A.1.1.1 Änderung eines öffentlichen Schlüssels des Kunden (Original B.6.2.1)

Realisierung Bank: verpflichtend
Realisierung Kunde: verpflichtend

a) Kundennachricht

- **Beschreibung**

Diese Nachricht ist nur bei Verwendung des RDH-Verfahrens möglich. Der Nachricht muss eine Dialoginitialisierung vorausgehen. Der Auftrag muss mit dem alten Signierschlüssel signiert werden.

Es muss unterschieden werden, ob die Schlüsseländerung auch das Sicherheitsprofil wechselt oder nicht.

Die folgenden Wechselmöglichkeiten bestehen, falls Sicherheitsprofilwechsel unterstützt sind:

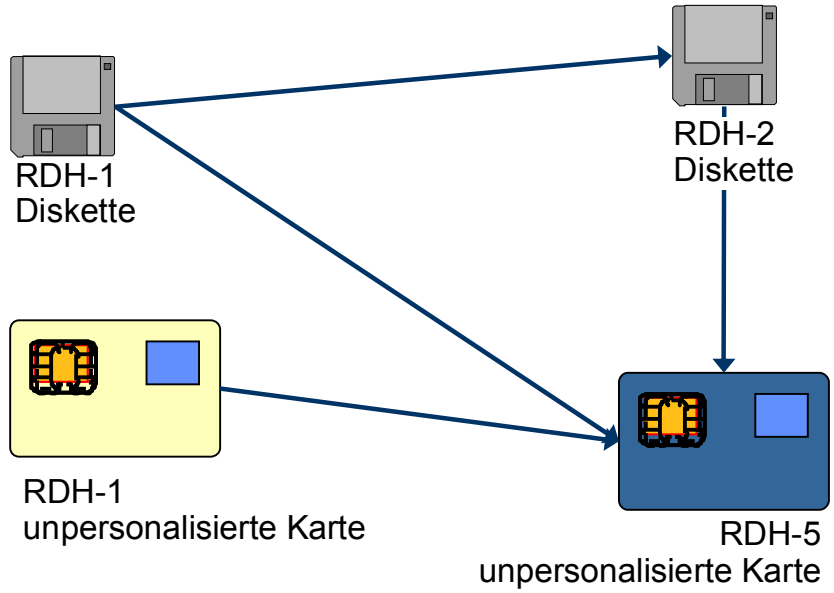

Abbildung 1: Unterstützte Sicherheitsprofilwechsel

Konkret sind dies folgende Wechselmöglichkeiten:

RDH-x (aktuelles Verfahren)	**RDH-y (neues Verfahren)**
RDH-1 Diskette	RDH-2 Diskette
RDH-1 Diskette	RDH-5 unpersonalisierte Karte
RDH-1 unpersonalisierte Karte	RDH-2 Diskette
RDH-1 unpersonalisierte Karte	RDH-5 unpersonalisierte Karte
RDH-2 Diskette	RDH-5 unpersonalisierte Karte

1. ohne Wechsel des Sicherheitsprofils:

   Nach der erfolgreichen Durchführung der Schlüsseländerung wird der vorher aktuelle Schlüssel automatisch gesperrt. Es ist darauf zu achten, dass die Version des neuen Schlüssels höher ist als die des alten Schlüssels.

2. mit Wechsel des Sicherheitsprofils (vgl. Abbildung 1: Unterstützte Sicherheitsprofilwechsel):

   Bei einem Sicherheitsprofilwechsel muss der Kunde immer beide HKSAKSegmente einstellen. Nach der erfolgreichen Durchführung der Schlüsseländerung wird durch das Kreditinstitut mitgeteilt, ob der vorher aktuelle RDH-x-Schlüssel automatisch gesperrt wurde. Diese Nachricht wird mit den RDH-x-Schlüsseln abgesichert. Wurden die RDH-x-Schlüssel institutsseitig nicht gesperrt, wird der Dialog unter Absicherung der RDH-x-Schlüssel beendet. Es ist darauf zu achten, dass die Nummer der RDH-2-Schlüssel 2 ist, die Version kann mit 1 beginnen. Bei RDH-5 sind Schlüsselnummer und –version vorgegeben.

> Falls das Kreditinstitut nicht in der Lage ist, zwei Schlüsselpaare zu einem Kunden gleichzeitig zu halten und somit die Endenachricht mit den RDH-x-Schlüsseln nicht mehr bedienen kann, ist dies dem Kundenprodukt durch den HIRMS-Code 3250 mitzuteilen. Das Kundenprodukt soll dann keine Endenachricht mehr senden und den Bankdatensatz von der RDH-x-Diskette löschen.

Es empfiehlt sich, die RDH-x-Schlüssel nach einem erfolgreichen Abschluss des Dialoges durch einen Sperrdialog ungültig zu machen.

: Falls der Kunde eine Schlüsseländerungsnachricht sendet, diese aber aus kreditinstitutsinternen Verarbeitungsgründen nicht beantwortet wird, sollte das Kundenprodukt zunächst einen neuen Dialog auf Basis eines der Schlüsselpaare aufbauen. Falls diese Nachricht abgelehnt wird ist ein erneuter Versuch auf Basis eines anderen Schlüsselpaares vorzunehmen. Aus der Reaktion des Kreditinstituts ist für das Kundenprodukt ersichtlich, ob die Schlüsseländerung erfolgreich war oder wiederholt werden muss.
Da ein D-Schlüssel, der ja eine natürliche Person identifizieren soll, nicht ohne weiteres geändert werden kann, dürften nur "1..2" HKSAK-Segmente eingestellt werden.

Zum Verfahren s. Kap. **Fehler! Verweisquelle konnte nicht gefunden werden.**.

- **Format**

Name:	Änderung eines öffentlichen Schlüssels des Kunden
Typ:	Nachricht
Version:	4
Sender:	Kunde

Nr.	Name	Typ	Kennung	Status	Anzahl	Anmerkungen
1	Nachrichtenkopf	SEG	HNHBK	M	1	s. [Formals], Kap. II.5.1
2	Signaturkopf	SEG	HNSHK	M	1	
3	Schlüsseländerung	SEG	HKSAK	M	1..3	
4	Signaturabschluss	SEG	HNSHA	M	1	
5	Nachrichtenabschluss	SEG	HNHBS	M	1	s. [Formals], Kap. II.5.2

- **Belegungsrichtlinien**

Schlüsseländerung

b) Der Kunde stellt entweder seinen neuen öffentlichen Signierschlüssel, seinen neuen öffentlichen Chiffrierschlüssel oder beide Schlüssel ein.Kreditinstitutsnachricht

- **Format**

Name: Kreditinstitutsnachricht allgemein
Typ: Nachricht
Format: s. [Formals], Kap. II.8.1

- **Erläuterungen**

Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel
0020	Öffentlicher Schlüssel wurde geändert
3250	RDH-1-Schlüssel wurden gesperrt. Endenachricht nicht mehr möglich.
3260	RDH-1-Schlüssel weiterhin gültig. Schlüsselsperre wird empfohlen.
9210	Schlüsseländerung von RDH-1 auf RDH-2 zur Zeit nicht möglich
9010	Schlüsseländerung zur Zeit nicht möglich
9010	Sicherheitsverfahren unterstützt keine öffentlichen Schlüssel
9210	Eingereichter Schlüssel ist mit dem aktuellen Schlüssel identisch