A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr GmbH
Landstraßer Hauptstraße 5
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

(english translation)

Version: 0.6
Date: 16th September 2016

Contents

Datum	Rev	Autor	Änderungen
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
- Synchronization settings
- 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.

As **per default** the REST interface is available over both HTTP and HTTPS (TLS secured connection). This configuration is **sufficient for operation in a trusted local network**.

If the a.sign RK HSM is accessed via **Internet or untrusted networks**, it is necessary to limit the access to **HTTPS only with username/password authentication** (see next section). 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]
   ```

3. **Updating the nginx configuration**

   The nginx configuration must be adapted in a way that the REST interface is only accessible via HTTPS. Therefore the following file is adjusted.
   `/etc/nginx/nginx.conf`

   In the first step, the HTTP interface is forwarded to the HTTPS interface. Therefore the server part for port 80 in the config file must be changed. The result is shown in the following listing.

```
http {
  server {
  listen 80 default_server;
  ...
  location /aSignRkHsm/ {
      return 301 https://$host$request_uri;

      #proxy_pass http://127.0.0.1:2003/aSignRkHsm/;
      #proxy_redirect off;
      #proxy_set_header Host '127.0.0.1';
      #proxy_set_header X-Real-IP $remote_addr;
      #proxy_set_header x-Forwarded-For $proxy_add_x_forwarded_for;
      #proxy_max_temp_file_size 0;
    }
  }
}
```

In the second step, the authentication for the server port 443 part (SSL / TLS) is activated. Therefore two lines are uncommented in this part. The result of the changes is shown in the following listing.

```
http {
  server {
  listen 443 default_server;
  ...
    location /aSignRkHsm/ {
      auth_basic "REST-API";
      auth_basic_user_file /etc/nginx/.htpasswdapi;

      proxy_pass http://127.0.0.1:2003/aSignRkHsm/;
      proxy_redirect off;
      proxy_set_header Host '127.0.0.1';
      proxy_set_header X-Real-IP $remote_addr;
      proxy_set_header x-Forwarded-For $proxy_add_x_forwarded_for;
      proxy_max_temp_file_size 0;
    }
  }
}
```

After saving the changes in the file `/etc/nginx/nginx.conf` the nginx serivce must be restarted. For this the following command is to be executed in the console.

```
systemctl restart nginx
```

The two configuration files are listed in Annex B.

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.

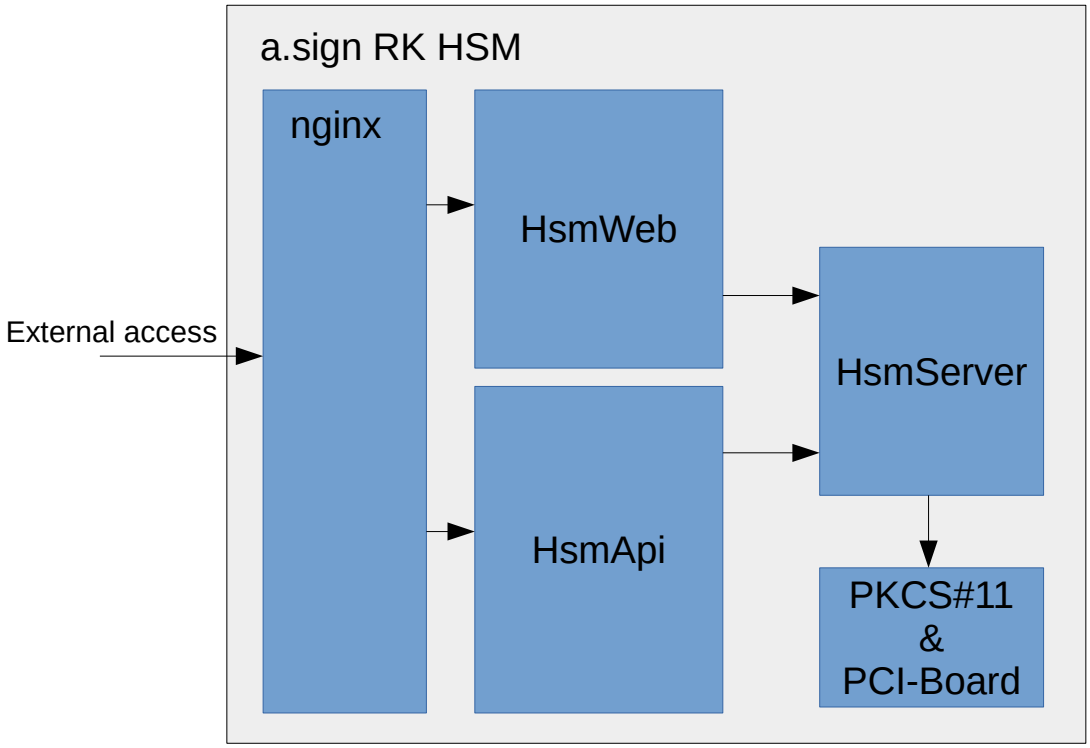

Figure 1: Overview of processes and communication

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.

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

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

HsmServer: 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.

4.2 Basic data about the processes

4.2.1 nginx

Stop service: `systemctl stop nginx`

Start Service: `systemctl start nginx`

Service state: `systemctl status nginx`

Configuration: `/etc/nginx/nginx.conf`

Logging directory: `/var/log/nginx/`

4.2.2 HsmWeb

Stop service: `systemctl stop HsmWeb`

Start Service: `systemctl start HsmWeb`

Service state: `systemctl status HsmWeb`

Configuration: `/opt/HsmWebInterface/Web.config`

Service Configuration: `/etc/systemd/system/HsmWeb.service`

Internal address: `tcp:127.0.0.1:9000`

Logging directory `/var/log/HsmWeb/`

4.2.3 HsmApi

Stop service: `systemctl stop HsmApi`

Start Service: `systemctl start HsmApi`

Service state: `systemctl status HsmApi`

Configuration: `/opt/HsmApi/asignRKHsm.exe.config`

Service Configuration: `/etc/systemd/system/HsmApi.service`

Internal address: `http://127.0.0.1:2003/aSignRkHsm/`

Logging directory `/var/log/HsmApi/`

4.2.4 HsmServer

Stop service: `systemctl stop HsmServer`

Start Service: `systemctl start HsmServer`

Service state: `systemctl status HsmServer`

Configuration: `/opt/HsmServer/HsmServer.exe.config`

Service Configuration: `/etc/systemd/system/HsmServer.service`

Internal address: `http://127.0.0.1:2002/aSignRkHsm/v1/`

Logging directory `/var/log/HsmServer/`

4.2.5 HsmKeystoreWatcher

Stop service: `systemctl stop HsmKeystoreWatcher`

Start Service: `systemctl start HsmKeystoreWatcher`

Service state: `systemctl status HsmKeystoreWatcher`

Configuration: `/opt/sync/sync.conf`

Service Configuration: `/etc/systemd/system/HsmKeystoreWatcher.service`

Logging directory `/var/log/HsmKeystoreWatcher/;/var/log/HsmKeystoreSync`

5 Network

The network card of the server operates in the configuration **Network Teaming** (see [Red16]). The configuration files for Network Teaming are listed below.

Team configuration: `/etc/sysconfig/nework-scripts/ifcfg-team0`

Network card 1: `/etc/sysconfig/nework-scripts/ifcfg-eno1`

Network card 2: `/etc/sysconfig/nework-scripts/ifcfg-eno2`

Network card 3: `/etc/sysconfig/nework-scripts/ifcfg-eno3`

Network card 4: `/etc/sysconfig/nework-scripts/ifcfg-eno4`

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 HsmKeystoreWatcher-Service of every server must be updated to reflect the configuration of the network interfaces.

An administrator will need to udpate the configuration file of HsmKeystoreWatchers on the a.sign RK HSM server. (See section 4.2.5)

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 RSA 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 rsa -b 2048
```

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-copy-id 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": "HsmApi",
      "Active": "active",
      "Load": "loaded",
      "Sub": "running"
    },
    {
      ...
    },
    ...
  ],
  "DiskSpace": [
    {
      "FileSystem": "/dev/mapper/centos-root",
      "Size": 52403200,
      "Used": 11036716,
      "Available": 41366484,
      "UsePercent": "22%",
      "MountedOn": "/"
    },
    {
      ...
    },
    ...
  ],
  "CpuUsage": 3.3,
  "MemUsage": 21.6,
  "TestSignature": false,
  "UpTime": "5 days, 22 hours, 45 minutes",
  "OverallStatus": false,
  "Warnings": [
    "Service HsmServer fehlerhaft",
    "Test Signatur fehlerhaft"
  ]
```

```
37 }
```

Line 2: List of HSM Services and there state

Line 14: List of Mount points with their size and available space

Line 28: Current CPU usage in percent

Line 29: Current memory usage in percent

Line 30: State of test signature

Line 31: Uptime of server

Line 32: Overall state of server, same as HTTP status code

Line 33: If an error occurs, the error messages are listed here.

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.

Figure 2: Registration in Finanzonline

A Frequently Asked Questions (FAQ)

A.1 Operating system updates

The server does not perform automated updates. The system must be updated manually by the customer. It is recommended to make the server inaccessible from the internet so that only critical security updates must be installed.

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, the Administration page is only accessible via HTTPS (SSL/TLS) and password authentication. The REST interface is accessible via HTTP and HTTPS (SSL/TLS).

```
events {
  worker_connections 768;
}

http {
  ##
  # Basic Settings
  ##
  sendfile on;
  tcp_nopush on;
  tcp_nodelay on;
  keepalive_timeout 65;
  types_hash_max_size 2048;

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

  ##
  # Logging Settings
  ##
  access_log /var/log/nginx/access.log;
  error_log /var/log/nginx/error.log;


  ##
  # Virtual Host Configs
  ##
  include /etc/nginx/conf.d/*.conf;


  server {
    listen 80 default_server;
    client_max_body_size 20M;
    server_name temp;

    root /usr/share/nginx/html;
    index Default.aspx default.aspx index.html index.htm;

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

    location /aSignRkHsm/ {
      #return 301 https://$host$request_uri;

      proxy_pass http://127.0.0.1:2003/aSignRkHsm/;    ## HsmApi
      proxy_redirect off;
      proxy_set_header Host '127.0.0.1';
      proxy_set_header X-Real-IP $remote_addr;
      proxy_set_header x-Forwarded-For $proxy_add_x_forwarded_for;
      proxy_max_temp_file_size 0;
    }

  }
```

```
55   server {
56     listen 443 default_server;
57     client_max_body_size 20M;
58     server_name temp;
59
60     ssl on;
61     ssl_certificate /etc/nginx/ssl/ssl.crt;
62     ssl_certificate_key /etc/nginx/ssl/ssl.key;
63     ssl_session_timeout 5m;
64
65     ## bettercrypto.org
66     ssl_prefer_server_ciphers on;
67     ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # not possible to do exclusive
68     ssl_ciphers 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA256:EECDH:+
           CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!
           SEED:!IDEA:!ECDSA:kEDH:CAMELLIA128-SHA:AES128-SHA';
69
70     root /usr/share/nginx/html;
71     index Default.aspx default.aspx index.html index.htm;
72
73     location / {
74       auth_basic "Administrationsseite";
75       auth_basic_user_file /etc/nginx/.htpasswd;
76
77       fastcgi_index Default.aspx;
78       fastcgi_buffering off;
79       fastcgi_pass 127.0.0.1:9000;
80       include /etc/nginx/fastcgi_params;
81     }
82
83     location /aSignRkHsm/ {
84       #auth_basic "REST-API";
85       #auth_basic_user_file /etc/nginx/.htpasswdapi;
86
87       proxy_pass http://127.0.0.1:2003/aSignRkHsm/;    ## HsmApi
88       proxy_redirect off;
89       proxy_set_header Host '127.0.0.1';
90       proxy_set_header X-Real-IP $remote_addr;
91       proxy_set_header x-Forwarded-For $proxy_add_x_forwarded_for;
92       proxy_max_temp_file_size 0;
93     }
94   }
95 }
```

Listing 1: Default nginx Configuration

Lines 31-54 Configuration of HTTP connection

Lines 55-95 Configuration of HTTPS (SSL/TLS) connection

Lines 40 Requests to the administration interface via HTTP will be redirected to the HTTPS page.

B.2 nginx configuration for Internet and untrusted networks

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

```
1 events {
2   worker_connections 768;
```

```
}

http {
  ##
  # Basic Settings
  ##
  sendfile on;
  tcp_nopush on;
  tcp_nodelay on;
  keepalive_timeout 65;
  types_hash_max_size 2048;

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

  ##
  # Logging Settings
  ##
  access_log /var/log/nginx/access.log;
  error_log /var/log/nginx/error.log;


  ##
  # Virtual Host Configs
  ##
  include /etc/nginx/conf.d/*.conf;


  server {
    listen 80 default_server;
    client_max_body_size 20M;
    server_name temp;

    root /usr/share/nginx/html;
    index Default.aspx default.aspx index.html index.htm;

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

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

      #proxy_pass http://127.0.0.1:2003/aSignRkHsm/;   ## HsmApi
      #proxy_redirect off;
      #proxy_set_header Host '127.0.0.1';
      #proxy_set_header X-Real-IP $remote_addr;
      #proxy_set_header x-Forwarded-For $proxy_add_x_forwarded_for;
      #proxy_max_temp_file_size 0;
    }

  }
  server {
    listen 443 default_server;
    client_max_body_size 20M;
    server_name temp;

    ssl on;
    ssl_certificate /etc/nginx/ssl/ssl.crt;
    ssl_certificate_key /etc/nginx/ssl/ssl.key;
    ssl_session_timeout 5m;

    ## bettercrypto.org
    ssl_prefer_server_ciphers on;
    ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # not possible to do exclusive
    ssl_ciphers 'EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:EECDH+aRSA+SHA256:EECDH:+
```

```
        CAMELLIA128:+AES128:+SSLv3:!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!
        SEED:!IDEA:!ECDSA:kEDH:CAMELLIA128-SHA:AES128-SHA';
69
70      root /usr/share/nginx/html;
71      index Default.aspx default.aspx index.html index.htm;
72
73      location / {
74        auth_basic "Administrationsseite";
75        auth_basic_user_file /etc/nginx/.htpasswd;
76
77        fastcgi_index Default.aspx;
78        fastcgi_buffering off;
79        fastcgi_pass 127.0.0.1:9000;
80        include /etc/nginx/fastcgi_params;
81      }
82
83      location /aSignRkHsm/ {
84        auth_basic "REST-API";
85        auth_basic_user_file /etc/nginx/.htpasswdapi;
86
87        proxy_pass http://127.0.0.1:2003/aSignRkHsm/;    ## HsmApi
88        proxy_redirect off;
89        proxy_set_header Host '127.0.0.1';
90        proxy_set_header X-Real-IP $remote_addr;
91        proxy_set_header x-Forwarded-For $proxy_add_x_forwarded_for;
92        proxy_max_temp_file_size 0;
93      }
94    }
95  }
```

Listing 2: nginx configuration for Internet and untrusted networks

Lines 31-54 Configuration of HTTP connection

Lines 55-95 Configuration of HTTPS (SSL/TLS) connection

Lines 43-52 These lines need to be adjusted for the deactivation of the REST interface via HTTP. The proxy settings are removed, so that no forwarding is performed. The line 44 is added, so requests received via HTTP will be redirected to the HTTPS port.

Lines 84,85 These two lines are added to activate the authentication for the REST interface.

References

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

[Red16] Red Hat Inc.: *Chapter 5. Configure Network Teaming*, 2016. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Networking_Guide/ch-Configure_Network_Teaming.html, besucht: 2016-07-13.