Updating SCU.DE.CryptoVision

The following document proposes the changes needed to support the new functionalities of the CryptoVision TSE V2 hardware and firmware.

This document assumes the direct use of the transport layer with no imported dependencies.

According to the changelog, the changes introduced at transport layer level are:

The renaming of:

- **MapERStoKey -> RegisterClient**
- **Deactivate -> Lock**
- **Activate -> Unlock**

This should not be a breaking change because the command code and the input format are the same (i.e 0017, 0013, 0014). However, for code clarity, the function name should be refactored eventually in order to be consistent with the documentation.

The fix of encoded TAR file got when exporting:

The newest V2 hardware and firmware solves a problem that was present in previous versions - When exporting the TAR file (according to TR-03151), the EndOfTar mark was not included by the device. This had to be done by the host library as part of data decoding. In the newest hardware revisions, the exported data now includes the filemark.

In the CryptoVision Package, we first have to check if we need to append the mark and make the appropriate modifications.

These changes also apply to: **GetCertificates** and **ExportMoreData** functions because the output is also encoded as TAR.

The introduction of new behaviour in V2 for:

- **InitiaizePins**

This is likely to be a breaking change because the command encoding changed from V1 to V2. It is no longer needed to provide the Admin PUK, PIN, TimeAdmin PUK and PIN. The **new format** takes the User ID and the PUK value. Only Admin and TimeAdmin users are allowed to be passed in the User ID field.

The introduction of new functions supported by the V2 hardware:

- **GetMinSignatureCounter**

This returns the lowest signature counter in the transaction-log and is only available in TSE V2 firmware. It should **not be mandatory** to implement but rather a nice to have feature.

- **GetMaxSignatureCounter**

This returns the highest signature counter in the transaction-log and is only available in TSE V2 firmware. It should **not be mandatory** to implement but rather a nice to have feature.

- **GetNextSignatureCounter**

This returns the next signature counter in the transaction-log and is only available in TSE V2 firmware. It should **not be mandatory** to implement but rather a nice to have feature.

- **GetCertificate**

This is not to be confused with GetCertificates (returns the whole certificate chain). The new command is only available in TSE V2 firmware and returns the certificate of the signature key. This **SHOULD** be implemented as it may be needed down the line when integrating with the **Sperrliste.**

- **ListClients**

This returns the cash registers that are currently paired with the module. It is only available in TSE V2 firmware. This **SHOULD** be implemented as it may be a good cross-validation source of information - we could check if the stored mappings when creating the SCU are also consistent with what we have stored in the module.

Summary

- We should define the new functions in the IVisionProxy Interface and provide an implementation for each one;
- We should check for inconsistencies when exporting data from V1 and V2 hardware (because of the file markers);
- We should define a way to mark interface implementations based on the hardware that they work on;
- We should provide a new overload for the **InitializePins** function that knows how to work with V2 hardware;
- We should read and store the hardware version (i.e V1, V2) of the TSE in the CryptVisionSCU class so we have that available;
- Upon creation of the CryptoVisionSCU class we should query and get the digital certificate serial number so we can have access to it with regard to Sperrliste cross-validation;