Important note on verifying Secure Execution host key documents

The certificates of the host key signing keys that are needed to verify host key documents will expire on

- April 24, 2024 for IBM z15® and IBM® LinuxONE III
- March 29, 2024 for IBM z16™ and IBM LinuxONE 4.

Due to a requirement from the Certificate Authority (DigiCert), the renewed certificates are equipped with a new Locality value ("Armonk" instead of "Poughkeepsie"). These renewed certificates cause the current versions of the ***genprotimg***, ***pvattest***, and ***pvsecret*** tools to fail the verification of host key documents.

The IBM Z team is preparing updates of the ***genprotimg***, ***pvattest***, and ***pvsecret*** tools to accept the new certificates and is working with Linux distribution partners to release the updated tools.

To build new Secure Execution images, attestation requests, or add-secret requests before the updated tools are available in Linux distributions, follow these steps:

Step 1:

Obtain the host key document, the host key signing key certificate, the intermediate certificate from the Certificate Authority, and the list of revoked host keys (CRL):

- For IBM z15 and IBM LinuxONE III, see:

  `https://www.ibm.com/support/resourcelink/api/content/public/secure-execution-gen1.html`

- For IBM z16 and IBM LinuxONE 4, see:

  `https://www.ibm.com/support/resourcelink/api/content/public/secure-execution-gen2.html`

Step 2:

Download the script ***check_hostkeydoc*** from

`https://github.com/ibm-s390-linux/s390-tools/blob/master/genprotimg/samples/check_hostkeydoc`

Step 3:

Verify each host key document using the ***check_hostkeydoc*** script. For example, issue:

```
# ./check_hostkeydoc HKD1234.crt ibm-z-host-key-signing.crt \
-c DigiCertCA.crt -r ibm-z-host-key.crl
```

This example verifies the host key document `HKD1234.crt` using the host key signing key certificate `ibm-z-host-key-signing.crt`, and the intermediate certificate of the Certificate Authority `DigiCertCA.crt`, as well as the list of revoked host keys `ibm-z-host-key.crl`.

After the host key documents are verified using the ***check_hostkeydoc*** script, you can safely call ***genprotimg***, ***pvattest***, or ***pvsecret*** with the `--no-verify` option.

For a description about how to manually verify host key documents, see:

`https://www.ibm.com/docs/en/linux-on-z?topic=execution-verify-host-key-document`