A-Trust Gesellschaft für Sicherheitssysteme
im elektronischen Datenverkehr 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

User manual
a.sign premium seal qualified

(english translation)

Version: 0.2
Date: 23.05.2019

Contents

Date	Vers.	Author	Changelog
23.05.2019	0.2	Patrick Hagelkruys	add live and test system urls add link to github add detail description of signature format
23.05.2019	0.1	Patrick Hagelkruys	first version

Table 1: document history

1 Overview

1.1 Summary

The `a.sign premium seal qualified` is qualified electonic seal in accordance with the eIDAS regulation [Cou14, Section 5, Article 38, Qualified certificates for electronic seals].

The `a.sign premium seal qualified` is a remote signature, therefore the seal private key is stored in a hardware security module in the A-Trust data center. For each signature request the client software has to issue a request to a A-Trust server to sign with the seal private key.

To order an `a.sign premium seal qualified` you will need to generate a PKCS#10 request for an authentication certificate, that will later authenticate every signing request to the A-Trust server.

This document describes the registration process and signature interface for the `a.sign premium seal qualified`.

2 a.sign premium seal qualified registration process

2.1 Preconditions

For the registration of the `a.sign premium seal qualified` a PKCS#10 request for an authentication certificate is required. The following steps descript the necessary OpenSSL commands to generate a private key and a PKCS#10 request.

The following command generates a new private key file `private_key.pem` and a certificate request file `certificate_request.txt`.

```
openssl req -nodes
            -new
            -newkey rsa:2048
            -sha256
            -out certificate_request.txt
            -keyout private_key.pem
```

Pay attention to the file `private_key.pem` file, it will be needed for every signature request.

2.2 Order process

To order a a.sign premium seal qualified visit the website https://www.a-trust.at/Bestellungen/asignsealqualified/, fill out the form and provide the necessary documents. An A-Trust Support employee will contact you regarding further action to complete the registration process.

After completing the registration process, A-Trust will provide you with the an `a.sign premium seal qualified` certificate and an authentication certificate.

2.3 Optional step, combining private key and authentication certificate

If your client software needs a PKCS#12 file rather than a seperate private key and certificate file, the following command creates the PKCS#12 file with the name `authentication_certificate.p12`

```
openssl x509 -inform der
             -in SealAuthenticationCertificate.cer
       -out SealAuthenticationCertificate.pem

openssl pkcs12 -export
               -out authentication_certificate.p12
               -inkey private_key.pem
               -in SealAuthenticationCertificate.pem
```

3 a.sign premium seal qualified signature interface

3.1 Overview

To communicate with the A-Trust server a REST interface (HTTP POST and HTTP GET) is used.

3.2 Get certificate information

This call requests the seal certificate for the authentication serial number.

URL schema

```
/SealQualified/v1/Certificate/[authcertserial]/[sessionid]
```

Listing 1: get certificate uri schema

The parameter `authcertserial` is the certificate serial number of the authentication certificate in decimal format. The parameter `sessionid` is assigned by the calling application and is used to connect the sessions between client and server.

Request

```
GET /SealQualified/v1/Certificate/1058733338/sessionid
Host: ...
```

Listing 2: get certificate request

Response

```
HTTP/1.1 200 OK
Cache-Control: no-store, no-cache
Content-Disposition: attachment;filename=asignSealQualified.cer
Content-Length: 1077
Content-Type: application/x-x509-ca-cert

[binary data]
```

Listing 3: get certificate response

3.3 Sign hash value

This call requests a signature with the seal private key for the authentication certificate.

Hashing of the data has to be done by the client, only the hash value is transmitted to the A-Trust server.

The signature created by the A-Trust server is an ECDSA signature in the following format:

$$signature = Base64\_url(\ R + \ S)$$
$$\text{where } R = \text{first coordinate of ECDSA point}$$
$$S = \text{second coordinate of ECDSA point}$$

URL schema

```
/SealQualified/v1/Sign/[sessionid]
```

Listing 4: get certificate uri schema

The parameter `sessionid` is assigned by the calling application and is used to connect the sessions between client and server.

Request

```
POST /SealQualified/v1/Sign/sessionid HTTP/1.1
Content-Type: application/json
Host: ...
Content-Length: 952

{
  "AuthSerial": "1058733338",
  "AuthCert": "MIIEiTCCA3GgAwIBAgI....",
  "Hash": "Dza/4+d+pQzueNkiecsIU+qXv...",
  "HashSignatureMechanism": "SHA256withRSA",
  "HashSignature": "wHP+yGEq8g9GT/IE..."
}
```

Listing 5: sign hash value request

The parameter `AuthSerial` contains the certificate serial number of the authentication certificate in decimal format. Instead of the `AuthSerial` you can also add the complete authentication certificate in base64 format as `AuthCert`. `Hash` contains the to-be-signed hash value and `HashSignature` contains the signature with the authentication certificate over the hash value. `HashSignatureMechanism` specifies the algorithm used to sign the hash value.

For `HashSignatureMechanism` the following values values are supported:

- SHA256withRSA
- SHA384withRSA
- SHA512withRSA
- SHA256withECDSA
- SHA384withECDSA
- SHA512withECDSA

Response

```
HTTP/1.1 200 OK
Content-Length: 130
Content-Type: application/json; charset=utf-8

{
  "Signature":"BC4jJ\/fdAvBBln+y6h...egC7U="
}
```

Listing 6: sign hash value response

3.4 Test call

This call serves only as a connection test and always returns with HTTP state 200 - OK.

Request

```
GET /SealQualified/v1/Test
Host: ...
```

Listing 7: test request

Response

```
HTTP/1.1 200 OK
```

Listing 8: test response

4 Live and test system

4.1 Live-System

The live system for a.sign premium seal qualifiedis available via the following link:

URL: https://www.a-trust.at/SealQualified/v1

4.2 Test-System

For testing purpose the following parameters can be used:

URL: https://hs-abnahme.a-trust.at/SealQualified/v1

The required authentication certificate is available on github https://github.com/A-Trust/ASignSealQualified including free sample code and test clients.

References

[Cou14] Council of European Union: *Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, 2014. https://eur-lex.europa.eu/eli/reg/2014/910/oj.