Black•Vault HSM.TSA

User Guide

Revision 11.1.1.5

9565 Soquel Drive, Aptos, CA 95003

+1 831.688.1021

+1 877.ENGAGE4

https://www.engageblack.com

https://www.engageinc.com

sales@engageblack.com

Disclaimer and Warranty

Engage Black is a business unit of Engage Communication.

Engage Communication makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability of fitness for any particular purpose. Information in this document is subject to change without notice and does not represent a commitment on the part of Engage Communication, Inc. Product specifications are subject to change without notice. Engage Communication assumes no responsibility for any inaccuracies in this document or for any obligation to update the information in this document.

The Engage Black HSM.TSA offers a unique combination of FIPS level protection of the cryptographic key material and the reliability of a time stamp authority all-in-one, stand alone, network attached, multiprocessing network device that is innovative and unique in its design.

The dual network ports allow for the simultaneous connections of multiple host applications that consume the services of the HSM and TSA.

This Product is connected and managed by switches and / or PCs that are normally capable of multiprocessing and are not directly marketed to the public, these products are used by institutions that require these unique features.

Contents

1 Quick start reference

1.1 Issuing a time stamp

If the unit is up and running, create and verify a timestamp by running: [1]

```
openssl ts -query -data <ORIGINAL FILE> -out <REQUEST FILE>
curl -Ss <IP/DOMAIN> \
     -H "Content-Type:application/timestamp-query" \
     -f -g --data-binary "@<REQUEST FILE>" \
     -o <STAMP FILE>
openssl ts -verify \
        -in <STAMP FILE> \
        -data <ORIGINAL FILE> \
        -CAfile <(curl -Ss <IP/DOMAIN>:2020/ca.pem) \
        -untrusted <(curl -Ss <IP/DOMAIN>:2020/tsa_cert.pem)
```

[1] See *basic-usage* for detailed info.

2 Introduction

2.1 Dependencies

Required:

- **Black•Vault HSM** client utilities: Managing and configuring internal HSM.
- A web browser (e.g. Firefox): Managing the TSA.

Optional:

- OpenSSL: Utilities for creating/verifying RFC 3161 requests.
- `curl`: Command line tool for accessing time stamp server through HTTP API.

2.2 Hardware

The **Black•Vault HSM.TSA** ships with everything needed to get started. The box should contain:

- **Black•Vault HSM.TSA** *unit*: **Black•Vault HSM.TSA**/**Black•Vault HSM** unified bundle.
- *Engage Black CD*: CD containing documentation and client utilities.
- *Engage Black Smartcards*: Ten smart cards for **Black•Vault HSM** management.
- *Power Cord* and *AC power Adapter*: Power supply for the unit.
- *Ethernet cables*: Two Ethernet cables for accessing the TSA and HSM through a local network.

3 Management

3.1 Overview

Black•Vault HSM.TSA defaults:

- IP: `192.168.1.11`
- Admin user: `admin`
- Admin password: `admin`

Black•Vault HSM defaults:[2]

- IP: `192.168.1.7`

[2]See the **Black•Vault HSM** user guide for setting up and managing the HSM.

3.2 Initial connection and set up

Notes and Troubleshooting

- Reboot does not automatically refresh the management console. You must reload the page or go to another one after 30 seconds.
- If the time stamping service is configured but returns response code 500, check the status page in the management console. It is likely that NTP has not synchronized yet and so the service will not issue time stamps.
  - NTP may take up to 10 minutes to synchronize after a reboot.

Connection

After connecting via Ethernet and booting the device, open your web browser and navigate to the default IP address, `192.168.1.11`. Note that you may have to modify your PCs IP address to match the `192.168.1.x` sub-net.

Logging in

To use any part of the management portal, you must login. The default user should be `admin`, the default password should also be `admin`.

Default settings

After logging in, the first step should be changing the IP settings and Admin password. To change the Admin password:

- Click on the *admin* link on the right side of the menu bar (to the left of *Logout*).
- Select the *Change password* option.
- Fill in the fields and select *Change Password*.
- At this point you should be logged out automatically.

Changing the IP address:

- Click on the *Configuration* drop-down at the top of the page and select *Network Configuration*.
- Change the *IP Address*, *Subnet*, and *Gateway* fields as needed.
- Select *Submit*.

For any changes to be registered, you must reboot the system:

- Select *Reboot* in the *Configuration* drop-down.
- After the page loads, click on the *Reboot* button.

3.3 Time stamping service configuration

3.3.1 TSA signing certificate

To configure the **Black•Vault HSM.TSA** time stamping service you must have an initialized **Black•Vault HSM**. After logging in to the management portal:

- Navigate to *Network configuration* in the *Configuration* drop-down.
- Set the *HSM IP* and *HSM IP Port* to the IP and port of your **Black•Vault HSM**.
- Reboot.

Now, we need to export the signing CSR.

- Log in and navigate to the *Export CSR* link in the *Configuration* drop-down.
- Select a key size (the default is 2048).
- Specify the correct info in the subject field. The format is, `C=US/ST=State/L=City/O=Organization/OU=Unit/CN=Common Name`.[3]
- Click on the *Export* button. This will trigger the generation of the TSA signing key on the HSM.[4]
- After the key has been generated, the web page will prompt you to download a file named `tsa.csr.pem`.

Note that when signing the time stamping certificate there are required X509 extensions. See *Generating test certificates* for more information. After the CSR has been signed by a Certificate Authority we will need to import the CA certificate and the new signing certificate.

- Select *TSA Configuration* in the *Configuration* drop-down.
- Find your CA certificate using the file explorer.
- Find your TSA certificate using the file explorer.
- Click the *Save and upload* button to finish the upload.

[3] The common name (`CN`) is required. If the country is specified (`C`) it must be two letters.

[4] This step may take a short while. Currently, the TSA only supports RSA 4096 signing keys. The generated key will be labeled `bvtsa Token Object (Signing Key)`.

Finally, reboot. When the device starts again, the time stamp response server should be running. Verify this by using your web browser:

- Navigate to `<IP/DOMAIN>:2020`.
- The page should be found and have the text: `BVTSA Version <BVTSA VERSION>`.

Generating test certificates

When setting up for testing, the following OpenSSL commands may help with bootstrapping some test certificates. First, we need to modify our local OpenSSL configuration file to include the following sections:

```
[v3_ca]
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
basicConstraints = critical,CA:true
keyUsage = cRLSign, keyCertSign

[v3_tsa]
basicConstraints=CA:FALSE
keyUsage = nonRepudiation, digitalSignature
extendedKeyUsage = critical,timeStamping
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid,issuer:always
```

These sections allow us to specify the proper extensions on the generated TSA certificate. Next we need to create a local CA:

```
openssl req \
  -new -x509 -nodes \
  -out ca.crt.pem \
  -keyout ca.key.pem \
  -extensions v3_ca
```

Once this self-signed root CA is created we can take the TSA CSR and issue a certificate:

```
openssl x509 -req \
  -in tsa.csr.pem -out tsa.crt.pem \
  -CA ca.crt.pem -CAkey ca.key.pem \
  -CAcreateserial \
```

```
-extfile ossl.conf.txt \
-extensions v3_tsa
```

The certificate can be checked using:

```
openssl x509 -text -in tsa.crt.pem
```

After checking that the proper extensions are in the certificate, continue with certificate upload outlined in the previous section.

3.3.2 SSL configuration

After configuring and uploading the time stamp service signing certificate we can set up SSL. To set up SSL with the time stamping service we need to follow some similar steps to generating the signing certificate:

- Navigate to *Export SSL CSR* in the *Configuration* drop-down.
- Select a key size (the default here is 2048).
- Specify the correct info in the subject field. The format is, `C=US/ST=State/L=City/O=Organization/OU=Unit/CN=Common Name`.[5]
- When the subject is correct, select the export button.

When the CSR is signed, return to the *TSA Configuration* page in the *Configuration* drop-down. Here we will import both the CA certificate and the SSL certificate:

- Find the certificate for the CA that signed the certificate, using the file browser.
- Find the SSL certificate, using the file browser.[6]
- Click the *Save and upload* button to finish the upload.

Finally, reboot. If the signing certificate has been configured already, SSL should be running when the device boots. Access the TSA using `https://<IP/DOMAIN>:2020`.

Enable/Disable SSL

On the *TSA Configuration* page, there is also a *Enable SSL* section. Use the checkbox to enable or disable SSL after it has been set up. After enabling or disabling, you must reboot. The time stamping service URL must be correct when connecting:

- For SSL use: `https://<IP/DOMAIN>:2020`
- Otherwise use: `http://<IP/DOMAIN>:2020` or simply `<IP/DOMAIN>:2020`

[5] The common name (`CN`) is required. If the country is specified (`C`) it must be two letters.
[6] After the SSL certificate is uploaded, SSL will be enabled for the next boot.

3.4 Firmware upgrades

To upgrade the **Black•Vault HSM.TSA** firmware you must be logged in and have a encrypted upgrade ready.

- Navigate to *Firmware Upgrade* in the *Configuration* drop-down.
- Use the file selector to find and select the upgrade.
- Click the submit button.
- Once the Firmware has been verified a status message will be printed to the page.
- Reboot. Note that the boot time may take up to five minutes after a new upgrade.

3.5 NTP configuration

Make sure you are logged in to the TSA management portal. To change the NTP sources:

- Navigate to *NTP Configuration* in the *Configuration* drop-down.
- Modify the NTP server URLs to point to the desired locations.
- Click *Submit*.
- Reboot.

3.6 Export Logs

To export the TSA logs, navigate to *Export Logs* in the *Configuration* drop-down. On the *Export Logs* page, click *Export*.

3.7 TSA Reset

To reset the TSA modules, click on the *admin* link in the upper right of the management portal. On this page, select *Reset settings*. After selecting one or more modules, click *Reset* to reset them.

4 Basic usage

The following commands use `curl` and `openssl` to create requests and issue time stamps. Other tools may be used to access the HTTP API. Or verify the resulting time stamp.

4.1 Downloading the root certificate

The root certificate is located at <IP/DOMAIN>:2020/ca.pem. To download the certificate run:

```
curl -Ss <IP/DOMAIN>:2020/ca.pem > ca.pem
```

4.2 Downloading the TSA certificate

The TSA signing certificate is located at <IP/DOMAIN>:2020/tsa_cert.pem. To download the certificate run:

```
curl -Ss <IP/DOMAIN>:2020/tsa_cert.pem > tsa_cert.pem
```

4.3 Creating a time stamp request

The OpenSSL command-line tool can be used to create time stamps. For example:

```
openssl ts -query -data <ORIGINAL FILE> -out <REQUEST FILE>
```

4.4 Viewing a time stamp request

OpenSSL can also be used to view time stamp requests:

```
openssl ts -query -text -in <REQUEST FILE>
```

4.5 Issuing the time stamp

To issue a time stamp you must send a properly formatted HTTP request to the server:

```
curl -Ss <IP/DOMAIN>:2020 \
     -H "Content-Type:application/timestamp-query" \
     -f -g --data-binary "@<REQUEST FILE>" \
     -o <STAMP FILE>
```

4.6 Viewing time stamp information

Use OpenSSL to display the resulting time stamp:

```
openssl ts -reply -text -in <REQUEST FILE>
```

4.7 Verifying the generated time stamp

Verifying the time stamp can be done with OpenSSL:

```
openssl ts -verify \
        -CAfile ca.pem \
        -untrusted tsa_cert.pem \
        -data <ORIGINAL FILE> \
        -in <STAMP FILE>
```