C.1.3.1 Verfahren zur Ermittlung der Sicherheitsreferennummern

Auf der Bankensignaturkarte wird kein eigenständiger Sequenzzähler (wie das Element EF_SEQ im HBCI DDV-Verfahren) verwaltet, sondern es werden jeweils chipkarteninterne „Usage Counter“ der beiden zur Signatur verwendeten Schlüssel S_K.CH.DS und S_K.CH.AUT$_{C/S}$ herangezogen.

Für jedes Signaturschlüsselpaar wird ein separater Usage Counter verwaltet.Dieser kann jeweils zwei, drei oder vier Byte lang sein.

Da die Usage Counter auf der Chipkarte dekrementiert werden, als Sicherheitsreferenznummer („Signatur-ID“) aber ein streng monoton aufsteigender Zähler gefordert ist, wird die konkrete Sicherheitsreferenznummer nach folgendem Algorithmus ermittelt:

1. Auslesen des 2 bis 4 Byte langen Usage Counter (UC) UC_{DS} des Schlüssels S_K.CH.DS bzw. UC_{AUT} des Schlüssels S_K.CH.AUT$_{C/S}$.
2. Sei **neg**(UC) die bitweise logische Negation von UC. Dann ist die Sicherheitsreferenznummer (SRN)

$$SRN_{DS} = \mathbf{neg}(UC_{DS})$$

$$SRN_{AUT} = \mathbf{neg}(UC_{AUT})$$

Die einzelnen Usage Counter haben folgende Wertebereiche:
von 0 bis 65.535 bei Länge(UC) = 2 Byte
von 0 bis 16.777.215 bei Länge(UC) = 3 Byte
von 0 bis 4.294.967.295 bei Länge(UC) = 4 Byte

Damit muss die Sicherheitsreferenznummer SRN über die entsprechenden Wertebereiche verfügen und benötigt zur Darstellung ebenfalls mindestens 2, 3 oder 4 Byte.

Ein Wrap-Around bei Erreichen des jeweiligen Maximalwerts findet nicht statt, da das Erreichen eines Usage Counter 0 den Schlüssel der Chipkarte für die weitere Verwendung sperrt.

Beispiel:

UC_{DS} = ’00 0A‘ (dezimal 10) ⇒ SRN_{DS} = **neg**(UC_{DS}) = ‘FF F5‘ (dezimal 65.525)

UC_{AUT} = ‘FA 1D‘ (dezimal 64.029) ⇒ SRN_{AUT} = **neg**(UC_{AUT}) = ’05 E2‘(dezimal 1506)

Dieser Algorithmus ist in der jeweiligen Anwendungssoftware zu realisieren.

Typ: DE
Format: an
Länge: ..14
Version: 1

Sicherheitsprofil

Verfahren zur Absicherung der Transaktionen, das zwischen Kunde und Kreditinstitut vereinbar wurde. Das Sicherheitsprofil wird anhand der Kombination der beiden Elemente „Sicherheitsverfahren“ und „Version“ bestimmt (z.B. RDH-3, DDV-1). Für das Sicherheitsverfahren PINTAN ist als Code der Wert PIN und als Version der Wert 1 einzustellen.

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Sicherheitsverfahren, Code	DE	code	3	M	1	DDV, RDH, PIN
2	Version des Sicherheitsverfahrens	DE	num	..3	M	1	1, 2, 3, 4, 5, 6, 7, 8, 9, 10

Typ: DEG
Format:
Länge:
Version: 1

Sicherheitsreferenznummer

Sicherheitsrelevante Nachrichtenidentifikation (Signatur-ID), welche zur Verhinderung der Doppeleinreichung, respektive Garantie der Nachrichtensequenzintegrität eingesetzt werden kann.

Bei chipkartenbasierten Verfahren ist der Sequenzzähler der Chipkarte einzustellen. Dies ist bei Typ-1 Karten der Wert „EF_SEQ“ in der Application DF_BANKING und bei SECCOS Bankensignaturkarten der Wert „usage counter“ der beiden Signierschlüssel SK.CH.DS und SK.CH.AUT.

Bei softwarebasierten Verfahren wird die Sicherheitsreferenznummer auf Basis des DE Kundensystem-ID und des DE Benutzerkennung der DEG Schlüsselnamen verwaltet.

Typ: DE
Format: num
Länge: ..16
Version: 1

Sicherheitsverfahren, Code

Code des unterstützten Signatur- bzw. Verschlüsselungsalgorithmus.

Weitere Informationen zu den Verfahren sind Kapitel B.1 zu entnehmen.

Codierung:

DDV: DES-DES-Verfahren

RDH: RSA-DES-Hybridverfahren