secureboot/introduction_habv4.txt

2. Generating a PKI tree

The first step is to generate the private keys and public keys certificates.
The HAB architecture is based in a Public Key Infrastructure (PKI) tree.

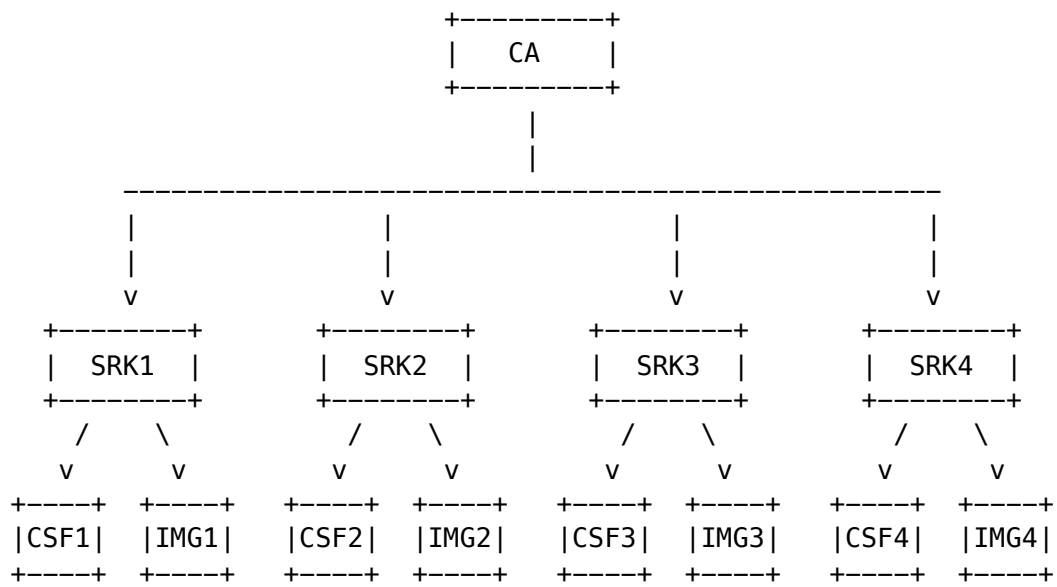
The Code Signing Tools package contains an OpenSSL based key generation script
under keys/ directory. The hab4_pki_tree.sh script is able to generate a PKI
tree containing up to 4 Super Root Keys (SRK) as well as their subordinated
IMG and CSF keys.

A new PKI tree can be generated by following the example below:

- Generating 2048-bit PKI tree on CST (starting from v3.1.0):

```
$ ./hab4_pki_tree.sh
...
Do you want to use an existing CA key (y/n)?: n
Do you want to use Elliptic Curve Cryptography (y/n)?: n
Enter key length in bits for PKI tree: 2048
Enter PKI tree duration (years): 5
How many Super Root Keys should be generated? 4
Do you want the SRK certificates to have the CA flag set? (y/n)?: y
```

The diagram below illustrate the PKI tree:



After running the script users can check the private keys under keys/ directory
and their respective X.509v3 public key certificates under crts/ directory.
Those files will be used during the signing and authentication process.