



CERTIFICATE AUTHORITY BASED ON CRYPTOGRAPHIC HARDWARE SECURITY MODULE

The specifications and information in this document are subject to change without notice. Companies names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason without the express written permission of RCDevs Security.

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

Certificate Authority based on Cryptographic Hardware Security Module

[CA](#) [HSM](#) [WebADM](#) [PKI](#) [Certificat](#) [Public Key Infrastructure](#) [Certificate Authority](#) [Rsignd](#)

1. Overview

This HowTo describes how to configure Rsignd service (PKI service) of WebADM on a PKCS11 cryptographic hardware security module (HSM). The objective is to involve the HSM for all CA signing operations and to increase the protection of the private key. This configuration is probably the most secure setup for a PKI service because the logical and physical access to the HSM is limited to one or few persons in a company.

If your WebADM servers has been compromised for any reason, the CA private key is not accessible through the WebADM servers. The private key of the certificate authority will be located on the HSM, which is protected by a passphrase/PIN configured during the HSM setup.

To compromise the private key of your certificate authority based on an HSM, the attacker needs:

- > root access on the WebADM server in order to get the passphrase/PIN which is also encrypted by WebADM mechanisms,
- > Decrypt the encrypted PIN/Passphrase,
- > Have physical access to the HSM,
- > Unlock it and steal the private key.

The PKCS11 HSMs are also protected against bruteforce attacks and the HSM is automatically locked after several unsuccessful attempts. Refer to your PKCS11 HSM documentation for more information.

This setup can be done during the WebADM installation or after when WebADM is already configured and running.

For high availability, consider to plug 2 HSMs on your master WebADM server. Rsignd service is currently running only on the first WebADM server deployed (master) but RCDevs is implementing a fully redundant PKI service, so in futur versions, you could plug only one HSM per WebADM server or for very critical PKI services, 2 HSMs per WebADM node part of the same cluster.

2. Certificate Authority setup

RCDevs provides different setups for the certificate authority.

- > WebADM can be configured as a [standalone CA](#), which is the default configuration.
- > WebADM can be configured as a [subordinate CA](#) of an existing enterprise CA.

Refer to the previous documentation according to the setup you want to achieve.

WebADM setup script will guide you in your CA setup according to your choice.

If you want to reconfigure a WebADM installation previously configured as a standalone CA and you want to make it as subordinate CA of your existing CA, please refer to the secondary link.

If you choose new Standalone CA, then the CA certificate and key are generated during the WebADM setup and will be located in `/opt/webadm/pki/ca/` folder.

If you choose subordinate CA setup, then the certificate needs to be already copied in `/opt/webadm/pki/ca/`. The CA key will be temporarily located on the file system until you programmed your HSM with the CA private key.

3. Program your HSM with your CA private key

In that documentation, we will not explain how to configure the HSM itself as we already provide documentations which cover these topics. Refer to [MirKey/eHSM devices configuration](#) or [Smartcard HSM](#) documentation. For any other HSM, please contact RCDevs Service team. All standard PKCS11 HSMs are supported by WebADM.

4. WebADM configuration to use CA private key from the HSM

Now that you CA private key is located on your HSM(s), you have to configure WebADM to use your HSM(s).

There is 2 configuration files to do it, the first is `/opt/webadm/conf/webadm.conf` and the second is `/opt/webadm/conf/rsignd.conf`. Found below, the configuration needed for each file.

4.1 webadm.conf

```
# Hardware Cryptography Module
# Yubico YubiHSM and SCHSM are currently supported for hardware encryption.
# Up to 8 HSM modules can be concurrently attached to the server.

hsm_model SCHSM
hsm_keyid 1
hsm_pincode XXXXXX

## If you have 2 HSMs, then :

hsm_model SCHSM
hsm_keyid 2
hsm_pincode XXXXXX
```

The PIN code value can be encrypted in order to not be stored in clear text in `webadm.conf` file. Please, refer [pwcrypt usage](#)

4.2 rsignd.conf

Found below the mandatory settings :

```
# HSM certificate authority (CA)
# The HSM model and PIN code are configured in webadm.conf.
hsm_ca yes
hsm_keyid 0
```

Optionally, if the CA certificate/key in PEM format are protected by a password, you have to enable that `ca_password` setting and the password will be asked when WebADM services are starting. `hsm_keyid` value must refer the slot id of the HSM where you deployed the CA private key.

```
# Set to yes if the CA or RSignd private keys requires a decryption password.
```

```
# PEM passwords will be prompted at WebADM startup.
```

```
ca_password yes
```

```
rsignd_password no
```

This manual was prepared with great care. However, RCDevs Security S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs Security S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs Security S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs Security S.A. The latter especially applies for data processing systems. RCDevs Security S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs Security. © 2024 RCDevs Security S.A., All Rights Reserved