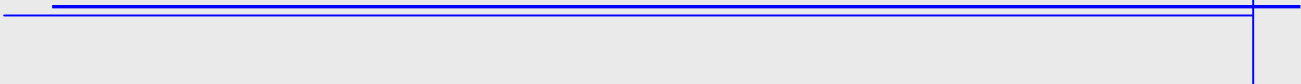
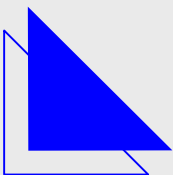


FinTS V4.0 Kompendium
Financial Transaction Services

Der Einstieg in die neue Welt
des Online-Banking



Vorwort

Das vorliegende FinTS V4.0 Kompendium versucht in knapper aber doch vollständiger Form Aufbau und Inhalt der FinTS V4.0 Spezifikation des Zentralen Kreditausschusses (ZKA) zu beschreiben. Es wendet sich primär an den interessierten Leser, der nur einen Überblick über FinTS erhalten möchte, soll aber auch dem technisch versierten Leser den Einstieg in die eigentliche Spezifikation erleichtern.

Das Kompendium erscheint seit der Version 1.0 des HBCI-Standards im Februar 1998 etwa zeitgleich mit der jeweiligen Version der Spezifikation. Mit dem Übergang auf die neue Bezeichnung FinTS – Financial Transaction Services ging mit der Version 3.0 mehr als nur eine Namensänderung vorstatten – der Standard erhielt mit der Banken-Signaturkarte ein gemeinsames strategisches Sicherheitsmedium und öffnete sich durch die Unterstützung des klassischen PIN/TAN-Verfahrens für neue Zugangswege. Auch die neue Dokumentenstruktur zeigte, dass sich FinTS auf den Weg gemacht hat, von einem klassischen Homebankingstandard zu einem Multifkanalbaukastensystem zu werden, das durch die Kombination verschiedener Kommunikations- und Sicherheitsverfahren auf Basis einer gemeinsamen Datenschnittstelle – bestehend aus Protokoll und multibankfähig definierten Geschäftsvorfällen – enorme Synergie- und Kosteneinsparungspotentiale mit sich bringen sollte.

FinTS V4.0 Die neue Version FinTS V4.0 macht nun den entscheidenden Schritt in Richtung Neuausrichtung des Standards. Endlich ist es gelungen, anstatt der doch etwas in die Jahre gekommenen Trennzeichensyntax auf zeitgemäße Standards der XML-Familie zu migrieren – und das mit aller Konsequenz. XML-Schema, XML-Signature und –Encryption sorgen zusammen mit den modernsten Modellierungstechniken dafür, dass FinTS den Grundstein für eine internationale Verwendung legt. Durch Datagrammtechnik und die neue Rolle des Intermediärs öffnet FinTS V4.0 den Weg für Push-Services und Portalunterstützung. Die verteilte Signatur macht den Standard für Firmenkunden interessant.

Ich hoffe, dass die Lektüre des vorliegenden FinTS V4.0 Kompendiums die Attraktivität dieser neu erschienenen ZKA-Spezifikation vermitteln und dazu beitragen kann, dem Standard zu breiter Akzeptanz am Markt zu verhelfen.

Kurt Haubner, Juni 2004

Inhaltsverzeichnis

1 Ausgangssituation 1997 und heute	1
1.1 Warum entstand 1997 HBCI?	1
1.2 Der Schritt von HBCI zu FinTS V3.0 und V4.0	3
1.2.1 Marktanalyse der Online-Banking Endgeräte	4
1.2.2 Anforderungen an FinTS V3.0 und V4.0.....	6
1.2.3 Neue Funktionen mit FinTS V3.0.....	6
1.2.4 Neue Funktionen mit FinTS V4.0.....	7
2 FinTS Formals und XML Syntax	9
2.1 Syntax.....	9
2.1.1 Zeichensatz.....	9
2.1.2 Inzwischen Historie: Die Trennzeichensyntax.....	9
2.1.3 XML-Syntax.....	10
2.1.4 Struktur der XML-Modellierung.....	10
2.1.5 Syntaktische Einheiten	12
2.1.6 Nachrichtenaufbau	13
2.2 Dialoge und Datagramme	14
2.2.1 Neu in FinTS V4.0 - Intermediäre und Szenarien	15
2.2.2 Initialisierung	16
2.2.3 Verallgemeinerung des Dialogbegriffs mit FinTS V4.0	18
2.2.4 Datagrammtechnik.....	18
2.2.5 Publish / Subscribe und Push-Services.....	19
2.2.6 Rückmeldecodes	19
2.2.7 Statusprotokoll.....	19
2.2.8 Verteilte Signaturen.....	20
2.3 Parameterdaten in FinTS V3.0	21
2.3.1 Allgemeines zu FinTS V3.0-Parameterdaten.....	21
2.3.2 Neu mit FinTS V4.0 – IPD und UPDI.....	22
2.3.3 Aufbau der BPD (Bankparameterdaten)	22
2.3.4 Aufbau der UPD (Userparameterdaten) und IPD	23
3 FinTS Security	24
3.1 Sicherheitsaspekte	24
3.1.1 Authentisierung des Kunden.....	25
3.1.2 Gegenseitige Authentisierung Kundensystem / Banksystem	25
3.1.3 Nachweis der Herkunft	25
3.1.4 Integrität - Elektronische Signatur	25
3.1.5 Geheimhaltung - Verschlüsselung / Chiffrierung	26
3.1.6 Validität - Doppeleinreichungskontrolle	26
3.1.7 Schlüsselverwaltung (Key-Management)	27

3.2 Sicherheitsverfahren HBCI.....	27
3.2.1 Sicherheitsmedien	29
3.2.2 Sicherheitsprofile	31
3.2.3 Sicherheitsklassen	32
3.2.4 Komprimierung.....	33
3.3 Sicherheitsverfahren PIN/TAN.....	33
4 FinTS Messages.....	34
4.1 Zahlungsverkehr Inland	34
4.1.1 Einzelaufträge.....	34
4.2 Sammelaufträge	35
4.2.1 Sammelüberweisung und Sammellastschrift	35
4.2.2 Terminierte Sammelüberweisung und Sammellastschrift	35
4.3 Umsatzinformationen.....	35
4.3.1 Abruf von Kontoumsätzen	35
4.3.2 Saldenabfrage	36
4.4 Termineinlagen	36
4.5 Wertpapiere	37
4.5.1 Wertpapierorder	37
4.5.2 Statusinformationen	37
4.5.3 Depotinformationen	37
4.5.4 Wertpapierinformationen.....	38
4.6 Zahlungsverkehr Ausland	38
4.7 Karten, Schecks und Formulare	38
4.8 Sorten, Devisen und Reiseschecks.....	39
4.9 Informationen	39
4.9.1 Freitextmeldungen	39
4.9.2 Formatierte Meldungen.....	39
4.10 Sonstiges	40
4.10.1 Freistellung von Zinserträgen.....	40
4.10.2 Transfer von beliebigen Dokumenten.....	40
4.10.3 GeldKarten-Transaktionen	40
4.10.4 Empfangsquittung	41
4.11 Ausblick - Weitere Geschäftsvorfälle in Planung.....	42
5 Transportmedienspezifische Festlegungen	43
5.1 Transportverfahren bis einschließlich FinTS V3.0.....	43
5.1.1 T-Online Classic mit ETSI 300 072 ("CEPT") / EHKP / BtxFIF	43
5.1.2 TCP/IP.....	43
5.1.3 https mit PIN/TAN-Sicherheit	44

5.2 Transportverfahren mit FinTS V4.0	44
5.2.1 Webservices und SOAP	44
5.3 Chipkartenanwendungen	44
5.3.1 DDV-Chipkarten Typ-0 und Typ-1	44
5.3.2 ZKA Banken-Signaturkarte mit SECCOS-Betriebssystem.....	45
6 FinTS-Kundensysteme	46
6.1 Infrastruktur-Sicherheit	46
6.2 Typisierung der FinTS Kundensysteme	47
6.2.1 Finanz-Management-Software	47
6.2.2 Browserbasierte Lösungen	47
6.2.3 Mobile Banking	48
6.2.4 Sonstige Kundensysteme.....	49
7 Positionierung im internationalen Umfeld	50
7.1 OFX – Open Financial Exchange	50
7.2 IFX – Interactive Financial Exchange	50
7.3 SWIFT XML	50
7.4 ebXML – electronic Business XML.....	51
7.5 Ausblick.....	52

© SIX SIGMA EDV-Konzepte, 2004

Das vorliegende FinTS V4.0 Kompendium ist ein urheberrechtlich geschütztes Dokument und Eigentum der Six Sigma EDV-Konzepte Kurt Haubner, München.

Weitergehende Veröffentlichungen, Nachdruck, Vervielfältigungen oder Speicherung - gleich in welcher Form, ganz oder teilweise - sind nur mit Zustimmung des Autors zulässig.

Bitte beachten Sie, dass es sich bei der vorliegenden Dokumentation um ein im Sinne des Copyright (©) geschütztes Dokument handelt!

Diese Dokumentation enthält neben Erläuterungen, Bewertungen und eigenen Erhebungen Beschreibungen von Herstellerprodukten, Schnittstellen und Konzepten, die auf entsprechenden Veröffentlichungen der jeweiligen Hersteller beruhen.

1 Ausgangssituation 1997 und heute

Das vorliegende FinTS V4.0 Kompendium erscheint – wie bei den HBCI-Vorgängerversionen – parallel zum entsprechenden Banking-Standard des ZKA („Zentraler Kredit Ausschuss“ der Spitzenverbände der Privatbanken, Genossenschaftsbanken, Sparkassen und öffentlichen Banken).

Anders als in den vorausgegangenen HBCI-Kompendien V1.0 bis V3.0 kündigt sich nun aber eine Neuausrichtung des Standards an, welche eine grundlegende Überarbeitung der Beschreibung der Ausgangssituation erfordert. Um andererseits die wesentlichen Aspekte der Beweggründe für die Schaffung des Standards HBCI – Homebanking Computer Interface - und heute FinTS besser nachvollziehen zu können, finden Sie nachfolgend jedoch auch ein Kapitel zur historischen Entwicklung.

1.1 Warum entstand 1997 HBCI?

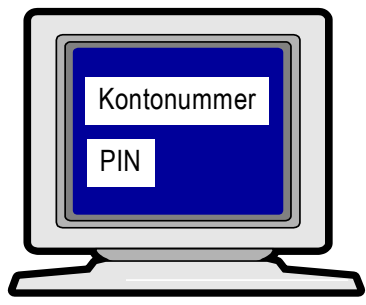
Zunächst zur damaligen Definition des Begriffes "Homebanking": In Abgrenzung zu Telefonbanking mit einem Call Center, wo die Kommunikation mit Sprachmitteln erfolgt, kommen für Homebanking Personal Computer oder andere intelligente Endgeräte (z. B. Komforttelefon, Set-Top-Boxen, Mobiltelefone) zum Einsatz. In jedem Falle handelt es sich bei Homebanking aber nicht nur um Informationsabruf, sondern auch um Geschäftsabwicklung. Dabei ist es im ersten Ansatz unerheblich, ob diese Abwicklung „Online“, d. h. in einem Dialog mit bestehender Telefonverbindung oder „Offline“ erfolgt, wobei die Aufträge zunächst lokal erfasst und dann gebündelt übertragen werden.

FinTS ist ein Standard zur Kommunikation zwischen intelligenten Kundensystemen und entsprechenden Bankrechnern zur Durchführung von Homebanking-Transaktionen, der 1997 in einer ersten Version veröffentlicht wurde und nun durch FinTS V4.0 abgelöst bzw. neu ausgerichtet wird. Der Datentransfer wird bei FinTS über eine Nachrichtenschnittstelle abgewickelt, die – ursprünglich auf einer EDIFACT-ähnlichen Trennzeichensyntax basierend - mit der Version 4.0 durch moderne XML-Technologien repräsentiert wird.

Für die Kreditwirtschaft gab es Mitte der 90er Jahre mehrere Gründe für die Einführung von HBCI:

1997 wurde Homebanking größtenteils auf Basis des seit 1984 etablierten PIN/TAN-Verfahrens betrieben, das damals als Grundlage für das klassische Btx-Homebanking (heute T-Online Classic) eingeführt wurde. Auch viele der neuen Internet Homebanking-Lösungen setzten anfangs auf den bestehenden Btx-Bankanwendungen auf und ließen somit die alten Applikationen nur in einem neuen Gewand erscheinen (Facelifting).

Zur Absicherung des Banken-Dialoges wird bei Sessionaufbau zum Bankrechner eine sog. „Persönliche Identifikations-Nummer“ (PIN) gesendet und geprüft. Eine bankfachliche Transaktion wird zusätzlich jeweils durch eine einmalig gültige „Transaktionsnummer“ (TAN) abgesichert. Transaktionsnummern werden dem Kunden in Form von TAN-Listen per Briefpost mitgeteilt. Die Verwaltung dieser Listen ist auf Kunden- und Bankseite sehr aufwändig und umständlich.



Überweisungsformular

Empfängername

Kontonummer Bankleitzahl

Kreditinstitut 1.000.000,00

Verwendungszweck

Auftraggebername

Kontonummer

TAN-Liste	
984572	964476
235466	467895
834562	536653
432236	135623
437424	568524
335565	808644
535665	440044
336573	365786
235673	234555
466323	986535

536653

Abbildung 1: PIN- / TAN-Verfahren

Auf bestehende theoretische Sicherheitsprobleme durch Abhören und Modifizieren von Homebanking-Aufträgen soll hier nicht eingegangen werden. Dieser Thematik ist in Kapitel „Infrastruktursicherheit“ ein eigener Abschnitt gewidmet.

Aus der damaligen Analyse ergab sich eine Reihe von Anforderungen an einen neuen Homebanking-Standard.

- Die Datenschnittstelle musste sehr leistungsfähig und flexibel sein.
- Sie musste unabhängig von Präsentationsdiensten sein.
- Die Datenschnittstelle musste unabhängig vom Transportnetz und dadurch auch Internet geeignet sein. Zugrunde liegende Transportlayer sollten jedoch genau spezifiziert werden, um multibankfähige Kundensysteme mit gemeinsamer Zugangscharakteristik herstellen zu können.
- Erweiterte Sicherheitsfunktionen sollten den Betrieb in unsicheren Netzen ermöglichen und den Bedienungskomfort erhöhen.
- Die Betriebssicherheit musste gewährleistet sein. Der Status eines Auftrags sollte jederzeit online kontrollierbar sein.
- Die gesamte Lösung sollte multibankfähig sein, um mit den gleichen Mechanismen alle Kontoverbindungen verwalten zu können. Sie sollte idealerweise auch herstellerunabhängig sein, um beim Einsatz von mobilen Endgeräten z. B. in Hotelfoyers nicht auf Kompatibilitätsprobleme zu stoßen.
- Dem Homebanking-Bereich sollte durch Erschließung neuer Geschäftsarten, die über die damals üblichen Überweisungen und Umsatzabfragen weit hinausgingen, zu größerer Attraktivität verholfen werden.

- Der Standard sollte sich nahtlos in die gesamte Welt des Online-Bankings, z. B. auch die Banken-Selbstbedienung integrieren lassen, um den Kunden gleich bleibende Funktionalität über alle Endgeräte und den Kreditinstituten einfache Erstellung und Wartbarkeit von Anwendungen zu gewährleisten.
- Das deutsche Kreditgewerbe wollte durch die Vereinbarung des HBCI-Standards dazu beitragen, dass Hersteller eine langfristige Planungssicherheit bei der Gestaltung kundenfreundlicher Homebanking-Programme und -Systeme erhielten.

1.2 Der Schritt von HBCI zu FinTS V3.0 und V4.0

HBCI versuchte in den Jahren 1998 bis 2002 mit den Versionen 2.01, 2.1 und 2.2 diesen Kriterien gerecht zu werden, schaffte dies jedoch nicht auf breiter Basis, da sich durch die Einführung des Internet das Kundenverhalten grundlegend änderte. Hierdurch gelangte das damals tot gesagte PIN/TAN-Verfahren zu neuer Blüte und drängte HBCI mit seinen hohen Anforderungen, speziell im Sicherheitsbereich, in eine Nische für anspruchsvolle Endkunden, die sich bereit erklärten, Chipkartenleser an ihrem PC zu installieren und / oder einen Ini-Brief-Austausch mit ihrer Bank zur Erstinitialisierung durchzuführen.

Dies sollte sich mit FinTS V3.0 nun grundlegend ändern. FinTS ist kein neuer Standard, sondern stellt nur eine Namensänderung und Erweiterung des bestehenden HBCI dar. HBCI selbst beschreibt im Baukastensystem FinTS nur noch die signaturgestützten Sicherungsverfahren mit Chipkarte oder Diskette.

Mit FinTS V4.0 findet die eigentliche Neupositionierung des Standards statt. Die konsequente Internetausrichtung wird durch den Schritt zu XML und http / https deutlich.

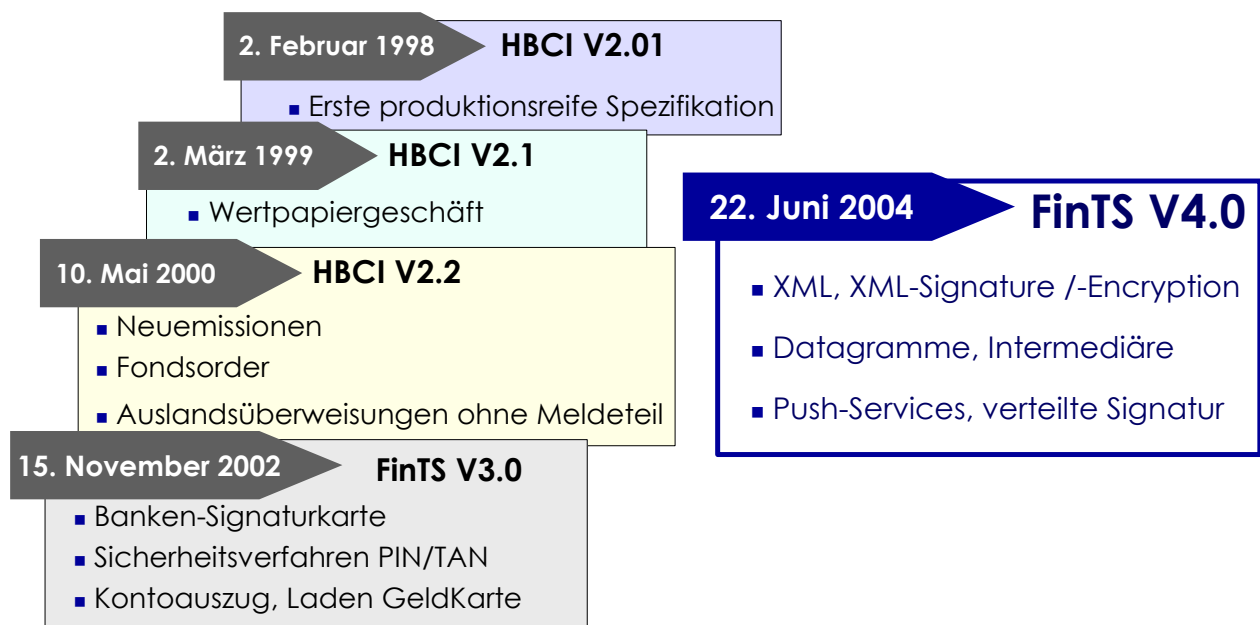


Abbildung 2: Historische Entwicklung von HBCI bis zu FinTS V4.0

Doch bevor die Inhalte des FinTS-Standards dargestellt werden, erfolgt zunächst eine kurze Analyse der bestehenden Online-Banking Verfahren.

1.2.1 Marktanalyse der Online-Banking Endgeräte

Der Markt stellt sich bei Einführung von FinTS V4.0 folgendermaßen dar:

Browserbasierte Verfahren

Als Ablösung des klassischen Btx Homebanking haben sich browserbasierte HTML-Anwendungen mit PIN/TAN als Sicherheitsverfahren etabliert. Diese gingen in der ersten Generation meist aus Java Applet-Lösungen hervor, die über entsprechende Konverter an die alten Btx-Anwendungen angeknüpft waren. Doch diese unhandlichen und wenig benutzerfreundlichen Lösungen gehören längst der Vergangenheit an.

Aktuelle Internet Banking Lösungen bieten zahlreiche Geschäftsvorfälle und meist auch Serverfunktionalitäten z. B. zum Speichern von vorbereiteten Überweisungsformularen an, um Mehrfacheingaben zu vermeiden.

Damit werden Defizite ausgeglichen, die in der Natur des Browser-Verhaltens liegen: im Endgerät können keine Daten gespeichert werden – es erfolgt eine reine Präsentation der Daten. Im Gegenzug besitzt man den Vorteil der Ortsunabhängigkeit.

Was für die Anwendungsdaten gilt, gilt in besonderem Maße für die Sicherheit. Ein Standard-Browser besitzt keine Möglichkeit, auf Chipkartenleser und HBCI-Chipkarte zuzugreifen; auch können keine Signaturberechnungen im Rahmen der RDH-Softwarelösung durchgeführt werden. Alleine deshalb bietet sich auch das PIN/TAN Verfahren als ideale Variante an, da in diesem Fall keine über Präsentationselemente hinausgehende Intelligenz im Kunden-Endgerät vorausgesetzt wird.

Als Spielarten dieser reinen Browserlösung existieren am Markt solche, die zumindest einige Programmteile im Endgerät ausführen – und seien es nur die Signaturfunktionen oder die Chipkartenansteuerung. Auf diese Weise können HBCI-Verfahren auch in einem Quasi-Browserkontext verwendet werden.

Abgerundet wird die Palette an Browseranwendungen durch Java-Lösungen, bei denen die gesamte Anwendung auf das Endgerät geladen und dort ausgeführt wird. Im Unterschied zu den Banking-Lösungen der ersten Generation werden diese Programme nur einmal initial installiert oder bei Update automatisch nachgeladen. Der Vorteil solcher Lösungen liegt in der komfortablen Benutzeroberfläche und der lokalen Intelligenz, wie sie z. B. für intelligente Agenten im Euro-Zahlungsverkehr eingesetzt werden kann.

Online-Banking Kundenprodukte

Nach wie vor gibt es eine große Anzahl von Online-Banking Kunden, die ein fest installiertes PC-Programm für die Verwaltung ihrer Finanzen verwenden. Diese Softwareprodukte gibt es von einfachen Homebanking-Modulen bis hin zu ausgereiften Finanz-Managementsystemen im Privat- und Firmenkundenbereich.

Da HBCI sich aufgrund der geschilderten Entwicklung bisher nicht als flächendeckender Standard durchsetzen konnte, mussten die Kundenprodukte dies ausgleichen, indem sie meist eine Reihe von Schnittstellen zu Banken und Sparkassen anbieten. Neben HBCI und T-Online Classic (meist ZKA-Dialog) werden auch noch herstellerspezifische Internet-Protokolle unterstützt.

Denn einige Rechenzentren erklärten sich unter dem Druck des .com Hype bereit, entsprechende Gateways zu betreiben, um eine elegantere Anbindung der selbst vermarkteten Homebanking-Produkte anbieten zu können.

Die nun folgende Darstellung des Standards gleicht vom Aufbau her in etwa der Kapitelstruktur der FinTS-Spezifikation V4.0. Zusätzlich befinden sich am Ende noch einige Bemerkungen des Autors zur Einordnung von FinTS V4.0 in die Welt anderer geplanter oder teilweise schon realisierter Übertragungsverfahren im Finanzsektor.

1.2.2 Anforderungen an FinTS V3.0 und V4.0

Getrieben durch die stetig steigenden Anschlusszahlen im Online-Banking-Bereich und die inhomogene Vorrechnerlandschaft besteht nun nach 5 Jahren HBCI-Geschichte wieder dringender Handlungsbedarf, um unter dem Schlagwort Multikanalmanagement die Zugangssysteme zu konsolidieren. Verstärkt wird dieser Trend zusätzlich durch zahlreiche Fusionen im Bereich der Institute und Rechenzentren, was die Vielfalt der unterschiedlichen Serversysteme noch steigert.

Als Werkzeug für die Konsolidierung bietet sich FinTS an, da trotz momentan noch relativ geringer Nutzung doch die meisten Institute diese Datenschnittstelle unterstützen. Folge ist eine geforderte Neuausrichtung des Standards unter neuen Vorzeichen, was durch die Einführung von FinTS V4.0 nun gelingen soll.

1.2.3 Neue Funktionen mit FinTS V3.0

Nach dieser Vorrede zur HBCI-Historie nun zunächst zu den wesentlichen Neuerungen in FinTS V3.0:

- Ersetzen der HBCI-Dokumentation durch ein Baukastensystem von Einzel-Spezifikationen
- Integration von PIN/TAN als neuem Sicherheitsverfahren
 - https als Transportverfahren bei PIN/TAN
 - dadurch implizit: SSL als Transportverschlüsselung bei PIN/TAN
- Unterstützung der ZKA Banken-Signaturkarte
- Einführung von Sicherheitsprofilen und Sicherheitsklassen
- Einführung von Komprimierungsverfahren
- Life-Indikator Nachricht
- neue Geschäftsvorfälle, z. B.
 - elektronischer Kontoauszug
 - Euro STP Zahlung
 - GeldKarten-Transaktionen

Durch die Integration von PIN/TAN als zusätzlichem Sicherheitsverfahren entschloss man sich nicht nur, dem Standard einen neuen Namen zu geben, sondern es entstand auch ein dynamisch erweiterbares Baukastensystem, bestehend aus eigenständigen Dokumenten, die je nach Thema unterschiedliche Einsatzbereiche und Versionen haben können.

FinTS Formals	Allgemeine Festlegungen für multibankfähige Online-Verfahren der deutschen Kreditwirtschaft	<input type="checkbox"/> Nachrichtenaufbau <input type="checkbox"/> Dialogablauf <input type="checkbox"/> Bankparameterdaten <input type="checkbox"/> Userparameterdaten <input type="checkbox"/> Data Dictionary <input type="checkbox"/> Anlagen
FinTS Security	Sicherheitsverfahren HBCI	<input type="checkbox"/> Verfahrensbeschreibung <input type="checkbox"/> Chipapplikationen <input type="checkbox"/> Data Dictionary <input type="checkbox"/> Anlagen
	Sicherheitsverfahren PIN/TAN	<input type="checkbox"/> Verfahrensbeschreibung <input type="checkbox"/> Data Dictionary <input type="checkbox"/> Anlagen
FinTS Messages	Multibankfähige Geschäftsvorfälle	<input type="checkbox"/> Mehrfach verwendete Elemente <input type="checkbox"/> Geschäftsvorfälle <input type="checkbox"/> Data Dictionary <input type="checkbox"/> Anlagen
	Belegungsrichtlinien für Finanzdatenformate der deutschen Kreditwirtschaft	<input type="checkbox"/> DTAUS / DTAZV <input type="checkbox"/> SWIFT-Formate <input type="checkbox"/> Anlagen

1.2.4 Neue Funktionen mit FinTS V4.0

F_{inTS V4.0} Nach dieser Vorrede zur HBCI und der Neuordnung der Spezifikation mit FinTS V3.0 nun endlich zu den angekündigten Neuerungen in FinTS V4.0 im Überblick:

- Ersetzen der Trennzeichensyntax durch XML-Technologien wie XML-Schema, XML-Signature und XML-Encryption
- Durch geeignetes XML-Design wird ein homogenes Einbinden von anderen XML-basierten Message-Typen wie z. B. SWIFT XML erreicht.
- Entfernen aller Barrieren des statischen Dialogablaufs z. B. durch FinTS-Datagramme

- Unterstützen von synchronen und zusätzlich jetzt auch asynchronen Kommunikationsverfahren z. B. E-Mail
- Ergänzen von neuen Szenarien für asynchrone Verarbeitung wie Push-Services und Publish /Subscribe Verfahren
- Einführen der neuen Rolle des Intermediärs zur komfortablen Einbindung von Portalen für einen parametrisierbaren Betrieb
- Neue Features für Firmenkunden – im Speziellen die örtlich und zeitlich unabhängige verteilte Mehrfachsignatur.

Diese kurze Aufstellung macht sicherlich deutlich, welchen Generationswechsel die Einführung von FinTS V4.0 bedeutet und welche neuen Szenarien sich damit abbilden lassen.

Im Folgenden werden nun die einzelnen Bände der FinTS V4.0 Spezifikation kurz erläutert, um einen Überblick über die zur Verfügung stehenden Funktionen zu geben und den Einstieg in die eigentliche Spezifikation zu erleichtern.

2 FinTS Formals und XML Syntax

Im Band „FinTS Formals“ befinden sich alle protokoll-spezifischen Festlegungen des FinTS-Standards. Dies beinhaltet Syntax und Zeichensatz, den Nachrichtenaufbau und Dialogablauf und letztlich die Struktur der Parameter für Bank, Intermediär und Kunde. Diese Aspekte werden im Folgenden detailliert beschrieben.

2.1 Syntax

2.1.1 Zeichensatz

FinTS V4.0 verwendet im Unterschied zu den Vorgängerversionen den UTF-8 Zeichensatz, wie er in der XML-Schema Spezifikation empfohlen wird. Unterstützt werden alle in europäischen Sprachen vorkommenden Zeichen und das €-Symbol.

Dieser Zeichensatz gilt für alle Textformate, nicht jedoch für binäre oder transparente Daten. Binär sind alle Arten von Programmen, Multimediadaten, o. ä., transparent sind FinTS-Fremdformate, die normalerweise aus dem Kreditbereich stammen (z. B. DTAUS, S.W.I.F.T.), ihrer eigenen Syntax gehorchen und zum Teil auch einen eigenen Zeichensatz verwenden (z. B. DTAUS). Um die UTF-8 Daten transparent übertragen zu können, findet eine base-64 Konvertierung statt.

2.1.2 Inzwischen Historie: Die Trennzeichensyntax

Bis einschließlich FinTS V3.0 wurde eine Trennzeichensyntax zur Darstellung der Daten verwendet. Diese war an UN/EDIFACT angelehnt, die Formate selbst wurden jedoch nach eigenen Regeln aufgebaut.

Eine Trennzeichensyntax hatte den Vorteil der Flexibilität und der Minimierung des Datenvolumens. Es wurden nämlich die Daten nur in der aktuell benötigten Länge übertragen. Beschreibende Informationen, wie Feldname und Feldlänge waren implizit in der jeweiligen Segmentdefinition enthalten und wurden somit ebenfalls nicht gesendet.

Eine zusätzliche Verringerung der Übertragungsmenge wurde durch logische Komprimierung erreicht - optionale Felder standen jeweils am Ende einer Datenstruktur und konnten so problemlos weg gelassen werden. Auch das Auslassen nicht benötigter Datenelemente war mittels Trennzeichensyntax problemlos und effektiv möglich.

Folgende Trennzeichen wurden verwendet:

+	Datenelement Ende
:	Gruppendatenelement Ende
`	Segment Ende
?	Freigabezeichen (bei Steuerzeichen im Text)
@	Kennzeichen für binäre Daten

Die Trennzeichensyntax war zu einer Zeit, in der Modems mit Übertragungsraten von 14.400 bit/s arbeiteten, sicherlich die richtige Wahl und auch heute heben sich diese kryptischen Datenströme von den üblichen Datenvolumina ab. Jedoch bringt diese Art der Syntax außer dem inzwischen proprietären Ansatz entscheidende Einschränkungen mit sich: es können nur zwei, indirekt bis zu maximal drei Hierarchien abgebildet werden – ein Defizit, das sich bei der Modellierung komplexerer Geschäftsvorfälle sehr negativ bemerkbar macht.

Diese Tatsache und die Notwendigkeit der Verwendung von international etablierten Standards führte zum Wechsel auf moderne XML-Technologien.

2.1.3 XML-Syntax

F_{inTS V4.0} Das lange Warten auf die XML-Version von FinTS hat sich gelohnt. Die Technologien besitzen inzwischen einen Reifegrad, der eine effektive Umsetzung der FinTS-Syntaxregeln ermöglicht. Die DTD-Phase konnte übersprungen werden und mit der aktuell standardisierten Schema-Spezifikation lassen sich die komplexen Zusammenhänge erstaunlich effektiv abbilden. Andere XML-basierte Standards – allen voran SWIFT XML – können leicht integriert werden. Dies bedeutet, dass solche Finanzdatenformate durchgängig interpretiert und auf korrekte Syntax geprüft werden können. Dies war bei den Vorgängerversionen von FinTS bei Fremdformaten nicht möglich.

Es war nämlich von jeher Ansatz von HBCI, geeignete, bestehende Formate aus dem Kreditbereich (DTAUS, S.W.I.F.T.) überall dort zu verwenden, wo bank- und kundenseitig standardisierte Routinen herangezogen werden können. So genannte „FinTS-Eigenformate“ decken den Bereich ab, der bisher noch in keinem Gremium endgültig und zufrieden stellend genormt wurde und bieten außerdem die Möglichkeit, neue Geschäftsvorfälle multibankfähig zu gestalten. Die Multibankfähigkeit wird unter anderem auch dadurch erreicht, dass ein Mindestumfang von Datenelementen, der für die reibungslose Abwicklung eines Geschäftsvorfalles nötig ist, als MUSS-Felder definiert ist, wogegen Informationen, die nicht alle Institute verarbeiten können in optionalen KANN-Feldern abgelegt werden. Dadurch wird zum einen die bankenübergreifende Definition erreicht, zum anderen die Flexibilität nicht eingeschränkt.

Über CONDITIONAL definierte Felder können schließlich noch Belegungsrichtlinien unter bestimmten Bedingungen festgelegt werden, was eine gleiche Interpretation auf Kunden- und Institutsseite zudem fördert.

2.1.4 Struktur der XML-Modellierung

Die folgenden Kapitel führen den interessierten Leser grob in die verwendeten Modellierungstechniken ein, um die unter www.fints.org bereitgestellten Schemadefinitionen leichter verstehen und eine Verbindung zur alten HBCI-Welt herstellen zu können.

Als erstes wird auffallen, dass die Schemadefinitionen durchgängig in englisch gehalten sind. Dies öffnet den Standard für den internationalen Gebrauch und lässt auch die Anlehnung an SWIFT-Namenskonventionen zu. In den Schemata selbst befinden sich als Kommentare die ursprünglich deutschen Feldnamen, die auch in den restlichen Dokumenten, z. B. der Geschäftsvorfallesbeschreibung verwendet werden.

2.1.4.1 FinTS Namespace

Es wäre vermessen, anzunehmen, dass es gelingen könnte, ein internationales, standard-übergreifendes Data Dictionary aufzubauen. Denn obwohl bei FinTS Namenskonventionen aus der SWIFT-Modellierung übernommen wurden, gibt es bei vielen Feldern semantische Unterschiede. Daher wurden von XML so genannte Namespaces eingeführt, um einen Standard bzgl. der Namensgebung unabhängig gestalten zu können. Der FinTS-Namespace lautet folgendermaßen:

<http://www.fints.org/spec/xmlschema/4.0/final/>
<types | structures | transactions>

Unter dieser Adresse lassen sich aktuell bereits alle verwendeten Schemata finden und z. B. mit einem geeigneten Browser anzeigen.

Dieses sehr allgemein gehaltene Konzept ermöglicht es leicht, neue Namensräume für spezielle Verwendungszwecke aufzubauen. Ersetzt man die allgemeine ZKA-Adresse www.fints.org durch eine verbands- oder institutsspezifische Adresse, so können dort spezifische Geschäftsvorfälle hinterlegt werden. Bei entsprechend flexiblem Design von Kundenprodukten können die betreffenden Schemadefinitionen leicht abgefragt und integriert werden.

2.1.4.2 XML Schemaverzeichnis: types

Unter dem Verzeichnis types sind folgende Schemata zusammengefasst:

common.xsd	grundsätzliche Definitionen der FinTS-Begriffe wie z. B. Segment, Geschäftsvorfall, Antwortdaten oder Parameterdaten
formats.xsd	Definition der Basisformate wie <i>an</i> , <i>num</i> oder <i>txt</i> , womöglich auf Basis von Standard XML Messagetypes
message.xsd	abstrakte Definition der FinTS-Nachricht mit allen vorkommenden Nachrichtentypen, z. B. Auftragsnachricht (Order) oder Bank Parameterdaten (BankParamData).
paramdata	abstrakte Definition der FinTS Parametersegmente
patterns	Ablösung der bisher verwendeten „abgeleiteten Formate“, z. B. Kontoverbindung (acct)
structures	Beschreibung der in FinTS verwendeten „mehrfach verwendeten Elemente (MVE)“.

Im Gegensatz zu den proprietär definierten Basisformaten in FinTS V3.0 verwendet FinTS V4.0 wo immer möglich standardisierte XML Messagetypes, die auch von jedem marktüblichen Parser interpretiert werden können. Dies bietet enorme Vorteile, wie das Beispiel eines Datumsfeldes verdeutlichen soll.

Beispiel: Während der alte HBCI Nachrichtentyp „dat“ selbst definierte Datenformate enthielt (Beispiel: 20041121), deren korrektes Format durch Eigenimplementierungen geprüft werden musste, ist die Prüfung des XML-Messagetype „date“ in jedem Standardprodukt unterstützt (2004-11-21).

Ein 30. Februar wird somit bereits im Parser als Syntaxfehler erkannt und entsprechend gemeldet.

Die so genannten abgeleiteten Formate in FinTS V3.0 (Beispiel: Kontoverbindung) werden ersetzt durch XML **patterns**, welche mit den Möglichkeiten der XML-Modellierung die gleichen fachlichen Inhalte abbilden (Beispiel: acct).

2.1.4.3 XML Transaktionen (Schemaverzeichnis: *transactions*)

In diesem Pfad finden sich alle ZKA-weit einheitlichen Geschäftsvorfälle, z. B. AcctBal-7.xsd für die Saldenabfrage. Hierbei bezeichnet der angehängte Suffix die Segmentversion des jeweiligen Geschäftsvorfalles.

2.1.5 Syntaktische Einheiten

Auch bei den verwendeten syntaktischen Einheiten gibt es Neuerungen mit FinTS V4.0. Während sich mit der FinTS V3.0-Trennzeichensyntax nur 3 logische Hierarchieebenen abbilden ließen, fällt diese Restriktion nun weg.

Hier die Begriffswelt von FinTS V3.0:

1. Datenelemente

Diese entsprechen den einzelnen Feldern eines Segmentes. Im einfachsten Fall wird durch ein Datenelement (DE) z. B. eine "Bankleitzahl" abgebildet, im Extremfall verbirgt sich dahinter ein gesamtes, transparent eingestelltes S.W.I.F.T.-Format. Datenelemente (und auch DE-Gruppen) besitzen keinen administrativen Overhead in Form eines Headers. Die Beschreibung über die Feldeigenschaften ist implizit über die Position innerhalb des Segmentes beschrieben.

2. Datenelementgruppen

Logisch zusammengehörige Datenelemente werden zu Datenelementgruppen (DEG) zusammengefasst. Die enthaltenen Elemente werden dann als Gruppendatenelemente (GD) bezeichnet.

3. Segmente

Alle logisch zusammengehörigen Datenelemente und Datenelementgruppen werden zu einem **FinTS-Segment** zusammengefasst. Im bankfachlichen Sinn entspricht ein Segment im Allgemeinen einem Geschäftsvorfall, z. B. einer Einzelüberweisung.

Im Gegensatz zu den Hierarchien DE und DEG wird ein Segment zusätzlich durch einen administrativen Zusatz, den *Segmentkopf* beschrieben. Darin befindet sich vor allem die eindeutige Segmentkennung, über die auf den Inhalt des Segmentes und aller darin enthaltenen Datenelemente und -gruppen geschlossen werden kann. So beschreibt z. B. die Segmentkennung „HKUEB“ die Kundennachricht für die Einzelüberweisung inklusive der Attribute aller enthaltenen Datenelemente wie die der Auftraggeberkontonummer (max. 30-stellig, alphanumerisch, MUSS-Feld).

Segmente können nicht nur bankfachliche Informationen enthalten, sondern dienen allgemein als syntaktische Einheit in FinTS V3.0. So gibt es beispielsweise auch die Steuerstrukturen *Nachrichtenkopf* und *-abschluss*, *Signaturkopf* und *-abschluss*, u. ä..

2.1.5.1 Syntaktische Einheiten bei FinTS V4.0

Grundsätzlich ist bei FinTS V4.0 eine beliebig tiefe Schachtelung von Strukturen möglich. Daher passen die Begriffe Datenelement und Datenelementgruppe nicht mehr in diese neue Welt. Der Begriff des Segmentes wird weiterhin verwendet – er bezeichnet die einzelnen syntaktischen Einheiten innerhalb der XML-Messages.

Um die Vorteile von XML voll ausnützen zu können, wurden die vorhandenen FinTS-Datentypen wo möglich in XML Standard Datentypen überführt. Die Referenzierung – z. B. auf fehlerhafte Elemente in einem Auftrag – wurde bisher mit Hilfe von Referenzen in der Antwortnachricht durchgeführt. Der W3C Standard XPath bietet hier weitaus elegantere Möglichkeiten.

2.1.6 Nachrichtenaufbau

Durch ein Segment kann nur der bankfachliche Teil eines Geschäftsvorfalles abgedeckt werden. Erst die Kombination von mehreren Segmenten bildet eine **FinTS-Nachricht**, die in Form einer Kunden- bzw. Kreditinstitutsnachricht als abgeschlossene Einheit übertragen werden kann. Innerhalb einer Nachricht können sich mehrere – auch unterschiedliche - Geschäftsvorfall-Segmente befinden, also z. B. drei Einzelüberweisungen und zwei Saldenabfragen.

2.1.6.1 Nachrichtenaufbau bei FinTS V3.0

Eine FinTS-Nachricht hat in FinTS V3.0 im Allgemeinen folgenden Aufbau:

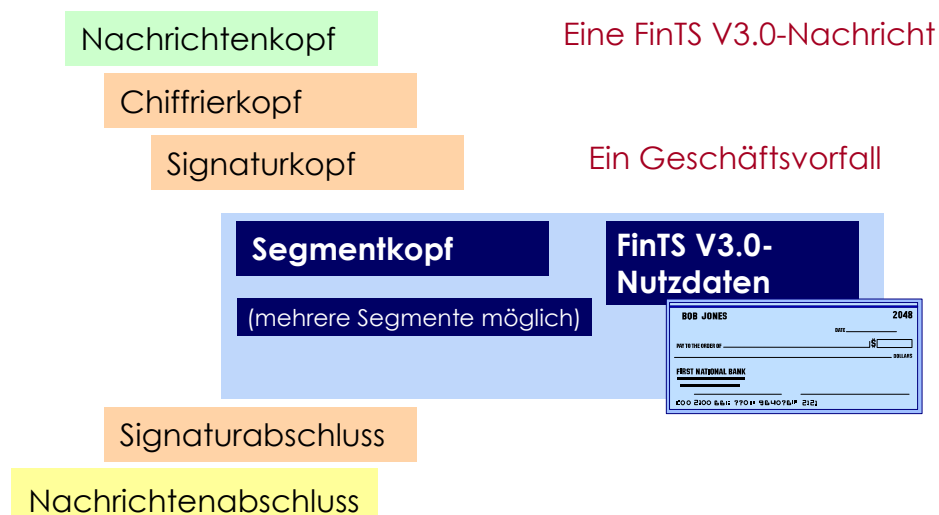


Abbildung 3: Nachrichtenaufbau bei FinTS V3.0

Hinzu kommen noch ein *Chiffrierkopf* bei Verschlüsselung der Daten und evtl. weitere *Signaturköpfe* und *-abschlüsse* bei Mehrfachunterschriften. Signaturkopf und *-abschluss* sind bei Kreditinstitutsnachrichten optional.

Im *Nachrichtenkopf* befinden sich administrative Informationen, wie z. B. die Nachrichtennummer und die Nummer der Bezugsnachricht des Kunden bei Kreditinstitutsnachrichten. Im *Nachrichtenabschluss* befindet sich eine Referenz auf den Nachrichtenkopf. Diese Mimik ist aus dem Header/Trailer-Verfahren von UN/EDIFACT übernommen.

Der *Signaturkopf* enthält Informationen für die Beschreibung der anzuwendenden Sicherheitsverfahren und außerdem eine eindeutige Referenznummer zur Doppeleinreichungskontrolle beim Kreditinstitut. Im *Signaturabschluss* befindet sich die elektronische Signatur für die gesamte Nachricht.

Bei Kreditinstitutsnachrichten befinden sich in den Geschäftsvorfallsegmenten unter Verweis auf das Kundensegment auch Rückmeldecodes, die Auskünfte über den Verarbeitungsstatus ermöglichen.

2.1.6.2 Nachrichtenaufbau in FinTS V4.0

FinTS V4.0 Bzgl. der Geschäftsvorfallssegmente (Order) ergeben sich bei FinTS V4.0 im Wesentlichen keine Änderungen – der Begriff wurde sinngemäß übernommen. Die administrativen Segmente – speziell im Sicherheitsbereich – sind grundlegend anders aufgebaut, was unter anderem auch an der Verwendung der Standards XML-Signature und XML-Encryption liegt. Starken Einfluss genommen haben aber auch die neuen Intermediärszenarien und die Neuorientierung des Kommunikationsprotokolls.

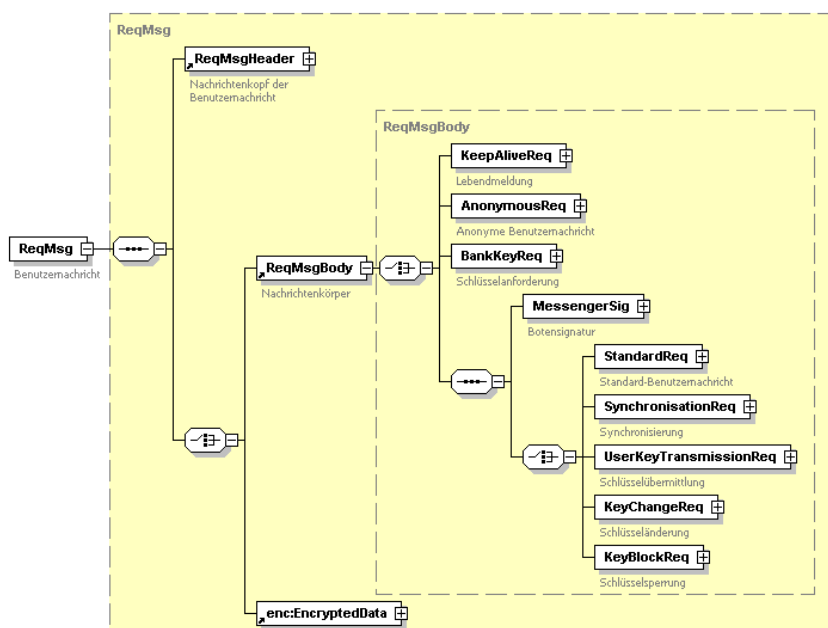


Abbildung 4: Aufbau der Benutzernachricht (Quelle: FinTS V4.0 Spezifikation – XML-Syntax)

2.2 Dialoge und Datagramme

Während bis FinTS V3.0 generell Dialoge verwendet wurden, bietet FinTS V4.0 hier weitgehende Erweiterungen an – bis zu einem asynchronen Betrieb wie z. B. bei E-Mail. Bevor jedoch auf die Kommunikationsverfahren näher eingegangen wird, soll die mit FinTS V4.0 neu eingeführte Rolle des Intermediärs erläutert werden.

2.2.1 Neu in FinTS V4.0 - Intermediäre und Szenarien

F_{inTS V4.0} Mit HBCI wurde bisher das Protokoll an der Schnittstelle zwischen Kunde und Kreditinstitut beschrieben. Seit einigen Jahren ergeben sich jedoch immer wieder Szenarien, in denen der Kunde nicht direkt mit seinem Institut kommuniziert, sondern sich eines Überbringers oder Intermediärs bedient.

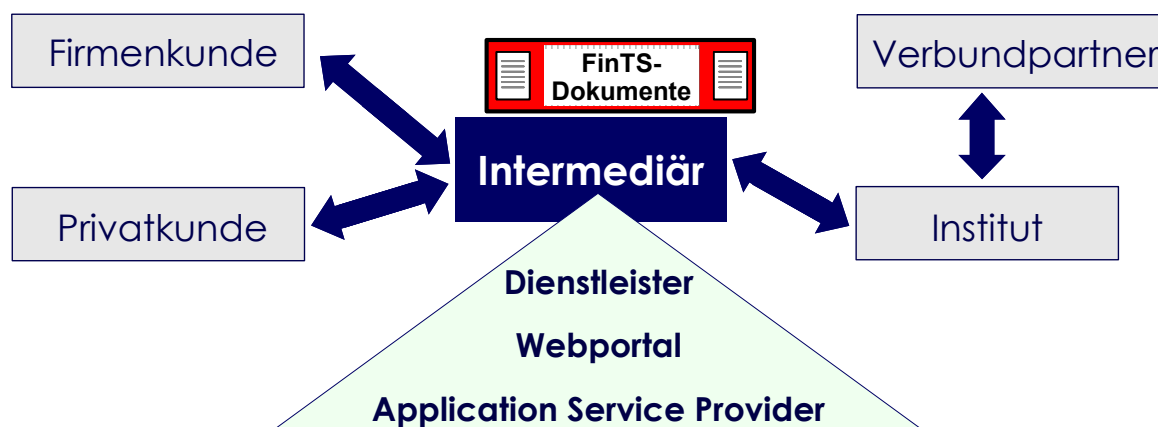


Abbildung 5: Neu mit FinTS V4.0: Die Rolle des Intermediärs

Die Anwendungsfälle hierfür können weit gestreut sein, z. B. bei der Verwendung des FinTS-Protokolls in einem Callcenter-Szenario: hier stellt der Callcenter-Agent den Intermediär dar, der aus Authentifizierungssicht eine eigene Rolle einnimmt. Ein anderes Beispiel sind Finanzportale, über die ein Kunde seine Aufträge akkumuliert und mit Zusatzservices anreichert. Auch hier muss geregelt sein, welchen Handlungsspielraum solch ein Portalbetreiber haben darf. FinTS V4.0 kann hierzu Antworten liefern und beschreibt die in der Praxis vorkommenden unterschiedlichen Portalszenarien. Die Rolle des Intermediärs unterscheidet sich in den Szenarien je nach Einflussnahme, d. h. ob er als Herausgeber oder Bote fungiert und ob er die Auftragsdaten des Kunden einsehen kann oder nur weiterleitet.

2.2.1.1 Direkte Kommunikation

Das bereits aus den früheren FinTS-Versionen etablierte Kommunikationsverfahren wird als direkte Kommunikation zwischen Kunde und Institut bezeichnet und unterstützt keine Intermediäre.

2.2.1.2 Szenario A: Intermediär als Herausgeber

Tritt ein Intermediär als Herausgeber auf, so hat er gegenüber den vertraglichen Bindungen des Kunden mit seiner Bank gewisse Rechte, z. B. tritt er als Verfügungsberechtigter auf. Ein Beispiel hierfür ist ein Callcenter-Szenario, bei dem der Callcenter-Agent per Telefon nach Nennen der PIN die Aufträge des Kunden per FinTS einreicht. Das Beispiel zeigt, dass das Protokoll auf der Strecke zwischen Kunde und Intermediär durch FinTS nicht festgelegt ist.

2.2.1.3 Szenario B: Intermediär als PIN/TAN-Überbringer

Im Szenario B spricht der Intermediär mit dem Kunden ebenfalls ein bilateral vereinbartes Protokoll. Der Intermediär erhält auf diesem Weg die Auftragsdaten inklusive PIN und ggf. TAN des Kunden und baut daraus eine FinTS-Nachricht auf, die er als Bote signiert. Anwendungsbeispiel könnte ein Finanzportal sein, das dem Kunden außer einem Informationsteil (z. B. Börsenkursen) auch die Möglichkeit der multibankfähigen Auftragsabwicklung anbietet. Der Portalbetreiber muss hierbei eine vertraute Instanz sein, da er in Besitz von PIN und TAN des Kunden gelangt.

2.2.1.4 Szenario C: Intermediär als HBCI-Überbringer

Das Szenario C ist mit dem vorhergehenden bis auf das Sicherheitsverfahren identisch – hier verwendet der Kunde seine HBCI-Chipkarte und signiert seine Aufträge als Herausgeber bzw. Zeuge. Der Intermediär kann somit die Aufträge nicht mehr ändern; er kann sie jedoch entschlüsseln und ggf. mit weiteren Informationen kombinieren. Auch hier unterschreibt der Intermediär als Bote, sendet aber die Aufträge und Signaturen des Kunden unverändert mit.

2.2.1.5 Szenario D: Intermediär als HBCI-Überbringer / verschlüsselt

Beim letzten Szenario tritt der Intermediär lediglich als Router auf. Er kann die signierten und verschlüsselten Aufträge empfangen, anhand von lesbaren Informationen im Header Instituten zuordnen und die Aufträge als Bote einreichen. Dieses Szenario verwendet die vollständige HBCI-Sicherheitsfunktionalität zwischen Kunde und Institut.

2.2.2 Initialisierung

Bis FinTS V3.0 war die gezeigte starre Abfolge von Dialogen mit Dialoginitialisierung, Auftragsnachrichten und explizitem Dialogende obligatorisch. Diese Form des Nachrichtenaustauschs ist auch mit FinTS V4.0 noch unterstützt und wird nun als erste Möglichkeit beschrieben, da sich die Wirkungsweise des FinTS-Protokolls damit gut darstellen lässt.

FinTS-Nachrichten sind zwar in sich abgeschlossene Verarbeitungseinheiten, sie benötigen jedoch einen Kontext, der die Rahmenbedingungen für die Auftragsausführung regelt. Dieser Kontext kann z. B. über einen Dialogbezug (bis FinTS V3.0 die einzige Möglichkeit) hergestellt werden, der folgendermaßen aufgebaut ist:

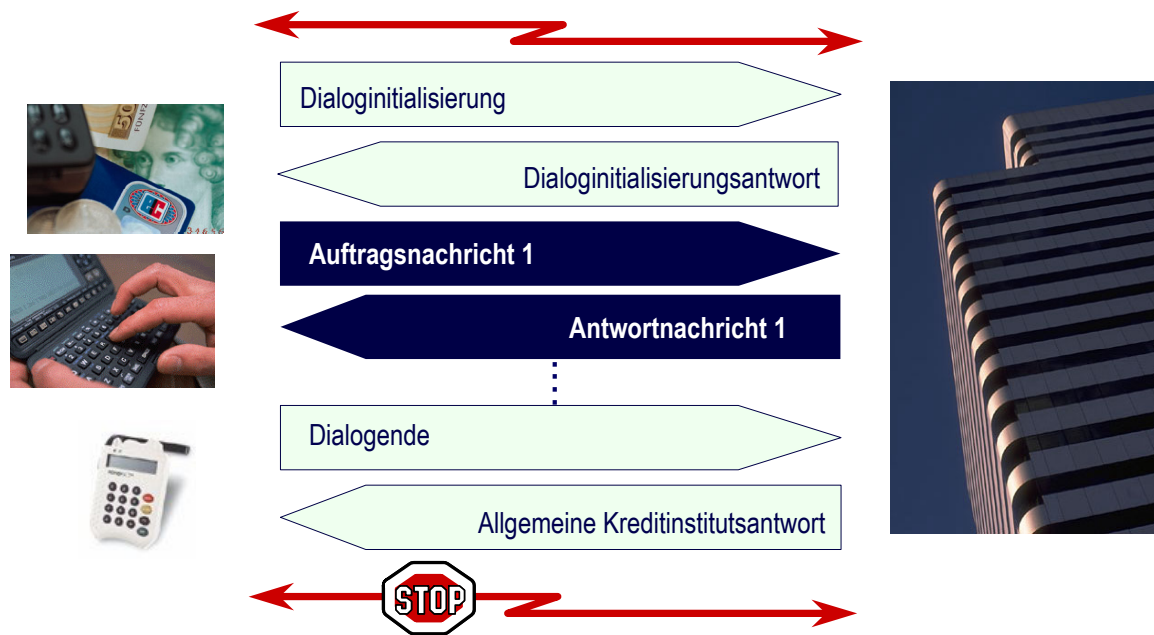


Abbildung 6: FinTS Dialogablauf bis FinTS V3.0

Der dargestellte Ablauf zeigt, dass ein FinTS V3.0-Dialog grundsätzlich synchron abläuft, d. h., dass jede Nachricht vom Kreditinstitut beantwortet werden muss, bevor eine neue Kundennachricht gesendet werden kann.

Auch muss während des gesamten Dialoges eine Transportverbindung bestehen, die nach Austausch aller Auftragsnachrichten auch explizit wieder durch ein Dialogende auf FinTS-Ebene abgebaut werden muss.

Die Dialoginitialisierung dient der gegenseitigen Authentisierung der beiden Partner (Kunde und Bank), um die Übertragung der folgenden Auftragsnachrichten in einer sicheren Umgebung durchführen zu können. Zusätzlich werden im Rahmen der Dialoginitialisierung auch die Verschlüsselungs- und Komprimierungs-Verfahren ausgehandelt und die Versionen der Bank-Parameterdaten (BPD, vergleiche Kapitel 2.3) und User-Parameterdaten (UPD) abgeglichen. Ggf. werden in der Kreditinstitutsnachricht neue Versionen für BPD oder UPD übertragen. Ähnliches gilt für den Abgleich der Versionen für die öffentlichen Schlüssel des Kreditinstitutes.

In der Kreditinstitutsnachricht können auch kundenspezifische Mitteilungen enthalten sein, z. B. **"Ihre neue ec-Karte liegt zur Abholung für Sie bereit"**.

Als Spezialfall wird auch ein so genannter *"Anonymer Zugang"* über eine Bankleitzahl als Einstieg ermöglicht. Hiermit kann ein Kunde beispielsweise über die in der Antwort gesendete BPD das Angebot des entsprechenden Institutes kennen lernen oder nicht signaturpflichtige Aufträge (z. B. „Gastmeldungen“) senden.

Nach erfolgreicher Dialoginitialisierung und nachdem alle Auftragsnachrichten übertragen und beantwortet wurden, wird der Dialog durch eine Dialogbeendigungsnachricht abgeschlossen. Dadurch ist implizit sichergestellt, dass alle vorhergehenden Nachrichten auch komplett und korrekt übertragen wurden.

2.2.3 Verallgemeinerung des Dialogbegriffs mit FinTS V4.0

F_{inTS V4.0} Das im vorigen Kapitel Gesagte gilt als Spezialfall auch für FinTS V4.0. Allerdings ersetzt der Begriff „Initialisierung“ die Dialoginitialisierung, da sie nicht zwingend in einem Dialogkontext verwendet werden muss – doch davon später.

FinTS V4.0 erlaubt das Senden von Aufträgen zusammen mit der Initialisierung. Dadurch wird zwar die Möglichkeit des Aktualisierens von Parameterdaten unterbunden bzw. muss diese nachgeholt werden – es ergeben sich jedoch verbesserte Performancewerte, da die explizite Initialisierung als separater Prozessschritt wegfällt. Ebenso kann die letzte Auftragsnachricht ein Ende-Kennzeichen enthalten, wodurch sich ein explizites Dialogende erübrigt. Im Extremfall kann also ein FinTS V4.0 „Dialog“ aus Initialisierung, Auftrag und implizitem Dialogende aufgebaut sein, was eine sehr kompakte Verarbeitung erlaubt.

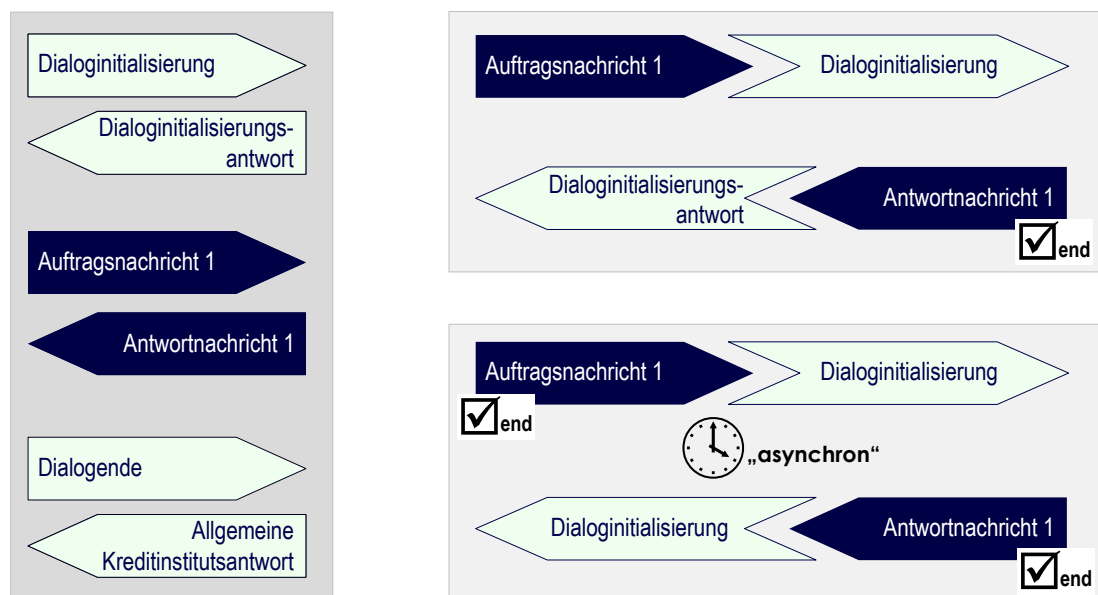


Abbildung 7: Dialogtechniken und Datagramme bei FinTS V4.0

2.2.4 Datagrammtechnik

F_{inTS V4.0} Bei der Verwendung von Datagrammen geht FinTS V4.0 noch einen Schritt weiter: Während die im vorigen Kapitel vorgestellten kompakten Dialognachrichten mit implizierter Initialisierung und Endekennzeichen noch eine synchrone Beantwortung erforderten, hat man sich mit der Datagrammtechnik auch davon frei gemacht. Datagramme benötigen kein synchrones Trägermedium, sie können Zustandslos eingereicht und verarbeitet werden. Die Beantwortung kann über einen asynchronen Dienst, z. B. ein Statusprotokoll erfolgen.

Mit dieser Technik können Aufträge auch über asynchrone Kommunikationsverfahren, z. B. E-Mail ausgetauscht werden. Auch muss zum Absenden eines Folgeauftrags nicht auf die Bestätigung des Erstauftrags gewartet werden. Die einzelnen Nachrichten werden eindeutig bezeichnet und können somit leicht referenziert werden. Diese Technik kann die Verarbeitungslogik von Ausgangskorb-orientierten Kundenprodukten revolutionieren und die Verarbeitung auf beiden Seiten enorm straffen.

2.2.5 Publish / Subscribe und Push-Services

F_{inTS V4.0} Mit den Verallgemeinerungen im Dialogablauf und der Datagrammtechnik lassen sich mit FinTS V4.0 völlig neue Szenarien abbilden. Der Kunde kann über so genannte Publish-/Subscribe-Geschäftsvorfälle Abonnements einrichten und somit nach geregelten Vereinbarungen vom Institut Nachrichten erhalten. So können ihm z. B. täglich um 14:00 Uhr aktuelle Kontenumsätze per E-Mail übermittelt werden.

Grundsätzlich ist jeder Geschäftsvorfall subscribe-fähig, allerdings kann ein Institut per Parametrisierung die unterstützten Geschäftsarten auch einschränken. Die Geschäftsvorfälle für die Pflege der Subscribe-Services sind im Band FinTS Formals, Abschnitt III.6 beschrieben. Sie dienen zum Definieren, Ändern und Löschen von Abonnements. In der jetzigen Ausbaustufe ist es nur möglich, zeitliche Bedingungen festzulegen, logische Abfragen (z. B. Benachrichtigung, wenn ein erwarteter Umsatz auf einem bestimmten Konto eintrifft) werden bei Bedarf folgen.

2.2.6 Rückmeldecodes

Im Rahmen der Kreditinstitutsnachrichten werden standardisierte Rückmeldecodes übertragen (Multibankfähigkeit!), die auf Basis der Referenzinformationen im Nachrichten- und Segmentkopf ein fehlerhaftes Datenelement genau identifizieren und aufgrund des Codes eine intelligente Reaktion des Kundensystems zulassen. Beispielsweise kann ein Kundensystem nach Erkennen einer fehlerhaften Empfänger-Bankleitzahl (Code 9210) dem Benutzer eine Bankleitzahlensuche anbieten, um den entsprechenden Auftrag richtig zu stellen. Die Rückmeldecodes sind auf Datenelementbasis normalisiert und in Fehlerklassen eingeteilt, die eine sehr detaillierte Reaktion des Kundensystems ermöglichen. Fehlerreaktionsvorschriften erleichtern zudem die Implementierung. Zusätzlich besteht auch die Möglichkeit, bankindividuelle Texte mit zu senden, um die Interpretation der Codes, gerade bei weniger intelligenten Endgeräten (z. B. PDAs oder Mobiltelefonen) zu erleichtern.

2.2.7 Statusprotokoll

Im Gegensatz zu herkömmlichen Verfahren, bei denen nach einem Leitungsabbruch der Status der gesendeten Aufträge unbekannt ist und nur durch "Try on Error" über Neuabsenden unter Verwendung der gleichen TAN verifiziert werden kann, gibt es in FinTS V3.0 zwei elegante Möglichkeiten, sich über den Zustand der abgesendeten Nachrichten zu informieren.

1. Initialisierung mit Synchronisation

Hierbei wird in die Initialisierungsnachricht ein Synchronisationssegment eingefügt, das in der Kreditinstitutsnachricht die Nummer der zuletzt verarbeiteten Nachricht zurückliefert.

2. Statusprotokoll

In einem speziellen Segment vom Typ "Statusprotokoll" wird dem Kunden der Status aller Aufträge der zuletzt gesendeten FinTS V3.0-Nachricht in Form von Rückmeldecodes mitgeteilt.

Das Statusprotokoll kann zudem, auch bei normaler Verarbeitung ohne Fehlersituationen, dazu dienen, einen Kunden über den Fortschritt seiner Aufträge zu informieren.

Dabei kann ein Geschäftsvorfall von "Auftrag entgegengenommen" bis "Auftrag ausgeführt" mehrere Stati annehmen, die je Bank unterschiedlich sein können.

□ Dialoginitialisierung mit Synchronisation

Durch Vergleich von Zählerwerten im Kunden- und Banksystem wird ermittelt, ob die letzte Nachricht entgegengenommen werden konnte.

$$1+1=3$$

□ Anfordern eines Statusprotokolls

Durch Anfordern eines FinTS V3.0-Statusprotokolls kann zusätzlich zur Auftragsbestätigung auch der Verarbeitungsstatus erfragt werden.

Abbildung 8: Betriebsicherheit

2.2.8 Verteilte Signaturen

F_{inTS V4.0} In FinTS gibt es seit der ersten Version die Möglichkeit, Mehrfachsignaturen einzusetzen. Dieses Feature ist jedoch für den Einsatz im Firmenkundengeschäft nicht ausreichend, da hier die Forderung nach zeitlicher und örtlicher Unabhängigkeit besteht. FinTS V4.0 bietet hierfür eine Lösung an: so ist es z. B. möglich, dass ein Bote einen Auftrag einreicht – im Sonderfall sogar ohne Herausgeber-Signatur oder aber z. B. mit einer Chipkarte signiert. Der Auftrag wird mit einer Auftrags-ID versehen und beim Institut gespeichert.

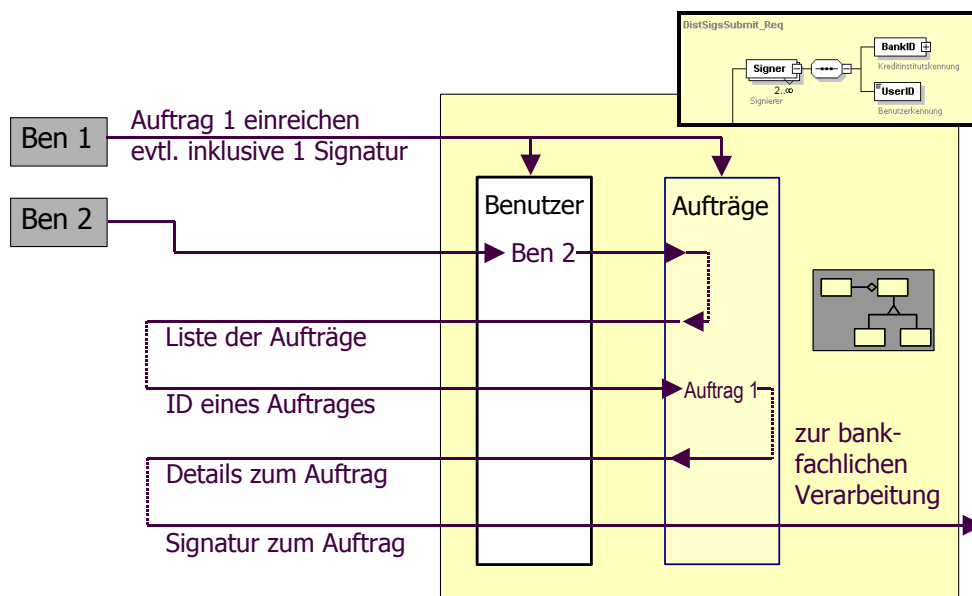


Abbildung 9: Abläufe bei der verteilten Signatur

Ein Zweit-Signierer kann eine Liste der für ihn bestimmten offenen Aufträge abrufen und fehlende Signaturen ergänzen. Dabei kann er auch ein unterschiedliches Signaturverfahren wie PIN/TAN benutzen. Für die Selektion der offenen Aufträge ist es möglich, dass der Zweit-Signierer sich den gesamten Auftrag auf seinen Client (z. B. Browser) holt. Da im Zahlungsverkehr große Datenmengen auftreten können, ist es auch möglich, nur bestimmte charakteristische Kenngrößen (E-Satz-Summe bei DTA oder ähnliches) zum Client zu übertragen und mit diesem Wissen dann den Auftrag freizugeben.

Verteilte Signaturen sind eine wichtige Neuerung für den Einsatz von FinTS im Bereich der gewerblichen Kunden. Für die genaue Ausgestaltung – z. B. Filterfunktionen für die Auftragsselektion – sind genügend Freiräume vorhanden.

Abgerundet wird diese Funktion noch durch Möglichkeiten der Statusabfrage, z. B. über abgeschlossene Aufträge, Anzahl geleisteter und noch fehlender Signaturen usw. Auch eine Funktion zum Löschen von Aufträgen ist vorhanden.

Details zu den zugehörigen Geschäftsvorfällen befinden sich im Band FinTS Formals, Abschnitt III.7.

2.3 Parameterdaten in FinTS V3.0

2.3.1 Allgemeines zu FinTS V3.0-Parameterdaten

Bei der Gestaltung von multibankfähigen Systemen stößt man zwangsweise an Grenzen, die durch die unterschiedlichen Verarbeitungssysteme bei den verschiedenen Kreditinstituten hervorgerufen werden. Ein einfaches Beispiel ist die Anzahl der Verwendungszweckzeilen bei einer Überweisung. Generell sind beim DTA-Format 14 Zeilen für den Verwendungszweck vorgesehen; je nach Institut werden jedoch oft nur 3 bis 4 Zeilen interpretiert (und auch von der Zulieferersoftware erwartet). Diese Unterschiede gilt es durch eine Parametersteuerung zu eliminieren, so dass ein Kunde für all seine Bankverbindungen die gleiche Verarbeitungslogik erkennen kann. Dazu muss das Kundensystem natürlich in der Lage sein, die Parametersteuerung entsprechend umzusetzen. Solche Verarbeitungsrestriktionen sind in der BPD abgelegt.

Weiterhin gibt es auch kundenspezifische Unterschiede zu beachten. Der Einstieg bei der Initialisierung erfolgt über eine wie auch immer geartete Benutzererkennung, die den Benutzer (genauer: das Sicherheitsmedium des Benutzers) identifiziert.

Um nun auch die zugeordneten Konten und die erlaubten Auftragsarten an das Kundensystem übermitteln zu können, gibt es die UPD.

Generell haben BPD und UPD keine rechtliche Relevanz, da sie dem Kundensystem nur vorab mitteilen, welche Prüfungen und Restriktionen institutsseitig wohl zu erwarten sind. Die Prüfungen selbst werden parallel im Banksystem bei der Einreichung der Aufträge nochmals durchgeführt.

Es können bankseitig auch Aufträge abgelehnt werden, die im Kundensystem auf Basis von BPD/UPD akzeptiert wurden, wenn z. B. Prüfkriterien vorliegen, die zeitlich noch nicht in den Parameterdaten eingearbeitet sind.

Dies betrifft vor allem Informationen wie Limite des Kunden, die ja doch etlichen Einflüssen unterworfen sind. Die Aktualisierung (der Ersatz) der BPD respektive UPD geschieht über einen Versionsabgleich im Zuge der Initialisierung.

Grundsätzlich ist die Implementierung der BPD und UPD sowohl für Kunden- als auch für Bankensysteme obligatorisch, da sich der Bedienungskomfort für den Kunden dadurch enorm erhöhen kann. Allerdings bezieht sich die Verpflichtung nur auf einen kleinen Teil der Informationen, die als MUSS-Felder definiert sind. Dies ist darauf zurückzuführen, dass es sich bei der Einführung der Parameterdaten mit HBCI V2.01 um ein völlig neues Konzept handelte, das noch in keinem Kreditinstitut existierte. Inzwischen haben sich diese Restriktionen jedoch weitgehend erübrigt.

2.3.2 Neu mit FinTS V4.0 – IPD und UPDI

FinTS V4.0 Bedingt durch die Rolle des Intermediärs wird mit FinTS V4.0 eine weitergehende Parametrisierung angeboten, die IPD und UPDI:

- **Intermediärs-Parameterdaten (IPD)**
In Kapitel 2.2.1 wurde der Begriff des Intermediärs eingeführt und es wurden gültige Szenarien definiert. Zur Umsetzung dieser Szenarien muss ein Intermediär im Institut bekannt sein, d. h. er muss sich registrieren. Mit der Registrierung, die außerhalb von FinTS erfolgt, erhält er auch eine IPD, welche alle Geschäftsvorfälle enthält, die der Intermediär grundsätzlich anbieten darf.
- **UPD über Intermediär (UPDI)**
Ist ein Intermediär bei einem Institut registriert, so kann ein Kunde über einen speziellen FinTS-Geschäftsvorfall „Intermediäre auflisten“ (FinTS Formals, Abschnitt V.7) ermitteln, welche Portale er für die Kommunikation mit einem Institut verwenden darf; er erhält insbesondere die ID des gewünschten Intermediärs. Mit weiteren Geschäftsvorfällen kann er nun festlegen, welche Auftragsarten er mit welchen Einschränkungen (z. B. Betragsgrenzen) bei welchem Intermediär durchführen will.

Ruft ein Kunde nun das gewünschte Portal auf, so kann der Intermediär durch die Verknüpfung von IPD mit UPDI dem Kunden das zugelassene Portfolio an Geschäftsvorfällen anbieten.

Wie die in Kapitel 2.2.1 beschriebenen Szenarien für Callcenter usw. zeigen, kann es sich bei den IPDs auch um Geschäftsvorfälle handeln, die dem Kunden über Internet-Banking überhaupt nicht angeboten werden. Hier hat ein Institut alle Freiheiten, die vorhandenen Prozesse optimal umzusetzen.

2.3.3 Aufbau der BPD (Bankparameterdaten)

In den **Bankparameterdaten** wird dem Kundensystem die Infrastruktur des jeweiligen Kreditinstitutes mitgeteilt.

- Ein **allgemeiner Teil** beschreibt die generellen Rahmenbedingungen, wie z. B. den exakten Namen des Institutes, die unterstützten Sprachen u. ä.
- Im Segment **Kommunikationszugang** werden verfügbare Transportmedien beschrieben.

- Unter **Sicherheits- und Komprimierungsverfahren** sind die von der Bank unterstützten Verfahren aufgeführt.
- Die restlichen Segmente enthalten die sog. **Geschäftsvorfallparameter**, in denen die Restriktionen pro Geschäftsvorfall beschrieben sind. In einem Rumpfteil sind wieder gemeinsame Kenngrößen, wie z. B. die Anzahl der zugelassenen Signaturen oder die maximale Anzahl an Aufträgen pro Nachricht definiert. Der Rest enthält nun wirklich die geschäftsvorfallspezifischen Einschränkungen, wie die oben erwähnte Anzahl von Verwendungszweckzeilen bei der Überweisung.

2.3.4 Aufbau der UPD (Userparameterdaten) und IPD

In den **Userparameterdaten** erhält das Kundensystem Informationen über das Profil eines Kunden, genauer über einen Benutzer (entspricht meist dem Sicherheitsmedium). Bei entsprechender Ausgestaltung der UPD kann das Kundensystem zu einem wirklich intelligenten Cash-Management-System ausgebaut werden, da es u. a. Informationen über Limite pro Konto erhält und so den Geldfluss optimieren kann.

- Unter **Userparameter allgemein** finden sich u. a. die Benutzererkennung und Daten zur Versionskontrolle.
- Die restlichen Segmente sind vom Typ **Kontoinformation** und enthalten pro Konto wiederum allgemeine Informationen, wie z. B. die Kontonummer und Produktbezeichnung, aber auch die erlaubten Geschäftsvorfälle bis hin zu Limiten.

Gleiches gilt für die mit FinTS V4.0 neu hinzugekommene IPD und UPDI. Die IPD stellt dabei nur eine abgespeckte UPD dar, die beschreibt, welche Geschäftsvorfälle ein Intermediär anbieten darf.

In der UPDI kann ein Kunde die Geschäftsvorfälle und Konten definieren, die er z. B. über ein Portal bearbeiten möchte. Hier sind auch optionale Parameter wie Limite erlaubt.

3 FinTS Security

FinTS bietet eine ganze Reihe von Sicherheitsalternativen an, die hier kurz aufgelistet und später genauer erläutert werden:

- RDH-Verfahren¹ auf Basis von asymmetrischen RSA-Algorithmen² und folgenden Sicherheitsmedien:
 - ZKA-Signaturkarte (seit FinTS V3.0)
 - RDH-Softwareverfahren
 - nicht standardisierte RDH-Interimskarten
- DDV-Verfahren³ auf Basis von symmetrischen Triple-DES- und MAC-Algorithmen⁴
 - DDV-Chipkarte mit ec-Karten-Betriebssystem Typ-0 oder Typ-1
- PIN/TAN-Verfahren mit SSL als Transportverschlüsselung (seit FinTS V3.0)

All diese Verfahren dienen dazu, auf unterschiedliche Art und Weise verschiedene Aspekte der Sicherheit abzubilden, die im folgenden Kapitel kurz dargestellt sind.

3.1 Sicherheitsaspekte

Nachdem unter dem Baukastensystem FinTS unterschiedliche Sicherheitsverfahren zu betrachten sein werden, werden zunächst die grundsätzlichen Aspekte der Sicherheit kurz erläutert. Die verwendeten Syntaxstrukturen beziehen sich dabei auf das in FinTS V3.0 verwendete Verfahren. In FinTS V4.0 werden stattdessen die Verfahren XML-Signature und XML-Encryption verwenden, was aber auf die folgende grundsätzliche Darstellung keine Auswirkung hat.

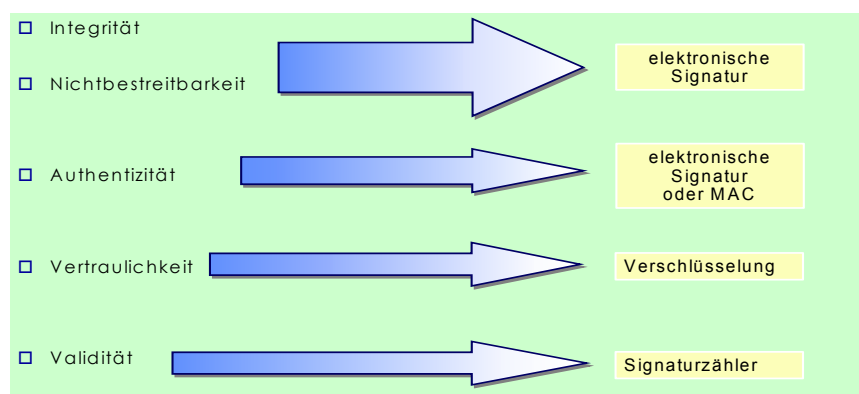


Abbildung 10: Sicherheitsaspekte

¹ RDH: RSA-DES-Hybridverfahren, Signatur mittels RSA und Verschlüsselung durch Triple-DES

² RSA: Rivest, Shamir, Adleman – die Erfinder des asymmetrischen Kryptoverfahrens

³ DDV: DES-DES-Verfahren, Signatur und Verschlüsselung mittels Triple-DES
MAC: Message Authentication Code

⁴ DES: Data Encryption Standard, Triple-DES: 3-fache Anwendung des DES-Algorithmus

3.1.1 Authentisierung des Kunden

Unter Authentisierung des Kunden (auch "Authentifikation" genannt) wird hier die Berechtigungsprüfung gegenüber dem Sicherheitsmedium verstanden. Konkret wird vor der Ausführung von Sicherheitsfunktionen zur Eingabe eines Passwortes aufgefordert, das lokal geprüft wird (also das Kundensystem nicht verlässt). Bei chipkartengestützten Verfahren wird diese Prüfung in der SmartCard durchgeführt, bei Softwareverfahren in der PC-Software des Kundensystems.

3.1.2 Gegenseitige Authentisierung Kundensystem / Banksystem

Beim Vorgang der gegenseitigen Authentisierung machen sich die beiden kommunizierenden Parteien miteinander bekannt. Dies geschieht beim HBCI-Verfahren während der Initialisierung durch Signieren der Kunden- und Kreditinstitutsnachricht. Kann vom Partner die Signatur erfolgreich verifiziert werden, ist die Authentifikationsprüfung erfolgreich abgeschlossen. Beim RDH-Verfahren erfolgt bis zur Version FinTS V3.0-Version optional nur eine einseitige Authentisierung des Kunden, mit FinTS V4.0 ist auch die institutsseitige Signatur verpflichtend.

Beim PIN/TAN-Verfahren dient die Übermittlung der Benutzerkennung und der PIN zur Authentisierung des Kunden. Durch die Server-Authentisierung bei SSL wird auch die Identität des Kreditinstitutssystems sichergestellt.

3.1.3 Nachweis der Herkunft

Bei eingereichten Aufträgen ist es wichtig, dass die Herkunft eindeutig nachgewiesen werden kann ("non repudiation of origin"). Dies wird durch die jeweilige elektronische Signatur gewährleistet. Beim DDV-Verfahren besteht die theoretische Möglichkeit der Signatur eines Kundenauftrages durch das Kreditinstitut. Dies wird allerdings durch das Vertrauensverhältnis Kunde / Kreditinstitut aufgehoben. Eine echter Herkunftsnachweis ist nur bei asymmetrischen kryptografischen Verfahren wie z. B. dem RDH-Verfahren möglich.

3.1.4 Integrität - Elektronische Signatur

Die elektronische Signatur (nur bei HBCI-Verfahren) soll beweisen, dass die FinTS-Nachricht auf dem Übertragungsweg nicht modifiziert wurde. Dazu wird zunächst ein so genannter „Hash-Wert“ - eine Art kryptografische Prüfsumme - über die gesamte Nachricht gebildet. Aus dem Ergebnis wird dann gemäß MAC⁵ bzw. RSA eine elektronische Signatur berechnet, die in das FinTS V3.0-Segment *Signaturabschluss* eingestellt wird. Bei FinTS V4.0 wird die Signatur unter dem entsprechenden Tagnamen in die Struktur nach XML-Signature eingebettet.

Der Empfänger bildet den Hashwert nach dem gleichen Algorithmus und überprüft die Signatur mittels Secret Key (DDV) respektive Public Key (RDH).

⁵ MAC: Message Authentication Code

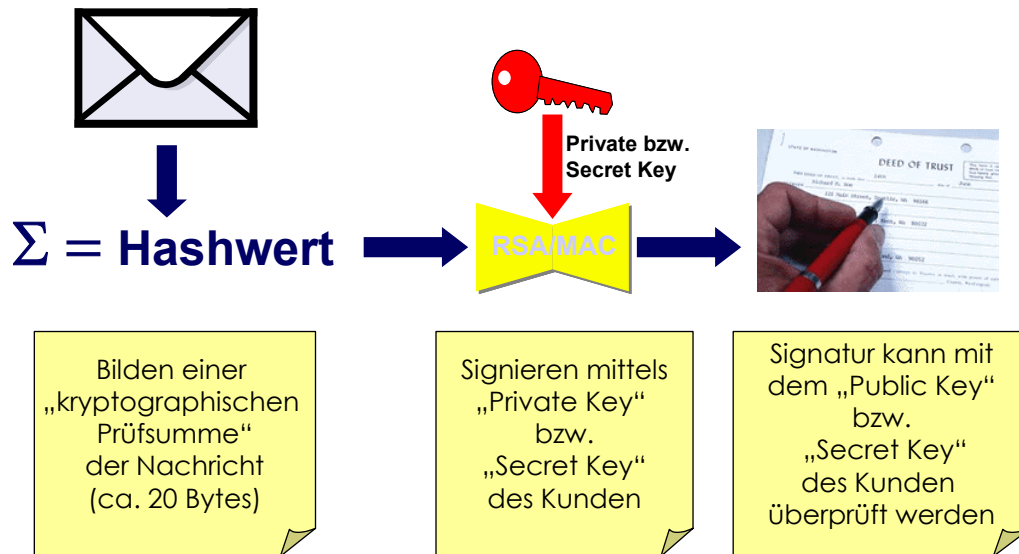


Abbildung 11: Signaturbildung nach DDV- bzw. RDH-Verfahren

3.1.5 Geheimhaltung - Verschlüsselung / Chiffrierung

Im Gegensatz zur elektronischen Signatur, bei der die Nachricht ja immer noch lesbar ist, wird bei der Verschlüsselung die gesamte Nachricht kryptografisch behandelt und somit unleserlich gemacht. Dies hat vor allem Vorteile bei der Übertragung vertraulicher Informationen wie z. B. von Umsatzdaten.

Bei FinTS V3.0 mit Sicherheitsverfahren HBCI wird zur Verschlüsselung der Daten generell Triple-DES verwendet. Als Schlüssel wird aus Sicherheitsgründen nicht der eigentliche Chiffrierschlüssel benutzt, sondern ein nachrichtenspezifischer Schlüssel. Dieser wird für jede Nachricht neu aus einer Zufallszahl gebildet, die mit dem Chiffrierschlüssel gemäß DDV respektive RDH verschlüsselt und der Nachricht vorangestellt wird.

Bei FinTS V4.0 wird außer der Verschlüsselung nach dem HBCI-Verfahren auch SSL für die Verschlüsselung angeboten. Da SSL oder https im Internetbereich den Standard für die Transportverschlüsselung darstellen, wird das HBCI-Verschlüsselungsverfahren nur in folgenden Situationen verwendet werden:

- auf Strecken, die kein https unterstützen (z. B. E-Mail mit SMTP)
- in Szenarien, die eine streckenübergreifende Ende-zu-Ende Verschlüsselung erfordern. Hierbei kann es zu doppelter Verschlüsselung durch SSL und HBCI-Verfahren kommen.

3.1.6 Validität - Doppeleinreichungskontrolle

Einer der möglichen Angriffe in einem kryptografischen System besteht darin, Daten auf einer Leitung abzuhören und die gespeicherte Information wiederholt einzuspielen ("replay attack"). Eine Überweisung würde in so einem Fall gegen den Willen des Kunden mehrfach durchgeführt werden.

Offt wird deshalb als Kriterium für die Eindeutigkeit ein Zeitstempel herangezogen, was aber zum einen nicht von allen FinTS-Endgerätetypen unterstützt wird (z. B. SmartPhones), zum anderen auch nicht zuverlässig funktioniert, da man ja nicht davon ausgehen kann, dass jede PC-Uhr plausible Werte liefert.

In FinTS wurde deshalb ein ausgeklügeltes Verfahren zur Doppeleinreichungskontrolle spezifiziert, das zum einen Missbrauch ausschließt, zum anderen die Flexibilität kaum einschränkt.

Es besteht aus einer Kombination eines *Sequenzzählers*, der parallel auf dem Sicherheitsmedium und im Kreditinstitut geführt wird und einer Liste von bereits eingereichten Sequenzen, in welcher die Lücken über einen bestimmten Zeitraum festgehalten werden. Dies ist nötig, da im Offline-Betrieb, d. h. wenn Aufträge zu verschiedenen Zeiten von verschiedenen Personen ohne Leitungsverbindung erfasst und später in anderer Reihenfolge gesendet werden, nicht sichergestellt werden kann, dass die Sequenznummern aufsteigend beim Kreditinstitut eintreffen.

3.1.7 Schlüsselverwaltung (Key-Management)

Im Band „*Security HBCI*“ sind spezielle Geschäftsvorfälle für das Ändern und Sperren von Schlüsseln beschrieben. Diese Verfahren betreffen nur das RSA-Verfahren, da die Schlüssel beim MAC-Verfahren fest in der Chipkarte abgelegt sind.

Für das RSA-Verfahren gelten auch die – mit FinTS V3.0 neu hinzugekommenen – Verfahren zur Erstinitialisierung zunächst noch mit Hilfe von Ini-Briefen zur Sicherstellung der Authentizität der Partner. Dieses doch recht umständliche Verfahren wird im Zuge der Spezifikation einer einheitlichen RSA-Chipkarte durch Zertifikate abgelöst werden.

3.2 Sicherheitsverfahren HBCI

Grundlegend werden beim Sicherheitsverfahren HBCI die zwei unterschiedlichen kryptografischen Verfahren RDH und DDV eingesetzt. Hier nur eine Kurzbeschreibung zum besseren Verständnis der folgenden Abschnitte:

□ RDH-Verfahren (RSA-DES-Hybridverfahren)

Beim *asymmetrischen* RSA-Verfahren werden jeweils Schlüsselpaare verwendet, die immer aus einem *privaten* Schlüssel ("private Key") und einem *öffentlichen* Schlüssel ("public key") bestehen. Die Idee besteht darin, dass ein Kunde per Software oder auf einer Chipkarte ein persönliches Schlüsselpaar erzeugt und seine Aufträge mit seinem Private Key signiert. Das Kreditinstitut kann mittels dem zuvor übermittelten Public Key die elektronische Unterschrift auf Korrektheit prüfen.

Der Public Key beweist einerseits die Herkunft der Signatur eindeutig, muss andererseits nicht geheim gehalten werden, da mit ihm nur Signaturen überprüft, jedoch nicht erzeugt werden können.

Entsprechend kann ein Kunde vertrauliche Daten mit dem öffentlichen Schlüssel des Kreditinstitutes verschlüsseln. Nur dieses kann anschließend mit Hilfe seines privaten Schlüssels die Daten wieder entschlüsseln und so lesbar machen.

Bei HBCI werden für RDH in der Maximalausprägung bei der ZKA-Signaturkarte drei Schlüsselpaare verwendet, nämlich ein *Signierschlüsselpaar* (D-Schlüssel)

zum rechtswirksamen Unterschreiben von Nachrichten, ein *Authentisierungsschlüsselpaar* (S-Schlüssel) zum Nachweis der Authentizität des Kunden-/Banksystems und ein *Chiffrierschlüsselpaar* (V-Schlüssel) zum Verschlüsseln der Nachrichten mittels Nachrichten-Chiffrierschlüssel. Bei den meisten Geschäftsvorfällen ist der Einsatz des Authentisierungsschlüsselpaares zur Signaturbildung ausreichend – das Signaturschlüsselpaar, dessen Verwendung meist durch explizite Eingabe der Karten-PIN pro Geschäftsvorfall abgesichert ist, wird nur bei Aufträgen verwendet, die eine rechtswirksame elektronische Signatur erfordern, z. B. Kontoeröffnungen u. ä.. Beim RDH-Softwareverfahren und beim Einsatz von RDH-Interimskarten steht kein Schlüsselpaar für rechtswirksame Signaturen zur Verfügung.

□ **DDV-Verfahren
(DES-DES-Verfahren)**

Das DDV-Verfahren ist ein *symmetrisches* Verfahren, das heißt, die Schlüssel, welche zum Signieren bzw. Chiffrieren herangezogen werden, müssen beiden Partnern bekannt, also vorher auf alternativem Wege ausgetauscht worden sein. Es handelt sich bei dem gemeinsamen Schlüssel um einen geheimen Schlüssel ("secret key"), da die Sicherheit davon abhängt, dass nur die beiden involvierten Parteien diesen Schlüssel kennen. Bei HBCI werden zwei Schlüsselarten verwendet, nämlich ein *Signierschlüssel* („S-Schlüssel“) zum Unterschreiben von Nachrichten und ein *Chiffrierschlüssel* („C-Schlüssel“) beim Verschlüsseln der Nachrichten mittels Nachrichten-Chiffrierschlüssel. Die hier zum Einsatz kommenden kryptografischen Funktionen werden auf der Basis des Triple-DES-Verfahrens durchgeführt.

Beide aufgeführten Verfahren und Mechanismen sind in der FinTS V4.0-Spezifikation im Band zu HBCI-Sicherheit ausführlich beschrieben. Die Anwendung ist für Kunden- und Banksysteme größtenteils zwingend vorgeschrieben. Freiheitsgrade bestehen lediglich beim Signieren von Banknachrichten im RDH-Verfahren. Seit HBCI Version 2.01 muss jede Nachricht zwingend verschlüsselt werden.

3.2.1 Sicherheitsmedien

Als Zielsystem wird eine RSA-basierende Lösung mit einer vom ZKA zertifizierten Chipkarte angestrebt. Da RSA-Chipkarten erst in letzter Zeit die erforderlichen Leistungsdaten liefern können, wurde mit FinTS V3.0 die Banken-Signaturkarte als gemeinsames Medium eingeführt. Deshalb wurden in den Vorgängerversionen die beiden Sicherheitsverfahren spezifiziert, die in großen Teilen softwarekompatibel sind und auch leicht in das Zielsystem migrierbar sind:

„Generelles Ziel aller Verbände ist ein asymmetrisches Sicherungsverfahren, basierend auf einer ZKA-weit standardisierten Banken-Signaturkarte.“

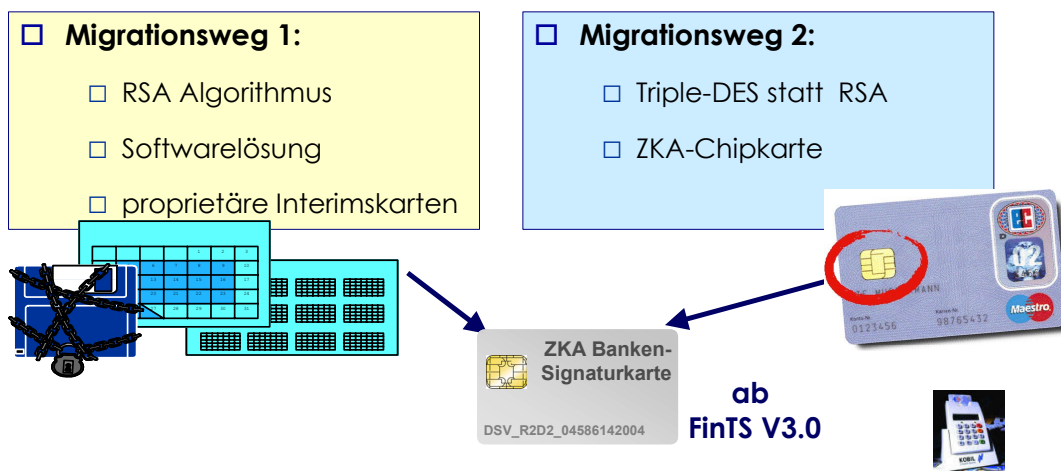


Abbildung 12: HBCI Sicherheitsverfahren

DDV-Verfahren mit ZKA-Chipkarte



Diese Alternative hat den Vorteil einer Chipkarte als Hardware-Medium. Alle sensitiven kryptografischen Prozesse laufen im Chip ab, sind also von außen nicht zugänglich. Die Sicherheit ist in Form der Chipkarte auch portabel, d. h. diese Lösung kann auch in einem unbekanntem Environment (z. B. öffentliches FinTS Kundensystem in einem Hotelfoyer) problemlos eingesetzt werden. Das DDV-Verfahren hat als einzigen Nachteil die Nichtbeweisbarkeit der Herkunft; dies wird jedoch durch das Vertrauensverhältnis Kunde - Bank aufgehoben. Auf Grund dieser fehlenden Beweisbarkeit kann mit der DDV-Karte auch keine rechtsgültige Signatur gebildet werden.

Als Sicherheitsmedium kommt eine ZKA-Chipkarte zum Einsatz, wie sie auch als ec-Chipkarte (Geldkarte) Verwendung findet.

RDH-Verfahren als Softwarelösung

Das RDH-Verfahren ist, wie oben schon ersichtlich, das Zielsystem für die HBCI-Sicherheit. Bei der Softwarelösung werden die gesamten kryptografischen Funktionen im Endgerät durchgeführt. Vorteil dabei ist, dass man dieses Verfahren ohne zusätzliche Hardware-Investitionen (Chipkartenleser) einsetzen kann.

Die Mobilität kann - innerhalb einer sicheren Umgebung – mit Hilfe einer Disketten oder einem USB Memorystick erreicht werden.

Die Diskussionen über die Sicherheit im Internet zusammen mit den Auswirkungen aus dem Signaturgesetz haben in den letzten Jahren die Sensibilität gegenüber der Abwicklung von Bankgeschäften am Home-PC dramatisch verschärft. Außerdem wurde erreicht, dass die Anschaffung eines Chipkartenlesers für den Privatkunden heute keine Hemmschwelle mehr darstellt. Hierdurch hat sich auch im RSA-Bereich ein Schwenk in Richtung Chipkarte ergeben. Umso größer wurde der Druck, zeitnah eine einheitliche RSA-Chipkartenstrategie zu besitzen, um nicht über diesen Punkt die Multibankfähigkeit von HBCI zu gefährden. Als Ergebnis wurde die ZKA Banken-Signaturkarte entwickelt, die jedoch erst seit FinTS Version 3.0 zur Verfügung steht.

RDH-Interimskarten

Aufgrund dieser Situation wurden bereits mit den letzten HBCI-Versionen vermehrt im Markt auch RSA-Chipkartenlösungen eingesetzt, die zum Teil auch das HBCI Keymanagement-Verfahren in modifizierter Form anwenden. All diese RSA-Chipkartenlösungen sind nicht multibankfähig und werden wohl in einer der nächsten FinTS-Versionen durch die ZKA Banken-Signaturkarte abgelöst werden.

ZKA Banken-Signaturkarte



Neue Sicherheitsmechanismen waren von Anfang an das Kernstück der HBCI-Architektur. Als Basis diente hierbei zu großen Teilen das ZKA-Abkommen "DFÜ mit Kunden", das für die Kommunikation mit Geschäftskunden spezifiziert wurde. Gerade im Sicherheitsbereich wurden viele Details aus diesem Verfahren übernommen.

Eine weitere Motivation für die sicherheitstechnische Ausgestaltung des HBCI-Standards waren die Anforderungen aus dem Signaturgesetz, welche eine rechtsgültige Abwicklung von Geschäften auf elektronischem Wege ermöglichen.

Obwohl zusätzlich zum kryptografischen Verfahren und der entsprechenden Karte noch viele Fragen gelöst werden mussten, bevor von einem Home-PC aus signaturgesetzkonforme Geschäfte abgewickelt werden können, unterstützte HBCI von Anfang an die wichtige Methodik von Kontext-Signaturen, d. h. die Daten eines Geschäftsvorfalles gehen in die Signaturbildung mit ein. Hierdurch wird der Vorgang des Unterschreibens eines Dokumentes in eine elektronische Variante umgesetzt, wobei jedoch der ursprüngliche Gedanke des Kontextbezuges erhalten bleibt. Dem gegenüber garantieren Transportsicherungsverfahren, wie sie bei anderen internationalen Standards eingesetzt werden, nur für die Authentizität und Vertraulichkeit, da hier nur der zu übertragende Datenstrom ohne Inhaltsbezug mit einer kryptografischen Prüfsumme versehen wird (mehr Informationen hierzu finden Sie im Kapitel „Positionierung“).

Obwohl HBCI hier generell einen Schritt weiter geht, wird erst mit der Banken-Signaturkarte die Möglichkeit geschaffen, rechtsverbindliche Signaturen zu erzeugen.

Die ZKA Banken-Signaturkarte auf Basis des neuen SECCOS-Betriebssystems verfügt über ein eigenes Signaturschlüsselpaar, das zur Bildung dieser Art von Signaturen herangezogen wird (D-Schlüssel).

Hierzu befindet sich auf der Banken-Signaturkarte eine Standard-Signatur-Anwendung, welche generell für die Signaturbildung auch in anderen Umfeldern wie z. B. einer elektronischen Steuererklärung (ELSTER) verwendet werden kann.

Das bedeutet, dass jede Banken-Signaturkarte, die durch die Verlage der Banken- und Sparkassen ausgegeben wird, für HBCI eingesetzt werden kann. Trotzdem wird es spezielle HBCI-Signaturkarten geben, welche zur Erhöhung des Komforts ein Notizbuch (EF_Notepad) zur Aufnahme von Bankverbindungen enthalten.

Mit der Banken-Signaturkarte können somit Geschäftsvorfälle je nach Anwendungsbezug unterschiedlich signiert werden:

- Durch Verwendung des Authentifizierungsschlüsselpaares („S-Schlüssel“) können Signaturen wie bisher durchgeführt werden.
- Durch Verwendung des Signierschlüsselpaares („D-Schlüssel“) können rechtsgültige Signaturen erzeugt werden, wobei jede Signatur nochmals explizit durch Eingabe der Karten-PIN für den privaten Signierschlüssel bestätigt werden muss.

Durch Einführung dieser beiden Signierverfahren, die seit FinTS V3.0 noch durch Kombination mit dem PIN/TAN-Verfahren ergänzt werden, ergibt sich die Notwendigkeit der Einführung von geschäftsvorfalls-spezifischen Sicherheitsklassen, die im Folgenden noch dargestellt werden. Zunächst sollen aber die ebenfalls neu eingeführten Sicherheitsprofile kurz erläutert werden.

3.2.2 Sicherheitsprofile

Zusätzlich zu den unterschiedlichen Hard- und Software-basierten Verfahren, wird seit FinTS V3.0 auch eine sicherheitstechnische Erweiterung vorgenommen. Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) wurden für eine sichere Abwicklung Rahmenbedingungen vorgegeben, die FinTS in den Sicherheitsprofilen umsetzt. Hierzu gehören Schlüssellängen und sogenannte Paddingverfahren zum Ergänzen von Nachrichten durch Füllzeichen.

Zusätzlich wurden auch neue Verfahren in FinTS V3.0 eingeführt, die von der Banken-Signaturkarte unterstützt werden und damit in FinTS zumindest theoretisch ebenfalls zur Verfügung stehen.

□ RDH-1

Mit RDH-1 wird ein Migrationsprofil bezeichnet, das bezogen auf Schlüssellänge, Paddingverfahren und Sicherheitsmedien die RDH-Sicherheitsmechanismen aus HBCI V2.2 und früher abbildet.

□ RDH-2

Bei RDH-2 werden die Anforderungen an Schlüssellängen und Paddingverfahren des BSI erfüllt (Stand 2004). Als Sicherheitsmedien werden RDH-Disketten und RDH-Interimskarten unterstützt.

□ RDH-3

Mit RDH-3 wird die ZKA Banken-Signaturkarte unterstützt; es werden die BSI-Anforderungen Stand 2004 auf Basis der in HBCI bereits verwendeten Algorithmen unterstützt: RipeMD 160 für Hashwertbildung und ISO 9596-2 (D-Schlüssel) bzw. PKCS#1 (S-Schlüssel) als Paddingverfahren.

- RDH-4

Es werden von der ZKA Banken-Signaturkarte unterstützte und vom BSI zugelassene alternative Algorithmen unterstützt – dies sind SHA-1 für die Hashwertbildung und PKCS#1 als Paddingverfahren.

- DDV-1

Dieses Profil beschreibt die Nutzung der DDV-Algorithmen und der entsprechenden Karte, wie aus HBCI V2.2 bekannt.

3.2.2.1 Bankenprofil 2004

Die Schilderung der Sicherheitsprofile reizt zwar die Möglichkeiten der verfügbaren SECCOS-Signaturkarte voll aus, die Anwendung bringt aber Nachteile in Bezug auf Multibankfähigkeit, da nicht alle Institute das volle Portfolio an Algorithmen unterstützen. Hinzu kommt, dass der für Firmenkunden definierte ZKA-Standard „DFÜ mit Kunden“ unter dem Signaturverfahren „A004“ ebenfalls die SECCOS-Signaturkarte verwendet – allerdings mit einigen Einschränkungen. Daher hat man sich mit FinTS V4.0 entschlossen, ein so genanntes Bankenprofil 2004 (vgl. Band Security HBCI, Kapitel II.1.1) zu definieren, das sich auf das Sicherheitsprofil RDH-3 und eine Schlüssellänge von 1024 bit beschränkt. Sukzessive werden je nach BSI-Empfehlungen Erweiterungen vorgenommen werden.

3.2.3 Sicherheitsklassen

Unter den ebenfalls neu eingeführten Sicherheitsklassen wird beschrieben, welche Art der Signaturbildung für einen Geschäftsvorfall vorgeschrieben ist:

- Authentifikation
Es wird unter Verwendung des Authentifikations-Schlüsselpaares – wie bei HBCI V2.2 – signiert.

Die weiteren Sicherheitsklassen betreffen nur die Verwendung der ZKA-Signaturkarte analog §2, Signaturgesetz:

- fortgeschrittene elektronische Signatur
- fortgeschrittene elektronische Signatur mit Zertifikatsprüfung
- qualifizierte elektronische Signatur mit Zertifikatsprüfung

Unter einer fortgeschrittenen Signatur wird verstanden, dass der Inhaber des Signaturschlüsselpaares mit den ihm zur Verfügung stehenden Einrichtungen eine Signatur bildet, die durchgehend auf Veränderungen geprüft werden muss.

Eine qualifizierte elektronische Signatur wird zum Erstellungszeitpunkt auf Basis eines gültigen qualifizierten Zertifikates unter Verwendung einer sicheren Signaturerstellungseinheit erzeugt.

Welcher Geschäftsvorfall nach welcher Sicherheitsklasse zu behandeln ist, wird über die BPD mitgeteilt.

3.2.4 Komprimierung

Seit FinTS V3.0 wird erstmals auch ein Komprimierungsverfahren spezifiziert. Als Algorithmus wird „Deflate“ als Default festgelegt, da dieses Verfahren u.a. lizenzfrei erhältlich ist.

Komprimierung ist ein sinnvolles Feature, um z. B. bei großen Zahlungsverkehrsdatensätzen im Zusammenhang mit Sammelaufträgen die Übertragung zu optimieren.

Mit der Einführung der XML-Syntax mit FinTS V4.0 ist die Verwendung eines Komprimierungsverfahrens unverzichtbar.

TAN-Liste	
984572	864476
235466	467898
834562	336653
432236	135623
437424	568524
335565	808644
535665	440044
336573	865786
235673	234555
466323	886535

3.3 Sicherheitsverfahren PIN/TAN

Als neues Sicherheitsverfahren wurde mit FinTS V3.0 das weit verbreitete PIN/TAN-Verfahren integriert. Integration bedeutet im Wesentlichen, dass in den Signaturen anstelle eines Kryptogramms PIN und TAN transportiert werden. Somit bleibt der Nachrichtenaufbau gleich und die Erweiterungen auf Kunden- und Institutsseite sind überschaubar.

Da beim PIN/TAN-Verfahren keine kryptografischen Funktionen zur Verfügung stehen, kann auch keine Verschlüsselung wie beim HBCI-Verfahren durchgeführt werden. An dessen Stelle tritt die im Standard-Browser integrierte SSL-Verschlüsselung mit Server-Authentifizierung.

Über ein spezielles Parametersegment *HIPINS* wird dem Kundensystem mitgeteilt, welche Geschäftsvorfälle eine TAN erfordern.

Praktischer Hinweis – PIN/TAN Erweiterung V1.01 mit HBCI V2.2

Die Einführung des PIN/TAN-Verfahrens hat die Spezifikationsarbeit des ZKA schier überrollt. Somit war bereits vor Veröffentlichung von FinTS V3.0 eine stabile Spezifikation am Markt verfügbar und umgesetzt, die nun auf breiter Basis in Implementierungen unterstützt wird: die PIN/TAN-Erweiterung V1.01. Von der Funktionalität her ist diese Version mit der offiziellen FinTS V3.0 identisch. Änderungen ergeben sich in der Funktionsfähigkeit des PIN/TAN-Managements.

PIN/TAN mit FinTS V4.0

Während die vorhandenen Verfahren die PIN und TAN in den Signaturen transportiert, wurde dieses Feature mit FinTS V4.0 als One-Time-Password sauber ausmodelliert. Bzgl. des PIN/TAN Managements ergeben sich keine Änderungen zur Vorversion.

PIN/TAN-Management

Auch beim PIN/TAN-Verfahren sind Möglichkeiten vorhanden, um z. B. ein PIN zu sperren oder eine TAN-Liste frei zu schalten. Da diese Prozesse jedoch seit Einführung des PIN/TAN-Verfahrens existieren und in den Rechenzentren in unterschiedlicher Weise zur Verfügung stehen, sind diese Management-Funktionen nicht multibankfähig. Es ist also nicht möglich, eine von Institut A ausgegebene TAN-Liste bei Institut B zu verwenden. Trotzdem bietet die Gesamtheit der Geschäftsvorfälle zum PIN/TAN Management eine komfortable Möglichkeit, um mit einem Kundenprodukt mehrere Kreditinstitute in gleicher Weise verwalten zu können.

4 FinTS Messages

Die FinTS Geschäftsvorfälle sind unabhängig von den FinTS-Versionen zu sehen und werden bei Bedarf fortlaufend ergänzt. Es existiert eine große Anzahl von ZKA-weit einheitlichen Geschäftsvorfällen, die in den folgenden Kapiteln vorgestellt werden. Zusätzlich gibt es eine ganze Reihe von verbandsspezifischen Geschäftsvorfällen, die aber den Rahmen dieser Darstellung sprengen würden.

4.1 Zahlungsverkehr Inland

4.1.1 Einzelaufträge

Einzelaufträge für den Zahlungsverkehr Inland sind als FinTS-Eigenformat angelegt, um mit einem Grundformat alle betroffenen Geschäftsarten abwickeln zu können. Die Kontoverbindungen für Auftraggeber und Empfänger sind als standardisierte Datenelementgruppen definiert. Parameter, wie z.B. die Anzahl der Verwendungszweckzeilen sind über die BPD pro Institut einstellbar. Aufbauend auf diesem FinTS-Grundformat für Einzelaufträge im Inlandszahlungsverkehr werden z. B. für die Abwicklung von Daueraufträgen spezifische Erweiterungen vorgenommen.

Folgende Geschäftsarten fallen unter die Rubrik „Einzelaufträge“:

Einzelüberweisung	
Sonderformen der Einzelüberweisung	Spendenzahlungen
	Überweisung mit prüfziffergesicherten Zuordnungsdaten (BZÜ)
	Umbuchung auf ein Konto beim gleichen Institut
	Eilüberweisung
	Garantierte Überweisung
Terminierte Überweisung	Einreichen terminierter Überweisungen
	Ändern terminierter Überweisungen
	Bestand terminierter Überweisungen abrufen
	Löschen terminierter Überweisungen
Daueraufträge	Dauerauftragseinrichtung
	Dauerauftragsänderung
	Dauerauftragsaussetzung
	Dauerauftragsbestand abrufen
	Dauerauftragsänderungsvormerkungen abrufen
	Dauerauftragslöschung
Vorbereitete	Vorbereitete Überweisung anlegen

Überweisung	
	Vorbereitete Überweisung ändern
	Bestand vorbereiteter Überweisungen anzeigen
	Vorbereitete Überweisung löschen
Eingereichte Aufträge	Eingereichte Aufträge anzeigen
Einzellastschrift	
Lastschriftwiderspruch	

4.2 Sammelaufträge

4.2.1 Sammelüberweisung und Sammellastschrift

Für die Sammelüberweisung und -lastschrift wird das DTAUS-Format verwendet und somit transparent in FinTS eingestellt. Grund dafür sind die nach geschalteten, bereits vorhandenen Verarbeitungssysteme bei den Kreditinstituten, die Aufträge über FinTS gleich denen von anderen Quellen behandeln (z. B. DTA Datenträger-Einreichung).

Sammelüberweisungen sind ein typisches Beispiel für *asynchrone* Aufträge, die ab FinTS V4.0 elegant mit Datagrammen abgewickelt werden können. Hier ist es - gerade bei größeren Datenmengen - sinnvoll, die Nachricht entgegenzunehmen, zu bestätigen und anschließend die Verbindung zu beenden. Der Verarbeitungsfortschritt kann über den Abruf des *Statusprotokolls* verfolgt werden.

4.2.2 Terminierte Sammelüberweisung und Sammellastschrift

Seit FinTS V3.0 gibt es auch die Geschäftsvorfälle für die terminierte Sammelüberweisung und Sammellastschrift. Die Erweiterung besteht in der zusätzlichen Angabe eines Ausführungsdatums in Feld A 11b des DTA-Satzes.

Auch die Möglichkeit der Eilüberweisung (Sammel) besteht.

4.3 Umsatzinformationen

4.3.1 Abruf von Kontoumsätzen

Die Anforderung von Umsätzen erfolgt über einen *Abholauftrag*. Als Antwort werden über S.W.I.F.T. MT940- und MT942-Formate gebuchte respektive noch nicht verbuchte Umsätze gesendet. Bei der Übertragung umfangreicher Umsatzdaten ist die Verwendung des Datenelementes *Aufsetzpunkt* sinnvoll. Darüber wird dem Kundensystem bei großen Datenmengen mitgeteilt, welchen Aufsetzpunkt es bei einem weiteren Abholauftrag mitliefern soll, um lückenlos die nächsten Umsätze zu erhalten. Über ein Feld *Maximale Anzahl* kann die Ausgabe im Umfang eingeschränkt werden, so dass Endgeräte mit eingeschränkten Darstellungsmöglichkeiten (z. B. Mobiltelefone) nicht mit Daten „überschwemmt“ werden.

□ **Kontoumsätze / Zeitraum**

Dies ist die klassische Umsatzabfrage mit der Möglichkeit, den Abfragezeitraum entsprechend einzugrenzen.

□ **Kontoumsätze / neue Umsätze**

Mit dieser Geschäftsart wird die doppelte Übertragung von Umsatzdaten vermieden, was z. B. für Finanz-Management-Software von entscheidendem Vorteil ist.

□ **Kontoauszug**

Im Unterschied zur Übermittlung von Umsätzen stellt der Geschäftsvorfall „Kontoauszug“ eine echte Ablösung des Papierauszuges dar. Das heißt, dass nach erfolgreichem Abholen der Auszüge diese nicht mehr für eine nochmalige Übertragung zur Verfügung stehen.

Jahrelang wurden die rechtlichen Rahmenbedingungen für den elektronischen Kontoauszug definiert. Deren Beschreibung ist nicht in der FinTS-Spezifikation enthalten. Auch die Anerkennung der elektronischen Kontoauszüge durch die Finanzbehörden ist teilweise noch in Klärung.

Es ist aber zu erwarten, dass dieser Geschäftsvorfall in den nächsten Jahren im Privatkundengeschäft die Verteilung von Kontoauszügen revolutionieren wird.

□ **Kontoinformationen**

Bei diesem Geschäftsvorfall werden alle allgemeinen Stamm- und Vertragsdaten für eines oder mehrere Konten übertragen.

4.3.2 Saldenabfrage

Die Saldenabfrage wird über ein FinTS-Eigenformat abgewickelt. Es werden gängige Saldenwerte zur Verfügung gestellt und optional auch Informationen über Kreditlimite geliefert. Die Saldenabfrage ist ein Prototyp für einen so genannten *Abholauftrag*. Bei der Saldenabfrage sind als Informationen entweder eine Kontonummer oder aber die Information „alle Konten“ einzustellen. Bei dem zweiten Suchbegriff werden die Salden aller vorhandenen Konten zurückgemeldet.

4.4 Termineinlagen

Derzeit sind nur Festgeldanlagen vorgesehen; die Anlage von Kündigungsgeldern ist nicht möglich. Termineinlagen sind FinTS -Eigenformate, die wiederum auf einem gemeinsam verwendeten Grundmodell aufbauen.

- Festgeldkonditionen
- Festgeldneuanlage
- Festgeldänderung
- Festgeldprolongation
- Festgeldbestandsabfrage
- Widerruf einer Festgeldneuanlage
- Widerruf einer Festgeldprolongation

4.5 Wertpapiere

Generell werden für das Wertpapiergeschäft S.W.I.F.T. Formate zugrunde gelegt, um eine automatisierte Weiterverarbeitung zu ermöglichen.

4.5.1 Wertpapierorder

Hierfür kommt das S.W.I.F.T. Format MT502 zum Einsatz.

Vor der Ordereinreichung kann sich der Kunde durch Abholen von *wichtigen Informationen* Hintergrundwissen zu der geplanten Transaktion aneignen. Unterschieden wird hierbei zwischen allgemeinen wichtigen Informationen des Kreditinstitutes und zwischen Informationen zu bestimmten Wertpapieren.

Eine einmal abgesetzte Order kann nachträglich geändert oder auch gestrichen werden, wenn die Verarbeitung nicht schon zu weit fortgeschritten ist.

Eine spezielle Form der Wertpapierorder sind Festpreisangebote des Kreditinstitutes, bei denen der Kunde anhand von zuvor übermittelten Preisen Wertpapiere zu festen Konditionen erwirbt. Hierzu wurde ein eigener Geschäftsvorfall **Festpreisorder** eingeführt.

Fondsorder

Aufgrund der wachsenden Bedeutung des Fondsgeschäftes wurde der Fondsorder ein eigener Geschäftsvorfall gewidmet, der einen Extrakt der allgemeinen Wertpapierorder darstellt und somit einfacher zu verarbeiten ist.

Neuemissionen

Auch für das Geschäftsfeld der Neuemissionen sind in FinTS zwei Geschäftsvorfälle enthalten. Mit „Neuemissionen anzeigen“ kann eine Liste der aktuell verfügbaren Neuemissionen übertragen werden, die alle relevanten Informationen über geplante Emissionen enthält. Mit „Neuemission zeichnen“ können die entsprechenden Papiere gezeichnet werden.

4.5.2 Statusinformationen

Zur Abfrage des Orderstatus werden die S.W.I.F.T. Formate MT 502 (Umsatzanzeige), MT 513 (Ausführungsanzeige) und MT 515 (Wertpapierabrechnung) verwendet. Der Kunde hat generell die Möglichkeit, sich über alle Aufträge für seine Depots zu informieren. Es bestehen zahlreiche Funktionalitäten zur Eingrenzung des Statusabrufs.

Als Spezialfall ist auch die Abfrage einer *Wertpapierorderhistorie* möglich, da zwischen Beauftragung und Ausführung zum Teil mehrere Transaktionen erfolgt sein können.

4.5.3 Depotinformationen

Die Depotinformationen werden über die SWIFT-Formate MT 535 (Depotauszug) und MT 536 (Depotumsätze) übermittelt.

4.5.4 Wertpapierinformationen

Unter diesem Kapitel sind folgende Informationsquellen zusammengefasst:

- Wertpapierstammdaten
- Wertpapierkurse
- Abfrage von Wertpapierinformationen
hierunter sind u. a. Auswertungen und Kursentwicklungen zu verstehen

4.6 Zahlungsverkehr Ausland

Die Einreichung von „Zahlungsaufträgen im Außenwirtschaftsverkehr“ erfolgt im DTAZV-Format. Die Prüfung auf vollständige Datenübertragung erfolgt anhand des Z-Satzes. Die Ausgestaltung des gesamten Bereiches *Auslandszahlungsverkehr* ist hauptsächlich Aufgabe des Kundenproduktes, nicht der FinTS-Schnittstelle. So kann eine Kundensoftware durch entsprechende Belegung von nur einigen relevanten Feldern des DTAZV-Formates eine *Euroüberweisung* abbilden. Genauso ist das Kundensystem aber verantwortlich, den Kunden auf eine ggf. bestehende Meldepflicht hinzuweisen. Die FinTS-Spezifikation enthält hierzu einige relevante Hinweise.

Unter bestimmten Voraussetzungen kann eine Auslandsüberweisung auch ohne Bundesbankmeldung abgewickelt werden. Hierzu ist der Geschäftsvorfall „Auslandsüberweisung ohne Meldeteil“ geeignet. Dieser in FinTS-Syntax aufgebaute Geschäftsvorfall vereinfacht die Einreichung von Zahlungsaufträgen in bestimmte vorgegebene Länder bis zu einem länderabhängigen Höchstbetrag erheblich.

Wenn die Überweisung innerhalb der Mitgliedsstaaten der Europäischen Union erfolgt, 12.500 Euro nicht überschreitet und außerdem der Empfänger per IBAN und BIC identifiziert werden kann, so stellt der neue Geschäftsvorfall „Euro STP-Zahlung“ die beste Alternative dar. STP steht hier für „Straight Through Processing“ was bedeutet, dass dieser Zahlungsauftrag alle geforderten Kriterien für eine vollautomatische Verarbeitung erfüllt. Ist dies nämlich der Fall, so fallen für die Ausführung eines solchen Auftrages geringere Gebühren an – seit Mitte 2003 dürfen diese die Gebühren für Inlandszahlungen nicht überschreiten. Die Grundlage für diesen Geschäftsvorfall bildet das DTAZV-Format mit den entsprechenden Belegungsregeln für STP-Fähigkeit.

4.7 Karten, Schecks und Formulare

Vordruckbestellung

In diesem Kapitel sind alle Arten von Formularbestellungen hinterlegt, die natürlich von Bank zu Bank sehr unterschiedlich sind. Deshalb wird die BPD hier dafür verwendet, dem Kundenprodukt die verfügbaren Formulare zu übermitteln. Da dieser Bereich bisher nicht standardisiert war, wird ein FinTS-Eigenformat verwendet. In der Spezifikation wird explizit darauf hingewiesen, dass unter anderem der Bereich des postalischen Versendens in Zukunft durch neue FinTS-Geschäftsvorfälle abgelöst werden soll.

Folgende Formulararten sind gängig:

- Überweisungs-, Lastschrift- und Dauerauftragsformulare
- Zahlungsverkehrsvordrucke und Schecks

Kartenanzeige

Über diesen Geschäftsvorfall können alle relevanten Daten über an einen Benutzer ausgegebene Karten angezeigt werden.

Kartensperre

Durch diesen Geschäftsvorfall kann eine spezielle Karte online gesperrt werden, wenn das Kreditinstitut dies automatisch unterstützt. Evtl. fehlende Kartendaten können durch den oben beschriebenen Geschäftsvorfall „Kartenanzeige“ abgefragt werden.

4.8 Sorten, Devisen und Reiseschecks

Devisenkurse

Es werden die verfügbaren aktuellen Devisenkurse übertragen.

Sorten- und Reisescheck-Konditionen anfordern

Es werden alle für eine anschließende Bestellung relevanten Informationen und Konditionen übertragen.

Sorten- und Reisescheckbestellung

Auf Basis der zuvor angeforderten Konditionen können online Sorten- und Reiseschecks bestellt werden. Die Auslieferung erfolgt auf dem Postweg.

4.9 Informationen

Ähnlich der Vordruckbestellung ist auch der Bereich des Informationsaustausches bisher nicht standardisiert und wird deshalb über ein FinTS-Eigenformat abgewickelt.

4.9.1 Freitextmeldungen

□ Kundenmeldungen

In einer Kundenfreitextmeldung, die signiert sein muss, können auch Aufträge an das Kreditinstitut übermittelt werden. Dies gilt hauptsächlich für die Geschäftsarten, die in FinTS noch nicht standardisiert sind. Allerdings wird darauf hingewiesen, dass es sich hierbei nicht um zeitkritische Geschäftsarten (z. B. Wertpapierorder) handeln sollte. Dem gemäß ist die Kreditinstitutsantwort auch sehr informell gehalten und bestätigt lediglich den Erhalt der Meldung.

□ Gastmeldungen

Auch über den anonymen Zugang können Freitextmeldungen eingereicht werden. Da diese jedoch nicht signiert werden können, steht der Informationscharakter im Vordergrund.

4.9.2 Formatierte Meldungen

Bei formatierten Meldungen handelt es sich naturgemäß ebenfalls um FinTS-Eigenformate.

□ **Kreditinstitutsangebote abholen / Informationsbestellung**

Hierüber kann ein Kreditinstitut dem Kunden eine Übersicht über vorhandenes Informationsmaterial zur Verfügung stellen. Vom Vorgehen her wird zunächst mit diesem Geschäftsvorfall eine Liste der verfügbaren Informationen übermittelt, aus welcher der Kunde dann per Code auswählen kann.

Der Code wird als Geschäftsvorfall *Informationsbestellung* an das Kreditinstitut übermittelt. Die Auslieferung erfolgt derzeit auf dem Postweg.

□ **Terminvereinbarung**

Mit dieser Geschäftsart kann der Kunde auf strukturierte Weise einen Terminwunsch äußern. Dieser ist jedoch, wie bei den anderen Informationsangeboten, nicht verbindlich und bedarf derzeit der schriftlichen oder fernmündlichen Bestätigung.

4.10 Sonstiges

4.10.1 Freistellung von Zinserträgen

Es können Daten bzgl. der von der Zinsabschlagsteuer freigestellten Beträge abgefragt werden.

4.10.2 Transfer von beliebigen Dokumenten

Mit Hilfe dieser Geschäftsvorfälle ist es möglich, beliebige Dokumente über den gesicherten FinTS-Weg zu senden und zu empfangen. Dies können zum nicht in FinTS spezifizierte SWIFT-Formate (z. B. MT100) sein, aber auch jede andere Art von Dokumenten. Die vom Institut unterstützten Dokumentenformate werden über die BPD mitgeteilt. Folgende Geschäftsvorfälle sind vorgesehen:

Dokument senden

Der Kunde kann über diesen Weg ein unterstütztes Dokument einreichen.

Bearbeitungsstatus über Dokument anfordern

Ähnlich dem Statusprotokoll kann der Kunde den Verarbeitungsstatus eines Dokumentes abfragen.

Liste der bereitgestellten Dokumente anfordern

Der Kunde erhält eine Liste der für ihn bereitgestellten Dokumente.

Dokument anfordern

Der Kunde kann aus der bereitgestellten Liste ein Dokument abholen.

4.10.3 GeldKarten-Transaktionen



Das Laden der GeldKarte steht seit FinTS V3.0 zur Verfügung. Diese Funktion wurde auf Messen bereits mehrfach prototypisch gezeigt - jedoch mussten die sicherheitstechnischen Rahmenbedingungen erst verbindlich definiert werden.

4.10.3.1 An- und Abmeldung einer Geldkarte

Vor Einleiten des Ladevorganges muss die zu verwendende Geldkarte erst beim Banksystem bekannt gemacht werden. Dieses Registrieren – sowie auch ein Abmelden einer Karte – kann mit FinTS-Geschäftsvorfällen geschehen.

4.10.3.2 Laden der GeldKarte

Die Ladetransaktion besteht aus vier fest definierten Schritten, die in vorgegebener Reihenfolge ablaufen müssen.

□ Vorbereiten

Das Vorbereiten läuft in einem HBCI-gesicherten Dialog ab. Der Ladebetrag wird in diesem Schritt durch eine entsprechende bankseitige Verarbeitung „für das Laden bereitgestellt“. Ob dies eine Kontodisposition oder ähnliches ist, befindet sich nicht im Scope von FinTS.

Aus Sicht der ZKA-Spezifikation für das Laden der GeldKarte handelt es sich um „Laden gegen andere Zahlungsmittel“, was auch ermöglicht, die GeldKarte ohne Eingabe der ec-PIN zu laden.

□ Ladevorgang

Die Funktionen *Laden Einleiten*, *Durchführen* und *Bestätigen* sind in der ZKA-Spezifikation zum Laden der GeldKarte festgelegt. Dieser Datenaustausch zwischen GeldKarte, Ladeterminal und Ladezentrale geschieht aus Sicht von FinTS in einem anonymen Dialog, d. h. es findet ein Wechsel des Sicherheitsverfahrens statt, der ggf. auch von einem Kartenwechsel (z. B. RDH-Chipkarte entfernen – GeldKarte einlegen) begleitet ist.

4.10.3.2.1 Laden GeldKarte Status

Über diese in der ZKA-Spezifikation zum Laden der GeldKarte beschriebene Statusabfrage kann nachgeprüft werden, ob der Ladevorgang erfolgreich war.

4.10.3.2.2 Laden GeldKarte Storno

Sollte ein Ladevorgang nicht erfolgreich abgeschlossen worden sein, so kann auf diesem Wege ein Storno des Ladebetrages veranlasst werden. Durch die in der Geldkartenspezifikation beschriebenen Schritte *Storno Vorbereiten*, *Durchführen* und *Bestätigen* kann diese Funktion über FinTS abgewickelt werden.

4.10.4 Empfangsquittung

Die Empfangsquittung wird z. B. im Rahmen des elektronischen Kontoauszugs verwendet, um den Erhalt der Auszugsdaten verbindlich zu bestätigen. Dies entspricht dem Entnehmen des Papierauszugs aus dem Auszugsschacht des Kontoauszugsdruckers.

Dieser Geschäftsvorfall kann jedoch generell eingesetzt werden, wenn eine explizite Bestätigung erforderlich ist.

4.11 Ausblick - Weitere Geschäftsvorfälle in Planung

Der FinTS Band zur Beschreibung der Geschäftsvorfälle hat sich inzwischen zu einem umfangreichen Werk entwickelt. Zusätzlich bestehen noch verbands-spezifische Geschäftsvorfälle, die von den entsprechenden Bankengruppen angeboten werden.

Das Geschäftsvorfallsprinzip hat sich in den letzten Jahren gut etabliert, so dass zum einen alle multibankfähig relevanten Geschäftsvorfälle spezifiziert sind oder bei Bedarf kurzfristig nachgeliefert werden, zum anderen auch individuelle Ausprägungen auf der gleichen Infrastruktur angeboten werden.

Dynamisiert wird dieses Konzept zukünftig noch dadurch werden, dass Geschäftsvorfälle unabhängig von FinTS-Releases veröffentlicht werden sollen. Diese künstlich festgelegte Verbindung zwischen HBCI-Version und Geschäftsvorfall ist seit FinTS V3.0 offiziell aufgehoben. Damit ist es z. B. möglich, dass neue Geschäftsvorfälle auch unter älteren FinTS-Versionen angeboten werden oder aber, dass ältere Geschäftsvorfallversionen unter neuen FinTS-Versionen zum Einsatz kommen.

5 Transportmedienspezifische Festlegungen

In den vorangegangenen Kapiteln wurden zahlreiche Aspekte beleuchtet, welche die Flexibilität des FinTS Standards herausstellten. In diesem Kapitel ist der Ansatz genau umgekehrt. In Richtung Transportprotokolle hat FinTS das Ziel, möglichst genau und restriktiv die einzelnen Zugangsvarianten festzulegen, damit zwei willkürlich zusammentreffende Kommunikationspartner ohne große Abstimmungsprozesse sofort miteinander kommunizieren können. Dabei muss man wieder zwischen HBCI / FinTS V3.0 und FinTS V4.0 unterscheiden

5.1 Transportverfahren bis einschließlich FinTS V3.0

Definiert sind in FinTS V3.0 folgende Kommunikationsprotokolle

- T-Online Classic
- TCP/IP über Port 3000
- https für das Sicherheitsverfahren PIN/TAN (ab FinTS V3.0)

5.1.1 T-Online Classic mit ETSI 300 072 ("CEPT") / EHKP / BtxFIF

Dieser Kommunikationsweg ist nur noch aus historischen Gründen in FinTS V3.0 enthalten. Die meisten Rechenzentren bieten diesen optionalen Zugang nicht bzw. nicht mehr an, da jeder T-Online-Nutzer die Möglichkeit hat, auch mittels Internet über Port 3000 mit dem Rechenzentrum zu kommunizieren.

Bei dieser Kommunikationsart werden CEPT und EHKP lediglich als Transportrahmen für transparente Daten benutzt, welche die eigentlichen FinTS-Informationen enthalten. Da es in EHKP eine Restriktion aufgrund der maximalen Dialogfeldgröße von ca. 1600 Byte gibt, wurde das „Btx File Interchange Format (BtxFIF)“ als Chaining-Protokoll herangezogen, um beliebig große FinTS-Nachrichten austauschen zu können. Innerhalb dieses Kapitels sind bezüglich CEPT, EHKP und BtxFIF alle Parameter definiert, um so den Kommunikationsweg eindeutig zu beschreiben. Auf gewisse optionale Funktionen des BtxFIF, wie z. B. Restartfähigkeit wurde aus Rücksicht auf einfacher gestaltete Kundensysteme bewusst verzichtet.

5.1.2 TCP/IP

TCP/IP ist, wie der Name schon sagt, **das** Internet Protokoll. Hier sind klassische PPP-Zugänge unterstützt. Als Schnittstelle zur Anwendung dient die TCP Socket-Schnittstelle (Streamsocket), bestehend aus IP-Adresse und Port-Nummer (als FinTS Port-Nummer wurde "3000" beim entsprechenden Internet Committee registriert). Wichtig ist an dieser Stelle anzumerken, dass auch in FinTS V3.0 für das Sicherheitsverfahren HBCI nur die TCP-Transportschnittstelle spezifiziert ist, jedoch nicht die darüber liegenden Session- und Präsentationsschichten. Dies hat unter anderem den Grund, dass für die Erzeugung eines FinTS-Datenstromes, sei es über fest installierte Programme oder z. B. auf der Basis von Java-Applets, ohnehin Intelligenz im Endgerät vorhanden sein muss. Mit diesen Mitteln kann dann ohne weiteres eine Kommunikation über TCP Port 3000 aufgebaut werden, um FinTS-Nachrichten zu übermitteln. Dadurch erspart man sich zum einen den für die

Nettodatenübertragung unnötigen http-Overhead und kann zum anderen den Server-Prozess für Port 3000 auf der Kreditinstitutsseite speziell absichern.

Als nachteilig hat sich herausgestellt, dass die Nutzung des Port 3000 bei der Verwendung von FinTS über Firmen- oder Universitätsnetze ein Problem darstellt, da dieser Port in den meisten Firewalls nicht durchgelassen wird. Dies wird mit FinTS V4.0 durch die Definition eines https-Zugangs auch für HBCI-Sicherheit gelöst.

5.1.3 https mit PIN/TAN-Sicherheit

Da für das Sicherheitsverfahren PIN/TAN nur ein Standard-Browser ohne zusätzliche Programmteile Voraussetzung ist und man durch die fehlenden Kryptoalgorithmen auf Transportsicherungsverfahren angewiesen ist, wurde – zunächst – für diesen Spezialfall http mit SSL als Kommunikationsverfahren definiert.

Es gibt außer der Benennung der Protokolle keine weiteren Festlegungen.

5.2 Transportverfahren mit FinTS V4.0

F_{inTS V4.0} Im Rahmen der kompletten Neuausrichtung mit FinTS V4.0 ist auch der Bereich der Transportprotokolle stark betroffen. T-Online Classic und TCP/IP Port 3000 sind in der Spezifikation nicht mehr enthalten. Als synchrones Protokoll hält http / https auf breiter Basis Einzug. Dies ist bei der mit FinTS V4.0 verfolgten Zielsetzung der Erhöhung des Standardisierungsgrades nicht weiter verwunderlich.

Für die asynchronen Verfahren erscheint SMTP neu in der Liste der unterstützten Verfahren. Diesem Protokoll kommt im Zusammenhang mit Datagrammen und Publish/Subscribe Services per E-Mail ebenfalls eine wichtige Rolle zu.

5.2.1 Webservices und SOAP

Zusätzlich zu der reinen http-Welt besitzt FinTS V4.0 auch ein Kapitel über die Integration in Webservices. Diese neuen und noch nicht als stabil zu bezeichnenden Standards werden zukünftig auch bei FinTS stärker Einzug halten. Heute sind bereits die geeigneten Integrationsmöglichkeiten in SOAP und WSDL beschrieben – Beispieldefinitionen runden das Thema ab.

5.3 Chipkartenanwendungen

5.3.1 DDV-Chipkarten Typ-0 und Typ-1



Beim symmetrischen Verfahren kommt die Chipkarte gemäß ZKA-Spezifikation zum Einsatz. Diese arbeitet mit demselben Betriebssystem wie die ec-Chipkarte, die auch für die elektronische Geldbörse (GeldKarte) verwendet wird. Die Homebanking-Erweiterung auf dieser Chipkarte besteht nur aus einigen zusätzlichen Feldern (keine speziellen Kommandos!) für die Abbildung folgender Informationen:

- Eigene *Banking-PIN*, die getrennt von der generellen ec-PIN zu sehen und in Zukunft auch änderbar sein wird.
- kundenindividueller *Signier- und Chiffrierschlüssel*

- Feld für den *Sequenzzähler* für die Doppeleinreichungskontrolle von Aufträgen
- mehrere (bis zu 5) Bankverbindungen mit folgendem Aufbau:
 - Kurzbezeichnung der Bank
 - Bankleitzahl und Benutzerkennung
 - Zugangskennung (IP-Adresse/URL bzw. T-Online-Gatewayseitennummer)

Dieser Aufbau zeigt, dass die Karte erstens multibankfähige Informationen enthält und zweitens über die unterschiedlichen Zugangsdaten auch für den mobilen Einsatz geeignet ist.

Seit dem 4. Quartal 2000 werden Karten einer neuen Betriebssystemgeneration (Typ-1) ausgegeben. Hierfür wurde die FinTS Chipkartenapplikation entsprechend angepasst und im Anhang der Spezifikation dokumentiert.

5.3.2 ZKA Banken-Signaturkarte mit SECCOS-Betriebssystem



Bei der mit FinTS V3.0 neu eingeführten Banken-Signaturkarte kommt die Chipkarte gemäß ZKA-Spezifikation auf Basis des SECCOS-Betriebssystems zum Einsatz (s. Kap. 3.2.1). Für die Signaturprozesse wird die anwendungsübergreifend spezifizierte **Signatur-Anwendung** zum Einsatz gebracht. Die Homebanking-Erweiterung auf dieser Chipkarte besteht nur aus einigen zusätzlichen Feldern (keine speziellen Kommandos!) für die Abbildung folgender Informationen:

- Authentisierungs-Passwort und Signatur-PIN für den Zugriff auf die entsprechenden RSA-Schlüsselpaare
- kundenindividuelles Schlüsselpaar für *Authentisierung, Signaturbildung und Verschlüsselung*
- standardmäßig vorhandene *Sequenzzähler* pro Schlüsselpaar für die Doppeleinreichungskontrolle von Nachrichten.

Die Online-Banking-Erweiterung auf der Banken-Signaturkarte besteht nur aus einer – ebenfalls standardmäßig nutzbaren – Struktur EF_NOTEPAD für die Speicherung der Zugangsdaten für mehrere Institute.

6 FinTS-Kundensysteme

Generell gibt es verschiedene Arten von Kunden-Endgeräten, die für einen Betrieb mit FinTS in Frage kommen.

Bevor diese jedoch einzeln betrachtet werden, folgt hier zunächst die Einordnung von FinTS-Kundensystemlösungen unter dem Gesichtspunkt der Infrastruktursicherheit.

6.1 Infrastruktur-Sicherheit

Kritische Berichte zum Thema Online-Banking im Internet verwirren in rascher Folge die Verbraucher. Eines ist diesen gezeigten Angriffen gemeinsam: jedes Szenario setzt eine böswillige „Verunreinigung“ des Systems durch Viren, trojanische Pferde oder sonstige Unarten voraus. Diese Gefahren sind real und sollen hier nicht bagatellisiert werden. Und genauso real ist die Tatsache, dass auch FinTS gegen diese Art von Angriffen nicht geschützt ist. Denn was nützt es, wenn ein Hashwert in der Chipkarte signiert wird, wenn dieser schon gar nicht mehr der Anzeige auf dem Bildschirm entspricht? Die eigentliche Frage ist jedoch die der Beweislast. Denn wenn auf diese Weise Missbrauch betrieben wird, ist derzeit in den meisten Fällen der Kunde für den Schaden haftbar.

Dies wird sich in der nächsten Zeit wahrscheinlich relativieren. Denn gerade seit FinTS V3.0 besteht z. B. durch Einsatz der Banken-Signaturkarte in Verbindung mit einem höherwertigeren Chipkartenleser mit eigener Tastatur und ggf. eigenem Display die Möglichkeit, die relevanten Daten außerhalb des Betriebssystems zu signieren.

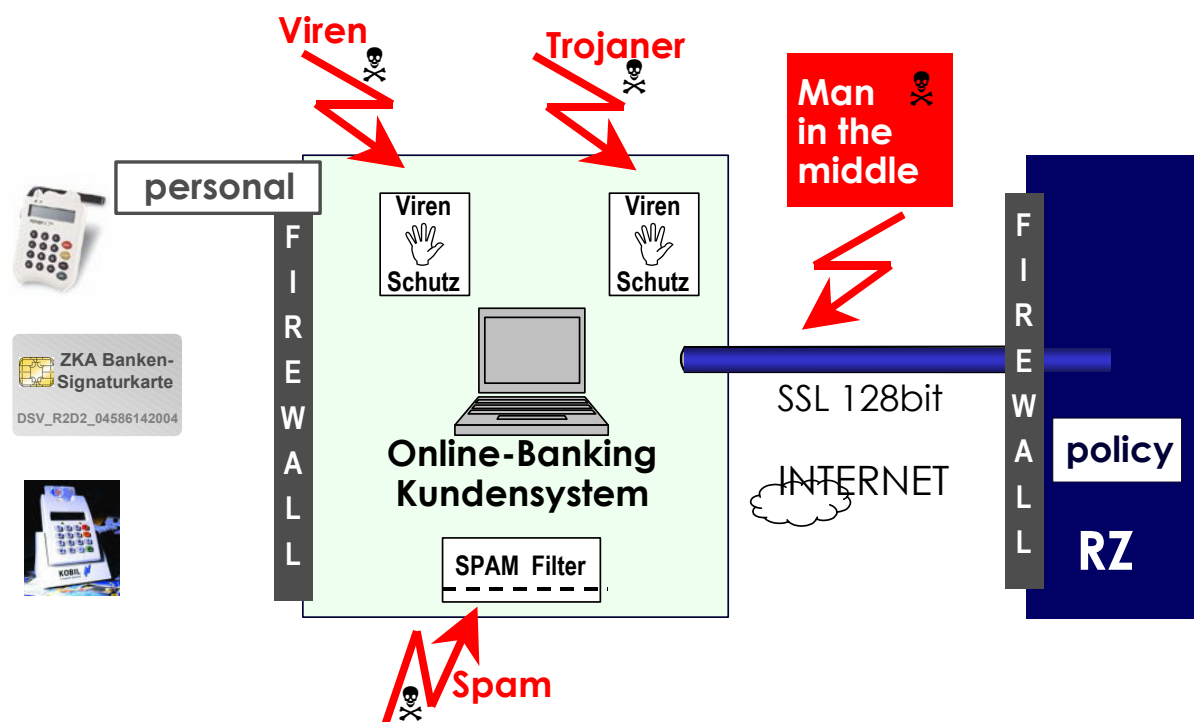


Abbildung 13: Der Online-Banking PC als Ziel unterschiedlichster Angriffe

Derzeit ist leider gegen diese Angriffe kein 100% wirksamer Schutz vorhanden. Doch kann man – wenn man den Empfehlungen der Institute und auch des BSI (Bundesamt für Sicherheit in der Informationstechnik, www.bsi.de) folgt, durch Kombination von Virenschutz, Firewall, Chipkarte und Chipkartenleser mit integrierter Tastatur sowie entsprechenden Sorgfaltspflichten die Hürde für Angriffe sehr hoch legen.

Nach diesen Vorbemerkungen nun also zu der Typisierung der Kundensysteme.

6.2 Typisierung der FinTS Kundensysteme

6.2.1 Finanz-Management-Software

Eine Klasse unterstützter Endgeräte stellen spezielle Finanz-Management-Programme dar, wie sie seit Jahren auf dem Markt sind. FinTS bringt für diese Art von Endgeräten aber entscheidende Vorteile:

- effektive und schnelle Nettodatenübertragung
- Unabhängigkeit vom Transportdienst
- Unabhängigkeit vom Sicherheitsverfahren
- automatische Konfigurierbarkeit mit Hilfe von UPD und BPD
- mehr Komfort in puncto Sicherheit
- erhöhte Betriebssicherheit durch intelligente Auswertung der FinTS-Rückmeldungen und Statusprotokolle
- neue Geschäftsvorfälle, welche die Kreativität der KundenproduktHersteller herausfordern
- Multibankfähigkeit
- keine Probleme mehr bei der Pflege der Bankzugänge

Die Liste ließe sich noch erweitern, doch die Hauptaspekte von FinTS sind sicherlich erkennbar. Zu erwähnen ist dabei noch, dass auch einige Bankengruppen verstärkt Produkte mit eigenem Funktionsumfang und eigener Darstellung am Markt etabliert haben, um FinTS gerade im Marketing- und Servicebereich stärker für ihre Belange nutzen zu können.

Wichtig ist aus Sicht der Kreditinstitute und Rechenzentren, dass durch Einsatz dieser eigenen Kundenprodukte erreicht wird, dass mehr und mehr Kunden über die einheitliche Eingangsschnittstelle FinTS ihre Aufträge einreichen. Somit können als Perspektive andere Zugänge (insbesondere T-Online Classic) mittelfristig eingespart werden.

6.2.2 Browserbasierte Lösungen

Dieser Abschnitt beschreibt einen weiteren Schritt der FinTS-Entwicklung für Kunden mit einem völlig anderen Benutzerverhalten. Denn im Unterschied zu einer zentralen Finanzverwaltung geht es hier um die nahtlose Integration der Abwicklung von Geldgeschäften in ein vorhandenes Werkzeug, das in der Lage sein muss,

innerhalb des Kundensystems FinTS-Nachrichten inklusive der Sicherheitsfunktionen zu erzeugen. Vorteil bei diesem Anwendungsprofil ist die Mobilität und die technische und geographische Unabhängigkeit vom Endgerät, wenngleich der Einsatz von Chipkarten hier (noch) eine gewisse Hürde darstellt. Der Einsatz des FinTS PIN/TAN Verfahrens ist jedoch dabei sich rasch am Markt zu etablieren.

6.2.2.1 FinTS Chipkarten-Clients mit Java / ActiveX

Die aktuelle Browsergeneration hat bereits Produkte hervorgebracht, die in der Lage sind, kryptografische Funktionalität abzudecken und die somit auch als FinTS-Clients in Frage kommen. Verwendet werden je nach Hersteller unterschiedliche Standards, z. B. *Java-Applets*⁶ und *ActiveX-Controls*⁷.

Es gibt dabei grundsätzlich zwei Ansätze:

1. Verwenden einer Voll-HBCI-Implementierung, z. B. unter Verwendung des Java-basierten Banking-Kernels und lokale Speicherung der Programmteile auf Basis der Java Signed Applet Technologie
2. Einsatz von essentiell benötigten Kryptoklassen als Java-Applets / ActiveX-Controls und Verwenden eines Web-Servers für Business Logic und Präsentation

Beide Fälle verfolgen unterschiedliche Einsatzzwecke. Im Szenario 1 ersetzt die Java-Applikation eine Finanz-Management-Anwendung und verwendet das Java-Deployment für Systemmanagement und Softwareverteilung.

Im 2. Szenario entsteht die Light-Version einer Finanzsoftware, deren Einschränkung in Mobilität und Flexibilität in der Unterstützung eines externen Device - Chipkartenleser oder Diskettenlaufwerk - besteht.

6.2.2.2 PIN/TAN-Verfahren mit nativem Browser

Diese Einschränkungen bestehen mit Verwendung des PIN/TAN-Verfahrens nicht. Dort kann es sich um eine komplette WEB-Server Applikation handeln, die keine zu installierenden Teile am Endgerät erfordert.

6.2.3 Mobile Banking

Beim Begriff "Online-Banking" wird generell die Verwendung eines PC oder Internet-Browsers impliziert. Es existieren inzwischen Lösungen am Markt, welche zumindest Kontostandsabfragen und Umsatzanzeigen, teils auch Überweisungen und Wertpapiertransaktionen, auf Mobiltelefonen anbieten.

6.2.3.1 Mobiltelefone

In Verbindung mit dem ersten WAP Hype entstanden auch Banking-Lösungen auf Basis der damaligen Endgerätegeneration. Diese Anwendungen erlitten das gleiche Schicksal wie alle WAP-Anwendungen: sie waren zu unkomfortabel, zu langsam und zu teuer. Mit GPRS, UMTS und WAP V2.0 entstehen neue Möglichkeiten für die

⁶ Java ist ein Warenzeichen der Sun Microsystems GmbH

⁷ ActiveX ist ein Warenzeichen der Microsoft Corporation

Abbildung von Online-Banking auf mobilen Endgeräten. Es bleibt abzuwarten, ob dieser zweite Anlauf dem mBanking zu mehr Attraktivität verhilft, doch in jedem Fall lassen sich technisch zwei Ansätze unterscheiden:

- Browserbasierte Anwendungen mit WAP V1.x
- SMS-basierte Anwendungen

Die WAP-Anwendungen – auch die der neuen Generation – sind als Browser-Applikationen zu betrachten. Daher kommt im Normalfall das PIN/TAN-Verfahren zum Einsatz. Nach Abwicklung der gerätespezifischen Präsentation werden Daten extrahiert und können dann im Rechenzentrum über die FinTS-Schnittstelle eingereicht werden. FinTS spielt hier also primär eine RZ-organisatorische Rolle. Die im Zusammenhang mit WAP definierte Transport Layer Security (TLS) sorgt für die Verschlüsselung der Daten. Das restliche Verhalten ist vergleichbar mit der Umsetzung im Internet-Browser.

SMS-basierte Applikationen verhalten sich anders. Hier ist keine Transportsicherheit integriert. Obwohl einige Anbieter auf die sichere „Luft-Übertragung“ vertrauen, sind solche Lösungen aus Sicherheitsicht nicht ideal. Abhilfe können hier Verfahren schaffen, die z. B. im Rahmen einer SIM Toolkit Anwendung eine eigene Verschlüsselung und Authentisierung integrieren und auf dieser sicheren Basis dann SMS-Nachrichten austauschen. Auf diese Weise lassen sich sogar HBCI-ähnliche Signaturen bilden und es kann auf die Eingabe von PIN und TAN verzichtet werden. Der Rest der Verarbeitung geschieht wieder analog zum WAP-Szenario – die Daten werden extrahiert und RZ-intern über die FinTS-Schnittstelle eingereicht.

6.2.3.2 PDA

Das PDA-Szenario ist vom Datenfluss her eine kleine Abwandlung der WAP-Lösung. Anstelle von WML können hier html-basierte Präsentationsstandards wie cHTML verwendet werden.

Eine interessante Variante stellt das Abspeichern von Schlüsseln im PDA-Speicher dar. Bei entsprechend sicherem Speicherdesign kann das PDA-Memory als RDH-Diskette verwendet werden. Es existieren Produkte am Markt, die eine vollständige HBCI-Abwicklung im PDA integriert haben.

6.2.4 Sonstige Kundensysteme

Bei der Beschreibung der Kundensysteme wurde bereits mehrfach angedeutet, dass FinTS als reine Datenschnittstelle verwendet wird. Spinnt man diesen Gedankengang weiter, so kommt man zu einer Multikanal-Lösung, die als gemeinsame Datenschnittstelle FinTS verwendet und andere Protokolle in dieses Standardformat umsetzt. Es würde den Rahmen dieses Kompendiums sprengen, diesen Multikanalansatz zu beschreiben. Doch haben beispielhafte Entwicklungen in den letzten Jahren gezeigt, dass FinTS auch als Basis für Callcenter-Anwendungen, Kiosk-Systeme oder sogar SB-Geräte dienen kann.

Gerade die Einführung des FinTS Baukastensystems und die Öffnung für neue Sicherheitsverfahren und Kommunikationsstandards legt die Vermutung nahe, dass FinTS sich in diese Richtung weiter entwickeln kann.

7 Positionierung im internationalen Umfeld

Zur Abrundung der Beschreibung von FinTS soll an dieser Stelle noch kurz auf vergleichbare Entwicklungen im internationalen Bereich eingegangen werden.

7.1 OFX – Open Financial Exchange



Open Financial Exchange – entstanden aus „OFC“ von Microsoft und „Open Exchange“ von Intuit – ist ein Homebanking-Standard, der auf einer HTML-ähnlichen Tag-Language (ursprünglich SGML, seit Version 2.0 im April 2000 XML) basiert und SSL als Transportsicherheitskomponente verwendet. Für die Authentifikation wird ein Kennwort verwendet, das über zuvor ausgetauschte Zufallszahlen sicher verschlüsselt übertragen wird (Challenge Response Verfahren). Zur Abdeckung der Transaktionssicherheit kommen heute noch vielfach TANs zum Einsatz, Kontextsignaturen sind derzeit nicht vorgesehen. OFX ist fest auf Internet als Transportmedium zugeschnitten. Die definierten Geschäftsvorfälle orientieren sich momentan (Version 2.0.2 vom 22.01.2004) noch stark am amerikanischen Markt. Obwohl der Standard als offen gilt, liegt die Kontrolle bei den Herstellern Microsoft, Intuit und CheckFree. Nach eigenen Angaben verwenden derzeit ca. 2.000 Banken weltweit OFX.
(<http://www.ofx.net>)

7.2 IFX – Interactive Financial Exchange



Bei Erscheinen der beiden konkurrierenden Standards OFX von Microsoft und Gold von IBM wurden bereits Pläne geschmiedet, diese zumindest auf hohem Niveau zusammenzufassen. Dies führte zur Gründung eines Konsortiums unter der Leitung von BITS (besser bekannt unter Bankers Roundtable), dem außer den Herstellern Checkfree, IBM, Intuit, Microsoft und Visa auch zahlreiche namhafte amerikanische und kanadische Banken angehören. Ziel ist die Definition von gemeinsamen Geschäftsvorfällen, die dann jeweils ein Mapping in die entsprechende Zielsyntax erfahren. Eine interessante Entwicklung betreibt IFX derzeit durch Integration namhafter Hersteller im Selbstbedienungsbereich.

Durch diese Workgroup sind in der aktuellen Version auch Messages für den Bereich der SB-Geräte (Sicherheit, MAC, EMV, Cash-Recycling, ...) enthalten. Seit April 2004 existiert die Version 1.0 eines ATM Implementation Guide.

Die IFX-Spezifikation liegt in einer Version 1.5 vom Januar 2004 vor und basiert inzwischen ebenfalls auf XML Schema Technologie.
(<http://www.ifxforum.org>)

7.3 SWIFT XML



Das SWIFT-Konsortium hat bereits seit einigen Jahren mit der Modellierung von Geschäftsvorfällen begonnen mit dem Ziel, die bewährte Welt der FIN-Messages zu abstrahieren und aus dem abstrakten UML-Modell (Unified Modelling Language) beliebige Syntax-Ausprägungen abzuleiten. Aus der Modellierung entsteht ein abstraktes SWIFT Standards Financial Dictionary.

Konkretes Ziel dieser Methodik ist die Entstehung eines SWIFTStandards XML auf Basis von DTD und Schema, der die Verwendung von SWIFT im Internet unterstützen soll. Bei SWIFT werden diese beiden Ausprägungen als FIN-Standards (klassische MT-Formate) und XML-Standards bezeichnet.

Diese Entwicklung geht konform mit dem Aufbau eines IP-basierten SWIFTNet V4.x, welches das klassische SWIFT-Netzwerk ablösen soll.

Zusätzlich plant SWIFT auch, ergänzend zur etablierten B2B-Kommunikation, die Kommunikationsstrecke zum Kunden zu integrieren. Hierzu arbeitet man auch sehr eng mit fpl (FIX⁸ Protocol Limited) zusammen und ist bestrebt, auf Basis von ISO 20022 XML die beiden Standards zu harmonisieren und somit eine Lösung für die B2C und B2B Kommunikation zu erhalten.

Konkrete Messages im Bereich B2C liegen zur Zeit noch nicht vor, sind aber im Standardisierungsprozess. Es ist abzusehen, dass diese SWIFT-Entwicklung den Bereich des Zahlungsverkehrs stark beeinflussen wird, wenn man sich auf entsprechend attraktive Nachrichtendefinitionen geeinigt hat.

Derzeit aktuell ist der SWIFT Standards Release Guide 2003 vom 14.02.2003 und die FIX Spezifikation 4.4 vom 30.04.2003.

(<http://www.swift.com> und <http://www.fixprotocol.org>)

7.4 ebXML – electronic Business XML



Die EDIFACT Community hat sich bereits sehr früh auf XML als Datenbeschreibungssprache konzentriert. ebXML ist ein Standard, gefördert von UN/CEFACT und OASIS. Der Standard ebXML übernimmt die Rolle von EDIFACT. Die Standardisierung ist fachlich orientiert und nach Branchen geordnet. Für die technische Basis bildet ebXML die Anforderungen in zunehmenden Maß auf Webservices⁹ ab. Zugleich berücksichtigt die Initiative für Webservice verstärkt die ebXML-Anforderungen.

ebXML besteht aus einem Set von Spezifikationen, die über jeweils eigene Versionsführungen verfügen.

(<http://www.ebxml.org>)

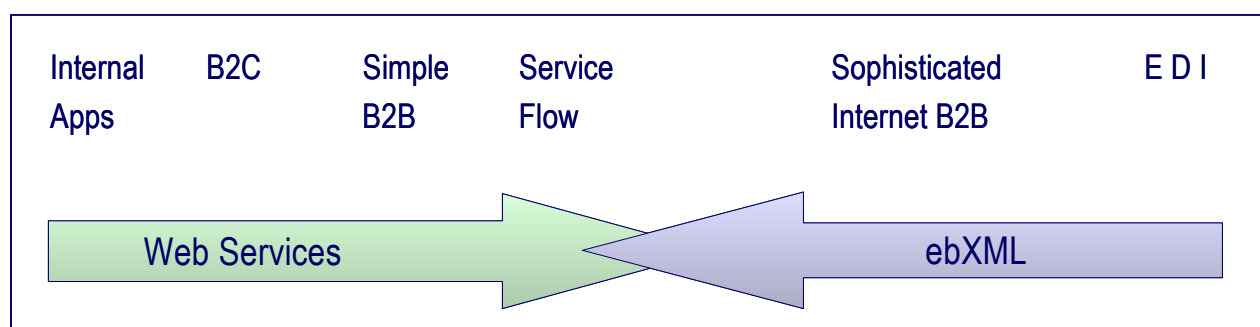


Abbildung 14: Zusammenspiel ebXML und Web-Services

⁸ FIX – Financial Exchange Protocol

⁹ Bei Webservices handelt es sich um eine neue Technologie zur Definition von Services im Internet. Die Standardisierung erfolgt durch das W3C und wird sehr stark durch große Industriepartner wie z. B. IBM und Microsoft geprägt.

7.5 Ausblick

Ziel der deutschen Kreditwirtschaft ist es, FinTS V4.0 als Industriestandard zu etablieren. Die Einführung der Banken-Signaturkarte und die wichtige Integration des Sicherheitsverfahrens PIN/TAN, sowie neue Funktionalitäten wie Push-Services, die Integration von Portalen und neue auch Geschäftsvorfälle wie verteilte Signaturen oder die Übertragung von Dateien als Filetransfer kann FinTS V4.0 diesem Ziel sehr viel näher bringen. Entscheidend für den FinTS-Anteil am Online-Banking Geschäft wird dabei sein, inwieweit FinTS außer bei den Kundenprodukten auch in den Browserbanking-Markt eindringen kann.

Ein anderer Aspekt ist das momentan entstehende Signaturlbündnis im Rahmen der Agenda 2010 zur Unterstützung des Einsatzes von Signaturkarten. Hilft dieses Engagement wirklich, den Markt für rechtsgültige Signaturen zu öffnen, kann FinTS im Finanzbereich eine bedeutende Rolle spielen.

Als letztes muss sich FinTS V4.0 als nationaler Standard auch im internationalen, speziell im europäischen Umfeld behaupten. Dies wird mit der XML-basierten Version 4.0 sicherlich leichter geschehen können. Man darf also gespannt sein, wann es FinTS gelingen wird in Europa weiter Fuß zu fassen.