

## #

Key Management System

## #

Introduction

[Tendermint KMS](#)[Open in new window](#) is a key management service that allows separating key management from Tendermint nodes. In addition it provides other advantages such as:

- Improved security and risk management policies
- Unified API and support for various HSM (hardware security modules)
- Double signing protection (software or hardware based)

## #

Building

Detailed build instructions can be found [here](#)[open in new window](#).

TIP

When compiling the KMS, ensure you have enabled the yubihsm features: `cargo install tmkms--features = yubihsm--version = 0.10.0-beta2`

## #

Initialization

Initialize configuration files for IRIShub

```
tmkms init-n irishub /path/to/kms/home
```

## #

Configuration

To enable KMS, you need to edit `thepriv_validator_laddr` in your `config/config.toml` file first. e.g.:

# TCP or UNIX socket address for Tendermint to listen on for

## connections from an external PrivValidator process

### priv\_validator\_laddr

"localhost:26658" Then, download [priv\\_validator\\_state.json example](#)[open in new window](#) and modify all field values to match your `data/priv_validator_state.json` values.

Next, you just need to edit the configuration file `/path/to/kms/home/tmkms.toml` as follows:

- Configure `state_file`
- as `thepriv_validator_state.json`
- completed in the previous step.
- Write your Yubihsm password to file `yubihsm-password.txt`
- and configure `password_file`
- as it.
- Edit `addr`
- to point to your iris
- instance (note: no need to specify the connection id, just like `tcp://localhost:26658`).
- Adjust `chain_id`

- to match your/config/genesis.json
- settings.
- Editauth
- to authorize access to your Yubihsm.
- Editkeys
- to determine which pubkey you will be using.
- Editprotocol\_version
- to v0.34.

Then start tmkms:

```
tmkms start-c /path/to/kms/home/tmkms.toml
```

<#>

Using a YubiHSM

Detailed information on how to setup a KMS with YubiHSM2 can be found [hereopen in new window](#).

If you want to import an existing IRIShub private\_key:

```
tmkms yubihsm keysimport < iris_home> /config/priv_validator.json-i < id> -t json-c /path/to/kms/home/tmkms.toml
```