B.3.1.3 Asymmetrische Schlüssel für RDH

Grundsätzlich können Kunde und Kreditinstitut beim asymmetrischen Verfahren (RDH) über maximal drei Schlüsselpaare verfügen:

- ein Signierschlüsselpaar
- ein Chiffrierschlüsselpaar
- ein Schlüsselpaar für die Erzeugung Digitaler Signaturen (DS)

Der Signierschlüssel sowie der DS-Schlüssel werden zum Unterzeichnen von Nachrichten verwendet, während der Chiffrierschlüssel zum Verschlüsseln von Nachrichten dient (vgl. Kapitel B.1.1).

Falls ein Kreditinstitut seine Nachrichten nicht signiert, kann es auf das Signier-Schlüsselpaar verzichten.

B.3.1.3.1 Schlüsselgenerierung

Die Schlüsselpaare des Kunden sind vom Kundenprodukt bzw. von der Chipkarte zu erzeugen. Die Schlüsselpaare des Kreditinstituts sind vom Kreditinstitut zu erzeugen. Die privaten Schlüssel sind jeweils geheim zu halten.

Die Schlüsselgenerierung hat gemäß dem folgenden Ablauf stattzufinden:[9]

1. Es wird ein konstanter öffentlicher Exponent e und ein für jeden Kunden individueller Modulus n für jedes eingesetzte RSA-Schlüsselsystem verwendet.
2. Der konstante öffentliche Exponent e wird auf die 4. Fermat'sche Primzahl festgelegt: $e = 2^{16} + 1$
3. Der Modulus n eines jeden RSA-Schlüsselsystems hat eine Länge von N Bit. Es sind keine führenden 0-Bits erlaubt, so dass auf jeden Fall gilt: $2^{N-1} \leq n < 2^N$
4. Der Zielwert für N ist bei RDH-1 768, wobei eine aus der Suche nach starken Primzahlen resultierende Unterschreitung dieses Wertes um maximal 60 Bit zulässig ist. Bei RDH-2, RDH-3 und RDH-5 liegt der Zielwert für N zwischen 1024 und 2048. Bei RDH-6, RDH-7, RDH-8, RDH-9 und RDH-10 liegt der Zielwert für N zwischen 1536 und 4096.

   - Schlüsselgenerierung bei RDH-10:
   - Das Kundensystem muss sicher stellen, dass die Schlüssellänge eines neu generierten Schlüsselpaares des Kunden ~~kleiner oder~~ gleich der Länge des öffentlichen Signierschlüssels des Instituts ist, falls das Institut Bankensignaturen unterstützt. Anderenfalls ist die Länge des Chiffrierschlüssels maßgebend.

5. n ist das Produkt zweier großer, zufällig ausgewählter Primzahlen p und q. Folgende Anforderungen werden an die Faktoren p und q gestellt:
   - p hat eine vorher festgelegte minimale Länge
   - p - 1 hat einen großen Primteiler[10] r

---

[9] Das Verfahren entspricht dem des DFÜ-Abkommens.