Information on activating a certificate for a.sign RK HSM

1 Requirements

- a.sign RK HSM is reachable in your network and the IP address is known.
- Access to A-Trust webshop (<u>https://www.a-trust.at/shop</u>)

The HSM is delivered with a large number of pre-generated keys (open key labels), these keys cannot be used without a certificate. To issue a certificate for a classification key (VAT-ID, GLN, ...), the following steps must be taken:

Certificate issuance is a two-step process: first, you have to generate a certificate request (certificate signing request) on the HSM. Next, you have to upload the request file into the A-Trust web shop. Finally, you have to import the result file from the web shop into the HSM.

2 Create a new certificate (manually)

2.1 Creating a certificate request

Open the a.sign RK HSM website by entering its IP address in the web browser.

Select the menu item Issue Certificates. The figure below shows this function highlighted in blue.



On the following page the data which will appear in the a.sign RK HSM certificate is entered. The certificate type is selected from the dropdown menu **Classification Key**. The choices available are: Value-Added Tax Identification Number (VAT-ID), Global Location Number (GLN), and Tax Number. Additionally, the adjacent text field must be filled with the value corresponding to the type. This field simple validation checks to ensure that the format is correct.

After entering the E-Mail address the certificate request can be generated via the button **Issue Certificate (manually)**.

| | Home | Issue Certificate | Inventory | Maintenance | Resources & Documents |
|------------------------------------|------------------|---------------------|-----------------|---------------|-----------------------------|
| Issue Import | | | | | |
| ssue new certificate | | | | | |
| Open keylabels | | | | | |
| HGDDMXVPSXJDQAKVJCDSZK | QJZTPBBGNA | T | | | |
| Classication key * | | | | | |
| Tax Identification Number (VAT-II |) • (C | | | | |
| e-Mail Adresse * | | | | | |
| | | | | | |
| Issue certificate (manually) | | | | | |
| | | | 4. 4h - A Tours | | |
| import the issued certificate in t | he "Import" tab. | upioad this request | to the A- Irust | webshop manua | lly. Afterwards you have to |
| | | | | | |
| lesue cortificate (online) | | | | | |
| issue certificate (online) | | | | | |

The value in the field keylabel (here HGDDMX...BGNA) is used to select the key to sign with over the REST interface.

On the next page you see a summary of the certificate request and can download it. Click on **Donwload export file** to download the certificate request.

| | | а | Language: english V char .sign RK HSM |
|---|---------------------------------------|-----------------------|--|
| infach sicher | Home Issue Certificate | Inventory Maintenance | Resources & Documents |
| New certificate prepared | | | |
| Ordnungsbegriff UID-Nummer: ATU12345678 | | | |
| e-Mail: test@test.com | | | |
| Download export file | | | |
| <u>a.sign RK HSM - user manual (german) a.sign RK HSM - user manual (english)</u> | | | |
| 00 2016 A Truct Gacallechaff für Sicharbaitesustame | a im alaktranischan Datanvarkahr GmbH | | |

2.2 Issuing a certificate in the A-Trust Webshop

Use your login credentials to sign in to the A-Trust Webshop (<u>https://www.a-trust.at/shop</u>). In the following screenshot the sign-in functions are marked in blue. You can use either of these to login.



After successful login, the menu item **a.sign RK HSM** becomes visible (marked in blue in the screenshot) on the left-hand side under **Konto Bereich**. Select this menu item to start issuing a certificate.



On the following page, choose the certificate request you created earlier and then click on the button **Exportdatei laden**.

| C TRUST | Einkaufskorb Sie haben keine Artikel im Korb. zur Kasse |
|--|--|
| einfach sicher | Kontrast Schwarz/Gelb Aa aA |
| <u>Startseite A-Trust Homepage a.sign RK C</u> | ONLINE ausstellen Abmelden |
| Konto | Neues Zertifikat ausstellen (a.sign RK HSM) |
| Zurück zum Webshop | Exportdatei aus dem a sign RK HSM hochladen |
| Übersicht | |
| Passwort ändern | |
| Abmelden | Exportdatei laden |
| a.sign RK ONLINE | |
| Neues Zertifikat ausstellen | |
| Ausgestellte Zertifikate | |
| a.sign RK HSM | |
| Neues Zertifikat ausstellen | |
| © 2000-2016 A-Trust Gesellschaft für Sicherheitsevsteme im | elektronischen Datenverkehr GmbH |

In place of the button, the text **Bitte warten, Anfrage wird bearbeitet** appears. A certificate is now generated. This can take a few seconds. After successful processing you are redirected to the next page automatically.

| C TRUST | Einkaufskorb Sie haben keine Artikel im Korb. zur Kasse |
|--|--|
| einfach sicher | Kontrast Schwarz/Gelb Aa aA |
| Startseite A-Trust Homepage a.sign RK (| ONLINE ausstellen Abmelden |
| Konto | Neues Zertifikat ausstellen (a.sign RK HSM) |
| Zurück zum Webshop | Exportdatei aus dem a.sign RK HSM hochladen |
| Übersicht | Datei auswählen export ZRKOWUQRKTVWBBAWOAKGHWTYUZIEFIFR.ison.sig |
| Passwort ändern | |
| Abmelden | Bitte warten, Anfrage wird bearbeitet |
| a.sign RK ONLINE | |
| Neues Zertifikat ausstellen | |
| Ausgestellte Zertifikate | |
| a.sign RK HSM | |
| Neues Zertifikat ausstellen | |
| © 2000-2016 A-Trust Gesellschaft für Sicherheitssysteme in | n elektronischen Datenverkehr GmbH |

On the following page load the certificate data using the button **Download Zertifikatsdaten**. This data will be required in the next step where you load it into your HSM.

| A TRUST | Einkaufskorb Sie haben keine Artikel im Korb. zur Kasse |
|--|---|
| einfach sicher | Kontrast Schwarz/Gelb Aa aA |
| <u>Startseite A-Trust Homepage a.si</u> ç | n RK ONLINE ausstellen Abmelden |
| Konto | Zertifikatsdaten für a.sign RK HSM |
| Zurück zum Webshop | Bitte heben Sie sich die Zertifikatsdaten umbedingt auf, diese können nicht |
| Übersicht | wiederhergestellt werden. |
| Passwort ändern | Download Zertifikatsdaten |
| Abmelden | |
| a.sign RK ONLINE | |
| Neues Zertifikat ausstellen | |
| Ausgestellte Zertifikate | |
| a.sign RK HSM | |
| Neues Zertifikat ausstellen | |
| ⊉ 2000-2016 A-Trust Gesellschaft für Sicherheitssy | steme im elektronischen Datenverkehr GmbH |

2.3 Import Certificate Data into a.sign RK HSM

Navigate to the a.sign RK HSM page and select the menu item Issue Certificate. This is shown marked in blue in the following screenshot.

| | | | | | а | Language: english V change |
|--|----------------------------|------|-------------------|-----------|-------------|----------------------------|
| einfach sicher | | Home | Issue Certificate | Inventory | Maintenance | Resources & Documents |
| a.sign RK HSM licensed for: | | | | | | |
| | | | | | | |
| A-Trust | G | mbl | н | | | |
| A-Trust | G | mb | н | | | |
| A-Trust Partner ID: RK00 | Gr | mbl | H | | | |
| A-Trust Partner ID: RK00 | Gr | mbl | H | | | |
| A-Trust Partner ID: RK000 | Gr 00 96 | mb | Η | | | |
| A-Trust Partner ID: RK000 Number of available certificates Number of used certificates | G 00 96 13 | mb | Η | | | |
| A-Trust Partner ID: RK000 Number of available certificates Number of used certificates Number of unused certificates | G r 00 | mb | Η | | | |

On the next page choose the menu item Import. This is shown marked in blue in the following screenshot.

| A | Language: english 🔻 | change |
|---|--|--------|
| TRUST | a.sign RK HS | М |
| einfach sicher | Home Issue Certificate Inventory Maintenance Resources & Documents | 5 |
| Issue Import | | |
| Import new certificate | | |
| Import file from A-Trust webshop Choose Files No file chosen | | |
| Import certificates | | |
| | | |
| © 2000-2016 A-Trust Gesellschaft für Sicherheitssyster | im elektronischen Datenverkehr GmbH | |

On the next page choose the certificate file you generated in section 2.2 and then click on the button **Import certificates**.

| A | | | Language: english V change |
|--|--|-----------------------|----------------------------|
| TRUST | | ; | a.sign RK HSM |
| einfach sicher | Home Issue Certificate | Inventory Maintenance | Resources & Documents |
| Issue Import | | | |
| Import new certificate |) | | |
| Import file from A-Trust websho Choose Files import_HGDDM | י ף « «VPSXJDQAKVJCDSZKQJZTPBBGNA.jso | n | |
| Import certificates | | | |
| | | | |
|) 2000-2016 A-Trust Gesellschaft für Sicherhe | itssysteme im elektronischen Datenverkehr Gmbł | ł | |

©A-Trust GmbH 2016

If the import is successful you will see the following screen. The certificate with the given keylabel is now operational.

| A | | | | Language: english V change |
|--|-----------------------------------|---------------------|---------------------|----------------------------|
| TRUST | | | a | .sign RK HSM |
| einfach sicher | Home Issue Certif | Inventory | Maintenance | Resources & Documents |
| Import succeeded! | | | | × |
| Zertifikatsdetails | | | | |
| Key label: | | CIN: | | |
| HGDDMXVPSXJDQAKVJCDSZKQJZTF | PBBGNA | 302209822881 | | |
| State: | | CSN: | | |
| aktiviert | | 1 | | |
| Classification key: | | Serial number of s | igning certificate | (hexadecimal): |
| UID-Nummer: ATU12345678 | | 3EED435D | | |
| e-mail address: | | Serial number of s | igning certificate | (decimal): |
| test@test.com | | 1055736669 | | |
| | | ZDA ID: | | |
| | | AI 1 | | |
| | | | | |
| Download signature certificate Download | d cetificate chain (DEP format) | Download cetificate | e chain (PEM format | |
| Test Europtionen | | | | |
| | | | | |
| Test signature | | | | |
| | | | | |
| © 2000 2016 A Truck Cocollocheft für Sichart - the state | me im elektronischen Determeter | Cmbl | | |
| © 2000-2010 A-Irust Gesenschalt für Sicherheitssyste | me im elektronischen Datenverkenr | Gillon | | |

3 Create a new account (automatically)

If your a.sign RK HSM has internet access, certificates can be issued using the following simplified process.

Navigate to the a.sign RK HSM website by entering the IP address of your HSM in your web browser – this may have the form <u>http://192.168.1.1/</u> – where of course you must enter the IP address of your HSM.

Select the menu item Issue Certificate. This is marked in blue in the following screenshot.



On the following page the data which will appear in the a.sign RK HSM certificate is entered. The certificate type is selected from the dropdown menu **Classification Key**. The choices available are: Value-Added Tax Identification Number (VAT-ID), Global Location Number (GLN), and Tax Number. Additionally, the adjacent text field must be filled with the value corresponding to the type. This field simple validation checks to ensure that the format is correct.

After entering the E-Mail address the certificate request can be generated via the button **Issue certificate (online)**.

| infach sicher | Home Issue Certificate Inventory Maintenance Resources & Documents |
|--|--|
| Issue | |
| SSUE NEW CERTIFICATE | • |
| JAAGXDSFXQIEMPOXANQUL | RYIMSJZVZIL • |
| Classication key * | |
| Tax Identification Number (VAT | T-ID) • ATU12345678 |
| e-Mail Adresse * | |
| test@a-trust.at | |
| Issue certificate (manually) A certificate request will be ge import the issued certificate in | enerated, you have to upload this request to the A-Trust webshop manually. Afterwards you have to n the "Import" tab. |
| Issue certificate (online) | actly to the A.Trust webshop and issues and installs the certificate automatically. An internet |
| The HAM conver connects dire | ectly to the A-irust webshop and issues and installs the certificate automatically. An internet |

The screen now shows the message **Please wait, work in progress...** The processing can take a number of seconds.

| nfach sicher | Home | Issue Certificate | Inventory | Maintenance | Resources & Documents |
|--|---|--|----------------|------------------------------------|---|
| Issue | | | | | |
| ssue new certificate | • | | | | |
| Open keylabels | | | | | |
| JAAGXDSFXQIEMPOXANQU | LRYIMSJZVZIL • | | | | |
| Classication key * | | | | | |
| Tax Identification Number (VA | T-ID) • | ATU12345678 | | | |
| e-Mail Adresse * | | | | | |
| test@a-trust.at | | | | | |
| A certificate request will be g import the issued certificate i The HSM server connects dir connection is required. | enerated, you have to u n the "Import" tab. ectly to the A-Trust we | upload this request t bshop and issues ar | to the A-Trust | webshop manua certificate autom | lly. Afterwards you have to natically. An internet |

Finally the certificate details screen is shown. The certificate has now been issued and the account can be used.



4 Inventory



The taskbar item Inventory provides an overview of all keys (keylabels). Issued certificates together with their corresponding classification keys (e.g. ATU12345678) can be seen. It is also possible to filter according to predefined search terms, or to see how many keys are still available.