

FinTS

Financial Transaction Services

Schnittstellenspezifikation

Formals

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

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.

Die Schnittstellenspezifikation ist urheberrechtlich geschützt. Zur Implementation in Kunden- und Kreditinstitutssysteme wird interessierten Herstellern unentgeltlich ein einfaches Nutzungsrecht eingeräumt. Im Rahmen des genannten Zwecks darf die Schnittstellenspezifikation auch - in unveränderter Form - vervielfältigt und zu den nachstehenden Bedingungen verbreitet werden.

Umgestaltungen, Bearbeitungen, Übersetzungen und jegliche Änderung der Schnittstellenspezifikation sind untersagt. Kennzeichnungen, Copyright-Vermerke und Eigentumsangaben dürfen in keinem Fall geändert werden.

Im Hinblick auf die Unentgeltlichkeit des eingeräumten Nutzungsrechts wird keinerlei Gewährleistung oder Haftung für Fehler der Schnittstellenspezifikation oder die ordnungsgemäße Funktion der auf ihr beruhenden Produkte übernommen. Die Hersteller sind aufgefordert, Fehler oder Auslegungsspielräume der Spezifikation, die die ordnungsgemäße Funktion oder Multibankfähigkeit von Kundenprodukten behindern, der Deutschen Kreditwirtschaft zu melden. Es wird weiterhin ausdrücklich darauf hingewiesen, dass Änderungen der Schnittstellenspezifikation durch Die Deutsche Kreditwirtschaft jederzeit und ohne vorherige Ankündigung möglich sind.

Eine Weitergabe der Schnittstellenspezifikation durch den Hersteller an Dritte darf nur unentgeltlich, in unveränderter Form und zu den vorstehenden Bedingungen erfolgen.

Dieses Dokument kann im Internet abgerufen werden unter <http://www.fints.org>.

Versionsführung

Das vorliegende Dokument wurde von folgenden Personen erstellt bzw. geändert:

Name	Organi- sation	Datum	Version	Dokumente	Anmerkungen
	SIZ	22.06.2004	4.0 Final Version	FinTS_4.0_Formals.doc	
Haubner	für SIZ	20.01.2014	4.1 Final Version	FinTS_4.1_Formals_201 4-01-20_FV.docx	
Haubner	für SIZ	06.10.2017	4.1 Final Version	FinTS_4.1_Formals_201 7-10-06_final_version. docx	

Unterstützte FinTS XML-Namespaces

Die durch die FinTS-Dokumentenversion 4.1 unterstützten Namespaces sind im FinTS Hauptdokument [Master] beschrieben.

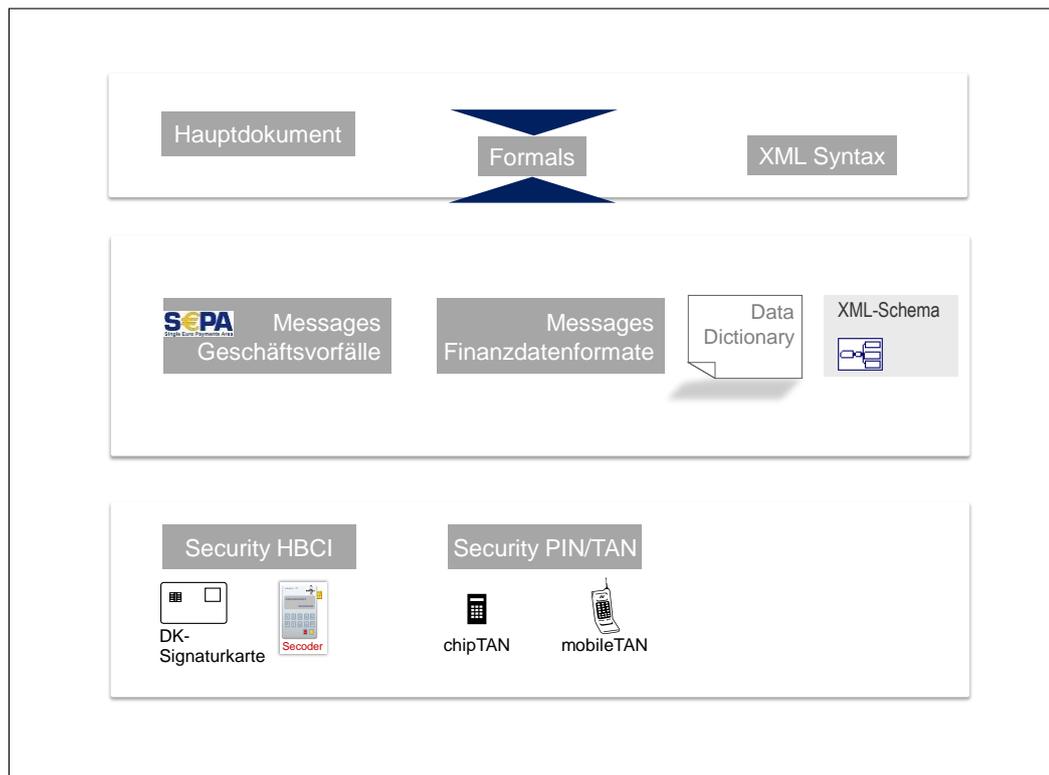
Änderungen gegenüber der Vorversion:

Änderungen zur Vorversion sind im Dokument durch einen Randbalken markiert. Falls sich die Kapitelnummerierung geändert hat, bezieht sich die Kapitelangabe auf die neue Nummerierung.

Ifd. Nr.	Kapitel	Kapitelnummer	Ken-nung ¹	Art ²	Beschreibung
1	Diverse	Diverse	0497	E	Unterstützung der starken Kundenauthentifizierung gemäß PSD2

Dokumentenstruktur

Das vorliegende Dokument steht in folgendem Bezug zu den anderen Bänden der FinTS-Spezifikation:



Dokumenteninhalte, Abkürzungen, Definitionen und Literaturhinweise befinden sich im FinTS Hauptdokument [Master].

¹ nur zur internen Zuordnung

² F = Fehler; Ä = Änderung; K = Klarstellung; E = Erweiterung

Kapitel:	I	Version:	4.1 FV	Financial Transaction Services (FinTS)
		Dokument:		Formals - Grundsätzliche Festlegungen
Seite:	2	Stand:	06.10.2017	Kapitel: Inhaltsverzeichnis

II.8	Verbindungsabbruch	39
II.9	Benutzernachrichten allgemein	45
II.9.1	Aufträge	46
II.9.2	Abholauftrag.....	47
II.9.3	Transaktionsauftrag.....	50
II.10	Kreditinstitutsnachrichten allgemein	51
II.10.1	Rückmeldungen zur Nachricht	52
II.10.2	Rückmeldungen zum Auftragsteil	52
II.10.3	Rückmeldungen zu Aufträgen	53
II.10.4	Datensegmente	53
II.11	RückmeldungsCodes	55
II.11.1	Grundkonzept.....	55
II.11.2	Reaktionsvorschriften.....	55
II.11.3	Code-Bedeutungen	58
II.12	Nachrichtentypen	59
II.12.1	Unverschlüsselte Nachricht	59
II.12.2	Teilverschlüsselte Nachrichten	60
II.12.3	Verschlüsselte Nachrichten	61
II.12.4	Vorgehensweise beim Signieren und Verschlüsseln	62
II.12.5	Vorgehensweise beim Entschlüsseln und Prüfen der Signaturen	63
II.13	Verschlüsselung der Kommunikation	64
II.14	Komprimierung	66
II.15	Initialisierung	67
II.15.1	Benutzernachricht	67
II.15.1.1	Identifikation.....	67
II.15.1.2	Verarbeitungsvorbereitung	68
II.15.2	Kreditinstitutsnachricht	69
II.15.2.1	Bankparameterdaten	69
II.15.2.2	User-Parameterdaten	70
II.15.2.3	Übermittlung eines öffentlichen Schlüssels	70
II.15.2.4	Kreditinstitutsmeldung	71
II.15.3	Empfehlung für die Bildung von Kommunikationsreferenzen.....	71
II.16	Dialogabbruchnachricht	73
II.17	Anonymer Zugang	74
II.17.1	Administrativer Teil.....	74
II.17.2	Initialisierung	74
II.17.3	Auftragsteil	75

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: I
Kapitel: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 3

III. AUFTRAGSVERFAHREN	77
III.1 Allgemeines	78
III.2 Statusprotokoll	79
III.3 Synchronisierung	81
III.4 Adressregistrierung	85
III.4.1 Registrieren einer Adresse	86
III.4.2 Abfragen der registrierten Adressen	86
III.4.3 Löschen einer registrierten Adresse	86
III.5 Bestätigung von Aufträgen und Lebendmeldung	87
III.5.1 Quittierung von Aufträgen	87
III.5.2 Willenserklärung des Kunden	87
III.5.3 Lebendmeldung in Dialogen	88
III.6 Das Publish/Subscribe-Verfahren	90
III.6.1 Einreichen eines Subscription-Auftrags (Subscription)	91
III.6.2 Abfragen der bisher eingereichten Subscription-Aufträge	92
III.6.3 Löschen eines Subscription-Auftrags	93
III.7 Verteilte Signaturen	94
III.7.1 Einreichen eines Auftrages zur verteilten Signatur	94
III.7.2 Details zu eingereichten Aufträgen anfordern	95
III.7.3 Verteilte Signatur leisten	97
III.7.4 Auftrag zur verteilten Signatur löschen	98
 IV. BANKPARAMETERDATEN (BPD)	 100
IV.1 Allgemeines	101
IV.2 Aufbau	104
IV.2.1 Bankparameter allgemein	104
IV.2.2 Kommunikationszugang	105
IV.2.3 Sicherheitsverfahren	106
IV.2.4 Komprimierungsverfahren	106
IV.2.5 Geschäftsvorfallparameter	106
IV.3 Anforderung der BPD in einem Szenario mit Intermediär	108
 V. USER-PARAMETERDATEN (UPD)	 109
V.1 Allgemeines	110
V.2 Aufbau	112
V.2.1 User-Parameter allgemein	112
V.2.2 Kontoinformation	112
V.2.2.1 Geschäftsvorfälle ohne Kontobezug	112

Kapitel:	Version:	Financial Transaction Services (FinTS)
I	4.1 FV	Dokument: Formals - Grundsätzliche Festlegungen
Seite:	Stand:	Kapitel: Inhaltsverzeichnis
4	06.10.2017	

V.3	UPD für anonymen Zugang.....	114
V.4	UPD des Intermediärs (IPD)	115
V.5	UPD des Benutzers für Intermediärzugang (UPDI).....	116
V.6	Explizite Anforderung von UPD	118
V.7	Pflege der Intermediärzugänge und der UPDI	119
	V.7.1.1 Intermediäre auflisten	119
	V.7.1.2 An- und Abmelden der Intermediär-Benutzung	119
	V.7.1.3 UPDI bearbeiten	119
VI.	Transportmedienspezifische Festlegungen.....	121
VI.1	HTTP	122
VI.2	SMTP	125
VI.3	Sonstige Kommunikationsdienste	127
VI.4	Codierung	127
VI.5	Zulässige Kombinationen von Kommunikationsart, Transportprotokoll und Sicherheitsverfahren	127
VII.	FinTS-Versionsverwaltung	129
VII.1	Allgemeines	129
VII.2	Abruf unterstützter FinTS-Versionen	130
VII.3	Aktuell unterstützte Namespaces.....	131

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: I
Kapitel: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 5

Abbildungsverzeichnis

Abbildung 1: Übersicht der Schnittstellenbeziehungen	7
Abbildung 2: Allgemeiner Nachrichtenaufbau	11
Abbildung 3: Benutzer, mehreren Kunden zugeordnet.....	16
Abbildung 4: Kunde, mehreren Benutzern zugeordnet.....	16
Abbildung 5: Direkte Kommunikation	20
Abbildung 6: Kommunikation unter Einbeziehung eines Intermediärs.....	20
Abbildung 7: Intermediärszenario A	21
Abbildung 8: Intermediärszenario B	22
Abbildung 9: Intermediärszenario C.....	23
Abbildung 10: Intermediärszenario D	24
Abbildung 11: Rollenverteilung bei Kommunikation mit und ohne Intermediär	26
Abbildung 12: Nachrichtenabfolge im synchronen Verfahren.....	27
Abbildung 13: Nachrichtenabfolge im asynchronen Verfahren.....	29
Abbildung 14: Dialogabfolge	30
Abbildung 15: Einzelkunde	31
Abbildung 16: Mehrere Kunden	32
Abbildung 17: Einbeziehung eines Intermediärs	33
Abbildung 18: Intermediär und mehrere Kreditinstitute	34
Abbildung 19: Intermediär sammelt Kundenaufträge	35
Abbildung 20: Datagramme	38
Abbildung 21: Verbindungsabbruch Fall 1	40
Abbildung 22: Verbindungsabbruch Fall 2	41
Abbildung 23: Verbindungsabbruch Fall 3	42
Abbildung 24: Verbindungsabbruch Fall 4	42
Abbildung 25: Verbindungsabbruch Fall 5	43
Abbildung 26: Verbindungsabbruch Fall 6	44

Kapitel:	I	Version:	4.1 FV	Financial Transaction Services (FinTS)
		Dokument:		Formals - Grundsätzliche Festlegungen
Seite:	6	Stand:	06.10.2017	Kapitel: Inhaltsverzeichnis

Abbildung 27: Fehlerreaktionsvorschriften (Beispiel)	57
Abbildung 28: Unverschlüsselte Benutzernachricht	60
Abbildung 29: Teilverschlüsselte Benutzernachricht	61
Abbildung 30: Verschlüsselte Nachricht.....	62
Abbildung 31: Ablauf Adressregistrierung und –verifikation	85
Abbildung 32: Funktionsweise der KeepAlive-Nachricht	89
Abbildung 33: Publish/Subscribe-Verfahren.....	91
Abbildung 34: Auftrag zur verteilten Signatur einreichen.....	95
Abbildung 35: Liste der verteilt zu signierenden Aufträge anfordern	96
Abbildung 36: Verteilt zu signierenden Auftrag anfordern	97
Abbildung 37: Verteilte Signatur leisten	98
Abbildung 38: Auftrag zur verteilten Signatur löschen.....	99
Abbildung 39: Mögliche Beziehungen zwischen BPD, UPD, IPD und UPDI.....	117
Abbildung 40: Beispiel für Pflege der UPDI.....	120
Abbildung 41: Kommunikationsart, Transportprotokoll und Sicherheitsverfahren..	128
Abbildung 42: Zusammenhang der Namespaces bei FinTS4	129
Abbildung 43: Der Aufbau des FinTS-namespace 0.0.....	130

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: I
Kapitel: EINLEITUNG Abschnitt: Begriffsbestimmung	Stand: 06.10.2017	Seite: 7

I. EINLEITUNG

Die vorliegenden Financial-Transaction-Services-Spezifikationen (FinTS) bilden die Grundlage für eine automatisiert nutzbare multibankfähige Online-Banking-Schnittstelle. Eine übergangsweise parallele Nutzung alternativer Kreditinstitutszugänge wie z. B. browserbasiertes Internet-Banking bleibt hiervon unberührt.

Beschrieben wird die Schnittstelle zwischen Kundenprodukt und Kreditinstitutssystem, sowohl ohne als auch unter Einbeziehung eines Intermediärs, über den die Kommunikation zwischen Kunde und Kreditinstitut abgewickelt werden kann. Um die Multibankfähigkeit zu gewährleisten, ist zusätzlich eine Beschreibung der Schnittstelle zwischen Kundenprodukt und Sicherheitsmedium erforderlich. Daher findet sich in [HBCI] eine Spezifikation der Schnittstelle zwischen einem FinTS-Kundenprodukt und einer Chipkarte bzw. einer Diskette oder einem USB-Stick. [HBCI] enthält auch die Spezifikation zur Integration des Secoders in FinTS. Zur Abwicklung des PIN/TAN-Verfahrens findet sich die Schnittstellenspezifikation in [PINTAN].

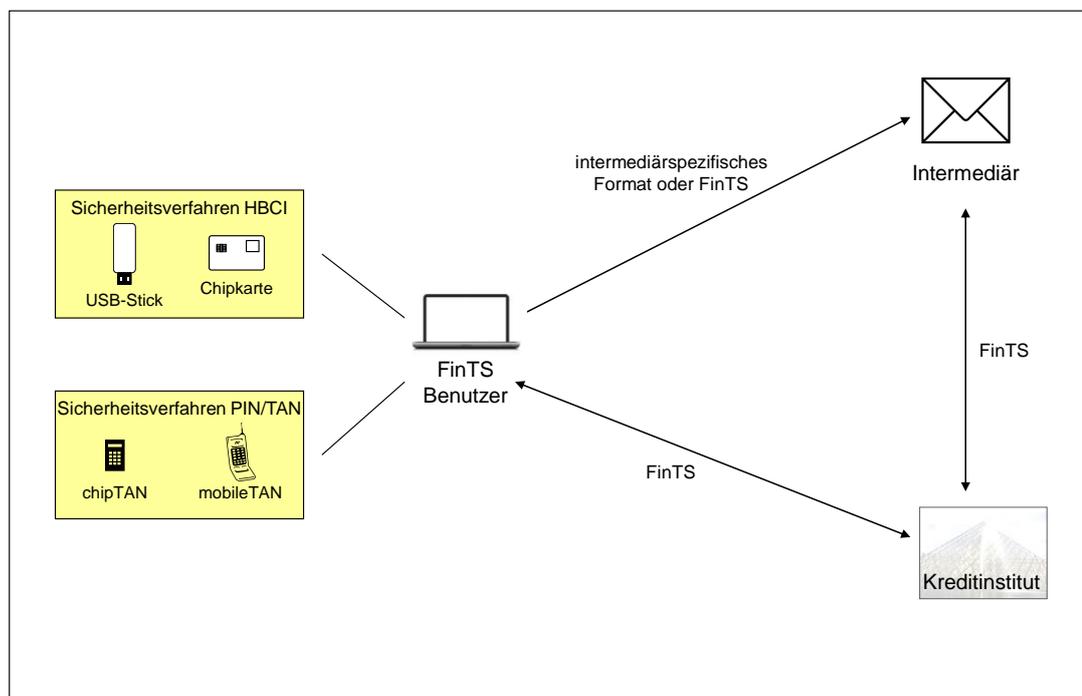


Abbildung 1: Übersicht der Schnittstellenbeziehungen

Im Rahmen dieser Schnittstellenbeschreibung findet grundsätzlich keine Spezifikation von Kunden-, Kreditinstituts- oder Intermediärsystemen statt. Lediglich werden an einigen gekennzeichneten Stellen Empfehlungen für die Präsentation im Kundenprodukt bzw. für die Verarbeitung im Kreditinstituts- oder Intermediärsystem gegeben¹. Diese Ausführungen sind jedoch nicht als Teil der eigentlichen Schnittstellenspezifikation zu verstehen.

¹ Das Symbol  steht für Hinweise an Kundenprodukthersteller. Das Symbol  bezeichnet Implementierungshinweise für Kreditinstitutssysteme. Das Symbol  steht für Hinweise an Intermediärsystemhersteller.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: I
Kapitel: EINLEITUNG Abschnitt: Begriffsbestimmung	Stand: 06.10.2017	Seite: 8

Grundsätzlich ist die Schnittstellenbeschreibung plattform- und endgeräteunabhängig. Ein Teil der Beschreibungen erfordert jedoch Endgeräte mit lokaler Speichereintelligenz.

Die Spezifikation ist als Schichtenstruktur aufgebaut und somit grundsätzlich unabhängig vom zugrunde liegenden Transportmedium. Um eine einheitliche und multibankfähige Schnittstelle zu gewährleisten, werden jedoch hierzu in den Anlagen ([E Transportmedienspezifische Festlegungen]) einige grundsätzliche Festlegungen getroffen.

Für einzelne Teile der Schnittstelle (z. B. Signatur, Verschlüsselung, Komprimierung und Standard-Finanzdatenformate) wird in [Anlagen] auf weitere allgemein zugängliche Spezifikationen verwiesen.

In [Messages] ist eine Vielfalt von Geschäftsvorfällen zwischen Kunde und Kreditinstitut beschrieben. Da hiermit jedoch nicht sämtliche Anforderungen aller beteiligten Kreditinstitute abgebildet werden können, steht es den Verbänden der Deutschen Kreditwirtschaft frei, eigene Geschäftsvorfälle, die in diesem Dokument nicht enthalten sind, zu definieren und anzubieten. Die Klassifizierung in DK-weit definierte und verbandsspezifische Geschäftsvorfälle erfolgt dabei über XML-Namespaces.

Auf die zu verwendenden XML-Namespaces wird in [Syntax] näher eingegangen. Innerhalb eines Namespace werden XML-Tags definiert, ohne mit ggf. in anderen Namespaces definierten Tags gleichen Namens zu Konflikten zu führen.

Die Vergabe und Koordination der DK-weit definierten XML-Tags übernimmt Die Deutsche Kreditwirtschaft. Die Vergabe und Koordination der übrigen XML-Tags übernehmen die jeweiligen Verbände. Interne XML-Tags können von Herstellern bei Bedarf beliebig verwendet werden, haben jedoch keine DK-weite Gültigkeit.

Das XML-basierte FinTS 4.1 ist konsequent auf die Nutzung der im XML-Umfeld bestehenden bzw. sich entwickelnden Standards ausgerichtet. Für die Einbindung der HBCI-Sicherheit greift FinTS 4.1 auf die Standards XML-Signature und XML-Encryption zurück. Für die nahtlose Einbindung der SwiftML-Geschäftsvorfälle ist FinTS4 vorbereitet.

Für weitere Fragen und Informationen zu FinTS wenden Sie sich bitte an die unter www.fints.org in der Rubrik „Impressum“ angegebenen Adressen.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Begriffsbestimmung	Stand: 06.10.2017	Seite: 10

II.12 Nachrichtentypen	59
II.12.1 Unverschlüsselte Nachricht	59
II.12.2 Teilverschlüsselte Nachrichten	60
II.12.3 Verschlüsselte Nachrichten	61
II.12.4 Vorgehensweise beim Signieren und Verschlüsseln	62
II.12.5 Vorgehensweise beim Entschlüsseln und Prüfen der Signaturen	63
II.13 Verschlüsselung der Kommunikation	64
II.14 Komprimierung	66
II.15 Initialisierung	67
II.15.1 Benutzernachricht	67
II.15.1.1 Identifikation	67
II.15.1.2 Verarbeitungsvorbereitung	68
II.15.2 Kreditinstitutsnachricht	69
II.15.2.1 Bankparameterdaten	69
II.15.2.2 User-Parameterdaten	70
II.15.2.3 Übermittlung eines öffentlichen Schlüssels	70
II.15.2.4 Kreditinstitutsmeldung	71
II.15.3 Empfehlung für die Bildung von Kommunikationsreferenzen	71
II.16 Dialogabbruchnachricht	73
II.17 Anonymer Zugang	74
II.17.1 Administrativer Teil	74
II.17.2 Initialisierung	74
II.17.3 Auftragsteil	75

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Begriffsbestimmung	Stand: 06.10.2017	Seite: 11

II.1 Begriffsbestimmung

II.1.1 Nachrichtenelemente

Die folgenden Nachrichtenelemente bezeichnen FinTS Protokollstrukturen. Es handelt sich hierbei jedoch um normale XML-Strukturen. Vor diesem Hintergrund werden die Bezeichnungen Segment, Datenelement und Datenelementgruppe nur zum besseren Verständnis verwendet. Sie verfügen ansonsten aber über keine speziellen Eigenschaften.

◆ Nachrichten

Die Kommunikation zwischen Benutzer und Kreditinstitut erfolgt bei FinTS über das Versenden von Nachrichten. Nachrichten sind die größten im FinTS-Format definierten Datenelementgruppen (DEGs), die selbst nicht mehr als Bestandteil anderer DEGs auftreten. (s. Abbildung 2). Alle Nachrichten (Benutzer an Kreditinstitut und umgekehrt) enthalten ein Nachrichtenkopfsegment. Es können Initialisierungs- und Geschäftsvorfallsegmente (ggf. verschlüsselt, komprimiert und signiert) auf unterschiedlichen Schachtelungsebenen folgen. Es wird zwischen Benutzernachrichten und Kreditinstitutsnachrichten unterschieden, die sich im Detail in ihrem Aufbau unterscheiden. Der allgemeine Nachrichtenaufbau ist in den jeweiligen Kapiteln zu Benutzer- und Kreditinstitutsnachrichten beschrieben (siehe *II.9 Benutzernachrichten allgemein* und *II.10 Kreditinstitutsnachrichten allgemein*).

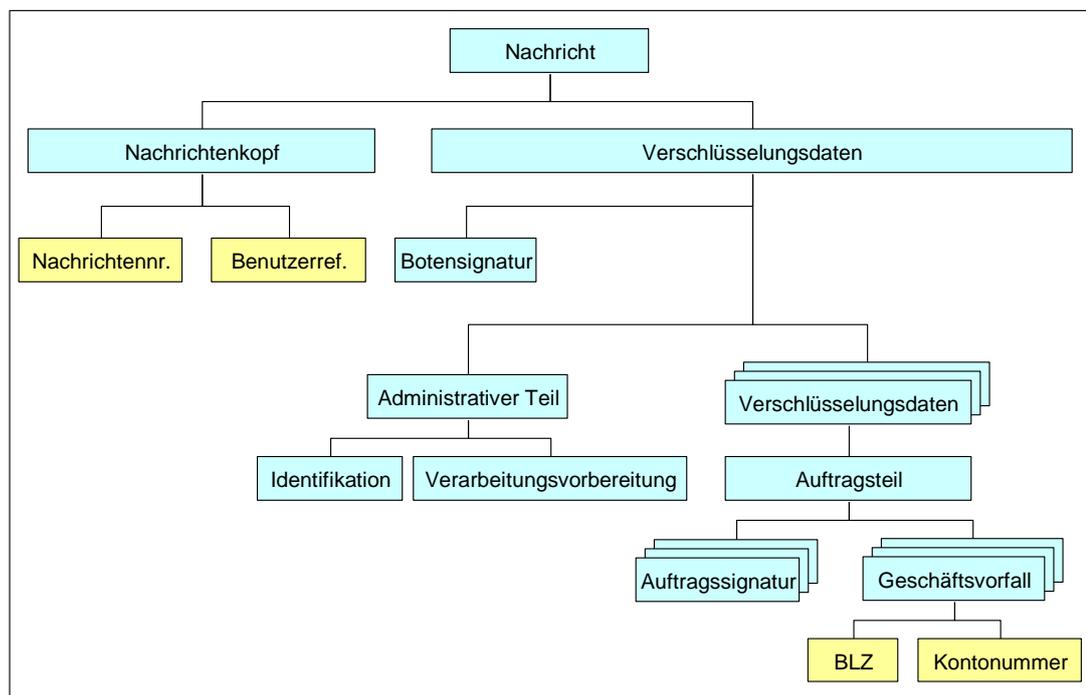


Abbildung 2: Allgemeiner Nachrichtenaufbau

◆ Datenelemente

Datenelemente (DE) sind die kleinsten syntaktischen Informationseinheiten. Sie sind durch einzelne numerische, alphanumerische oder binäre Zeichenreihen gegeben (in Abbildung 2 gelb dargestellt).

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Begriffsbestimmung	Stand: 06.10.2017	Seite: 12

◆ Datenelementgruppen

Zusammengehörende Datenelemente können zu größeren syntaktischen Einheiten zusammengefasst werden. Diese Datenelementgruppen (DEG) bestehen in ihrer einfachsten Form ausschließlich aus einfachen Datenelementen, sie können jedoch auch DEGs enthalten. Jede DEG kann beliebig viele DEs/DEGs enthalten. Eine DEG kann beliebig tief verschachtelt sein (in Abbildung 2 türkis dargestellt).

◆ Segmente

Datenelementgruppen mit einer hervorgehobenen Bedeutung innerhalb des FinTS-Formates können auch als Segment bezeichnet werden. So stellt beispielweise jeder Geschäftsvorfall ein Segment dar. Auch DEGs, die spezielle Header-Informationen enthalten, werden als Segmente bezeichnet (z. B. Nachrichtenkopf und Signatur). Die Bezeichnung einer DEG als Segment hat aber keinerlei syntaktische Bedeutung.

◆ Nachrichtenköpfe

Jede FinTS-Nachricht enthält einen Nachrichtenkopf. Hierbei unterscheidet sich der Nachrichtenkopf einer Benutzernachricht im Aufbau von dem einer Kreditinstitutsnachricht. Ein Nachrichtenkopf ist immer unverschlüsselt und kann daher von jedem eingesehen werden. Er kann jedoch signiert und dadurch vor Veränderungen von außen geschützt sein.

Ein Nachrichtenkopf enthält Steuerinformationen, die der Empfänger der Nachricht für deren Weiterverarbeitung benötigt. Hier sind die Referenzwerte und Nachrichtennummern enthalten, durch die eine Nachricht einer Kommunikation und eine Antwortnachricht der zugehörigen Benutzernachricht zugeordnet werden kann. Weiterhin beinhaltet der Nachrichtenkopf auch Kundenprodukteigenschaften wie z. B. den Produktidentifikator. In einem Datagramm kann hier auch eine alternative asynchrone Rückantwortadresse enthalten sein, an die das Kreditinstitut seine Antwortnachricht senden soll. Es sind jedoch keine Daten enthalten, die Rückschlüsse auf den bankfachlichen Inhalt zulassen, sofern der Rest der FinTS-Nachricht verschlüsselt ist. Der genaue Aufbau eines Nachrichtenkopfes wird in */// AUFTRAGSVERFAHREN* und in [Syntax] beschrieben.

◆ Signatur

Bei Verwendung eines HBCI-Sicherheitsverfahrens kann eine FinTS-Nachricht eine oder mehrere elektronische Signaturen der Herausgeber und Zeugen eines Auftrages sowie zusätzlich des Boten dieser Nachricht enthalten. Für jede dieser elektronischen Signaturen ist ein sogenanntes Signatur-Segment (kurz Signatur) vorhanden.

In einer Signatur sind alle Daten enthalten, die für die Verarbeitung der elektronischen Signatur notwendig sind. Diese können sich je nach verwendetem Sicherheitsverfahren in Aufbau und Umfang voneinander unterscheiden. Bei Mehrfachsignaturen ist deren Reihenfolge innerhalb der Nachricht ohne Bedeutung. Auch sind die Signaturen in beliebiger Reihenfolge verifizierbar.

Der genaue Inhalt einer Signatur ist in [HBCI], Abschnitt *II.5.1 Signatur-Segment* näher beschrieben. Der genaue Aufbau einer Signatur wird in [Syntax] beschrieben.

◆ Secoder

Wird im Rahmen eines Signaturverfahrens ein Secoder als empfohlener Chipkartenleser der Deutschen Kreditwirtschaft im Sogenannten Applikationsmodus eingesetzt, handelt es sich auch in FinTS um ein spezielles Sicherheitsverfahren mit zusätzlichen Rahmenbedingungen, speziell zum Visualisieren der Daten. Zudem kann

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Begriffsbestimmung	Stand: 06.10.2017	Seite: 13

bei Verwendung eines Secoders zusätzlich eine Visualisierungsbestätigungssignatur angefügt werden.

◆ **OneTimePassword**

Wird anstelle eines HBCI-Sicherheitsverfahrens das PIN/TAN-Verfahren verwendet, so werden anstelle von Signaturen OneTimePassword-Segmente in die Nachricht eingestellt.

In einem OneTimePassword sind alle Daten enthalten, die für die Verarbeitung des PIN/TAN-Verfahrens notwendig sind.

Der genaue Inhalt eines OneTimePasswords ist in [PINTAN] näher beschrieben. Der genaue Aufbau eines OneTimePasswords wird in [Syntax] beschrieben.

◆ **UserDefinedSignature**

Anstelle der obigen Sicherheitsverfahren können zwischen Benutzer und Kreditinstitut auch bilateral vereinbarte Verfahren eingesetzt werden. Hierzu sind statt der obigen Segmente UserDefinedSignature-Segmente in die Nachricht einzustellen.

Der tatsächliche Aufbau dieser Segmente hängt vom zwischen Benutzer und Kreditinstitut vereinbarten Verfahren ab und kann daher hier nicht näher festgelegt werden. In [Syntax] ist jedoch beschrieben, wie die für das jeweilige Verfahren benötigten Daten in die UserDefinedSignature einzubetten sind.

◆ **Verschlüsselungsdaten**

Eine FinTS-Nachricht kann an verschiedenen Stellen verschlüsselte Daten enthalten. Bei diesen Daten kann es sich um eine Folge von signierten bankfachlichen Aufträgen handeln oder um eine komplette FinTS-Nachricht, welche dann zusätzlich zu den bankfachlichen Aufträgen administrative Segmente und eine Botensignatur enthalten kann.

Verschlüsselte Daten werden immer in ein Verschlüsselungsdaten-Segment eingebettet, welches darüber hinaus alle Daten enthält, die für die Verarbeitung der Verschlüsselung notwendig sind. Diese können sich je nach verwendetem Sicherheitsverfahren in Aufbau und Umfang voneinander unterscheiden.

Der genaue Inhalt der Verschlüsselungsdaten ist in [HBCI], Abschnitt *II.5.2 Verschlüsselungsdaten* näher beschrieben. Der genaue Aufbau der Verschlüsselungsdaten wird in [Syntax] beschrieben.

◆ **Kommunikationsreferenzen**

Eine FinTS-Nachricht enthält in ihrem Nachrichtenkopf Referenzwerte, welche vom Benutzer und dem Kreditinstitut vergeben werden und zur eindeutigen Zuordnung der Nachricht zu einer Kommunikation dienen. Hierbei bilden Kunden- und Kreditinstitutsseite unabhängig voneinander ihre Referenzwerte. Wie diese Werte erzeugt werden können, wird in *II.15.3 Empfehlung für die Bildung von Kommunikationsreferenzen* näher beschrieben.

II.1.2 **Kommunikation**

Die Kommunikation zwischen Benutzer und Kreditinstitut besteht aus Benutzernachrichten und zugehörigen Kreditinstitutsnachrichten, die jeweils nach den Vorschriften von FinTS aufgebaut sind.

Zur Gruppierung von Nachrichten innerhalb einer Kommunikation wird vom Kundensystem eine eindeutige Benutzerreferenz vergeben. Die Nachrichten innerhalb einer Kommunikation werden zusätzlich mit einer Nachrichtennummer versehen. Zu jeder Benutzernachricht existiert eine Kreditinstitutsnachricht mit der gleichen Nach-

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Begriffsbestimmung	Stand: 06.10.2017	Seite: 14

richtennummer. Das Senden einer Kreditinstitutsnachricht ist immer auf eine zuvor vom Kreditinstitut erhaltene Benutzernachricht zurückzuführen.

Die Kommunikation zwischen Benutzer und Kreditinstitut kann synchron oder asynchron erfolgen.

◆ **Dialoge**

Innerhalb eines Dialogs wartet der Benutzer nach dem Senden einer Nachricht immer auf den Empfang der zugehörigen Kreditinstitutsnachricht, bevor er seine nächste Nachricht versendet (synchrone Kommunikation). Hierdurch ist die Reihenfolge, in der die Nachrichten eines Dialogs beim Empfänger eintreffen, immer wohldefiniert. Nachrichten können vorhergehende Nachrichten auf dem Transportweg nicht überholen.

Bei der Kommunikation in einem Dialog müssen Nachrichten des Kundensystems eine gleiche eindeutige Benutzerreferenz enthalten. Weiterhin müssen die Benutzernachrichten bei 1 beginnend in Einerschritten durchnummeriert sein. Die erste Nachricht des Kundensystems muss eine sogenannte Initialisierung enthalten. Das Kreditinstitut teilt in der Antwortnachricht auf die Initialisierung durch das Kundenprodukt seinerseits eine Referenznummer mit, die den Dialog auf Kreditinstitutsseite eindeutig identifiziert. Auch diese Kreditinstitutsreferenz bleibt während des gesamten Dialogs konstant und muss in Folgenachrichten des Kundensystems angegeben werden.

◆ **Datagramme**

Bei der Kommunikation über Datagramme enthält jedes vom Kundensystem gesendete Datagramm eine Initialisierung. Die Benutzerreferenz kann einen beliebigen Wert annehmen, sollte jedoch eindeutig sein. Die Nachrichtennummer muss immer 1 sein. In jedem Datagramm vermerkt das Kundensystem, dass die Kommunikation nach Verarbeitung des Datagramms beendet werden soll. Die Kreditinstitutsreferenz wird in der Antwortnachricht des Kreditinstituts zurückgemeldet, hat aber keine weitere Bedeutung, da keine Folgenachricht durch das Kundensystem versendet wird. Der Benutzer darf in keines seiner Datagramme eine Kreditinstitutsreferenz einstellen.

II.1.3 **Benutzer und Kunde**

Die Identifizierung des Benutzers sowie die Festlegung der Rechte, die einem Benutzer im Rahmen einer FinTS-Kommunikation offen stehen, erfolgt in FinTS anhand der Begriffe 'Benutzer' und 'Kunde' bzw. anhand der zugeordneten Identifikationsmerkmale 'Benutzerkennung' und 'Kunden-ID'.

Weiterhin besteht für einen Benutzer die Möglichkeit, Nachrichten nicht direkt mit einem Kreditinstitut auszutauschen, sondern über eine dritte Partei als Vermittler. Diese dritte Partei wird im Weiteren als 'Intermediär' bezeichnet.

Zu den genannten Begriffen sind folgende Unterscheidungen zu treffen:

Benutzer

Ein Benutzer ist eine natürliche Person, die als Inhaber oder Berechtigter (z. B. Bevollmächtigter) eines Kontos über ein Kundenprodukt/-endgerät am FinTS-Verfahren teilnimmt. Jeder Benutzer kann von seinem Kreditinstitut User-Parameterdaten erhalten, in denen er über seine Rechte im Rahmen des FinTS-Verfahrens informiert wird. Dem Kreditinstitut gegenüber tritt der Benutzer als Inhaber eines Sicherheitsmediums auf.

Die Identifizierung des Benutzers erfolgt anhand des DE Benutzerkennung.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Begriffsbestimmung	Stand: 06.10.2017	Seite: 15

Kunde

Neben dem allgemeinen Gebrauch des Kundenbegriffs in Abgrenzung zum Kreditinstitut kann der Begriff 'Kunde' optional dazu verwendet werden, eine kreditinstitutsindividuelle Differenzierung eines Benutzers zu ermöglichen, um die Rolle, in der er auftritt, zu spezifizieren. So lässt sich zum Beispiel unterscheiden, ob ein Benutzer die Kommunikation in der Eigenschaft als Privatperson oder als Bevollmächtigter einer Firma führen möchte (siehe *Abbildung 3: Benutzer, mehreren Kunden zugeordnet*). Durch die Rolle werden die Rechte festgelegt, die dem Benutzer während einer FinTS-Kommunikation zur Verfügung stehen.

Die Identifizierung des 'Kunden', bzw. der Rolle, in welcher der Benutzer auftritt, kann anhand des DE Kunden-ID erfolgen, d.h. die Benutzererkennung in Zusammenhang mit der Kunden-ID legt eindeutig die Rolle fest, in der ein Benutzer gegenüber dem Kreditinstitut auftritt

Es steht dem Kreditinstitut jedoch frei, dem Benutzer für jede Rolle eine eigene Benutzererkennung und ggf. auch ein separates Sicherheitsmedium zur Verfügung zu stellen. Diese Rolle muss nicht zwingend über eine eigene Kunden-ID im FinTS-System festgelegt werden. Bei Gleichheit von Benutzererkennung und Kunden-ID im FinTS-System wird die Rolle des Benutzers im nachgelagerten operativen System festgelegt. Sie entscheidet sich durch die Verknüpfungen zwischen Benutzererkennung und 'interner' Kundennummer und den dazugehörigen Konten mit ihren jeweiligen Vollmachten.

Der Kundenbezug gilt immer für den gesamten Kommunikationskontext, d. h. für sämtliche Benutzer, die im Rahmen der Kommunikation als Signierende auftreten (d. h. auch für eventuelle Zweit- und Drittsignierende).



Da Kunden-ID und Benutzererkennung voneinander abweichen können, ist im Kundenprodukt eine Eingabemöglichkeit für die Kunden-ID vorzusehen.

Im Einzelnen sind folgende Belegungsvarianten für Benutzererkennung und Kunden-ID möglich:

- Benutzererkennung und Kunden-ID sind identisch:

In diesem Fall wird kreditinstitutsseitig keine logische Differenzierung zwischen Kunde und Benutzer vorgenommen. Die Benutzererkennung wird in das Feld 'Kunden-ID' eingestellt. Die Rolle des Benutzers ergibt sich, wie oben dargestellt, erst im nachgelagerten System.

- Benutzererkennung und Kunden-ID sind nicht identisch:

Es wird kreditinstitutsseitig eine logische Differenzierung zwischen Kunde und Benutzer vorgenommen, um die Rolle festzulegen, in welcher der Benutzer auftritt.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Begriffsbestimmung	Stand: 06.10.2017	Seite: 16

Die folgenden Abbildungen gelten für den Fall, dass die Kunden-ID genutzt wird, um die Rolle des Benutzers festzulegen:

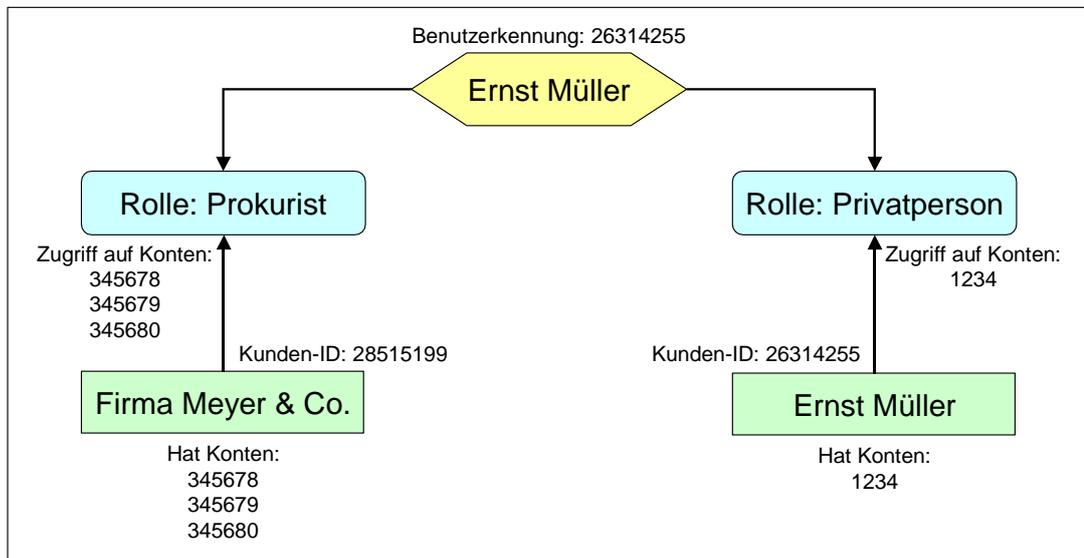


Abbildung 3: Benutzer, mehreren Kunden zugeordnet

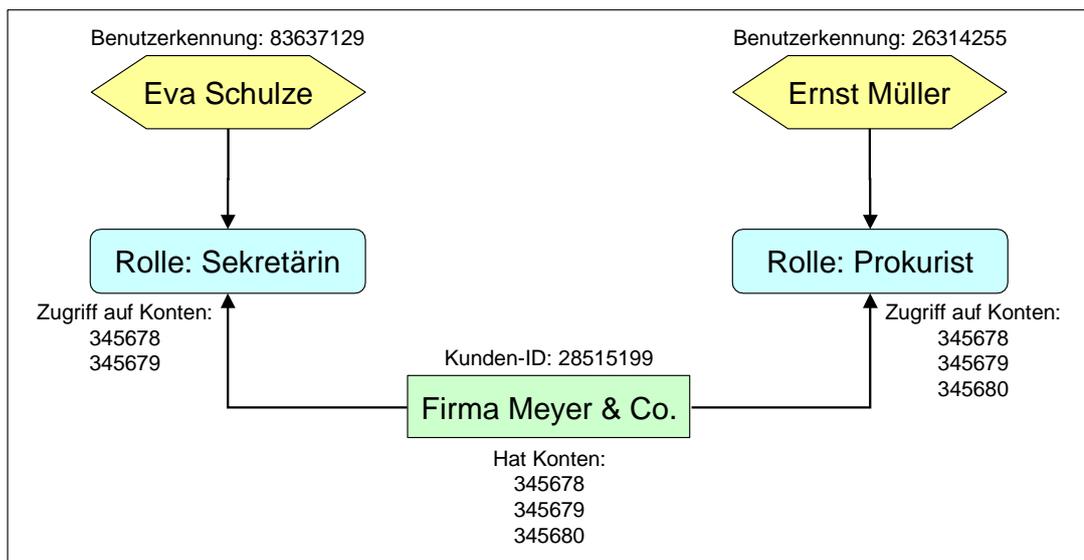


Abbildung 4: Kunde, mehreren Benutzern zugeordnet

Bote

Benutzer, welcher den Dialog mit dem Kreditinstitut führt. Er führt die administrativen Vorgänge innerhalb der Kommunikation mit dem Kreditinstitut durch.

Der Bote kann auch der Herausgeber des Auftragsteils der Nachricht sein, muss dies jedoch nicht. Im letzteren Fall hat der Bote nicht die Berechtigung, die im Auftragsteil enthaltenen Aufträge auszuführen. Diese müssen daher vom Herausgeber der Aufträge signiert sein, welcher die Berechtigung haben muss. Der Bote ist hier nur der Überbringer der Aufträge.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Begriffsbestimmung	Stand: 06.10.2017	Seite: 17

Der Bote muss keine Kenntnis über den Inhalt eines Auftragsteils besitzen. Der Herausgeber kann diesen somit auch verschlüsseln und so vor Einsicht durch den Boten schützen.

Herausgeber

Benutzer, welcher den Auftragsteil einer Benutzernachricht signiert und ggf. auch verschlüsselt.

Der Herausgeber kann auch Bote der Nachricht sein. In diesem Fall muss er den Auftragsteil nicht gesondert signieren, sondern braucht nur seine Botensignatur zu erstellen, die den Auftragsteil mitsigniert.

Zeuge

Benutzer, welcher zusätzlich zum Herausgeber den Auftragsteil einer Benutzernachricht signiert. Seine Signatur ist genau dann von Nöten, wenn der Herausgeber allein nicht die Berechtigung besitzt, die Aufträge im Auftragsteil auszuführen.

Intermediär

Neben der direkten Kommunikation zwischen Benutzer und Kreditinstitut können Nachrichten über einen Intermediär ausgetauscht werden, siehe *II.3.2 Kommunikation über Intermediär*.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Syntaktische Festlegungen	Stand: 06.10.2017	Seite: 18

II.2 Syntaktische Festlegungen

◆ Datenformate

Das FinTS-Format legt eine Reihe von DE-Typen für numerische, alphanumerische oder binäre Werte fest. Nur diese Elementtypen dürfen für den Aufbau von Nachrichten verwendet werden. (siehe hierzu [Syntax])

◆ Status und Anzahl

Das FinTS-Format legt für jedes Vorkommen eines DE bzw. einer DEG fest, wie oft dieses auftreten darf, ob es vorkommen muss oder weggelassen werden kann. Wenn mit der Angabe eine Bedingung verknüpft ist, wann das Element angegeben werden muss, weggelassen werden kann oder nicht angegeben werden darf, wird dies unter Belegung textuell beschrieben, da diese durch die XML-Schematechnik nicht erfasst werden.

◆ Restriktionen

Durch Restriktionen können die Werte, die eine Datenstruktur annehmen kann, oder die Bedingung, unter denen eine Datenstruktur auftreten kann, näher spezifiziert werden. Für die XML-Syntax werden Restriktionen im XML-Schema beim jeweiligen Element aufgeführt. Diese können sein:

- Zulässige Werte (insbesondere beim Datentyp ‚code‘)
- Wertebereiche (z. B. > 100)

Nicht vollständig im XML-Schema abgebildet werden können:

- konditionale Belegungsregeln

Konditionale Belegungsregeln werden insbesondere in [Messages] für Datenstrukturen mit dem Status „konditional“ aus Geschäftsvorfall-Segmenten angewendet. In diesem Fall beschreibt die Restriktion, unter welcher Bedingung das Element welchen Status annimmt bzw. welcher Wertebereich zulässig ist.

◆ Längenangaben

Für einige der zulässigen DE-Typen ist definiert, wie lang ein gültiger Wert sein kann oder muss. Für diejenigen DE-Typen, für die diese Längenangaben noch nicht festgelegt worden sind, wird dies je Vorkommen getan. Es kann eine Maximallänge, eine exakt einzuhaltende Länge oder eine beliebige Länge ohne Beschränkung definiert werden. (siehe hierzu [Syntax])

◆ Transparente Daten

Das FinTS-Format bietet die Möglichkeit, Fremdformate in das FinTS-Format einzubetten. Diese Fremdformate haben keinerlei Bedeutung für das eigentliche FinTS-Format und werden daher bei der Verarbeitung des eigentlichen FinTS-Formats nicht weiter beachtet. Ihre Struktur ist für die FinTS-verarbeitenden Schichten transparent. (siehe hierzu [Syntax])

◆ Datums- und Uhrzeitangaben

Generell besitzen Datums- und Uhrzeitangaben, die von Kundensystemen automatisch generiert werden (z. B. Zeitpunkt der Signatur), keinen rechtsverbindlichen Charakter, da nicht davon ausgegangen werden kann, dass Kundensysteme diese Daten korrekt erzeugen.

Datum und Uhrzeit, die vom Kundensystem gesendet werden, besitzen somit keine verarbeitungstechnische Bedeutung, sondern lediglich dokumentarischen Charakter. Dies bezieht sich nicht auf Datums- und Uhrzeitangaben, die vom Benutzer

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Syntaktische Festlegungen	Stand: 06.10.2017	Seite: 19

selbst eingegeben werden (z. B. Ausführungsdatum von terminierten Überweisungen).

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Kommunikationsszenarien	Stand: 06.10.2017	Seite: 20

II.3 Kommunikationsszenarien

Dieser Abschnitt beschreibt die beiden möglichen Kommunikationsszenarien für FinTS: die direkte Kommunikation zwischen Benutzer und Kreditinstitut sowie die Kommunikation über einen Intermediär.

II.3.1 Direkte Kommunikation

Bei der direkten Kommunikation unterhält der Benutzer eine direkte Kommunikation mit seinem Kreditinstitut im FinTS-Protokoll.

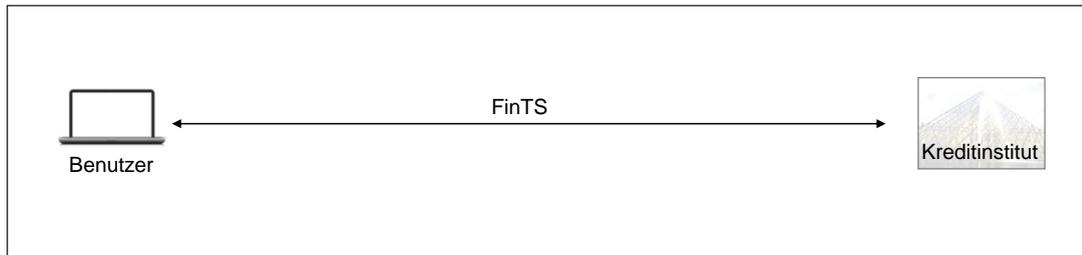


Abbildung 5: Direkte Kommunikation

II.3.2 Kommunikation über Intermediär

Neben der direkten Kommunikation zwischen Benutzer und Kreditinstitut können Nachrichten über einen Intermediär ausgetauscht werden. Je nach Einsatzszenario kann der Intermediär in verschiedenen Rollen auftreten. Allen Szenarien gemein ist, dass der Intermediär stets die technische Schnittstelle zwischen Benutzer und Kreditinstitut bildet. Darüber hinaus kann der Intermediär die Rolle einer fachlichen Schnittstelle einnehmen.

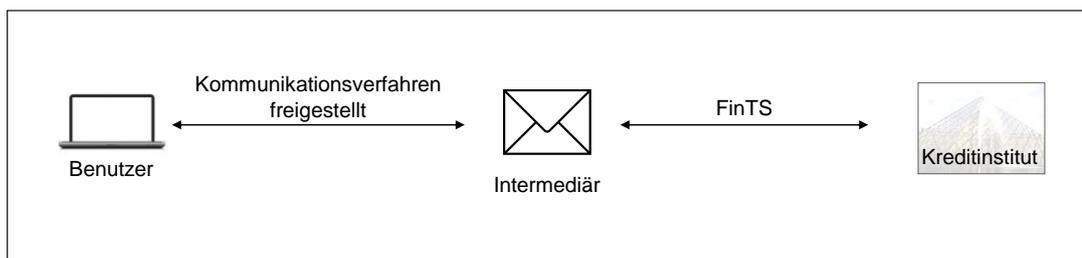


Abbildung 6: Kommunikation unter Einbeziehung eines Intermediärs

Das Kommunikationsprotokoll zwischen Benutzer und Intermediär kann in allen Szenarien beliebig vereinbart werden. Zwischen Intermediär und Kreditinstitut wird das FinTS-Protokoll zum Nachrichtenaustausch verwendet. Daher muss der Intermediär gegebenenfalls die vom Benutzer erhaltenen Aufträge in FinTS-Form umwandeln und an das Kreditinstitut weitergeben. Die vom Kreditinstitut erhaltenen Antworten bereitet der Intermediär so auf, dass das Kundenprodukt die Antworten interpretieren kann.

Die Kommunikation zwischen Intermediär und Kreditinstitut läuft verschlüsselt ab. Dabei kann sowohl eine FinTS-konforme Verschlüsselung als auch eine Transportverschlüsselung zum Einsatz kommen.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Kommunikationsszenarien	Stand: 06.10.2017	Seite: 21

Zur Verdeutlichung der möglichen Rollen eines Intermediärs werden im Folgenden vier Szenarien betrachtet, in denen ein Benutzer nicht direkt mit einem Kreditinstitut Nachrichten austauscht, sondern eine dritte Partei, der Intermediär, als Vermittler zwischen Kreditinstitut und Benutzer fungiert.

II.3.2.1 Szenario A (Intermediär als Herausgeber)

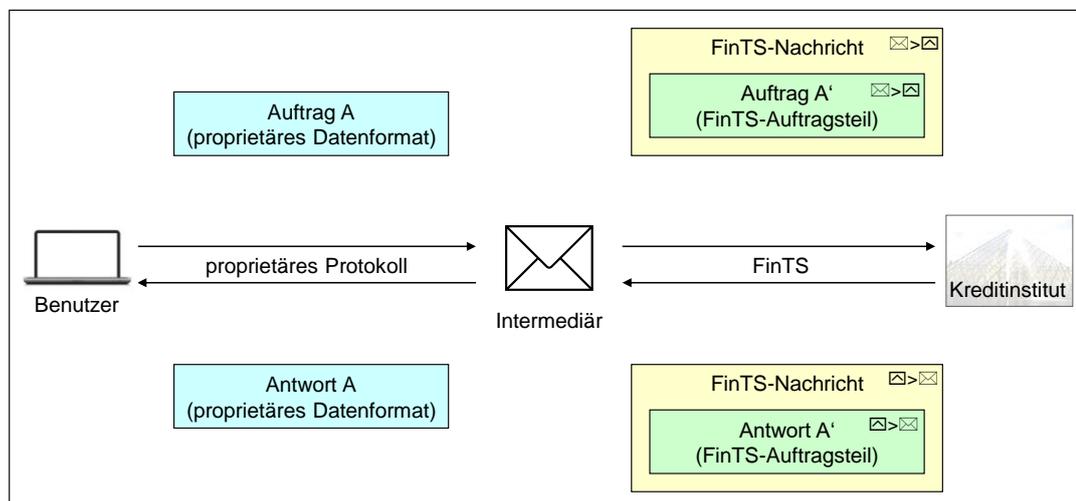


Abbildung 7: Intermediärszenario A

In diesem Szenario erhält der Intermediär vom Benutzer alle notwendigen Informationen, um eine FinTS-Nachricht an das Kreditinstitut aufzubauen. Der Intermediär baut die FinTS-Nachricht auf und signiert sie im Auftrag des Benutzers. Im Allgemeinen werden die gleichen Schlüssel für alle Benutzer verwendet. Der Intermediär hat in diesem Szenario die Rollen des Herausgebers und des Boten. Der Intermediär tritt dem Kreditinstitut gegenüber als normaler Benutzer auf.

Das Kreditinstitut signiert die Antwortnachricht an den Intermediär und verschlüsselt sie so, dass nur der Intermediär die Antwortnachricht entschlüsseln kann. Der Intermediär setzt die Antwortnachricht des Kreditinstituts in das Nachrichtenformat um, das für die Kommunikation zwischen Intermediär und Benutzer verwendet wird, und sendet die Antwortnachricht an den Benutzer. Das Kundenprodukt benötigt in diesem Szenario keine Kenntnisse des FinTS-Protokolls.

Dem Intermediär stehen die User-Parameterdaten (UPD) des Benutzers zur Verfügung, da er selbst als dieser Benutzer auftritt. Der Intermediär kann dem Benutzer ein Menü anbieten, das an die für ihn erlaubten Geschäftsvorfälle angepasst ist. Dieser Komfort bedingt jedoch, dass der Intermediär Einsicht in gegebenenfalls private Daten des Benutzers hat (siehe auch *V.5 UPD des Benutzers für Intermediärzugang (UPDI)*).

Außerdem signiert der Intermediär die Aufträge rechtlich bindend im Auftrag und im Namen des Benutzers. Der Intermediär erlangt in dieser Rolle die volle Verfügungsberechtigung des Auftrag gebenden Kunden im Rahmen der verwendeten Benutzer-ID. Im Vorfeld muss deshalb ein kontobezogenes Rechtsverhältnis zwischen Intermediär und Benutzer geschaffen werden. Handelt der Intermediär im Auftrag des Kreditinstituts, kann das Rechtsverhältnis zwischen Kreditinstitutskunde und Kreditinstitut den Intermediär gegebenenfalls mit einschließen, indem das Kreditinstitut gegenüber seinem Kunden in die Verantwortung tritt.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Kommunikationsszenarien	Stand: 06.10.2017	Seite: 22

Der Benutzer trägt in diesem Szenario das Risiko, dass er eventuelle Korruptionen seiner Aufträge nicht zeitnah erkennen kann, wenn er seine Transaktionen ausschließlich über den Intermediär übermittelt. Der Benutzer steht somit in der Verpflichtung, die korrekte Ausführung seiner Transaktionen regelmäßig über einen alternativen Weg zu kontrollieren.

II.3.2.2 Szenario B (Intermediär als PIN/TAN-Überbringer)

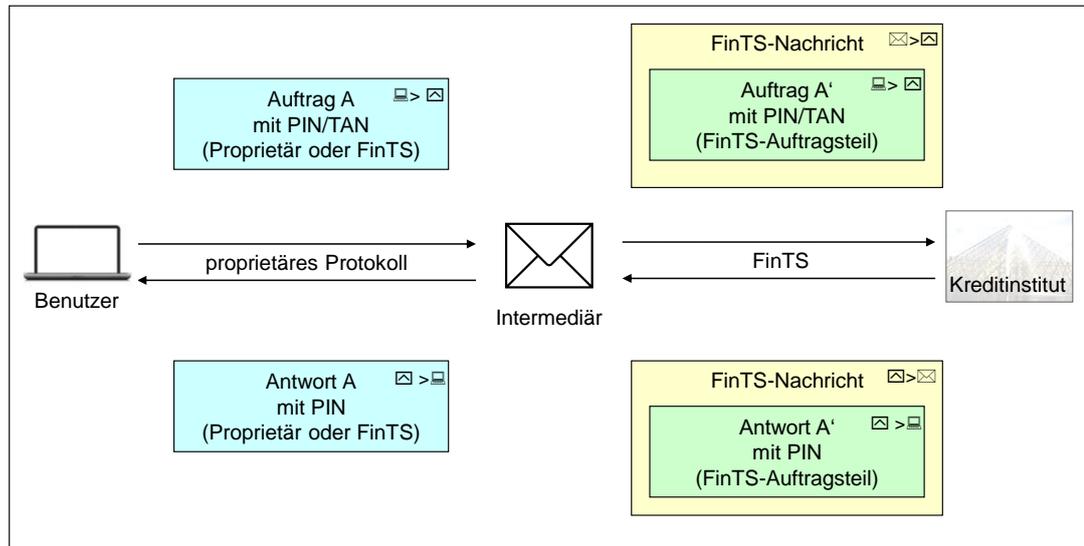


Abbildung 8: Intermediärszenario B

In diesem Szenario erhält der Intermediär vom Benutzer wie in Szenario A alle notwendigen Informationen, um eine FinTS-Nachricht an das Kreditinstitut aufzubauen. Zusätzlich überträgt der Benutzer aber auch seine PIN und ggf. eine TAN an den Intermediär.

Der Intermediär baut eine FinTS-Nachricht auf und fügt den Auftrag des Benutzers in diese ein. Er erstellt eine Auftragssignatur des Benutzers mit dessen PIN und ggf. der TAN. Er selbst signiert die Nachricht als Bote.

Der Intermediär hat Zugriff auf die UPD des Benutzers, wenn er zu deren Abfrage beim Kreditinstitut berechtigt ist (siehe V.6 *Explizite Anforderung von UPD*). Nur in diesem Fall kann der Intermediär dem Benutzer ein Menü anbieten, das an die für ihn erlaubten Geschäftsvorfälle angepasst ist. Gleiches gilt für den Benutzer selbst, der nun nicht mehr als Bote auftritt und somit seine UPD explizit über einen dafür vorgesehenen GV anzufordern hat. Darüber hinaus tritt der Intermediär als eigenständiger Benutzer auf, der als solcher Zugriff auf seine eigene UPD hat (siehe V.4 *UPD des Intermediärs (IPD)*).

Das Kreditinstitut signiert die Antwortnachricht an den Intermediär und verschlüsselt sie so, dass nur der Intermediär die Antwortnachricht entschlüsseln kann. Der Intermediär setzt die Antwortnachricht des Kreditinstituts in das Nachrichtenformat um, das für die Kommunikation zwischen Intermediär und Benutzer verwendet wird, und sendet die Antwortnachricht an den Benutzer. Das Kundenprodukt benötigt in diesem Szenario weiterhin keine Kenntnisse des FinTS-Protokolls, kann wahlweise die Aufträge aber auch bereits im FinTS-Format anliefern.

Der Intermediär tritt in diesem Szenario selbst nicht mehr als der Herausgeber der Aufträge auf. Im Gegensatz zu Szenario A erhält der Intermediär hier also nicht die Verfügungsberechtigung des Auftrag gebenden FinTS-Benutzers. Dennoch trägt der

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Kommunikationsszenarien	Stand: 06.10.2017	Seite: 23

Benutzer aufgrund der Verwendung des PIN/TAN-Verfahrens das Risiko, dass er eventuelle Korruptionen seiner Aufträge nicht zeitnah erkennen kann, wenn er seine Transaktionen ausschließlich über den Intermediär übermittelt. Der Benutzer steht somit in der Verpflichtung, die korrekte Ausführung seiner Transaktionen regelmäßig über einen alternativen Weg zu kontrollieren.

Ein bindendes Rechtsverhältnis zwischen Intermediär und Benutzer ist in diesem Szenario nicht zwingend notwendig. Zwischen Kreditinstitut und Intermediär muss jedoch ein Rechtsverhältnis bestehen, da der Intermediär dem Kreditinstitut gegenüber als Benutzer und damit als Inhaber eines Sicherheitsmediums auftritt.

Das Kreditinstitut kann anhand der Benutzererkennung, die innerhalb der Botensignatur übermittelt wird, den Intermediär als solchen erkennen. Hierüber kann das Kreditinstitut dem Intermediär den Sonderstatus einräumen, Aufträge unter der FinTS-Kunden-ID des Benutzers als Bote einzureichen. Alternativ kann das Kreditinstitut der Benutzererkennung des Intermediärs eine Vollmacht zu allen zugelassenen Auftraggeberkonten einräumen.

II.3.2.3 Szenario C (Intermediär als Überbringer mit HBCI-Sicherheit)

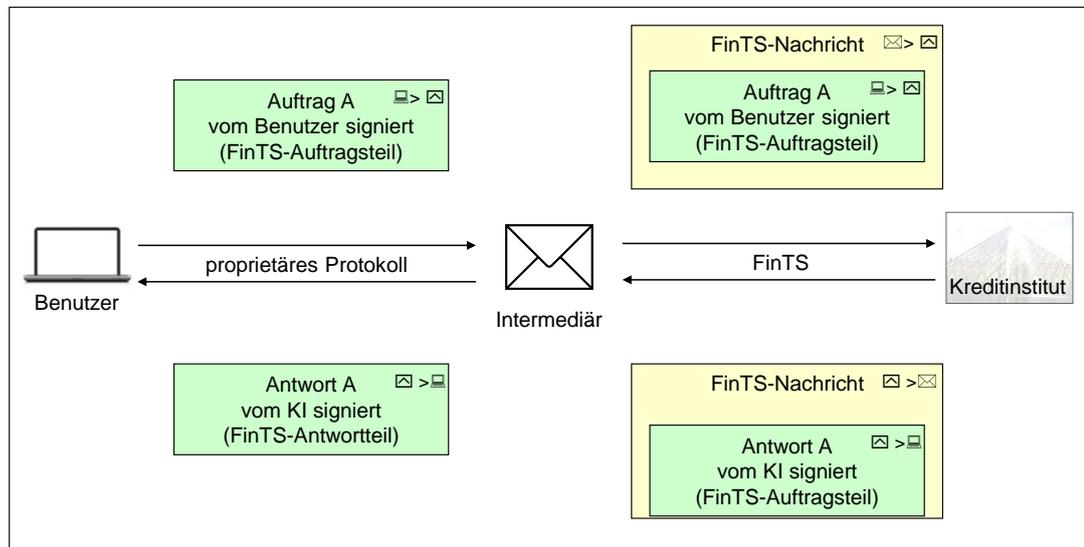


Abbildung 9: Intermediärszenario C

In diesem Szenario baut der Benutzer einen oder mehrere FinTS-Aufträge in Form eines FinTS-Auftragsteils auf und signiert diese als Herausgeber unter Verwendung eines HBCI-Sicherheitsverfahrens (siehe [HBCI]). Die Nachricht des Benutzers wird an den Intermediär übertragen. Zum Nachrichtenaustausch wird ein proprietäres Protokoll verwendet, das zwischen Benutzer und Intermediär vereinbart ist.

Der Intermediär kann auch mehrere Auftragsteile von verschiedenen Benutzern entgegennehmen und in dieselbe Nachricht einstellen.

Der Intermediär nimmt den vom Benutzer erstellten und als Herausgeber signierten FinTS-Auftragsteil entgegen. An dieser Stelle kann der Intermediär die Signatur des Benutzers prüfen, um sicherzugehen, dass der Einreicher des Auftragsteils wirklich der angegebene Benutzer ist. Der Intermediär fügt den Auftragsteil des Benutzers in eine selbst erzeugte FinTS-Nachricht ein, signiert diese Nachricht als Bote, verschlüsselt sie und übermittelt sie an das Kreditinstitut. Das Kreditinstitut verarbeitet den Auftrag und gibt die Antwortnachricht FinTS-konform verschlüsselt an den Intermediär zurück. Der Intermediär entschlüsselt die Antwortnachricht und leitet die

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Kommunikationsszenarien	Stand: 06.10.2017	Seite: 24

zum Auftrag des Benutzers gehörenden Antwortdaten über das proprietäre Protokoll an den Benutzer weiter. Der Benutzer kann nun seinerseits anhand der Signatur prüfen, ob die Antwort wirklich vom Kreditinstitut kommt.

Der Intermediär hat Zugriff auf die UPD des Benutzers, wenn er zu deren Abfrage beim Kreditinstitut berechtigt ist (siehe *V.6 Explizite Anforderung von UPD*). Nur in diesem Fall kann der Intermediär dem Benutzer ein Menü anbieten, das an die für ihn erlaubten Geschäftsvorfälle angepasst ist. Gleiches gilt für den Benutzer selbst, der nun nicht mehr als Bote auftritt und somit seine UPD explizit anzufordern hat. Darüber hinaus tritt der Intermediär als eigenständiger Benutzer auf, der als solcher Zugriff auf seine eigene UPD hat (siehe *V.4 UPD des Intermediärs (IPD)*).

Im Gegensatz zu Szenario A erhält der Intermediär nicht die Verfügungsberechtigung des Auftrag gebenden FinTS-Benutzers. Da dieser als Herausgeber mit einem HBCI-Sicherheitsverfahren signiert, können sowohl Kreditinstitut als auch Benutzer die Unversehrtheit und Authentizität der Aufträge sicherstellen. Allerdings erlangt der Intermediär auch hier wie in den Szenarien A und B Kenntnis von den Aufträgen seiner Kunden, so dass Benutzer nur dann diesen Weg wählen sollten, wenn sie dem Intermediär vertrauen.

Ein bindendes Rechtsverhältnis zwischen Intermediär und Benutzer ist wie in Szenario B nicht zwingend notwendig. Zwischen Kreditinstitut und Intermediär muss jedoch ein Rechtsverhältnis bestehen, da der Intermediär dem Kreditinstitut gegenüber als Benutzer und damit als Inhaber eines Sicherheitsmediums auftritt.

Wie in Szenario B kann das Kreditinstitut anhand der Benutzererkennung, die innerhalb der Botensignatur übermittelt wird, den Intermediär als solchen erkennen. Hierüber kann das Kreditinstitut dem Intermediär den Sonderstatus einräumen, Aufträge unter der FinTS-Kunden-ID des Benutzers als Bote einzureichen. Alternativ kann das Kreditinstitut der Benutzererkennung des Intermediärs eine Vollmacht zu allen zugelassenen Auftraggeberkonten einräumen.

II.3.2.4 Szenario D (Intermediär als Überbringer mit HBCI-Sicherheit, verschlüsselt)

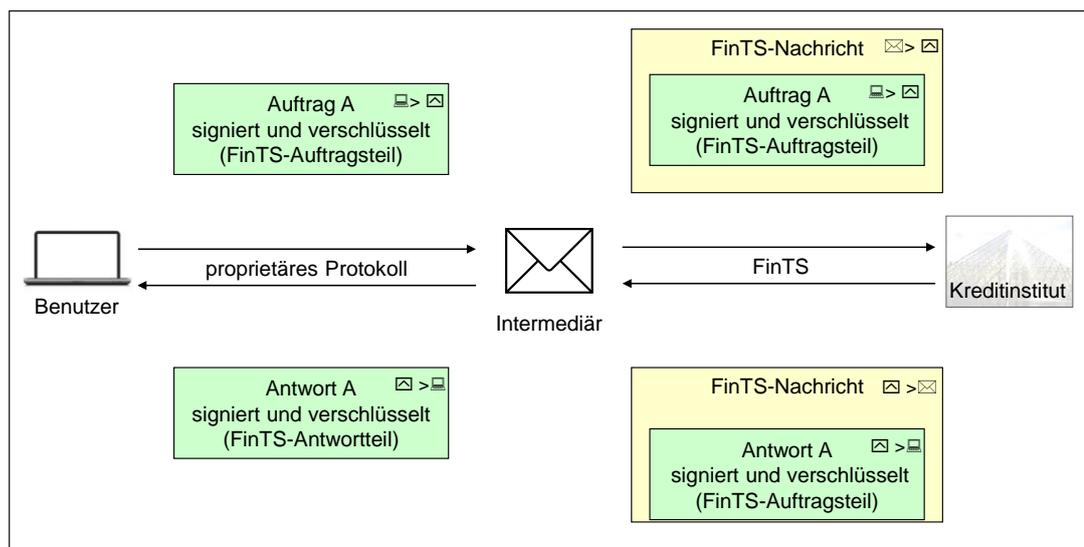


Abbildung 10: Intermediärszenario D

Wie in Szenario C baut der Benutzer in diesem Szenario einen oder mehrere FinTS-Aufträge, die an das Kreditinstitut gesendet werden sollen, in Form eines FinTS-Auftragsteils auf und signiert diesen als Herausgeber mit Hilfe eines HBCI-

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Kommunikationsszenarien	Stand: 06.10.2017	Seite: 25

Sicherheitsverfahrens (siehe [HBCI]). Der FinTS-Auftragsteil wird zusätzlich mit dem gleichen Sicherheitsverfahren verschlüsselt, bevor er an den Intermediär gesendet wird. Der Intermediär erlangt folglich keine Kenntnis vom Inhalt des erhaltenen Auftragsteils.

Wie in Szenario C kann der Intermediär auch mehrere Auftragsteile in dieselbe Nachricht einstellen, auch das Mischen verschlüsselter und unverschlüsselter Auftragsteile ist möglich.

Der Intermediär bettet den verschlüsselten Auftragsteil des Benutzers in eine selbst erzeugte FinTS-Nachricht ein und signiert diese als Bote. Da die enthaltenen Aufträge zu diesem Zeitpunkt bereits verschlüsselt sind, kann der Intermediär durch seine Botensignatur nur den ordnungsgemäßen Transport der Daten bestätigen, jedoch keine Aussage zum Inhalt der übermittelten Aufträge machen.

Der Intermediär übermittelt die FinTS-Nachricht an das Kreditinstitut. Das Kreditinstitut verarbeitet die Nachricht und übermittelt dem Intermediär eine verschlüsselte Antwortnachricht. Analog zur Einreichung enthält die Antwortnachricht einen zusätzlichen für den Benutzer verschlüsselten Auftragsteil mit den Antwortdaten. Der Intermediär entnimmt den für den Benutzer bestimmten verschlüsselten Auftragsteil aus der Nachricht und leitet ihn an den Benutzer weiter. Der Benutzer entschlüsselt den Auftragsteil und prüft die darin enthaltene Signatur des Kreditinstituts.

Die Situation ähnelt der in Szenario C, mit dem Unterschied, dass der Intermediär keine Kenntnis von den Transaktionen seiner Kunden erlangt. Den Benutzern steht somit die volle FinTS-Sicherheit zur Verfügung.



Im Firmenkundengeschäft ist organisatorisch sicherzustellen, dass bei Einsatz eines HBCI-Sicherheitsverfahrens alle verfügbungsberechtigten Benutzer eines Firmenkunden über denselben Verschlüsselungsschlüssel verfügen oder eine zentrale Stelle zur Ver- und Entschlüsselung eingerichtet ist.



Bestimmte administrative Auftragsarten können syntaktisch nur in besondere Nachrichtentypen eingebettet werden (Keymanagement, Synchronisierung). Der Intermediär kann in diesem Szenario aber die Aufträge nicht einsehen, daher muss diese Zusatzinformation im proprietären Protokoll zwischen Benutzer und Intermediär übermittelt werden, so dass dieser den korrekten Nachrichtentyp für den Auftragsteil wählen kann.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Signatur-Rollenverteilung bei Kommunikation mit und ohne	Stand: 06.10.2017	Seite: 26

II.4 Signatur-Rollenverteilung bei Kommunikation mit und ohne Intermediär

In Abbildung 11: Rollenverteilung bei Kommunikation mit und ohne Intermediär sind die möglichen Verteilungen der Rollen *Herausgeber*, *Zeuge* und *Bote* für die Szenarien A bis D aus II.3.2 *Kommunikation über Intermediär* zusammen mit dem Fall der direkten Kommunikation zwischen Benutzer und Kreditinstitut ohne Intermediär dargestellt.

Für jedes der fünf Szenarien ist angegeben, wer welchen Teil der Nachricht signiert und verschlüsselt, und mit welcher Rolle er dies tut.

In den Szenarien A und „Ohne Intermediär“ sind hierbei stets zwei Alternativen vorhanden. Es kann entweder eine einzelne Botensignatur mit der Rolle des Herausgebers erstellt werden, wodurch der Auftragsteil implizit vom Herausgeber signiert wird, oder es werden getrennte Boten- und Herausgebersignaturen mit den jeweils passenden Rollen erstellt. Eine Signatur der Nachricht (Botensignatur) hat immer implizit die Rolle „Bote“, die Rolle „Herausgeber“ kann ihr wie in diesen beiden Szenarien zusätzlich zugewiesen werden.

Szenario	Rollen und Sicherheit			
	Benutzer		Intermediär	
	Auftragsteil	Nachricht	Auftragsteil	Nachricht
A	-	-	-	H - S+V
			H - S	B - S+V
B	PIN/TAN	-	H - S	B - S+V
C	H - S	-	-	B - S+V
D	H - S+V	-	-	B - S+V
Ohne Intermediär	-	H - S+V	-	-
	H - S	B - S+V	-	-

Rollen:
 H - Herausgeber oder Zeuge
 B - Bote

Sicherheit:
 S - Signatur
 V - Verschlüsselung

Abbildung 11: Rollenverteilung bei Kommunikation mit und ohne Intermediär

Das Kreditinstitut signiert grundsätzlich immer mit der Rolle „Herausgeber“.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Unterstützte Kommunikationsverfahren im Überblick	Stand: 06.10.2017	Seite: 27

II.5 Unterstützte Kommunikationsverfahren im Überblick

Im Rahmen von FinTS existieren zwei grundsätzlich unterschiedliche Verfahren für die Kommunikation zwischen Benutzer und Kreditinstitut:

- das synchrone Verfahren und
- das asynchrone Verfahren

◆ Synchrones Verfahren (Dialog)

Unter „synchron“ sind Kommunikationsverfahren zu verstehen, bei denen im Rahmen eines Dialoges Informationen zwischen Benutzer und Kreditinstitut wechselseitig ausgetauscht werden. Das Kundensystem wartet mit dem Senden von Aufträgen, bis die Antwortnachricht des Kreditinstituts auf die vorhergehende Nachricht eingetroffen ist. Eingereichte Aufträge werden vom Kreditinstitut sofort synchron beantwortet, wobei es sich je nach Verarbeitungssystem um eine komplette Bestätigung der Durchführung oder nur eine Quittierung des korrekten Auftragseingangs handeln kann. Durch die Einreichung von Abholaufträgen angeforderte Informationen werden vom Kreditinstitut sofort zurückgemeldet.

Das synchrone Verfahren wird durch die in HBCI V2.2 und FinTS V3.0 bereits definierten HBCI-Transportdienste abgedeckt. Generell sind für das synchrone Verfahren all jene Transportdienste einsetzbar, bei denen ein physischer Dialog aufgebaut und gehalten wird, solange die FinTS-Kommunikation besteht.

Weitere Informationen zum synchronen Kommunikationsverfahren sind unter II.6 zu finden.

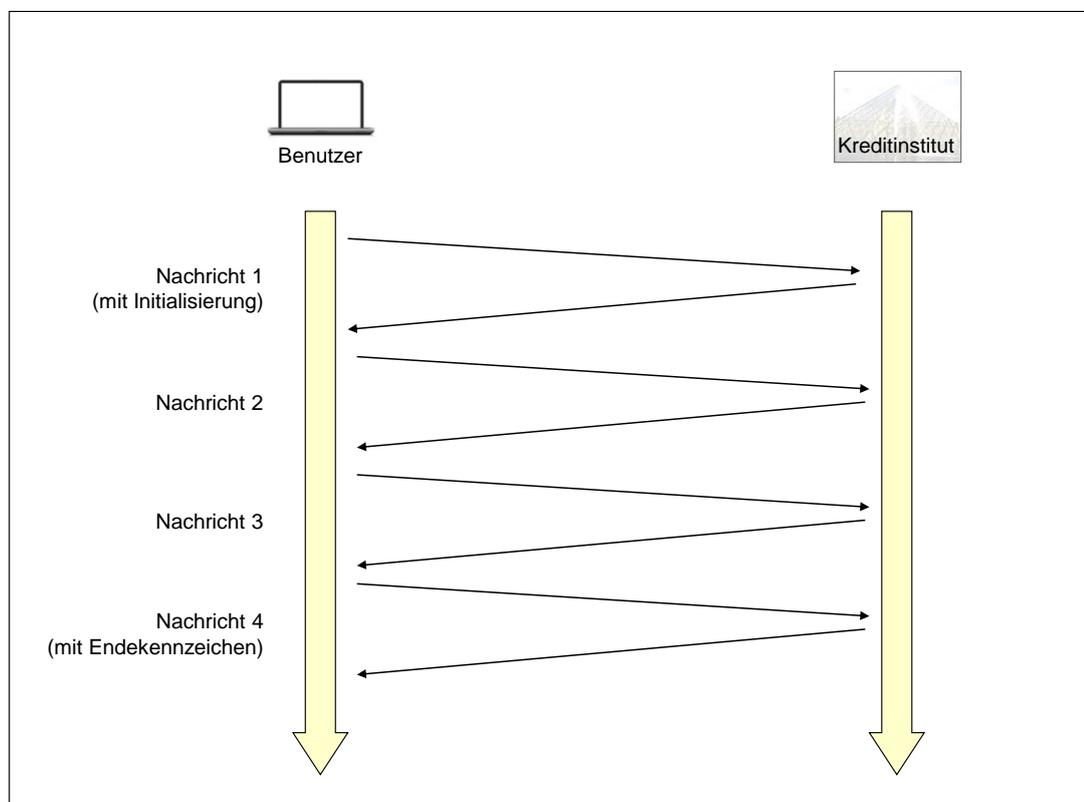


Abbildung 12: Nachrichtenabfolge im synchronen Verfahren

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Unterstützte Kommunikationsverfahren im Überblick	Stand: 06.10.2017	Seite: 28

◆ **Asynchrone Verfahren**

Bei asynchronen Verfahren erfolgt die Übertragung der Benutzer- und Kreditinstitutsinformationen zeitlich unabhängig voneinander, d. h. Benutzernachrichten werden in eine Warteschlange gestellt (Message-Queuing) und asynchron durch Kreditinstitutsnachrichten beantwortet. Der Benutzer wartet vor dem Versenden der nächsten Nachricht also nicht auf das Eintreffen der vorherigen Kreditinstitutsnachricht. Während der Kommunikation zwischen Benutzer und Kreditinstitut besteht keine dauerhafte physische Verbindung.

Da sich bei asynchronen Verfahren einzelne Nachrichten beim Transport überholen können, kann keine Aussage darüber gemacht werden, in welcher Reihenfolge die Nachrichten das Kreditinstitut erreichen. Jede Nachricht muss daher für sich allein bearbeitbar sein. Für solche asynchrone Verfahren eignen sich FinTS-Datagramme am besten, da diese immer einen Initialisierungsteil enthalten. Das bedeutet, dass über asynchrone Kommunikationsverfahren „FinTS-Dialoge“ abgewickelt werden, die aus genau einer Benutzernachricht und der zugehörigen Kreditinstitutsnachricht bestehen.

Als asynchrones Verfahren ist in der vorliegenden FinTS-Version der E-Mail-Dienst im Internet unterstützt. Weitere asynchrone Verfahren könnten jedoch auch Message-Queuing-Systeme darstellen, über die – ähnlich wie bei Filetransfer-Verfahren – Aufträge meist von Firmenkunden beim Kreditinstitut eingereicht werden. Die FinTS-Nachricht würde hierbei in Form einer Datei vorliegen.

Generell sind für die asynchrone Kommunikation all jene Transportdienste geeignet, bei denen keine dauerhafte physische Verbindung während einer Kommunikation gehalten wird, sondern die ihrerseits asynchron funktionieren. Beim E-Mail-Verfahren werden dem Benutzer die Kreditinstitutsnachrichten vom Kreditinstitutsystem zugesendet.

Über asynchrone Verfahren ist es auch möglich, dass ein Kreditinstitut aktiv Nachrichten an den Benutzer sendet, wenn dies mit dem Benutzer zuvor entsprechend vereinbart wurde. Die Kreditinstitutsnachricht bezieht sich dann auf eine vorangegangene Benutzernachricht, in der diese Vereinbarung stattfand (siehe *III.6 Das Publish/Subscribe-Verfahren*).

Asynchrone Verfahren stehen dem Benutzer ab FinTS V4.0 zur Verfügung. Anwendungsfälle ergeben sich z. B. im Firmenkundenbereich, im Bereich der browserorientierten Verarbeitung, in Internet-Portaldiensten oder Banking-Apps für Smartphones und Tablets.

Weitere Informationen zum asynchronen Kommunikationsverfahren sind unter *II.7 FinTS Datagramme* zu finden.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Unterstützte Kommunikationsverfahren im Überblick	Stand: 06.10.2017	Seite: 29

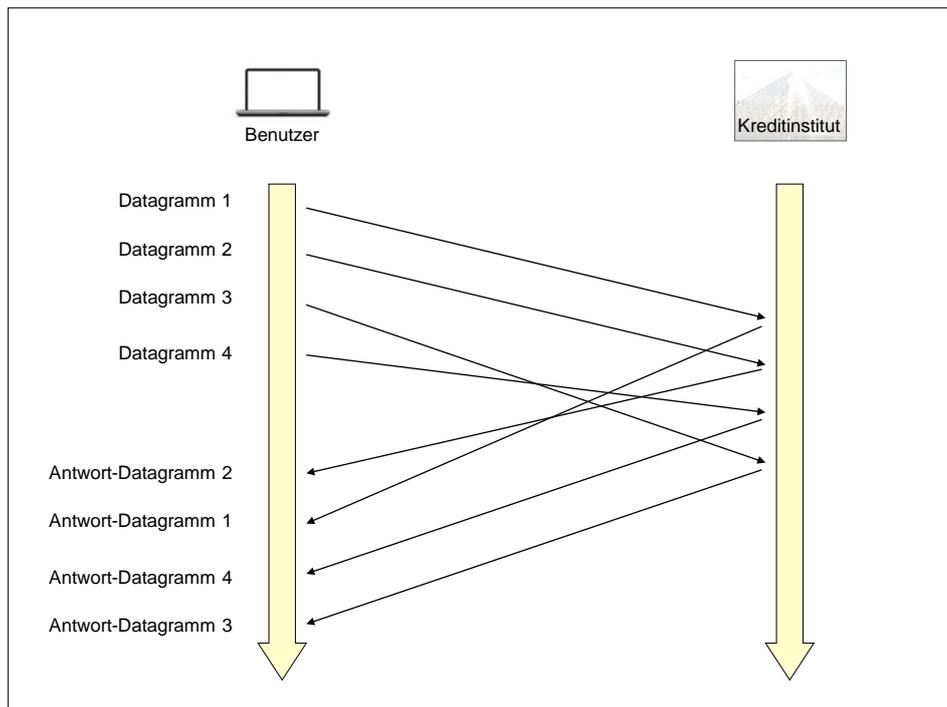


Abbildung 13: Nachrichtenabfolge im asynchronen Verfahren



Bei wechselweiser Verwendung des synchronen und des asynchronen Verfahrens durch denselben Benutzer kann es vorkommen, dass sich die Bearbeitung von Dialogen und Datagrammen kreditinstitutsseitig zeitlich überschneidet. Bei Verwendung softwarebasierter Sicherheitsmedien oder des PIN/TAN-Verfahrens kann ein Benutzer prinzipiell auch mehrere synchrone Dialoge gleichzeitig führen. Diese Situationen sind grundsätzlich zulässig und müssen vom Kreditinstitut behandelt werden können. Siehe dazu auch die Auswirkungen auf die Synchronisierung der letzten Nachrichtennummer in *III.3 Synchronisierung*.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: FinTS Dialoge	Stand: 06.10.2017	Seite: 30

II.6 FinTS Dialoge

II.6.1 Dialogabfolge

Die Initiierung eines Dialogs geht stets vom Benutzer aus. Auf eine Benutzernachricht wird stets mit einer genau definierten Kreditinstitutsnachricht unmittelbar geantwortet. Erst wenn der Benutzer diese Kreditinstitutsnachricht vollständig erhalten hat, darf er die nächste Nachricht an das Kreditinstitut übermitteln (Ausnahme: nach einem Verbindungsabbruch sendet der Benutzer im nächsten Dialog eine Nachricht an das Kreditinstitut, ohne vorher eine vollständige Antwortnachricht erhalten zu haben). Sowohl Benutzer als auch Kreditinstitut dürfen jeweils nur eine Nachricht auf einmal übermitteln. Das Kundensystem hat die Pflicht, solange zu warten, bis das Kreditinstitut die entsprechende Antwortnachricht übermittelt hat.

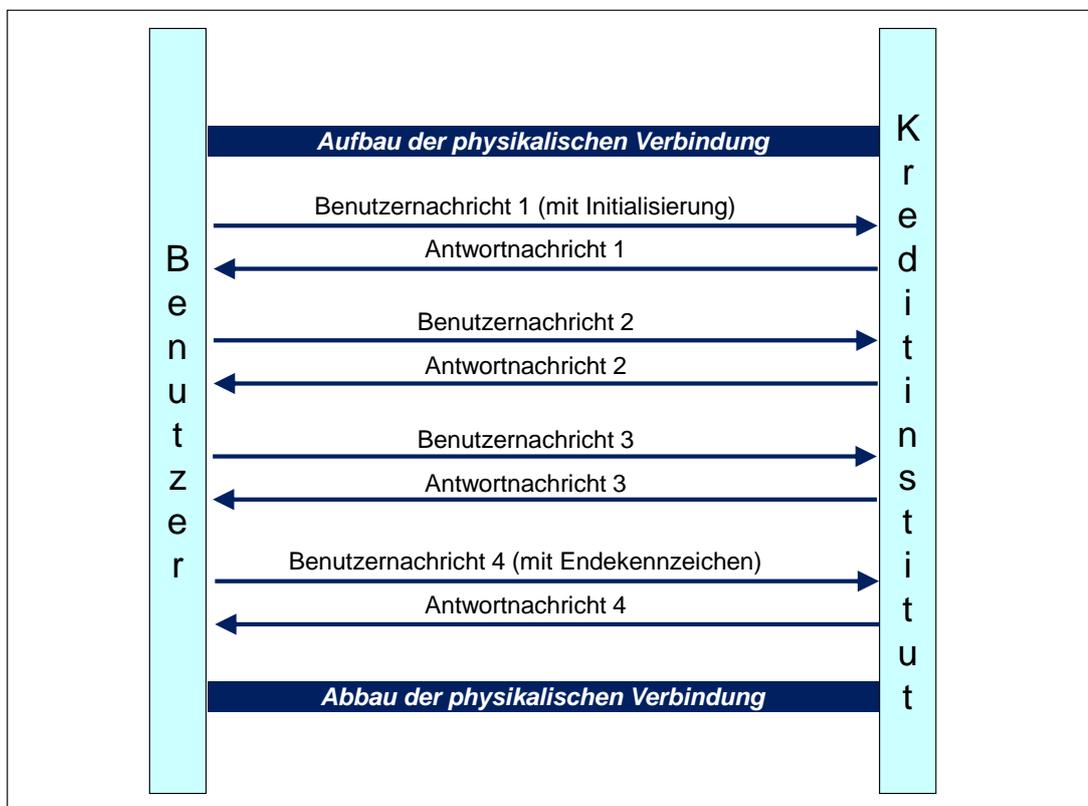


Abbildung 14: Dialogabfolge

Die erste Nachricht eines Dialoges enthält immer eine Initialisierung. Erst wenn das Kundensystem die Bestätigungsnachricht erhalten hat, darf die nächste Benutzernachricht gesendet werden. Sollen keine weiteren Benutzernachrichten mehr gesendet werden, so hat das Kundensystem mit seiner letzten Nachricht eine Beendigung zu senden. Mit der Rückmeldung auf diese Nachricht erhält das Kundensystem die Ende-Bestätigung des Kreditinstituts.

Im Ausnahmefall kann das Kreditinstitut den Dialog auch von sich aus beenden (z. B. bei wiederholter ungültiger Authentifizierung des Benutzers). Hierzu sendet es als Antwort auf eine Benutzernachricht eine Nachricht, in der das Endekennzeichen gesetzt ist und die den Rückmeldungscode 9800 („Dialog abgebrochen“, vgl. [RM-Codes]) enthält. Danach kann es die Transportverbindung abbauen. Das Kundenprodukt hat den Dialog in diesem Fall als beendet anzusehen und darf keine Been-

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: FinTS Dialoge	Stand: 06.10.2017	Seite: 31

digung mehr schicken. Das Kreditinstitut kann den Dialog außerdem von sich aus beenden, wenn über einen bestimmten Zeitraum keine Nachrichten mehr empfangen wurden (Timeout). Da dieser Abbruch nicht durch eine Benutzernachricht initiiert wird, kann in diesem Fall auch keine Kreditinstitutsnachricht mit entsprechender Rückmeldung gesendet werden. Der Benutzer erhält eine solche Meldung vielmehr erst dann, wenn er versucht, für den kreditinstitutsseitig bereits abgebrochenen Dialog eine weitere Nachricht einzureichen. Der Benutzer kann durch eine spezielle administrative Nachricht anzeigen, dass der Dialog noch offen gehalten werden soll, siehe dazu *III.5.3 Lebendmeldung in Dialogen*.

Ein Dialog bezieht sich immer auf einen Kunden. Aufträge eines Dialogs können von verschiedenen Benutzern signiert sein, welche dann jedoch dem gleichen Kunden zugeordnet sein müssen (siehe Abbildung 15: Einzelkunde).

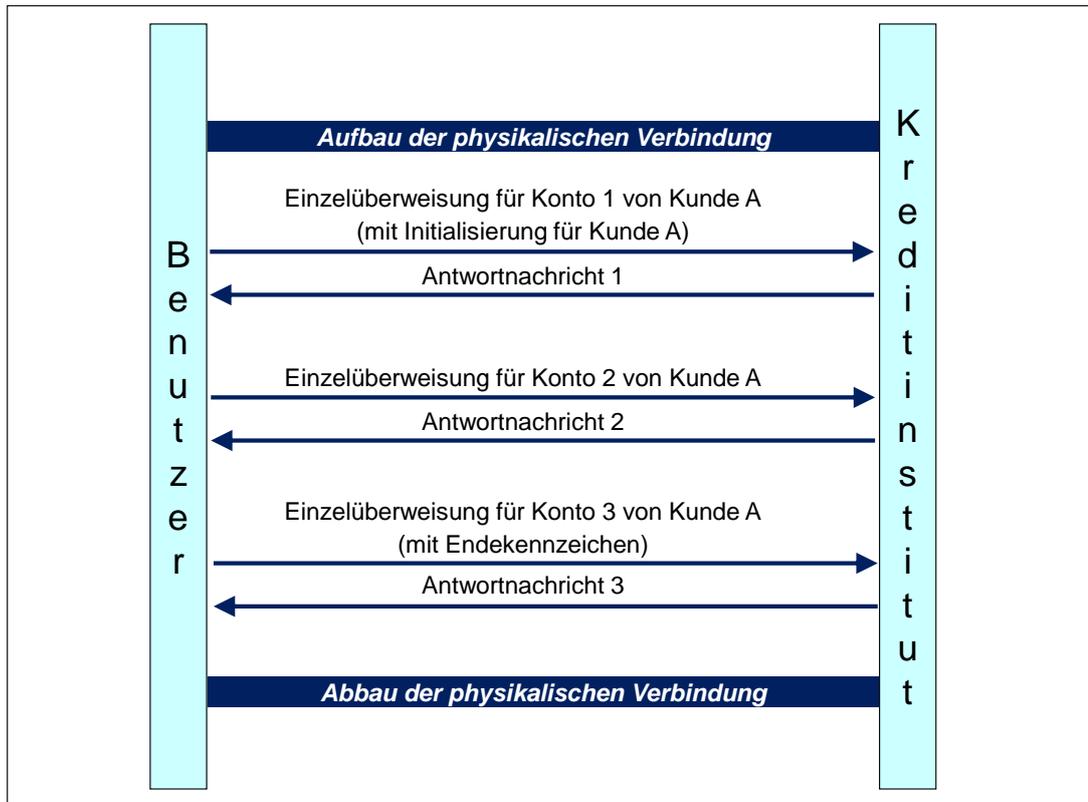


Abbildung 15: Einzelkunde

Sollen Aufträge für mehrere Kunden gesendet werden, ohne dass die physische Verbindung unterbrochen wird, so ist für jeden neuen Kundenbezug eine neue Initialisierung durchzuführen (siehe Abbildung 16: Mehrere Kunden).

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: FinTS Dialoge	Stand: 06.10.2017	Seite: 32

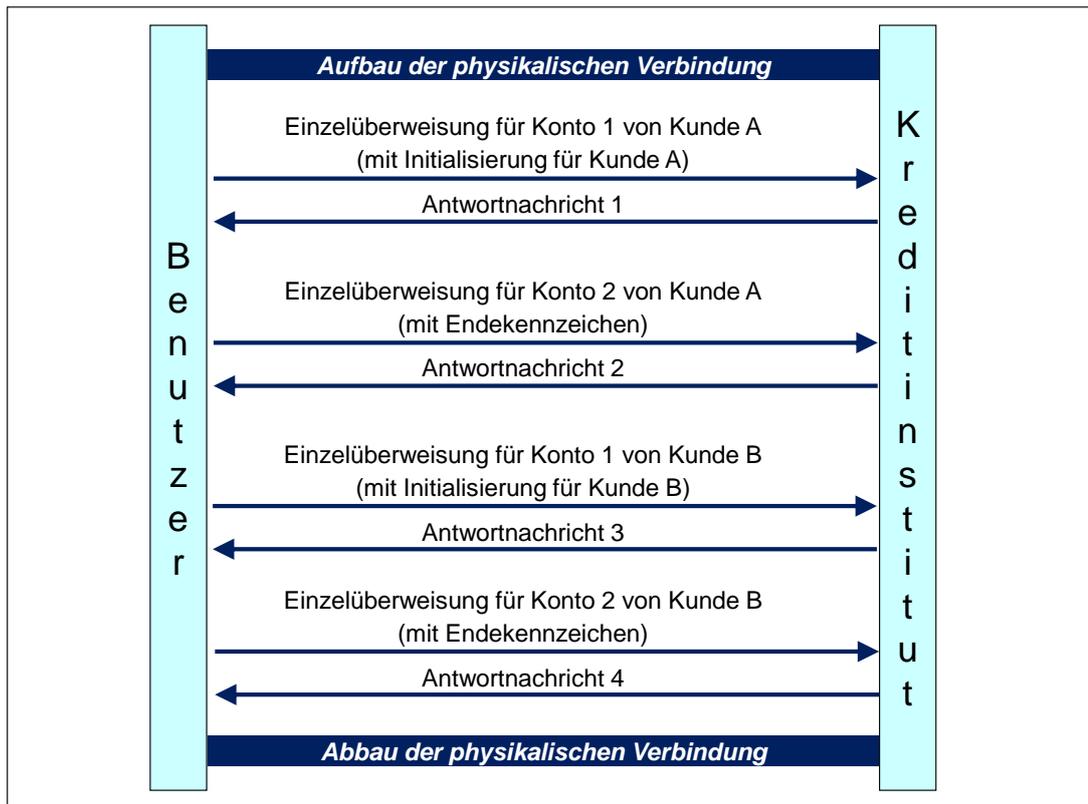


Abbildung 16: Mehrere Kunden

Unter Einbeziehung eines Intermediärs muss die Dialogabfolge in zwei Teilschritten betrachtet werden. Die Dialogspezifikation für die Kommunikation zwischen Benutzer und Intermediär kann bilateral zwischen beiden vereinbart werden. Insbesondere ist freigestellt, ob die Kommunikation synchron oder asynchron geführt wird und ob der Benutzer bei der Übermittlung der Aufträge eine passive bzw. aktive Rolle hat. Für die Kommunikation zwischen Intermediär und Kreditinstitut ist die oben dargestellte Dialogabfolge gültig (siehe Abbildung 15: Einzelkunde und Abbildung 16: Mehrere Kunden).

Im einfachsten Fall reicht ein Benutzer Aufträge ein, die alle für das gleiche Kreditinstitut bestimmt sind. Der Intermediär kann diese Aufträge dann innerhalb einer physischen Verbindung an das Kreditinstitut übermitteln (siehe Abbildung 17: Einbeziehung eines Intermediärs).

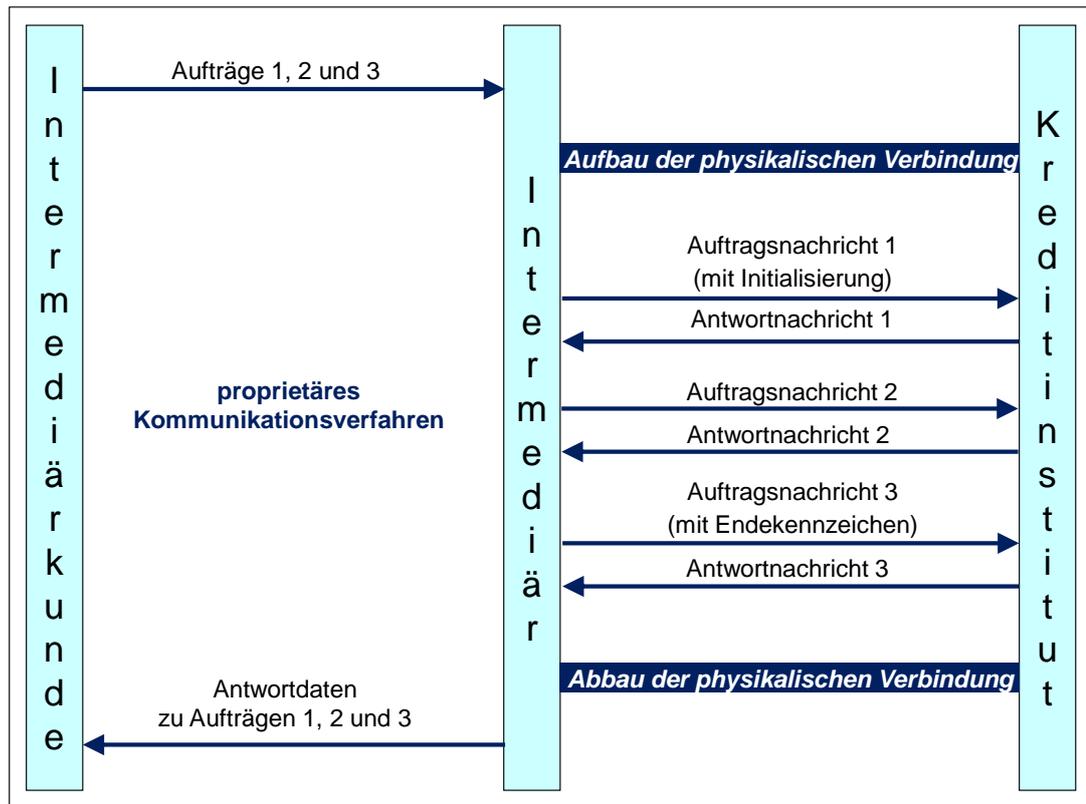


Abbildung 17: Einbeziehung eines Intermediärs

Kann der Benutzer vereinbarungsgemäß Aufträge für verschiedene Kreditinstitute einstellen, so führt der Intermediär diese Aufträge mit jedem Kreditinstitut in gesonderten FinTS-Dialogen innerhalb verschiedener physischer Verbindungen aus (siehe Abbildung 18: Intermediär und mehrere Kreditinstitute).

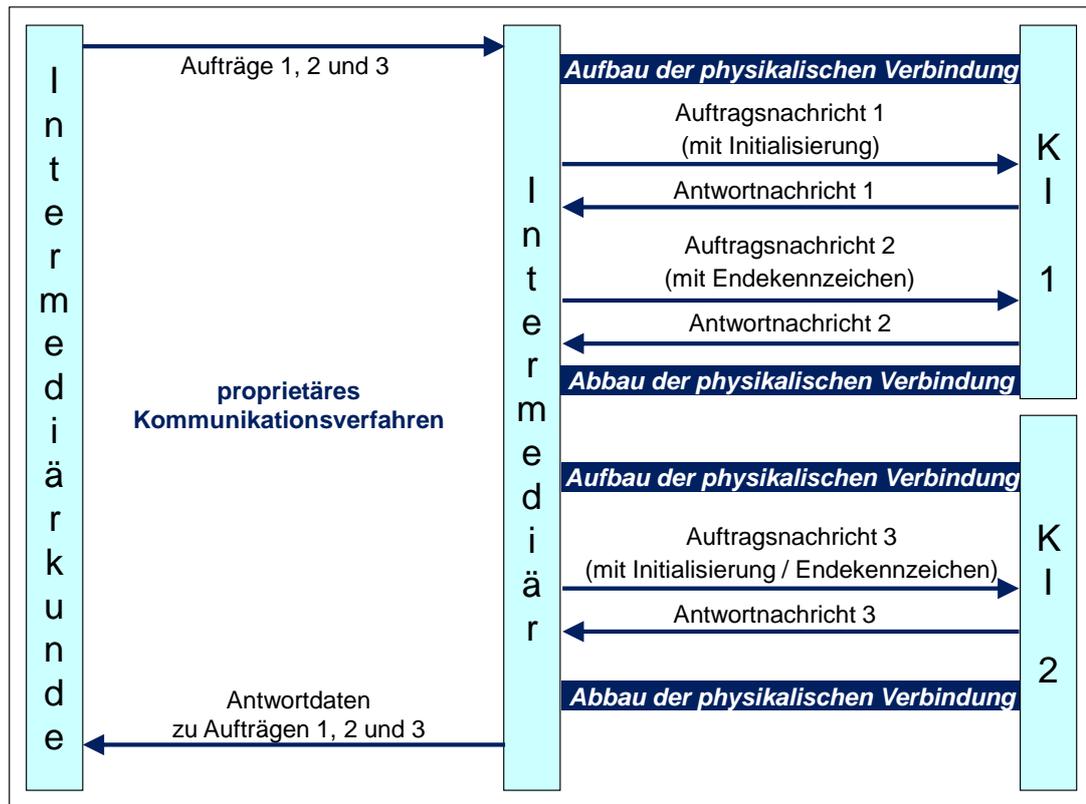


Abbildung 18: Intermediär und mehrere Kreditinstitute

Im Allgemeinen ist es dem Intermediär freigestellt, beliebige Aufträge in einem Dialog zu verarbeiten. Der Intermediär erhält somit die Möglichkeit, Aufträge verschiedener Benutzer des gleichen Kunden zu sammeln und in einem Dialog abzuarbeiten (siehe Abbildung 19: Intermediär sammelt Kundenaufträge).

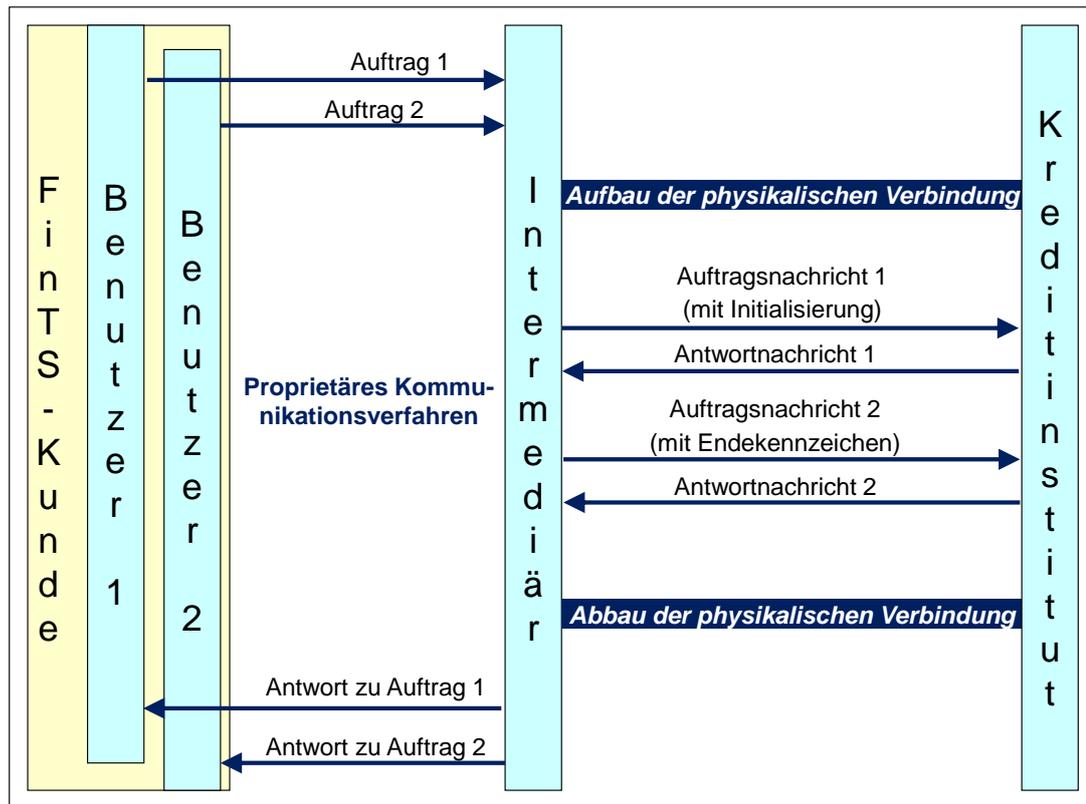


Abbildung 19: Intermediär sammelt Kundenaufträge

II.6.2 Dialogbeendigung und Endenachrichten

Der Benutzer bekundet seinen Wunsch zur Beendigung des Dialoges durch das Setzen des Endekennzeichens in der letzten Auftragsnachricht. Das Kreditinstitut bestätigt die Dialogbeendigung ebenfalls durch das Endekennzeichen in der Antwortnachricht. Weiterhin wird der Rückmeldungscode 0100 („Dialog beendet“, vgl. [RM-Codes]) gesendet.

Nach Erhalt der Kreditinstitutsantwortnachricht ist der Dialog logisch beendet. Anschließend kann das Kundenprodukt entweder die Kommunikation physisch beenden oder einen neuen Dialog beginnen. Weitere Auftragsnachrichten des Benutzers ohne Initialisierung im administrativen Teil werden vom Kreditinstitut abgelehnt. Falls der Benutzer keine Dialogbeendigung sendet und eine synchrone physische Verbindung besteht, wird der Dialog kreditinstitutsseitig physisch nach einem transportmedienabhängigen Timeout beendet.

Falls der Benutzer in der letzten übermittelten Nachricht das Endekennzeichen nicht gesetzt hat, jedoch keine weiteren Aufträge mehr schicken möchte, sendet er eine Nachricht ohne Auftragsteil, in der das Endekennzeichen gesetzt ist. Diese so genannte Endenachricht muss wie sämtliche Nachrichten signiert und verschlüsselt sein. Die Endenachricht kann vom Benutzer auch gesendet werden, wenn erst nach dem Erhalt der letzten Kreditinstitutsantwort entschieden wurde, den Dialog zu beenden, jedoch keine weiteren bankfachlichen Aufträge mehr zu senden sind.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: FinTS Dialoge	Stand: 06.10.2017	Seite: 36



Das Endekennzeichen kann auch bereits in einer Nachricht mit Initialisierung gesetzt werden. Formal stellt die Nachricht damit ein Datagramm dar, das über einen synchronen Kommunikationskanal eingereicht und synchron beantwortet wird.

Aus Performancegründen wird ausdrücklich empfohlen, dass Ausgangskorb-orientierte Kundensysteme auch bei synchroner Kommunikation grundsätzlich Aufträge sammeln und gebündelt in einem Datagramm einreichen statt einen mehr-schrittigen Dialog zu führen. Siehe dazu *II.7.2 Aufbau von FinTS-Datagrammen*.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: FinTS Datagramme	Stand: 06.10.2017	Seite: 37

II.7 FinTS Datagramme

II.7.1 Kommunikation mittels FinTS-Datagrammen

Neben der synchronen Kommunikation besteht für den Benutzer die Möglichkeit, Auftragsnachrichten asynchron an ein Kreditinstitut zu senden, d. h. die Kreditinstitutsantwort erfolgt nicht unmittelbar. In Abgrenzung zur kontextgebundenen synchronen Dialogabfolge werden die Nachrichten, die bei dieser kontextfreien Kommunikationsform übertragen werden, als Datagramme bezeichnet.

Datagramme eignen sich daher besonders für asynchrone Kommunikationsverfahren. In der vorliegenden FinTS-Version wird als asynchrones Transportprotokoll SMTP (E-Mail) unterstützt.



Das Kundenprodukt sollte asynchrone Transportprotokolle unterstützen oder geeignete Standardprodukte einbinden können. Insbesondere sollte das Kundenprodukt die Möglichkeit bieten, alternative Transportwege und Kommunikationsadressen definieren zu können.

Die Initiierung eines Auftrags geht stets vom Kunden aus. Antwortnachrichten sendet das Kreditinstitut nach dem Eingang und der Bearbeitung einer Benutzernachricht oder der Bearbeitung eines zuvor über das Publish/Subscribe-Verfahren eingereichten Kundenauftrages (vgl. *III.6 Das Publish/Subscribe-Verfahren*). Im Unterschied zur Dialogabfolge bei synchroner Kommunikation muss der Benutzer nach dem Versenden einer Auftragsnachricht auf asynchronem Kommunikationsweg nicht auf die Antwortnachricht des Kreditinstituts warten. Der Benutzer kann sofort weitere Auftragsnachrichten versenden.



Das Kreditinstitut muss durch geeignete Maßnahmen sicherstellen, dass ein bereitgestellter Kundenauftrag zeitnah verarbeitet wird.

Der Benutzer stellt die Auftragsnachricht über einen geeigneten Transportweg zur Abholung durch das Kreditinstitut bereit. Das Kreditinstitut holt die Auftragsnachricht vom Bereitstellungsort ab, verarbeitet den Auftrag und sendet die Antwortnachricht wie im Folgenden beschrieben an den Benutzer zurück. Dem Benutzer ist es freigestellt, zu welchem Zeitpunkt er die bereitgestellte Antwortnachricht abholt.



Die Durchführung einer starken Kundenauthentifizierung gemäß [PSD2] ist im Datagrammodus nicht möglich.



Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: FinTS Datagramme	Stand: 06.10.2017	Seite: 38

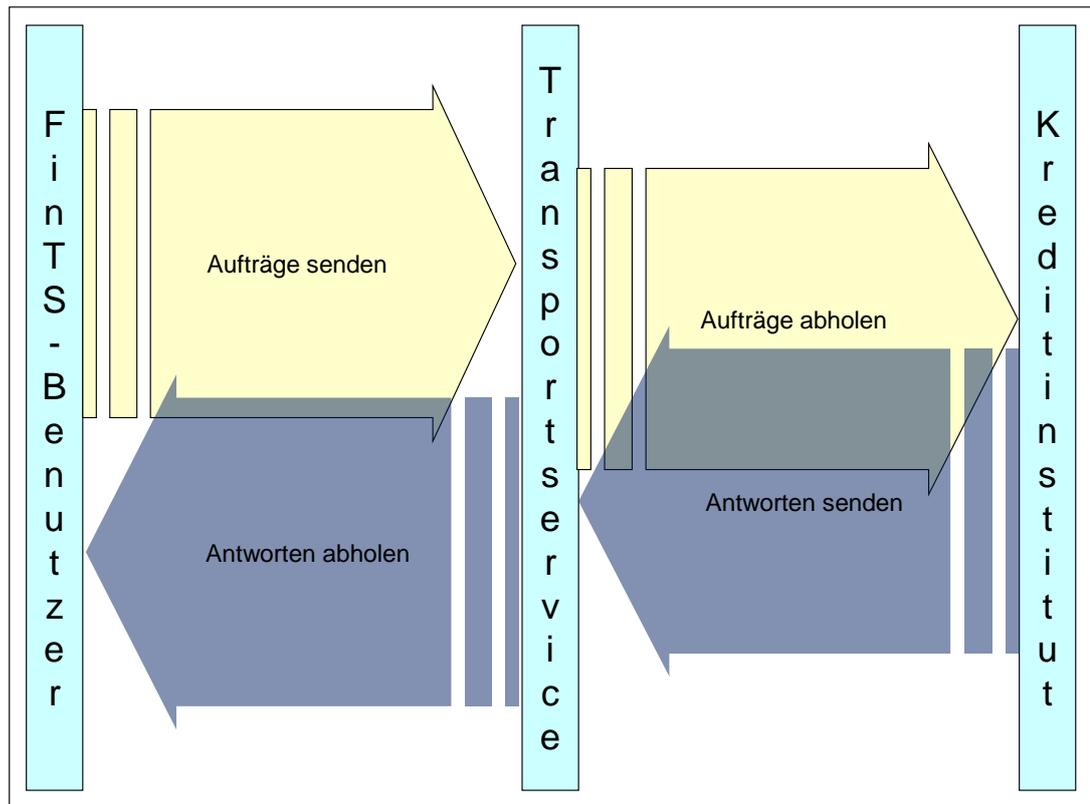


Abbildung 20: Datagramme

Die Antwortnachricht wird standardmäßig an die Kommunikationsadresse zurückgesendet, von der aus der Benutzer die Auftragsnachricht eingereicht hat. Alternativ kann der Benutzer jedoch im Nachrichtenkopf eine andere Rückantwortadresse angeben. Diese Rückantwortadresse muss nicht als Kommunikationsadresse beim Kreditinstitut registriert sein. Die Unversehrtheit dieser Rückantwortadresse wird jedoch durch die Botensignatur, die auch den Nachrichtenkopf umfasst, sichergestellt.

II.7.2 Aufbau von FinTS-Datagrammen

Ein FinTS-Datagramm ist gegeben durch eine gültige FinTS-Nachricht, für die die Einschränkung gilt, dass sie eine Initialisierung enthalten und das Endekennzeichen gesetzt sein muss. Hierdurch wird sichergestellt, dass eine via Datagrammen geführte Kommunikation per Definition nur aus einer einzelnen Nachricht besteht und nach deren Bearbeitung endet.

Da ein Datagramm formal eine normale FinTS-Nachricht mit besonderen Belegungsvorgaben darstellt, ist sein Einsatz nicht an das asynchrone Kommunikationsverfahren gebunden. Datagramme können also auch im synchronen Kommunikationsverfahren verwendet werden - dies wird aus Performancegründen sogar ausdrücklich empfohlen (siehe dazu auch II.6.2 *Dialogbeendigung und Endenachrichten*).

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Verbindungsabbruch	Stand: 06.10.2017	Seite: 39

II.8 Verbindungsabbruch

In FinTS erfolgt in keinem Fall kreditinstitutsseitig ein Abbruch der Übertragung von Benutzernachrichten; auch dann nicht, wenn kreditinstitutsseitig bereits während der Übertragung ein Fehler in der Nachricht festgestellt wird. Der Abbruch wird aus Gründen der Einheitlichkeit nicht durchgeführt, weil entsprechende Funktionalitäten nicht bei allen Kommunikationsdiensten zur Verfügung stehen.

Bzgl. Verbindungsstörungen bzw. Abbrüchen bei synchroner Kommunikation sind aus Sicht des Kreditinstituts folgende Fälle zu unterscheiden:

Fall 1: Abbruch während der Benutzer eine Initialisierung ohne Auftragsteil an das Kreditinstitut sendet

In diesem Fall ignoriert das Kreditinstitut das erhaltene Nachrichtenfragment.

Fall 2: Abbruch nachdem der Benutzer eine Initialisierung ohne Auftragsteil an das Kreditinstitut gesendet hat

Die Nachricht wurde erhalten. Anschließend wurde der Benutzer identifiziert und die Legitimation erteilt. Das Kreditinstitut erwartet weitere Auftragsnachrichten. Diese können jedoch nicht eintreffen, da der Benutzer die zur Initialisierung gehörende Antwortnachricht nicht erhalten hat.

Fall 3: Abbruch während der Benutzer eine Nachricht mit Auftragsteil an das Kreditinstitut sendet

In diesem Fall ignoriert das Kreditinstitut das erhaltene Nachrichtenfragment.

Fall 4: Abbruch nachdem der Benutzer eine Nachricht mit Auftragsteil an das Kreditinstitut gesendet hat

Der Abbruch erfolgt hierbei bevor oder während das Kreditinstitut die Antwortnachricht an den Benutzer sendet. In diesem Fall wird die erhaltene Nachricht vom Kreditinstitut bearbeitet.

Bei einem Abbruch wird die Kommunikation genau dann nicht ordnungsgemäß beendet, wenn die bisher erhaltenen Benutzernachrichten noch kein Endekennzeichen enthielten. Dies tritt nur dann auf, wenn das Kundensystem im synchronen Dialogverfahren mit dem Kreditinstitut kommuniziert hat, weil bei Datagrammen kundenseitig stets das Endekennzeichen eingestellt wird. Das Kreditinstitut hat dennoch den Dialog als abgeschlossen zu betrachten, da der Benutzer einen neuen Dialog beginnen muss, um sich über den Status der abgebrochenen Nachricht zu informieren.

Bei asynchroner Kommunikation besteht zwar keine physische Verbindung zwischen Benutzer und Kreditinstitut, dennoch kann es zu Fehlern beim Transport von Datagrammen zwischen Benutzer und Kreditinstitut kommen. Hierbei sind aus Sicht des Kreditinstituts die beiden weiteren Fälle zu unterscheiden:

Fall 5: Das Datagramm geht auf dem Weg zum Kreditinstitut verloren oder ist unlesbar

In diesem Fall findet auf Seite des Kreditinstituts keine Verarbeitung statt, weil es nicht von der Existenz des Datagramms erfährt.

Fall 6: Das Antwort-Datagramm geht auf dem Weg zum Benutzer verloren oder ist unlesbar

In diesem Fall hat eine Verarbeitung stattgefunden.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Verbindungsabbruch	Stand: 06.10.2017	Seite: 40



Verhalten auf Kundenseite:

Erfolgt der Abbruch während oder nach der Initialisierung (Fall 1 und 2) und enthielt die Benutzernachricht noch keinen Auftragsteil, ist der Dialog auf jeden Fall mit einer erneuten Initialisierung zu beginnen. Eine Synchronisierung muss nicht durchgeführt werden, da noch keine Aufträge gesendet wurden (siehe *III.3 Synchronisierung*).

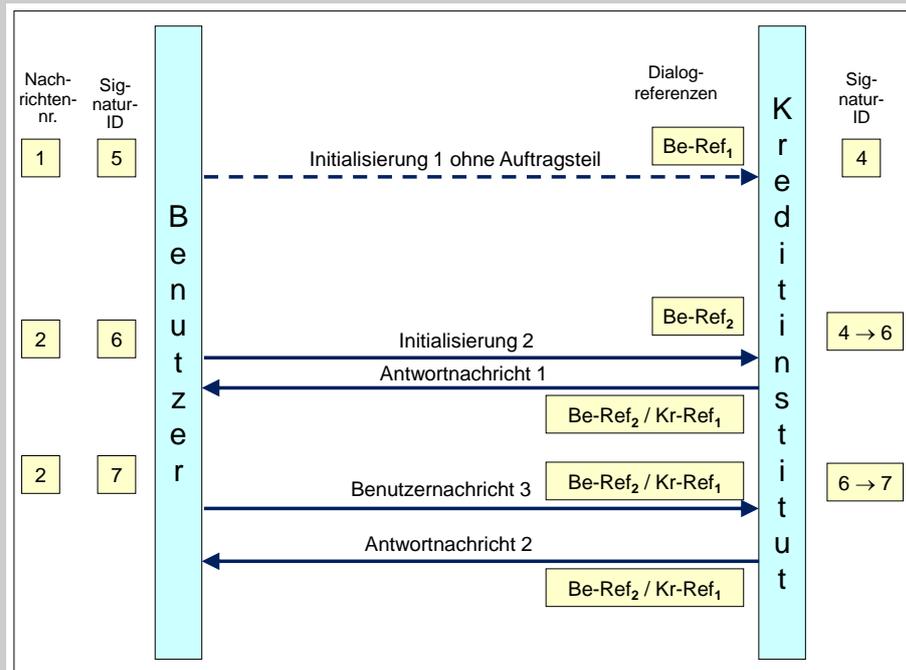


Abbildung 21: Verbindungsabbruch Fall 1

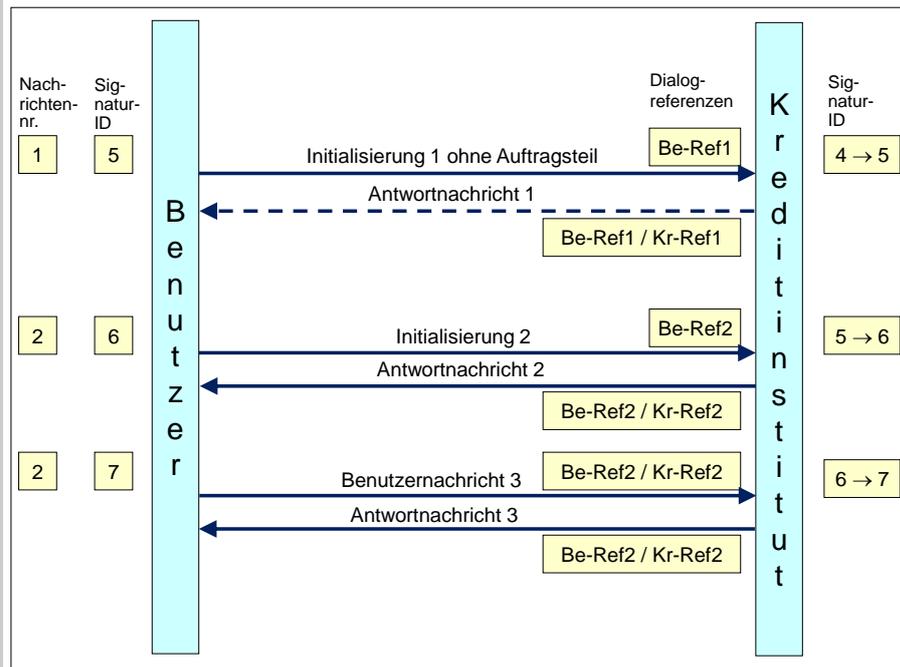


Abbildung 22: Verbindungsabbruch Fall 2

In einer synchronen Kommunikation ist im Falle eines Abbruchs während oder nach dem Senden einer Nachricht mit Auftragsteil (Fall 3 und 4) für das Kundenprodukt im Regelfall nicht nachvollziehbar, zu welchem dieser beiden Zeitpunkte der Abbruch erfolgt ist. Dieses Kenntnis ist jedoch erforderlich, um zu entscheiden, ob der Auftragsteil erneut gesendet werden muss.

Das Kundenprodukt sendet hierzu eine Synchronisierungsnachricht (siehe III.3 Synchronisierung). In der Antwortnachricht erhält es die letzte Nachrichtennummer der Benutzernachricht, die im abgebrochenen Dialog noch verarbeitet wurde. Anhand dieser Information ist für das Kundenprodukt ersichtlich, ob ein Auftragsteil erneut gesendet werden muss (Fall 3) oder ob dies nicht notwendig ist (Fall 4).

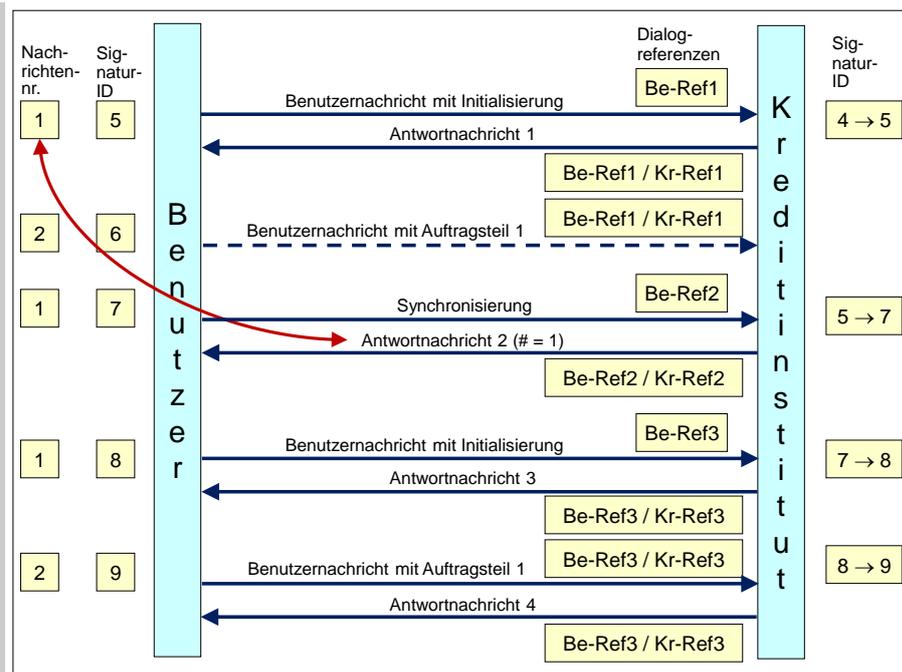


Abbildung 23: Verbindungsabbruch Fall 3

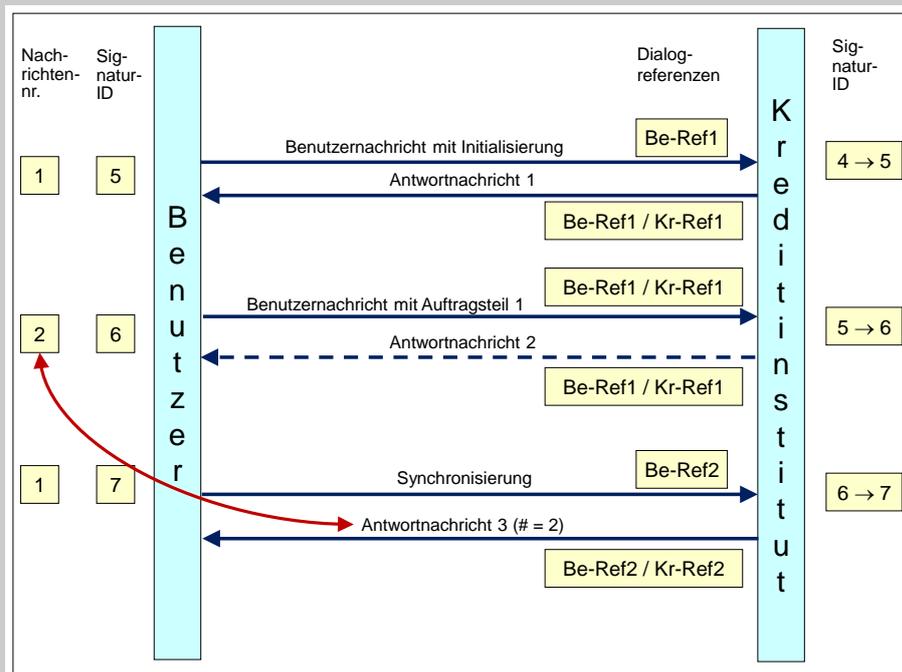


Abbildung 24: Verbindungsabbruch Fall 4

Eine erneut zu sendende Nachricht darf unverändert (bit-identisch) gesendet werden, sofern die in ihr enthaltenen Signatur-IDs (siehe [HBCI], Abschnitt II.5.1 Signatur-Segment) vom Kreditinstitut noch nicht als verbraucht gekennzeichnet wurden. Falls dies doch der Fall ist, müssen die Signaturen innerhalb der Nachricht mit neuen Signatur-IDs versehen und neu berechnet werden. Dies bedeutet, dass ggf. auch Herausgeber und Zeugen eines Auftragsteils neu signieren müssen.

Hat ein Benutzer bei asynchroner Kommunikation keine Antwort auf ein von ihm gesendetes Datagramm bekommen, kann er eine Synchronisierung bzgl. der Kundenreferenz durchführen, um vom Kreditinstitut zurückgemeldet zu bekommen, ob das durch die Referenz bezeichnete Datagramm verarbeitet wurde (siehe III.3 Synchronisierung). Damit ist für den Benutzer die Unterscheidung möglich, ob ein von ihm gesendetes Datagramm nicht beim Kreditinstitut angekommen ist und somit noch einmal gesendet werden muss (Fall 5) oder ob lediglich die Antwort des Kreditinstituts verloren gegangen ist (Fall 6).

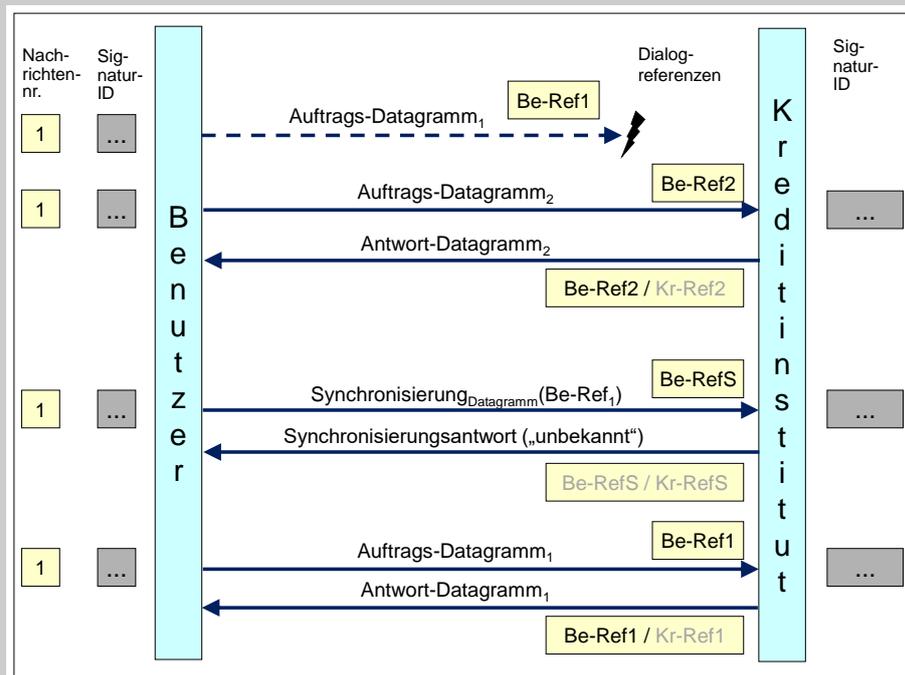


Abbildung 25: Verbindungsabbruch Fall 5

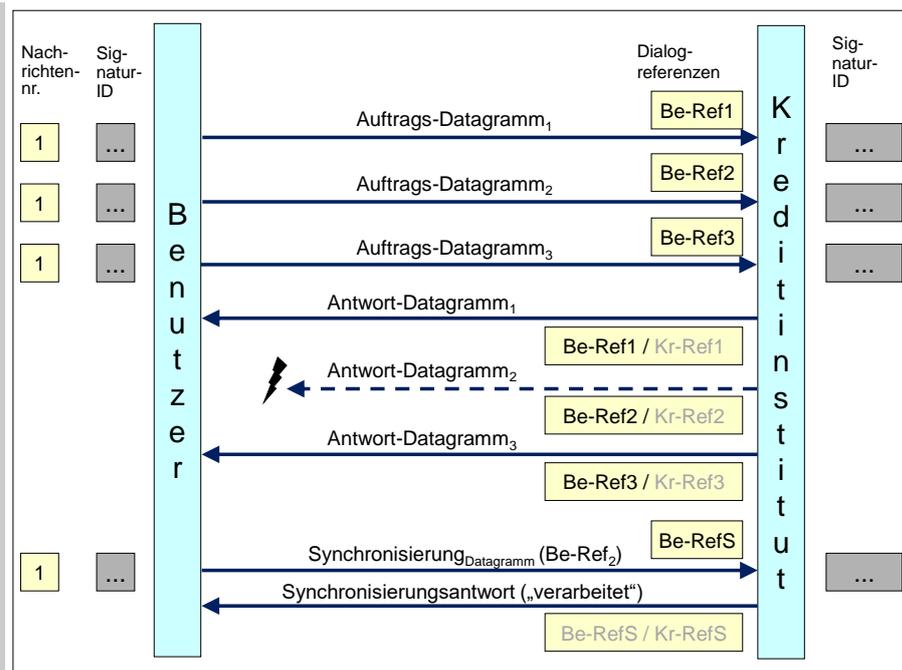


Abbildung 26: Verbindungsabbruch Fall 6

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Benutzernachrichten allgemein	Stand: 06.10.2017	Seite: 45

II.9 Benutzernachrichten allgemein

Eine Benutzernachricht kann je nach Anwendungsfall HBCI-verschlüsselt übertragen werden. Nach der Entschlüsselung kann sie ggf. noch teilverschlüsselt sein.

Sowohl administrativer Teil als auch Auftragsteil einer Benutzernachricht sind optional. Die erste Benutzernachricht in einer Kommunikation enthält jedoch immer eine Initialisierung im administrativen Teil. Alle ggf. noch folgenden weiteren Nachrichten dieser Kommunikation enthalten keine solche Initialisierung mehr.

Der Benutzer stellt in die Nachrichtenköpfe seiner Nachrichten eine von ihm gewählte Benutzerreferenz ein, die es ihm ermöglichen soll, seine eigenen Nachrichten zu verwalten. Die ebenfalls im Nachrichtenkopf einstellbare Kreditinstitutsreferenz wird von ihm zunächst leer gelassen. Erst, wenn er innerhalb eines Dialoges von der Kreditinstitutsseite über deren Antwortnachrichten eine Kreditinstitutsreferenz zurückerhalten hat, stellt auch der Benutzer diese in seine noch folgenden Benutzernachrichten des gleichen Dialoges ein.

Ist ein Auftragsteil vorhanden, so ist keine kundenseitige Priorisierung der Aufträge durch deren Reihenfolge möglich.

Ist der Bote einer Nachricht gleichzeitig auch Herausgeber der Nachricht, so ist es ausreichend, wenn er allein eine Botensignatur leistet. Hierdurch hat er auch den Auftragsteil mitsigniert. Die Botensignatur übernimmt dann die Funktion der Herausgebersignatur.

Sind Bote und Herausgeber der Nachricht verschieden, signiert der Herausgeber den Auftragsteil und der Bote die Gesamtnachricht.

Ein Zeuge signiert, falls notwendig, stets nur den Auftragsteil.



Eine falsche Botensignatur führt immer zur Ablehnung der gesamten Nachricht. Eine falsche Auftragssignatur führt zur Ablehnung der damit signierten Aufträge, andere Aufträge in der Nachricht können aber verarbeitet werden.

Für einen Auftrag relevante Signaturen können ignoriert werden, wenn sie in einem laut BPD für die Auftragsart nicht zulässigen Sicherheitsverfahren (siehe IV.2.3 *Sicherheitsverfahren*) erstellt sind. Sie führen nicht unmittelbar zur Ablehnung eines Auftrags.

Ein Auftrag wird nur dann weiter verarbeitet, wenn die Anzahl seiner - laut BPD in einem für die Auftragsart zulässigen Sicherheitsverfahren erstellten - Signaturen die Minimalzahl an Signaturen gemäß BPD und UPD erreicht und sich darunter eine Herausgebersignatur (ISS) befindet.

Durch die Struktur der Nachrichten ist es möglich, den Auftragsteil einer Nachricht ohne Beisein des Boten durch Herausgeber und Zeugen aufbauen und signieren zu lassen. Der Bote, welcher später den Transport der Aufträge innerhalb eines Dialoges abwickelt, hat somit keine Möglichkeit, die Aufträge nachträglich zu verändern. Falls gewünscht, kann der Herausgeber den Auftragsteil nach dem Signieren noch verschlüsseln. Er kann hierdurch den Inhalt der Aufträge vor dem Boten verbergen, welcher dennoch in der Lage ist, die Aufträge zur Verarbeitung weiterzuleiten.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Benutzernachrichten allgemein	Stand: 06.10.2017	Seite: 46

In einer Benutzernachricht sind prinzipiell beliebig viele Geschäftsvorfälle unterschiedlicher Geschäftsvorfallsarten zugelassen (z. B. drei Einzelüberweisungen neben einer Saldenabfrage). Eine Beschränkung der maximal möglichen Anzahl von Geschäftsvorfallsarten und Geschäftsvorfällen einer Art innerhalb einer Benutzernachricht ist über die Bankparameter möglich.

Bezüglich der Reihenfolge der in die Nachricht einzustellenden Aufträge wird keine Vorgabe getroffen. Da die Reihenfolge der Weiterleitung von Aufträgen an die Verarbeitungssysteme kreditinstitutsspezifisch ist, beeinflusst die Anordnung der Aufträge nicht zwingend die Reihenfolge der Verarbeitung bzw. Ausführung. Insbesondere ist daher auch keine kundenseitige Priorisierung der Aufträge durch deren Anordnung in der Nachricht möglich. Ist eine Priorisierung gewünscht, so sind die Aufträge in mehreren Dialogschritten einzureichen.



Das Kundenprodukt sollte grundsätzlich vor dem Senden des Auftrags prüfen, ob der vom Benutzer gewählte Geschäftsvorfall für das angegebene Konto zulässig ist. Beispielsweise können für ein Wertpapierkonto keine Kontoumsätze zurück gemeldet werden.

II.9.1 Aufträge

Die Auftragsteile einer Benutzernachricht enthalten die Auftragssegmente des Benutzers. In [Messages] sind die Auftragssegmente für die in FinTS abgebildeten Geschäftsvorfälle definiert. Zu einem Auftragssegment ist jeweils auch ein Parameter-Segment für die Verwendung in den Bankparameterdaten (siehe *IV BANKPARAMETERDATEN (BPD)*) und, falls der Auftrag vom Kreditinstitut über den Verarbeitungsstatus hinaus mit Daten beantwortet wird, ein Datensegment spezifiziert.

Auftragssegmente können beliebig auf mehrere Auftragsteile verteilt werden, die Verwendung mehrerer Auftragsteile in einer Nachricht ist jedoch vorrangig in echten Intermediär-Szenarien sinnvoll (vgl. *II.12.2 Teilverschlüsselte Nachrichten*).

Jedes Segment kann dabei beliebig oft und in beliebiger Reihenfolge auftreten. Das Kreditinstitut hat jedoch mit Hilfe der Bankparameterdaten die Möglichkeit, die Art und Anzahl der erlaubten Segmente einzuschränken:

- Die erlaubten Auftragssegmente gibt das Kreditinstitut je Sicherheitsverfahren an (siehe *IV.2.3 Sicherheitsverfahren*)
- Die maximale Anzahl von Segmenten einer Geschäftsvorfallsart pro Nachricht kann mit Hilfe des DE „Maximale Anzahl Aufträge“ eingestellt werden (siehe *IV.2.1 Bankparameter allgemein*).
- Die maximale Anzahl von Geschäftsvorfallsarten pro Nachricht kann mit Hilfe des DE „Anzahl Geschäftsvorfallsarten“ eingestellt werden (siehe *IV.2.1 Bankparameter allgemein*).

Darüber hinaus kann in den BPD festgelegt werden, ob für einen Auftrag der Erhalt der Antwortdaten quittiert werden muss (vgl. *III.5.1 Quittierung von Aufträgen* sowie *III.5.2 Willenserklärung des Kunden*) oder ob er abonniert werden kann (vgl. *III.6 Das Publish/Subscribe-Verfahren*).

Aufträge unterliegen einer Versionierung. Ist zu einem Auftragssegment ein zugehöriges Datensegment definiert, so werden diese stets gemeinsam versioniert. Das gleiche gilt für das zugehörige Parameter-Segment.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Benutzernachrichten allgemein	Stand: 06.10.2017	Seite: 47

Das Segmentformat ist beim jeweiligen Geschäftsvorfall spezifiziert, siehe [Messages] und [Syntax]. Die Erläuterungen in den folgenden Abschnitten beziehen sich auf die dort angegebenen Felder.

II.9.2 Abholauftrag

Abholaufträge werden an das Kreditinstitut gesendet, um die kreditinstitutsseitige Generierung und Übermittlung von spezifischen Informationen einzuleiten (z. B. Kontoumsätze, Börsenkurse, ggf. Statusprotokoll).

Hat ein Abholauftrag einen Kontobezug, so sind vom Benutzer ggf. Angaben über die gewünschte Kontoverbindung einzustellen, auf die sich der Auftrag bezieht. Der Benutzer hat darüber hinaus die Möglichkeit, den Umfang der Daten, die er mit dem Abholauftrag anfordert, zu beschränken und einzugrenzen. Dies kann durch die Angabe von Zeiträumen, Wertebereichen oder Maximalanzahlen geschehen. Weiterhin kann die Anforderung von Daten an bestimmten Stellen fortgesetzt werden. Hierzu ist ein spezieller Aufsetzpunkt notwendig, welcher dem Benutzer vom Kreditinstitut innerhalb der Antwort zu einem vorangegangenen Abholauftrag zurückgesendet wurde.

Kontoverbindung international Auftraggeber

Es ist diejenige Kontoverbindung des Benutzers einzustellen, für die im Abholauftrag Daten zurückgemeldet werden sollen. Es darf nur ein Konto eines Kreditinstituts angegeben werden, für das sich der Benutzer im Rahmen der Initialisierung legitimiert hat. Falls der noch zur Ausführung anstehende Auftrag nicht in Beziehung zu einem bestimmten Konto steht (z. B. Abruf von Devisenkursen, Abruf des Statusprotokolls) oder sich auf alle Konten bezieht, kann die Kontoverbindung entfallen.

Falls im Abholauftrag keine Währung angegeben wird, entspricht die Währung, in der die Kreditinstitutsantwort auf den Abholauftrag erfolgt, stets der Währung des Kundenkontos.

Alle Konten

Mit dieser Option kann gewählt werden, ob die angeforderten Informationen (z. B. Salden, Umsätze) nur zu dem angegebenen oder zu allen Anlagekonten des Kunden, für die er eine Zugriffsberechtigung besitzt, zurückgemeldet werden sollen.



Aufsetzpunkte können evtl. nicht korrekt zugewiesen werden, wenn mehrere Antwortsegmente gesendet werden. Daher sollte die Option „Alle Konten“ nur erlaubt werden, wenn ein Aufsetzpunkt aufgrund der kreditinstitutsseitigen Verarbeitung nicht vorkommen kann.

Zeiträume (Von Datum, Bis Datum)

Mit Hilfe dieser Angaben kann die Menge der zurückzumeldenden Daten (z. B. Buchungspositionen) anhand eines Zeitraums eingegrenzt werden. Wird kein Zeitraum angegeben, so werden stets alle verfügbaren Einträge zurückgemeldet. Wird ein Zeitraum angegeben, so werden nur diejenigen Einträge zurückgemeldet, die im Zeitraum (einschließlich der angegebenen Grenzen) liegen. Die Eingabemöglichkeiten sind der nachfolgenden Tabelle zu entnehmen.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Benutzernachrichten allgemein	Stand: 06.10.2017	Seite: 48

Falls der Zeitraum inkonsistent ist (Anfangsdatum größer als Enddatum), wird der Auftrag abgelehnt. Ein Zeitraum darf nicht gleichzeitig mit einem Kennungsbereich (s. u.) angegeben werden.

Beispiele:

Von Datum	Bis Datum	Bedeutung
01.07.2013	31.07.2013	liefert alle Einträge, die im angegebenen Zeitraum liegen
01.07.2013	leer	liefert alle Einträge, die am 1.7.2013 oder danach angefallen sind
leer	31.07.2013	liefert alle Einträge, die am 31.7.2013 oder davor angefallen sind
leer	leer	liefert alle verfügbaren Einträge

Wertebereiche (Von <Kennung>, Bis <Kennung>)

Hier kann der Abholbereich durch bankfachliche Informationen (z. B. Dauer-auftrags-ID, Wertpapiernamen) eingegrenzt bzw. genauer spezifiziert werden, sofern dies durch den betreffenden Geschäftsvorfall unterstützt wird.

Falls die Informationen zu einer bestimmten Kennung (z. B. Betrag xy) abgeholt werden sollen, so ist in beide Felder dieselbe Kennung einzutragen.

Im Übrigen gelten die Festlegungen zu den Feldern „Von Datum“ und „Bis Datum“.

Aufsetzpunkte

Falls das Kreditinstitut den Benutzerauftrag nicht in einem einzigen Antwortsegment beantworten kann, besteht die Möglichkeit, dass es die Beantwortung an einem bestimmten Punkt kontrolliert beendet und dem Benutzer in der Antwortnachricht mit dem Rückmeldungscode einen Aufsetzpunkt mitteilt. Hierzu ist der spezielle Rückmeldungscode 3040 („Es liegen weitere Informationen vor“, vgl. [RM-Codes]) vorgesehen. Der Aufsetzpunkt kann ein beliebiger kreditinstitutsinterner Ordnungsbegriff sein, der vom Kundenprodukt nicht interpretiert werden soll. Bei transparenten Daten kann die Fragmentierung beliebig (z. B. logisch oder binär) erfolgen. Es ist lediglich zu fordern, dass die Zusammensetzung der Fragmente im Kundensystem problemlos möglich ist.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Benutzernachrichten allgemein	Stand: 06.10.2017	Seite: 49



Falls das Kreditinstitut einen Aufsetzpunkt rückmeldet, wird vom Kundenprodukt erwartet, dass es denselben Abholauftrag unter Hinzufügung des Aufsetzpunktes erneut schickt. In der Antwortnachricht erhält der Benutzer den folgenden Teil der Informationen (evtl. inkl. eines erneuten Aufsetzpunktes) rückgemeldet. Dieses Verfahren kann sich solange wiederholen, bis die komplette Informationsmenge übertragen wurde. Die Generierung der Folgenachrichten sollte automatisch, d. h. ohne Einwirkung des Benutzers, erfolgen.

Das Kreditinstitut kann die Gültigkeit der zurück gemeldeten Aufsetzpunkte zeitlich begrenzen, bei Aufträgen in synchronen Dialogen bleibt ein Aufsetzpunkt aber mindestens während des gesamten Dialogs gültig. Einen Abholauftrag mit einem nicht mehr gültigen Aufsetzpunkt wird das Kreditinstitut als fehlerhaft abweisen.

Maximale Anzahl Einträge

Dieser Parameter dient dazu, die maximale Anzahl Einträge für jedes der Antwortsegmente zu begrenzen. So wird Endgeräten, die aufgrund technischer Restriktionen nur eine begrenzte Anzahl rückgemeldeter Einträge (z. B. Umsatzinformationen im Kontoauszug) gleichzeitig verarbeiten können, die Möglichkeit gegeben, den Umfang der einzelnen Kreditinstitutsnachrichten zu begrenzen. Falls der Benutzer keine Begrenzung wünscht, wird das DE ausgelassen. Der Wert 0 ist nicht zulässig.

Falls im angegebenen Bereich weniger Einträge vorliegen als in „Maximale Anzahl Einträge“ angegeben, werden nur die vorliegenden Einträge rückgemeldet. Falls mehr Einträge vorliegen, werden laut untenstehender Tabelle pro Antwortsegment nur <Anzahl> Einträge rückgemeldet. In diesem Fall erhält das Kundensystem durch Rückmeldungscode 3040 (vgl. [RM-Codes]) mitgeteilt, dass noch weitere Informationen vorliegen. Im Rückmeldungsparameter wird dem Kundensystem ein Aufsetzpunkt (s. o.) zurückgemeldet, mit Hilfe dessen die über <Anzahl> hinausgehenden Einträge abgerufen werden können.

Beispiel:

In den Beispielen wird von 10 Einträgen ausgegangen. Sind weniger Einträge vorhanden, werden nur die vorhandenen übertragen.

Von Datum	Bis Datum	Anzahl	Bedeutung
01.07.2017	31.07.2017	10	liefert die <u>ersten</u> 10 Einträge ab 1.7.2017
01.07.2017	leer	10	liefert die <u>ersten</u> 10 Einträge ab 1.7.2017
leer	31.07.2017	10	liefert die <u>letzten</u> 10 Einträge vor dem 31.07.2017
leer	leer	10	liefert von allen verfügbaren Einträgen die <u>letzten</u> 10

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Benutzernachrichten allgemein	Stand: 06.10.2017	Seite: 50



Die Einträge werden dem Benutzer stets in aufsteigender Reihenfolge rückgemeldet. Eine hiervon abweichende Sortierung (z. B. absteigend oder nach anderen Kriterien) kann das Kundenprodukt bei Bedarf dem Benutzer anbieten.

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
3010	Es liegen keine Einträge vor
3040	Auftrag nur teilweise ausgeführt
3040	Es liegen weitere Informationen vor
9210	Keine gültige Kontoverbindung des Kunden
9210	Zeitraum hier nicht erlaubt
9210	Kennungen hier nicht erlaubt
9210	Bereichende darf nicht vor Bereichanfang liegen
9210	Aufsetzpunkt unbekannt

II.9.3 Transaktionsauftrag

Ein Transaktionsauftrag hat im Gegensatz zum Abholauftrag nicht nur einen Informationsfluss, sondern eine reale Transaktion auf Seiten des Kreditinstituts zur Folge (z. B. Überweisungsauftrag). Transaktionsaufträge haben spezielle Felder und Eigenschaften, die für den jeweiligen Geschäftsvorfall benötigt werden (siehe [Messages]).

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein	Stand: 06.10.2017	Seite: 51

II.10 Kreditinstitutsnachrichten allgemein

Eine Kreditinstitutsnachricht wird verschlüsselt übertragen, wenn der Nachrichtenkörper der Benutzernachricht verschlüsselt war. Nach der Entschlüsselung kann sie ggf. noch teilverschlüsselt sein. Dies ist sie genau dann, wenn die zugehörige Benutzernachricht teilverschlüsselt war. Analoges gilt für die Verwendung von Komprimierung.

Sowohl administrativer Teil als auch die Auftragsteile einer Kreditinstitutsnachricht sind optional. Allerdings ist es stets von der zugehörigen Benutzernachricht abhängig, welche Teile in der Kreditinstitutsnachricht anzugeben sind. Enthielt die Benutzernachricht einen administrativen Teil, so ist auch in der Kreditinstitutsnachricht ein administrativer Teil mit zugehörigen Antwortdaten einzustellen. Enthielt die Benutzernachricht einen Auftragsteil, so ist auch in der Kreditinstitutsnachricht ein Auftragsteil mit zugehörigen Antwortdaten einzustellen.



Die Antwortteile müssen in der Reihenfolge der zugehörigen Auftragsteile in die Nachricht eingestellt werden, damit das Kundensystem die Antworten zuordnen kann, falls es mehrere Auftragsteile erstellt hat.

Das Kreditinstitut stellt in die Nachrichtenköpfe seiner Nachrichten eine von ihm gewählte Kreditinstitutsreferenz ein, die es ihm ermöglichen soll, die eigenen Nachrichten zu verwalten. Die ggf. vom Benutzer im Nachrichtenkopf eingestellte Benutzerreferenz wird vom Kreditinstitut ebenfalls übernommen. Alle folgenden Nachrichten des laufenden Dialoges beider Seiten (Benutzer/Kreditinstitut) beinhalten damit jeweils identische Benutzer- und Kreditinstitutsreferenzen.

Signaturen und Verschlüsselungen sind analog zur zugehörigen Benutzernachricht aufzubauen: ein Auftragsteil einer Kreditinstitutsnachricht ist genau dann vom Kreditinstitut zu signieren, wenn der Auftragsteil signiert und ein Auftragsüberbringer angegeben war. Die Signatur ist hierbei so zu erstellen, dass sie von diesem Überbringer verifiziert werden kann.

War ein Benutzerauftragsteil zusätzlich zur Signatur auch verschlüsselt, so ist auch der zugehörige Antwortteil in der Kreditinstitutsnachricht zu verschlüsseln. Die Daten sind hierbei so zu verschlüsseln, dass sie der Auftragsüberbringer entschlüsseln kann.

Die Botensignatur der Kreditinstitutsnachricht ist so zu erstellen, dass der Bote der Benutzernachricht diese verifizieren kann.

Wenn der Nachrichtenkörper der Auftragsnachricht verschlüsselt war, ist der Nachrichtenkörper so zu verschlüsseln, dass er vom Boten der Benutzernachricht wieder entschlüsselt werden kann.

Es ist dem Kreditinstitut freigestellt, ob es als Signatur-ID (siehe [HBCI], Abschnitt *II.5.1 Signatur-Segment* und [HBCI], Abschnitt *II.4 Bankfachliche Anforderungen*) die vom Benutzer gesendete ID verwendet oder einen eigenen Zähler verwaltet.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein	Stand: 06.10.2017	Seite: 52



Falls Kreditinstitutsnachrichten signiert werden, hat das Kundenprodukt deren Signatur zu prüfen. Falls die Prüfung negativ ausfällt, hat es dem Benutzer eine entsprechende Rückmeldung zu geben und den Dialog zu beenden. Falls die Prüfung auch bei einem erneuten Dialog negativ ausfällt, muss von einem Sicherheitsproblem ausgegangen werden.

Durch das Senden eines verschlüsselten Benutzerauftragsteils kann dessen Herausgeber sicherstellen, dass der Bote der Benutzernachricht keine Kenntnis über den Inhalt des Auftragsteiles erhält. Darüber hinaus erreicht er, dass auch der zugehörige Kreditinstitutsauftragsteil für ihn verschlüsselt übertragen wird. Somit sind auch die zu den Aufträgen gehörenden Antwortdaten vor dem Boten verborgen. Die Kommunikation zwischen Herausgeber und Kreditinstitut kann vom Boten somit nicht eingesehen werden. Dennoch ist er in der Lage, Aufträge wie Antworten zwischen Herausgeber und Kreditinstitut zu übermitteln.

Die Unversehrtheit der Antwortdaten wird in jedem Fall durch die ggf. vorhandenen Kreditinstitutssignaturen sichergestellt. Der Bote kann in jedem Fall die Botensignatur verifizieren. Je nach verwendetem Sicherheitsverfahren könnte er ggf. auch die Signatur eines unverschlüsselten Kreditinstitutsauftragsteils verifizieren. In jedem Fall ist dies jedoch dem Herausgeber des zugehörigen Benutzerauftragsteils möglich.

II.10.1 Rückmeldungen zur Nachricht

Die Kreditinstitutsnachricht enthält beliebig viele Rückmeldungen zu Elementen der Nachricht sowie genau eine Gesamtrückmeldung.

Die Rückmeldungen beziehen sich auf diejenigen Teile der Nachricht, die außerhalb der Auftragsteile liegen (z. B. Initialisierung, Botensignatur, Nachrichtenkopf). Darüber hinaus können Rückmeldungen zu syntaktischen Fehlern in beliebigen Elementen der Nachricht enthalten sein, wenn solche Fehler dazu führen, dass die gesamte Nachricht nicht interpretierbar ist. Es sind keine inhaltlichen Rückmeldungen zum Benutzerauftragsteil enthalten.

Die Meldungen können eine Referenz auf ein Element der Benutzernachricht enthalten, auf das sie sich beziehen (z. B. Initialisierung).

Der Meldungscode der syntaktisch ausgezeichneten Gesamtrückmeldung gibt die maximale Rückmeldungs-kategorie über alle enthaltenen Rückmeldungen zur Nachricht, zu den Auftragsteilen und zu den Aufträgen an (siehe auch *II.11.2 Reaktionsvorschriften*).

Rückmeldungen zur Nachricht sind für den Boten einer Nachricht von Bedeutung. Aufgrund ihrer Position innerhalb der Nachrichtensyntax ist gewährleistet, dass sie nur für diesen verschlüsselt und signiert werden.

II.10.2 Rückmeldungen zum Auftragsteil

Der Kreditinstitutsauftragsteil enthält beliebig viele Rückmeldungen zu Elementen des Kreditinstituts- bzw. Benutzerauftragsteils sowie genau eine Gesamtrückmeldung.

Zu den an dieser Stelle möglichen Rückmeldungen zählen zum Beispiel Meldungen über Fehler bei der Ver- und Entschlüsselung. Inhaltliche Rückmeldungen zu einzelnen Aufträgen sind hier nicht enthalten.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein	Stand: 06.10.2017	Seite: 53

Die Meldungen können eine Referenz auf ein Element des Benutzerauftragsteils enthalten, auf das sie sich beziehen (z. B. eine Signatur).

Der Meldungscode der syntaktisch ausgezeichneten Gesamtrückmeldung gibt die maximale Rückmeldungsklasse über alle enthaltenen Rückmeldungen zu diesem Auftragsteil und zu dessen Aufträgen an (siehe auch *II.11.2 Reaktionsvorschriften*).

Rückmeldungen zum Auftragsteil sind insbesondere in Intermediärszenarien von Bedeutung: falls ein Benutzer dem Intermediär verschlüsselte Auftragsteile einreicht, erhält er die Rückmeldungen zum Auftragsteil für ihn verschlüsselt und signiert zurück. Die Rückmeldungen zur Nachricht sind hingegen nur für den Intermediär bestimmt.



Die Kreditinstitutsnachricht enthält grundsätzlich zu jedem Auftragsteil der Benutzernachricht einen entsprechenden Antwortteil („Kreditinstitutsauftragsteil“). Wenn ein gesamter Auftragsteil in der Kreditinstitutsantwort nicht aufgebaut werden kann (beispielsweise bei fehlgeschlagener Verschlüsselung, vgl. *II.10 Kreditinstitutsnachrichten allgemein*), enthält dieser lediglich eine oder mehrere Rückmeldungen zum Auftragsteil und keine Auftragsantworten.

II.10.3 Rückmeldungen zu Aufträgen

Zu jedem Auftrag des Benutzers wird mindestens eine Rückmeldung eingestellt (z. B. Auftrag verarbeitet, fehlerhafte Inhalte, unzureichende Berechtigungen). Abschnitt *II.11.2 Reaktionsvorschriften* beschreibt, nach welchen Regeln daraus der Verarbeitungsstatus des Auftrags hervorgeht.



Wird in einer Rückmeldung zu einem Auftrag gemeldet, dass dieser fehlerhaft war, dürfen keine Antwortdaten zu diesem Auftrag zurückgemeldet werden.

Rückmeldung und Antwortdaten dürfen nur dann beide fehlen, wenn der Auftrag aufgrund syntaktischer Fehler in der Auftragsnachricht gar nicht erkannt oder aufgrund kryptographischer Fehler nicht verarbeitet werden konnte (siehe *II.10.1 Rückmeldungen zur Nachricht*, *II.10.2 Rückmeldungen zum Auftragsteil*).

Rückmeldungen zu einem Auftrag sind für dessen Herausgeber und Zeugen von Bedeutung. Aufgrund ihrer Position innerhalb der Nachrichtensyntax ist gewährleistet, dass sie (falls dies vom Herausgeber gewünscht war) für diesen verschlüsselt und signiert werden.

II.10.4 Datensegmente

Zu einem Auftragssegment kann ein Datensegment definiert sein. Hier werden die Daten eingestellt, die über einen Verarbeitungsstatus hinausgehen (z. B. Kontoumsätze). Auf ein Benutzersegment hin (z. B. „Dauerauftragsbestand abrufen“) sendet das Kreditinstitut genau ein Antwort- bzw. Datensegment zurück. Datensegmente können mehrere Informationsblöcke enthalten (z. B. Daten zu mehreren Daueraufträgen). Datensegmente unterliegen einer Versionierung. Sie werden immer gemeinsam mit den zugehörigen Auftrags- und Parametersegmenten versioniert.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Kreditinstitutsnachrichten allgemein	Stand: 06.10.2017	Seite: 54



Falls das Kreditinstitut mehrere Versionen eines Geschäftsvorfalles unterstützt, hat es stets mit einem Segment derjenigen Version zu antworten, die dem Auftragssegment der Benutzernachricht entspricht.

Das Segmentformat ist beim jeweiligen Geschäftsvorfall in [Messages] spezifiziert.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Rückmeldungs_codes	Stand: 06.10.2017	Seite: 55

II.11 Rückmeldungs_codes

II.11.1 Grundkonzept

Die Änderung und Ergänzung von Rückmeldungs_codes erfolgt in Abstimmung mit allen beteiligten Verbänden (Gewährleistung der Multibankfähigkeit). Die aktuell definierten Rückmeldungs_codes sind dem Dokument [RM_Codes] zu entnehmen.

Institutsindividuelle Rückmeldungen (z. B. Konditionen, Werbung, Hinweise) sind über den Codebereich "Kreditinstitutsindividuelle Rückmeldung" zu generieren.



Die Rückmeldungs_codes sollen Kundensystemen automatisierte Reaktionen auf Kreditinstitutsnachrichten ermöglichen; z. B. kann bei der Rückmeldung "Institut falsch" das Kundensystem automatisiert zur Korrektur des Instituts (als Bestandteil der IBAN) aus einer hinterlegten Tabelle auffordern.

Der „Rückmeldungstext“ dient dazu, den Benutzer klartextliche Informationen zu übermitteln. Kundenprodukte sollten die kreditinstitutsseitigen Rückmeldungen im vollständigen Klartext anzeigen. Ebenso sollte der numerische Rückmeldungscode stets angezeigt werden, um den Kreditinstituten eine einfachere Bearbeitung von Kundenrückfragen zu spezifischen Rückmeldungstexten zu ermöglichen.

Rückmeldungen beziehen sich auf unterschiedliche Datenstrukturen (Nachricht, DEG, DE, etc.). In Bezug auf eine Datenstruktur können mehrere Rückmeldungen zurückgeliefert werden.



Der Umfang der Online-Prüfung (z. B. nur physische Entgegennahme der Nachricht oder auch Syntax- und bankfachliche Prüfung) ist kreditinstitutsindividuell.



II.11.2 Reaktionsvorschriften

Die Rückmeldungs_codes sind klassifiziert. Die erste Ziffer des Codes gibt die Klasse an:

- ◆ Erfolgsmeldung (Klasse 0)
- ◆ Hinweis (Klasse 1)
- ◆ Warnung (Klasse 3)
- ◆ Fehlermeldung (Klasse 9).

Für die Verwendung als Gesamtrückmeldung eines Auftragsteils oder der Nachricht gilt:

- ◆ Eine Erfolgsmeldung (Klasse 0) als Gesamtrückmeldung wird genau dann verwendet, wenn auf dieser Ebene und den niedrigeren Ebenen kein Rückmeldungscode der Klassen 3 oder 9 vorhanden ist. Sie zeigt damit an, dass alle Aufträge komplett bearbeitet wurden.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Rückmeldungscode	Stand: 06.10.2017	Seite: 56

- ◆ Eine Hinweismeldung (Klasse 1) wird als Gesamtrückmeldung nicht verwendet. Wenn auf dieser und den niedrigeren Ebenen nur Meldungen der Klassen 0 oder 1 enthalten sind, wird als Gesamtrückmeldung eine Erfolgsmeldung eingestellt.
- ◆ Eine Warnung (Klasse 3) als Gesamtrückmeldung wird genau dann verwendet, wenn auf dieser Ebene und den niedrigeren Ebenen mindestens ein Rückmeldungscode der Klassen 3, aber keiner der Klasse 9 vorhanden ist. Sie zeigt damit an, dass kein Auftrag komplett abgelehnt wurde, aber Warnungen vorliegen.
- ◆ Eine Fehlermeldung (Klasse 9) als Gesamtrückmeldung wird genau dann verwendet, wenn auf dieser Ebene und den niedrigeren Ebenen mindestens ein Rückmeldungscode der Klasse 9 vorhanden ist. Sie zeigt damit an, dass der Auftragsteil bzw. die Nachricht teilweise fehlerhaft ist und möglicherweise einzelne Aufträge abgelehnt wurden. Es sind dann die weiteren Einzelrückmeldungen zu prüfen.

Für die Verwendung als Rückmeldung zu einem Auftragsteil oder einer Nachricht gilt:

- ◆ Meldungen der Klassen 0, 1, 3 und 9 können ihrer Bedeutung entsprechend eingesetzt und beliebig kombiniert werden.

Für die Verwendung als Rückmeldung zu einem Auftrag sind nur bestimmte Kombinationen der Fehlerklassen zulässig, da der Verarbeitungsstatus des Auftrags stets eindeutig erkennbar sein muss:

Klasse 0 (Erfolg)	Klasse 1 (Hinweis)	Klasse 3 (Warnung)	Klasse 9 (Fehler)	Verarbeitungsstatus des Auftrags
1	0-n	0-n	-	angenommen
-	0-n	1-n	-	teilweise ausgeführt
-	0-n	0-n	1-n	abgelehnt

Um Kundenprodukten die Auswertung zu erleichtern, soll die jeweils wichtigste Meldung zum Auftrag als erste eingestellt werden (Klasse 0 oder 9, falls vorhanden)

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Rückmeldungscode	Stand: 06.10.2017	Seite: 57

Beispiel:

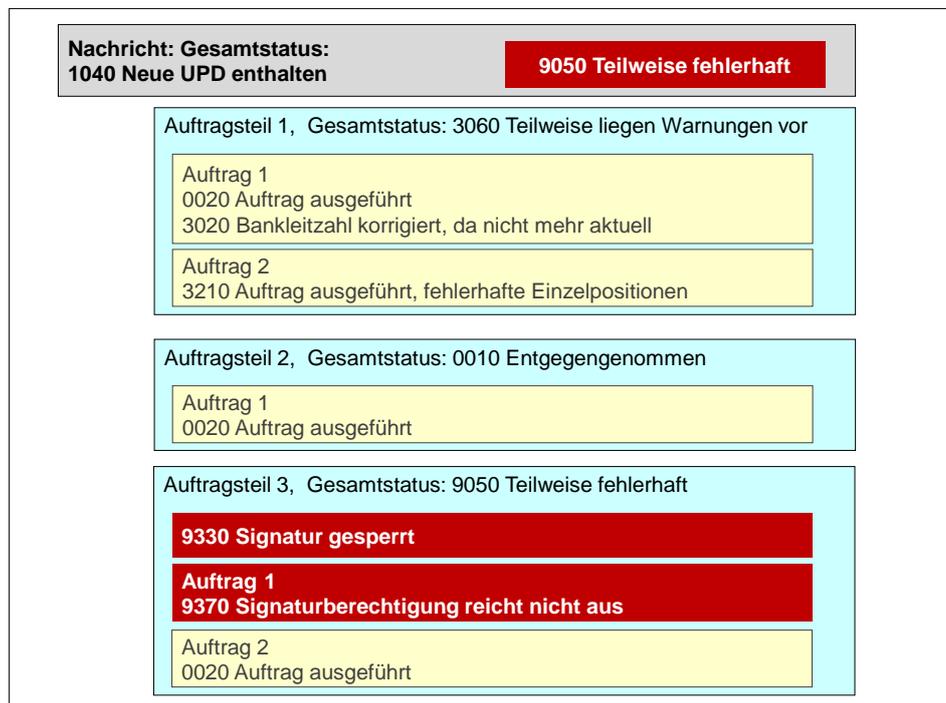


Abbildung 27: Fehlerreaktionsvorschriften (Beispiel)

Bei Syntaxfehlern innerhalb der Nachricht (z. B. Verstoß gegen die syntaktischen Festlegungen in [Syntax]) ist stets die gesamte Nachricht abzulehnen, weil bei fehlerhaften Nachrichtenteilen die Inhalte der restlichen Nachricht nicht zweifelsfrei rekonstruiert werden können. Bei inhaltlichen Fehlern im administrativen Teil oder im Nachrichtenkopf einer Nachricht wird diese ebenfalls nicht vom Kreditinstitut verarbeitet (vgl. auch *II.10.1 Rückmeldungen zur Nachricht*). Bei inhaltlichen Fehlern innerhalb eines Auftrages wird dieser Auftrag nicht weiter verarbeitet, die übrigen Aufträge jedoch schon, sofern sie inhaltlich fehlerfrei sind.

Eine Nachricht ist gültig, wenn sie entsprechend dem zugrunde gelegten XML-Schema aufgebaut ist.

Eine Nachricht, die die XML-Aufbauvorschriften grundlegend nicht einhält, muss nicht mit einer Kreditinstitutsnachricht beantwortet werden. In diesem Fall darf das Kreditinstitut von sich aus die Transportverbindung ohne Rückmeldung beenden. Ansonsten sind Nachrichten, die gegen grundlegende FinTS-Aufbauvorschriften verstoßen, mit dem Rückmeldungscode 9110 „Unbekannter Aufbau“ zu beantworten.

Grundsätzlich werden dem Benutzer alle auftretenden Meldungen mitgeteilt.

Ausnahmen:

- Tritt in einer Nachricht ein Fehler auf, der dazu führt, dass eine syntaktische Einheit (z. B. Nachricht, DEG) komplett ungültig ist oder nachfolgende Teile der syntaktischen Einheit ebenfalls fehlerhaft sind (Folgefehler), so kann die Bearbeitung der syntaktischen Einheit nach diesem Fehler abgebrochen werden.
- Zu nachgeordneten syntaktischen Einheiten brauchen keine Meldungen rückgemeldet zu werden, falls deren Code derselbe ist wie derjenige der übergeordneten syntaktischen Einheit (Beispiel: Falls die Nachricht insgesamt fehlerfrei ist,

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Rückmeldungscode	Stand: 06.10.2017	Seite: 58

brauchen für die einzelnen Segmente keine Erfolgsmeldungen rückgemeldet zu werden).



Wurde ein Auftrag abgelehnt, so ist darauf zu achten, dass nach der Fehlerbehebung bei einem eventuellen neuen Senden durch das Kundensystem die Nachricht neu aufgebaut wird, d. h. insbesondere eine neue Signatur eingestellt wird.

Bei Transaktionsaufträgen kann bei der kreditinstitutsinternen Verarbeitung unter Umständen ein Fehler auftreten, bei dem für das rückmeldende System nicht ersichtlich ist, ob der Fehler vor oder nach der Verarbeitung des Auftrags aufgetreten ist. In diesem Fall wird dem Kundenprodukt der Rückmeldungscode 9000 „Status indifferent“ mitgeteilt. Das Kundenprodukt darf den Auftrag anschließend nicht erneut einreichen, da er dann eventuell doppelt verarbeitet wird. Stattdessen hat der Benutzer den Status des Auftrags ggf. auf anderem Wege in Erfahrung zu bringen (vgl. *III.2 Statusprotokoll, falls dieses vom Institut unterstützt wird*). Das Kundenprodukt sollte dem Benutzer einen entsprechenden Hinweis geben.

II.11.3 Code-Bedeutungen

Die Bedeutung der einzelnen Rückmeldungscode wurde in ein separates Dokument „Financial Transaction Services (FinTS) – Rückmeldungscode“ [RM-Codes] ausgelagert.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Nachrichtentypen	Stand: 06.10.2017	Seite: 59

II.12 Nachrichtentypen

Die Nachrichten in FinTS können auf verschiedene Arten klassifiziert werden:

- bzgl. ihrer inhaltlichen Bedeutung,
- bzgl. ihres Senders oder
- bzgl. ihres syntaktischen Aufbaus.

Auf die inhaltliche Bedeutung verschiedener Nachrichten wird in späteren Kapiteln eingegangen. Hier soll zunächst nur der unterschiedliche syntaktische Aufbau betrachtet werden. Danach werden die Unterschiede im Aufbau von Benutzer- und Kreditinstitutsnachrichten betrachtet.

II.12.1 Unverschlüsselte Nachricht

Eine unverschlüsselte Nachricht besteht aus einem Nachrichtenkopf und einem Nachrichtenkörper, welcher alle weiteren Nachrichtenteile umfasst.

Der Nachrichtenkörper kann in einer Benutzernachricht eine Botensignatur, Initialisierungssegmente, administrative Segmente (z. B. Synchronisierung, Schlüsselanforderung) und/oder Auftragssegmente enthalten. In einer Kreditinstitutsnachricht kann er entsprechend die zugehörigen Rückmeldungs- und Antwortdatensegmente zu Initialisierung, administrativen Segmenten und/oder Aufträgen enthalten.

Bei den Auftrags- bzw. den zugehörigen Antwortsegmenten können weitere Signaturen eingestellt werden, die dann ausschließlich diese Segmente signieren (Auftragssignaturen). Im Folgenden werden diese Teile einer Nachricht *Auftragsteile* genannt. Alle Teile einer Nachricht, die sich auf Initialisierung und administrative Vorgänge beziehen, werden im Folgenden als *administrativer Teil* bezeichnet.

Auftragssignaturen signieren immer Aufträge (Geschäftsvorfälle) des sie enthaltenden Auftragsteils. Dies können alle Aufträge (in Abbildung 28 blau markiert) oder nur ausgewählte sein (in Abbildung 28 orange und türkis markiert).

Die Botensignatur signiert immer die vollständige Nachricht, also administrativen Teil, Auftragsteile und den Nachrichtenkopf (in Abbildung 28 gelb markiert). Hierbei kann im dargestellten Beispiel der Bote die Aufträge lesen aber nicht mehr verändern. Soll jedoch der Inhalt der Aufträge vor dem Boten verborgen werden, so ist der Weg über eine teilverschlüsselte Nachricht zu wählen, in der der Bote den Auftragsteil nur verschlüsselt erhält (siehe II.12.2 *Teilverschlüsselte Nachrichten*).

Unverschlüsselte Nachrichten können komprimiert sein. Die Komprimierung ist syntaktisch analog zu einer Verschlüsselung, siehe dazu die folgenden Abschnitte über

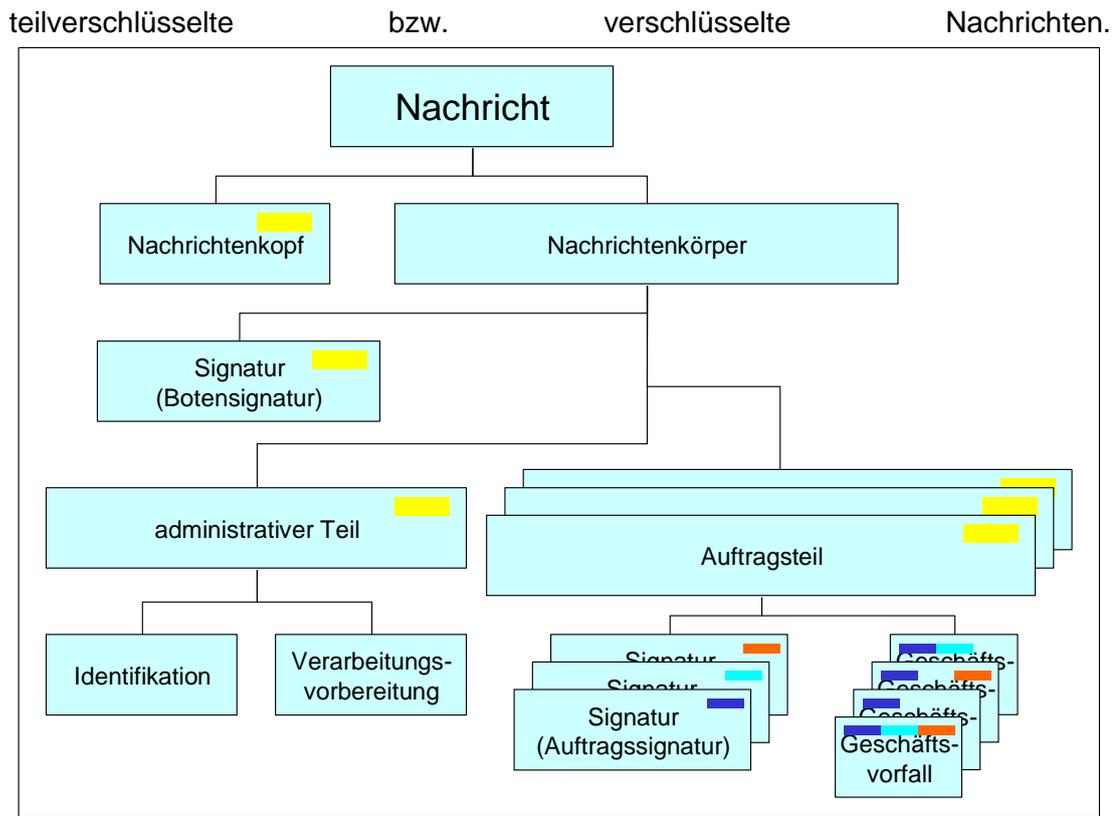


Abbildung 28: Unverschlüsselte Benutzernachricht

II.12.2 Teilverschlüsselte Nachrichten

FinTS bietet dem Herausgeber eines Auftragsteils die Möglichkeit, diesen gesondert zu verschlüsseln und so dessen Inhalt vor dem Boten zu verbergen (in Abbildung 29 rot/blau schattiert). Eine solche Nachricht, die verschlüsselte Auftragsteile enthält, deren übrige Segmente aber noch in unverschlüsselter Form vorliegen, heißt teilverschlüsselte Nachricht. Verschlüsselte und unverschlüsselte Auftragsteile können kombiniert werden.

Teilverschlüsselte Nachrichten werden in der Regel nicht direkt zwischen Benutzer und Kreditinstitut ausgetauscht, sondern können temporär als Zwischenprodukt auf dem Weg von einer unverschlüsselten zu einer verschlüsselten Nachricht und wieder zurück auftreten. Ihre Verwendung ist jedoch optional.

Ist Teilverschlüsselung vom Herausgeber gewünscht, so ist die Botensignatur erst über die teilverschlüsselte Nachricht zu erstellen, d. h. der Bote einer Nachricht signiert erst nach der Verschlüsselung der Auftragsteile (in Abbildung 29 gelb markiert). Der Inhalt des Auftragsteils kann so vom Herausgeber der Aufträge vor dem Boten verborgen werden, da dieser ihn nur in verschlüsselter Form erhalten muss.

Eine teilverschlüsselte Nachricht kann komprimiert sein. Dabei ist eine Komprimierung sowohl für verschlüsselte als auch für unverschlüsselte Auftragsteile sowie auch für den gesamten Nachrichtenkörper möglich. Die Komprimierung ist syntaktisch analog zur Verschlüsselung. Wird sie mit Verschlüsselung kombiniert, so wird zuerst komprimiert, dann verschlüsselt.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Nachrichtentypen	Stand: 06.10.2017	Seite: 61

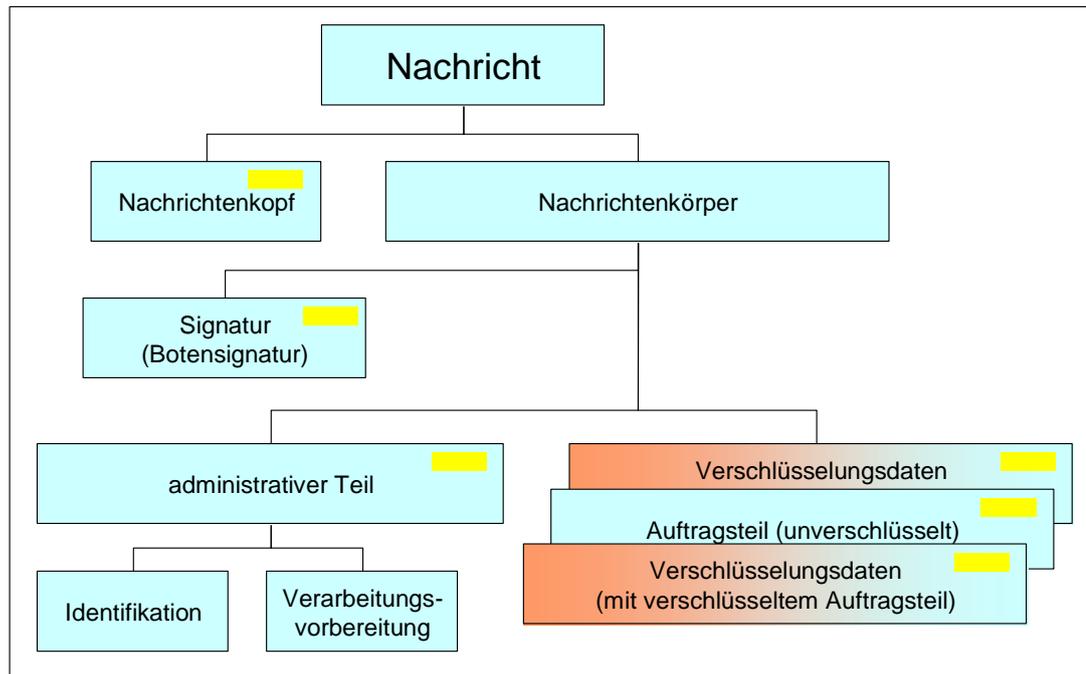


Abbildung 29: Teilverschlüsselte Benutzernachricht

II.12.3 Verschlüsselte Nachrichten

Eine verschlüsselte Nachricht besteht aus einem unverschlüsselten aber signierten Nachrichtenkopf und Verschlüsselungsdaten (siehe [HBCI], Abschnitt *II.5.2 Verschlüsselungsdaten*), welche den verschlüsselten Nachrichtenkörper enthalten. Eine verschlüsselte Nachricht kann wahlweise direkt aus einer unverschlüsselten Nachricht oder aus einer zunächst teilverschlüsselten Nachricht gebildet werden. Woraus sie gebildet wurde, ist einer verschlüsselten Nachricht nicht mehr zu entnehmen, sondern erst wieder nach deren Entschlüsselung.

Da der Nachrichtenkopf signiert ist (in Abbildung 30: Verschlüsselte Nachricht gelb markiert), ist er vor Veränderungen von außen geschützt. Die zugehörige Signatur ist jedoch Bestandteil der vom Boten verschlüsselten Daten und nicht lesbar (in Abbildung 30: Verschlüsselte Nachricht gelb/blau schattiert). Die Signatur kann daher erst nach der Entschlüsselung geprüft und Veränderungen des Nachrichtenkopfes erst dann festgestellt werden.

Eine verschlüsselte Nachricht kann komprimiert sein. Die Komprimierung ist syntaktisch analog zur Verschlüsselung und kann an allen Stellen vorkommen, an denen auch verschlüsselt werden kann. Wird sie mit der Verschlüsselung kombiniert, so wird zuerst komprimiert, dann verschlüsselt.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Nachrichtentypen	Stand: 06.10.2017	Seite: 62

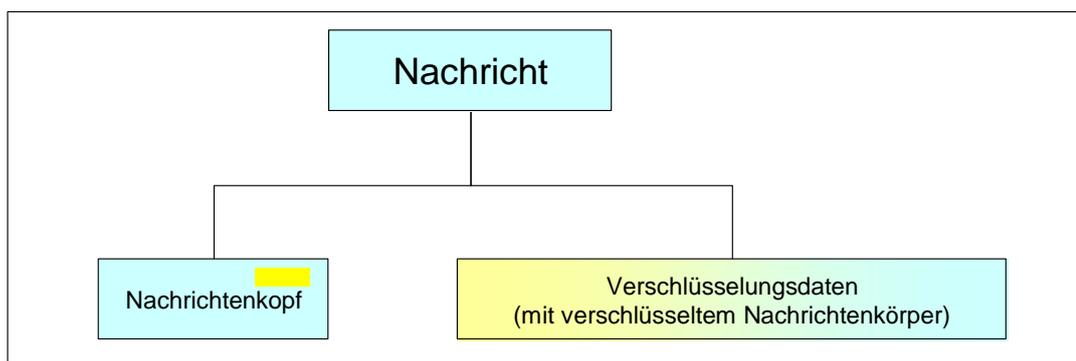


Abbildung 30: Verschlüsselte Nachricht

II.12.4 Vorgehensweise beim Signieren und Verschlüsseln

Für den Aufbau von signierten und verschlüsselten Nachrichten ist folgendes Vorgehen einzuhalten:

1. Ein Auftragsteil ist unverschlüsselt aufzubauen.
2. Herausgeber und Zeugen signieren den Auftragsteil. In einer Kreditinstitutsantwort wird für denjenigen Benutzer signiert, dessen Auftragssignatur in der zugehörigen Auftragsnachricht als Überbringersignatur (siehe auch [HBCI], Abschnitt *II.5.1 Signatur-Segment*) gekennzeichnet ist. Das Kreditinstitut signiert stets alle Antworten zu diesem Auftragsteil, unabhängig davon, welche Aufträge durch die Überbringersignatur signiert waren.
3. Soll eine teilverschlüsselte Nachricht aufgebaut werden, ist jetzt der Auftragsteil vom Herausgeber zu verschlüsseln und entsprechende Verschlüsselungsdaten zu bilden. In einer Kreditinstitutsantwort wird für denjenigen Benutzer verschlüsselt, dessen Auftragssignatur in der zugehörigen Auftragsnachricht als Überbringersignatur gekennzeichnet ist (siehe auch [HBCI], Abschnitt *II.5.1 Signatur-Segment*). Gegebenenfalls wird der Auftragsteil noch vor der Verschlüsselung komprimiert.
4. Nachrichtenkopf und administrativer Teil der Nachricht sind vom Boten zu erzeugen.
5. Der Bote erhält von den Herausgebern die unverschlüsselten Auftragsteile bzw. die Verschlüsselungsdaten mit verschlüsseltem Auftragsteil.
6. Der Bote baut den Nachrichtenkörper auf. Er signiert Nachrichtenkopf und Nachrichtenkörper.
7. Der Nachrichtenkörper ist vom Boten zu verschlüsseln und entsprechende Verschlüsselungsdaten zu bilden. Gegebenenfalls wird der Nachrichtenkörper noch vor der Verschlüsselung komprimiert.
8. Nachrichtenkopf und Verschlüsselungsdaten sind zur verschlüsselten Nachricht zusammenzufügen.

Ist der Herausgeber der Nachricht auch gleichzeitig Bote und sind keine Zeugensignaturen notwendig, kann auf die Auftragssignaturen verzichtet werden. Es wird stattdessen nur eine Botensignatur erstellt, die gleichzeitig auch als Herausgeber-signatur fungiert.

1. Der Auftragsteil ist unverschlüsselt aufzubauen.
2. Nachrichtenkopf und administrativer Teil der Nachricht sind zu erzeugen.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Nachrichtentypen	Stand: 06.10.2017	Seite: 63

3. Der Nachrichtenkörper wird aus administrativem Teil und Auftragsteilen aufgebaut (in diesem Szenario vorzugsweise nur ein Auftragsteil). Der Bote/Herausgeber signiert Nachrichtenkopf und Nachrichtenkörper.
4. Der Nachrichtenkörper ist vom Boten/Herausgeber zu verschlüsseln und entsprechende Verschlüsselungsdaten zu bilden, optional wird der Nachrichtenkörper noch vor der Verschlüsselung komprimiert.
5. Nachrichtenkopf und Verschlüsselungsdaten sind zur verschlüsselten Nachricht zusammenzufügen.

II.12.5 Vorgehensweise beim Entschlüsseln und Prüfen der Signaturen

Für das Entschlüsseln einer signierten Nachricht ergibt sich die folgende Vorgehensweise:

1. Der verschlüsselte Nachrichtenkörper ist zu entschlüsseln und anstelle der Verschlüsselungsdaten in die Nachricht einzustellen. Gegebenenfalls ist das Ergebnis der Entschlüsselung noch zu dekomprimieren. Man erhält eine unverschlüsselte bzw. eine noch teilverschlüsselte Nachricht.
2. Die Botensignatur ist zu überprüfen. Hierdurch kann die Unversehrtheit des Nachrichtenkopfes verifiziert werden.
3. Liegt eine teilverschlüsselte Nachricht vor, sind jetzt die verschlüsselten Auftragsteile zu entschlüsseln und anstelle der Verschlüsselungsdaten in die Nachricht einzustellen. Gegebenenfalls ist das Ergebnis der Entschlüsselung noch zu dekomprimieren. Man erhält eine unverschlüsselte Nachricht.
4. Die Auftragssignaturen sind zu überprüfen.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Verschlüsselung der Kommunikation	Stand: 06.10.2017	Seite: 64

II.13 Verschlüsselung der Kommunikation

Grundsätzlich sind sowohl alle Kunden- als auch alle Kreditinstitutsnachrichten einer Kommunikation zu verschlüsseln. Von dieser Regel ausgenommen sind die folgenden Kommunikationsarten:

- Anonymer Zugang (siehe *II.17 Anonymer Zugang*)
- Erstmalige Anforderung der öffentlichen Schlüssel des Kreditinstituts (siehe [HBCI], Abschnitt *II.6.1.2 Erstmalige Anforderung der Schlüssel des Kreditinstituts*)
- Schlüsselsperrung durch den Kunden (siehe [HBCI], Abschnitt *II.6.1.4 Schlüsselsperrung durch den Benutzer*)²
- Lebendmeldung (siehe *III.5.3 Lebendmeldung in Dialogen*)
- Kommunikationen, die über einen Weg abgewickelt werden, der eine Transportverschlüsselung bietet (vgl. [Anlagen], Abschnitt *I. Transportmedienspezifische Festlegungen*)



Unverschlüsselte Nachrichten, die keiner der oben genannten Ausnahmen zuzuordnen sind, sind vom empfangenden System abzulehnen.



Falls eine beabsichtigte Verschlüsselung der Kreditinstitutsnachricht nicht möglich ist, dürfen bestimmte Teile der Nachricht nicht gesendet werden:

- wenn der Antwortteil zu einem Auftragsteil nicht verschlüsselt werden kann, darf dieser Teil in der gesendeten Nachricht nicht enthalten sein.
- wenn der gesamte Nachrichtenkörper nicht verschlüsselt werden kann, dürfen keine unverschlüsselten Antwortteile in der gesendeten Nachricht enthalten sein.

Alle Benutzernachrichten einer Kommunikation sind vom Boten der Nachricht für das Kreditinstitut zu verschlüsseln. Alle Kreditinstitutsnachrichten sind vom Kreditinstitut für den Boten der Benutzernachricht zu verschlüsseln.

War der Auftragsteil einer Benutzernachricht vom Herausgeber verschlüsselt, so ist auch der Auftragsteil der Kreditinstitutsnachricht für den Herausgeber zu verschlüsseln.

Bote und Kreditinstitut haben stets dasselbe Verschlüsselungs- und Signaturverfahren anzuwenden. Gleiches gilt für Herausgeber und Kreditinstitut. Ein Benutzer gibt in den Verschlüsselungsdaten (siehe [HBCI], Abschnitt *II.5.2 Verschlüsselungsdaten*)

² Es liegt im Ermessen des Kreditinstituts, ob es auch unverschlüsselte Sperren (z. B. aufgrund Schlüsselverlust des Kunden) entgegennimmt.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Verschlüsselung der Kommunikation	Stand: 06.10.2017	Seite: 65

ten) den von ihm verwendeten Verschlüsselungsalgorithmus und dessen Version an und bestimmt damit ebenfalls den Algorithmus und die Version, den das Kreditinstitut anzuwenden hat. Bote, Herausgeber und Zeugen dürfen jedoch unterschiedliche Verfahren verwenden, sofern dies nicht durch die BPD ausgeschlossen wird (siehe *IV.2.3 Sicherheitsverfahren*).

Weder Benutzer noch Kreditinstitut dürfen das Verfahren während des Dialoges wechseln. Das vom Kreditinstitut anzuwendende Verfahren ist im Falle eines Verfahrenswechsels durch den Benutzer nicht definiert, d. h. das Kreditinstitut kann in diesem Fall mit einer unverschlüsselten und unsignierten Antwort den Dialog beenden.

Ein Benutzer darf nur ein Verfahren wählen, das vom Kreditinstitut unterstützt wird. Die vom Kreditinstitut unterstützten Verfahren werden dem Kundensystem in den Bankparameterdaten im Segment „Sicherheitsverfahren“ (siehe *IV.2.3 Sicherheitsverfahren*) mitgeteilt.



Falls das Kreditinstitut das vom Benutzer gewählte Verschlüsselungsverfahren nicht unterstützt, ist dem Benutzer eine entsprechende Rückmeldung zu geben und der Dialog zu beenden. Das Kundenprodukt kann diese Nachricht möglicherweise nicht entschlüsseln, wenn es das Verschlüsselungsverfahren des Kreditinstituts nicht unterstützt. Das Kundenprodukt hat in diesem Fall den Verschlüsselungsdaten der Kreditinstitutsnachricht zu entnehmen, dass es ein dem Kreditinstitut nicht bekanntes Verschlüsselungsverfahren verwendet. In diesem Fall hat der Bote über den (unverschlüsselten) anonymen Zugang die aktuellen Bankparameterdaten anzufordern, in denen die Verschlüsselungsverfahren des Kreditinstituts angegeben sind. Ggf. muss der Bote den Herausgeber informieren, wenn das von diesem gewählte Verfahren nicht unterstützt wird.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Komprimierung	Stand: 06.10.2017	Seite: 66

II.14 Komprimierung

Alle Benutzer- und Kreditinstitutsnachrichten mit Ausnahme der Benutzernachricht zur Lebendmeldung können optional komprimiert werden. Dies gilt auch für Nachrichten in einer anonymen Kommunikation. Die Komprimierung findet stets vor einer eventuellen Verschlüsselung statt.

War die Benutzernachricht vom Boten komprimiert, so ist auch die gesamte Kreditinstitutsnachricht komprimiert. War der Auftragsteil einer Benutzernachricht vom Herausgeber komprimiert, so ist auch der Auftragsteil der Kreditinstitutsnachricht zu komprimieren.

Bote und Kreditinstitut wenden stets dasselbe Komprimierungsverfahren an. Gleiches gilt für Herausgeber und Kreditinstitut. Der Bote der Benutzernachricht bzw. der Herausgeber eines Auftragsteils bestimmen dabei das zu verwendende Verfahren. Bote und Herausgeber dürfen allerdings durchaus unterschiedliche Verfahren einsetzen. Das Kreditinstitut kann vorgeben, welche Komprimierungsverfahren es unterstützt (siehe *IV.2.4 Komprimierungsverfahren*).



Falls die beabsichtigte Komprimierung der Kreditinstitutsnachricht oder eines Antwortteils nicht möglich ist, wird der betreffende Teil unkomprimiert aufgebaut.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Initialisierung	Stand: 06.10.2017	Seite: 67

II.15 Initialisierung

Die erste Nachricht eines Dialogs und jedes Datagramm enthalten eine Initialisierung. Die Initialisierung dient folgenden Zwecken:

1. Prüfung, ob der Kommunikationspartner ein sendeberechtigter Benutzer ist
2. Festlegung der Benutzer- und Kreditinstitutsreferenzen
3. Prüfung auf Aktualität der im Kundensystem vorhandenen BPD und UPD sowie ggf. deren Aktualisierung
4. Prüfung auf Aktualität der öffentlichen Schlüssel des Kreditinstituts sowie ggf. deren Aktualisierung (nur bei asymmetrischen Sicherheitsverfahren)
5. Übermittlung vorbereitender Informationen für die kunden- und kreditinstitutsseitige Verarbeitung
6. Übertragung von Kreditinstitutsmeldungen

Während die Aufträge einer Nachricht von deren Herausgeber und ggf. deren Zeugen zu signieren sind, wird die Initialisierung von demjenigen Benutzer signiert, welcher in der Rolle des Boten auftritt. Im Regelfall ist dieser Benutzer auch Herausgeber der nachfolgenden Aufträge. Während eines Dialoges dürfen nur Aufträge für Auftraggeberkonten gesendet werden, die der bei der Initialisierung angegebenen Kunden-ID zugeordnet sind.

II.15.1 Benutzernachricht

Realisierung Kreditinstitut: verpflichtend
Realisierung Kundenprodukt: verpflichtend

Die Initialisierung innerhalb einer Benutzernachricht besteht aus einer Identifikation und einer Verarbeitungsvorbereitung. Der genaue Aufbau dieser Segmente wird im Kapitel Syntax näher beschrieben. Dort findet sich auch ein Beispiel.

II.15.1.1 Identifikation

Das Identifikations-Segment wird vom Benutzer gesendet. Es enthält Kontextinformationen, die für die gesamte Kommunikation Gültigkeit haben. Anhand dieser Daten wird die Sendeberechtigung des Benutzers geprüft. Eine Prüfung der transportmedienspezifischen Kennung (z. B. E-Mail-Adresse) des Benutzers erfolgt nicht.

Falls dem Benutzer die Berechtigung zum Senden weiterer Nachrichten nicht erteilt werden kann, ist ein entsprechender Rückmeldungscode in die Kreditinstitutsantwort einzustellen. Es steht Kreditinstituten frei, in bestimmten Fällen auf eine Identifizierung des Benutzers zu verzichten. Dies ist zum Beispiel für den anonymen Zugang erforderlich, bei dem z. B. mit einem Nichtkunden kommuniziert wird.

Die Identifikation umfasst die folgenden Daten:

Kreditinstitutskennung

Es ist die Kennung des Kreditinstituts anzugeben, zu dem der Zugang gewünscht wird. In nachfolgenden Auftragsnachrichten dürfen nur Auftraggeberkonten dieses Kreditinstituts angegeben werden.

Kunden-ID

Es ist diejenige Kunden-ID des Benutzers einzustellen, welche die Rolle festlegt, in der er im Rahmen der Kommunikation auftritt (siehe *II.1.3 Benutzer*

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Initialisierung	Stand: 06.10.2017	Seite: 68

und Kunde). Diese Kunden-ID gilt ebenso für eventuelle Zweit- und Drittsignierende.

◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0020	Informationen fehlerfrei entgegengenommen
9210	Unbekannter Kunde

II.15.1.2 Verarbeitungsvorbereitung

Die Verarbeitungsvorbereitung wird vom Benutzer gesendet. Sie dient der Übermittlung von Informationen über das Kundensystem, mit Hilfe derer das Kreditinstitut individuell auf Anforderungen des Benutzers reagieren kann.

Die Verarbeitungsvorbereitung umfasst die folgenden Daten:

BPD-Version

Es ist die aktuelle Version der im Kundenprodukt vorliegenden BPD einzustellen. Falls noch keine BPD vorliegen, ist der Wert auszulassen. Anhand dieser Information prüft das Kreditinstitut, ob der Benutzer über die aktuelle BPD verfügt.

UPD-Version

Es ist die aktuelle Version der im Kundenprodukt vorliegenden UPD einzustellen. Falls noch keine UPD vorliegen, ist der Wert auszulassen. Anhand dieser Information prüft das Kreditinstitut, ob der Benutzer über die aktuelle UPD verfügt.

Dialogsprache

Der Benutzer darf lediglich ein Sprachkennzeichen einstellen, das im Rahmen der BPD vom Kreditinstitut an das Kundensystem übermittelt wurde.

Wenn noch keine BPD vorliegen, sollte das Kundensystem den Wert „0“ einstellen. Das Kreditinstitut antwortet in diesem Fall in seiner Standardsprache durch ein entsprechendes Länderkennzeichen gemäß ISO-639-1.

Produktname

Der Benutzer hat hier den Namen seines Kundenproduktes anzugeben.

Produktversion

Der Benutzer hat hier die Version seines Kundenproduktes anzugeben.

Produktidentifikator

Wenn zwischen Kreditinstitut und Produkthersteller die Lieferung eines Produktidentifikators vereinbart ist, sollte dieser vom Kundenprodukt hier eingestellt werden. Anhand des Produktidentifikators können z. B. für dieses Kundenprodukt auf Basis von Vereinbarungen zusätzliche Services bereitgestellt werden. Die Reaktion auf einen fehlenden oder unbekanntem Produktidentifikator ist institutsspezifisch. Produktidentifikatoren können abhängig vom Institut z. B. alphanumerische Kennungen oder Zertifikate sein.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Initialisierung	Stand: 06.10.2017	Seite: 69

◆ Ausgewählte Beispiele für Rückmeldungscode

Code	Beispiel für Rückmeldungstext
0020	Informationen fehlerfrei entgegengenommen
1010	Es liegen neue Kontoinformationen vor
1040	BPD nicht mehr aktuell. Aktuelle Version folgt
1050	UPD nicht mehr aktuell. Aktuelle Version folgt
3340	RAH-10-Kundenschlüssel neu generieren und einreichen. Wird noch ... Tage akzeptiert.
9210	Sprache wird nicht unterstützt
9210	Produktidentifikator nicht unterstützt

Zwangswise Wechsel der Schlüssel des Kunden

Mit dem Rückmeldungscode 3340 kann das Kreditinstitut dem Kundensystem signalisieren, dass es die RAH-10-Kundenschlüssel neu generieren soll. Dies kann z. B. bei einer Aufhebung der Einschränkungen bezüglich der maximalen Schlüssellängen des Bankenprofils (siehe [HBCI], Abschnitt *II.1.1 Sicherheitsprofile*) erforderlich sein. Die neu generierten öffentlichen RAH-10-Schlüssel des Kunden müssen anschließend an das Kreditinstitut übermittelt werden (siehe [HBCI], Abschnitt *II.6.1.1 Änderung eines öffentlichen Schlüssels des Benutzers*).

II.15.2 Kreditinstitutsnachricht

Realisierung Kreditinstitut: verpflichtend
Realisierung Kundenprodukt: verpflichtend

Sofern die Initialisierungsnachricht des Benutzers fehlerhaft ist, darf die Kreditinstitutsnachricht nur dazu genutzt werden, dem Benutzer die betreffenden Rückmeldecodes mitzuteilen. Es dürfen in diesem Fall keine Datensegmente (z. B. BPD, UPD) rückgemeldet werden.

Andernfalls umfassen die Antwortdaten zu einer Initialisierung die aktuellen Bank- und User-Parameterdaten (falls neue vorliegen), die Übermittlung öffentlicher Schlüssel des Kreditinstituts (falls aktualisiert) und aktuelle Kreditinstitutsmeldungen (freie Textmeldungen des Instituts). Ein Beispiel findet sich in [Syntax].

◆ Ausgewählte Beispiele für Rückmeldungscode

Code	Beispiel
0020	Initialisierung erfolgreich
9800	Dialogabbruch

II.15.2.1 Bankparameterdaten

Die Bankparameterdaten werden vom Kreditinstitut gesendet. Entspricht die vom Benutzer übermittelte BPD-Version nicht der aktuellen im Kreditinstitut gespeicherten Version, so erhält der Benutzer automatisch die aktuellen Bankparameterdaten. Dies gilt auch, wenn ihm zu einem früheren Zeitpunkt bereits dieselben BPD gesendet wurden. Die BPD werden sofort aktiv, d. h. sie sollten dann vom Kundenprodukt unmittelbar verwendet werden.

Die Bankparameterdaten müssen stets komplett übertragen werden, das Auslassen einzelner Segmente ist nicht zulässig.

In den Bankparameterdaten wird vom Kreditinstitut angegeben, welche Geschäftsvorfälle mit welchen Restriktionen zulässig sind, welche Sicherheits- und Komprimierungsverfahren zur Verfügung stehen und welche Kommunikationszugänge ge-

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Initialisierung	Stand: 06.10.2017	Seite: 70

wählt werden können. Eine genaue Beschreibung des Aufbaus der Bankparameterdaten befindet sich in Kapitel *IV BANKPARAMETERDATEN (BPD)*.



Da die Bankparameterdaten im administrativen Teil der Nachricht übertragen werden, sind sie im Intermediärszenario zunächst lediglich für den Intermediär sichtbar. Mittels eines speziellen Auftrags können jedoch auch in diesem Szenario die Benutzer die BPD selbst anfordern: siehe *IV.3 Anforderung der BPD in einem Szenario mit Intermediär*.



II.15.2.2 User-Parameterdaten

Die User-Parameterdaten werden vom Kreditinstitut gesendet. Entspricht die vom Benutzer übermittelte UPD-Version nicht der aktuellen im Kreditinstitut gespeicherten Version, so erhält der Benutzer automatisch die aktuellen User-Parameterdaten. Dies gilt auch, wenn ihm zu einem früheren Zeitpunkt bereits dieselben UPD gesendet wurden. Die UPD werden sofort aktiv, d. h. sie sollten dann vom Kundenprodukt unmittelbar verwendet werden.

In den UPD eines Benutzers wird vom Kreditinstitut angegeben, welche weiteren Restriktionen für diesen Benutzer gelten. So kann hier der Zugriff auf Konten und der je Konto zulässige Umfang an Geschäftsvorfällen weiter eingeschränkt werden. Eine genaue Beschreibung des Aufbaus der User-Parameterdaten befindet sich in Kapitel *V USER-PARAMETERDATEN (UPD)*.



Es ist zu beachten, dass lediglich die User-Parameterdaten des Boten aktualisiert werden. Falls mehrere Benutzer an der Erstellung der Aufträge beteiligt sind (Herausgeber und Zeuge), so ist sicherzustellen, dass auch für die passiven Benutzer, die die Aufträge nicht versenden, sondern lediglich signieren, stets die aktuellen UPD vorliegen.



Hierzu haben sich die passiven Benutzer in regelmäßigen Abständen beim Kreditinstitut mit einer Initialisierung anzumelden, damit ggf. ihre User-Parameterdaten aktualisiert werden können. Dieses Verfahren kann vom Kundenprodukt durch eine automatische Aufforderung unterstützt werden.

In Intermediär-Szenarien verwenden die Benutzer einen speziellen Auftrag zur Abfrage ihrer speziellen UPD für den Intermediärzugang (siehe *V.6 Explizite Anforderung von UPD*).

Gleiches gilt für den Intermediär selbst, der zusätzlich zu seinen eigenen auch die UPD seiner Benutzer für den Intermediärzugang anfordern möchte.

II.15.2.3 Übermittlung eines öffentlichen Schlüssels

Eine Übermittlung öffentlicher Schlüssel wird vom Kreditinstitut gesendet. Falls einer der öffentlichen Schlüssel des Kreditinstituts aktualisiert wurde, werden dem Benutzer diese in diesem Segment zurückgemeldet. Das Segment kann sowohl für den Signierschlüssel als auch für den Chiffrierschlüssel eingestellt werden. Hat sich der jeweilige Schlüssel nicht geändert, so wird das Segment nicht gesendet.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Initialisierung	Stand: 06.10.2017	Seite: 71

Zur Verifizierung der Richtigkeit des öffentlichen Schlüssels muss entweder die Initialisierungs-Antwortnachricht signiert sein oder es muss auf alternativem Weg (z. B. Ini-Brief) ein neuer Hash-Wert übermittelt werden.

Der genaue Aufbau ist in [Syntax] beschrieben.



Es wird nur die Aktualität der Schlüssel desjenigen Benutzers geprüft, der als Bote der Nachricht auftritt. Für die anderen beteiligten Benutzer gilt wie auch für die automatische Aktualisierung der BPD und UPD, dass die Benutzer sich für die Aktualisierung selbst in der Botenrolle initialisieren oder den speziellen Geschäftsvorfall für den Abruf der Schlüssel senden müssen ([HBCI], Abschnitt *II.6.1.2 Erstmalige Anforderung der Schlüssel des Kreditinstituts*).

II.15.2.4 Kreditinstitutsmeldung

Kreditinstitutsmeldungen werden vom Kreditinstitut gesendet. Sie können z. B. Werbenachrichten oder auch kundenrelevante Informationen zu Geschäftsvorfällen beinhalten, die nicht in Rückmeldungs-codes abgebildet werden können. Diese werden dem Benutzer automatisch im Rahmen der Initialisierungsantwortnachricht übermittelt. Dadurch wird gewährleistet, dass die Zustellung dieser Meldungen nicht auf Initiative des Benutzers erfolgen muss.

Eine Kreditinstitutsmeldung besteht aus einem Betreff-Feld und einer Freitextmeldung. Es ist lediglich die Übermittlung von unformatierten Textnachrichten möglich.



Kreditinstitutsmeldungen können dem Benutzer unmittelbar nach Erhalt, also zum Beispiel während im Hintergrund der Dialog abläuft, angezeigt werden.

Hersteller von Kundenprodukten sollten darüber hinaus eine Möglichkeit zur Verwaltung von Kreditinstitutsmeldungen vorsehen. Falls mehrere Meldungen gleichzeitig vorliegen, sollte der Benutzer die Möglichkeit haben, die Meldungen nacheinander zu bearbeiten (Funktionen „Nächste lesen“, „Vorherige lesen“). Ferner sollten Kreditinstitutsmeldungen gespeichert, gelöscht und ausgedruckt werden können.

II.15.3 Empfehlung für die Bildung von Kommunikationsreferenzen

◆ Kommunikationsreferenz

Jede Nachricht muss von Kundenseite als auch Kreditinstitutsseite eindeutig identifiziert und einem Dialog zugeordnet werden können. Dazu muss ein eindeutiger Wert erzeugt werden, welcher auf den zur Nachricht gehörenden Dialog verweist. Nachrichten des gleichen Dialoges sind darüber hinaus durch eine eindeutige Nummerierung voneinander unterscheidbar. Eine Kommunikationsreferenz wird vom Benutzer und dem Kreditinstitut als Benutzer- bzw. Kreditinstitutsreferenz in die Nachricht eingestellt.

Bei der Bildung von Kommunikationsreferenzen sollte darauf geachtet werden, dass diese möglichst eindeutig über Kunden- und Kreditinstitutsgrenzen hinweg sind. Der zur Bildung verwendete Algorithmus sollte dies mit möglichst hoher Wahrscheinlichkeit sicherstellen. Eine echte Eindeutigkeit der Benutzerreferenz ist jedoch nur für

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Initialisierung	Stand: 06.10.2017	Seite: 72

den betreffenden Benutzer notwendig. Gleiches gilt für die Kreditinstitutsreferenz und das betreffende Kreditinstitut.

Die Hersteller von Kunden- bzw. Institutssystemen müssen die Eindeutigkeit dieser Referenzen sicherstellen.

◆ **Zusätzliche textuelle Referenz**

Über die technische Kommunikationsreferenz hinaus können Nachrichten vom Benutzer mit einer weiteren textuellen Referenz versehen werden. Diese Referenz ist ein beliebig zu wählender Text. Die Belegung der Referenz ist optional, kann aber für einzelne Transportverfahren verpflichtend sein. Eine Eindeutigkeit der textuellen Referenz wird nicht gefordert. Auch können sie sich für verschiedene Nachrichten des gleichen Dialoges unterscheiden.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Dialogabbruchnachricht	Stand: 06.10.2017	Seite: 73

II.16 Dialogabbruchnachricht

In bestimmten Fällen kann es erforderlich sein, dass das Kreditinstitut aufgrund einer fehlerhaften Benutzernachricht oder eines kreditinstitutsinternen Problems einen Dialog abbrechen muss.

Bei einem solchen Dialogabbruch muss unterschieden werden, ob es sich bei der zu verarbeitenden Benutzernachricht um eine Initialisierungsnachricht oder um eine Auftragsnachricht handelt, da abhängig davon dem Kreditinstitutssystem eventuell nicht alle Daten wie Nachrichtennummer oder Dialog-ID zur Verfügung stehen. In bestimmten Situationen kann dann das Kreditinstitut eine unverschlüsselte und nicht signierte Nachricht mit festem Aufbau an das Kundensystem senden.

Folgende Situationen, in denen ein Dialog durch das Kreditinstitut abgebrochen werden muss, sind u. a. denkbar:

- Kreditinstitut vorübergehend gesperrt (Release-Einsatz)
- BLZ unbekannt (nach einer Fusion)
- Fehlerhafter Nachrichtenkopf
- Unbekannte HBCI- bzw. FinTS-Version (wird nicht mehr unterstützt)

Zusätzlich besteht die Möglichkeit eines unbeantworteten Dialogabbruchs bei schwerwiegenden Fehlern (siehe *II.11.2 Reaktionsvorschriften*) sowie durch Timeout (siehe *IV.2.2 Kommunikationszugang*).

Die Abbruchnachricht hat den Aufbau einer unverschlüsselten und unsignierten Kreditinstitutsnachricht mit leerem Auftragsteil, deren administrativer Teil ausschließlich Rückmeldungen zur Gesamtnachricht enthält und in der das Endkennzeichen gesetzt ist.

Der Nachrichtenkopf der Nachricht ist soweit wie möglich mit gültigen Werten zu befüllen. Falls dies nicht möglich ist (z. B. Benutzerreferenz nicht bekannt), sind die Felder auszulassen.

Die Rückmeldungen zur Gesamtnachricht sind mit Rückmeldungs-codes und Texten zu belegen, die den aufgetretenen Fehler möglichst genau angeben.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Anonymer Zugang	Stand: 06.10.2017	Seite: 74

II.17 Anonymer Zugang

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

Um Benutzern die Möglichkeit zu geben, sich anonym anzumelden, um sich z. B. über die angebotenen Geschäftsvorfälle fremder Kreditinstitute (von denen sie keine BPD besitzen) zu informieren bzw. nicht-signierungspflichtige Aufträge bei fremden Kreditinstituten einreichen zu können, kann sich der Benutzer anonym (als Gast) anmelden.

Bei anonymem Zugang werden Nachrichten weder signiert, noch können sie verschlüsselt werden. Eine Komprimierung ist allerdings optional zulässig.

Das Nachrichtenformat für den anonymen Zugang ist so gestaltet, dass eine anonyme Nachricht grundsätzlich eine Initialisierung enthält und das Endekennzeichen gesetzt ist. Damit entspricht jede anonyme Nachricht formal einem Datagramm; mehrschrittige Dialoge sind über den anonymen Zugang nicht möglich. Der anonyme Zugang kann unabhängig davon jedoch sowohl in synchroner als auch in asynchroner Kommunikation genutzt werden.

II.17.1 Administrativer Teil

a) Benutzernachricht

Es darf keine Botensignatur erstellt werden. Die Nachricht darf nicht verschlüsselt werden. Eine Komprimierung ist möglich.

b) Kreditinstitutsnachricht

Falls das Kreditinstitut seine Nachrichten auch in anonymen Dialogen signieren möchte, so kann es dies durch Einstellen einer Botensignatur tun. Weitere Signaturen sind nicht zulässig. Eine Verschlüsselung ist ebenfalls nicht zulässig.

II.17.2 Initialisierung

a) Benutzernachricht

Für den Initialisierungsteil einer anonymen Benutzernachricht ist ein spezieller Identifikationsteil definiert, für den die folgenden Belegungsrichtlinien gelten:

Anonyme Identifikation

Die Datenelemente der anonymen Identifikation sind wie folgt zu belegen:

- Kreditinstitutskennung: Länderkennzeichen und Kreditinstitutskennung (Bank-Code, in Deutschland i. A. die BLZ) des gewünschten Kreditinstituts
- die Kunden-ID kann nicht angegeben werden.

Verarbeitungsvorbereitung

Mit diesem Segment fordert der Benutzer die Bankparameterdaten des Kreditinstituts und, falls vorhanden, die User-Parameterdaten des anonymen Benutzers an.

Sofern schon von einem früheren anonymen Zugang Bank- oder User-Parameterdaten dieses Kreditinstituts vorliegen, ist die jeweilige Versionsnummer anzugeben.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: II
Kapitel: Szenarien und Nachrichtenaufbau Abschnitt: Anonymer Zugang	Stand: 06.10.2017	Seite: 75

b) Kreditinstitutsnachricht

Die Antwort auf eine anonyme Initialisierung enthält niemals öffentliche Schlüssel des Kreditinstituts, ist ansonsten aber identisch zu einer personalisierten Initialisierungsantwort aufgebaut. Auch die Bankparameterdaten sind inhaltlich identisch.

Bei den User-Parameterdaten und den Kreditinstitutsmeldungen ist Folgendes zu beachten:

User-Parameterdaten

In den Gast-UPD (siehe *V.3 UPD für anonymen Zugang*) sind diejenigen Geschäftsvorfälle aufgeführt, die der Gast ausführen darf. Dies können jedoch nur Geschäftsvorfälle sein, für die keine Signatur erforderlich ist, wie z. B. der Abruf von Börsenkursen oder die Sendung einer Gastmeldung (die Festlegung, für welche Geschäftsvorfälle eine Signatur erforderlich ist, ist kreditinstitutsspezifisch).

Kreditinstitutsmeldung

Bei den Meldungen kann es sich lediglich um allgemeine, d. h. nicht benutzerspezifische Informationen handeln.

II.17.3 Auftragsteil

a) Benutzernachricht

Es sind keine Signaturen einzustellen, noch ist der Auftragsteil zu verschlüsseln.

Es dürfen lediglich nicht-signierungspflichtige Geschäftsvorfälle (z. B. Abruf von Börsenkursen, Gastmeldung) eingestellt werden. Welche Geschäftsvorfälle signierungspflichtig sind, bestimmt das Kreditinstitut in der UPD des Kunden.

Fall ein Kreditinstitut dem anonymen Benutzer Geschäftsvorfälle mit Kontobezug bereitstellt, so sind diese Geschäftsvorfälle sowie die zugehörigen Konten (Demokonten) in der UPD des anonymen Benutzers aufgeführt.

Außer der Erstanforderung der öffentlichen Kreditinstitutsschlüssel sind über den anonymen Zugang keine weiteren administrativen Vorgänge (z. B. Synchronisierung, Schlüsseländerung) möglich.

b) Kreditinstitutsnachricht

Die Antwortdaten zu den zuvor eingereichten Aufträgen sind wie im personalisierten Fall aufzubauen. Es ist keine Signatur zu erstellen. Falls das Kreditinstitut Antwortnachrichten innerhalb anonymer Dialoge signiert, so wird dies ausschließlich über die Botensignatur getan.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: III
Kapitel: AUFTRAGSVERFAHREN Abschnitt: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 77

III. AUFTRAGSVERFAHREN

III.1 Allgemeines	78
III.2 Statusprotokoll	79
III.3 Synchronisierung	81
III.4 Adressregistrierung	85
III.4.1 Registrieren einer Adresse	86
III.4.2 Abfragen der registrierten Adressen	86
III.4.3 Löschen einer registrierten Adresse	86
III.5 Bestätigung von Aufträgen und Lebendmeldung	87
III.5.1 Quittierung von Aufträgen	87
III.5.2 Willenserklärung des Kunden	87
III.5.3 Lebendmeldung in Dialogen	88
III.6 Das Publish/Subscribe-Verfahren	90
III.6.1 Einreichen eines Subscription-Auftrags (Subscription)	91
III.6.2 Abfragen der bisher eingereichten Subscription-Aufträge	92
III.6.3 Löschen eines Subscription-Auftrags	93
III.7 Verteilte Signaturen	94
III.7.1 Einreichen eines Auftrages zur verteilten Signatur	94
III.7.2 Details zu eingereichten Aufträgen anfordern	95
III.7.3 Verteilte Signatur leisten	97
III.7.4 Auftrag zur verteilten Signatur löschen	98

Kapitel: III	Version: 4.1 FV	Financial Transaction Services (FinTS)
Seite: 78	Stand: 06.10.2017	Kapitel: AUFTRAGSVERFAHREN Abschnitt: Allgemeines

III.1 Allgemeines

Dieses Kapitel beschreibt administrative Abläufe und besondere Dienste in FinTS 4.1, die durch spezielle Aufträge realisiert werden.

Alle hier genannten Aufträge mit Ausnahme von *Lebendmeldung in Dialogen*, *Einreichen eines Auftrags zur verteilten Signatur* und *Verteilte Signatur leisten* beziehen sich auf einen bestimmten Benutzer, der im Auftrag oder (bei *Synchronisierung*) in der Nachricht explizit genannt wird. Bei direkter Kommunikation eines Kunden mit dem Kreditinstitut muss mindestens eine Signatur dieses Benutzers als Herausgebersignatur (Signatur mit Rolle ISS) vorhanden sein, die sich auf diesen Auftrag bezieht. Folglich können die Aufträge ausschließlich in einem personalisierten Dialog eingereicht werden. Die Herausgebersignatur kann als Boten- oder als Auftragssignatur ausgeführt sein, weitere zusätzliche Signaturen sind möglich. Soll ein Intermediär einen solchen Auftrag im Namen des Benutzers einreichen (siehe *II.3.2 Kommunikation über Intermediär*, Szenario A), signiert er selbst als Herausgeber. In diesem Fall muss der Intermediär – wie auch bei normalen Transaktions- und Abholaufträgen – die Verfügungsberechtigung für diesen administrativen Auftrag besitzen.



Für die in UPD und BPD aufgeführten Geschäftsvorfälle (dies sind alle hier genannten außer *Synchronisierung* und *Lebendmeldung in Dialogen*, vgl. auch *V USER-PARAMETERDATEN (UPD)*, *IV BANKPARAMETERDATEN (BPD)*) kann das Kreditinstitut prinzipiell eine minimale Signaturanzahl von ‚0‘ vorgeben. Die o.g. Forderung zur Herausgebersignatur gilt jedoch in jedem Fall. Ein Kundenprodukt muss also für diese administrativen Aufträge in jedem Fall eine solche Herausgebersignatur erzeugen.



Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: III
Kapitel: AUFTRAGSVERFAHREN Abschnitt: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 79

III.2 Statusprotokoll

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

Um dem Benutzer bzw. dem Kundensystem die Möglichkeit zu geben, den Verarbeitungsstatus von Nachrichten abzufragen, kann kreditinstitutsseitig ein Statusprotokoll geführt werden, in dem die Status aller Aufträge aufgeführt sind. Die kreditinstitutsseitige Unterstützung des Statusprotokolls ist optional. Es ist also zulässig, dass ein Kreditinstitut den Geschäftsvorfall „Statusprotokoll anfordern“ in den BPD nicht anbietet.

Das Statusprotokoll ist beispielsweise sinnvoll, um Benutzern die Ausführung ihrer Aufträge mitzuteilen, da online ggf. lediglich der Empfang der Aufträge bestätigt werden kann und die weitere Verarbeitung offline erfolgt. Ferner dient das Statusprotokoll dazu, nach einem Verbindungsabbruch den Status der übermittelten Aufträge zu erfahren, insbesondere wenn durch das Kundensystem eine Nachricht vollständig an das Kreditinstitut übermittelt wurde, beim Senden der Antwort seitens des Kreditinstituts jedoch ein Fehler auftrat.



Bei asynchroner Kommunikation kann der Zeitunterschied vom Absenden der Nachricht bis zum Eingang beim Kreditinstitut nicht näher spezifiziert werden. Bei der Verwendung des Statusprotokolls in Kombination mit asynchroner Kommunikation ist daher zu berücksichtigen, dass im Protokoll nicht aufgeführte Aufträge das Kreditinstitut eventuell noch gar nicht erreicht haben.

Über das Publish/Subscribe-Verfahren hat der Benutzer auch die Möglichkeit, sich sein Statusprotokoll über einen asynchronen Kommunikationsweg zyklisch zuschicken zu lassen. Er muss dieses somit nicht immer aktiv anfordern, sondern muss nur einmal das zyklische Zusenden mit dem Kreditinstitut vereinbaren (siehe *III.6 Das Publish/Subscribe-Verfahren*).

Grundsätzlich erzeugen sämtliche Geschäftsvorfälle aus Benutzernachrichten einen Eintrag in das Statusprotokoll. Beim anonymen Zugang wird kein Statusprotokoll erzeugt.

Meldungen im Statusprotokoll sind identisch mit den Rückmeldungen zu Aufträgen und zur Gesamtnachricht in Kreditinstitutsnachrichten (vgl. *II.10 Kreditinstitutsnachrichten allgemein*). Zu einem Auftrag können im Statusprotokoll eine oder mehrere Auftragsrückmeldungen enthalten sein. Diese Rückmeldungen sind zeitlich sortiert. Die jeweils letzten Meldungen sind die aktuellsten. Veraltete Meldungen können weggelassen werden. Somit ist zu jedem Zeitpunkt der Verarbeitung eines Auftrages deren Status durch die jeweils letzte(n) Rückmeldung(en) definiert.

Die Festlegung, welcher Teil der Rückmeldungen im Rahmen der Online-Prüfung (z. B. „Auftrag entgegengenommen“) und welcher Teil durch die Offline-Prüfung (z. B. „Auftrag ausgeführt“) generiert wird, ist kreditinstitutspezifisch.

Da Meldungen, die erst bei der Weiterverarbeitung generiert werden, identisch mit den Online-Meldungen sind, kann das Kundenprodukt auch bei asynchroner Verarbeitung wie beim Online-Betrieb auf Meldungen des Kreditinstituts reagieren.

Kapitel: III	Version: 4.1 FV	Financial Transaction Services (FinTS)
Seite: 80	Stand: 06.10.2017	Kapitel: AUFTRAGSVERFAHREN Abschnitt: Statusprotokoll

Statusmeldungen werden stets dem Absender des Auftrags zugeordnet, d. h. Status sind benutzerbezogen und nicht kontenbezogen.

Die Frage, wie detailliert der Benutzer über das Fortschreiten der kreditinstitutsinternen Verarbeitung informiert werden soll, wird kreditinstitutsindividuell gehandhabt.

Wenn das Kreditinstitut Statusprotokolle unterstützt, müssen Statusinformationen im Protokoll als Abgleichhilfe mindestens bis zum Ablauf von 2 Buchungstagen nach dem nächsten Dialog, jedoch höchstens 6 Monate vorgehalten werden. Auf diese Weise ist sichergestellt, dass dem Kunden keine Statusmeldungen verloren gehen (z. B. bei längerem Urlaub etc.). Gleichzeitig wird das kreditinstitutsseitig vorzuhaltende Datenvolumen minimiert, indem die Statusmeldungen bereits 2 Tage nach dem nächsten Dialog gelöscht werden können.



Das Kundenprodukt sollte über ein Journal verfügen, in das sämtliche Statusmeldungen chronologisch eingetragen werden, um auch zu einem späteren Zeitpunkt die Rückverfolgung von Aufträgen zu gewährleisten.

a) Benutzernachricht

Die Anforderung eines Statusprotokolls hat das Format eines Abholauftrages (siehe *II.9.2 Abholauftrag*). Der Benutzer hat die Möglichkeit, den rückzumeldenden Zeitraum einzugrenzen, den Umfang der Einträge zu begrenzen und nach einem vorherigen unvollständigen Datentransport wiederaufzusetzen.

Von Datum, Bis Datum

Werden beide Felder nicht belegt, werden automatisch alle aktuellen Statusmeldungen (d. h. die neuen Statusmeldungen und zusätzlich die Meldungen, die aufgrund der 2-Tage-Regel noch nicht gelöscht wurden) zurückgemeldet.



Das Kundenprodukt muss damit rechnen, dass aufgrund der 2-Tage-Regel derselbe Status u. U. mehrfach vom Kreditinstitut gesendet wird.

Eine vollständige Syntaxbeschreibung befindet sich in [Syntax].

b) Kreditinstitutsrückmeldung

Für jeden Auftrag, für den ein Statusprotokoll verfügbar ist, sind ein oder mehrere Segmente einzustellen, welche die zugehörigen Statusmeldungen enthalten. Zusätzlich können Segmente eingestellt sein, die Rückmeldungen zu Gesamtnachrichten enthalten, also keinen Auftragsbezug besitzen.

Zu jeder Statusmeldung ist eine Referenz auf diejenige Benutzernachricht enthalten, auf die sich die Statusmeldung bezieht.

Eine vollständige Syntaxbeschreibung befindet sich in [Syntax].

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: III
Kapitel: AUFTRAGSVERFAHREN Abschnitt: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 81

III.3 Synchronisierung

Realisierung Kreditinstitut: verpflichtend
Realisierung Kundenprodukt: verpflichtend

Bei der Verarbeitung des FinTS-Protokolls haben die protokollspezifischen Daten und Zähler auf der Seite des Kreditinstituts Vorrang vor denen auf der Kundenseite. Unter einer Synchronisierung ist der Abgleich dieser Daten zu verstehen, d. h. das Anfordern eines Wertes vom Kreditinstitut durch den Benutzer. Eine Synchronisierung ist erforderlich,

- wenn für das vom Benutzer verwendete Endgerät noch keine Kundensystemkennung vergeben wurde. Dies ist nur bei Verwendung von Software-basierten Sicherheitsverfahren erforderlich, da bei Chipkarten-basierten Sicherheitsverfahren kreditinstitutsseitig keine Verwaltung respektive Generierung einer Kundensystemkennung erfolgt. Im Rahmen der Initialisierungs-Antwortnachricht erhält das entsprechende Kundensystem eine neue Kundensystemkennung mitgeteilt. Im PIN/TAN-Verfahren ist die Kundensystemkennung optional.



Bevor ein Benutzer bei Verwendung eines Software-basierten Sicherheitsverfahrens von einem neuen Kundensystem Aufträge erteilen kann, hat er im Wege einer Synchronisierung eine Kundensystemkennung für dieses System anzufordern. Diese ID ist im Folgenden stets anzugeben, wenn der Benutzer von diesem Kundensystem aus Nachrichten sendet. Wenn eine Synchronisierung der Kundensystemkennung durchgeführt wird, ist die in den Properties einer kryptographischen Signatur anzugebende „Kundensystemkennung“ beliebig befüllbar. (siehe auch [Syntax]). Auch ist eine Doppeleinreichungskontrolle bei FinTS-Nachrichten ohne echte Kundensystemkennung nicht notwendig, da diese noch keine bankfachlichen Aufträge enthalten können, für die eine solche Prüfung sinnvoll wäre. Aus diesem Grund kann auch die Signatur-ID in den Signatur-Properties beliebig befüllt werden. Ihr Wert wird für Signaturen ohne Kundensystemkennung nicht überprüft.

Kundensystemkennungen, die länger als 6 Monate nicht beim Kreditinstitut eingereicht wurden, können im Kreditinstitut gelöscht werden. Meldet sich der Benutzer mit dieser Kundensystemkennung erneut an, wird keine Legitimierung zum Senden von Auftragsnachrichten erteilt. Der Benutzer hat in diesem Fall eine erneute Synchronisierung durchzuführen.

Da jedes Kreditinstitut die Kundensystemkennung unabhängig von anderen Kreditinstituten vergibt, muss das Kundenprodukt in der Lage sein, für jeden Kreditinstitutszugang eine eigene Kundensystemkennung zu verwalten.

- wenn aufgrund eines Verbindungsabbruchs auf einem synchronen Kommunikationsweg nicht ersichtlich ist, welche Nachrichten vom Kreditinstitut bereits entgegengenommen wurden. In diesem Fall wird dem Benutzer in der Antwort die

Kapitel: III	Version: 4.1 FV	Financial Transaction Services (FinTS)
Seite: 82	Stand: 06.10.2017	Kapitel: AUFTRAGSVERFAHREN Abschnitt: Synchronisierung

Nummer der im vorangegangenen Dialog vom Kreditinstitut zuletzt verarbeiteten Nachricht zurückgemeldet (siehe auch *II.8 Verbindungsabbruch*). Eine Synchronisierung der Nachrichtennummer ist daher nur für den letzten Auftragsdialog des sendenden Benutzers möglich. Eine abgebrochene Synchronisierungsnachricht überschreibt die letzte Nachrichtennummer nicht.



Im PIN/TAN-Verfahren ist die Verwendung einer Kundensystemkennung optional. Auch ist es im Allgemeinen nicht erforderlich, dass ein Kundensystem für asynchrone und synchrone Kommunikation eines Benutzers unterschiedliche Kundensystemkennungen verwendet.



Wie in *II.5 Unterstützte Kommunikationsverfahren im Überblick* dargestellt, kann sich allerdings in bestimmten Situationen die Bearbeitung von Dialogen desselben Benutzer kreditinstitutsseitig zeitlich überschneiden. Im hier beschriebenen Synchronisierungsmodus ist jedoch das Ergebnis der Anfrage nur dann eindeutig, wenn der *vorangegangene Dialog* eindeutig bestimmt ist. In den genannten Situationen kann diese Eindeutigkeit nur über die Kundensystemkennung bzw. die ID des Sicherheitsmediums erreicht werden. Wenn das Kundensystem diesen Synchronisierungsmodus benötigt und zugleich aufgrund des Einsatzszenarios die Überschneidung von Dialogen zu erwarten ist, sollten für synchrone und asynchrone Kommunikation unterschiedliche Kundensystemkennungen verwendet und auch im PIN/TAN-Verfahren mit einer Kundensystemkennung gearbeitet werden.



Das Kundensystem sollte bei automatisierter Synchronisierung von Nachrichten das Wiedereinreichen verlorengangener Nachrichten nicht automatisieren, da bei längeren Ausfallzeiten betroffene Aufträge evtl. bereits auf anderem Wege beim Kreditinstitut eingereicht wurden.

- wenn aufgrund eines Problems auf einem asynchronen Kommunikationsweg nicht ersichtlich ist, welche Datagramme vom Kreditinstitut bereits entgegengenommen wurden. In diesem Fall wird dem Benutzer in der Antwort mitgeteilt, ob ein Datagramm mit der vom Benutzer angegebenen Benutzerreferenz vom Kreditinstitut verarbeitet worden ist. Eine Synchronisierung auf eine bestimmte Benutzerreferenz muss auch nach der Verarbeitung bereits weiterer Benutzernachrichten noch möglich sein, da der Benutzer im asynchronen Verfahren ja generell mehrere Datagramme gleichzeitig an das Kreditinstitut senden kann und so ggf. erst sehr viel später bemerkt, dass zu einem einzelnen Datagramm keine Antwort des Kreditinstituts erstellt wurde. Hier verhält sich eine Synchronisierung auf eine Benutzerreferenz also anders als eine Synchronisierung der Nachrichtennummer.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: III
Kapitel: AUFTRAGSVERFAHREN Abschnitt: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 83



Analog zum Statusprotokoll muss das Kreditinstitut Auskunft über die möglicherweise länger zurückliegende Verarbeitung eines Datagramms geben können.



Das Kreditinstitut muss die Synchronisierung der Nachrichtennummer sowie der Benutzerreferenz nicht auf das jeweilige bei den beiden Modi genannte Kommunikationsverfahren beschränken. Für das Kundensystem ist allerdings zu beachten, dass alle Nachrichten eines Dialogs dieselbe Benutzerreferenz besitzen und andererseits jedes Datagramm die Nachrichtennummer ,1' besitzt.



- wenn bei Verwendung eines Software-basierten RAH-Verfahrens die Signatur-ID (siehe [HBCI], Abschnitt *II.5.1 Signatur-Segment*) abhanden gekommen ist. Da bei fehlender Signatur-ID die ordnungsgemäße Erzeugung der Signatur nicht möglich ist, kann in diesem Fall als Signatur-ID ein beliebiger Wert verwendet werden. Das Kreditinstitut prüft die Signatur-ID im Falle einer Synchronisierung der Signatur-ID nicht. In der Antwortnachricht wird die bisher höchste vom Benutzer bei diesem Kreditinstitut eingereichte Signatur-ID zurückgemeldet.¹ Bei Chipkarten-basierten Sicherheitsverfahren ist diese Synchronisation nicht zulässig.



Wenn ein Sicherheitsmedium für die Kommunikation mit mehreren Kreditinstituten eingesetzt wird, muss im Fall des Verlusts der Signatur-ID bei jedem Kreditinstitut, bei dem der Benutzer Signaturen eingereicht hat, eine Synchronisierung vorgenommen werden. Für zukünftige Signaturen ist dann der höchste aller zurückgemeldeten Werte inkrementiert um 1 zu verwenden.

Bestehende Aufträge, die noch nicht abgeschickt wurden, sind nach der Synchronisierung der Signatur-ID neu zu signieren, da ansonsten neu erfasste Aufträge aufgrund einer Doppeleinreichung abgelehnt würden.



Bei einer Synchronisierung der Kundensystemkennung oder der Signatur-ID sollte für die Synchronisierungsnachricht keine Doppeleinreichungskontrolle durchgeführt werden.

Die Syntax einer Synchronisierungsnachricht ist so definiert, dass sie nur einen administrativen Teil (mit Initialisierung) aber keine bankfachlichen Aufträge enthalten kann. Auch ist die durch sie begonnene Kommunikation implizit sofort wieder been-

¹ Es ist zu beachten, dass das Kreditinstitut nicht unbedingt die letzte, sondern immer die höchste eingereichte Signatur-ID zurückmeldet. Dies ist notwendig, weil die Aufträge nicht zwingend mit aufsteigender Signatur-ID beim Kreditinstitut eingereicht werden müssen und daher die Verwendung der aktuellen Signatur-ID u. U. zu einer Doppeleinreichung führen könnte.

Kapitel: III	Version: 4.1 FV	Financial Transaction Services (FinTS)
Seite: 84	Stand: 06.10.2017	Kapitel: AUFTRAGSVERFAHREN Abschnitt: Synchronisierung

det. Es dürfen anschließend also keine Aufträge ohne eine neue Initialisierung gesendet werden.

a) Benutzernachricht

Der Benutzer schickt mit seiner Synchronisierungsnachricht den von ihm gewünschten Synchronisierungsmodus an das Kreditinstitut. Hiermit teilt er mit, ob er

- eine neue Kundensystemkennung anfordert,
- eine Synchronisierung der Signatur-ID durchführt,
- eine Synchronisierung der Nachrichtennummer durchführt,
- oder eine Synchronisierung einer Benutzerreferenz durchführt.

◆ **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt
9210	Kundensystemkennung wird vom Kreditinstitut nicht unterstützt
9210	Synchronisierung der Signatur-ID ist nicht zulässig

b) Kreditinstitutsnachricht

Das Kreditinstitut sendet in seiner Antwortnachricht je nach vom Benutzer erhaltenem Synchronisierungsmodus

- eine neue für den Benutzer eindeutige Kundensystemkennung,
- die höchste bisher vom Benutzer über das aktuelle Kundensystem eingereichte Signatur-ID sowie ggf. die höchste eingereichte Signatur-ID des Schlüssels zur Erzeugung digitaler Signaturen,
- die Nummer der letzten vom Benutzer erhaltenen und vollständig verarbeiteten Nachricht, die keine Synchronisierung war,
- oder eine Mitteilung, ob ein Datagramm mit der vom Benutzer angegebenen Benutzerreferenz empfangen und verarbeitet worden ist.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: III
Kapitel: AUFTRAGSVERFAHREN Abschnitt: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 85

III.4 Adressregistrierung

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

Der Benutzer kann mittels der Adressregistrierung dem Kreditinstitut eine Adresse mitteilen, an die dieses Antworten senden soll, wie sie etwa im Publish/Subscribe-Verfahren entstehen. Auch bei asynchroner Kommunikation können diese Adressen verwendet werden. Das Kreditinstitut verifiziert die Korrektheit der vom Benutzer eingestellten Adresse, indem es an diese Adresse einen Verifikationswert sendet. Ein Verifikationswert ist eine vom Kreditinstitut generierte eindeutige Referenz auf den Benutzerauftrag. Der Benutzer übermittelt diesen Verifikationswert in einem Quittungssegment wieder an das Kreditinstitut (vgl. III.5.1 Quittierung von Aufträgen).

Es ist dem Benutzer freigestellt, die Auftragsnachricht über das herkömmliche FinTS-Dialogverfahren oder mittels asynchroner Datagrammtechnik einzureichen. Zum Zeitpunkt der Registrierung einer Kommunikationsadresse muss diese jedoch zwecks Verifizierung bereits gültig und verfügbar sein.

Die Abbildung zeigt den vollständigen Ablauf der Geschäftsvorfälle einer Adressregistrierung und -verifikation. Dazu gehört auch das Senden einer Quittung vom Benutzer an das Kreditinstitut.

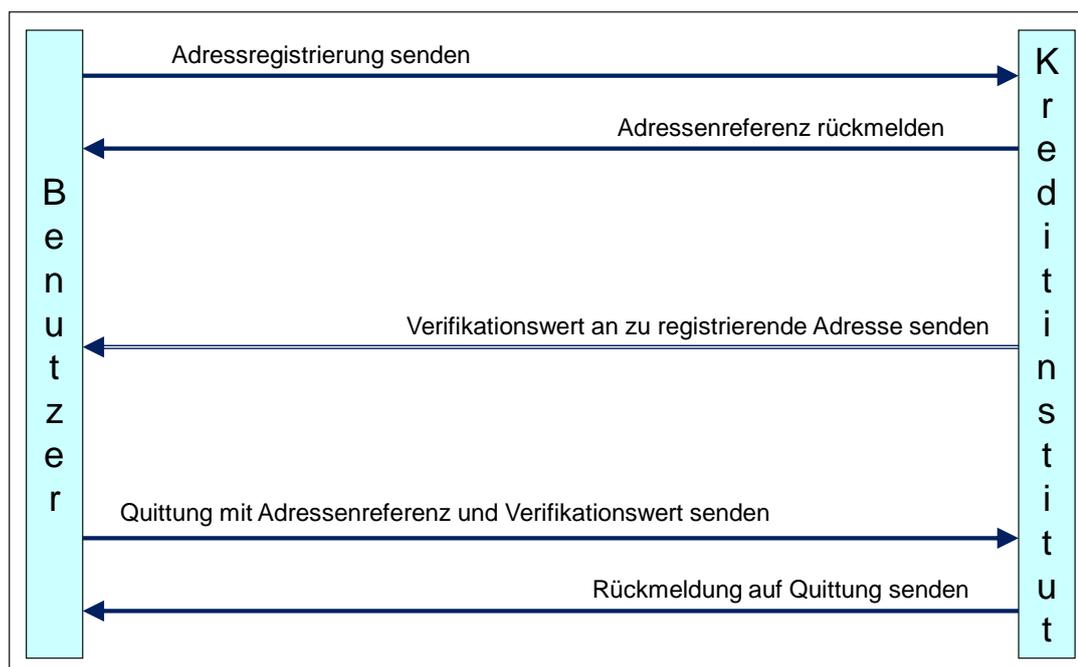


Abbildung 31: Ablauf Adressregistrierung und –verifikation

Für die Adressregistrierung sind folgende Geschäftsvorfälle vorgesehen:

- Registrieren einer Adresse
- Abfragen der registrierten Adressen
- Löschen einer registrierten Adresse

Kapitel: III	Version: 4.1 FV	Financial Transaction Services (FinTS)
Seite: 86	Stand: 06.10.2017	Kapitel: AUFTRAGSVERFAHREN Abschnitt: Adressregistrierung

III.4.1 Registrieren einer Adresse

Mit diesem Auftrag übermittelt der Benutzer eine Adresse an das Kreditinstitut, das diese für asynchrone Antworten wie im Publish/Subscribe-Verfahren verwenden kann. Ebenso ist es möglich, dass der Benutzer eine dem Kreditinstitut schon bekannte Adresse durch eine andere Adresse ersetzt.

Der Auftrag enthält die vom Benutzer gewünschte Adresse. Dies kann z. B. eine gültige E-Mail-Adresse sein. Auch Adressen eines anderen Transportverfahrens, welches zwischen Kunde und Kreditinstitut vereinbart wurde, können eingestellt werden.

Will der Benutzer eine zuvor registrierte Adresse auf die im Auftrag eingestellte ändern, so muss er zusätzlich die Referenz der bereits registrierten Adresse einstellen. Ist keine solche Referenz angegeben, wird automatisch eine Neuregistrierung durchgeführt. Die Änderung einer Adresse wirkt sich auf bereits registrierte Publish/Subscribe-Aufträge aus. Es ist daher keine Löschung und Wiedereinrichtung des Abonnements erforderlich.

Das Kreditinstitut sendet in seiner Antwortnachricht eine Referenz auf die registrierte Adresse an den Benutzer zurück. Gleichzeitig sendet das Kreditinstitut einen Verifikationswert an die neu registrierte Adresse. Der Verifikationswert muss vom Benutzer innerhalb einer Quittung an das Kreditinstitut zurückgesendet werden. Erst dann ist die Registrierung der Adresse abgeschlossen. Der Benutzer kann die Adresse nun z. B. im Publish/Subscribe-Verfahren verwenden.

Eine vollständige Beschreibung der Syntax des Auftrags- und Datensegmentes befindet sich in [Syntax].

III.4.2 Abfragen der registrierten Adressen

Mit diesem Auftrag kann der Benutzer Informationen zu den Adressen abfragen, die er beim Kreditinstitut registriert hat.

Ist die Referenz einer zuvor registrierten Adresse eingestellt, werden nur Informationen zu dieser Adresse zurückgemeldet. Ist keine solche Referenz angegeben, erhält der Benutzer Informationen zu all seinen registrierten Adressen.

Die Informationen zu einer registrierten Adresse umfassen die bei der Registrierung vom Benutzer angegebenen Daten und zusätzlich die vom Kreditinstitut vergebene Referenz der Adresse.

Eine vollständige Beschreibung der Syntax des Auftrags- und Datensegmentes befindet sich in [Syntax].

III.4.3 Löschen einer registrierten Adresse

Mit diesem Auftrag teilt der Benutzer dem Kreditinstitut mit, dass eine für ihn registrierte Adresse gelöscht werden soll. Hierzu stellt er die Referenz der zu löschenden Adresse ein.

Das Kreditinstitut sendet nach der Löschung keine weiteren Datensegmente zurück.

Eine vollständige Beschreibung der Syntax des Auftragssegmentes befindet sich in [Syntax].

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: III
Kapitel: AUFTRAGSVERFAHREN Abschnitt: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 87

III.5 Bestätigung von Aufträgen und Lebendmeldung

III.5.1 Quittierung von Aufträgen

Realisierung Kreditinstitut:	verpflichtend, wenn Geschäftsvorfälle unterstützt werden, die eine Quittierung erfordern
Realisierung Kundenprodukt:	verpflichtend, wenn Geschäftsvorfälle unterstützt werden, die eine Quittierung erfordern

In den BPD kann für einzelne Aufträge eine Quittierung durch den Benutzer gefordert werden. Hierdurch wird dem Kreditinstitut bestätigt, dass der Auftrag auf Kundenseite erfolgreich abgeschlossen wurde. So kann auf diese Weise z. B. der erfolgreiche Empfang von zuvor übermittelten Daten mitgeteilt oder die Korrektheit einer zu registrierenden Antwortadresse bestätigt werden.

Eine Quittung enthält einen Quittungscode, welcher dem Benutzer zuvor vom Kreditinstitut mitgeteilt wurde und der für das Kreditinstitut den zu quittierenden Auftrag eindeutig referenziert. Es bestehen verschiedene Möglichkeiten, wie der Benutzer diesen Verifikationswert erhalten kann:

- Er ist in dem Antwortsegment enthalten, dessen erfolgreicher Empfang quittiert werden soll.
- Er wird auf einem anderen Nachrichtenweg an den Benutzer gesendet, um die Gültigkeit dieses Nachrichtenweges zu überprüfen (Beispiel: Registrieren einer Adresse; der Quittungscode wird als Verifikationswert vom Kreditinstitut an die zu registrierende Adresse gesendet).

Das Kreditinstitut sendet nach dem Erhalt einer Quittung keine weiteren Datensegmente zurück.

In den geschäftsvorfallspezifischen Bankparameterdaten zur Quittierung ist angegeben, welche Geschäftsvorfälle eine Quittierung erfordern.

Eine vollständige Beschreibung der Syntax des Auftragssegmentes befindet sich in [Syntax].

III.5.2 Willenserklärung des Kunden

Realisierung Kreditinstitut:	verpflichtend, wenn Geschäftsvorfälle unterstützt werden, die eine Willenserklärung erfordern
Realisierung Kundenprodukt:	verpflichtend, wenn Geschäftsvorfälle unterstützt werden, die eine Willenserklärung erfordern

Mit diesem Geschäftsvorfall ist es möglich, ein zuvor übertragenes Datenelement „Bestätigungstext“ eines Bezugs-Geschäftsvorfalles durch eine bewusste Interaktion des Kunden als Willenserklärung bestätigen zu lassen. Die rechtliche Wirksamkeit dieser Willenserklärung ist abhängig vom verwendeten Sicherheitsverfahren.

Der GV „Willenserklärung des Kunden (DeclarationIntention)“ kann nicht eigenständig ausgeführt werden, sondern muss auf einen anderen Bezugs-Geschäftsvorfall (z. B. „Elektronischen Kontoauszug beantragen (ApplyAcctStatement)“, vgl. [Messages]) folgen, bei dem in der Kreditinstitutsnachricht das Datenelement „Bestätigungstext“ und ggf. ein entsprechender Bestätigungscode und auch eine Auftragsreferenz übertragen wird. Auf diese Angaben (z. B. in ApplyAcctStatement_Resp) bezieht sich die Willenserklärung des Kunden, die dann mit DeclarationIntention eingereicht wird.

Die Willenserklärung bezieht sich immer auf die unmittelbar vorangegangene Kreditinstitutsantwortnachricht innerhalb eines Dialoges.

Kapitel: III	Version: 4.1 FV	Financial Transaction Services (FinTS)
Seite: 88	Stand: 06.10.2017	Kapitel: AUFTRAGSVERFAHREN Abschnitt: Bestätigung von Aufträgen und Lebendmeldung

Geschäftsvorfälle, für die prinzipiell die Möglichkeit einer Willenserklärung besteht, weisen in den Bankparameterdaten ein entsprechendes Kennzeichen „Willenserklärung erforderlich“ auf. Durch das Setzen dieses Kennzeichens teilt das Kreditinstitut mit, dass eine derartige Willenserklärung erforderlich ist.



Ein Kundenprodukt sollte dem Kunden den „Bestätigungstext“ anzeigen und ihm die Möglichkeit geben, diesen z. B. mit Hilfe einer Checkbox zu bestätigen. Der Kunde sollte darauf hingewiesen werden, dass er durch Absenden dieser Maske dem angezeigten Text ausdrücklich zustimmt.

III.5.3 Lebendmeldung in Dialogen

Realisierung Kreditinstitut: verpflichtend
Realisierung Kundenprodukt: optional

Falls in einem laufenden Dialog über einen längeren Zeitraum keine weiteren Benutzernachrichten mehr geschickt werden, ist es für ein Kreditinstitutssystem nicht ersichtlich, ob der Benutzer noch weitere Nachrichten senden wird oder den Dialog bereits abgebrochen hat.

Insbesondere für Kundenprodukte, die im Online-Modus arbeiten (d. h. der Dialog wird nach dem Senden der Aufträge nicht automatisch beendet), steht daher mit der *KeepAlive*-Nachricht eine Möglichkeit zur Verfügung, dem Kreditinstitutssystem anzuzeigen, dass der Dialog aufrecht erhalten werden soll, so dass eine Dialogbeendigung aufgrund eines Timeouts durch das Kreditinstitutssystem vermieden wird.

Das Kreditinstitut teilt in den Bankparameterdaten einen minimalen und einen maximalen Timeout-Wert mit, der dem Kundensystem eine Information darüber gibt, nach welchem Zeitraum eine Life-Indikator-Nachricht frühestens gesendet werden darf bzw. nach welchem Zeitraum das Kreditinstitut den Dialog voraussichtlich beenden wird.

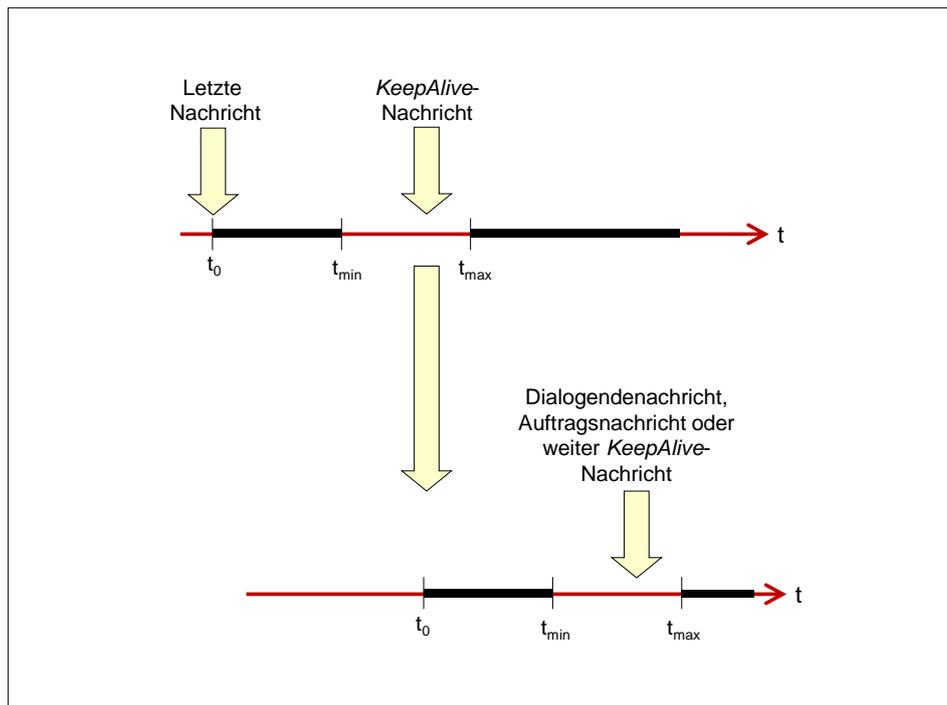


Abbildung 32: Funktionsweise der KeepAlive-Nachricht

Das Senden einer *KeepAlive*-Nachricht führt jedoch nicht zwingend zur Aufrechterhaltung eines Dialogs. Unabhängig von gesendeten *KeepAlive*-Nachrichten und dem Timeout-Wert in den Bankparameterdaten hat das Kreditinstitut jederzeit die Möglichkeit, den Dialog abzubrechen.

Eine *KeepAlive*-Nachricht kann über jeden Kommunikationskanal versendet werden, für den in den BPD Timeout-Werte angegeben sind.

Die *KeepAlive*-Nachricht darf nicht außerhalb der Dialogschrittfolge gesendet werden, d. h. nicht, wenn noch die Beantwortung eines Auftrags durch das Kreditinstitut aussteht. Obwohl die Nachricht bei personalisierten Dialogen innerhalb eines signierten und verschlüsselten Dialoges gesendet wird, ist sie unsigniert, unverschlüsselt und nicht komprimiert.

a) Benutzernachricht

Das Kundenprodukt sendet die *KeepAlive*-Nachricht ohne Parameter. Das Senden einer *KeepAlive*-Nachricht hat keine Auswirkungen auf die aktuelle Nachrichtennummer. Der Inhalt des Feldes „Nachrichtennummer“ ist mit „0“ zu belegen. Auch wird die Nummer einer *KeepAlive*-Nachricht nie bei einer Synchronisierung der Nachrichtennummer zurückgeliefert. Benutzerreferenz und Kreditinstitutsreferenz sind in der Nachricht allerdings korrekt anzugeben.

b) Kreditinstitutsnachricht

Das Kreditinstitut antwortet auf die *KeepAlive*-Nachricht mit einer speziellen Antwortnachricht ohne Auftrags- und Nachrichtenrückmeldungen. Wie auch die Benutzernachricht ist die Antwortnachricht nicht signiert und nicht verschlüsselt. Falls der Dialog bereits geschlossen ist, antwortet das Kreditinstitut mit einer nicht signierten, unverschlüsselten Standardantwort mit entsprechendem Rückmeldungscode.

Eine vollständige Beschreibung der Syntax des Auftragssegmentes befindet sich in [Syntax].

Kapitel: III	Version: 4.1 FV	Financial Transaction Services (FinTS)
Seite: 90	Stand: 06.10.2017	Kapitel: AUFTRAGSVERFAHREN Abschnitt: Das Publish/Subscribe-Verfahren

III.6 Das Publish/Subscribe-Verfahren

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

Das Publish/Subscribe-Verfahren erlaubt es dem Benutzer, Aufträge einzureichen, die das Kreditinstitut wiederholt in einem festgelegten Zyklus oder auch ereignisgesteuert und dann ggf. nur einmalig ausführen soll (Subscription-Auftrag). Die dabei erzeugten Antwortnachrichten des Kreditinstituts werden dem Benutzer dann mittels asynchroner Kommunikationswege zugestellt (siehe *II.7 FinTS Datagramme*). Im Gegensatz zum Einreichen von sofort auszuführenden Aufträgen kann der Benutzer zu einem Subscription-Auftrag eine beliebige Antwortadresse angeben, an welche die Antwortnachrichten gesendet werden sollen. Diese Antwortadresse muss der Benutzer zuvor beim Kreditinstitut registriert haben (siehe *III.4 Adressregistrierung*). Die zyklischen/ereignisgesteuerten Ausführungsnachrichten des Kreditinstituts werden stets asynchron an die eingestellte Kommunikationsadresse übermittelt.

Die Autorisierung der abonnierten Aufträge erfolgt implizit über die Autorisierung des Subscription-Auftrags. Es ist somit keine gesonderte Autorisierung für jede Auftragsausführung erforderlich.



Es dürfen nur solche Aufträge eingestellt werden, die zur zyklischen bzw. ereignisgesteuerten Ausführung geeignet sind, die innerhalb ihrer Felder also keine zeitlichen oder sonstigen Abhängigkeiten aufweisen und damit bei gleichbleibenden Feldinhalten mehrfach ausgeführt werden können. Die entsprechenden Geschäftsvorfälle werden innerhalb der BPD des Kreditinstituts in den geschäftsvorfallspezifischen Parametern des Subscription-Auftrags entsprechend ausgewiesen.



Es ist zu beachten, dass das Kreditinstitut nach erfolglosem Senden an die Adresse eines Benutzers die weitere Ausführung der Aufträge nicht abbricht. Der Benutzer muss daher ggf. seinen Subscription-Auftrag erneuern, indem er ihn zunächst löscht und dann neu einrichtet.



Dem Kreditinstitut ist es freigestellt, einen Mechanismus einzurichten, der es einem Kundenbetreuer ermöglicht, den betroffenen Benutzer zu kontaktieren, falls Antworten auf Subscription-Aufträge erfolglos gesendet wurden.

Für Publish/Subscribe sind folgende Geschäftsvorfälle vorgesehen:

- Einreichen eines Subscription-Auftrags (Subscription)
- Abfragen der bisher eingereichten Subscription-Aufträge

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: III
Kapitel: AUFTRAGSVERFAHREN Abschnitt: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 91

- Löschen eines Subscription-Auftrags

Für das Publish/Subscribe-Verfahren kann der Benutzer jede seiner bereits registrierten Adressen verwenden. Hat der Benutzer bis dato keine Adresse registriert, führt er zunächst eine Adressenregistrierung aus.

Innerhalb der Antwort auf einen neu eingereichten Subscription-Auftrag erhält der Benutzer eine Subscription-ID, mit der er dann zukünftig den Status dieses Auftrags anfordern oder den Auftrag auch wieder löschen kann.

Die Kreditinstitutsnachrichten zu den zyklisch ausgeführten Benutzeraufträgen sendet das Kreditinstitut an die gewünschte registrierte Antwortadresse. Der Benutzer kann die Kreditinstitutsnachrichten zu beliebigen Zeitpunkten entgegennehmen bzw. abholen.

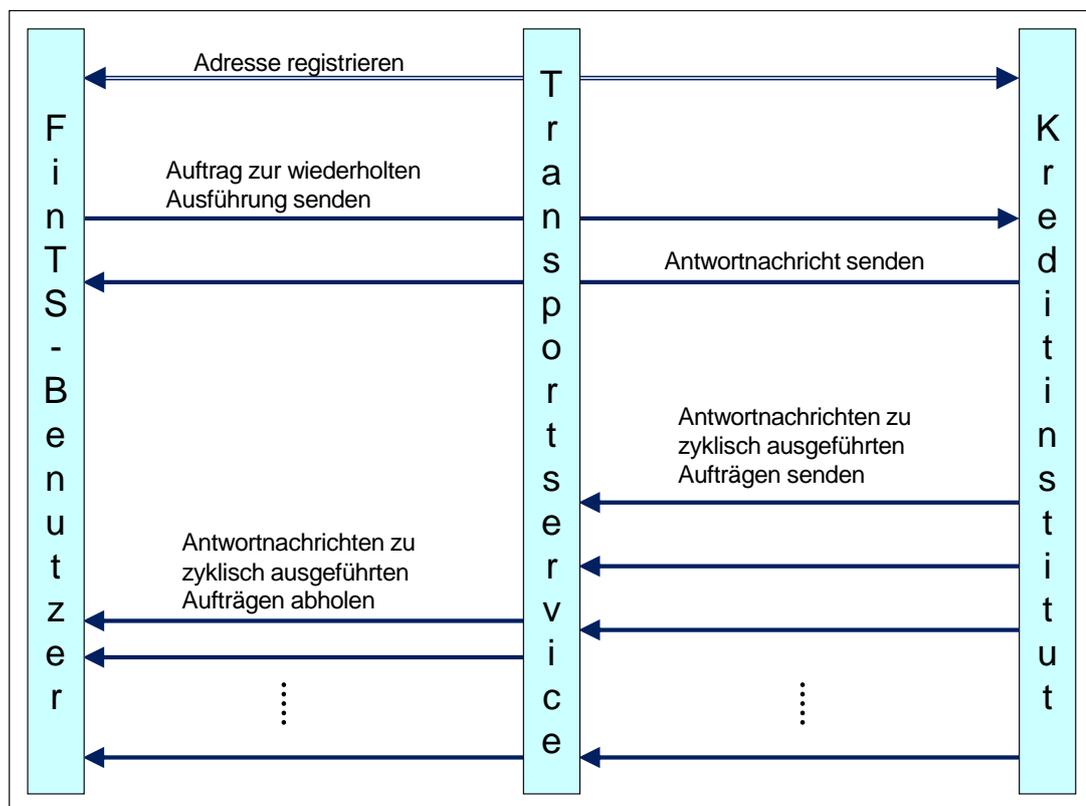


Abbildung 33: Publish/Subscribe-Verfahren

III.6.1 Einreichen eines Subscription-Auftrags (Subscription)

Mit einer Subscription übermittelt der Benutzer einen Auftrag an das Kreditinstitut, der durch das Kreditinstitut wiederholt in bestimmten Abständen oder bei Eintreten eines Ereignisses ausgeführt werden soll. Sie enthält ein Zeitfenster, in dem der eingestellte Auftrag ausgeführt werden soll. Dieses wird durch Anfangs- und Enddatum und -uhrzeit festgelegt.

Eine Subscription enthält einen Ausführungsturnus bei zyklisch auszuführenden Aufträgen und ein Ausführungsereignis bei ereignisgesteuerten Aufträgen.

Der Ausführungsturnus gibt eine Periode in Monaten, Wochen, Tagen oder Stunden an, in der sich der Auftrag wiederholen soll. Je nach Periodentyp wird darüber hin-

Kapitel: III	Version: 4.1 FV	Financial Transaction Services (FinTS)
Seite: 92	Stand: 06.10.2017	Kapitel: AUFTRAGSVERFAHREN Abschnitt: Das Publish/Subscribe-Verfahren

aus der Kalender-, Wochentag bzw. die Stunde oder Minute festgelegt, zu der die Ausführung stattfinden soll.



Es ist vom Benutzer zu beachten, dass die Ausführungstage, -stunden und -minuten nur einen frühestmöglichen, nicht aber einen exakten Ausführungszeitpunkt festlegen.

Ein Ausführungsereignis ist eine Bedingung, bei deren Eintreten der Auftrag ausgeführt werden soll. Ereignistypen können vom Kreditinstitut oder einer Organisation definiert und mit beliebigen Parametern ausgestattet werden (Beispiel: Kontostand eines bestimmten Kontos des Benutzers erreicht ein festgelegtes Limit).

Die Subscription enthält die Referenz auf eine asynchrone Rückantwortadresse, an die die Antwortnachrichten zu senden sind. Diese Referenz muss zuvor vom Kreditinstitut im Rahmen einer Adressregistrierung vergeben worden sein (siehe *III.4 Adressregistrierung*).

Die Subscription kann einen textuellen Kommentar des Benutzers enthalten, welcher dann vom Kreditinstitut in den zugehörigen Antwortnachrichten eingestellt wird. Hierdurch wird es dem Benutzer erleichtert, die Antworten den zugehörigen Subscription-Aufträgen zuzuordnen.

Abschließend enthält die Subscription den auszuführenden Subscription-Auftrag selbst. Dieser ist in exakt der Form eingestellt, in der er später (ggf. wiederholt) ausgeführt werden soll. Alle betreffenden Felder sind vom Benutzer so mit Werten zu belegen, dass eine spätere oder ggf. mehrfache Ausführung sinnvoll ist.

Das Kreditinstitut sendet in seiner Antwort auf eine Subscription eine Referenz in Form einer Subscription-ID an den Benutzer zurück. Diese Referenz wird in allen weiteren Aufträgen des Benutzers verwendet, in denen er sich auf den soeben eingereichten Subscription-Auftrag beziehen muss.

In den BPD wird festgelegt, welche Aufträge durch eine Subscription abonniert werden können und welche Turnus- und Ereignistypen unterstützt werden..



Die Signatur eines Subscription-Auftrags signiert sowohl die Subscription als auch implizit die spätere Ausführung des Auftrags. Da diese Definition je nach Sicherheitsverfahren unterschiedliche technische Realisierungen erfordert (im PIN/TAN-Verfahren beispielsweise muss bedacht werden, dass eine TAN nicht mehrmals verwendet werden kann), kann das Kreditinstitut die Abonnierbarkeit von Aufträgen in den BPD je Sicherheitsverfahren unterschiedlich festlegen.

Eine vollständige Beschreibung der Syntax der Auftrags-, Daten- und Parametersegmente befindet sich in [Syntax].

III.6.2 Abfragen der bisher eingereichten Subscription-Aufträge

Mit diesem Auftrag kann der Benutzer Informationen zu seinen bereits eingereichten Subscription-Aufträgen abfragen.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: III
Kapitel: AUFTRAGSVERFAHREN Abschnitt: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 93

Er kann die Subscription-ID eines zuvor eingereichten Auftrages einstellen, um nur die Information zu diesem Auftrag abzufragen. Wird keine solche ID eingestellt, werden die Daten zu allen eingereichten Subscription-Aufträgen zurückgeliefert.

Die vom Kreditinstitut zurückgemeldeten Informationen zu einem Subscription-Auftrag umfassen die seinerzeit vom Benutzer eingereichte Subscription in unveränderter Form, zusätzlich die Subscription-ID und bei zyklischen Subscription-Aufträgen den nächsten Ausführungszeitpunkt in Form eines Datums und einer Uhrzeit.

Eine vollständige Beschreibung der Syntax der Auftrags- und Datensegmente befindet sich in [Syntax].

III.6.3 Löschen eines Subscription-Auftrags

Mit diesem Auftrag teilt der Benutzer dem Kreditinstitut mit, dass ein Subscription-Auftrag gelöscht werden soll. Der Benutzer stellt hierzu die Subscription-ID des betreffenden Subscription-Auftrages ein.

Das Kreditinstitut meldet neben einer entsprechenden FinTS-Rückmeldung keine weiteren Daten zurück.

Eine vollständige Beschreibung der Syntax des Auftragssegmentes befindet sich in [Syntax].

Kapitel: III	Version: 4.1 FV	Financial Transaction Services (FinTS)
Seite: 94	Stand: 06.10.2017	Kapitel: AUFTRAGSVERFAHREN Abschnitt: Verteilte Signaturen

III.7 Verteilte Signaturen

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional

Für den Kunden besteht die Möglichkeit, einen Auftrag nicht sofort bei dessen Einreichung durch alle notwendigen Benutzer signieren zu lassen, sondern diese Signaturen ggf. erst später in weiteren Nachrichten nachzuliefern. Hierbei wird dann von einer verteilten Signatur gesprochen, da die signierenden Benutzer nicht zur selben Zeit am selben Ort ihre Signaturen leisten, sondern dies sowohl zeitlich als auch räumlich voneinander getrennt geschehen kann.

Für die Abwicklung verteilter Signaturen werden vier administrative Geschäftsvorfälle (im Folgenden VS-GV) eingeführt. Mit ihrer Hilfe kann jeder beliebige andere Geschäftsvorfall über eine verteilte Signatur abgesichert werden.

Einen Spezialfall der verteilten Signatur stellt das Zwei-Schritt-TAN-Verfahren dar (vgl. [PIN/TAN, Abschnitt II.2]). Dort werden verpflichtend die Geschäftsvorfälle *Einreichen eines Auftrages zur verteilten Signatur* und *Verteilte Signatur leisten* für die Autorisierung mittels TAN verwendet. Optional können auch die VS-GV *Details zu eingereichten Aufträgen anfordern* und *Auftrag zur verteilten Signatur löschen* (bei FinTS V3.0 *Stornieren*) auftreten.

III.7.1 Einreichen eines Auftrages zur verteilten Signatur

Soll ein Geschäftsvorfall GV verteilt signiert werden, so ist dieser wie gewohnt aufzubauen, dann jedoch in den dafür vorgesehen VS-GV *Einreichen eines Geschäftsvorfalles zur verteilten Signatur* einzustellen. Dieser VS-GV enthält neben dem Auftrag GV selbst noch folgende weitere Steuerinformationen:

- eine Liste der signierpflichtigen Benutzer. Wenn die Liste angegeben ist, regelt eine bilaterale Vereinbarung zwischen Kreditinstitut und Benutzer, wie sie zu interpretieren ist. Wenn sie nicht enthalten ist, entscheidet das Kreditinstitut allein, welche Benutzer den Auftrag autorisieren können. Das Kreditinstitut gibt über die Bankparameterdaten vor, ob die Angabe der Liste für den Einreicher erlaubt ist.
- eine textuelle Referenz zum Auftrag GV, welche diesen für die signierpflichtigen Benutzer identifizierbar macht
- eine asynchrone Rückantwortadresse, an die die Antwortdaten nach der Ausführung von GV zu senden sind, analog zu der in *II.1.1 Nachrichtenelemente* beschriebenen.

Der VS-GV wird von dessen einreichendem Benutzer wie gewohnt signiert (wie auch bei anderen Nachrichten erfolgt diese Herausgebersignatur hierbei in Szenarien ohne Intermediär im Allgemeinen als Botensignatur auf Nachrichtenebene, bei Einreichung über einen Intermediär als Signatur des Auftragsteils - vgl. *II.4 Signatur-Rollenverteilung bei Kommunikation mit und ohne Intermediär*). Hierdurch wird auch bereits GV signiert, so dass die Signatur des Einreichers ggf. bei den notwendigen Signaturen für GV berücksichtigt werden kann. Auf Seite des Kreditinstituts findet eine erste Prüfung von GV statt. Danach wird dem Auftrag eine eindeutige ID zugeordnet, die dem Einreicher in der Antwortnachricht mitgeteilt wird. In Abbildung 34: Auftrag zur verteilten Signatur einreichen ist ein Beispiel dargestellt, bei dem GV ein 3-fach zu signierender Auftrag ist und die Signatur des Einreichers bereits als erste zu leistende Signatur gewertet wird.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: III
Kapitel: AUFTRAGSVERFAHREN Abschnitt: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 95

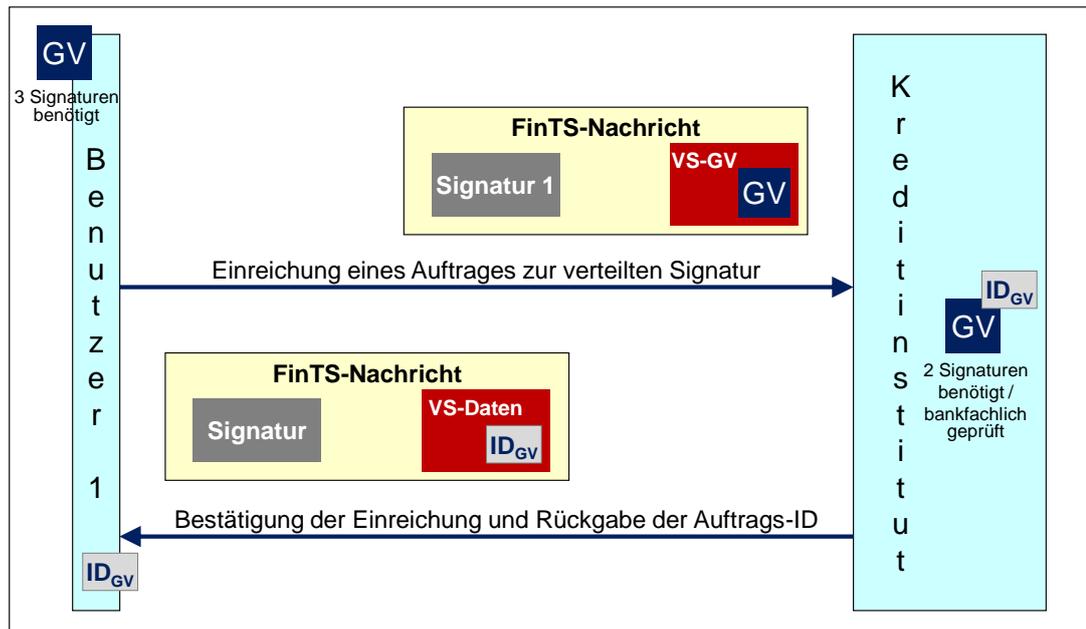


Abbildung 34: Auftrag zur verteilten Signatur einreichen

III.7.2 Details zu eingereichten Aufträgen anfordern

Für die weiteren signierpflichtigen Benutzer muss die Möglichkeit bestehen, sich zum einen darüber zu informieren, ob Aufträge vorliegen, die sie zu signieren haben, und zum anderen einzelne Aufträge oder signifikante Teile davon anzufordern, um diese zu signieren.

Hierzu wird der *VS-GV Details anfordern* verwendet. Er enthält ein Kennzeichen, welche Informationen des zu signierenden Auftrags angefordert werden:

- die textuellen Referenzen aller Aufträge, die vom anfordernden Benutzer zu signieren sind
- die Daten des zu signierenden Geschäftsvorfalles selbst für einen über die ID referenzierten Auftrag. Zusätzlich werden zurück gemeldet: die textuelle Referenz, welche Benutzer diesen Auftrag zu welchem Zeitpunkt signiert haben, welche Benutzer noch signieren müssen sowie die Antwortadresse für die asynchrone Ausführung des vollständig signierten Geschäftsvorfalles
- eine verkürzte Darstellung der Daten des zu signierenden Geschäftsvorfalles (inklusive der zusätzlichen Daten wie im vorigen Punkt) für einen über die ID referenzierten Auftrag. Im Falle von sehr großen Geschäftsvorfällen ist es sinnvoll, nicht den kompletten Datenstrom zu übertragen. Das Kreditinstitut kann daher für Sammelaufträge eine verkürzte Version festlegen, beispielsweise die *DEG Summenfeld* bei einer SEPA-Sammelüberweisung. Es ist dem Kreditinstitut im Falle von Sammelaufträgen freigestellt, ob es überhaupt eine verkürzte Darstellung definiert oder auch bei Anforderung der Kurzform stets die gesamten Daten überträgt. Andererseits kann es bei Sammelaufträgen auch entscheiden, stets nur die verkürzte Version zu liefern - selbst wenn im Auftrag explizit die Langversion angefordert wird. Bei allen anderen Geschäftsvorfällen darf keine Kurzversion definiert werden, hier wird auch bei deren expliziter Anforderung die Langversion geliefert.

In Abbildung 35: Liste der verteilt zu signierenden Aufträge anfordern ist ein Beispiel dargestellt, in dem der Benutzer keine ID in den VS-GV einstellt. Er erhält somit eine

Kapitel: III	Version: 4.1 FV	Financial Transaction Services (FinTS)
Seite: 96	Stand: 06.10.2017	Kapitel: AUFTRAGSVERFAHREN Abschnitt: Verteilte Signaturen

Liste von textuellen Referenzen zu den aktuell eingereichten und von ihm zu signierenden Aufträgen inklusive deren IDs.

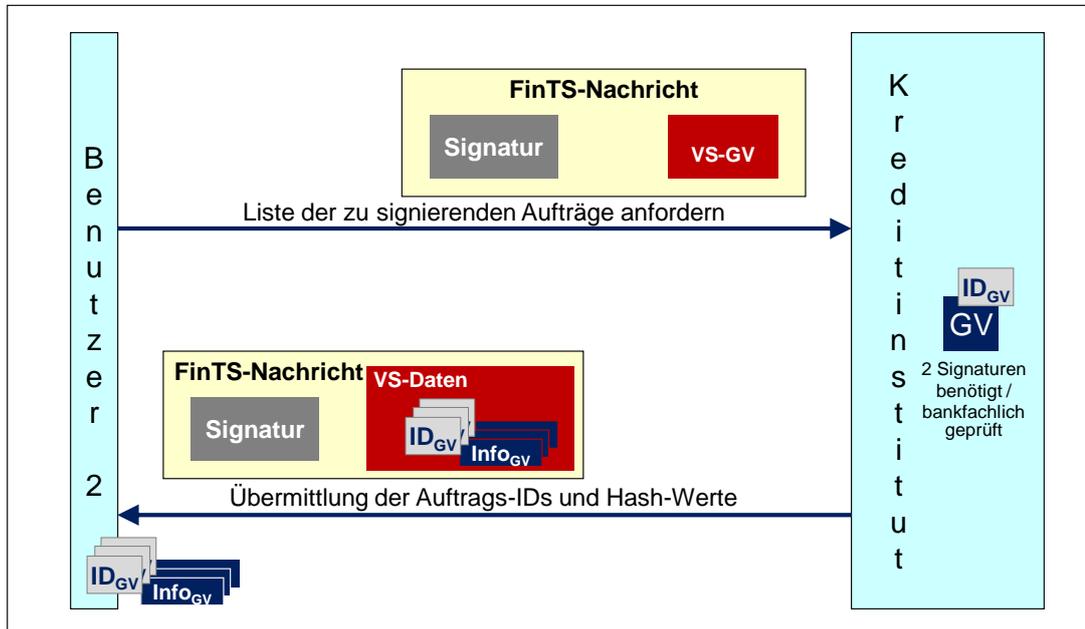


Abbildung 35: Liste der verteilt zu signierenden Aufträge anfordern

Der Sinn im Anfordern eines zuvor eingereichten Geschäftsvorfalles liegt darin, dass der Benutzer für seine verteilte Signatur Daten benötigt, die er signieren kann. Hierzu ist der Geschäftsvorfall selbst am besten geeignet, da auf diese Weise dem Benutzer der Inhalt des zu signierenden Auftrags am einfachsten transparent gemacht werden kann.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: III
Kapitel: AUFTRAGSVERFAHREN Abschnitt: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 97

In Abbildung 36: Verteilt zu signierenden Auftrag anfordern ist ein Beispiel dargestellt, in dem der Benutzer eine zuvor angeforderte Auftrags-ID dazu verwendet, den zugehörigen Geschäftsvorfall komplett anzufordern. Der so angeforderte Geschäftsvorfall kann nun von ihm eingesehen und überprüft werden.

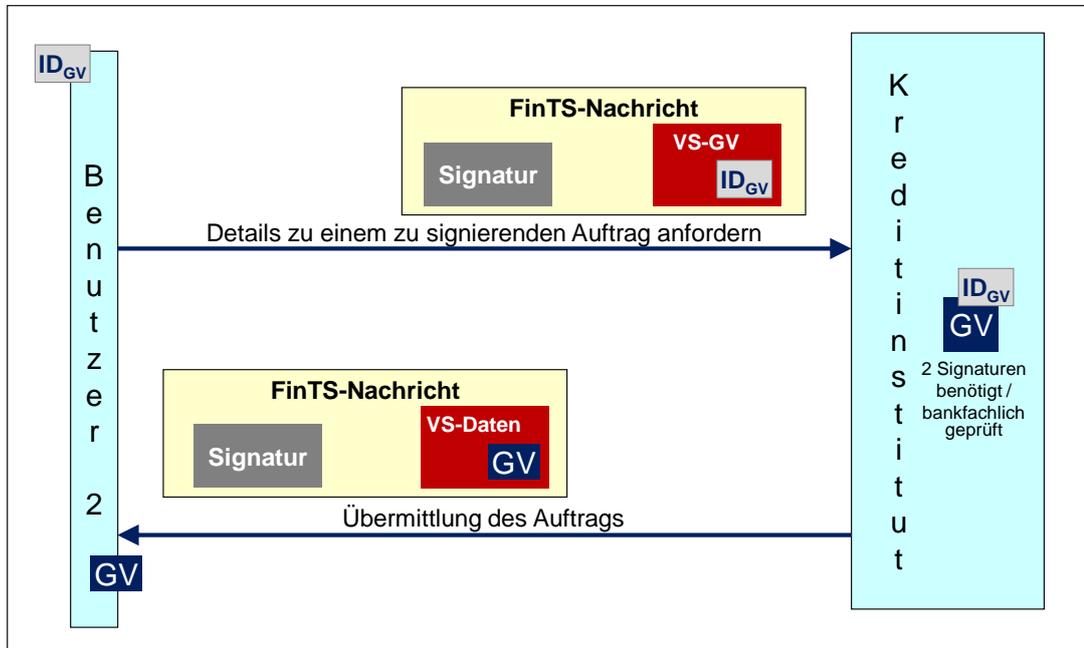


Abbildung 36: Verteilt zu signierenden Auftrag anfordern

III.7.3 Verteilte Signatur leisten

Hat ein signierpflichtiger Benutzer einen von ihm zu signierenden Auftrag komplett oder teilweise angefordert und diesen entsprechend geprüft, kann er ihn signieren. Hierzu stellt er den zuvor angeforderten Datenstrom zusammen mit der zugehörigen Auftrags-ID (*Auftragsreferenz, DistSigsID*) in den dafür vorgesehen VS-GV *verteilte Signatur leisten*. Dieser VS-GV wird von ihm signiert, wodurch auch der zu signierende Auftrag mitsigniert wird. Das Kreditinstitut prüft nach Erhalt des VS-GV, ob die darin enthaltene ID und der Auftragsdatenstrom zusammen passen, ob die Signatur korrekt ist und ob der signierende Benutzer einer der signierpflichtigen Benutzer ist. Falls dies der Fall ist, wird die erfolgreiche Signatur entsprechend vermerkt. Ist der Auftrag nun ausreichend signiert, wird dieser verarbeitet, andernfalls wird weiter auf die noch fehlenden Signaturen gewartet.

Kapitel: III	Version: 4.1 FV	Financial Transaction Services (FinTS)
Seite: 98	Stand: 06.10.2017	Kapitel: AUFTRAGSVERFAHREN Abschnitt: Verteilte Signaturen

In Abbildung 37: Verteilte Signatur leisten ist ein Beispiel dargestellt, in dem zwei Benutzer die noch fehlenden Signaturen leisten. Beide haben zuvor den Geschäftsvorfall angefordert, Benutzer 2 komplett und Benutzer 3 in verkürzter Form. Sie senden die zuvor erhaltenen Datenströme nun innerhalb des dafür vorgesehenen VS-GV mit ihrer eigenen Signatur versehen zurück. Das Kreditinstitut verringert mit jeder eintreffenden Signatur den Zähler der noch fehlenden Signaturen. Sind ausreichend Signaturen eingegangen, wird der Auftrag verarbeitet.

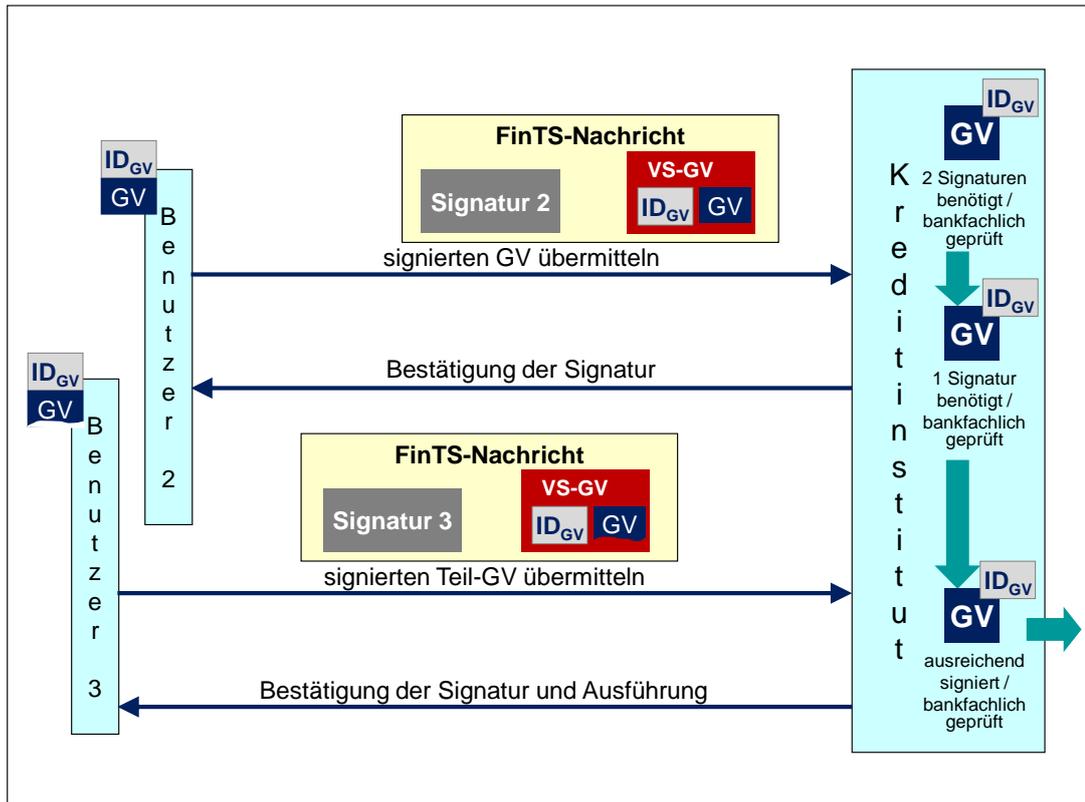


Abbildung 37: Verteilte Signatur leisten

III.7.4 Auftrag zur verteilten Signatur löschen

Ist ein Auftrag fälschlich oder fehlerhaft zur verteilten Signatur eingereicht worden, so kann dieser jederzeit von jedem signierpflichtigen Benutzer gelöscht werden, solange noch auf fehlende Signaturen gewartet wird. Hierzu ist der VS-GV *Auftrag zur verteilten Signatur löschen* vorgesehen. Der Auftrag enthält die Auftrags-ID (*Auftragsreferenz, DistSigsID*) des zu löschenden Auftrags.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: III
Kapitel: AUFTRAGSVERFAHREN Abschnitt: Inhaltsverzeichnis	Stand: 06.10.2017	Seite: 99

In Abbildung 38: Auftrag zur verteilten Signatur löschen ist die Löschung eines eingereichten Auftrages beispielhaft dargestellt.

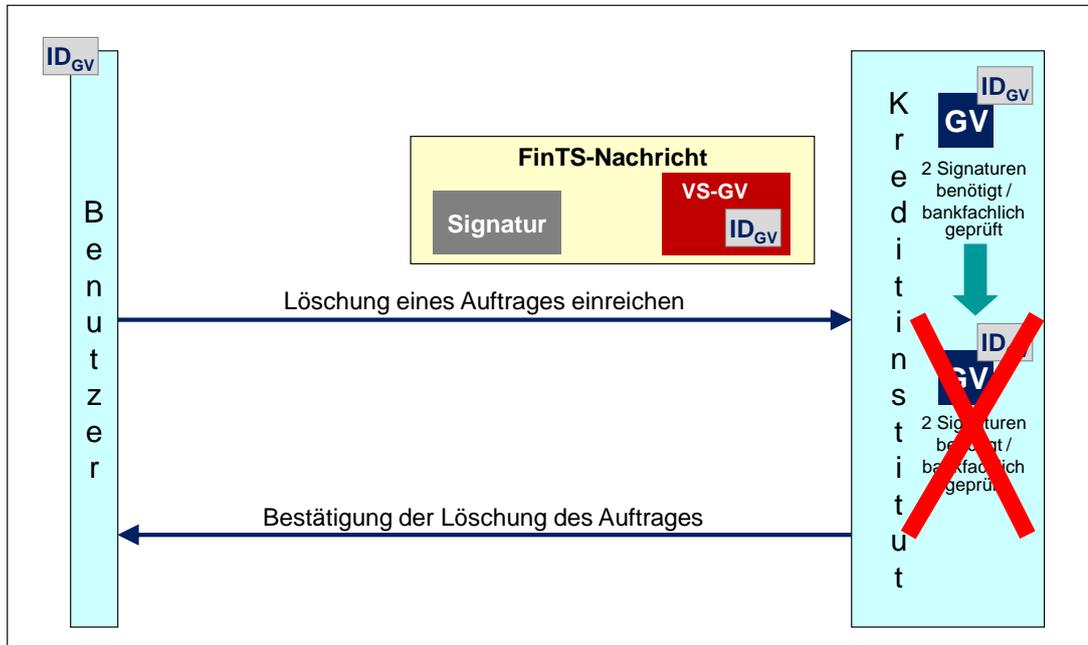


Abbildung 38: Auftrag zur verteilten Signatur löschen

Kapitel: IV	Version: 4.1 FV	Financial Transaction Services (FinTS) Formals - Grundsätzliche Festlegungen
Seite: 100	Stand:	Kapitel: BANKPARAMETERDATEN (BPD) Abschnitt: Verteilte Signaturen

IV. BANKPARAMETERDATEN (BPD)

IV.1 Allgemeines	101
IV.2 Aufbau	104
IV.2.1 Bankparameter allgemein.....	104
IV.2.2 Kommunikationszugang	105
IV.2.3 Sicherheitsverfahren	106
IV.2.4 Komprimierungsverfahren	106
IV.2.5 Geschäftsvorfallparameter	106
IV.3 Anforderung der BPD in einem Szenario mit Intermediär	108

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: IV
Kapitel: BANKPARAMETERDATEN (BPD) Abschnitt: Allgemeines	Stand: 06.10.2017	Seite: 101

IV.1 Allgemeines

Realisierung Kreditinstitut: verpflichtend
Realisierung Kundenprodukt: verpflichtend

Die Bankparameterdaten dienen zum einen zur automatisierten kreditinstitutsspezifischen Konfiguration von Kundensystemen und zum anderen zur dynamischen Anpassung an kreditinstitutsseitige Vorgaben hinsichtlich der Auftragsgenerierung.

Weiterhin ist es mit Hilfe der BPD möglich, bestimmte Fehler bereits auf der Kundenseite zu erkennen, was sich wiederum positiv auf die kreditinstitutsseitige Verarbeitung der Auftragsdaten auswirkt.

Beispiel:

Zur Einreichung einer Überweisung bei einem Kreditinstitut, das nur zwei Verwendungszweckzeilen zulässt, hat der Benutzer im entsprechenden Bildschirmformular auch nur zwei Eingabezeilen zur Verfügung. Bei der Einreichung einer Überweisung bei einem Kreditinstitut, das vier Verwendungszweckzeilen unterstützt, erscheinen vier Zeilen im Bildschirmformular.

Bei korrekter Nutzung durch das Kundensystem verhindert dieser Mechanismus somit, dass Informationen an die Kreditinstitute gesendet werden, die diese nicht darstellen bzw. verarbeiten können und somit ablehnen würden.



Da auf Schnittstellenebene nicht gewährleistet werden kann, dass das Kundenprodukt die Bankparameterdaten korrekt auswertet, hat auf jeden Fall eine entsprechende kreditinstitutsseitige Prüfung stattzufinden.

Bei kreditinstitutsseitigen Änderungen werden die aktualisierten Bankparameterdaten dem als Boten der Nachricht auftretenden Benutzer bei der nächsten Kommunikation automatisch im Rahmen der Initialisierung übermittelt. Die neuen BPD werden sofort, d. h. schon für die laufende Kommunikation, aktiv. In Szenarien mit Intermediär wird ein Auftrag zum expliziten Abruf der BPD benötigt, siehe *IV.3 Anforderung der BPD in einem Szenario mit Intermediär*.

Kapitel: IV	Version: 4.1 FV	Financial Transaction Services (FinTS) Formals - Grundsätzliche Festlegungen
Seite: 102	Stand:	Kapitel: BANKPARAMETERDATEN (BPD) Abschnitt: Allgemeines



Intelligente Kundenprodukte können in diesem Fall in der laufenden Kommunikation die Einhaltung der Vorgaben in den BPD prüfen und die Auftragsnachrichten wie geplant senden, falls die BPD-Änderungen keine Auswirkung auf die zur Versendung anstehenden Aufträge haben. Steht diese Intelligenz nicht zur Verfügung, muss nach Erhalt der neuen BPD die laufende Kommunikation vom Benutzer (Kundenprodukt) beendet, die Aufträge geprüft bzw. neu erfasst und dann eine neue Kommunikation begonnen werden.

Es ist zu beachten, dass es beim Einstellen von Aufträgen in die erste Nachricht einer Kommunikation (dies ist generell bei Datagrammen der Fall) zu Fehlermeldungen kommen kann, wenn diese Aufträge gegen die Restriktionen neuer schärferer BPD verstoßen, die mittlerweile aktiv sind. Das Kundenprodukt muss somit selbst dann eine mögliche Neubearbeitung eines Auftrages vorsehen, wenn es sich bei dessen Erzeugung an die zuletzt gültigen BPD gehalten hat.

In Abgrenzung zu den UPD (User-Parameterdaten) enthalten die BPD ausschließlich Daten, die für das jeweilige Kreditinstitut spezifisch sind, und damit eher seltener geändert werden müssen.



Die BPD gibt jeweils die Gesamtheit aller gültigen Geschäftsvorfälle wieder. Dies kann auch solche Geschäftsvorfälle einschließen, die der Benutzer selbst nicht sinnvoll einsetzen kann. So können hier z. B. Geschäftsvorfälle aufgeführt sein, die allein von Portalen oder bei Kommunikation über einen Intermediär eingereicht werden dürfen. Welche Geschäftsvorfälle tatsächlich erlaubt sind, wird in den UPD sowohl für Benutzer wie auch für Intermediäre jeweils näher erläutert (siehe auch *V USER-PARAMETERDATEN (UPD)*).



Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: IV
Kapitel: BANKPARAMETERDATEN (BPD) Abschnitt: Allgemeines	Stand: 06.10.2017	Seite: 103



Werden Bankparameterdaten in einer Form übergeben, die eine Dateibenennung erfordert (z. B. auf Diskette), ist als Name für Bankparameterdaten "*.bpd" zu wählen, wobei "*" durch die jeweilige Kreditinstitutskennung (in Deutschland die Bankleitzahl) zu ersetzen ist.¹

Über die Angebote fremder Kreditinstitute kann sich der Benutzer mit Hilfe derer BPD informieren. Es wird empfohlen, Kundenprodukte standardmäßig mit einer Auswahl von Bankparameterdaten gängiger Kreditinstitute auszustatten. Falls diese nicht auf dem Kundensystem verfügbar sind, muss ein Dialog mit dem Fremdinstitut geführt werden, während dessen die aktuellen BPD automatisch übertragen werden. Zur erstmaligen Verbindungsaufnahme mit dem Fremdinstitut sind dessen Zugangsdaten erforderlich. Diese erhält das Kundenprodukt entweder durch den Abruf der Kommunikationszugangsdaten (s. [Messages]) oder auf anderem Wege (z. B. direkt von diesem Kreditinstitut). Im letzteren Fall müssen die Zugangsdaten manuell eingegeben werden.

¹ Systeme, die Groß- und Kleinschreibung unterscheiden, sollten den Dateinamen wie abgebildet (d. h. in Kleinschreibung) verwenden.

Kapitel: IV	Version: 4.1 FV	Financial Transaction Services (FinTS) Formals - Grundsätzliche Festlegungen
Seite: 104	Stand:	Kapitel: BANKPARAMETERDATEN (BPD) Abschnitt: Aufbau

IV.2 Aufbau

Die Bankparameter setzen sich aus mehreren Segmenten zusammen, welche neben allgemeinen Informationen zum betreffenden Kreditinstitut Daten zu möglichen Kommunikationszugängen, zu unterstützten Sicherheitsverfahren, Komprimierungsverfahren und Geschäftsvorfällen enthalten. Hierbei können für einzelne Geschäftsvorfälle auch geschäftsvorfallspezifische Definitionen angegeben werden, sofern das FinTS-Format dies vorsieht.

In den folgenden Abschnitten wird näher auf die einzelnen Segmente eingegangen. Eine genaue Aufbaubeschreibung erfolgt in [Syntax].

IV.2.1 Bankparameter allgemein

Der allgemeine Teil der Bankparameterdaten enthält die aktuell gültige BPD-Version, die zugehörige Kreditinstitutskennung zuzüglich einer textuellen Bezeichnung sowie der BIC des Kreditinstituts, die unterstützten Sprachen und FinTS-Versionen sowie ggf. Beschränkungen bzgl. der maximal zulässigen Anzahl von Geschäftsvorfallarten je Auftragsteil und der maximal zulässigen Gesamtlänge einer FinTS-Nachricht.

Die übermittelte BPD-Version ist vom Kundensystem zusammen mit den BPD zu speichern. Innerhalb der Identifikation einer Initialisierung kann es diese dann angeben, so dass das Kreditinstitut weiß, welche BPD-Version beim Benutzer vorliegt. Ist diese BPD-Version nicht mehr aktuell, muss das Kreditinstitut die aktuellen BPD in die Initialisierungsantwort einstellen.

Darüber hinaus gelten die folgenden Belegungsrichtlinien:

Kreditinstitutskennung

Es ist die Kreditinstitutskennung des Kreditinstituts einzustellen, auf das sich die nachfolgenden Bankparameterdaten beziehen.

Anzahl Geschäftsvorfallsarten

Falls keine Restriktionen bzgl. der Anzahl an Geschäftsvorfallsarten bestehen, ist der Wert auszulassen.



Es ist zu beachten, dass diese Restriktion bereits dem Herausgeber eines Auftragsteils bekannt sein muss, da der Bote allein nicht immer für ihre Einhaltung sorgen kann. So hat bei teilverschlüsselten Nachrichten der Bote keine Kenntnis über die im verschlüsselten Auftragsteil enthaltenen Aufträge. Auch hat er nicht die Möglichkeit, einen unverschlüsselten Auftragsteil auf mehrere Nachrichten aufzuteilen, da hierdurch die Herausgeber/Zeugen-Signatur ungültig würde. Dies ist in allen Szenarien von Bedeutung, in denen der Bote der Nachricht nicht auch der Herausgeber des Auftragsteils ist.

Maximale Nachrichtengröße

Falls keine Restriktionen bzgl. der Nachrichtengröße bestehen, ist der Wert auszulassen. Die maximale Nachrichtengröße bezieht sich auf den Zustand der Benutzernachricht bei Erreichen des Kreditinstituts, also gegebenenfalls komprimiert und im korrekten Zeichensatz.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: IV
Kapitel: BANKPARAMETERDATEN (BPD) Abschnitt: Aufbau	Stand: 06.10.2017	Seite: 105



Sollte dieses DE belegt sein, hat das Kundenprodukt bei der Zusammenstellung der Nachricht diese Restriktion zu beachten. Zu große Nachrichten dürfen nicht zur Versendung freigegeben werden, das Kreditinstitut wäre berechtigt, sie abzulehnen. Eventuell hat das Kundenprodukt Nachrichten, die aus mehreren Aufträgen bestehen, in mehrere kleinere Nachrichten mit je einem Auftrag aufzuteilen. Kann die Nachrichtengröße bei umfangreichen Einzelaufträgen (z. B. Sammelüberweisungen) nicht verringert werden, so ist der Auftrag anwendungsseitig zu verkleinern.

Die Restriktion bezieht sich nicht auf die Größe der Nachrichten des Kreditinstituts. Das Kundenprodukt kann deren Größe beschränken, indem es im Bedarfsfall den Umfang der Antworten über die entsprechenden Parameter eines Abholauftrags fachlich einschränkt (z. B.: Anzahl Sätze, Bereich von..bis).

IV.2.2 Kommunikationszugang

Dieses Segment enthält transportmedienspezifische Informationen, die für den Zugang zum Kreditinstitut erforderlich sind.



Für den Erstzugang sind die dafür notwendigen Zugangsdaten auf einem anderen Weg (z. B. direkt durch einen Kundenbetreuer des Kreditinstituts) mitzuteilen.

Das Vorhandensein der Zugangsdaten in den BPD ermöglicht es dem Kreditinstitut, dem Kundenprodukt Änderungen dieser Parameter unaufgefordert innerhalb einer FinTS-Kommunikation mitzuteilen. Außerdem ist es möglich, die oben genannte Mitteilung der Daten für den Erstzugang durch Aushändigung der BPD abzuwickeln, beispielsweise in Form einer eines USB-Sticks.

Die Kommunikationszugangsdaten enthalten Angaben zu den verschiedenen möglichen Kommunikationsverfahren zwischen Kundensystem und Kreditinstitut. Für jedes Kommunikationsverfahren ist die Kommunikationsadresse anzugeben. Außerdem ist die Angabe weiterer transportmedienspezifischer Parameter möglich.

Es gelten die folgenden Belegungsrichtlinien.

Timeout-Werte

Mit den Werten für den minimalen und den maximalen Timeout wird angegeben, wann das Kundenprodukt frühestens nach dem Empfang der letzten Kreditinstitutsnachricht eine *KeepAlive*-Nachricht (siehe *III.5.3 Lebendmeldung in Dialogen*) senden sollte und wie lange der Kommunikationskanal eines bestehenden Dialoges kreditinstitutsseitig maximal geöffnet bleibt, wenn keine weitere Benutzernachricht empfangen wird.

Für *KeepAlive*-Nachrichten, die über einen Kommunikationskanal abgesendet werden, für den kein Timeout-Wert angegeben wurde, ist das Verhalten des Kreditinstituts undefiniert.

Kapitel: IV	Version: 4.1 FV	Financial Transaction Services (FinTS) Formals - Grundsätzliche Festlegungen
Seite: 106	Stand:	Kapitel: BANKPARAMETERDATEN (BPD) Abschnitt: Aufbau

IV.2.3 Sicherheitsverfahren

In diesem Segment sind die Sicherheitsverfahren, d. h. Signatur- und Verschlüsselungsalgorithmen, in den Versionen anzugeben, die das Kreditinstitut unterstützt. Zu jedem Verfahren wird eine Liste der in diesem Verfahren erlaubten Geschäftsvorfälle, ggf. mit weiteren Parametern, angegeben. Darüber hinaus kann festgelegt werden, ob die Mischung von verschiedenen Sicherheitsverfahren zulässig ist oder nicht.

Wenn das Mischen zulässig ist, dürfen verschiedene Benutzer (Bote, Herausgeber, Zeugen) unterschiedliche Verfahren einsetzen. Innerhalb einer Nachricht darf ein Benutzer jedoch nur Signatur-, Verschlüsselungs- und Komprimierungsalgorithmen aus einem einzigen Sicherheitsverfahren verwenden und er darf das Verfahren auch nicht von Nachricht zu Nachricht wechseln.

Ist Mischen nicht erlaubt, so müssen alle im Dialog verwendeten Algorithmen zu demjenigen Sicherheitsverfahren gehören, das der Bote in der ersten Nachricht des Dialogs verwendet, unabhängig vom jeweiligen Benutzer.



Insbesondere in Intermediär-Szenarien kann nicht unbedingt sichergestellt werden, dass Benutzer und Intermediär das gleiche Sicherheitsverfahren verwenden. Dies muss vom Kreditinstitut bedacht werden, wenn die Mischung von Sicherheitsverfahren nicht zugelassen werden soll.



IV.2.4 Komprimierungsverfahren

In diesem Segment sind die Komprimierungsverfahren in den Versionen anzugeben, die das Kreditinstitut unterstützt.

Eine Komprimierung von Nachrichtenteilen kann überall dort erfolgen, wo eine Verschlüsselung zulässig. Hierbei ist jeweils vor dem Verschlüsseln der Daten zu komprimieren.

Falls das Kreditinstitut Komprimierung unterstützt, ist der deflate- oder auch GZIP-Algorithmus gemäß [RFC 1951] zwingend anzubieten. Die anderen Algorithmen können zusätzlich optional angeboten werden.

IV.2.5 Geschäftsvorfallparameter

Zu jedem in FinTS definierten Geschäftsvorfall sind zugehörige Geschäftsvorfallparameter definiert. Sie beschreiben die konkrete kreditinstitutsindividuelle Ausgestaltung eines Geschäftsvorfalles. Ausnahmen bilden die administrativen Geschäftsvorfälle des Keymanagements [HBCI] und des TAN-Managements [PIN/TAN], die Synchronisation und die Lebendmeldung. Diese administrativen Vorgänge können durch das Kreditinstitut nicht ausgeschlossen oder parametrisiert werden und sind daher auch nicht Gegenstand der BPD.

Die Geschäftsvorfallparameter enthalten einen allgemeinen Teil, welcher Parameter enthält, die für jeden Geschäftsvorfall angegeben werden müssen. Sie können darüber hinaus weitere Teile enthalten, welche für den jeweiligen Geschäftsvorfall spezifische Parameter enthalten.

Die allgemeinen Parameter geben an, wie oft der Geschäftsvorfall in einer Nachricht maximal vorkommen darf und wie oft er mindestens signiert sein muss.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: IV
Kapitel: BANKPARAMETERDATEN (BPD) Abschnitt: Aufbau	Stand: 06.10.2017	Seite: 107

Ein Parametersegment ist für jeden Geschäftsvorfall in den Versionen einzustellen, die das Kreditinstitut in mindestens einem Sicherheitsverfahren unterstützt (vgl. *IV.2.3 Sicherheitsverfahren*). Wird ein Geschäftsvorfall in einer bestimmten Version in keinem Sicherheitsverfahren unterstützt, kann das Parametersegment der gleichen Version entfallen. Die Zuordnung der Geschäftsvorfallparameter zur jeweiligen Version des Geschäftsvorfalles erfolgt hierbei anhand des dem Parametersegment zugrundeliegenden XML-Schemas (siehe [Syntax]). Die Reihenfolge der Parametersegmente innerhalb der Nachricht ist ohne Bedeutung.



Da ein Kreditinstitut neben den in der Deutschen Kreditwirtschaft standardisierten Geschäftsvorfällen auch verbands- oder institutseigene Transaktionen unterstützen kann (siehe *I EINLEITUNG*), die dem Kundenprodukt unter Umständen nicht bekannt sind, darf ein Kundenprodukt Parametersegmente zu ihm unbekanntem XML-Schemas nicht als Fehler ablehnen, sondern sollte diese ignorieren.

Kapitel: IV	Version: 4.1 FV	Financial Transaction Services (FinTS) Formals - Grundsätzliche Festlegungen
Seite: 108	Stand:	Kapitel: BANKPARAMETERDATEN (BPD) Abschnitt: Anforderung der BPD in einem Szenario mit Intermediär

IV.3 Anforderung der BPD in einem Szenario mit Intermediär

Der Standardfall der BPD-Anforderung ist das Senden einer Initialisierung ohne oder mit veralteter BPD-Version. Dies ist jedoch nur für den Benutzer möglich, der als Bote einer Nachricht auftritt. Er erhält in diesem Fall die BPD.

Ein Benutzer, welcher ausschließlich über einen Intermediär an sein Kreditinstitut herantritt, tritt nie selbst als Bote einer Nachricht auf. Er sendet somit auch nie eine Initialisierung und kann daher nie die BPD innerhalb einer Initialisierungsantwort erhalten. Auch er benötigt eine Möglichkeit, die BPD in Form eines speziellen Auftrages innerhalb des Auftragsteils einer Nachricht anzufordern. Für diese Fälle ist ein spezieller administrativer Geschäftsvorfall *BPD anfordern* definiert. Der genaue Aufbau wird in [Syntax] beschrieben.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: V
Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: Anforderung der BPD in einem Szenario mit Intermediär	Stand: 06.10.2017	Seite: 109

V. USER-PARAMETERDATEN (UPD)

V.1 Allgemeines	110
V.2 Aufbau	112
V.2.1 User-Parameter allgemein.....	112
V.2.2 Kontoinformation	112
V.2.2.1 Geschäftsvorfälle ohne Kontobezug.....	112
V.3 UPD für anonymen Zugang.....	114
V.4 UPD des Intermediärs (IPD)	115
V.5 UPD des Benutzers für Intermediärzugang (UPDI).....	116
V.6 Explizite Anforderung von UPD	118
V.7 Pflege der Intermediärzugänge und der UPDI	119
V.7.1.1 Intermediäre auflisten	119
V.7.1.2 An- und Abmelden der Intermediär-Benutzung.....	119
V.7.1.3 UPDI bearbeiten	119

Kapitel: V	Version: 4.1 FV	Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen
Seite: 110	Stand: 06.10.2017	Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: Allgemeines

V.1 Allgemeines

Realisierung Kreditinstitut: verpflichtend
Realisierung Kundenprodukt: verpflichtend

Während die Bankparameterdaten die grundsätzlich vom Kreditinstitut angebotenen Geschäftsvorfälle angeben, gestatten die User-Parameterdaten kontenbezogene Berechtigungsprüfungen im Kundenprodukt. So kann das Kundenprodukt mit Hilfe der User-Parameterdaten prüfen, ob der Benutzer für die Ausführung eines der in den Bankparameterdaten angegebenen Geschäftsvorfälle in Verbindung mit einem bestimmten Konto berechtigt ist. Zusätzlich zu kontenbezogenen Informationen befinden sich im allgemeinen Teil der UPD ggf. weitere Einstellungen zum Benutzer und Angaben zu seiner Berechtigung für Geschäftsvorfälle ohne Kontenbezug.

Das Konto, das im jeweiligen Geschäftsvorfall für die Berechtigungsprüfung heranzuziehen ist, ist im Regelfall entweder das Auftraggeberkonto, das Depotkonto bei Wertpapieraufträgen oder das Anlagekonto bei Festgeldanlagen. In den Fällen, in denen es sich um ein hiervon abweichendes Konto handelt, ist dies in der Geschäftsvorfallbeschreibung vermerkt.

Die administrativen Geschäftsvorfälle des Keymanagements [HBCI] und des TAN-Managements [PIN/TAN], die Synchronisation und die Lebendmeldung können durch das Kreditinstitut nicht ausgeschlossen werden und sind daher nicht Gegenstand der UPD.

Bei Änderungen werden die User-Parameterdaten im Rahmen der Initialisierung für den als Bote auftretenden Benutzer automatisch aktualisiert. Die aktualisierten UPD werden sofort aktiv (siehe hierzu die Ausführungen zu den BPD in *IV BANKPARAMETERDATEN (BPD)*). In Szenarien mit Intermediär wird darüber hinaus ein Auftrag zur expliziten Anforderung von UPD benötigt, siehe dazu *V.6 Explizite Anforderung von UPD*.

Im nächsten Abschnitt *V.2 Aufbau* wird die Struktur der UPD näher erläutert, eine detaillierte Aufbaubeschreibung erfolgt in [Syntax].

Die darauf folgenden Abschnitte beschäftigen sich mit weiteren Ausprägungen der UPD, die bei anonymem Zugang und in Intermediärszenarien Verwendung finden. Die erforderlichen Aufträge zu deren Verwaltung werden dort ebenfalls aufgeführt.

Alle hier genannten administrativen Aufträge außer *Intermediäre auflisten* beziehen sich auf einen explizit im Auftrag genannten oder (bei *UPDI ändern*) implizit in eingereichten UPD-Daten enthaltenen Benutzer. Für diese gelten bezüglich der Berechtigungen und Signaturpflicht die Festlegungen aus *III.1 Allgemeines*, sie können folglich ausschließlich in personalisierten Dialogen mit entsprechender Herausgebersignatur verwendet werden.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: V
Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: Allgemeines	Stand: 06.10.2017	Seite: 111



Da auf Schnittstellenebene nicht gewährleistet werden kann, dass das Kundenprodukt die User-Parameterdaten korrekt auswertet, hat auf jeden Fall eine entsprechende kreditinstitutsseitige Prüfung stattzufinden.



Ein Kundensystem sollte davon ausgehen, dass das Kreditinstitut im Rahmen der Berechtigungsprüfung für einen Auftrag die UPD aller Signierenden des Auftrags heranzieht.

Obwohl die Einstellung der Kontoinformationen für das Kreditinstitut nicht verpflichtend ist, sollte es, im Interesse einer einfachen und komfortablen Kontenverwaltung für den Benutzer, diese Informationen für alle Konten des Benutzers bereitstellen.



Die Nutzung der UPD erfordert eine entsprechende Unterstützung durch das Kundenprodukt. Sofern es erforderlich ist, die UPD in einer Datei abzuspeichern, sollte die Datei vor unbefugtem Zugriff geschützt werden, da es sich um sensible Daten handelt.

Da die Einstellung der Kontoinformationen für das Kreditinstitut nicht verpflichtend ist, sollte das Kundenprodukt die Möglichkeit der manuellen Kontenerfassung vorsehen.

Vgl. auch Hinweise in *IV BANKPARAMETERDATEN (BPD)*.

Kapitel: V	Version: 4.1 FV	Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen
Seite: 112	Stand: 06.10.2017	Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: Aufbau

V.2 Aufbau

Die User-Parameter gliedern sich in einen allgemeinen Teil und in den Kontoinformationsteil, welcher je Konto die erlaubten Geschäftsvorfälle festlegt.

V.2.1 User-Parameter allgemein

Der allgemeine Teil der UPD enthält bei User-Parameterdaten eines Benutzers für den direkten Zugang die Benutzerkennung, bei User-Parameterdaten eines Intermediärs (IPD) die Intermediärkennung, bei User-Parameterdaten eines Benutzers für den Intermediärzugang beide Kennungen. Außerdem ist die aktuelle Version der UPD angegeben, optional der Name des Benutzers sowie der UPD-Verwendungsmodus. Dieser gibt an, ob die in den UPD nicht aufgeführten Geschäftsvorfälle für den Benutzer als gesperrt zu betrachten sind oder ob hierüber keine Aussage möglich ist. Weiterhin gibt es ein nicht weiter spezifiziertes Parameterfeld, mit dem einem Kundenprodukt weitere benutzerbezogene Informationen zur Verfügung gestellt werden können.

V.2.2 Kontoinformation

Die DEG „Kontoinformation“ sollte für jedes Konto, für das der Benutzer beim betreffenden Kreditinstitut eine Verfügungsberechtigung besitzt, eingestellt werden. Ein Benutzer kann auch für andere Konten als seine eigenen verfügungsberechtigt sein (z. B. Firmenkonten). Dabei kann er rollenabhängig verschiedene Berechtigungen für ein Konto haben (z. B. als Erfassender von Zahlungsaufträgen oder als Prokurist einer Firma). Nähere Erläuterungen zum Rollenkonzept für einen Benutzer befinden sich in *II.1.3 Benutzer und Kunde* bei den Ausführungen zu Benutzern und Kunden und in [HBCI], Abschnitt *II.5.1 Signatur-Segment*.

Die DEG enthält neben der Kontoverbindung, auf die es sich bezieht, die Kundenkennung und den Namen des Kontoinhabers. Darüber hinaus können Angaben zur Kontowährung, eine Kontoproduktbezeichnung, ein Kontolimit und eine Liste der auf dem Konto für den Benutzer erlaubten Geschäftsvorfälle vorhanden sein.

Daneben ist ein nicht weiter spezifiziertes Parameterfeld enthalten, mit dem einem Kundenprodukt ergänzende kontobezogene Informationen zur Verfügung gestellt werden können. Dieses DE „Unformatierte Kontoparameter“ wurde in FinTS V3 speziell auf Basis von JSON modelliert, um eine gezielte Abfrage von Bestandsdaten zu ermöglichen bzw. im Gegenzug unnötige Bestandsabfragen zu vermeiden. Die entsprechenden Festlegungen befinden sich in FinTS V3.0 im Band [Formals] in den Kapiteln *E.3.1 Aufbau der UPD-Erweiterung, kontobezogen* und *F FinTS-Prozesse*. JSON-Strukturen, die den dort gemachten Vorgaben entsprechen, können im DE „Unformatierte Kontoparameter“ transportiert werden. Eine XML-basierte Modellierung dieser Datenstrukturen wird ggf. zu einem späteren Zeitpunkt erfolgen, wenn eine entsprechende Marktabdeckung mit FinTS V4 basierten Kundenprodukten absehbar ist.

V.2.2.1 Geschäftsvorfälle ohne Kontobezug

Es kann auch ein Eintrag für nicht kontogebundene Geschäftsvorfälle (z. B. Informationsbestellung) eingestellt werden. Hierbei handelt es sich im Regelfall um Geschäftsvorfälle, die auch über den anonymen Zugang genutzt werden können. Dieser Eintrag enthält weder die Kontoverbindung noch sonstige kontobezogene Angaben.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: V
Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: Aufbau	Stand: 06.10.2017	Seite: 113

Werden Geschäftsvorfälle, die inhaltlich einen Kontenbezug enthalten, als nicht kontogebundene Geschäftsvorfälle eingestellt, gilt die Berechtigung für diese Geschäftsvorfälle für alle Konten, für die der Benutzer verfügungsberechtigt ist.



Ein Geschäftsvorfall, der im Abschnitt für „nicht kontogebundene Geschäftsvorfälle“ aufgeführt ist, darf nicht gleichzeitig unter einem konkreten Konto aufgeführt sein und umgekehrt.

In der Liste der erlaubten Geschäftsvorfälle kann je Geschäftsvorfall angegeben werden, wie oft dieser zu signieren ist und ob ein geschäftsvorfallsspezifisches Limit existiert. Die Anzahl der nötigen Signaturen kann hierbei nur größer oder gleich der für den Geschäftsvorfall in den BPD angegebenen Anzahl sein.

Kapitel: V	Version: 4.1 FV	Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen
Seite: 114	Stand: 06.10.2017	Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: UPD für anonymen Zugang

V.3 UPD für anonymen Zugang

Auch für Nachrichten über den anonymen Zugang sind UPD zur Regelung der Zugriffsberechtigungen vorzusehen („Gast-UPD“). Diese sind aufgebaut wie benutzerbezogene UPD, enthalten jedoch keine Benutzererkennung in den allgemeinen Parametern und keine kontobezogenen Abschnitte.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: V
Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: UPD des Intermediärs (IPD)	Stand: 06.10.2017	Seite: 115

V.4 UPD des Intermediärs (IPD)

Auch ein Intermediär besitzt UPD, welche im Folgenden mit Intermediärparameterdaten (IPD) bezeichnet werden. Der Aufbau der IPD ist identisch zu dem der UPD. Allerdings besitzt der Intermediär selbst keine Konten, so dass in der IPD nicht hinterlegt ist, auf welchen eigenen Konten er welche Geschäftsvorfälle ausführen kann. Vielmehr ist hier im Abschnitt für nicht-kontobezogene Geschäftsvorfälle hinterlegt, welche Geschäftsvorfälle er generell für einen Kunden des Kreditinstituts einreichen darf.

Das Kreditinstitut ordnet jedem von ihm unterstützten Intermediär IPD zu, wodurch für jeden Intermediär der maximale Funktionsumfang gegenüber dem Kreditinstitut festgelegt wird. Für einen bestimmten Benutzer kann der Intermediär jedoch nur solche Geschäftsvorfälle ausführen, für die dieser berechtigt ist - siehe dazu V.5 *UPD des Benutzers für Intermediärzugang (UPDI)*.

Kapitel: V	Version: 4.1 FV	Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen
Seite: 116	Stand: 06.10.2017	Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: UPD des Benutzers für Intermediärzugang (UPDI)

V.5 UPD des Benutzers für Intermediärzugang (UPDI)

Für die direkte Kommunikation eines Benutzers mit dem Kreditinstitut legen seine UPD die Berechtigungen fest.

Bei der Kommunikation über einen Intermediär sind für den Benutzer anstelle der UPD seine User-Parameterdaten für Intermediärzugang (UPDI) maßgeblich. Der Benutzer besitzt zu jedem Intermediär eine individuelle UPDI. In Syntax und Semantik entsprechen die UPDI den UPD, lediglich das Einsatzszenario ist unterschiedlich (Intermediärkommunikation bzw. direkte Kommunikation). Die Beziehungen zwischen BPD und den verschiedenen Arten von UPD werden in Abbildung 39: Mögliche Beziehungen zwischen BPD, UPD, IPD und UPDI gezeigt (im Diagramm steht das nachgestellte „n“ bei $UPDI_n$ und IPD_n dafür, dass es pro Intermediär einen solchen Parametersatz gibt). Insbesondere gilt:

- ◆ Die BPD umfassen alle Geschäftsvorfälle eines Instituts.
- ◆ UPD, IPD und UPDI sind jeweils Teilmengen der BPD, d.h. sie können den durch die BPD festgelegten Umfang nur einschränken und detaillieren, nicht aber erweitern.
- ◆ Die $UPDI_n$ sind immer eine Teilmenge der entsprechenden IPD_n (die Erlaubnis, Geschäftsvorfälle über einen Intermediär zu benutzen, ist nur sinnvoll, wenn der Intermediär diese auch unterstützt). Die $UPDI_n$ können eine Teilmenge der UPD oder sogar identisch mit diesen sein, sie können aber auch nur eine gemeinsame Schnittmenge mit den UPD haben oder völlig disjunkt zu diesen sein. Im Allgemeinen werden UPD und $UPDI_n$ voneinander abweichen, d.h. es gibt Geschäftsvorfälle, die der Benutzer nur direkt oder aber nur über einen bestimmten Intermediär ausführen kann.
- ◆ Die Schnittmenge aus IPD_n und UPD kann durchaus leer sein. Zwangsläufig sind dann auch die UPD und die $UPDI_n$ disjunkt, das heißt, es gibt keine Geschäftsvorfälle, die der Benutzer sowohl direkt als auch über diesen Intermediär ausführen kann.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: V
Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: UPD des Benutzers für Intermediärzugang (UPDI)	Stand: 06.10.2017	Seite: 117

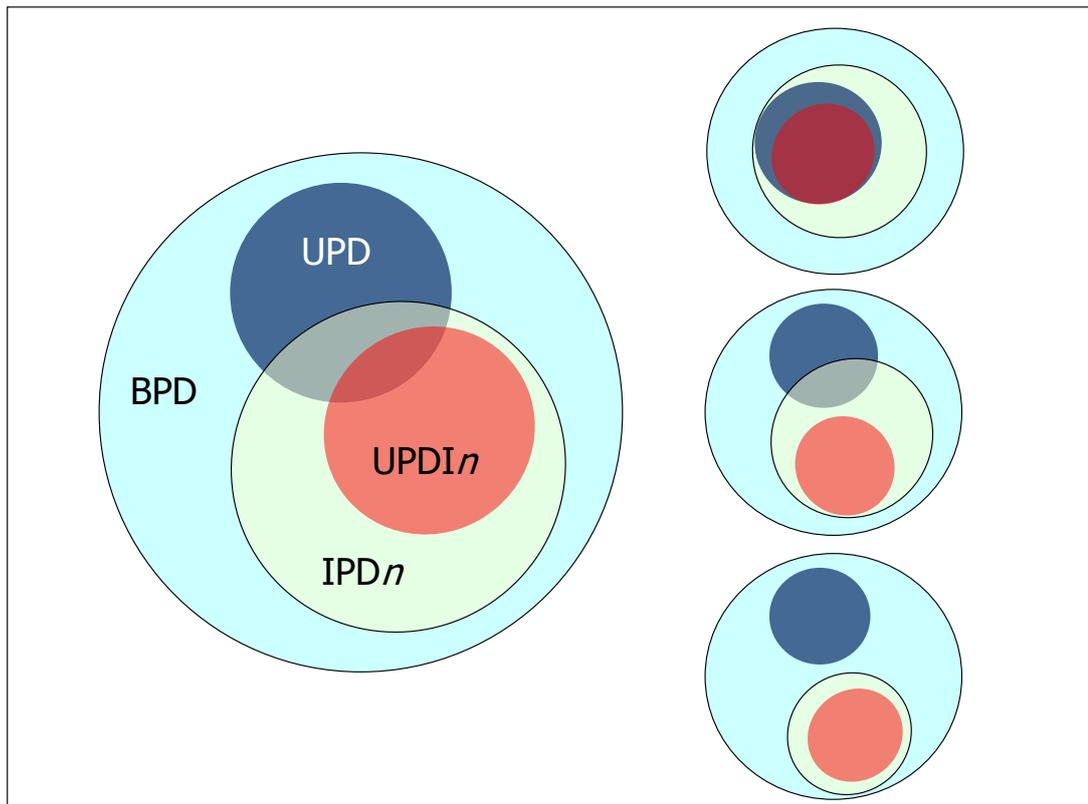


Abbildung 39: Mögliche Beziehungen zwischen BPD, UPD, IPD und UPDI

Die UPDI können mit gewissen Einschränkungen vom Benutzer über einen speziellen dafür vorgesehenen Geschäftsvorfall gepflegt werden. Siehe dazu den Abschnitt *V.7 Pflege der Intermediärzugänge und der UPDI*.

Kapitel: V	Version: 4.1 FV	Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen
Seite: 118	Stand: 06.10.2017	Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: Explizite Anforderung von UPD

V.6 Explizite Anforderung von UPD

Der Standardfall einer UPD-Anforderung ist das Senden einer Initialisierung ohne oder mit veralteter UPD-Version. Dies ist jedoch nur für den Benutzer möglich, der als Bote einer Nachricht auftritt. Er erhält in diesem Fall die eigenen UPD bzw., wenn es sich um einen Intermediär handelt, die eigenen IPD. Ein Benutzer, der über einen Intermediär kommuniziert, kann auf diese Weise seine UPD nicht erhalten. Außerdem wird im Intermediärszenario ein Mechanismus zur expliziten Anforderung von UPDI benötigt. Es bestehen also folgende Anforderungen:

- ◆ Ein Intermediär muss die UPDI der bei ihm angemeldeten Benutzer abfragen können.
- ◆ Ein Benutzer, der über einen Intermediär kommunizieren möchte, muss seine UPDI für diesen Intermediär abfragen können.
- ◆ Für die Pflege seiner UPDI muss ein Benutzer die IPD des betreffenden Intermediärs sowie seine eigenen UPD abfragen können (vgl. *V.7 Pflege der Intermediärzugänge und der UPDI*).

Für diese Fälle ist ein spezieller administrativer Geschäftsvorfall *UPD anfordern* definiert, mit welchem ein beliebiger Benutzer die UPD (bzw. IPD, UPDI) eines beliebigen anderen Benutzers anfordern kann. Ob er hierzu berechtigt ist, entscheidet das Kreditinstitut. Im Regelfall sollten genau die Berechtigungen für die in der obigen Aufzählung genannten Fälle erteilt werden.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: V
Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: Pflege der Intermediärzugänge und der UPDI	Stand: 06.10.2017	Seite: 119

V.7 Pflege der Intermediärzugänge und der UPDI

Der Benutzer kann eine Liste von unterstützten Intermediären anfordern, sich für den Zugang über einen Intermediär an- und wieder abmelden und je Intermediär die UPD-Daten zu einzelnen Konten freigeben und wieder sperren. Diese Geschäftsvorfälle sollen hier kurz vorgestellt werden. Der genaue Aufbau wird in [Syntax] beschrieben.

V.7.1.1 Intermediäre auflisten

Der Benutzer kann mit diesem Auftrag feststellen, welche Intermediäre registriert sind und welche Eigenschaften diese haben. Dazu gehören neben einer eindeutigen Kennung des Intermediärs die möglichen Zugangsadressen. Außerdem kann das Kreditinstitut jedem Intermediär eine textuelle Beschreibung zuordnen. Die eindeutige Kennung des Intermediärs wird für die Geschäftsvorfälle *Für einen Intermediär anmelden*, *Für einen Intermediär abmelden*, *UPDI ändern* benötigt.

V.7.1.2 An- und Abmelden der Intermediär-Benutzung

Will ein Benutzer Geschäftsvorfälle über einen Intermediär ausführen, muss er sich zuvor einmalig beim Kreditinstitut mit dem Geschäftsvorfall *Für einen Intermediär anmelden* für diesen registrieren (anmelden). Entsprechend kann der Benutzer mit dem Geschäftsvorfall *Für einen Intermediär abmelden* die Benutzung dieses Intermediärs wieder abmelden.

V.7.1.3 UPDI bearbeiten

Die UPDI eines Benutzers für einen bestimmten Intermediär werden initial vom Kreditinstitut vorgegeben. Sie sollten im Normalfall mindestens alle Möglichkeiten der Schnittmenge aus UPD des Benutzers und IPD des Intermediärs umfassen (diese Schnittmenge kann allerdings leer sein). Das Institut kann entscheiden, dem Benutzer darüber hinaus weitere Geschäftsvorfälle nur im Rahmen des Intermediärzugangs zu ermöglichen. Diese wären dann in den UPDI, nicht aber in den UPD enthalten.

Über einen speziellen Geschäftsvorfall *UPDI ändern* wird dem Benutzer die Modifikation seiner UPDI ermöglicht. Er kann Geschäftsvorfälle auf Konten zur Ausführung über den Intermediär zulassen oder sperren, allerdings nur im Rahmen der Möglichkeiten seiner eigenen UPD. Das bedeutet, er kann ausschließlich Geschäftsvorfälle *aus der Schnittmenge* zwischen UPD und IPD in die UPDI aufnehmen oder sie daraus entfernen. Der übrige Teil der UPDI wird allein durch das Kreditinstitut gepflegt. Siehe dazu auch Abbildung 39: Mögliche Beziehungen zwischen BPD, UPD, IPD und UPDI.

Kapitel: V	Version: 4.1 FV	Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen
Seite: 120	Stand: 06.10.2017	Kapitel: USER-PARAMETERDATEN (UPD) Abschnitt: Pflege der Intermediärzugänge und der UPDI

Die folgende Abbildung zeigt ein Beispiel für diese Sachverhalte (im Beispiel besteht die relevante Schnittmenge aus UPD und IPD für beide Konten aus den Geschäftsvorfällen „Einzelüberweisung“ und „Saldenabfrage“):

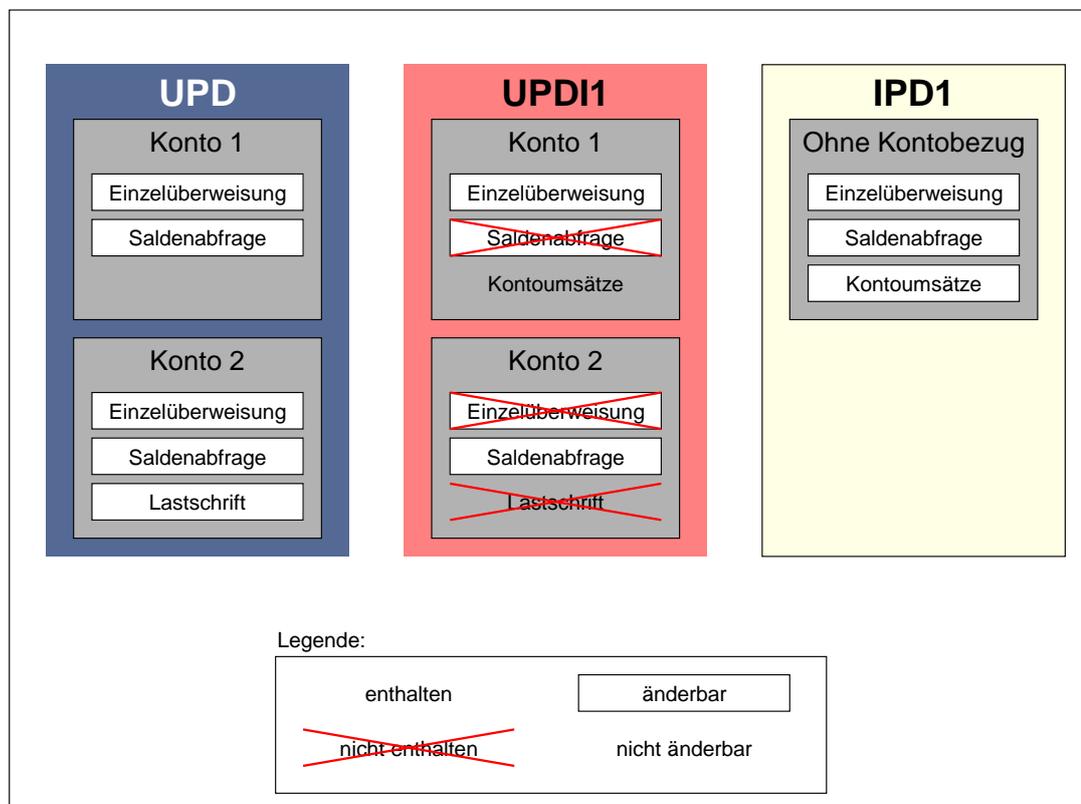


Abbildung 40: Beispiel für Pflege der UPDI

Als Voraussetzung für die Modifikation seiner UPDI benötigt ein Benutzer folglich seine UPD, die UPDI und die IPD des betreffenden Intermediärs. Er erhält diese mit dem Geschäftsvorfall *UPD anfordern* (siehe dazu auch *V.6 Explizite Anforderung von UPD*).

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: VI
Kapitel: Transportmedienspezifische Festlegungen Abschnitt: Pflege der Intermediärzugänge und der UPDI	Stand: 06.10.2017	Seite: 121

VI. TRANSPORTMEDIENSPEZIFISCHE FESTLEGUNGEN

Obwohl FinTS grundsätzlich unabhängig von darunter liegenden Kommunikationsschichten ist, müssen doch bestimmte Festlegungen für die zu liefernden Netze getroffen werden, um FinTS multibankfähig und einheitlich zu definieren.

Hierbei handelt es sich um folgende Aspekte:

- Einschränkung der Kombinationsmöglichkeit von Protokollen, die für die gesicherte Übertragung von FinTS-Nachrichten zugelassen werden.
- Festlegung von verwendeten Parametern.
- Abbilden von FinTS-Kommunikationsabläufen auf die darunter liegenden Strukturen.

Wenn eines der nachfolgend beschriebenen Protokolle eine ausdrücklich als zulässig gekennzeichnete Transportverschlüsselung bietet, ist diese alternativ oder zusätzlich zur Verwendung verschlüsselter FinTS-Nachrichten (HBCI-Sicherheit) einsetzbar. Sollte die Transportverschlüsselung zur Verschlüsselung von bereits verschlüsselten FinTS-Nachrichten eingesetzt werden, ist die Transportverschlüsselung nicht relevant.

Eine in einem übermittelten Datagramm angegebene asynchrone Rückantwortadresse (vgl. Abschnitt II.7 „FinTS Datagramme“ und [Syntax]), die von der durch das Transportverfahren vorgegebene Rückantwortadresse abweicht, wird bevorzugt benutzt.

Zurzeit sind die folgenden Transportdienste beschrieben:

- HTTP (zulässige Transportverschlüsselung: TLS)
- SMTP

Kapitel: VI	Version: 4.1 FV	Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen
Seite: 122	Stand: 06.10.2017	Kapitel: Transportmedienspezifische Festlegungen Abschnitt: HTTP

VI.1 HTTP

Realisierung Kreditinstitut: verpflichtend
Realisierung Kundensystem: verpflichtend

Der Transport von FinTS-Nachrichten über das „Hypertext Transfer Protocol“ (HTTP) stellt ein dialogorientiertes Verfahren zwischen Benutzer und Kreditinstitut dar. Die Kommunikation wird über die für HTTP bzw. HTTPS standardisierten Ports 80 bzw. 443 abgewickelt, so dass der Austausch von Nachrichten auch mit Kundenprodukten, die hinter einer Firewall lokalisiert sind, problemlos möglich ist.



Hersteller sollten ihre Produkte so flexibel gestalten, dass auch andere als die oben genannten Ports für die Kommunikation genutzt werden können.



Die Kommunikation erfolgt ausschließlich über HTTP/1.1 [RFC 2616]. FinTS-Nachrichten des Benutzers werden als Rumpf eines HTTP-Requests mittels der POST-Methode an das Kreditinstitut übertragen. Dieses sendet die Kreditinstitutsnachrichten im Rumpf einer HTTP-Response. Es werden immer vollständige FinTS-Nachrichten übertragen, eine Aufteilung in mehrere Requests bzw. Responses findet nicht statt. Wenn in Antworten des Kreditinstituts ein Statuscode geliefert wird, der nicht zwischen 200 und 299 (jeweils einschließlich) liegt, muss das Kundenprodukt dies als Fehler betrachten und die Kommunikation abbrechen.

Als MIME-Medientyp wird `application/vnd.fints` verwendet.

Die Kommunikation zwischen Benutzer und Kreditinstitut kann durch die SSL-Transportverschlüsselung gesichert werden. Dabei muss mindestens SSL Version 3.0 verwendet werden. SSL kann nach Vereinbarung zwischen den Kommunikationspartnern eine HBCI-Verschlüsselung vollständig ersetzen. Die Verwendung von TLS kann alternativ oder zusätzlich zur Verwendung verschlüsselter FinTS-Nachrichten erfolgen.



Um für den Benutzer sicherzustellen, dass er bei einer durch TLS gesicherten Kommunikation wirklich mit dem Kreditinstitut verbunden ist, sollte Server-Zertifizierung eingesetzt werden.

Bei der Kommunikation über HTTP zwischen Benutzer und Kreditinstitut besteht keine permanente Verbindung zwischen den Kommunikationspartnern, d. h. die Zugehörigkeit einzelner Nachrichten zu einer Kommunikation kann nur anhand der Kundenreferenz ermittelt werden. Die Kundenreferenz sollte nach den in [Formals], Abschnitt II.15.3 *Empfehlung für die Bildung von Kommunikationsreferenzen* angegebenen Regeln erfolgen.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: VI
Kapitel: Transportmedienspezifische Festlegungen Abschnitt: HTTP	Stand: 06.10.2017	Seite: 123



Das Kundenprodukt muss die Kommunikation mit dem Kreditinstitut über einen auf Kundenseite angesiedelten Proxy unterstützen. Dabei ist mittels geeigneter Parameterbelegung sicherzustellen, dass die Daten nicht über zwischengeschaltete Caches gespeichert werden.

Kundenprodukte müssen weiterhin eine ggf. vom Proxy geforderte Proxy-Authentifikation unterstützen.

Im Folgenden wird exemplarisch die Kommunikation zwischen Benutzer und Kreditinstitut vorgestellt. Das Kundenprodukt sendet bei der Kommunikation über HTTP/1.1 einen Request nach folgendem Muster:

```
POST fint.s.kredinst.de/fints/in HTTP/1.1
Host: fint.s.kredinst.de
Pragma: no-cache
Cache-Control: no cache
Content-Length: nnn
Content-Type:                application/vnd.fints;
charset="UTF-8"

<ReqMsg>
    ...
</ReqMsg>
```

Dabei ist in `<ReqMsg/>` eine gültige FinTS-Nachricht nach der vorliegenden Spezifikation einzusetzen. Für den Platzhalter *nnn* ist die Länge der Nachricht einzustellen. Als Zeichensatzcodierung ist ausschließlich UTF-8 zulässig.

Im Unterschied zur Kommunikation über HTTP/1.0 ist bei HTTP/1.1 zusätzlich zum `no-cache-Pragma` `,Cache-Control: no-cache'` und `,Host: fint.s.kredinst.de'` anzugeben:

Das Kreditinstitut beantwortet die Nachricht des Benutzers nach der Bearbeitung mit einer HTTP-Response nach folgendem Muster:

Kapitel: VI	Version: 4.1 FV	Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen
Seite: 124	Stand: 06.10.2017	Kapitel: Transportmedienspezifische Festlegungen Abschnitt: HTTP

```

HTTP/1.1 200 OK
Cache-Control: no-cache
Content-Length: mmm
Content-Type: application/vnd.fints;
charset="UTF-8"

<RespMsg>
  ...
</RespMsg>

```

Auch die Antwort ist ausschließlich in HTTP 1.1 angegeben. Zu beachten ist, dass auch der Server ‚Cache-Control: no-cache‘ einstellt und als Zeichensatzcodierung UTF-8 verwendet.



Eine Komprimierung der FinTS-Nachrichten über *Content-Encoding*, wie sie seit HTTP 1.1 möglich ist, wird nicht vorgenommen, weil FinTS von sich aus die Möglichkeit bietet, Nachrichten vor der Verschlüsselung zu komprimieren. Eine Komprimierung von bereits komprimierten oder verschlüsselten Daten wäre nicht sinnvoll. Bei SSL-gesicherter Übertragung wird die Komprimierung implizit vorgenommen.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: VI
Kapitel: Transportmedienspezifische Festlegungen Abschnitt: SMTP	Stand: 06.10.2017	Seite: 125

VI.2 SMTP

Realisierung Kreditinstitut: freigestellt

Realisierung Kundensystem: freigestellt

Dieses Transportverfahren stellt ein datei- und nachrichtenorientiertes Verfahren dar, bei dem FinTS-Nachrichten per E-Mail [RFC 821] zwischen Benutzer und Kreditinstitut ausgetauscht werden. Somit ist es z. B. in Situationen, in denen keine permanente Kommunikationsverbindung zwischen Kundenprodukt und Kreditinstitut aufgebaut werden soll oder kann, trotzdem möglich, Bankgeschäfte mittels FinTS abzuwickeln.

Bei der Kommunikation werden FinTS-Datagramme als normales E-Mail-Attachment nach [RFC2045] und [RFC2046] versendet. In einer E-Mail können mehrere FinTS-Datagramme versendet werden, für jedes Datagramm ist ein eigenes Attachment zu verwenden. Für das Attachment wird der MIME-Medientyp `application/vnd.fints` verwendet. Ein Content-Transfer-Encoding für das Attachment ist zulässig, wobei die FinTS-Datagramme in UTF-8-Kodierung vorliegen müssen.

```
Content-Type: multipart/mixed;
boundary=""=_51C1256DC_"
...
---=_51C1256DC_=
Content-Type: application/vnd.fints;
charset="UTF-8"Content-transfer-encoding: base64
...
```

Das Betreff-Feld und der Rumpf der E-Mail (bis auf das FinTS-Attachment) werden vom Kreditinstitut ignoriert. Somit ist es nicht möglich, Verarbeitungshinweise oder sonstige Daten über diesen Weg an das Kreditinstitut zu übermitteln.



Das Kundenprodukt kann z. B. zu Archivierungszwecken im Betreff-Feld der E-Mail nur für das Produkt selbst relevante Informationen unterbringen. Aus Datenschutzgründen muss aber darauf geachtet werden, dass hier keine sensiblen Daten preisgegeben werden.

Kapitel: VI	Version: 4.1 FV	Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen
Seite: 126	Stand: 06.10.2017	Kapitel: Transportmedienspezifische Festlegungen Abschnitt: SMTP



Das Kreditinstitut sollte – obwohl es den Betreff einer E-Mail nicht weiterverarbeitet – im Betreff-Feld der Antwort-E-Mail den Inhalt des Betreff-Feldes der Benutzernachricht widerspiegeln. Dabei kann der Feldinhalt aber um ein Präfix wie z. B. „Antwort:“ oder „Re:“ erweitert werden.

Eine Kreditinstitutsantwort, die nicht zugestellt werden konnte, wird vom Kreditinstitut nicht gepuffert oder erneut gesendet¹, da dies einen sehr hohen Verwaltungsaufwand bedeuten würde. Der Benutzer hat über die üblichen Mechanismen wie das Abholen des Statusprotokolls oder die Synchronisierung bzgl. der Kundenreferenz die Möglichkeit, sich beim Kreditinstitut nach dem Status seiner Auftragsnachricht zu erkundigen.

Es ist zu beachten, dass eine innerhalb einer Benutzernachricht angegebene Rückantwortadresse die aus der E-Mail entnommene Antwortadresse übersteuern kann, so dass der Benutzer nicht zwingend eine Antwort-E-Mail des Kreditinstituts an die Absenderadresse der E-Mail bekommt.

¹ Davon unbenommen sind die Mechanismen, die bei SMTP ohnehin vorgesehen sind, um bei kurzzeitigen Serverausfällen E-Mails zumindest für einen bestimmten Zeitraum zu puffern, um später einen weiteren Versuch zu unternehmen, diese E-Mail zuzustellen.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: VI
Kapitel: Transportmedienspezifische Festlegungen Abschnitt: Sonstige Kommunikationsdienste	Stand: 06.10.2017	Seite: 127

VI.3 Sonstige Kommunikationsdienste

Wird die Kommunikation über einen bisher nicht erfassten Kommunikationsdienst angestrebt, so sind zur Sicherstellung der Multibankfähigkeit vorab alle weiteren Spezifikationen durch Die Deutsche Kreditwirtschaft einheitlich festzulegen.

VI.4 Codierung

Die Codierung der Kommunikationswege erfolgt nach folgender Vorschrift:Code	Kommunikationsweg
3	HTTPS
4	SMTP
5	HTTP
6	SOAP mit HTTP-Binding (obsolet)

Tabelle 1: Codierung der Kommunikationswege

VI.5 Zulässige Kombinationen von Kommunikationsart, Transportprotokoll und Sicherheitsverfahren

Als zulässige Kommunikationsarten, über die ein Benutzer mit einem Kreditinstitut FinTS-Nachrichten austauschen kann, sind die synchrone Kommunikation (Dialog) und die asynchrone Kommunikation (Datagramme) in [Formals], Abschnitt *11.5 Unterstützte Kommunikationsverfahren im Überblick* beschrieben worden. Hiervon sollten beide Seiten bestimmte Transport- und Sicherheitsverfahren verpflichtend unterstützen, andere sind optional.

Der Begriff der „Verpflichtung“ ist unter dem Aspekt der Multibankfähigkeit als dringende Empfehlung zu verstehen, ohne deren Einhaltung eine DK-weit einheitliche Verwendung von FinTS nicht möglich ist. Dies bedeutet, dass ein Institut bzw. ein Kundensystem eine der folgenden Kombinationen unterstützen sollte, um einen multibankfähigen FinTS-Einsatz zu ermöglichen:

	Kundensystem	Kreditinstitut
Kommunikationsart:	synchron	synchron
Transportprotokoll:	HTTPS	HTTPS
Sicherheitsverfahren:	HBCI-RAH-7 / RAH-9 und PIN/TAN	HBCI-RAH-7 und / oder PIN/TAN

Tabelle 2: Empfehlungen für Transport- und Sicherheitsverfahren



Für Kundenprodukte wird dringend empfohlen, aus Gründen der Multibankfähigkeit, die Sicherheitsverfahren HBCI RAH-7, RAH-9 und PIN/TAN parallel zu unterstützen.

Kommunikationsart

Die synchrone Kommunikation muss aus den o. g. Gründen von jedem Institut verpflichtend unterstützt werden. Die asynchrone Kommunikation ist optional.

Kapitel: VI	Version: 4.1 FV	Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen
Seite: 128	Stand: 06.10.2017	Kapitel: Transportmedienspezifische Festlegungen Abschnitt: Zulässige Kombinationen von Kommunikationsart,

Transportprotokolle

Die zulässigen Transportprotokolle für den synchronen Fall sind HTTP und HTTPS wie in den vorangegangenen Kapiteln beschrieben. Hiervon ist HTTPS für beide Seiten verpflichtend. Die übrigen Protokolle sind optional.

Soll asynchrone Kommunikation unterstützt werden, so ist momentan SMTP das hierfür zulässige Transportprotokoll und damit verpflichtend bei Unterstützung von asynchroner Kommunikation.

In Kombination mit den unterschiedlichen Sicherheitsverfahren, die in FinTS zulässig sind, sind nicht alle Transportprotokolle sinnvoll einsetzbar. So sind Verfahren ohne Verschlüsselung (wie das PIN/TAN-Verfahren) nur über HTTPS sinnvoll einsetzbar, da nur hier eine Transportverschlüsselung verwendet werden kann, die die fehlende Verschlüsselung ersetzt. Über alle übrigen Transportkanäle wäre die Vertraulichkeit der Nachrichten nicht sichergestellt.

Auch würde die Kombination RAH-7 bzw. RAH-9 über HTTPS eine doppelte Verschlüsselung bedeuten. Empfohlen wird hier, entweder die Kombination „RAH-7 bzw. RAH-9 über HTTP“ oder die Kombination „RAH-7 bzw. RAH-9 über HTTPS ohne FinTS-Verschlüsselung“ zu unterstützen.

Sicherheitsverfahren

Von den zulässigen HBCI-Sicherheitsverfahren ist RDH-7 für beide Seiten verpflichtend. Die übrigen Verfahren sind optional.

Neben HBCI-RDH-7 bzw. RAH-9 kann zusätzlich oder ggf. auch alternativ das Sicherheitsverfahren PIN/TAN angeboten werden (vgl. Tabelle 2).

Die obigen Angaben sind in *Abbildung 41: Kommunikationsart, Transportprotokoll und Sicherheitsverfahren* noch einmal grafisch dargestellt.

Sicherheitsprofil	Kommunikationsverfahren	synchron		asynchron
		HTTP	HTTPS	SMTP
RAH-7		X	X	X
RAH-9		X	X	X
RAH-10		X	X	X
PIN/TAN		-	X	-

X anwendbar
 -- nicht anwendbar
 X anwendbar, ggf. ohne FinTS-Verschlüsselung

Abbildung 41: Kommunikationsart, Transportprotokoll und Sicherheitsverfahren

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: VII
Kapitel: FinTS-Versionsverwaltung Abschnitt: Allgemeines	Stand: 06.10.2017	Seite: 129

VII. FINTS-VERSIONSWERWALTUNG

Vor der Einführung von FinTS4 wurde die Konsistenz der administrativen Segmente durch die FinTS-Version hergestellt. So waren z. B. bei FinTS V3.0 die Protokollstrukturen aufeinander abgestimmt, was aber auch zur Folge hatte, dass bei jeder Änderung eines administrativen Segmentes eine neue FinTS-Version hätte erstellt werden müssen. Dieser Aufwand wurde mit den Sondersegmenten wie HKTAN, HKAZS oder HKSPA umgangen.

VII.1 Allgemeines

Mit FinTS V4.1 wird ein Versionskonzept auf Basis von XML Namespaces eingeführt, dass es zukünftig einfacher machen soll, notwendige Änderungen an administrativen Segmenten durchzuführen, wie die folgende Abbildung zeigen soll:

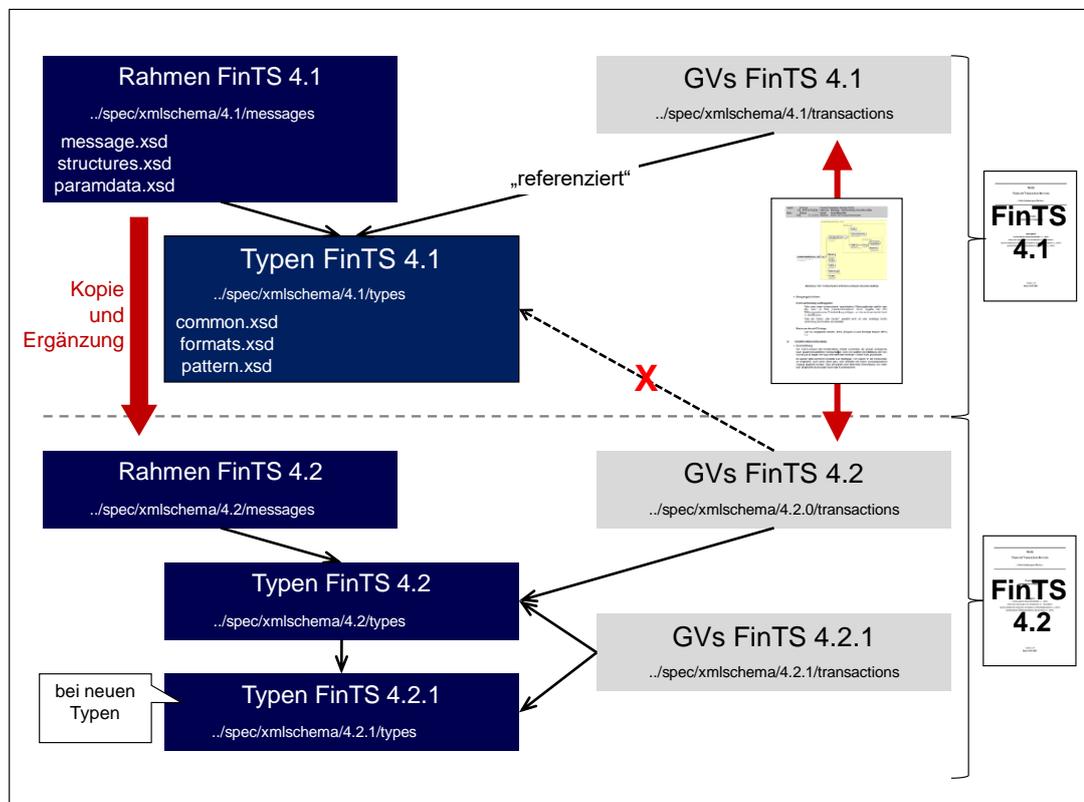


Abbildung 42: Zusammenhang der Namespaces bei FinTS4

Grundlage einer FinTS-Version bilden die Spezifikationsdokumente einer Hauptversion z. B. 4.1, der entsprechende XML-Namespace zugeordnet sind. Eine Hauptversion beinhaltet also die verschiedenen Bände der Spezifikation in einem konsistenten Stand und die Namespace-Verzeichnisse *messages*, *types*, *admintransactions* und *transactions*. Bei Hauptversionen wird der Suffix 0 weggelassen, so dass dann resultierend z. B. *FinTS V4.1* entsteht.

Wie bei allen FinTS-Versionen sind die Geschäftsvorfälle hierbei unabhängig von den *messages* und *types* zu sehen. So können die Nachrichtenstrukturen in *messages* ohne weiteres geändert und in eine neue Version überführt werden (z. B. 4.1 nach 4.2), ohne dass die Geschäftsvorfälle angepasst werden müssen (außer den Bezügen zum neuen Namespace 4.2).

Kapitel: VII	Version: 4.1 FV	Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen
Seite: 130	Stand: 06.10.2017	Kapitel: FinTS-Versionsverwaltung Abschnitt: Abruf unterstützter FinTS-Versionen

Ein neuer FinTS-Namespace entsteht dabei grundsätzlich durch Kopieren und Anpassen des bestehenden Namespace. Im neuen Namespace können dann administrative Segmente konsistent geändert werden. Handelt es sich um kleinere Änderungen wird nur die Sub-Version (z. B. 4.1 nach 4.1.1) geändert und es werden keine neuen FinTS-Spezifikationsdokumente veröffentlicht.

Ist es notwendig, die FinTS-Typen zu ändern oder zu erweitern und werden diese geänderten oder neuen Typen auch in den Geschäftsvorfällen verwendet, so müssen die Verzeichnisse *transactions* und *admintransactions* dupliziert und mit den jeweiligen Namespaces verbunden werden. Dies bedeutet dann für einen Übergangszeitraum auch eine doppelte redaktionelle Pflege der betroffenen Geschäftsvorfälle.

VII.2 Abruf unterstützter FinTS-Versionen

Um die Möglichkeit eines automatischen Versionsupdate zu schaffen, wurde mit FinTS V4.1 der neue Namespace 0.0 ausgearbeitet. Dieser stellt eine echte Untermenge des Namespace 4.1 dar und beinhaltet nur die notwendigen Syntaxelemente ohne Sicherheit und Parametrisierung für einen Versionsabgleich, wie die folgende Abbildung zeigt:

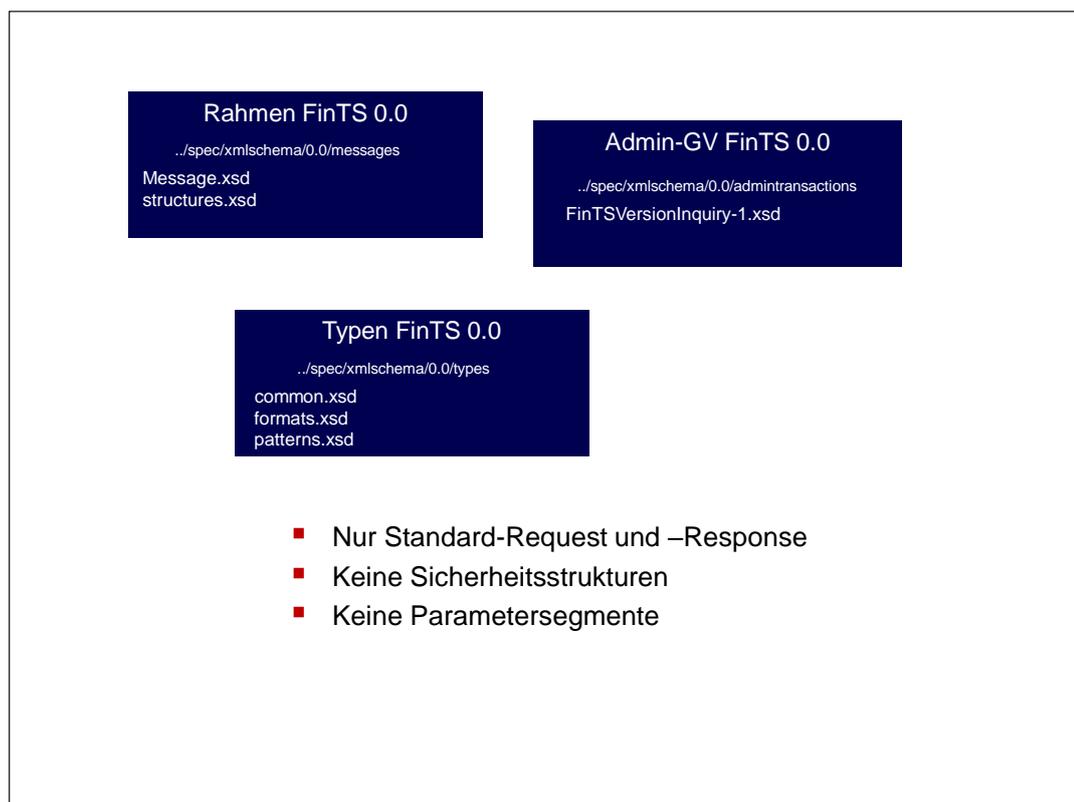


Abbildung 43: Der Aufbau des FinTS-Namespaces 0.0

Die Grundidee besteht darin, diesen Namespace über alle Versionen bzgl. seiner Protokollstrukturen hinweg unverändert zu lassen. Ausnahme bildet der administrative Geschäftsvorfall *FinTS-Versionsabfrage* (*FinTSVersionInquiry-1.xsd*), dessen Aufbau sich theoretisch ändern könnte, was jedoch ebenfalls nicht geplant ist.

Ein Kundenprodukt kann nun im Rahmen eines anonymen Dialogs eine FinTS-Versionsabfrage durchführen. Im Benutzerauftrag wird die höchstmögliche durch das Kundenprodukt unterstützte FinTS-Version eingestellt.

Financial Transaction Services (FinTS) Dokument: Formals - Grundsätzliche Festlegungen	Version: 4.1 FV	Kapitel: VII
Kapitel: FinTS-Versionsverwaltung Abschnitt: Aktuell unterstützte Namespaces	Stand: 06.10.2017	Seite: 131

Der Kreditinstitutsantwort können folgende Informationen entnommen werden:

- Alle vom Kreditinstitut unterstützten FinTS-Versionen
- Priorisierung der unterstützten FinTS-Versionen:
 - favorisiert
 - unterstützt
 - unterstützt bis <Enddatum>

Auf Basis dieser Informationen muss das Kundenprodukt die eigentliche Verarbeitung mit der höchsten vom Kreditinstitut favorisierten Version durchführen.

VII.3 Aktuell unterstützte Namespaces

Die durch die jeweilige FinTS-Dokumentversion z. B. 4.1 unterstützten Namespaces sind im FinTS Hauptdokument [Master] beschrieben.
