Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

FinTS

Financial Transaction Services

Schnittstellenspezifikation

Hauptdokument

Herausgeber:
Bundesverband deutscher Banken e.V., Berlin
Deutscher Sparkassen- und Giroverband e.V., Bonn/Berlin
Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., Berlin
Bundesverband Öffentlicher Banken Deutschlands e.V., Berlin

Version: 4.1 FV Stand: 23.02.2018 Final Version

Die vorliegende Schnittstellenspezifikation für eine automatisiert nutzbare multibankfähige Banking-Schnittstelle (im Folgenden: Schnittstellenspezifikation) wurde im Auftrag der Deutschen Kreditwirtschaft entwickelt. Sie wird hiermit zur Implementation in Kunden- und Kreditinstitutssysteme freigegeben.

Inhaltsverzeichnis

I. EINLEITUNG

FinTS steht für Financial Transaction Services und ist die Weiterentwicklung des 1996 erstmals von der Deutschen Kreditwirtschaft (DK) veröffentlichten Online-Banking Standards: "Homebanking Computer Interface (HBCI)".

Damals wie heute ist das Ziel dieses Standards die Vereinheitlichung der Schnittstelle zwischen dem Bankkunden - z. B. repräsentiert durch seine Finanzverwaltungs-Software oder mobile App - und einem oder mehreren Kreditinstituten in identischer Weise. Ziel ist dabei die Multibankfähigkeit.

Der Funktionsumfang von FinTS ist seit seiner ersten Veröffentlichung 1995 stark angestiegen, um den Anforderungen des Marktes zu genügen: die dot.com Phase hat mit zahlreichen neuen Geschäftsvorfällen im Wertpapierbereich den Standard entscheidend geprägt, genauso wie die kontinuierliche Verfeinerung der Sicherheitstechnik.

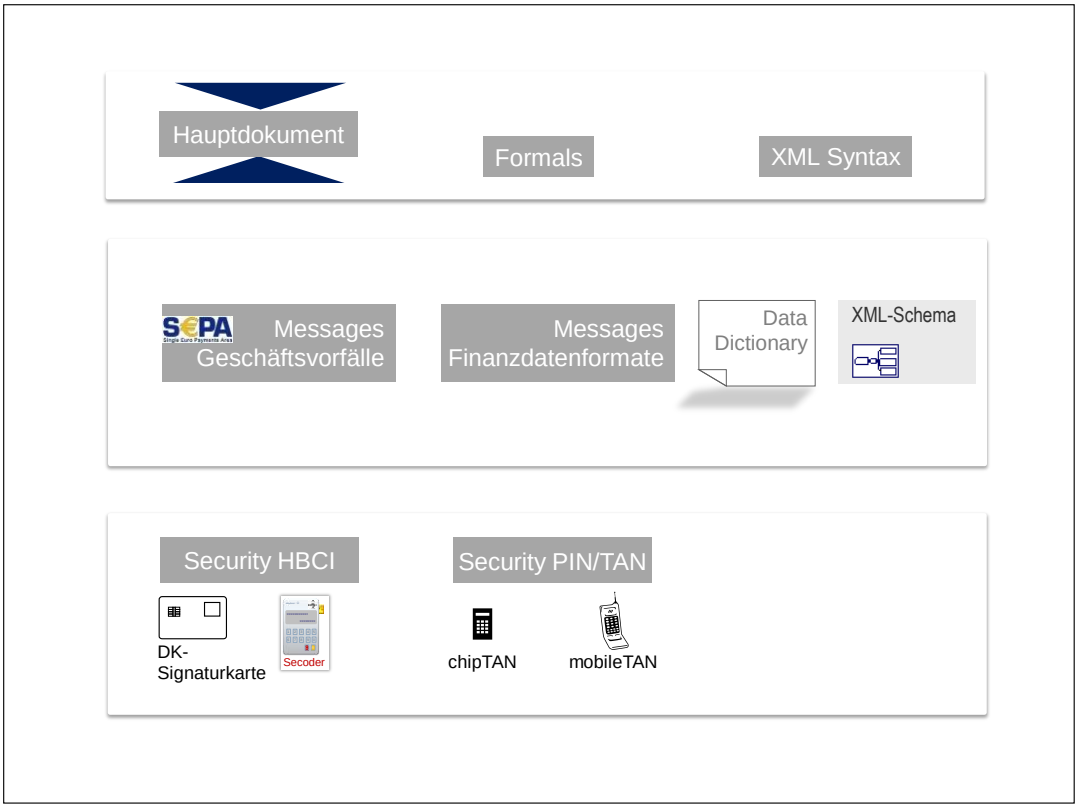
Mit neuen Rollenmodellen und Kommunikationsmöglichkeiten geht der Standard neue Wege und ermöglicht die Nutzung des Protokolls für alle elektronischen Vertriebswege. Ab der Version 3.0 wurde der FinTS-Standard neu gegliedert, um der Unabhängigkeit der Legitimationsverfahren, der Geschäftsvorfälle und der Finanzdatenformate von dem zugrunde liegenden Protokoll gerecht zu werden. Die Einzeldokumente sind in einer Gesamtspezifikation mit dem Titel FinTS - Financial Transaction Services – zusammengefasst.

Folgende HBCI- und FinTS-Versionen wurden von der Deutschen Kreditwirtschaft bisher veröffentlicht:

HBCI V2.01	obsolet
HBCI V2.1	obsolet
HBCI V2.2	obsolet
FinTS V3.0	wird redaktionell gepflegt
FinTS V4.0	obsolet
FinTS V4.1	aktuelle FinTS-Version

I.1 FinTS-Dokumentenstruktur

Einen Überblick über die Dokumentenstruktur zeigt die folgende Abbildung:



Die einzelnen Bände beschreiben folgende Inhalte der FinTS-Spezifikation

[Datenformate] In den FinTS-Geschäftsvorfällen verwendete Finanzdatenformate wie z. B. SEPA pain messages

[DataDictionary] Fachliche Beschreibung aller allgemeinen Datenstrukturen und –Elemente, die in den Bänden [HBCI], [Formals], [PINTAN] und [Syntax] verwendet werden.

[Formals] Beschreibung des generellen FinTS-Protokolls

[HBCI] Spezifikation der Protokollstrukturen und Verfahren zum Sicherheitsverfahren HBCI

[Master] Dieses Dokument; zentrale Beschreibung der Dokumentenstruktur, der verwendeten Begriffe und Abkürzungen und der Literaturhinweise

[Messages] Fachliche Beschreibung aller multibankfähigen FinTS-Geschäftsvorfälle inkl. eines zugehörigen Data-Dictionary

[PINTAN] Spezifikation der Protokollstrukturen und Verfahren zum Sicherheitsverfahren PIN/TAN inkl. der Secoder-Integration

[RM-Codes] Beschreibung der verwendeten Rückmeldungscodes und deren Bedeutung für die FinTS-Versionen 3.0 und 4.1

[Syntax] Festlegungen zur Verwendung der XML-Syntax in FinTS und Spezifikation der allgemeinen Protokollstrukturen als XML-Schemas

I.2 FinTS-Dokumente und deren Versionsstände

Die folgende Auflistung enthält die jeweils aktuellen Versionen der einzelnen Dokumente. Die Versionsbezeichnung ändert sich nur, wenn eine neue FinTS-Version publiziert wird, ansonsten bezeichnet das Releasedatum den Stand des Dokumentes.

Über die in […] verwendeten Schlüsselwörter wird in der gesamten FinTS-Spezifikation auf diese Dokumente verwiesen.

[Datenformate] Financial Transaction Services (FinTS) – Messages (Finanzdatenformate), Version 4.1 final version, 20.01.2014, Die Deutsche Kreditwirtschaft

[DataDictionary] Financial Transaction Services (FinTS) – Data Dictionary, Version 4.1 final version, 06.10.2017, Die Deutsche Kreditwirtschaft

[Formals] Financial Transaction Services (FinTS) – Formals, Version 4.1 final version, 06.10.2017, Die Deutsche Kreditwirtschaft

[HBCI] Financial Transaction Services (FinTS) – Security (Sicherheitsverfahren HBCI), Version 4.1 final version, tt.mm.2017, Die Deutsche Kreditwirtschaft

[Master] Financial Transaction Services (FinTS) – Hauptdokument, Version 4.1 final version, 23.02.2018, Die Deutsche Kreditwirtschaft

[Messages] Financial Transaction Services (FinTS) – Messages (Multibankfähige Geschäftsvorfälle), Version 4.1 final version, 25.07.2016, Die Deutsche Kreditwirtschaft

[PINTAN] Financial Transaction Services (FinTS) – Security (Sicherheitsverfahren PIN/TAN), Version 4.1 final version, 23.02.2018, Die Deutsche Kreditwirtschaft

[RM-Codes] Financial Transaction Services (FinTS) – Rückmeldungscodes, Version 3.0 / 4.1 final version, 23.02.2018, Die Deutsche Kreditwirtschaft

[Syntax] Financial Transaction Services (FinTS) – XML-Syntax, Version 4.1 final version, 23.02.2018, Die Deutsche Kreditwirtschaft

I.3 Unterstützte FinTS XML-Namespaces

Die Dokumentenversion 4.1 unterstützt gemäß der in [Formals] beschriebenen FinTS-Versionsverwaltung folgende Namespaces:

Version	Datum	URL	Anmerkungen
0.0	20.01.2014	http://www.fints.org\spec\xmlschema\0.0	FinTS4 Versionsverwaltung
4.1	20.01.2014	http://www.fints.org\spec\xmlschema\4.1	FinTS V4.1 initial
4.1.1	06.10.2017	http://www.fints.org\spec\xmlschema\4.1.1	FinTS V4.1 mit Unterstützung der starken Kundenauthentifzierung gemäß PSD2

II. ABKÜRZUNGSVERZEICHNIS

Abkürzung	Bedeutung
ABNF	Augmented Backus Naur Form (RFC2234), Syntaxbeschreibungssprache
AC	Access Condition
AEF	Application Elementary File
AES	Advanced Encryption Standard
AID	Application Identifier
AIS(P)	*Account Information Service (Provider),* Kontoinformationsdienst(anbieter) gemäß PSD2
ASPSP	*Account Servicing Payment Service Provider,* Kontoführender Zahlungsdienstleister gemäß PSD2
BaFin	*Bundesanstalt für Finanzdienstleistungsaufsicht*
BIC	Bank Identifier Code
BZÜ	Beleggebundenes Zahlscheinüberweisungsformular
C	Datenstruktur ist konditional
CAMT	Cash Management Nachrichten
CBC	Cipher Block Chaining
CGI	Common Gateway Interface, Schnittstelle für die Bereitstellung dynamischer Informationen in einem WWW-Server
CID	Cardholders Information Data (Kartenidentifikationsdaten der DK-Chipkarte)
CLA	Class Byte
CR	Carriage-Return (Wagenrücklauf)
DK	Die Deutsche Kreditwirtschaft
DE	Datenelement
DEG	Datenelementgruppe
DF	Dedicated File
DFÜ	Synonym verwendet für "Datenkommunikation, die in Form von Filetransfer, E-Mail, Online-Nachrichtenaustausch etc. erfolgen kann
DTA	s. DTAUS
DTAUS	Datensatzformat für den Inlandszahlungsverkehr (veröffentlicht in den Bedingungen für die Beteiligung von Kunden am beleglosen Datenträgeraustausch mittels Disketten)
DTAZV	Datensatzformat für den Auslandszahlungsverkehr
EBA	*European Banking Authority*, europäische Bankenaufsicht
EBICS	Electronic Banking Internet Communication Service, DK-Standard im Firmenkundenbereich
ECB	Electronic Code Book
EF	Elementary File
EF_ID	Elementary File ID der DK-Chipkarte. Die →CID ist Bestandteil des EF_ID
eIDAS	Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (EU) Nr. 910/2014
EU	Elektronische Unterschrift; basiert auf dem asymmetrischen RSA-Verfahren
EWWU	Europäische Wirtschafts- und Währungsunion
FCI	File Control Information
FCP	File Control Parameters

Abkürzung	Bedeutung
FCS	Frame Check Sequence
FinTS	Financial Transaction Services
FinTS3	Abkürzung für FinTS Version 3 und ggf. Sub-Versionen
FinTS4	Abkürzung für FinTS Version 4 und Sub-Versionen
FMD	File Management Data
GD	Gattungsdaten der Wertpapiermitteilungen
GV	Geschäftsvorfall
HBCI	Homebanking Computer Interface
HTTP	Hypertext Transfer Protocol (RFC2068), World-Wide-Web-Basisprotokoll
I	Information (z. B. Schlüsselart)
IANA	*Internet Assigned Numbers Authority*, Organisation der ➔IETF, die über die Vergabe von Bezeichnern und Nummern in Internet-Protokollen wacht
IBAN	International Banking Account Number
ID	Identifikationsmerkmal (Nummer oder alphanumerischer Code)
IESG	*Internet Engineering Steering Group*, Steuerungsorgan der ➔IETF
IETF	*Internet Engineering Task Force*, Organisation, die für die Standardisierung im Internet verantwortlich ist (http://www.ietf.org)
IP	*Internet Protocol*, Protokoll zur Übertragung von Datenpaketen im Internet
IPC	*Interprocess Communication*, Verfahren zur Kommunikation zwischen verschieden Prozessen auf einem oder mehrerer Rechnersysteme
ISIN	International Securities Identification Number
ISO	International Organisation for Standardisation
IV	Initialisierungsvektor
KGK	Key Generating Key
LF	Line-Feed (neue Zeile)
M	Datenstruktur muss vorhanden sein und ist inhaltlich korrekt zu füllen
MAC	Message Authentication Code; Symmetrisches Verfahren zur Erzeugung einer ➔elektronischen Signatur (derzeit für die ZKA-Chipkarte eingesetzt)
MF	Master File
MFC	Multifunktions-Chipkarte
MIME	Multipurpose Internet Mail Extensions (RFC2045-49), Erweiterung von ➔SMTP für die Übertragung multimedialer Daten
N	Nachricht
N	Nicht erlaubt (not allowed) (Datenstruktur darf nicht vorhanden sein)
O	Datenstruktur ist optional
PIN	Private Identifikationsnummer, hier Online-Banking-PIN
PIS(P)	*Payment Initiation Service (Provider),* Zahlungsauslösedienst(anbieter) gemäß PSD2
PIIS(P)	*Payment Instrument Issuing Service (Provider),* Karten-herausgebender Zahlungsdienstleistung(sanbieter) gemäß PSD2
PSP	Payment Service Provider, Zahlungsdienstleister (inkl. der Kreditinstitute)
PKD	Public-Key-Daten
PSD2	*Payment Service Directive 2*, Zahlungsverkehrsrichtlinie 2
PSU	Payment Service User, Zahlungsdienstnutzer gemäß PSD2
RAH	RSA-AES-Hybridverfahren
RFC	Request for Comment, Dokument der ➔IETF, nicht notwendigerweise ein Internet Standard
RSA	Asymmetrischer Algorithmus für die elektronische Unterschrift (EU) (vgl. MAC), benannt nach den Erfindern Rivest, Shamir und Adleman.

Abkürzung	Bedeutung
RTS	*Regulatory Technical Standard* der →EBA
SCA	*Strong Customer Authentication,* Starke Kundenauthentifizierung gemäß PSD2
SEG	Segment
SEPA	Single Euro Payments Area
SEQ	Sequenznummer
SF	Segmentfolge
SFI	Short File Identifier
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer, transparentes Protokoll von Netscape zur sicheren Übertragung von Daten im Internet
S.W.I.F.T.	Society for Worldwide Interbanking Financial Communication
T	Transaktion (z. B. Schlüsselart)
TLS	*Transport Layer Security*, in der Entwicklung befindliches Protokoll, das als Nachfolger des SSL-Protokolls für die Internet-Standardisierung vorgesehen ist
TPP	*Third Party Provider,* Drittdienstleister, Zahlungsdiensteanbieter gemäß PSD2
UN/EDIFACT	s. EDIFACT
UPD	User-Parameterdaten
WM	Wertpapiermitteilungen
WKN	Wertpapierkennnummer
WpHG	Wertpapierhandelsgesetz
XS2A-Interface	*Access to Account Interface,* Kontoserviceschnittstelle, Drittdiensteschnittstelle gemäß PSD2
XML	Extended Markup Language
ZKA	Zentraler Kreditausschuss, ehemalige Bezeichnung für →DK

III. FINTS-DEFINITIONEN

Begriff	Bedeutung
Abholauftrag	Synonym: Informationsauftrag. Ein ➔Auftrag an das Kreditinstitut, zur Bereitstellung und Übermittlung von Informationen (z. B. einen Kontoauszug), in Abgrenzung zu transaktionsrelevanten Aufträgen (z. B. Überweisungsauftrag), die nicht nur einen Informationsfluss, sondern reale Transaktionen zur Folge haben.
Administrativer Teil	Teil einer Nachricht, welcher die administrativen Segmente umfasst, welche nicht zum ➔Auftragsteil gehören. Der administrative Teil einer Nachricht wird zusammen mit dem Auftragsteil und der ➔Botensignatur verschlüsselt.
Auftrag	Nutzdatensegment des Kunden an das Kreditinstitut, mit der ein Transaktions- oder Abholauftrag erteilt wird. Dies kann ein bankfachlicher ➔Geschäftsvorfall oder ein FinTS-spezifischer administrativer Vorgang sein.
Auftragskategorie	Die ➔Aufträge, die der Kunde an das Kreditinstitut sendet, sind in die Kategorien "Transaktion" (Auftrag für finanzielle Transaktion) und "Information" (Auftrag zum Informationsabruf) eingeteilt.
Auftragssignaturen	➔Signaturen, welche die ➔elektronischen Signaturen des ➔Herausgebers und der ➔Zeugen enthalten, die die Auftrags- / Antwortsegmente einer Nachricht signieren.
Auftragsteil	Teil einer Nachricht, welcher die bankfachlichen Aufträge bzw. die zugehörigen Antwortdaten und die ➔Auftragssignaturen umfasst.
Auftrags-ID	(XML: *DistSigsID*), wird im Kontext *Verteilter Signaturen* (vgl. [Formals]) verwendet und ist gleichbedeutend mit der in den FinTS V3.0 PIN/TAN- und AZS-Verfahren verwendeten Auftragsreferenz
Benutzer	Eine natürliche Person, die als Inhaber oder Berechtigter eines Kontos über ein Kundenprodukt/-endgerät Online-Banking betreibt (vgl. Kunde).
Benutzernachricht	➔Nachricht des Kunden an das Kreditinstitut, welche einen ➔Auftragsteil mit ➔Aufträgen enthalten kann.
Bote	Der Überbringer einer ➔Nachricht, welcher die ➔Kommunikation mit dem ➔Kreditinstitut führt. Der Bote muss nicht notwendiger Weise auch der ➔Herausgeber des ➔Auftragsteils sein, dies ist jedoch möglich.
Botensignatur	➔Signatur, welche die ➔elektronische Signatur des ➔Boten enthält. Sie signiert den ➔Nachrichtenkopf und den ➔Nachrichtenkörper einer Nachricht.
Datagramm	➔Nachricht, welche zur Bearbeitung über asynchrone Kommunikationsverfahren versendet werden kann. Ein Datagramm enthält alle Elemente eines Dialogs (Initialisierung, Aufträge und Beendigung) und stellt damit einen ein-schrittigen Dialog dar.
Datenelement	FinTS V3.0: (DE) Atomarer Wert des FinTS-Formates (z. B. IBAN). Funktionale Untereinheit einer ➔DEG. Der Begriff Datenelement wird in FinTS4 als spezielle Form einer XML-Struktur verwendet.
Datenelementgruppe	FinTS V3.0: (DEG) Zu einer logischen und syntaktischen Einheit zusammengefasste ➔Datenelemente oder auch wieder DEGs (z. B. Nachrichtenkopf). (Gegensatz: einfaches DE) Der Begriff Datenelementgruppe wird in FinTS4 als spezielle Form einer XML-Struktur verwendet.

Begriff	Bedeutung
Datenstruktur	Oberbegriff für ➔Nachricht, ➔Segment, DE oder DEG (strukturierte Dateneinheit beliebiger "Ebene"). In FinTS4 ist hiermit eine XML-Struktur gemeint.
Dialog	Eine Folge von zusammengehörigen Benutzer- und Institutsnachrichten. Ein Dialog läuft synchron ab.
Elektronische Signatur	Kryptographisches Authentifikationsmerkmal, das auch zum Schutz gegen Veränderungen der Nachrichten, z. B. bei der Datenübertragung, dient. Hier im Einzelnen: Elektronische Unterschrift gemäß DFÜ-Abkommen nach einem spezifizierten RAH-Verfahren oder signaturgesetzkonform wie in [SigG] und [SigV] beschrieben.
FinTS	Oberbegriff über alle HBCI- und FinTS-Versionen. Der Begriff FinTS4 bezeichnet als Sammelbegriff FinTS-Versionen ab V4.0.
Firewall	System zum Schutz privater Netzwerke vor Zugriffen aus dem Internet
Gateway	System, dass üblicherweise Daten zwischen zwei verschiedenen Protokollen aber auch Netzwerken austauscht
Geschäftsvorfall	➔Auftrag, welcher bankfachlicher Natur ist.
Herausgeber	Der ➔Benutzer, welcher die ➔Aufträge innerhalb des ➔Auftragsteils initiiert. Er kann den ➔Auftragsteil ggf. auch verschlüsseln.
Ini-Brief	Begleitbrief; handschriftlich unterschriebener öffentlicher Schlüssel, der zu dessen Initialisierung an das Kreditinstitut gesandt wird.
Intermediär	Vermittler bei Kommunikation zwischen Benutzer und Kreditinstitut
Kommunikation	Austausch von FinTS-Nachrichten zwischen Kundensystem und Kreditinstitut.
Kommunikationsreferenz	Eindeutige ID, mit der die Kunden- und die Kreditinstitutsseite die Nachrichten einer Kommunikation eindeutig zuordnen können. Sowohl die Kunden- wie auch die Kreditinstitutsseite verwaltet unabhängig voneinander derartige Kommunikationsreferenzen.
Kopfteil	In definiertem Format vorangestellter "Header" (➔Nachrichtenkopf, ➔Signatur ➔Verschlüsselungsdaten)
Kreditinstitut	Allgemeingültig für die Kreditinstitutsseite in Abgrenzung zur Kundenseite.
Kreditinstitutsauftragsteil	➔Auftragsteil einer ➔Kreditinstitutsnachricht
Kreditinstitutsnachricht	➔Nachricht vom Kreditinstitut an den Kunden, die das Ergebnis der ➔Aufträge des Kunden enthält.
Kreditinstitutsreferenz	➔Kommunikationsreferenz, über die das Kreditinstitut die Nachrichten einer Kommunikation verwalten kann.
Kunde	Allgemeingültig für die Kundenseite in Abgrenzung zum ➔Kreditinstitut Rolle, in der ein ➔Benutzer im Rahmen einer Kommunikation auftritt
Kundenauftragsteil	➔Auftragsteil einer ➔Benutzernachricht
Kundenreferenz	➔Kommunikationsreferenz, über die der Kunde die Nachrichten einer Kommunikation verwalten kann.
Nachricht	Sende- bzw. Empfangseinheit. Es sind ➔Benutzernachrichten und ➔Kreditinstitutsnachrichten zu unterscheiden.
Nachrichtenkörper	Der Teil einer ➔Nachricht, welcher hinter dem ➔Nachrichtenkopf (verschlüsselt oder unverschlüsselt) eingestellt wird.
Nachrichtenkopf	Der Teil einer ➔Nachricht, welcher immer unverschlüsselt übertragen wird. Er enthält für die Weiterverarbeitung benötigte Steuerinformationen.

Begriff	Bedeutung
öffentlicher Schlüssel	RSA-Public-Key
PC-Banking	Online-Banking per Online-DFÜ-Dialog mit dem Kreditinstitut vom PC aus (in Abgrenzung zu Browser-basiertem Banking, das mit einem TAN-Verfahren, also auch ohne Eigenintelligenz für z. B. die Bildung der ➔elektronischen Signatur betrieben werden kann).
privater Schlüssel	RSA-Private-Key
Proxy	Begriff wird in Zusammenhang von Firewalls benutzt, bei denen über Systeme einer Firewall auf Internet-Dienste zugegriffen wird
Secoder	Unter Secoder wird eine neue Generation von DK Chipkarten-lesern verstanden, bei denen die Möglichkeit besteht, in einem so genannten Applikationsmodus Transaktionsdaten auf sichere Weise im Display anzuzeigen und mit Hilfe einer Bankensig-naturkarte zu signieren. Zur Signaturbildung wird die Signatur-Anwendung auf der Karte verwendet. Im Rahmen der vorlie-genden Spezifikation wird ein Secoder als Basis vorausgesetzt und durchgängig als „Secoder“ bezeichnet.
Secoder Metadata	(Secoder-) MetaData oder Metadaten werden als Eingangsschnittstelle zur Secoder-Anwendungsfunktion im Kundensystem benutzt. Sie entsprechen fachlich den Parameterstrukturen DSx, wie sie in den Data Confirmations des Secoders definiert sind. In FinTS4 werden die Metadaten im Rahmen der Struktur `SecurityMethodParam/SupportedMethod/Secoder/SecoderSignatureParam/SecoderVisualizationParams` abgebildet. Die Metadaten werden von der Secoder-Anwendungsfunktion verwendet und in ein logisches Secoder-Protokoll eingebettet, das physisch wiederum z. B. über PC/SC abgewickelt wird. Durch den Einsatz dieser Metadaten muss die Online-Banking-Applikation selbst kein Wissen bzgl. Protokoll und konkreter Datenschnittstelle zum Secoder besitzen.
Secoder-Anwendungsfunktion	Anwendungsfunktion, welche auf Basis übergebener Metadaten einen z. B. über PC/SC angeschlossenen Secoder protokoll- und datenmäßig bedienen kann. Die Secoder-Anwendungsfunktion kann eine Komponente einer Finanzmanagementsoftware bzw. im Browserkontext ein Java Applet oder PlugIn sein. Teile der Secoder-Anwendungsfunktion können sich auch auf einem Web-oder Application-Server befinden.
Secoder-Kryptogramm	Alternativer Begriff für Secoder-Signaturen. Bei Secoder-Signaturen fließen in die Secoder-Kryptogrammbildung die durch den Kunden bestätigten Daten (VisData) ein.
Secoder-spezifische Kommandos (SecCmds)	Diese Secoder-spezifischen Kommandos werden an der Schnittstelle zwischen Secoder-Anwendungsfunktion und dem Secoder selbst z. B. über PC/SC ausgetauscht. Beispiele hierfür sind „Select Application“ oder „Data Confirmation“.
Segment	FinTS V3.0: (SEG) ➔Datenelementgruppe mit einer herausgehobenen Bedeutung im Aufbau einer ➔Nachricht (z. B. Auftrag oder Nachrichtenkopf). Der Begriff Segment wird in FinTS4 als spezielle Form einer XML-Struktur verwendet.
Signatur	➔elektronische Signatur; ➔Signatur-Segment

Begriff	Bedeutung
Signatur-Segment	Segment, welches eine ➔elektronische Signatur und alle weiteren für die Verarbeitung notwendigen Werte enthält.
Syntaxzeichen	Zeichen mit besonderer Bedeutung im Rahmen der XML-Syntax (z. B. "<" und „>“als Begrenzer eines XML-Tagbezeichners).
Unterschrift	Wenn nicht ausdrücklich anders vermerkt, sind hierunter ➔elektronische Signaturen (RSA-EU) zu verstehen.
User	➔Benutzer
Verschlüsselungs-daten	Segment, welches verschlüsselte Daten und alle weiteren für deren Verarbeitung notwendigen Werte enthält.
VisAuthSig	Visualisierungsauthentikationssignatur (auch VisAuth-Signatur) des Secoders. Diese Signatur dient bei Verwendung der Secoder-Applikationen „aut“ und „sig“ zum Nachweis gegenüber dem Kreditinstitut, dass – falls ein Secoder am Kundenendgerät angeschlossen war – dieser sich zum Zeitpunkt der VisData-Signatur im Applikationsmodus befunden hat.
VisData	Analog der Secoder-Spezifikation wird hierunter der Aufbau der zu signierenden Daten im Secoder, d. h. zwischen Lesereinheit und Chipkarte verstanden.
VisDataSig	(auch VisData-Signatur)Signatur über den VisData-Bereich des Secoders.
WWW-Server	auch Webserver, System, das den Zugriff auf Daten über ➔http erlaubt
Zeuge	➔Benutzer, welcher ggf. den ➔Auftragsteil zusätzlich zum ➔Herausgeber signiert.

IV. LITERATURHINWEISE

Über die in […] verwendeten Schlüsselwörter wird in der gesamten FinTS-Spezifikation auf diese Dokumente verwiesen.

Als Bezugsquelle für RFC-Dokumente kann z. B. ftp://ftp.eunet.de/pub verwendet werden.

[AES] Federal Information Processing Standards 197 v. 26. November 2001, National Institute of Standards and Technology (NIST)

[Canonical XML] Canonical XML Version 1.0, W3C Recommendation 15 March 2001, http://www.w3.org/TR/xml-c14n

[DF_NOTEPAD] Anwendung Notepad für SECCOS 6, Version 1.0 vom 10.11.2006, Die Deutsche Kreditwirtschaft

[DFÜ] Abkommen über die Datenfernübertragung zwischen Kunden und Kreditinstituten (DFÜ-Abkommen), Zentraler Kreditausschuss, 2001

[DFÜ-Abkommen] Anlage 3 der Schnittstellenspezifikation für die Datenfernübertragung zwischen Kunde und Kreditinstitut gemäß DFÜ-Abkommen „Spezifikation der Datenformate“, in der jeweils höchsten Version, derzeit Version 2.6 – Die Deutsche Kreditwirtschaft

sowie

Kryptographische Verfahren des deutschen Kreditgewerbes für die Elektronische Unterschrift und für die Verschlüsselung im Rahmen der Kunde-Bank-Kommunikation in: Anlage 1 der Schnittstellenspezifikation für die Datenfernübertragung zwischen Kunde und Kreditinstitut gemäß DFÜ-Abkommen – Spezifikation für die EBICS-Anbindung, Version 2.5, 16.05.2011

[DINSIG] Chipcards with digital signature application/function according to SigG and SigV, Part 4: Basic Security Services, DIN V66291-4 vom 14. September 2001

[DK Krypto] ZKA Kryptographie – Teil 1: Empfohlene kryptographische Algorithmen, Version 1.0

[DTAUS] Bedingungen für den Datenträgeraustausch (DTAUS0), Anhang 4, Zentraler Kreditausschuss, 2002

[DTAZV] Auslandszahlungsverkehr im Datenaustausch zwischen Kunde und Bank (DTAZV), gültig ab 1. Juli 2003, Deutsche Bundesbank

[EBS 204] IBAN: International Bank Account Number (EBS 204), hrsg. v. European Committee for Banking Standards, November 1996 (http://www.ecbs.org/download.html)

[EBS 204] International Bank Account Number (IBAN), European Banking Standard EBS 204, Version 3.2, hrsg. v. European Committee for Banking Standards, August 2003 (http://www.ecbs.org)

[EU-Richtlinie] Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, Amtsblatt der Europäischen Gemeinschaften v. 19.01.2000

[Exclusive XML Canonicalization] Exclusive XML Canonicalization Version 1.0, W3C Recommendation 18 July 2002, http://www.w3.org/TR/xml-exc-c14n/

[HHD] Schnittstellenspezifikation für die ZKA Chipkarte – HandHeld-Device (HHD) zur TAN-Erzeugung, Version 1.4, 07.05.2010, Die Deutsche Kreditwirtschaft

[HHD-Belegung] ZKA TAN-Generator – Belegungsrichtlinien zur Dynamisierung der TAN, Version 1.4, Final Version, 12.11.2010, Zentraler Kreditausschuss

[HHD-Erweiterung] HHD-Erweiterung für unidirektionale Kopplung, Version 1.4 Final Version, 07.05.2010, Zentraler Kreditausschuss

[ISIS/MTT] ISIS/MTT (Industrial Signature Interoperability and MailTrusT Specification / MailTrusT) Version 1 – Part 1: Certificate and CRL Profiles.

[ISO 639.3] ISO 639.3:2007: Code for the representation of names of languages – Part 1: Alpha-2 code (http://lcweb.loc.gov/standards/iso639-2/iso639jac.html)

[ISO 3166] ISO 3166-1:2006: Code for the representation of names of countries and their subdivisions - Part 1: Country code (http://www.din.de/gremien/nas/nabd/iso3166ma/)

[ISO 3166] ISO 3166-1:1996: Code for the representation of names of countries and their subdivisions - Part 1: Country code (http://www.unece.org/trade/lcode/loc99.zip oder http://www.iso.org/iso/home/standards/country_codes/country_names_and_code_elements.htm)

[ISO 4217] ISO 4217:1995: Codes for the representation of currencies and funds

[ISO 6166] ISO 6166: International Securities Numbering System

[ISO 8601] ISO 8601:2000: Data elements and interchange formats – Information interchange -- Representation of dates and times

[ISO 8859] ISO 8859-1:1987: Information processing - 8 bit single-byte coded graphic character sets - Part 1: Latin alphabet No. 1

[ISO 9362] ISO 9362: Bank Identifier Code (BIC)

[ISO 9796] ISO 9796:2010 Information technology - Security techniques - Digital signature scheme giving message recovery

[ISO 9796-2] ISO 9796-2:2010 Information technology - Security techniques - Digital signature scheme giving message recovery – Part 2: Mechanisms using a hash-function[ISO 10116] ISO 10116:2006 Information technology Security techniques - Modes of operation for an n-bit block cipher algorithm

[ISO 10383] ISO 10383: Market Identifier Code (MIC)

[ISO 13616] ISO 13616: Banking and related services - International Bank Account Number (IBAN)

[ISO 15022-1] ISO 15022-1:1999 Securities - Scheme for messages (Data Field Dictionary) - Part 1: Data field and message design rules and guidelines (http://www.iso15022.org)

[ISO 15022-2] ISO 15022-2:1999 Securities - Scheme for messages (Data Field Dictionary) - Part 2: Maintenance of the Data Field Dictionary and Catalogue of Messages (http://www.iso15022.org)

[KT-KONZEPT] Schnittstellenspezifikation für die DK-Chipkarte, Konzept für die Unterstützung der Signatur-Anwendung der DK-Chipkarte durch das Internet-Kundenterminal, Version 1.0, 15. Februar 2002

[KT-SIG] Schnittstellenspezifikation für die DK-Chipkarte, Spezifikation des Internet-Kundenterminals für die Unterstützung der Signatur-Anwendung der DK-Chipkarte (ZKA-SIG-API), Version 2.0, 10. März 2008

[Laden GK] HBCI - Homebanking Computer Interface – Laden der GeldKarte, Konzept – Version 1.0, Zentraler Kreditausschuss, 17. Juli 2002

[Länderverz] Länderverzeichnis für die Zahlungsbilanzstatistik der Bundesrepublik Deutschland, Deutsche Bundesbank, Januar 2002 (http://www.bundesbank.de/melde/aussenwirtschaft/download/schluessel/laenderverzeichnis_0102.pdf)

[MaSI] Rundschreiben 4/2015 - Mindestanforderungen an die Sicherheit von Internet-Zahlungen (MaSI), Bundesanstalt für Finanzdienstleistungsaufsicht, 03.05.2015

[Namespaces] Namespaces in XML, W3C Recommendation 8 December 2009, http://www.w3.org/TR/REC-xml-names/

[PSD2] Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25.11.2015 über Zahlungsdienste im Binnenmarkt

[PKCS1] PKCS #1: RSA Cryptography Standard, Version 2.0, RSA Laboratories, October 1998 (http://www.rsasecurity.com/rsalabs/pkcs/pkcs-1/)

[RFC 1951] DEFLATE Compressed Data Format Specification version 1.3, May 1996 (ftp://ftp.isi.edu/in-notes/rfc1951.txt)

[Richtl. ZV] Richtlinien für einheitliche Zahlungsverkehrsvordrucke und Merkblätter für neutrale Zahlungsverkehrsvordrucke

[RSA] R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, vol. 21 no. 2, 1978.

[RTS-SCA] *Regulatory Technical Standards* for strong customer authentication and common and secure open standards of communication, European Banking Authority, Final Version, 27.11.2017

[SECCOS-6] Interface Specifications for the SECCOS ICC Secure Chip Card Operating System (SECCOS) Version 6.2.1, 11.11.2009

[Secoder] Secoder – Connected Mode Reader Applications, Version 2.2 Final Version, 05.08.2011, Zentraler Kreditausschuss

[SHA-256] Federal Information Processing Standards Publication 180-2 2002 August 1, (http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf)

[SigG] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften v. 16. Mai 2001, Bundesgesetzblatt Jahrgang 2001, Teil I Nr. 22

[SigV] Verordnung zur elektronischen Signatur v. 16. November 2001, Bundesgesetzblatt Jahrgang 2001, Teil I Nr. 59

[SIG 203] IBAN: Standard Implementation Guidelines (SIG 203), hrsg. v. European Committee for Banking Standards, November 1996 (http://www.ecbs.org/download.html)

[SOAP 1] SOAP Version 1.2 Part 1: Messaging Framework(Second Edition), W3C Recommendation 27 April 2007, http://www.w3.org/TR/soap12-part1/

[SOAP 2] SOAP Version 1.2 Part 2: Adjuncts (Second Edition), W3C Recommendation 27 April 2007, http://www.w3.org/TR/soap12-part2/

[S.W.I.F.T.] http://www.swift.com

[SWIFT] S.W.I.F.T. Standards Release Guide 2002

[TR 201] Register of European Account Numbers, Technical Report TR 201, Version 2.1, hrsg. v. European Committee for Banking Standards, September 1999 (http://www.ecbs.org)

[WSDL 1] Web Services Description Language (WSDL) Version 2.0, Part 1: Core Language, W3C Recommendation 26 June 2007, http://www.w3.org/TR/wsdl20

[WSDL 2] Web Services Description Language (WSDL) Version 2.0, Part 2: Adjuncts, W3C Recommendation 26 June 2007, http://www.w3.org/TR/wsdl20-patterns

[XML1.0] Extensible Markup Language (XML) 1.0 (Fifth Edition), W3C Recommendation 26 November 2008, http://www.w3.org/TR/REC-xml

[XML Encryption] XML Encryption Syntax and Processing, W3C Recommendation 10 December 2002, http://www.w3.org/TR/xmlenc-core/

[XML Schema 1] XML Schema Part 1: Structures Second Edition, W3C Recommendation 28 October 2004, http://www.w3.org/TR/xmlschema-1/

[XML Schema 2] XML Schema Part 2: Datatypes Second Edition, W3C Recommendation 28 October 2004, http://www.w3.org/TR/xmlschema-2/

[XML Signature] XML-Signature Syntax and Processing (Second Edition), W3C Recommendation 10 June 2008, http://www.w3.org/TR/xmldsig-core/

[XPath] XML Path Language (XPath) Version 1.0, W3C Recommendation 16 November 1999, http://www.w3.org/TR/xpath/

[XPath Filter] XML-Signature XPath Filter 2.0, W3C Recommendation 08 November 2002, http://www.w3.org/TR/xmldsig-filter2/

[X3.92] ANSI X3.92-1981 (R1987): Data Encryption Algorithm

[X3.106] ANSI X3.106-1983 (R1996): Data Encryption Algorithm, Modes of operation

[X9.23] ANSI X9.23-1995 (R1995): Financial Institution Encryption of Wholesale Financial Messages

[X509] RFC 3039: Internet X.509 Public Key Infrastructure Qualified Certificates Profile

[ZKASIG] Schnittstellenspezifikation für die DK-Chipkarte, Digital Signature Application, Version 1.3.1, 10. März 2011