

Spezifikation

FinTS - Format der RDH-10-Sicherheitsdiskette

Dokument-	
version:	1
Status:	Freigegeben
Datum:	20.06.2008
Autor:	Gabriele Wilms

Versionsführung für Dokument **Spezifikation der FinTS RDH-10 Sicherheitsdiskette V1.doc**

Name	Datum	Doku-ment-version	Bemerkungen
Gabriele Wilms	20.06.2008	1	Initialversion

Copyright
Dieses Dokument wurde von der PPI AG Informationstechnologie erstellt und ist gegenüber Dritten urheberrechtlich geschützt. Alle Rechte, auch die der Übersetzung, des Nachdrucks oder der Vervielfältigung des gesamten Dokumentes oder Teilen daraus, bedürfen der Zustimmung der PPI AG Informationstechnologie.

Inhaltsverzeichnis

1	Einleitung	4
2	Begriffsvereinbarungen	5
2.1	Kryptografische Primitive	5
2.1.1	Padding nach RFC 1423	5
2.1.2	Passwort Restriktionen	5
2.1.3	Schlüsselableitung	5
2.1.4	MAC-Bildung	5
2.1.5	Verschlüsselung	6
2.2	Typdefinitionen	6
2.3	TLV-Beschreibung	6
3	Aufbau der Diskette	7
3.1	Kopf der Diskettenbeschreibung	8
3.2	Kreditinstitutsverbindung	9
3.2.1	Kreditinstitutsverbindungsdaten	10
3.2.2	Schlüsseleintrag	12
3.3	Öffentliche Schlüssel des Kreditinstitutes	13
3.4	Datum	14
3.5	MAC	14
	Literaturverzeichnis	15

1 Einleitung

Diese Spezifikation beschreibt das Format der Sicherheitsdiskette für das RDH-10-Verfahren gemäß ZKA: *FinTS 3.0 Security Sicherheitsverfahren HBCI* ([3]). Es wird sowohl der formale Aufbau der Diskette als auch die Belegung der einzelnen Felder für die Verwendung als RDH-10-Sicherheitsmedium im Rahmen des FinTS-Protokolls beschrieben.

2 Begriffvereinbarungen

In den folgenden Abschnitten werden die in diesem Dokument gültigen Begriffe erläutert.

2.1 Kryptografische Primitive

Die verwendeten kryptografischen Definitionen werden nachfolgend dargelegt.

2.1.1 Padding nach RFC 1423

Das Padding wird nach RFC 1423 vorgenommen (siehe *RFC 1423 - Privacy Enhancement for Internet Electronic Mail* [2]). Dies geschieht wie folgt:

- Es wird auf das nächste Vielfache von 8 aufgefüllt, wobei folgende Paddings in hexadezimaler Darstellung möglich sind: 01, 0202, 030303, 04040404, 0505050505, 060606060606, 07070707070707 und 0808080808080808.
- Es werden 1 bis 8 Bytes gepadded.

2.1.2 Passwort Restriktionen

Das Passwort muss folgende Bedingungen erfüllen:

- die Mindestlänge beträgt 8 Zeichen
- es enthält mindestens eines der folgenden Sonderzeichen: . > < () + - & ? * ; , % : " ' \ =

2.1.3 Schlüsselableitung

Es wird die Schlüsselableitungsfunktion PBKDF2 des Kryptografie-Standards *PKCS #5 v2.1* (siehe *RSA Laboratories: PKCS #5 v2.1: Password-Based Cryptography Standard* [1]) verwendet, wobei Folgendes gilt:

- Das Salt ist auf der Diskette im Kopf der Diskettenbeschreibung (siehe Abschnitt *Kopf der Diskettenbeschreibung*, Seite 8) abgelegt.
- Die Anzahl der Iterationen ist im Kopf der Diskettenbeschreibung abgelegt.
- Das Passwort (siehe vorigen Abschnitt) wird vom Benutzer erfragt.

Des Weiteren wird bei der Schlüsselableitungsfunktion PBKDF2 (siehe *RSA Laboratories: PKCS #5 v2.1: Password-Based Cryptography Standard* [1]) ein HMAC mit SHA-256 gebildet.

2.1.4 MAC-Bildung

Der Schlüssel für die MAC-Bildung hat eine Länge von 32 Bytes und wird mittels Schlüsselableitung (siehe vorigen Abschnitt) gebildet.

Für die MAC-Bildung wird folgendes Authentifizierungsschema verwendet:

- HMAC-SHA-256 (siehe *RSA Laboratories: PKCS #5 v2.1: Password-Based Cryptography Standard* [1])

2.1.5 Verschlüsselung

Der Schlüssel DK (derived key) zur Verschlüsselung hat eine Länge von 24 Bytes und wird mittels Schlüsselableitung gebildet (siehe Abschnitt *Schlüsselableitung*, Seite 5). Für die einzelnen Verschlüsselungsschlüssel werden für Key_1 die Bytes 1-8, für Key_2 die Bytes 9-16 und für Key_3 die Bytes 17-24 verwendet.

Für die Verschlüsselung wird folgendes Verschlüsselungsschema verwendet:

- PKCS #5 (siehe *RSA Laboratories: PKCS #5 v2.1: Password-Based Cryptography Standard [1]*): DES-EDE3-CBC mit IV=0 und Padding nach RFC 1423, wobei für die Schlüsselableitung SHA-256 verwendet wird

2.2 Typdefinitionen

Sämtliche Längenangaben im Dokument erfolgen in Anzahl der belegten Bytes.

Folgende Typdefinitionen werden in dieser Spezifikation verwendet:

Format	Länge	Wertemenge	Beschreibung
Int	2		Little Endian Notation
Long	4		Little Endian Notation
Byte	Var	Binär	
Char	Var	ASCII-Zeichen	Inhalt linksbündig ausrichten und rechtsbündig mit Leerzeichen auffüllen
Keytype	1	X'00', X'01'	X'00' Signierschlüssel X'01' Chiffrierschlüssel

Byte-Folgen, welche als Zahl interpretiert werden, sind grundsätzlich im Little Endian-Format abgelegt.

2.3 TLV-Beschreibung

Die im Weiteren benutzte Formatbeschreibung setzt auf dem TLV-Format (Tag-Length-Value) auf. Sie kann ggf. auf weitere Untergruppierungen verweisen. Das TLV-Format ist folgendermaßen aufgebaut:

Feld	Format	Länge	Anzahl	Inhalt	Beschreibung
1	Byte	2	1		Tag
2	Int	2	1	Länge von Feld 3	Länge
3	Byte	Var	1		Wert

3 Aufbau der Diskette

Die Sicherheitsdiskette besteht auf oberster Ebene aus 5 Feldern, welche Informationen zur Diskette, die Kreditinstitutionsverbindungen des Kunden, die öffentlichen Schlüssel der Kreditinstitute, das Erstellungs- bzw. letzte Änderungsdatum und den MAC enthalten.

Die Diskette wird durch den MAC und partielle Verschlüsselung gegen Missbrauch geschützt:

- Der Gesamthalt wird durch einen MAC gegen Verfälschung gesichert.
- Der geheime private Schlüssel eines Schlüsseleintrags wird durch Verschlüsselung gegen missbräuchlichen Zugriff geschützt.

Feld	Tag	Länge	Anzahl	Beschreibung
1	VN = X'564E'	28	1	Kopf der Diskettenbeschreibung (siehe Abschnitt <i>Kopf der Diskettenbeschreibung</i> , Seite 8)
2	KV = X'4B56'	#	0..n	Kreditinstitutionsverbindung (siehe Abschnitt <i>Kreditinstitutionsverbindung</i> , Seite 9)
3	ÖS = X'D653'	#	0..n	Öffentliche Schlüssel des Kreditinstituts (siehe Abschnitt <i>Öffentliche Schlüssel des Kreditinstitutes</i> , Seite 13)
4	RD = X'5244'	14	1	Datum (siehe Abschnitt <i>Datum</i> , Seite 14)
5	DM = X'444D'	32	1	MAC über die Felder 1 bis 4 (siehe Abschnitt <i>MAC</i> , Seite 14)

Bemerkungen zur Belegung der Felder:

- Vor dem Arbeiten mit der Datei sollte diese geparkt werden und die Unversehrtheit durch Eingabe des Passwortes und anschließender Prüfung des MAC festgestellt werden. Danach können die Schlüssel genutzt werden.
- Es sind alle Felder lesbar mit Ausnahme der privaten geheimen Schlüssel (siehe Abschnitt *Geheimer Schlüssel*, Seite 12).
- Die Kreditinstitutionsverbindungen werden durch weitere TLV-Records beschrieben.
- Jede Kreditinstitutionsverbindung enthält die Verbindungsdaten sowie die für ein Kreditinstitut erzeugten Schlüsseleinträge zu den Kundenschlüsseln.

- Bei einem Schlüsselwechsel werden neue Schlüsseleinträge generiert. Sie gelten somit für genau diese Kreditinstitutsverbindung. Nach erfolgreicher Übertragung der neuen Schlüssel sind die alten Schlüsseleinträge zu löschen. Nach einem Wechsel des Signierschlüssels ist der Signaturzähler in den Kreditinstitutsverbindungsdaten zurückzusetzen.

3.1 Kopf der Diskettenbeschreibung

Feld	Format	Länge	Anzahl	Inhalt	Beschreibung
1	Int	2	1	10	RDH-Sicherheitsprofil
2	Int	2	1	1	Version der Diskettenbeschreibung
3	Byte	20	1		Salt
4	Long	4	1		Anzahl Iterationen

Bemerkungen zur Belegung der Felder:

- Das RDH-Sicherheitsprofil der Diskette wird mit 10 festgelegt.
- Die Version dieser Diskettenbeschreibung wird mit 1 festgelegt.
- Die Felder 1 und 2 können zur Unterscheidung einer RDH-10-Diskette von einer RDH-2-Diskette verwendet werden.
- Das Salt sollte kryptografisch einer möglichst breiten Verteilung genügen. Daher ist es sinnvoll, zur Erzeugung des Salt einen Zeitstempel zu verwenden, worüber mittels SHA-256 ein Hashwert gebildet wird (siehe *RSA Laboratories: PKCS #5 v2.1: Password-Based Cryptography Standard [1]*).
- Die Anzahl Iterationen sollte möglichst groß gewählt werden (siehe *RSA Laboratories: PKCS #5 v2.1: Password-Based Cryptography Standard [1]*).

3.2 Kreditinstitutsverbindung

Eine Kreditinstitutsverbindung besteht aus den Kreditinstitutsverbindungsdaten, die dem Kunden vom Kreditinstitut mitgeteilt werden oder über Nachrichten ausgetauscht werden, und den Schlüsseleinträgen, die von der Kundenanwendung generiert und dem Kreditinstitut mitgeteilt werden.

Feld	Tag	Länge	Anzahl	Beschreibung
1	KD = X'4B44'	237	1	Kreditinstitutsverbindungsdaten
2	SE = X'5345'	#	0, 2, 3, 4	Schlüsseleintrag

Bemerkungen zur Belegung der Felder:

- Die verschiedenen Kreditinstitutsverbindungen eines Kunden werden durch Länderkennzeichen, Kreditinstitutscode und Benutzerkennung referenziert. Diese finden sich in den Kreditinstitutsverbindungsdaten.
- In den Schlüsseleinträgen sind alle Daten zu den Kundenschlüsseln abgelegt. Es müssen keine Schlüsseleinträge vorhanden sein. Hierdurch besteht die Möglichkeit, die Kundenschlüssel erst bei Vorhandensein der Bankschlüssel in deren Länge zu generieren. Es müssen dann aber sowohl der Signier- als auch der Chiffrierschlüssel abgelegt werden.
- Für eine Schlüsseländerung können unabhängig voneinander entweder der Signier- oder der Chiffrierschlüssel oder beide neu generiert und abgelegt werden. Die maximale Anzahl der Schlüsseleinträge ist vier. Dann liegen zu den bereits übertragenen Signier- und Chiffrierschlüsseln jeweils noch nicht übertragene, neu generierte Signier- und Chiffrierschlüssel vor.
- Neu generierte und durch eine Schlüsseländerung zu übertragende Schlüssel werden an der höheren Schlüsselversion im Schlüsseleintrag erkannt. Die Schlüsselnummer wird nicht erhöht.

3.2.1 Kreditinstitutsverbindungsdaten

Länderkennzeichen, Kreditinstitutscode und Benutzerkennung bilden den Schlüssel für den Zugriff auf die Kreditinstitutsverbindungen. Die Verbindung zu den öffentlichen Schlüsseln des Kreditinstituts wird über Länderkennzeichen und Kreditinstitutscode gebildet.

Feld	Format	Länge	Anzahl	Inhalt	Beschreibung
1	Char	3	1		Länderkennzeichen
2	Char	30	1		Kreditinstitutscode
3	Char	60	1		Kreditinstitutsname
4	Char	30	1		Benutzerkennung
5	Char	30	1		Kunden-ID
6	Char	30	1		Kundensystem-ID
7	Byte	1	1		Kommunikationsdienst
8	Char	50	1		Kommunikationsadresse
9	Int	2	1		Signaturzähler
10	Byte	1	1		Schlüsselstatus

Bemerkungen zur Tabelle:

- Der Kreditinstitutsname kann vom Benutzer frei gewählt werden.
- Die Benutzerkennung und Kunden-ID (optional) werden dem Benutzer vom Kreditinstitut zugewiesen.
- Die Kundensystem-ID wird im Zuge der Erstinitialisierung übermittelt. Initial ist sie mit dem Zeichen 0 zu belegen.
- Die Kommunikationsdaten werden dem Benutzer vom Kreditinstitut mitgeteilt.
- Der Signaturzähler gibt den nächsten gültigen Wert für die Signatur-ID an. Er bezieht sich immer auf den aktiven Signierschlüssel, welcher anhand der niedrigeren Schlüsselversion erkennbar ist. Nach einem Wechsel des Schlüssels muss der Signaturzähler auf 1 zurückgesetzt werden.
- Der Schlüsselstatus enthält 8 Flags mit folgender Bedeutung:

Flag	Inhalt	Bedeutung
Bit 1	Ja=1, Nein=0	erstmalige Übermittlung der Kundenschlüssel notwendig
Bit 2	0	RFU (reserved for future use)
Bit 3	Ja=1, Nein=0	Institutsschlüssel sind validiert

Flag	Inhalt	Bedeutung
Bit 4	Ja=1, Nein=0	ausstehende Übermittlung des neuen öffentlichen Chiffrierschlüssels des Kunden bei Schlüsseländerung
Bit 5	Ja=1, Nein=0	ausstehende Übermittlung des neuen öffentlichen Signierschlüssels des Kunden bei Schlüsseländerung
Bit 6	Ja=1, Nein=0	Schlüsselsperre mit Erfolg durchgeführt (Information, da terminierte Sperrung erst in der Zukunft wirksam werden kann)
Bit 7	Ja=1, Nein=0	Leistungsprobleme bei Übermittlung neuer Schlüssel
Bit 8	0	RFU (reserved for future use)

3.2.2 Schlüsseleintrag

Feld	Format	Länge	Anzahl	Inhalt	Beschreibung
1	Byte	1	1	x'02'	RFU (reserved for future use)
2	Keytype	1	1		Schlüsseltyp
3	Int	2	1	10	Schlüsselnummer
4	Int	2	1		Schlüsselversion
5	Int	2	1		Länge öffentlicher Exponent
6	Byte	#	1	Little Endian	öffentlicher Exponent
7	Int	2	1		Länge öffentlicher Modulus
8	Byte	#	1	Little Endian	öffentlicher Modulus
9	Int	2	1		Länge des verschlüsselten geheimen Schlüssels
10	Byte	#	1	Little Endian	geheimer Schlüssel (verschlüsselt) (siehe Abschnitt <i>Geheimer Schlüssel</i> , Seite 12)

Bemerkungen zur Belegung der Felder:

- Die Schlüsselnummer ist mit 10 festgelegt.
- Die Schlüsselversion wird beim Generieren neuer Schlüssel um eins hochgezählt.
- Der geheime Schlüssel wird gemäß Verschlüsselung (siehe Abschnitt *Verschlüsselung*, Seite 6) mit dem Schlüssel DK verschlüsselt.
- Die Länge des Feldes 6 wird durch den Inhalt von Feld 5 festgelegt.
- Die Länge des Feldes 8 wird durch den Inhalt von Feld 7 festgelegt.
- Die Länge des Feldes 10 wird durch den Inhalt von Feld 9 festgelegt.

Geheimer Schlüssel

Der geheime Schlüssel ist Bestandteil eines Schlüsseleintrags. Er wird verschlüsselt abgelegt. Unverschlüsselt hat er folgenden Aufbau:

Feld	Format	Länge	Anzahl	Inhalt	Beschreibung
1	Int	2	1		Länge des Modulus n
2	Byte	#	1	Little Endian	Modulus $n=p*q$

Feld	Format	Länge	Anzahl	Inhalt	Beschreibung
3	Int	2	1		Länge der Primzahl p
4	Byte	#	1	Little Endian	Primzahl p
5	Int	2	1		Länge der Primzahl q
6	Byte	#	1	Little Endian	Primzahl q
7	Int	2	1		Länge von $d \bmod (p-1)$
8	Byte	#	1	Little Endian	$d \bmod (p-1)$
9	Int	2	1		Länge von $d \bmod (q-1)$
10	Byte	#	1	Little Endian	$d \bmod (q-1)$
11	Int	2	1		Länge von A_p
12	Byte	#	1	Little Endian	A_p
13	Int	2	1		Länge von A_q
14	Byte	#	1	Little Endian	A_q

Bemerkungen zur Belegung der Felder:

- Die Länge der Felder 2, 4, 6, 8, 10, 12 und 14 wird jeweils durch den Wert des Feldes festgelegt, das unmittelbar davor steht.
- A_p beinhaltet den Wert $q^{p-1} \bmod (n)$.
- A_q beinhaltet den Wert $n+1-A_p$.

3.3 Öffentliche Schlüssel des Kreditinstitutes

Die öffentlichen Schlüssel der Kreditinstitute werden über Länderkennzeichen und Kreditinstitutscode referenziert.

Feld	Format	Länge	Anzahl	Inhalt	Beschreibung
1	Char	3	1		Länderkennzeichen
2	Char	30	1		Kreditinstitutscode
3	Byte	1	1	x'02'	RFU (reserved for future use)
4	Keytype	1	1		Schlüsseltyp
5	Int	2	1		Schlüsselversion

Feld	Format	Länge	Anzahl	Inhalt	Beschreibung
6	Int	2	1		Schlüsselnummer
7	Char	30	1		Schlüsselname
8	Int	2	1		Länge öffentlicher Modulus
9	Byte	#	1	Little Endian	Öffentlicher Modulus
10	Int	2	1		Länge öffentlicher Exponent
11	Byte	#	1	Little Endian	Öffentlicher Exponent

Bemerkungen zur Belegung der Felder:

- Die Schlüsselverson und Schlüsselnummer werden dem Kunden vom Kreditinstitut mitgeteilt.
- Schlüsselname ist der Name des Schlüssels, der vom Kreditinstitut vergeben wurde.
- Die Länge des Feldes 9 wird durch den Inhalt des Feldes 8 festgelegt.
- Die Länge des Feldes 11 wird durch den Inhalt des Feldes 10 festgelegt.

3.4 Datum

Feld	Format	Länge	Anzahl	Inhalt	Beschreibung
1	Char	14	1		Datum letzter Änderung/Erstellung

Bemerkung zur Belegung der Felder:

- Das Datum liegt im Format JJJJMMTTHHMMSS vor.

3.5 MAC

Feld	Format	Länge	Anzahl	Inhalt	Beschreibung
1	Byte	32	1		MAC über den Disketteninhalt

Bemerkung zur Belegung der Felder:

- Der MAC wird gemäß MAC-Bildung (siehe Abschnitt *MAC-Bildung*, Seite 5) gerechnet.

Literaturverzeichnis

- [1] RSA Laboratories: PKCS #5 v2.1: Password-Based Cryptography Standard vom 05.10.2006
- [2] D. Balenson: RFC 1423 - Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers (Februar 1993)
- [3] ZKA: FinTS 3.0 Security Sicherheitsverfahren HBCI Final Draft vom 04.06.2007