USAGE OF PRIMESIGN RKSV SIGNATURE CARDS

Thank you very much for your confidence in PrimeSign RKSV signature cards. With this document, we guide you through the first steps to integrate our signature card in your products.

You receive the PrimeSign RKSV signature card already fully activated. The default signature PIN is set to 000000. The APDU sequences to read the RKSV signing certificate from the smart card, the issuing of a signature, and to change the signature PIN is described in the following sections.

1 Signing Certificate Extraction

It might not always be necessary to read the signing certificate from the smart card. However, especially during the integration it may be helpful. The certificate is stored in the application DF_QES (File ID: 3F 04) in the file EF_C_X509_CH_DS (File ID: C0 00). To read the file the following APDU commands are necessary:

```
// SELECT DF_QES
00 A4 08 0C 02 3F 04

// SELECT EF_C_X509_CH_DS
00 A4 02 0C 02 C0 00

// READ BINARY
00 B0 00 00 00 00
```

To generate a certificate object out of the returned Byte-Array following JAVA-code can be used:

```
byte[] certBytes = response.getValue();
try (ByteArrayInputStream is = new ByteArrayInputStream(certBytes)) {
        CertificateFactory fact = CertificateFactory.getInstance("X.509");
        Certificate cert = fact.generateCertificate(is);
} catch (Exception cause) {
        // Process exception
}
```

2 Triggering a Signature

To trigger a signature using be pre-calculated hast value following APDU commands are necessary:

```
// SELECT DF_QES
00 A4 08 0C 02 3F 04

// VERIFY PIN
00 20 00 81 08 26 00 00 00 FF FF FF FF
```

```
// Perform Security Operation - Compute Digital Signature
00 2A 9E 9A 20 xxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxx xxxxxxxxxxxxxxxx 00
```

For the VERIFY PIN command the PIN must be encoded in following format:

2y xx xx xx xF FF FF FF

The letter „y“ indicates the number of digits of the PIN (6-12, in the example above it is 7) and each letter „x“ indicates a digit of the PIN (0-9). The remainder must be filled with 0xF to get eight bytes in total. So, the representation of the default signature PIN is:

26 00 00 00 FF FF FF FF

To calculate the hash value following JAVA-code can be used:

```
byte[] dataToBeSigned = ...;
byte[] hashValue = null;
try {
        MessageDigest md = MessageDigest.getInstance("SHA-256");
        hashValue = md.digest(dataToBeSigned);
} catch (Exception cause) {
        throw new RuntimeException(cause);
}
// Build APDU
```

3 Change the Signature-PIN

The default signature PIN has been chosen as several cash registers do not allow another PIN. To protect the PrimeSign RKSV signature card against unauthorized access, we recommend to change the signature PIN. This can be done by using following APDU command:

```
// CHANGE REFERENCE DATA
00 24 00 81 10 2y xx xx xx FF FF FF FF 2Y XX XX XX XF FF FF FF
```

The lowercase letters „y“ and „x“ indicate the number of digits and the value of the old PIN, whereas the uppercase letter „Y“ and „X“ the number of digits and the value of the new PIN. In the example given above $y = 6$ and $Y = 7$, i.e. the old PIN had six digits and the new PIN seven digits.

This command must be executed within the application QES. Therefore, it may be necessary to select the application beforehand:

```
// SELECT DF_QES
00 A4 08 0C 02 3F 04
```