A-Trust GmbH
Landstraßer Hauptstraße 1b
The Mall E02
A-1030 Wien

https://www.a-trust.at
E-Mail: office@a-trust.at

Tel: +43 (1) 713 21 51 - 0
Fax: +43 (1) 713 21 51 - 350

a.sign RK HSM
Administrators Manual

Version: 1.0
Date:

Contents

Datum	**Rev**	**Autor**	**Änderungen**
11.12.2024	1.0	A. Kopp-Konopka	Aktualisierung Vorlage Anpassung nginx Config Anpassung Services
19.08.2022	0.8	A. Kopp-Konopka	Anpassung Netzwerkkonfiguration
22.02.2017	0.7	Patrick Hagelkruys	Anpassung Monitoring URL
14.09.2016	0.6	Patrick Hagelkruys	Englische Übersetzung hinzugefügt
29.08.2016	0.5	Daniel Kovacic Patrick Hagelkruys	Überarbeitung der Texte Kapitel Anmeldung in Finanzonline
26.08.2016	0.4	Patrick Hagelkruys Ramin Sabet	Überarbeitung der Texte Erweiterung FAQ
26.08.2016	0.3	Daniel Kovacic Patrick Hagelkruys	Kapitel Administrations-Webseite Kapitel REST-Schnittstelle Anhang nginx Konfiguration Kapitel Überwachung
11.08.2016	0.2	Patrick Hagelkruys	FAQ hinzugefügt
12.07.2016	0.1	Patrick Hagelkruys	Erste Version

Table 1: Document history

1. Overview

1.1. Summary

This document describes the a.sign RK HSM software, the individual processes and their interaction.

2. Administrators web interface

This web site is used for administration of the a.sign RK HSM and provides the following functions

- Issue and management of certificates
- Display server state
- Diagnostics options
- Resources and Documents

The administration web interface of the a.sign RK HSM is only reachable via TLS encrypted connection and protected with password authentication.

URL: `https://<ip_address_of_server>/`

User: admin

Password: produced individually for each customer

2.1. SSL certificate

The SSL certificate of the administration web interface is a self-signed certificate generated for each customer. This certificate is by default not trustworthy in any browser and must explicitly be imported as a trusted certificate.

3. REST interface

The REST interface is used by the respective client or the cash register to perform the signature of the receipt on the HSM.

The REST interface is available over HTTPS (TLS secured connection) and **access is limited via username and password**. Furthermore, it is recommended that self-signed certificates are pinned on the client (see [Ope16]).

3.1. Configuration for Internet and untrusted networks

To change the REST interface the following steps need to be carried out.

1. **Logon to the Linux server**
   The administrator must log in with the user `root` and supply the password delivered by A-Trust.
2. **Create user and passwords for accessing REST interface**
   The following command creates a new user. The `[user]` defines the username, the password is requested in the terminal.

   ```
   htpasswd /etc/nginx/.htpasswdapi [user]
   ```

   The following command deletes an existing user. The `[user]` defines the username.

   ```
   htpasswd -D /etc/nginx/.htpasswdapi [user]
   ```

4. Processes and communication in a.sign RK HSM

Figure 1 shows all processes and their communication with each other. The outer grey area represents the server, the blue boxes the individual processes.

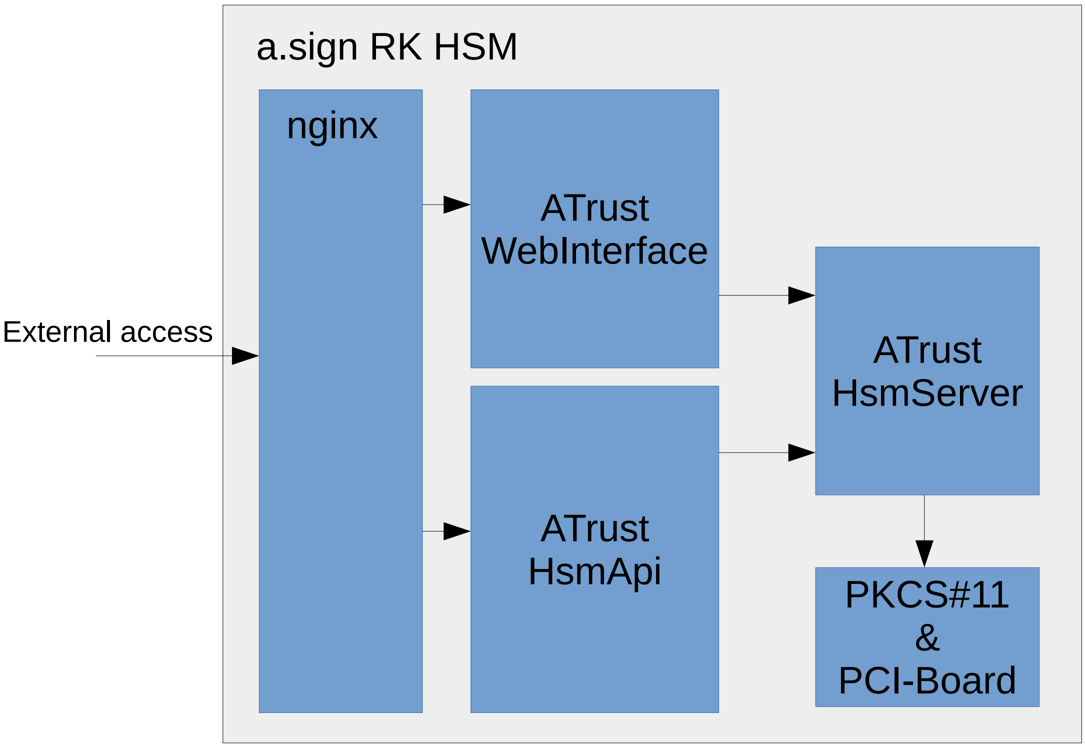


Figure 1: Overview of processes and communication

4.1. Description of the processes

nginx: nginx (https://nginx.org/en/) is an HTTP server and reverse proxy, which serves as external interface of the server. Any communication from outside is sent to nginx, which forwards the requests to the appropriate internal systems.

ATrustHsmWeb: Website for managing certificates and keys of the HSM.

ATrustHsmApi: REST-API interface for accessing the certificates and key of the a.sign RK HSM. A description of the interface is provided in [Hag16].

ATrustHsmServer: Server for internal key management and signatures, interface to the HSM hardware.

HsmKeystoreWatcher: Service for synchronization of multiple redundant a.sign RK HSM servers.

PKCS#11 & PCI-Karte: Drivers and hardware components of the HSM.

ATrustLogService: Receives log-lines from all services.

4.2. Basic data about the processes

4.2.1. manage services

start: `systemctl start` *name*

status: `systemctl status` *name*

stop: `systemctl stop` *name*

4.2.2. important log directories

ATrust Services: `/var/log/atrust/`

nginx: `/var/log/nginx/`

5. Network

The network card of the server operates in the configuration **Network Bonding** (see [Can22]). The configuration file for Network Bonding is listed below.

network configuration: `/etc/netplan/network-config.yaml`

5.1. Operating multiple a.sign RK HSM Server

When ordering multiple a.sign RK HSMs, these are provided as independent servers with the same key material. Issued certificates are automatically synchronized with the other servers. Configuration for load balancing must be configured by the customer. This can be done either by an upstream load balancer, DNS round robin or implementation in the client software.

5.2. Changing the IP address

If the IP address of one server changes, the hosts file of every server must be updated to reflect the configuration of the network interfaces.

An administrator will need to udpate the hosts file (`/etc/hosts`) on the a.sign RK HSM server.

Data transmission takes place via an encrypted SSH connection between the servers. Therefore the server must be able to communicate on port 22. For authentication purposes ed25519 key pairs are used. These keys should be redistributed after reconfiguration of a server.

To generate a new key pair on an a.sign RK HSM server, the following commands need to be executed in the terminal on the server.

```
chmod 640 .ssh/authorized_keys
ssh-keygen -t ed25519
```

To store the public key to another a.sign RK HSM, the following command must be run in a terminal on the server. This step must be repeated for each server.

```
ssh-copy-id root@HOST-DES-ANDEREN-SERVERS
```

The successful key exchange can be checked using the following command. If **no** password is required during the login, then the key exchange was successful.

```
ssh root@HOST-DES-ANDEREN-SERVERS
```

6. Monitoring

The a.sign RK HSM provides an interface for automatic monitoring. This is accessible via the following link: https://<a_sign_RK_HSM_IP>/api/Status.ashx.

Access to the Status.ashx page is secured by username and password. For the authentication the user and password of the administration's website is to be used. (See section 2)

The overall status of a.sign RK HSM is expressed via the HTTP status code. An HTTP status code of **200** is a **fully functional server**. An HTTP status code of **500** corresponds to a server in **error condition**.

For both HTTP status codes a JSON message is returned with the following format:

```
{
  "Services": [
    {
      "Name": "ATrustHsmApi",
      "Load": "loaded",
      "Active": "active",
      "Sub": "running",
      "OK": true
    },
    {
      ...
    },
    ...
  ],
  "DiskSpaceEntries": [
    {
      "FileSystem": "/dev/mapper/ubuntu--vg-ubuntu--lv",
      "Size": "137906712",
      "Used": 13,
      "Available": "113889048",
      "UsePercent": "13%",
      "MountedOn": "/"
    },
    {
      ...
    },
    ...
  ],
  "Warnings": [],
  "UpTime": "3 weeks,3 days,23 hours,23 minutes",
  "CpuUsage": 2,
  "MemUsage": 20,
  "OverallStatus": true,
  "TestSignature": true
}
```

Line 2: List of HSM Services and there state

Line 15: List of Mount points with their size and available space

Line 29: If an error occurs, the error messages are listed here.

Line 30: Uptime of server

Line 31: Current CPU usage in percent

Line 32: Current memory usage in percent

Line 33: Overall state of server, same as HTTP status code

Line 34: State of test signature

6.1. Calculation of overall state

The overall status is calculated from the various tests.

- Each service must have the state `loaded /active /running`, otherwise it is considered to be in the error state.
- The free disk space must be more thean 10%.
- The CPU and memory usage must be below 95%.
- The test signature must be successful.
- The server uptime is ignored for the overall calculation.

7. Registration in Finanzonline

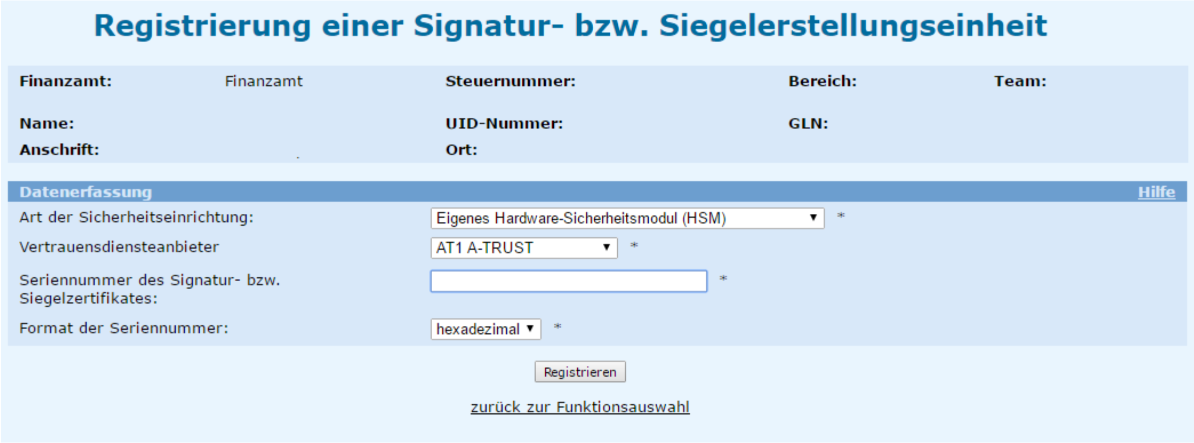
When registering a certificate in FinanzOnline, the following values should be selected:

Art der Sicherheitseinrichtung: (Type of safety device) Select the value „Eigenes Hardware-Sicherheitsmodule (HSM)“ (Custom Hardware Security Modules HSM).

Vertrauensdiensteanbieter: (trust service provider) Select the value „AT1 A-TRUST“.

Seriennummer des Signatur- bzw. Siegelzertifikates: (serial number of signature or seal certificate) certificate serial number from the a.sign RK HSM for the `keylabel`.

Format der Seriennummer: (format of serial number) The website of the a.sign RK HSM displays the format of each serial number indicated, please choose the appropriate value.



Registrierung einer Signatur- bzw. Siegelerstellungseinheit

Finanzamt:	Finanzamt	**Steuernummer:**	**Bereich:**	**Team:**	
Name:		**UID-Nummer:**	**GLN:**		
Anschrift:		**Ort:**			

Datenerfassung

Art der Sicherheitseinrichtung: Eigenes Hardware-Sicherheitsmodul (HSM) *

Vertrauensdiensteanbieter: AT1 A-TRUST *

Seriennummer des Signatur- bzw. Siegelzertifikates: *

Format der Seriennummer: hexadezimal *

Figure 2: Registration in Finanzonline

A. Frequently Asked Questions (FAQ)

A.1. Operating system updates

Per default the server **does not** update automatically. If auto updates are desired, the following steps have to be followed (Kernel will not be updated automatically):

- `systemctl enable apt-daily.timer`
- `systemctl enable apt-daily-upgrade.timer`

Updates are triggered ever 2nd tuesday at 02:00am. A redundant server is offset by 1 week.

To change the time/day of auto updates, the files `/etc/system/systemd/apt-daily.timer` and `/etc/system/systemd/apt-daily-upgrade.timer` have to be edited. Afterwards the command `systemctl daemon-reload` has to be executed.

A.2. Why is Internet access required?

Internet access is needed for the function "Issue certificates (online)".

If no Internet connection is available, the certificates can be issued in an offline process. In this case a file is exported from a.sign RK HSM, and is imported into the webshop. The result from the webshop is re-imported into the a.sign RK HSM.

A.3. What is important when changing the IP addresses?

Automatic synchronization does not work and has to be reconfigured. See chapter 5.2

A.4. SSL/TLS connection to a.sign RK HSM

It is possible to use SSL/TLS to secure the communicate to the a.sign RK HSM. See chapter 2.1 and chapter 3.1

A.5. How can multiple a.sign RK HSM servers be operated in fail-safe mode?

See chapter 5.1

A.6. Number of available certificates

The server comes with pre-generated keys for which the customer can issue certificates. The web interface provides an overview of available, used and unused certificates of the RK-HSM. If the sum of Number of used certificates and Number of unused certificates does not match with the Number of available certificates, then this means that a certificate request was cancelled or not finished.

B. nginx configuration

B.1. Default nginx configuration

In this configuration, both the administration side and the REST interface use HTTPS (SSL/TLS) with password authentication.

```
user www-data;
worker_processes auto;
pid /run/nginx.pid;
include /etc/nginx/modules-enabled/*.conf;

events {
  worker_connections 65535;
}
http {
  ##
  # Basic Settings
  ##
  # information disclosure
  server_tokens off;

  sendfile on;
  tcp_nopush on;
  types_hash_max_size 2048;

  keepalive_timeout 120;

  gzip on;

  include /etc/nginx/mime.types;
  default_type application/octet-stream;

  ##
  # limit number of requests
  #
  limit_req_zone $binary_remote_addr zone=ip:10m rate=1r/s;
  map $status $retry_after {
    default '';
    429 '120';
  }

  ##
  # SSL Settings
  ##

  # https://ssl-config.mozilla.org/#server=nginx
  ssl_protocols TLSv1.2 TLSv1.3;
  ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-CHACHA20-POLY1305;
  ssl_prefer_server_ciphers on; # we want fastest performance on the server

  ##
  # Logging Settings
  ##

  access_log /var/log/nginx/access.log;
  error_log /var/log/nginx/error.log;
  log_format main '$remote_addr - $remote_user [$time_local] "$request" '
                   '$status $body_bytes_sent "$http_referer" '
                   '"$http_user_agent" "$http_x_forwarded_for"';
```

```

##
# Services
##

upstream hsm_server {
  server 127.0.0.1:2002;
}

upstream rkapi {
  server 127.0.0.1:2003;
}

upstream webinterface {
  server 127.0.0.1:9000;
}

# auto redirect 443
server {
  listen 0.0.0.0:80;
  client_max_body_size 20M;
  server_name temp;

  location ~* ^/api/v1/status {
    auth_basic off;
    proxy_pass http://webinterface;
  }

  location / {
    return 301 https://$host$request_uri;
  }
}


server {
  listen 0.0.0.0:443 ssl;
  server_name temp;

  # ssl
  ssl_certificate /etc/nginx/ssl/ssl.crt;
  ssl_certificate_key /etc/nginx/ssl/ssl.key;

  ssl_session_timeout 5m;

  ## https://ssl-config.mozilla.org/#server=nginx
  ssl_protocols TLSv1.2 TLSv1.3;
  ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-CHACHA20-POLY1305;
  ssl_prefer_server_ciphers off;

  proxy_set_header Host $host;
  proxy_set_header X-Real-IP $remote_addr;

  proxy_read_timeout 120;


  location ~* ^/asignrkhsm/ {
    auth_basic "RKHSM API";
    auth_basic_user_file /etc/nginx/.htpasswdapi;

    rewrite "(?i)/asignrkhsm/(.*)" /$1 break;
    proxy_pass http://rkapi;
    #limit_req zone=ip burst=12 nodelay;
    add_header Retry-After $retry_after always;
    }

    location / {
      auth_basic "Administrationsseite";
      auth_basic_user_file /etc/nginx/.htpasswd;
      proxy_pass http://webinterface;
    }

    location ~* ^/api/v1/status {
      auth_basic off;
      proxy_pass http://webinterface;
    }
  }
}
```

Listing 1: Default nginx Configuration

B.2. nginx configuration for trusted networks

If the server is **not** exposed to the internet and is operated on a trusted network, the REST interace and the administration site may be exposed via HTTP without basic authentication

B.2.1. HTTP

To expose the REST interface and the administration site via HTTP, the lines `77-84` have to be replaced with the content of Listing 2

```
        location ~* ^/asignrkhsm/ {
            auth_basic "RKHSM API";
            auth_basic_user_file /etc/nginx/.htpasswdapi;

            rewrite "(?i)/asignrkhsm/(.*)" /$1 break;
            proxy_pass http://rkapi;
            #limit_req zone=ip burst=12 nodelay;
            add_header Retry-After $retry_after always;
        }

        location / {
            auth_basic "Administrationsseite";
            auth_basic_user_file /etc/nginx/.htpasswd;
            proxy_pass http://webinterface;
        }

        location ~* ^/api/v1/status {
            auth_basic off;
            proxy_pass http://webinterface;
        }
```

Listing 2: nginx HTTP Config

B.2.2. Basic Authentication

To disable basic authentication, all lines starting with

- `auth_basic`
- `auth_basic_user_file`

can be deleted

References

[Can22] Canonical Ltd.: *Netplan configuration example*, 2022. https://netplan.io/examples#configuring-interface-bonding, visited on 2022-08-19.

[Hag16] Hagelkruys, Patrick: *a.sign RK HSM Developer Manual*, 2016.

[Ope16] Open Web Application Security Project: *Certificate and Public Key Pinning*, 2016. https://www.owasp.org/index.php/Certificate_and_Public_Key_Pinning, visited on 2016-08-25.