional</i>
Search base (base DN):	e.g. ou=certificates

Table 3 - Technical data of the LDAP directory

- Further fields to be queried:
- givenName, surname, etc.
- 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	<i>optional</i>	
Street/House number	<i>optional</i>	
Zip code	<i>optional</i>	
City	<i>optional</i>	

Table 4 - desired defaults for the LDAP directory

i In order to fully automate the invitation process for your users, your LDAP directory must provide all required mandatory fields. These are: givenname, surname, certificate, telephone number, zipcode and city

³ 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.

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

5.6.1 Obtaining the Federal Employment Agency's encryption certificates manually

see chapter 3.1

5.6.2 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.

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


- 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:⁴

- 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.

5.6.3 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.

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.

Index of figures

- Figure 1 - searching for an encryption certificate 6
- Figure 2 - issuer certificates 7
- Figure 3 - e-mail notification: "Invitation for email encryption" 8
- Figure 4 - editing contact information 9
- Figure 5 – Certmanager certmgr.msc 10
- Figure 6 - Invitation process – address book for external contacts 12

Index of tables

- Table 1 - desired defaults for an administrative e-mail address..... 13
- Table 2 - desired defaults for domain certificates..... 14
- Table 3 - Technical data of the LDAP directory..... 15
- Table 4 - desired defaults for the LDAP directory 15