EINSATZ DER PRIMESIGN RKSV SIGNATURKARTEN

Herzlichen Dank für den Einsatz der PrimeSign RKSV Signaturkarte. In diesem Dokument werden die ersten Schritte zur Integration der Signaturkarte beschrieben.

Sie erhalten die PrimeSign RKSV Signaturkarte bereits vollständig aktiviert und mit 000000 als Default-Signatur-PIN gesetzt. Die APDU-Sequenzen zum Auslesen des RKSV Signaturzertifikates, dem Auslösen einer Signatur und dem Ändern der Signatur-PIN wird im Folgenden beschrieben.

1 Auslesen des Signaturzertifikates

Das Auslesen des Signaturzertifikates ist nicht zwingend erforderlich, kann aber gerade in der Integrationsphase hilfreich sein. Das Zertifikat ist in der Anwendung DF_QES (File ID: 3F 04) in der Datei EF_C_X509_CH_DS (File ID: C0 00) abgelegt. Dazu sind folgende APDU-Kommandos erforderlich:

```
// 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 00
```

Um aus dem zurückgegebenen Byte-Array ein Zertifikatsobjekt zu erzeugen kann folgender JAVA-Code verwendet werden:

```
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 Auslösen einer Signatur

Das Auslösen einer Signatur mit vorberechnetem Hash-Wert kann mit folgenden APDU-Kommandos erfolgen:

```
// 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
```

Für das VERIFY PIN Kommando muss die PIN in folgendem Format kodiert sein:

2y xx xx xx xF FF FF FF

Wobei y die Anzahl der Stellen der PIN angibt (6-12, im vorliegenden Fall 7) und x jeweils eine Stelle der PIN (0-9). Der Rest der Stellen ist mit 0xF auf acht Byte aufzufüllen. Für den Default-Signatur-PIN ergibt sich daher folgende Repräsentation:

26 00 00 00 FF FF FF FF

Um den Hash-Wert zu berechnen kann folgender JAVA-Code verwendet werden:

```
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 Ändern der Signatur-PIN

Die Default-Signatur-PIN wurde gewählt weil etliche Registrierkassen keine andere PIN zulassen. Um die PrimeSign RKSV Signaturkarte vor unbefugtem Zugriff zu schützen wird empfohlen die Signatur-PIN auf einen nur Ihnen bekannten Wert zu setzen. Dazu ist folgendes APDU-Kommando notwendig:

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

Hier bezeichnen y und x Länge bzw. Wert der alten PIN und Y bzw. X Länge und Wert der neuen PIN. In vorliegendem Beispiel wäre $y = 6$ und $Y = 7$, d.h. die alte PIN war sechsstellig und die neue PIN ist siebenstellig.

Dieses Kommando muss innerhalb der Applikation QES ausgeführt werde, daher kann es erforderlich sein zuvor noch die Anwendung auszuwählen:

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