B. VERFAHRENSBESCHREIBUNG

B.3 Allgemeines

B.3.1 Sicherheitsprofile

B.3.2 Sicherheitsklassen

…

Die Festlegungen durch die Sicherheitsklasse zum verpflichtenden Senden von Zertifikaten wird auch durch die Zertifikatssteuerung (Parametersegment HICERS) beeinflusst (siehe Kapitel B.3.2.3.2.1).

…

B.3 Abläufe

B.3.1 Schlüsselverwaltung

B.3.1.3 Asymmetrische Schlüssel für RAH und RDH

B.3.1.3.2 Behandlung von Zertifikaten

In FinTS ist die Verwendung von Zertifikaten durch die vorgesehenen Elemente unterstützt, es existieren jedoch außer der Zertifikatssteuerung durch das Parametersegment HICERS (siehe Kapitel B.3.2.3.2.1) keine Prozesse für das Zertifikatsmanagement. Diese sollen zu einem späteren Zeitpunkt auf Basis einer standardisierten Zertifizierungsinfrastruktur übernommen werden.

Folgende Festlegungen gelten für die Belegung der Zertifikats-Datenelemente in den FinTS-Segmenten:

1. Allgemein
   Bei Verwendung des Signaturschlüssels (D-Schlüssel) mit Sicherheitsklasse 3 bzw. 4 wird grundsätzlich in allen Nachrichten das entsprechende Zertifikat im Signaturkopf mit geschickt.

   Bei Verwendung des Authentifikationsschlüssels (S-Schlüssel) mit Sicherheitsklasse 2 kann das entsprechende Zertifikat in den Signaturkopf eingestellt werden.
   Ebenso kann ein Benutzer das Zertifikat seines Chiffrierschlüssels (V-Schlüssel) in den Verschlüsselungskopf einstellen. Ggf. dort eingestellte Verschlüsselungszertifikate können vom Institut ignoriert werden. Wird eine Kundennachricht nicht signiert (z. B. optional bei HKEND), so muss bei Verwendung von zertifikatsbasierten Sicherheitsverfahren das Zertifikat des Chiffrierschlüssels in den Verschlüsselungskopf eingestellt werden. Damit ist das Institut in der Lage, die

Antwort an das Kundenprodukt verschlüsselt zu übertragen und muss den Dialog nicht mit einer Fehlermeldung wegen eines fehlenden Verschlüsselungsschlüssels des Benutzers beenden. Vorgaben für die Belegung der Zertifikatselemente werden außer durch die Sicherheitsklasse des Geschäftsvorfalls (vgl. Kapitel B.3.2) auch durch die Zertifikatssteuerung (vgl. Kapitel B.3.2.3.2.1) festgelegt.

2. Erstmalige Übermittlung Kundenschlüssel bzw. Schlüsseländerung

   Bei der erstmaligen Übermittlung der Kundenschlüssel bzw. bei der Schlüsseländerung wird grundsätzlich der Authentifikationsschlüssel (S-Schlüssel) und wahlweise das zugehörige Zertifikat verwendet. Das Zertifikat wird in diesem Fall nur in das vorgesehene Element im Geschäftsvorfall (HKSAK bzw. HKISA) eingestellt (nicht in den Signaturkopf).

3. Signaturkarten-Profil mit drei unterschiedlichen Schlüsseln

   Wenn ein Signaturkarten-Profil mit drei unterschiedlichen Schlüsseln verwendet wird, muss bei der erstmaligen Übermittlung der Kundenschlüssel bzw. der Schlüsseländerung auch die Möglichkeit bestehen, das Zertifikat für den eigenen Verschlüsselungsschlüssel im jeweiligen Geschäftsvorfall (HKSAK bzw. HKISA) mitzuschicken.

B.3.1.3.2.1 Parametersegment Zertifikatssteuerung (HICERS)

Das Parametersegment „Zertifikatssteuerung (HICERS)“ legt übergreifende Regeln für die Übermittlung von Zertifikatsinformationen zwischen Kunden- und Institutssystem fest und ermöglicht so die Verwendung von Zertifikaten in FinTS ohne institutseigene Schlüsselverwaltung.

Ohne Verwendung der Zertifikatssteuerung werden ggf. auf der Bankensignaturkarte enthaltene Zertifikate nur im Rahmen der Schlüsselersteinreichung bzw. –Änderung und bei Geschäftsvorfällen in Abhängigkeit von der Sicherheitsklasse vom Kundensystem zum Kreditinstitut gesendet.

Ist in den BPD ein Parametersegment „Zertifikatssteuerung (HICERS)“ enthalten, so befinden sich darin zusätzliche Informationen, die im Speziellen die Übertragung von Zertifikaten während der Dialoginitialisierung regeln. Durch entsprechende Parametrisierung kann aber auch die Steuerung über die GV-Sicherheitsklasse außer Kraft gesetzt und damit sichergestellt werden, dass bei jedem Geschäftsvorfall relevante Zertifikatsinformationen mitgeschickt werden.

Abhängig von den Parametern der Zertifikatssteuerung gelten folgende Regeln für die Belegung der Zertifikatselemente in den Kundennachrichten:

D-Schlüssel	DEG „Zertifikat“ im Signaturkopf	bei Geschäftsvorfällen der Sicherheitsklasse 3 oder 4
S-Schlüssel	DEG „Zertifikat“ im Signaturkopf	Bei der Dialoginitialisierung und ggf. Geschäftsvorfällen der Sicherheitsklasse 1 oder 2
V-Schlüssel	DEG „Zertifikat“ im Verschlüsselungskopf	Bei der Dialoginitialisierung und ggf. Geschäftsvorfällen der Sicherheitsklasse 1 bis 4

~~Eine Übertragung von Zertifikaten pro Geschäftsvorfall wird nur in speziellen Situationen benötigt. Im Normalfall wird das Kreditinstitut die Zertifikatsinformationen aus der Dialoginitialisierung nach erfolgreicher Prüfung zwischenspeichern und für den gesamten Dialog verwenden.~~

Realisierung Bank: verpflichtend, falls ein Institut die Zertifikatssteuerung verwendet
Realisierung Kunde: verpflichtend, falls ein Institut die Zertifikatssteuerung verwendet

c) Bankparameterdaten

♦ Format

Name: Zertifikatssteuerung Parameter
Typ: Segment
Segmentart: Geschäftsvorfall mit Parametern
Kennung: HICERS
Bezugssegment: HKVVB
Version: 1
Sender: Kreditinstitut

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	1	DEG			M	1	
2	Maximale Anzahl Aufträge	1	DE	num	..3	M	1	
3	Anzahl Signaturen mindestens	1	DE	num	1	M	1	0, 1, 2, 3
4	Sicherheitsklasse	1	DE	code	1	M	1	0, 1, 2, 3, 4
5	Parameter Zertifikatssteuerung	1	DEG			M	1	

♦ Ausgewählte Beispiele für Rückmeldungscodes

Code	Beispiel
9351	Zertifikat noch nicht gültig
9352	Zertifikat zurückgezogen bzw. gesperrt
9353	Zertifikatssignatur falsch
9354	Zertifizierungsinstanz (Herausgeber) nicht akzeptiert
9355	Fehler im Zertifikatsaufbau
9356	Zertifikatstyp nicht akzeptiert
9357	Zertifikat erwartet aber nicht im Signaturkopf enthalten
9357	Zertifikat erwartet aber nicht im Chiffrierkopf enthalten

B.4 Formate für Signatur und Verschlüsselung

B.4.1 Verschlüsselungskopf

♦ **Beschreibung**

Der Verschlüsselungskopf enthält Informationen über die Art des Sicherheitsservice, die Verschlüsselungsfunktion und die zu verwendenden Chiffrierschlüssel.

Zum Abgleich mit den in den BPD definierten Verschlüsselungsverfahren DDV bzw. RAH und RDH wird das Feld „Bezeichner für Algorithmusparameter, Schlüssel“ in der DEG „Verschlüsselungsalgorithmus“ herangezogen.

♦ **Format**

Name: Verschlüsselungskopf
Typ: Segment
Segmentart: Administration
Kennung: HNVSK
Bezugssegment: -
Version: 3
Sender: Kunde/Kreditinstitut

Nr.	Name	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	DEG			M	1	
2	Sicherheitsprofil	DEG			M	1	
3	Sicherheitsfunktion, kodiert	DE	code	..3	M	1	4
4	Rolle des Sicherheitslieferanten, kodiert	DE	code	..3	M	1	1, 4
5	Sicherheitsidentifikation, Details	DEG			M	1	
6	Sicherheitsdatum und -uhrzeit	DEG			M	1	
7	Verschlüsselungsalgorithmus	DEG			M	1	
8	Schlüsselname	DEG			M	1	
9	Komprimierungsfunktion	DE	code	..3	M	1	
10	Zertifikat	DEG			C	1	O: kreditinstitutsseitig bei RAH-7, RAH-9, sowie RDH-1, RDH-2, RDH-3, RDH-5 RDH-6, RDH-7, RDH-8 und RDH-9 (vgl. B.3.1.3.2) bzw. kundenseitig bei RAH-7, RDH-6 und RDH-7 N: sonst

♦ **Belegungsrichtlinien**

Sicherheitsdatum und -uhrzeit

Als Bezeichner (DE Datum- und Zeitbezeichner, kodiert) wird „1“ (Sicherheitszeitstempel) eingestellt.

Zertifikat

Im Falle der Bankensignaturkarte ist das Zertifikat EF_C_X509.CH.KE anzugeben.

D. DATA DICTIONARY

P

Parameter Zertifikatssteuerung

Festlegung der Parameter für die Zertifikatssteuerung.

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Priorität der Zertifikatssteuerung	1	DE	code	1	M	1	0, 1
2	Zertifikatsverarbeitung verpflichtend	1	DE	jn	#	M	1	
3	Unterstützte Zertifikatsarten	1	DEG			O	1	
4	Unterstützte Sicherheitsverfahren	3	DEG			O	1..9	

♦ Belegungsrichtlinien

Unterstützte Zertifikatsarten

Ist diese Datenelementgruppe vorhanden, so dürfen nur Zertifikate der dort enthaltenen Zertifikatsarten (D, S, V) belegt und gesendet werden. Wird die DEG weggelassen sind situationsabhängig alle in der Bankensignaturkarte enthaltenen Zertifikate zu senden. Sind auf der Bankensignaturkarte weniger Zertifikate enthalten, als in den unterstützten Zertifikatsarten angegeben, so sind die nicht vorhandenen Zertifikatsarten zu ignorieren.

Beispiel: Laut Element „Unterstützte Zertifikatsarten“ sind die Zertifikate des Signier- und Chiffrierschlüssels zu übertragen. Es existieren jedoch Kartengenerationen, die nur einen gemeinsamen Signier-/Chiffrierschlüssel enthalten. In diesem Fall ist das Zertifikat des Signierschlüssels im Signaturkopf einzustellen und zu übertragen. Die DEG „Zertifikat“ im Verschlüsselungskopf bleibt hingegen leer. Für die Verschlüsselung der Nachricht auf Kreditinstitutsseite wird dann der öffentliche Schlüssel aus dem Zertifikat des Signierschlüssels verwendet.
Ausnahme: Handelt es sich um ein nicht signierte Kundennachricht (z. B. optional bei HKEND), so ist das Zertifikat des gemeinsamen Signier-/Chiffrierschlüssels in den Verschlüsselungskopf einzustellen.

Wird in „Unterstützte Zertifikatsarten“ nur das Signierzertifikat (S-Schlüssel) eingestellt, so wird dieses bei Geschäftsvorfällen der Sicherheitsklasse 1 oder 2 auch für die Verschlüsselung der Kreditinstitutsnachricht(en) genutzt. Handelt es sich jedoch um einen Geschäftsvorfall der Sicherheitsklasse 3 oder 4 mit verpflichtender Übertragung des Signaturzertifikats (D-Schlüssel), so ist das Signaturzertifikat in den Signaturkopf und das Verschlüsselungszertifikat in den Verschlüsselungskopf einzustellen.

Unterstützte Sicherheitsverfahren

Ist diese Datenelementgruppe vorhanden, so gelten die Parameter der Zertifikatssteuerung für die dort enthaltenen Sicherheitsprofile. Wird die DEG weggelassen, gilt die Parametrisierung für alle Sicherheitsprofile, die Zertifikate unterstützen.

Es dürfen nur Sicherheitsverfahren belegt werden, die auch Zertifikate unterstützen. Aktuell sind für die in der DEG enthaltenen Elemente also folgende Kombinationen für die Verfahren RAH-7, RDH-6 und RDH-7 möglich:

Sicherheitsverfahren, Code: RAH, RDH

Version des Sicherheitsverfahrens: 6, 7

Typ:	DEG
Format:	
Länge:	
Version:	1

Priorität der Zertifikatssteuerung

Festlegung des Wirkungsbereichs der Zertifikatssteuerung.

Code-Bedeutung :
0 : Zertifikate(e) Senden ist abhängig von der Sicherheitsklasse
1 : Zertifikate(e) Senden ist verpflichtend

Bei „0“ gelten die Angaben für die Zertifikatssteuerung nur für die Dialoginitialisierung und alle damit in Verbindung stehenden Segmente. Die Steuerung, ob ein Zertifikat bei einem signierten Geschäftsvorfall mit gesendet werden soll erfolgt über dessen Sicherheitsklasse.

Bei „1“ wird die Angabe der Sicherheitsklasse bei Geschäftsvorfällen ignoriert und Zertifikatsinformationen müssen für die definierten Sicherheitsprofile immer gesendet werden, wie in HICERS festgelegt.

Bei Geschäftsvorfällen in Segmentversionen, die vor FinTS V3.0 spezifiziert wurden ist die Sicherheitsklasse noch nicht als DE enthalten. Daher kann mit „Priorität der Zertifikatssteuerung“=1 bei Bedarf das generelle Senden von Zertifikaten erzwungen werden.

Typ:	DE
Format:	code
Länge:	1
Version:	1

U

Unterstützte Sicherheitsverfahren (Anm.: aus FinTS V3.0 Formals)

Information über die kreditinstitutsseitig unterstützten Sicherheitsverfahren. Anhand der Kombination der beiden Elemente „Sicherheitsverfahren“ und „Version“ wird das Sicherheitsprofil (z.B. RAH-7) bestimmt.

Die Definition der Felder ist in [HBCI] enthalten.

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

Um Multibankfähigkeit zu gewährleisten, ist die Unterstützung eines der Verfahren RAH-9 bzw. übergangsweise RDH-9 kunden- und kreditinstitutsseitig verpflichtend.

Typ: DEG
Format:
Länge:
Version: 3

Unterstützte Zertifikatsarten

Diese DEG enthält die relevanten Zertifikatsarten für die Zertifikatssteuerung. Es werden nur die dort definierten Zertifikatsarten (D, S, V) berücksichtigt.

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Zertifikat D-Schlüssel vorhanden	1	DE	jn	#	M	1	
2	Zertifikat S-Schlüssel vorhanden	1	DE	jn	#	M	1	
3	Zertifikat V-Schlüssel vorhanden	1	DE	jn	#	M	1	

Typ: DEG
Format:
Länge:
Version: 1

Z

Zertifikat D-Schlüssel vorhanden

Information, ob ein Zertifikat für den D-Schlüssel (Signaturschlüssel) vorhanden ist.

Typ: DE
Format: jn
Länge: #
Version: 1

Zertifikat S-Schlüssel vorhanden

Information, ob ein Zertifikat für den S-Schlüssel (Signierschlüssel) vorhanden ist.

Typ: DE
Format: jn
Länge: #
Version: 1

Zertifikat V-Schlüssel vorhanden

Information, ob ein Zertifikat für den V-Schlüssel (Chiffrierschlüssel) vorhanden ist.

Typ: DE
Format: jn
Länge: #
Version: 1

Zertifikatsverarbeitung verpflichtend

Festlegung, ob vom Kreditinstitut übertragene Zertifikate vom Kundensystem verpflichtend zu prüfen und zu verwenden sind. In diesem Fall werden über den FinTS-Key-Management-Geschäftsvorfall HKISA keine neuen Schlüssel des Kreditinstituts zur Verfügung gestellt.

Derzeit ist nur der Wert „n“ zugelassen.

Typ: DE
Format: jn
Länge: #
Version: 1