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

Die Deutsche Kreditwirtschaft

FinTS

Financial Transaction Services

Schnittstellenspezifikation

Security
Sicherheitsverfahren PIN/TAN
(inklusive Zwei-Schritt-Verfahren)

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

Version: 4.1 FV Stand: 06.10.2017 Final Version

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

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	Organisation	Datum	Version	Dokumente	Anmerkungen
	SIZ	22.06.2004	4.0	FinTS_4.0_Security_PINTAN.doc	Überarbeitungen
Haubner	für SIZ	20.01.2014	4.1 Final Version	FinTS_4.1_Security_PINTAN_2014-01-20-FV.doc	
Haubner	für SIZ	06.10.2017	4.1 Final Version	FinTS_4.1_Security_PINTAN_2017-10-06_final_version.docx	Ergänzen der starken Kundenauthentifizierung gemäß PSD2

Änderungen gegenüber der Vorversion:

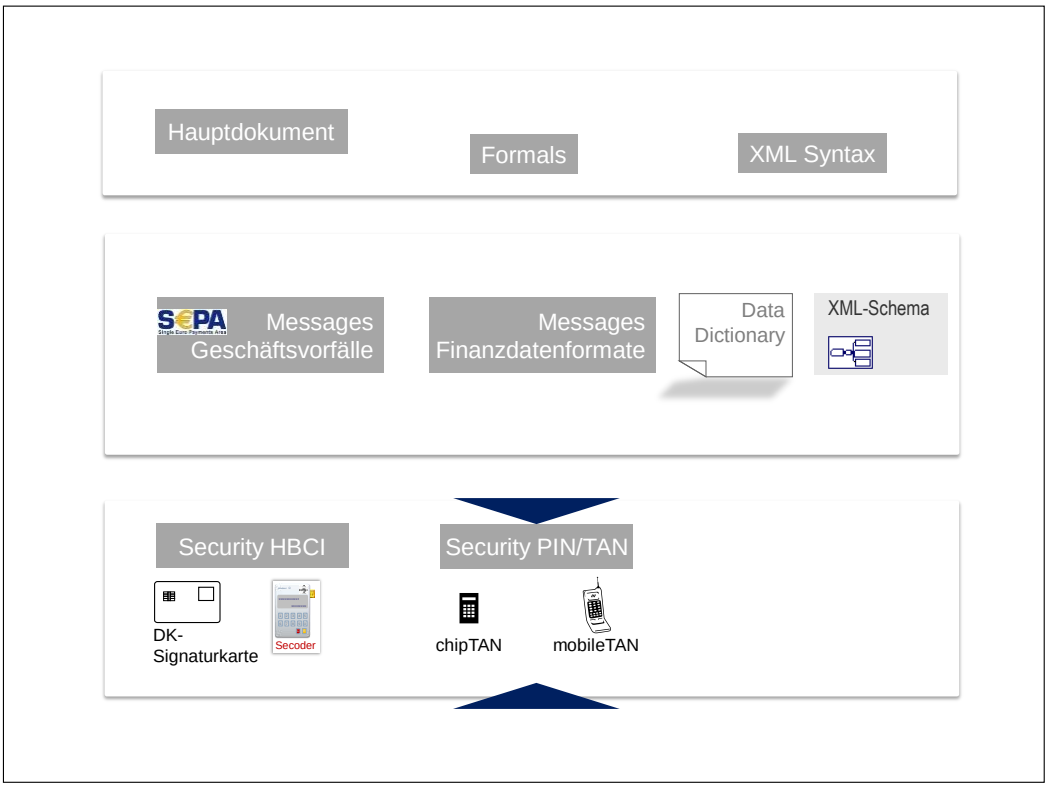
Änderungen sind im Dokument durch einen Randbalken markiert. Falls sich die Kapitelnummerierung geändert hat, bezieht sich die Kapitelangabe auf die neue Nummerierung.

Releasedatum 06.10.2017

lfd. Nr.	Kapitel	Kapitelnummer	Kennung	Art	Beschreibung
1	Management TAN-Medien	II.10.2	0475	E	Erweiterungen bei den folgenden GVs für bilateral vereinbarte Sicherheitsverfahren im Element „TAN-Medium-Klasse“: - DisplayTanGeneratorList-5 - ChangeTANGenerator-3 - RegisterMobilePhoneConnection-3 - ActivateMobilePhoneConnection-3 - ChangeMobilePhoneConnection-3 - DeactivateDeleteTANMedium-2
2	Starke Authentifizierung	II.3, II.4.2 und diverse Anpassungen	0480	E	Abläufe und Rahmenbedingungen zur starken Authentifizierung gemäß PSD2.
3	Diverse			Ä	Entfernen von SSL aus der Spezifikation und Ersetzen durch TLS

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].

Inhaltsverzeichnis

Abbildungsverzeichnis

I. EINLEITUNG

In dieser Spezifikation wird ein multibankfähiges Protokoll für das Sicherheitsverfahren PIN/TAN beschrieben. Dieses Sicherheitsverfahren kann in multibankfähigen Online-Banking-Verfahren der deutschen Kreditwirtschaft eingesetzt werden. Informationen bzgl. Nachrichtenaufbau und Kommunikationsablauf sind dem Dokument [Formals] zu entnehmen.

Um ein möglichst hohes Maß an Synergie nutzen zu können, wird für die Kommunikation zwischen Kundenprodukt und Kreditinstitut weitestgehend auf der FinTS-Spezifikation in der Version 4.1 aufgesetzt, insbesondere bzgl. Syntax, Datenformaten und Abläufen. Sofern nicht anders vermerkt gelten für den Nachrichtenaufbau, Kommunikationsablauf etc. die dort getroffenen Regelungen. Dieses Dokument beschreibt daher nur die für das PIN/TAN-Verfahren abweichenden Festlegungen.

Während HBCI seine Stärken derzeit insbesondere in der hohen Sicherheit hat, ist als Vorteil des PIN/TAN-Verfahrens beispielsweise die höhere Mobilität zu sehen. Dies bedeutet, der Benutzer kann Online-Banking ohne angeschlossenen Chipkartenleser und die dafür ggf. notwendige Treiberinstallation betreiben. PIN/TAN ist somit eine gute Lösung für die mobile Anwendung mit Smartphone, Tablet oder Laptop, während HBCI für die umfassende Kontenverwaltung mit einem Offline-Kundenprodukt in Frage kommt.

Die Kreditinstitute unterstützen daher oft beide Verfahren parallel. Dies führt dazu, dass der Benutzer zwar aus mehreren Alternativen das für ihn bestgeeignete Verfahren auswählen kann.

Ob ein Kreditinstitut PIN/TAN-Verfahren anbietet, erkennt das Kundenprodukt am Vorhandensein des Segments Parameterdaten PIN/TAN bzw. des Kommunikationsdienstes HTTPS in den Bankparameterdaten (siehe [Formals], Abschnitt *IV.2.3 Sicherheitsverfahren*).

Grundsätzlich können mit dem Sicherheitsverfahren PIN/TAN alle im Dokument [Messages] aufgeführten Geschäftsvorfälle verwendet werden. Dies gilt auch für verbandsindividuelle Erweiterungen. Welche Geschäftsvorfälle konkret zulässig sind, teilt das Kreditinstitut im Segment Parameterdaten PIN/TAN (siehe *II.7 Bankparameterdaten zum PIN/TAN-Verfahren*) mit.

Da bei PIN/TAN-Verfahren aufgrund der nicht vorhandenen kryptographischen Verfahren auf Protokollebene keine Verschlüsselung zum Einsatz kommen kann, wird ausschließlich https (TLS) auf Transportebene verwendet. Eine Verschlüsselung auf FinTS-Protokollebene entfällt komplett. Die Lösung verbindet damit die Sicherheit eines Einmalpassworts (TAN) mit der auch bei TLS eingesetzten Transportverschlüsselung.

Das Sicherheitsverfahren PIN/TAN tritt in FinTS bezüglich der Einreichung von TAN-pflichtigen Geschäftsvorfällen in zwei unterschiedlichen Ausprägungen auf, die sich vom Prozessablauf her unterscheiden:

Ein-Schritt-TAN-Verfahren

Beim Ein-Schritt-TAN-Verfahren wird der Geschäftsvorfall in einem Prozess-Schritt zusammen mit der TAN eingereicht, d. h. in einem Dialogschritt bestehend aus Auftrag und Antwort wird ein TAN-pflichtiger Geschäftsvorfall komplett abgewickelt. Diese Verfahrensweise entspricht dem Vorgehen bei signaturbasierten Verfahren

und war bis zur Einführung des Zwei-Schritt-Verfahrens die einzige Möglichkeit, TAN-pflichtige Aufträge über das FinTS-Protokoll einzureichen.
Mit dem Ein-Schritt-Verfahren kann keine starke Kundenauthentifizierung (vgl. [PSD2]) durchgeführt werden. Es wird jedoch benötigt, um PIN/TAN-Management-Geschäftsvorfälle wie z. B. eine initiale PIN-Änderung durchführen zu können.

Zwei-Schritt-TAN-Verfahren

Beim Zwei-Schritt-Verfahren werden die Auftragseinreichung und die TAN-Übermittlung in zwei Teilschritte zerlegt. Dadurch hat das Kreditinstitut auch die Möglichkeit, als Antwort auf die erste Nachricht eine so genannte „Challenge“ zu übermitteln, aus der der Kunde dann die zu verwendende TAN herleiten muss. Dadurch wird auch eine logische Bindung (auch als „Dynamic Linking“ bezeichnet) der TAN an den Auftrag erreicht. Ein Zwei-Schritt-Verfahren ist die Voraussetzung für die Durchführung einer starken Kundenauthentifizierung (vgl. [PSD2]).

Zwei-Schritt-TAN-Verfahren werden in FinTS wie verteilte Signaturen behandelt (*vgl. [Formals], Abschnitt III.7 Verteilte Signaturen*). So dienen die folgenden Geschäftsvorfälle als Grundlage:

- *Einreichen eines Auftrags zur verteilten Signatur*
  gemäß *[Formals], Abschnitt III.7.1*
- *Verteilte Signatur leisten*
  gemäß *[Formals], Abschnitt III.7.3*
- Im Bedarfsfall bei Mehrfach-TANs: *Details zu eingereichten Aufträgen anfordern*
  gemäß *[Formals], Abschnitt III.7.2*

Das Zwei-Schritt-Verfahren in FinTS beschreibt ausschließlich die Protokollabläufe und dient als abstrakte Beschreibung, die in konkreten Ausprägungen wie chipTAN oder mobileTAN verwendet werden kann. Die konkreten Ausprägungen selbst sind nicht Bestandteil dieser Spezifikation.

II. VERFAHRENSBESCHREIBUNG

II.1 Allgemeines

Es gelten die in [Formals] aufgeführten Formate und Belegungsrichtlinien.

Ergänzend hierzu gilt:

- PIN und TAN werden in die DEG PIN/TAN-Signatur eingestellt. Diese ersetzt die bei HBCI-Sicherheitsverfahren einzustellenden Signaturen nach XML-Signature-Standard.
- Für die Rückmeldungen wurden neue Codes definiert (siehe *II.5 Erweiterung der Rückmeldungscodes*)
- Die Einreichung von Benutzerschlüsseln, die Anforderung von Kreditinstitutsschlüsseln sowie Schlüsselsperr- und Schlüsseländerungsnachrichten ist verboten.
- Die Bankparameterdaten enthalten ein Parametersegment, welches die PIN/TAN-spezifischen Informationen des Kreditinstituts enthält.
- Die für den Benutzer zugelassenen Geschäftsvorfälle für das PIN/TAN-Management sind ihm über dessen UPD mitzuteilen.
- Diejenigen FinTS-Benutzer, die das PIN/TAN-Verfahren verwenden, können nicht auf FinTS-Protokollebene verschlüsseln. Es ist allein eine https (TLS)-Transportverschlüsselung möglich. Für den Boten einer Nachricht bedeutet dies, dass seine Botenverschlüsselung durch eine TLS-Transportverschlüsselung ersetzt werden kann. Für den Herausgeber eines Auftragsteils bedeutet dies jedoch, dass eine gesonderte Verschlüsselung des Auftragsteiles bei Verwendung des PIN/TAN-Verfahrens nicht möglich ist. Komprimierung ist jedoch auf beiden Ebenen möglich.
- Als Kommunikationsdienst ist HTTPS laut den Vorgaben des `CommSettings_Reply`-Segmentes aus den BPD zu verwenden (siehe [FORMALS], Abschnitt *IV. BANKPARAMETERDATEN (BPD)*).
- Das in diesem Dokument beschriebene Verfahren wird auf Syntaxebene als „PIN/TAN-Verfahren, Variante 1.1“ bezeichnet. Zukünftige andere Parametrisierungen oder Modifikationen des Verfahrens müssen eine andere eindeutige Variantenbezeichnung erhalten, um die Multibankfähigkeit der Produkte zu gewährleisten.

Für den Einsatz von Zwei-Schritt-TAN-Verfahren gelten zusätzlich die folgenden allgemeinen Festlegungen:

- 1 bis 98 unterschiedliche Zwei-Schritt-Verfahren pro Kreditinstitut
- Zur eindeutigen Bezeichnung eines Zwei-Schritt-TAN-Verfahrens wird das Element „Sicherheitsfunktion, kodiert“ verwendet:
  999: nur also Kodierung zum Abruf unterstützter Verfahren;
  900 … 997: Zwei-Schritt-TAN-Verfahren
  Die Verknüpfung von Code und Verfahren ist institutsspezifisch und wird i. A. in der BPD festgelegt (vgl. hierzu die Ausführungen zu Bankparameterdaten in [Formals] und [Syntax]).

- Alle unterstützten TAN-Verfahren (das Ein-Schritt-TAN-Verfahren und bis zu 98 in der BPD definierte konkrete Zwei-Schritt-TAN-Verfahren) gelten als gleichberechtigte PIN/TAN-Sicherheitsverfahren, denen in den entsprechenden BPD-und UPD-Abschnitten TAN-pflichtige Geschäftsvorfälle zugeordnet werden können.

  Ein TAN-pflichtiger Auftrag muss über irgendeines aber kein spezielles der unterstützten TAN-Verfahren autorisiert werden.

- Ist das Kundenprodukt nicht im Besitz einer aktuellen UPD, kann es diese mit dem neuen Rückmeldungscode *3920* ermitteln. Dem Benutzer werden in der Initialisierungsantwort die für ihn zugelassenen Zwei-Schritt-TAN-Verfahren mitgeteilt. Als Bezug für das Rückmeldungssegment wird die XML-Struktur *ProcPreparation* verwendet.
- Der Kunde übermittelt in der XML-Struktur *OneTimePassword* der Initialisierungsnachricht, mit welchem konkreten TAN-Verfahren er den Dialog führen will. Das konkrete TAN-Verfahren darf während des Dialogs nicht gewechselt werden.
- Die beiden Teilschritte des Zwei-Schritt-Verfahrens müssen nicht zwingend in einem einzigen Dialog abgewickelt werden, außer es handelt sich um eine Dialoginitialisierung. Über die Auftragsreferenz ist eine entsprechende Verkettung über mehrere Dialoge hinweg möglich.
- Mehrfach-TANs werden im Rahmen von Verteilten Signaturen (*vgl. [Formals], Abschnitt III.7 Verteilte Signaturen*) behandelt. Daher gelten die dort defnierten Regeln.So gilt ein konkretes Zwei-Schritt-Verfahren für den gesamten Dialog des jeweiligen Benutzers. Jeder Benutzer kann ein eigenes konkretes Zwei-Schritt-Verfahren verwenden.
- Eine im Rahmen der Dialoginitialisierung für die starke Kundenauthentifizierung verwendete TAN gilt nicht für weitere in diesem Dialog eingereichte TAN-pflichtige Aufträge (dies ist keine Session-TAN).

Gemäß §7 der „Bedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN“ dürfen sowohl die PIN als auch TANs nicht elektronisch im Kundenprodukt gespeichert werden.

II.2 Zwei-Schritt-TAN-Verfahren (*ZSV*)

Alle aktuell verwendeten TAN-Verfahren verwenden eine zwei-schrittige Logik, d. h. bei TAN-pflichtigen Aufträgen erfolgt eine Aufteilung zwischen Auftragseinreichung und Authentisierung / Autorisierung in zwei Prozess-Schritte, um dem Kunden in der Antwort des ersten Schrittes eine Sicherheitsfrage, die so genannte *Challenge* mitzuteilen, die er für die Ermittlung / Erzeugung der TAN benötigt. Damit wird die TAN über einen verfahrensabhängigen Algorithmus logisch an den Auftrag gebunden („Dynamic Linking“).

In FinTS4 folgt diese Aufteilung den Prozessen zur verteilten Signatur (vgl.hierzu *Abschnitt II.1 Allgemeines* unter *Zwei-Schritt-TAN-Verfahren*), d. h. das dort definierte Sicherheitsverfahren One-Time-Password (OTP) verwendet die Protokollumschläge für verteilte Signaturen, jedoch mit fest definierten Prozessabläufen und Belegungen.

Die Anforderung und Übertragung von Challenges erfolgt über die entsprechenden Strukturen in *OneTimePassword* und *OneTimePasswordReply (RespMsg/RespMsgBody/MessengerSig/OneTimePasswordReply/TANRequest)* im Rahmen der Verarbeitung der Geschäftsvorfälle zur verteilten Signatur.

Folgende Geschäftsvorfälle zur Bildung verteilter Signaturen (*vgl. [Formals], Abschnitt III.7 Verteilte Signaturen*) werden beim Zwei-Schritt-TAN-Verfahren eingesetzt:

- *Einreichen eines Auftrags zur verteilten Signatur (DistSigsSubmit)*
  gemäß *[Formals], Abschnitt III.7.1*
  Realisierung Kreditinstitut : verpflichtend, wenn ZSV angeboten wird
  Realisierung Kundenprodukt : verpflichtend, wenn ZSV angeboten wird

  Dieser Geschäftsvorfall dient zur Einreichung eines Auftrags (ohne TAN). Zu diesem Zeitpunkt kann bereits eine keine Challenge angefordert werden (XML-Pfad: *OneTimePassword/ChallengeRequest*). Im Rahmen der Kreditinstitutsantwort (XML-Tag: *TAN-Request*) wird die ggf. angeforderte Challenge an das Kundenprodukt übertragen. Soll ein Auftrag nur eingereicht und nicht signiert werden, erfolgt zu diesem Zeitpunkt keine Challenge-Anforderung.

- *Verteilte Signatur leisten (DistSigsSign)*
  gemäß *[Formals], Abschnitt III.7.3*
  Realisierung Kreditinstitut : verpflichtend, wenn ZSV angeboten wird
  Realisierung Kundenprodukt : verpflichtend, wenn ZSV angeboten wird

  Nachdem der Benutzer gemäß seinem konkreten TAN-Verfahren die Challenge überprüft und ggf. eine TAN erzeugt hat, reicht er diese als verteilte Signatur ein. Die Einreichung der TAN kann auch zeitversetzt auf Basis der korrekten *Auftragsreferenz* (*DistSigsID*) erfolgen. Diese kann der Benutzer durch eine Detail-Abfrage ermitteln.
  Bei solchen zeitversetzten Signaturen erfolgt über diesen Geschäftsvorfall auch die Challenge-Anforderung (über die XML-Strukturen in *OneTimePassword* und *OneTimePasswordReply* s. o.).

- bei Mehrfach-TANs: *Details zu eingereichten Aufträgen anfordern (DistSigsInfo)*
  gemäß *[Formals], Abschnitt III.7.2*
  Realisierung Kreditinstitut : optional
  Realisierung Kundenprodukt : optional

  Im Fall eines Auftrages mit mehreren TANs unterschiedlicher Benutzer oder wenn Einreicher und Signierer abweichend sind, kann der Signierer / Zweit-Signierer durch diesen Geschäftsvorfall Details über den zu signierenden Auftrag anfordern, bevor er eine Signatur leistet.

- zum Löschen eines Auftrags: *Auftrag zur verteilten Signatur löschen (DistSigs-Delete)*
  gemäß *[Formals], Abschnitt III.7.4*
  Realisierung Kreditinstitut : optional
  Realisierung Kundenprodukt : optional

  Soll ein bereits eingereichter, aber noch nicht ausreichend autorisierter Auftrag gelöscht werden, so kann dies gemäß den Festlegungen zu verteilten Signaturen auf Basis der *Auftragsreferenz* (*DistSigsID*) erfolgen.

Das Zwei-Schritt-Verfahren in FinTS beschreibt ausschließlich die Protokollabläufe zur Einreichung von Aufträgen, der Anforderung und Bereitstellung von Challenges und der Übermittlung der resultierenden TAN. FinTS besitzt jedoch keine Kenntnis über die Eigenschaften des verwendeten konkreten Verfahrens.

Beispiele für solche Zwei-Schritt-TAN-Verfahren sind Lösungen der Deutschen Kreditwirtschaft wie chipTAN oder mobileTAN. Aber auch zwischen Benutzer und Kreditinstitut bilateral vereinbarte Verfahren können über den FinTS-Kanal kommunizieren.

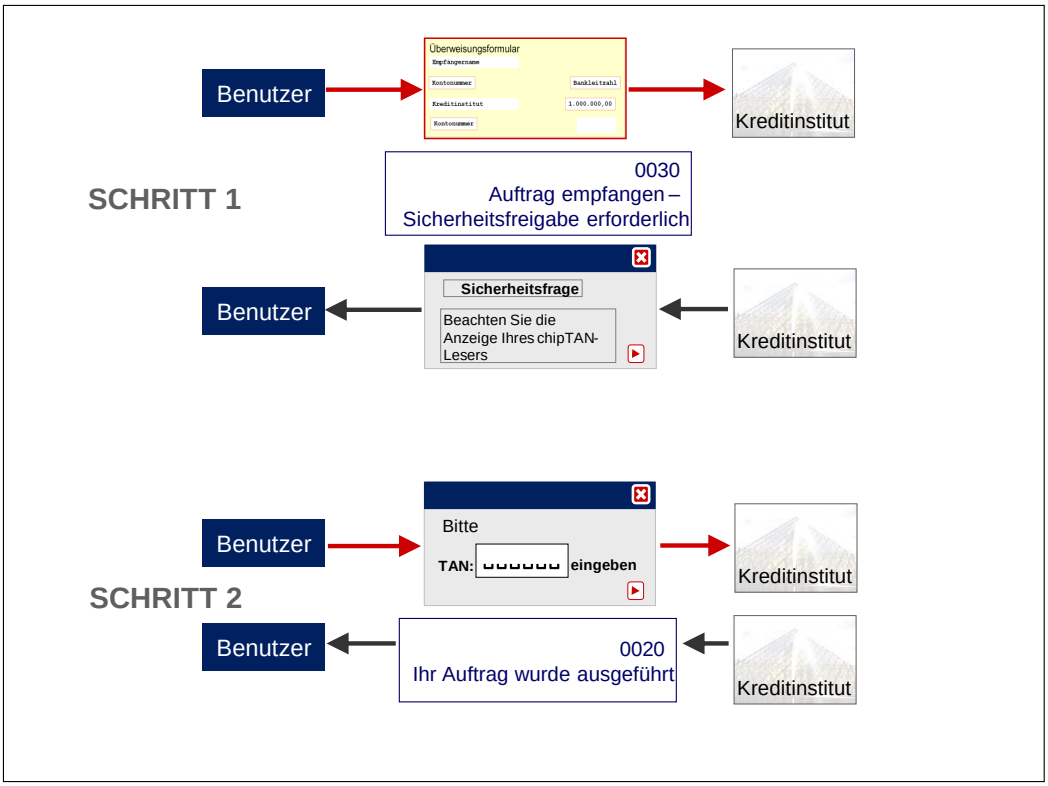


Abbildung 1: Benutzer-Interaktion beim Zwei-Schritt-Verfahren

Mit dem FinTS Zwei-Schritt-TAN-Verfahren wird keines dieser genannten Verfahren konkret spezifiziert – es erfolgt nur eine abstrakte Definition des Ablaufs, der über Parameter gesteuert wird. Der Ablauf selbst ist für alle Zwei-Schritt-Verfahren identisch. Die Parametrisierung eines konkreten Zwei-Schritt-Verfahrens erfolgt über die Parametrisierung in der BPD unter *Parameterdaten PIN/TAN*. Hierdurch ist die abstrakte Beschreibung von maximal 98 konkreten Zwei-Schritt-Verfahren in der BPD möglich, die über das Datenelement „Sicherheitsfunktion, kodiert“ referenziert werden.

Einem Benutzer können über die UPD seine für ihn zugelassenen konkreten Zwei-Schritt-Verfahren zugeordnet werden. Bei der Verwendung von Mehrfach-TANs kann jeder beteiligte Benutzer ein eigenes konkretes Zwei-Schritt-Verfahren ver-

wenden – die Verfahren können also innerhalb einer Nachricht unterschiedlich sein[1].

Die beiden folgenden Abbildungen zeigen Anwendungsbeispiele für die Parameterdaten PIN/TAN.

Sicherheitsfunktion kodiert (individuell)	995	996	950
Technische Identifikation TAN-Verfahren	„chipTAN“	„mobileTAN“	„individTAN“
ZKA-TAN-Verfahren	„HHDOPT1“	„mobileTAN“	
Version des ZKA-TAN-Verfahrens	„1.4“		
Name TAN-Verfahren	„smartTAN-optic“	„smsTAN“	„individTAN“
Länge TAN-Eingabe	6	6	20
Format TAN-Eingabe	2	2	1
Text Challenge	„Bitte beachten Sie die Anzeige Ihres chipTAN-Lesers“	„Bitte prüfen Sie die Angaben in der SMS“	„Kontroll-begriff“
Länge Challenge	..2048	..2048	32

1: num 2: an

Abbildung 2: Anwendungsbeispiele für die Parametrisierung im ZSV

Das Präsentationsbeispiel in Abbildung 3 soll zeigen, wie auf Basis der übermittelten Parameter eine Gestaltung eines konkreten Zwei-Schritt-Verfahrens aussehen kann.

[1] Da es im aktuellen Dialog nur einen Dialogführer geben kann, müssen die zulässigen konkreten Zwei-Schritt-Verfahren der weiteren Benutzer bereits vorab über separate Dialoge (und entsprechende UPD-Informationen) festgelegt worden sein.

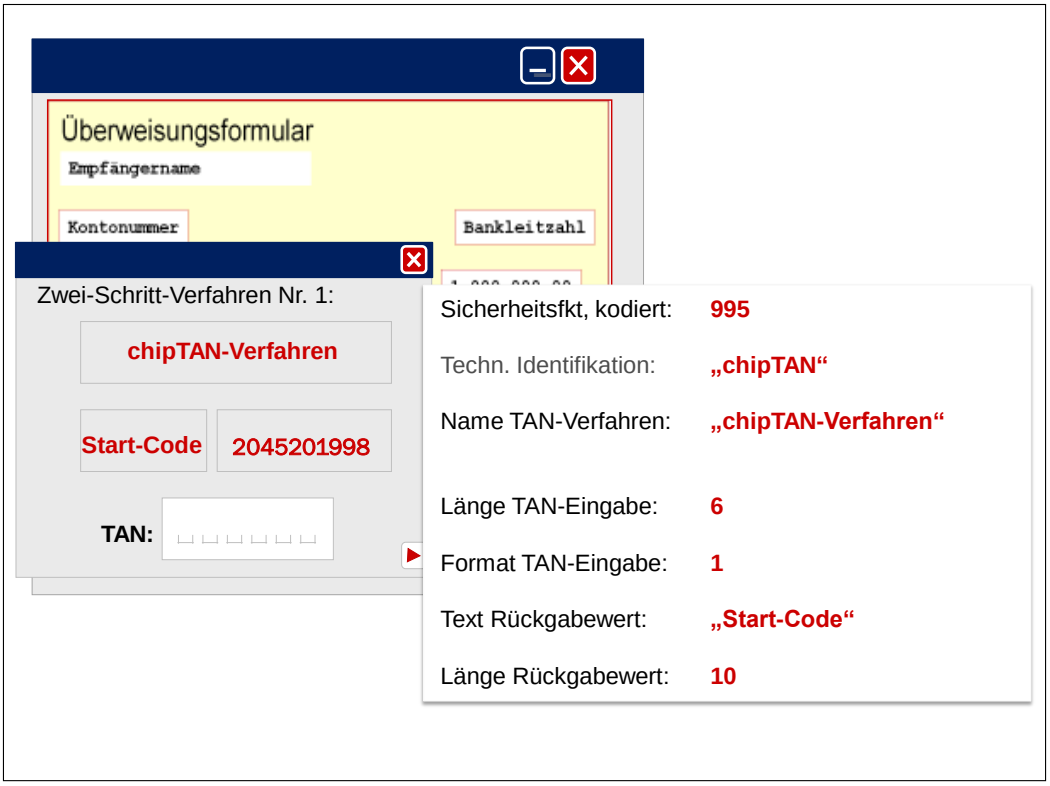


Abbildung 3: Präsentationsbeispiel für ein konkretes Zwei-Schritt-Verfahren

II.2.1 Analogien zu älteren FinTS-Versionen

Zwei-Schritt-TAN-Verfahren wurden bereits mit der HBCI V2.2 Erweiterung eingeführt. Zur Übertragung der Challengeinformationen wurde der administrative Hilfs-Geschäftsvorfall HKTAN verwendet. Bzgl. des Funktionsumfangs lassen sich mit FinTS4 folgende Analogien herstellen:

- Administrativer Hilfs-Geschäftsvorfall HKTAN
  Der Geschäftsvorfall wird ersatzlos gestrichen. Parametrisierung und Transport geschieht über BPD und UPD sowie die Geschäftsvorfälle der verteilten Signatur
- TAN Prozessvarianten 1 und 2
  Es erfolgt keine Unterscheidung nach Prozessvarianten. FinTS4 arbeitet analog Prozessvariante 2.
- Mehrfach-TANs und Dialogbezug
  Die FinTS4-Funktion der verteilten Signatur unterstützt die Einreichung im gleichen Dialog oder zeitversetzt ohne Einschränkungen.
- Details zu Aufträgen
  Geschäftsvorfall *Details zu eingereichten Aufträgen anfordern (DistSigsInfo)*, keine Entsprechung bei FinTS V3.0
- Stornieren von Aufträgen
  Das Stornieren von Aufträgen mittels HKTAN-Option wird durch die Verwendung des Geschäftsvorfalls *Löschen eines Auftrags zur verteilten Signatur (DistSigs-Delete)* ersetzt.
- Auftrags-ID (XML-Tag: *DistSigsID*) entspricht der Auftragsreferenz in FinTS V3.0.

- TAN-Listenverarbeitung wird ab FinTS V4.1 nicht mehr unterstützt.

II.3 Starke Kundenauthentifizierung

Durch [MaSI] und [PSD2] besteht die Forderung nach einer starken Kundenauthentifizierung (Strong Customer Authentication – SCA) bei Zugriff auf Kontodaten (Dialoginitialisierung) und Geschäftsvorfällen, die aufgrund ihres Missbrauchsrisikos entsprechend geschützt werden müssen (TAN-pflichtige Geschäftsvorfälle).

Zusätzlich enthält [PSD2] aber auch Ausnahmen von dieser starken Kundenauthentifizierung, d. h. unter bestimmten Rahmenbedingungen einen Verzicht auf die starke Kundenauthentifizierung, was ebenfalls durch entsprechende FinTS-Prozesse abzubilden ist. Da die Prüfung auf diese SCA-Ausnahmen zur Laufzeit erfolgen muss, wird die Entscheidung, ob eine TAN erforderlich ist dynamisch gefällt.Während die Rahmenbedingungen zur Durchführung einer starken Kundenauthentifizierung im Rahmen der Dialoginitialisierung in Abschnitt II.4.2.2 vollständig beschrieben sind, folgen an dieser Stelle noch einige allgemeine Festlegungen zu den Geschäftsvorfällen.

Da sich die PSD2-Vorgaben nur auf den Zahlungsverkehr beziehen, gibt es in FinTS weiterhin Geschäftsvorfälle, bei denen abhängig von der Deklaration im Parametersegment *Festlegung OTP-pflichtiger Geschäftsvorfälle für alle OTP-Verfahren* in keinem Fall oder immer eine TAN verwendet werden muss.

Durch die Einführung der Ausnahmen zur TAN-Pflicht ergeben sich für die FinTS-Verarbeitung vier unterschiedliche Authentifizierungsklassen, die auch Auswirkungen auf die Listung der Geschäftsvorfälle im Parametersegment *Festlegung OTP-pflichtiger Geschäftsvorfälle für alle OTP-Verfahren* haben:

Auth-Klasse	Beschreibung	TAN erforderlich
1	Nicht-Zahlungsverkehrs-Geschäftsvorfälle, für die grundsätzlich keine TAN erforderlich ist. Dies betrifft z. B. den Bereich Wertpapier.	N
2	Zahlungsverkehrs-Geschäftsvorfälle, für die im Rahmen der PSD2 die starke Kundenauthentifizierung inkl. ihrer Ausnahmen gilt. Diese sind zwar grundsätzlich als TAN-pflichtig definiert, die Notwendigkeit einer TAN-Eingabe wird jedoch erst zum Ausführungszeitpunkt durch das Kreditinstitut festgelegt. Dabei kann dann die statische Definition im Parametersegment dergestalt übersteuert werden, dass für einen als TAN-pflichtig gekennzeichneten Geschäftsvorfall aufgrund einer SCA Ausnahme doch keine TAN benötigt wird.	J
3	Nicht-Zahlungsverkehrs-Geschäftsvorfälle, für die grundsätzlich eine TAN erforderlich ist. Dies betrifft z. B. den Bereich Wertpapier.	J
4	PIN/TAN-Management-Geschäftsvorfälle, für die situationsbedingt eine starke Kundenauthentifizierung bis zum Abschluss des gesamten Prozesses ausgesetzt werden kann, z. B. im Rahmen einer initialen PIN-Änderung.	J

Die Authentifizierungsklassen 1 und 3 entsprechen den heutigen statischen TAN-Festlegungen auf Basis der Definitionen im Parametersegment *Festlegung OTP-pflichtiger Geschäftsvorfälle für alle OTP-Verfahren.*

Bei der Durchführung von Geschäftsvorfällen der Authentifizierungsklasse 2 – hierzu gehört auch die Dialoginitialisierung – fällt die Entscheidung, ob eine TAN erforderlich ist, erst nach dem Einreichen der Kundennachricht. Diese wird bei Authentifizierungsklasse 2 grundsätzlich durch Belegen des Elements *Starke Kundenauthentifizierung angefordert* mit *J* signalisiert. Institutsseitig wird nun gegen die in [PSD2] definierten Ausnahmen geprüft, wodurch zwei Möglichkeiten für die weitere Verarbeitung entstehen:

1. Fortführen des Zwei-Schritt-TAN-Verfahrens. Dies wird vom Kreditinstitut durch den Rückmeldungscode *0030 Auftrag empfangen - Sicherheitsfreigabe erforderlich* signalisiert.
2. Keine starke Kundenauthentifizierung erforderlich. Dies wird durch den Rückmeldungscode *3076 Keine starke Authentifizierung erforderlich* angezeigt, zusätzlich zu fachlichen Rückmeldungen zum eingereichten Auftrag wie z. B. *0010 Auftrag entgegengenommen*.

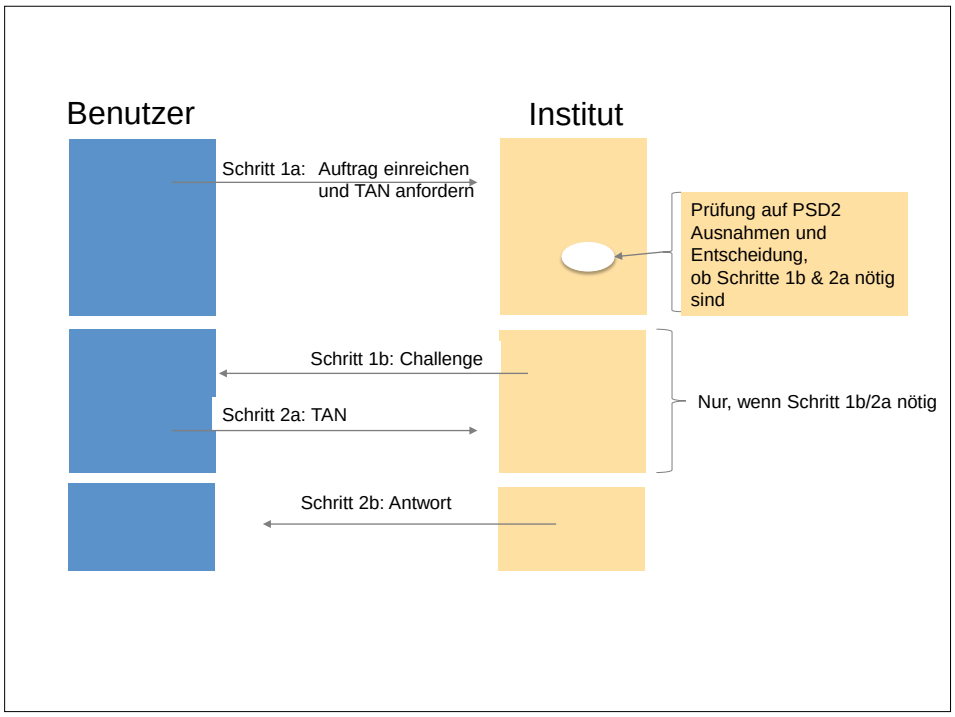


Abbildung 4: Wirkung der PSD2 Ausnahmen auf den Ablauf

Wird vom Kreditinstitut das Element *Starke Kundenauthentifizierung erforderlich* mit *J* belegt, muss ein Kundensystem auf diese beiden Möglickeiten der Auftragseinreichung entsprechend reagieren können.

Details zu den genauen Abläufen sind in Kapitel II.4.2.2 für die Initialisierung beschrieben. Das Verhalten beim Einreichen von Zahlungsverkehrsaufträgen ist bzgl. der Ausnahmen analog dazu zu sehen.

II.4 Abläufe beim Zwei-Schritt-TAN-Verfahren

Die Wirkungsweise des Zwei-Schritt-TAN-Verfahrens wird im Folgenden an zwei repräsentativen Abläufen gezeigt:

Ablauf 1: Auftragseinreichung durch einen Benutzer mit einer TAN

Ablauf 2: Auftragseinreichung durch zwei Benutzer mit je einer TAN in zwei Dialogen

Hinzu kommt folgender Ablauf für die Initialisierung mit starker Authentifizierung:

Ablauf 3: Initialisierung mit starker Authentifizierung

Diese konkreten Abläufe sind bezogen auf die einzelnen Prozessschritte exakt in der beschriebenen Form umzusetzen; die Bildung von anderen Derivaten ist nicht zugelassen. Zusätzlich mögliche Abläufe zur Abfrage von Details zum Auftrag werden nach den Regeln der FinTS verteilten Signatur behandelt.

In einem Dialog ist es grundsätzlich möglich aber nicht verpflichtend, dass mehrere in sich abgeschlossene Abläufe hintereinander durchgeführt werden. Es gelten hierbei als Rahmenbedingungen die für den gesamten Dialog getroffenen Festlegungen, z. B., dass das Sicherheitsverfahren nicht gewechselt werden darf.

Bei den im Folgenden beschriebenen Abläufen wird davon ausgegangen, dass sich nur ein TAN-pflichtiger Auftrag in der Nachricht befindet. In FinTS4 können jedoch auch beliebige Auftragslisten und / oder Aufträge verarbeitet werden.

Bei der Verwendung von Mehrfach-TANs sind Aufträge, bei denen mindestens eine TAN fehlerhaft ist, kreditinstitutsseitig zu verwerfen. Dies gilt unabhängig vom verwendeten Ein- oder Zwei-Schritt-Verfahren. Ferner gelten bei Mehrfach-TANs keine Ausnahmen zur starken Kundenauthentifizierung, d. h. jeder Benutzer muss den jeweiligen Auftrag mit einer TAN authentifizieren.

Um einen TAN-pflichtigen Auftrag im Zwei-Schritt-Verfahren einzureichen, müssen die im Folgenden beschriebenen Schritte durchgeführt werden. Dabei gilt bei einer TAN die grundlegende Abfolge der Segmente am Beispiel einer SEPA-Einzelüberweisung:

Schritt 1: SEPASingRemitt_1_Req und Umschlag für die Einreichung eines Auftrags mit verteilter Signatur

Schritt 2: Umschlag zur Einreichung der Signatur (=TAN) und Rückmeldungen zu SEPASingRemitt_1_Req

II.4.1.1 Auftragseinreichung durch einen Benutzer mit einer TAN

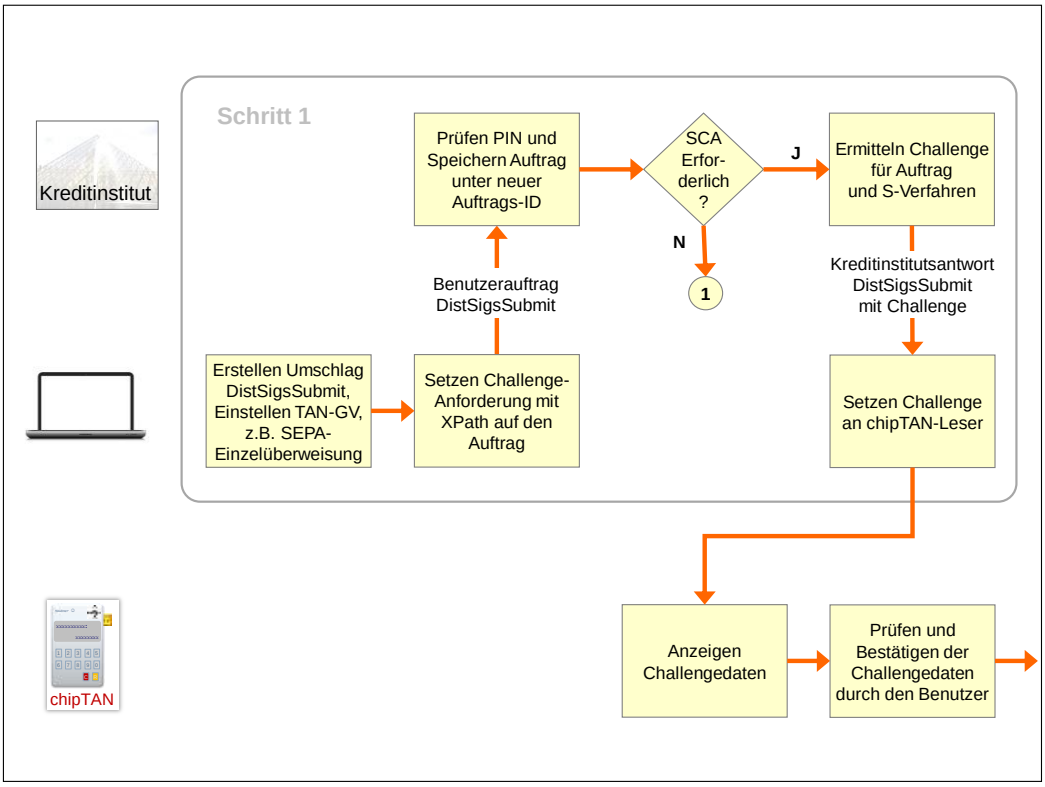


Abbildung 5: Auftragseinreichung durch einen Benutzer mit einer TAN (1 von 2)

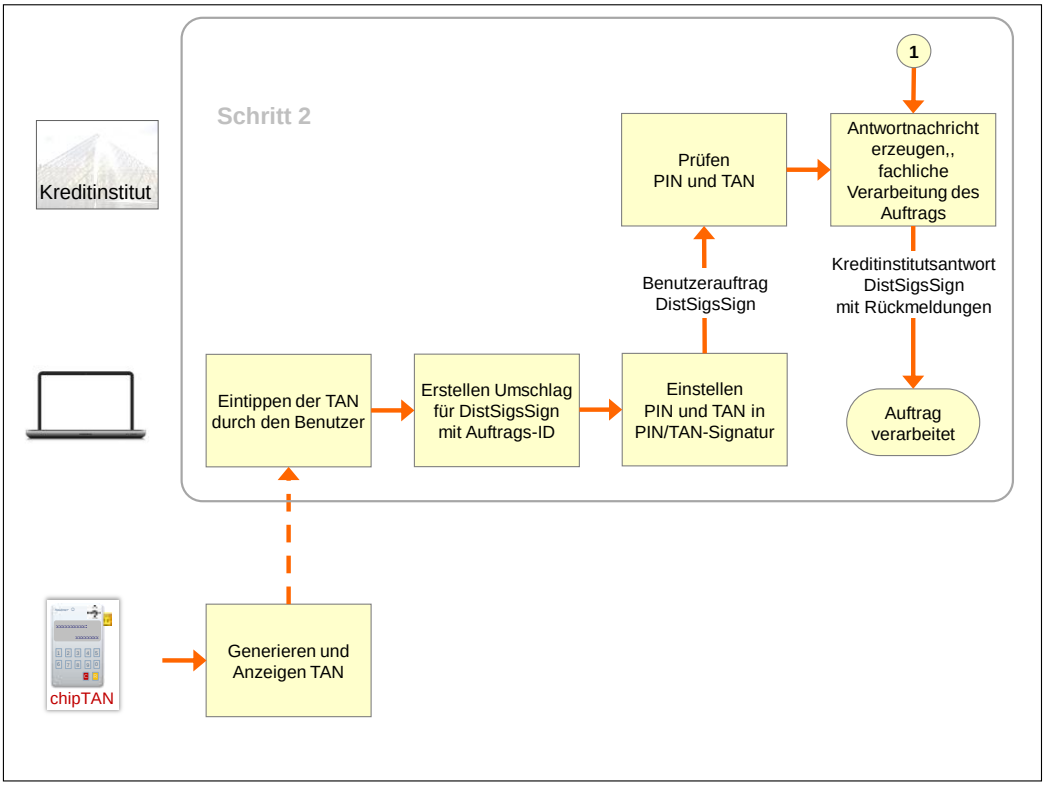


Abbildung 6: TAN-Einreichung durch einen Benutzer (2 von 2)

Der vollständige Ablauf sieht bei einem Auftrag mit nur einer benötigten TAN („Einfach-TAN“) folgendermaßen aus:

Auftragseinreichung durch einen Benutzer mit einer TAN Ausgangszustand: Die Initialisierung – ggf. mit starker Kundenauthentifizierung - ist erfolgt; der Benutzer hat dort durch Belegung des DE „Sicherheitsfunktion, kodiert“ ein konkretes Zwei-Schritt-TAN-Verfahren für sich gewählt und für den gesamten Dialog festgelegt.		
Schritt 1a z. B. SEPA-SingRemitt, DistSigsSubmit	→	Auftrag zur verteilten Signatur einreichen Ein TAN-pflichtiger Auftrag wird in den Umschlag *Auftrag zur verteilten Signatur einreichen (DistSigsSubmit)* eingestellt und in einer FinTS-Nachricht eingereicht. Die *Challenge-Anforderung (XML-Pfad: OneTimePassword/ChallengeRequest)* enthält einen XPath-Ausdruck für den zu signierenden Nachrichtenteil, auf den sich die angeforderte Challenge bezieht. Die *PIN/TAN-Signatur (XML-Tag: OneTimePassword)* enthält die PIN des Benutzers aber keine TAN. Als *Rolle des Signierenden (XML-Tag: SignerRole)* wird *ISS* für Herausgeber verwendet. *DistSigsSubmit_2_Req/SignerInfo/SigsNotComplete* zeigt an, dass dieser Auftrag aus Sicht des Benutzers noch signiert werden muss.
Schritt 1b DistSigsSubmit (Antwort)	←	Challenge senden Nach Verifizieren der PIN wird im Kreditinstitut überprüft, ob eine starke Kundenauthentifizierung benötigt wird oder der Auftrag sofort ausgeführt werden kann. Dies wird durch den Rückmeldungscode *3076 Keine starke Authentifizierung erforderlich* angezeigt (dann weiter mit Schritt 2b). Falls die Eingabe einer TAN erforderlich ist, erfolgt eine Zwischenspeicherung des Auftrags auf Institutsseite. Anschließend wird eine verfahrensspezifische Challenge ermittelt und dem Kundenprodukt in der Antwort *OneTimePasswordReply* im Element TAN-Anforderung (*XML-Tag: TANRequest*) mitgeteilt. Durch Verwenden des Rückmeldungscode *0030 Auftrag empfangen - Sicherheitsfreigabe erforderlich* zusammen mit der *Auftrags-ID (XML-Tag: DistSigsID)* aus der Antwort zu *DistSigsSubmit* erhält das Kundenprodukt die Information, dass der Kunde nun auf Basis der Challenge in vereinbarter Form eine TAN ermitteln muss.
Schritt 2a DistSigsSign	→	Verteilte Signatur (TAN) einreichen Mit dem Geschäftsvorfall *Auftrag mit verteilten Signaturen signieren* wird die ermittelte TAN zusammen mit der zugehörigen Auftrags-ID zum Kreditinstitut übermittelt. Wie beim Ein-Schritt-Verfahren enthält die *PIN/TAN-Signatur* die Benutzerkennung, PIN und TAN des aktiven Benutzers für diesen Auftrag. Als *Rolle des Signierers* wird *ISS* für Herausgeber verwendet. Über das Fehlen des Elements *SigsNotCom-*

		plete wird signalisiert, dass dies aus Benutzersicht die letzte und einzige TAN zu dem eingereichten Auftrag ist. Nach erfolgreicher TAN-Prüfung kann der Auftrag verarbeitet werden.
Schritt 2b z. B. Rückmeldungen zu SEPA-SingRemitt, DistSigsSign	←	Rückmeldungen senden Mit der Kreditinstitutsantwort zum eigentlichen Auftrag werden ggf. erzeugte Antwortsegmente, sowie die Rückmeldungen zum Auftrag selbst und ggf. zur TAN-Verifikation zum Kundenprodukt gesendet.

II.4.1.2 Auftragserinreichung durch zwei Benutzer mit je einer TAN in zwei Dialogen

Bereits beim Ein-Schritt-TAN-Verfahren war die Verwendung von Mehrfach-TANs möglich. Diese mussten dort in einem Schritt zusammen mit dem Auftrag eingereicht werden.

Mit den Mitteln der verteilten Signatur besteht durch Verwenden des VS-GV *Details zu eingereichten Aufträgen anfordern (DistSigsInfo)* gemäß *[Formals], Abschnitt III.7.2* die Möglichkeit, die Auftrags-IDs offener Aufträge eines Benutzers inkl. der Challenge-Informationen und ggf. auch weiteren Details zu übermitteln. Mithilfe einer so empfangenen Auftrags-ID kann ein Benutzer nun die korrespondierende Challenge anzeigen und bestätigen. Die resultierende TAN kann wie bei der Einfach-TAN durch den VS-GV *Verteilte Signatur leisten (DistSigsSign)* eingereicht werden.

Bei FinTS4 ist der Dialogbezug der TAN-Einreichung nicht relevant, TANs können im gleichen Dialog unter dem Erst-Signierer als Boten oder in einem neuen Dialog mit dem Zweit-Signierer als Dialogführer eingereicht werden.

Bei Einsatz von Mehrfach-TANs muss grundsätzlich für jeden Benutzer eine starke Kundenauthentifizierung durchgeführt werden.

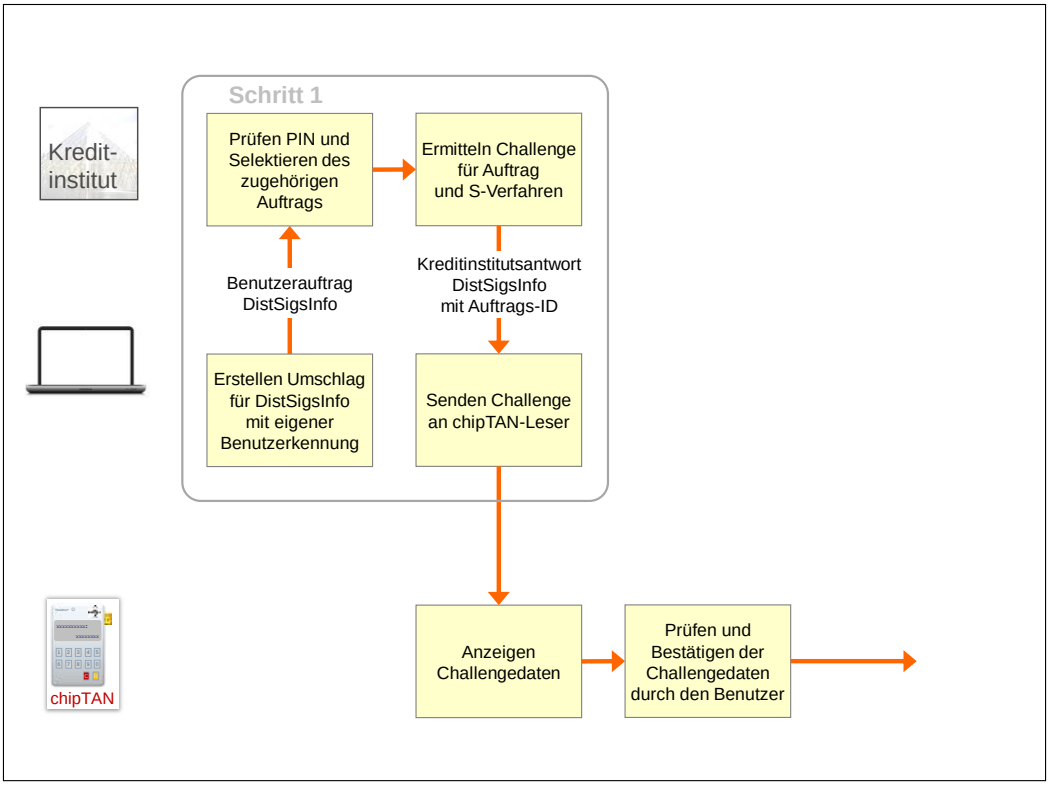


Abbildung 7: Auftragseinreichung durch zwei Benutzer mit je einer TAN (1 von 2)

Die Einreichung der TAN erfolgt dann wie in *Abbildung 6: TAN-Einreichung durch einen Benutzer (2 von 2)* gezeigt.

Der entsprechend erweiterte Ablauf sieht folgendermaßen aus:

Auftragseinreichung durch 2 Benutzer mit je einer TAN

Ausgangszustand:

- Beide Benutzer haben Online-Banking-Zugang und sind für ein TAN-Sicherheitsverfahren freigeschaltet.
- Der erste Benutzer hat den Auftrag zusammen mit der ersten TAN eingereicht und den Dialog beendet. Durch Einstellen des Elements *SigsNotComplete* weist das Kundenprodukt darauf hin, dass aus Benutzersicht noch eine zweite Signatur zu leisten ist.
- Kreditinstitutsseitig wird der Auftrag inklusive der Autorisierungsinformationen für die erste TAN zwischengespeichert. Auch eine Liste der noch fehlenden signaturberechtigten Benutzer wird mit hinterlegt.
- Der zweite Benutzer hat einen Dialog mit einem für ihn freigegebenen TAN-Verfahren eröffnet.

Schritt 1a DistSigsInfo	→	Offene Aufträge für Benutzer ermitteln Der Benutzer übermittelt den VS-GV *Details zu eingereichten Aufträgen anfordern*.
Schritt 1b DistSigsInfo	←	Auftrags-ID zu offenem Auftrag senden Für den Benutzer wird ein offener Auftrag gefunden. Dessen Auftrags-ID wird zusammen mit den Challengedaten an das Kundenprodukt gesendet. Der Benutzer ermittelt durch Anzeigen und Bestätigen der Challengedaten die resultierende TAN.
Schritt 2a DistSigs-Sign	→	Challenge anfordern Mit dem Geschäftsvorfall *Auftrag mit verteilten Signaturen signieren* wird für die ausgewählte Auftrags-ID eine Challenge angefordert. Die *Challenge-Anforderung (XML-Pfad: OneTimePassword/ChallengeRequest)* enthält einen XPath-Ausdruck für den zu signierenden Nachrichtenteil, auf den sich die angeforderte Challenge bezieht.
Schritt 2b DistSigs-Sign	←	Challenge senden Auf Institutsseite wird eine verfahrensspezifische Challenge ermittelt und dem Kundenprodukt in der Antwort *OneTimePasswordReply* im Element TAN-Anforderung (*XML-Tag: TANRequest*) mitgeteilt. Durch Verwenden des Rückmeldungscode 0030 – „Auftrag empfangen - Sicherheitsfreigabe erforderlich“ erhält das Kundenprodukt die Information, dass der Kunde nun auf Basis der Challenge in vereinbarter Form eine TAN ermitteln muss.
Schritt 3a DistSigs-Sign	→	Verteilte Signatur (TAN) einreichen Mit dem Geschäftsvorfall *Auftrag mit verteilten Signaturen signieren* wird die ermittelte TAN zusammen mit der zugehörigen Auftrags-ID zum Kreditinstitut übermittelt. Wie beim Ein-Schritt-Verfahren enthält die *PIN/TAN-Signatur* die Benutzerkennung, PIN und TAN des aktiven Benutzers für diesen Auftrag. Als *Rol-*

		le des Signierers wird *ISS* für Herausgeber verwendet. Über das Fehlen des Elements *SigsNotComplete* wird signalisiert, dass dies aus Benutzersicht die letzte der beiden benötigten TANs zu dem eingereichten Auftrag ist. Nach erfolgreicher TAN-Prüfung kann der Auftrag verarbeitet werden.
Schritt 3b z. B. Rückmeldungen zu SEPA-SingRemitt, DistSigs-Sign	←	Rückmeldungen senden Mit der Kreditinstitutsantwort zum eigentlichen Auftrag werden ggf. erzeugte Antwortsegmente, sowie die Rückmeldungen zur zweiten TAN-Prüfung und zum Auftrag selbst zum Kundenprodukt gesendet. Durch Einstellen des Elementes *SigsComplete* und die Antwort zu *DistSigsSign* wird signalisiert, dass die autorisierung des Auftrags vollständig erfolgt ist.

II.4.2 Abläufe bei der Initialisierung mit starker Kundenauthentifizierung

Durch [MaSI] und [PSD2] besteht die Forderung nach einer starken Kundenauthentifizierung u. a. beim Zugriff auf Kontendaten, also auch zum Zeitpunkt der FinTS-Initialisierung. Hierfür wurden Abläufe geschaffen, die eine Umsetzung der starken Kundenauthentifizierung bei TAN-Verfahren ermöglichen.

Wenn das Kreditinstitut das Element *SCARequired* (BPD) mit dem Wert *1=optional unterstützt* bzw. *2=verpflichtend unterstützt* belegt hat, wird in die Segmentfolge der *Initialisierung (InitReq)* durch das Kundenprodukt ein Umschlag *DistSigsSubmit* mit einem XPath-Ausdruck auf das Segment *Identification* eingestellt. Das Element *SCARequested* wird mit dem Wert *J* belegt.

II.4.2.1 Rahmenbedingungen für den Einsatz der starken Kundenauthentifizierung

- Voraussetzung für die Verwendung der starken Kundenauthentifizierung ist, dass ein Kundenprodukt bereits vor der Initialisierung die Sicherheitsverfahren und Parameter kennt. Daher muss ein Kreditinstitut das Abholen der BPD über einen anonymen Dialog zulassen, wenn es starke Authentifizierung verwenden möchte.
- Sind dem Kundenprodukt die konkreten, für den Benutzer zugelassenen Sicherheitsverfahren beim allerersten Zugang nicht bekannt, so können diese über eine Initialisierung mittels Einschritt-TAN-Verfahren angefordert werden. Die konkreten Verfahren werden dann über den *Rückmeldungscode 3920* zurückgemeldet. Im Rahmen dieses Prozesses darf keine UPD zurückgeliefert werden und die Durchführung anderer Geschäftsvorfälle ist in einem solchen Dialog nicht erlaubt.
- Die Bereitschaft bzw. Verpflichtung zur starken Kundenauthentifizierung wird durch das Kreditinstitut durch die Belegung *1=optional unterstützt* bzw. *2=verpflichtend unterstützt* für das Element *SCARequired* vorgegeben. Mit beiden Belegungen ist es möglich, in die Segmentfolge der *Initialisierung* eine TAN-Anforderung durch *DistSigsSubmit* zu integrieren. Dazu muss das Element *SCARequested* den Wert *J* besitzen.
- Bei Verwendung von chipTAN ist bei HHD V1.3.2 die Challenge-Klasse 02 (Anmelde-TAN) zu verwenden. Bei HHD V1.4 gilt die Schablone 01 bzw. 02 (Legitimation Kunde mit einem `Authentifizierungsmerkmal`). Die Auswahl der Schablone 01 bzw. 02 wird durch das Kreditinstitut getroffen und ist Inhalt des Start-Codes im Schritt 2a in den Abläufen. Das `Authentifizie-`

`rungsmerkmal` wird durch das Kreditinstitut festgelegt und mit dem Benutzer vereinbart.

- Nach Bestätigung der eingereichten TAN findet ein standardmäßiger FinTS-Dialog statt, in dem TAN-pflichtige und nicht-TAN-pflichtige Aufträge ausgeführt werden können. Der Dialog muss durch das Kundenprodukt mit einem Dialogendekennzeichen (*TermSession*) geschlossen werden.
- Migration: Durch Belegung des Elements *SCARequired* mit *1* oder *2* in den BPD signalisiert das Kreditinstitut die Fähigkeit zur Durchführung einer starken Kundenauthentifizierung. Enthält die Segmentfolge der *Initialisierung* keinen Umschlag *DistSigsSubmit* und enthält das Element *SCARequested* den Wert *1*, so handelt es sich um eine schwache Authentifizierung. Diese kann – solange zulässig – parallel zur starken Kundenauthentifizierung unterstützt werden. Durch Verwendung des Rückmeldungscode *3075 „Starke Authentifizierung ab dem … erforderlich“* kann ein Benutzer auf den Wegfall der schwachen Authentifizierung hingewiesen werden. Nach Ablauf dieser Frist kann eine Dialoginitialisierung ohne starke Kundenauthentifizierung durch den Rückmeldungscode *9075 „Starke Authentifizierung erforderlich“* abgewiesen werden.

Unterstützt ein Kreditinstitut die starke Kundenauthentifizierung mithilfe von *SCARequired = 1*, so sollte ein Kundenprodukt in die Segmentfolge der *Initialisierung* grundlegend einen Umschlag *DistSigsSubmit* einstellen und das Element *SCARequested* auf *J* setzen, um ggf. einen Rückmeldungscode *3075* bzw. *9075* zu vermeiden.
Das Kreditinstitut muss anhand der in den PSD2 Regularien beschriebenen Ausnahmen festlegen, ob eine starke Kundenauthentifizierung nötig ist (nur dann erfolgt der nächste Schritt des Zwei-Schritt-Verfahrens) oder ob die Initialisierung in der Antwortnachricht unmittelbar beantwortet werden kann.
Das Kundenprodukt steuert also nicht, ob es sich um eine starke oder schwache Authentifizierung handelt.

Im Rahmen der PIN/TAN-Management-Geschäftsvorfälle (vgl. Abschnitt II.10) ist in bestimmten Situationen eine Einreichung ohne starke Kundenauthentifizierung erforderlich (Authentifizierungsklasse 4, vgl. Kapitel II.3). Daher wird in einem solchen Fall über einen XPath-Ausdruck der jeweilige Geschäftsvorfall in der Nachricht referenziert, der isoliert in diesem Dialog eingereicht wird.

Bezeichnung	XML-Schema
PIN-Änderung	ChangePIN
PIN-Sperre aufheben	RevokePINBlock
PIN Sperren	BlockPIN
Anzeige der verfügbaren TAN-Medien	DisplayTanGeneratorList
TAN-Generator an- bzw. ummelden	ChangeTANGenerator
TAN-Generator Synchronisierung	SynchronizeTANGenerator
Mobilfunkverbindung registrieren	RegisterMobilePhoneConnection / RegisterMobilePhoneConnectionNoFee
Mobilfunkverbindung freischalten	AvtivateMobilePhoneConnection
Mobilfunkverbindung ändern	ChangeMobilePhoneConnection / ChangeMobilePhoneConnectionNoFee
Deaktivieren / Löschen von TAN-Medien	DeactivateDeleteTANMedium

In den nächsten Abschnitten sind die Rahmenbedingungen für repräsentative Prozesse solcher PIN/TAN-Management Geschäftsvorfälle beschrieben.

II.4.2.1.1 Rahmenbedingungen bei Erst-PIN-Änderung (*ChangePIN*)

Die folgenden Schritte gelten für die Einreichung einer Erst-PIN-Änderung, die ohne starke Kundenauthentifizierung erfolgt. Ggf. wurde ein zuvor durchgeführter Anmeldeversuch durch einen Rückmeldungscode `3916` (z. B. „PIN muss wegen erstmaliger Anmeldung zwangsweise geändert werden“) beantwortet.

- Erster Dialog – Ermitteln TAN-Verfahren
  - Zunächst wird ein Dialog mit dem TAN-Ein-Schritt-Verfahren ohne integrierten Umschlag *DistSigsSubmit* eröffnet.
  - Die Initialisierungsantwort enthält über den Rückmeldungscode *3920* die für den Benutzer zugelassenen TAN-Verfahren. Die Antwort darf keine UPD enthalten, da noch keine starke Kundenauthentifizierung vorliegt.
  - Anschließend hat das Kundensystem den Dialog durch Senden eines Dialogendekennzeichens (*TermSession*) zu beenden.
- Zweiter Dialog – PIN-Einreichung und Authentifizierung durch eine TAN[2]
  - Anschließend wird gemäß dem Ablauf in Kapitel II.4.2.2) unter Verwendung eines zugelassenen TAN-Verfahrens (diese wurden im ersten Dialog mit Rückmeldungscode *3920* zurück gemeldet) ein zweiter Dialog mit integriertem Umschlag *DistSigsSubmit* eröffnet, um die PIN-Änderung durchzuführen. Über einen XPath-Ausdruck wird der Geschäftsvorfall *PIN-Änderung* referenziert.
  - Hinweis: Ist die zur Durchführung des TAN-Prozesses benötigte *Bezeichnung des TAN-Mediums* noch nicht bekannt, so muss zunächst der hierfür vorgesehene Ablauf (vgl. Abschnitt II.4.2.1.3) in einem se-

[2] Das Senden einer TAN mit dem Geschäftsvorfall *ChangePIN* ist mit Einführung der starken Kundenauthentifizierung obligatorisch, da durch die PSD2 für das Ändern des Wissenselementes eine starke Kundenauthentifizierung erforderlich ist.

paraten Dialog durchgeführt werden. Erst dann kann der Dialog mit der PIN-Änderung erfolgen.

- Nach erfolgter Initialisierungsantwort wird in einem nächsten Schritt durch das Kundensystem der Geschäftsvorfall *PIN Ändern (Change-PIN)* eingereicht.
- Das Institut muss in der Antwort durch den Rückmeldungscode *0030* eine TAN zur Authentifizierung anfordern. Nach Eingabe der TAN durch den Benutzer wird diese durch das Kundensystem eingereicht.
- Unmittelbar nach Bestätigung der eingereichten TAN muss der Dialog durch das Kundensystem mit einem Dialogendekennzeichen (*TermSession*) geschlossen werden. Um Auftragsnachrichten zu schicken, kann das Kundenprodukt anschließend eine neue Dialoginitialisierung mit integriertem Umschlag *DistSigsSubmit* für diesen Benutzer senden.

II.4.2.1.2 Rahmenbedingungen bei Zwangs-PIN-Änderung (*ChangePIN*)

Die folgenden Schritte gelten für die Einreichung bei einer Zwangs-PIN-Änderung.

- Erster Dialog – Auslöser: Dialog mit fehlerhafter PIN
  - Auslöser ist ein Dialog mit wiederholt eingegebener fehlerhafter PIN. Das verwendete Sicherheitsverfahren ist dafür unerheblich.
  - Das Institut antwortet in diesem Fall mit einem Rückmeldungscode *3916* (z. B. *„PIN muss wegen zu vieler Fehlversuche zwangsweise geändert werden“*). Es wird davon ausgegangen, dass dem Kundensystem die für den Benutzer zugelassenen TAN-Verfahren bekannt sind bzw. diese der Kreditinstitutsanwort (Rückmeldungscode *3920*) entnommen werden. Die Antwort darf keine UPD enthalten, da durch Fehlen des Wissenselementes keine starke Kundenauthentifizierung vorliegt.
  - Anschließend hat das Kundensystem den Dialog durch Senden eines Dialogendekennzeichens (*TermSession*) zu beenden.
- Zweiter Dialog – PIN-Änderung und Authentifizierung durch eine TAN[3]
  - Anschließend wird gemäß dem Ablauf in Kapitel II.4.2.2 unter Verwendung eines zugelassenen TAN-Verfahrens ein zweiter Dialog mit integriertem Umschlag *DistSigsSubmit* eröffnet, um die PIN-Änderung durchzuführen. Über einen XPath-Ausdruck wird der Geschäftsvorfall *PIN-Änderung* referenziert.
  - Hinweis: Ist die zur Durchführung des TAN-Prozesses benötigte *Bezeichnung des TAN-Mediums* noch nicht bekannt, so muss zunächst der hierfür vorgesehene Ablauf (vgl. Abschnitt II.4.2.1.3) in einem separaten Dialog durchgeführt werden. Erst dann kann der Dialog mit der PIN-Änderung erfolgen.

[3] Das Senden einer TAN mit dem Geschäftsvorfall *ChangePIN* ist mit Einführung der starken Kundenauthentifizierung obligatorisch, da durch die PSD2 für das Ändern des Wissenselementes eine starke Kundenauthentifizierung erforderlich ist.

- Nach erfolgter Initialisierungsantwort wird in einem nächsten Schritt durch das Kundensystem der Geschäftsvorfall *PIN Ändern (Change-PIN)* eingereicht.
- Das Institut muss in der Antwort durch den Rückmeldungscode *0030* eine TAN zur Authentifizierung anfordern. Nach Eingabe der TAN durch den Benutzer wird diese durch das Kundensystem eingereicht.
- Unmittelbar nach Bestätigung der eingereichten TAN muss der Dialog durch das Kundensystem mit einem Dialogendekennzeichen (*TermSession*) geschlossen werden. Um Auftragsnachrichten zu schicken, kann das Kundenprodukt anschließend eine neue Dialoginitialisierung mit integriertem Umschlag *DistSigsSubmit* für diesen Benutzer senden.

II.4.2.1.3 Rahmenbedingungen zur Ermittlung möglicher TAN-Medien-Kennungen (*DisplayTanGeneratorList*)

Beim Erstzugang mit einem neuen TAN-Verfahren liegt einem Kundenprodukt ggf. noch keine TAN-Medien-Bezeichnung für dieses Verfahren vor. In diesem Fall muss der Geschäftsvorfall *Anzeige der verfügbaren TAN-Medien (DisplayTanGeneratorList)* ohne starke Kundenauthentifizierung durchführbar sein. Dies ist bei der Prüfung der SCA-Kriterien im Kreditinstitut zu berücksichtigen.

- Erster Dialog – Ermitteln der TAN-Medien-Bezeichnung
  - Es wird gemäß dem Ablauf in Kapitel II.4.2.2) unter Verwendung eines zugelassenen TAN-Verfahrens eine *Initialisierung* mit integriertem Umschlag *DistSigsSubmit* eröffnet, um die Abfrage der TAN-Medien-Kennungen durchzuführen. Über einen XPath-Ausdruck wird der Geschäftsvorfall *Anzeige der verfügbaren TAN-Medien* referenziert. Der vom Kundenprodukt hier als *Füllwert* gelieferte Inhalt des Elementes *Bezeichnung des TAN-Mediums* ist vom Kreditinstitut in dieser Situation zu ignorieren.
  - Das Kreditinstitut liefert nach erfolgreicher PIN-Prüfung im Antwortsegment die für den Benutzer eingereichten TAN-Medien und mit dem Rückmeldungscode *3920* die zugelassenen TAN-Verfahren für den Benutzer zurück (falls diese dem Kundensystem noch nicht bekannt waren).
  - Anschließend hat das Kundensystem den Dialog durch Senden eines Dialogendekennzeichens (*TermSession*) zu beenden bzw. kann weitere in diesem Kontext erlaubte Geschäftsvorfälle wie z. B. eine *PIN-Änderung (ChangePIN)* durchführen.
- Zweiter Dialog – Starke Kundenauthentifizierung
  - Anschließend wird unter Verwendung eines zugelassenen TAN-Verfahrens und TAN-Mediums ein zweiter Dialog zum Durchführen einer starken Kundenauthentifizierung eröffnet. Die SCA ist in diesem Fall obligatorisch, da es sich um die erste Nutzung dieses TAN-Verfahrens inkl. des gewählten TAN-Mediums handelt.
  - Im Rahmen dieses Dialoges können nach erfolgreicher Durchführung der starken Kundenauthentifizierung beliebige Geschäftsvorfälle durchgeführt werden.

II.4.2.1.4 Rahmenbedingungen zur Synchronisation von TAN-Generatoren (*SynchronizeTANGenerator*)

Bei mehrfacher TAN-Falscheingabe wird bei chipTAN zunächst davon ausgegangen, dass der TAN-Generator nicht synchronisiert ist, bevor eine TAN-Sperre gesetzt wird. In diesem Fall muss für den Benutzer der nicht-TAN-pflichtige Geschäftsvorfall *TAN-Generator synchronisieren (SynchronizeTAN-Generator)* ohne starke Kundenauthentifizierung durchführbar sein, um eine TAN mit dem zugehörigen aktuellen ATC einzureichen. Dies ist bei der Prüfung der SCA-Kriterien im Kreditinstitut zu berücksichtigen.

- Es wird eine Initialisierung gemäß dem in Kapitel II.4.2.2 beschriebenen Ablauf durchgeführt. Über einen XPath-Ausdruck wird der Geschäftsvorfall *TAN-Generator synchronisieren* referenziert.
- Das Kreditinstitut fordert nach erfolgreicher PIN-Prüfung den Benutzer mit dem Rückmeldungscode *3931* auf, den Geschäftsvorfall *SynchronizeTAN-Generator* für eine explizite Synchronisation des TAN-Generators auszuführen.
- Unmittelbar nach erfolgreicher Verifizierung von TAN und ATC muss der Dialog durch das Kundenprodukt durch ein Dialogendekennzeichen (*TermSession*) geschlossen werden.

II.4.2.2 Initialisierung mit starker Authentifizierung

Der vollständige Ablauf sieht bei einer Initialisierung mit möglicher starker Authentifizierung folgendermaßen aus:

Initialisierung mit starker Authentifizierung

Ausgangszustand:

- Vor dem allerersten Dialog mit dem Kreditinstitut bzw. falls die Informationen nicht vorliegen: Das Kundenprodukt hat über einen anonymen Dialog die aktuellen BPD abgeholt und ist somit in Kenntnis aller vom Kreditinstitut unterstützten Sicherheitsverfahren und Parameter.
- Der BPD-Parameter *SCARequired* ist mit *1* oder *2* belegt
- Vor dem allerersten Dialog mit dem Kreditinstitut bzw. falls die Informationen nicht vorliegen: Mit der Durchführung eines personalisierten Dialogs mit dem Ein-Schritt-TAN-Verfahren erhält das Kundenprodukt mit dem Rückmeldungscode *3920* alle für den Benutzer zugelassenen Ein- und Zwei-Schritt-Verfahren mitgeteilt. Eine UPD liegt zu diesem Zeitpunkt noch nicht vor. Dieser anonyme Dialog wird durch das Kundensystem durch Setzen des *Dialogendekennzeichens* (*TermSession*) beendet.
- Der Benutzer wählt durch entsprechende Belegung des DE *Option (Sicherheitsfunktion, kodiert)* ein konkretes Zwei-Schritt-Verfahren für den gesamten zweiten Dialog.

Schritt 1a *Initialisierung, DistSigsSubmit*	→	Initialisierung starten Es wird die Segmentfolge der *Initialisierung* eingereicht. Die Nachricht enthält auch einen Umschlag *Auftrag zur verteilten Signatur einreichen (DistSigsSubmit)* und eine XPath-Referenz auf das Segment *Identifizierung*. Durch die Belegung des Elements *SCARequested* wird gekenn-

		zeichnet, dass es sich um eine starke Kundenauthentifizierung handelt Der Signaturabschluss enthält die PIN des Benutzers, aber keine TAN. Durch eine Prüfung der eingereichten Daten, im Speziellen der Benutzerkennung und der PIN, gegen die SCA Ausnahmen legt das Kreditinstitut fest, wie weiter vorgegangen werden soll: • starke Kundenauthentifizierung erforderlich, angezeigt durch den Rückmeldungscode *0030 Auftrag empfangen - Sicherheitsfreigabe erforderlich* (→weiter mit Schritt 1b) • der Faktor Wissen ist ausreichend, angezeigt durch den Rückmeldungscode *3076 Keine starke Authentifizierung erforderlich* (→weiter mit Schritt 2b, Fall (A)).
Schritt 1b *DistSigsSubmit* (Antwort)	←	Challenge senden Es wird eine verfahrensspezifische Challenge ermittelt und dem Kundenprodukt in der Antwort *OneTimePasswordReply* im Element TAN-Anforderung (*XML-Tag: TANRequest*) mitgeteilt. Durch den *RM-Code 0030* und Verwenden der *Auftrags-ID (XML-Tag: DistSigsID)* aus der Antwort zu *DistSigsSubmit* erhält das Kundenprodukt die Information, dass der Kunde nun auf Basis der Challenge in vereinbarter Form eine Anmelde-TAN ermitteln muss.
Schritt 2a *DistSigsSign*	→	Verteilte Signatur (TAN) einreichen Mit dem Geschäftsvorfall *Auftrag mit verteilten Signaturen signieren* wird die ermittelte TAN zusammen mit der zugehörigen Auftrags-ID zum Kreditinstitut übermittelt. Wie beim Ein-Schritt-Verfahren enthält die *PIN/TAN-Signatur* die Benutzerkennung, PIN und TAN des aktiven Benutzers für diesen Auftrag. Als *Rolle des Signierers* wird *ISS* für Herausgeber verwendet. Über das Fehlen des Elements *SigsNotComplete* wird signalisiert, dass dies aus Benutzersicht die letzte und einzige TAN zu dem eingereichten Auftrag ist. Nach erfolgreicher TAN-Verifikation kann die erfolgreiche Prüfung auf starke Kundenauthentifizierung bestätigt werden.
Schritt 2b ggf. BPD, UPD, Rückmeldungen, *DistSigsSign* (Antwort)	←	BPD, UPD und Rückmeldungen senden (A) Ohne starke Kundenauthentifizierung: Mit der Kreditinstitutsantwort werden ggf. erzeugte BPD und UPD, sowie die Rückmeldungen zur *Initialisierung* zum Kundenprodukt gesendet. Das Element *OneTimePasswordReply* im Element TAN-Anforderung (*XML-Tag: TANRequest*) wird mit dem Wert *nochallenge* belegt. Die *Auftrags-ID (XML-Tag: DistSigsID)* enthält den Wert *noref*. Diese sind vom Kundenpro-

		dukt zu ignorieren. (B) Bei starker Kundenauthentifizierung: Mit der Kreditinstitutsantwort werden ggf. erzeugte BPD und UPD, sowie die Rückmeldungen zur TAN-Verifikation und zur Initialisierung selbst zum Kundenprodukt gesendet.

II.4.3 Allgemeine Festlegungen zum Zeitverhalten beim Zwei-Schritt-Verfahren

Bei Verwendung des Zwei-Schritt-Verfahrens wird auf Institutsseite das Zeitfenster zwischen den beiden Prozess-Schritten überwacht, um nicht freigegebene Aufträge nach Ablauf der Gültigkeit entsprechend kennzeichnen und die zugehörige TAN entwerten zu können. Das Zeitfenster selbst hängt von der Implementierung auf Institutsseite ab. Auch bei der Verarbeitung von synchronen bzw. zeitversetzten Mehrfach-TANs ergibt sich unterschiedliches Zeitverhalten, wie in den folgenden Abschnitten beschrieben.

Das Zeitfenster für die Eingabe einer TAN im Zwei-Schritt-Verfahren wird institutsindividuell geregelt, muss dem Kunden aber genügend Zeit für die Eingabe der TAN lassen und sollte daher einen Wert von 8 Minuten nicht unterschreiten.

Ein oberes Limit wird nur durch die Aufbewahrungsdauer offener Aufträge im Institut festgelegt.

Um dem Kundenprodukt eine übersichtliche Benutzerführung zu ermöglichen kann das Element *Gültigkeitsdatum und –uhrzeit für Challenge* in *OneTimePasswordReply/TANRequest* entsprechend belegt werden.

II.4.3.1 Verteilung von Aufträgen auf FinTS-Nachrichten

Da mit FinTS4 die syntaktischen Möglichkeiten bestehen, können TAN-pflichtige und PIN-pflichtige Aufträge beliebig gemischt werden. Auch mehrere TAN-pflichtige Aufträge innerhelb einer Nachricht sind unterstützt.

Durch das Zeitverhalten bei TAN-pflichtigen Aufträgen im Zwei-Schritt-Verfahren kann es zu Problemen in Kombination mit PIN-pflichtigen Aufträgen kommen, die eine lange Verarbeitungszeit erfordern wie z. B. Umsatzabfragen. Dadurch kann es möglich sein, dass die Antwortzeit der Umsatzabfrage das Zeitfenster für die Bereitstellung der TAN durch den Kunden so stark einschränkt, dass ein Timeout auftritt.

Diese Situation kann vermieden werden, wenn in solchen Fällen die Aufträge in separaten Nachrichten vorab übertragen werden und auf die Mischung mit den TAN-pflichtigen Aufträgen verzichtet wird.

II.4.3.2 Zeitüberwachung beim Zwei-Schritt-Verfahren bei Einfach-TANs

Die Eingabe einer TAN im Zwei-Schritt-Verfahren wird auf Institutsseite durch Timer überwacht, d. h. nach Übermittlung der Challenge bleibt dem Kunden nur ein bestimmtes Zeitfenster, um die TAN einzureichen. Ein Ausbleiben der TAN wird als fehlerhafter Versuch gewertet und die TAN wird als ungültig markiert. Dies wird bei der Auftragsantwort im jeweiligen TAN-Prozess-Schritt über den Rückmeldecode 9951 – „Zeitüberschreitung im Zwei-Schritt-Verfahren – TAN ungültig“ signalisiert.

Diese Zeitüberwachung gilt bei jeder Einreichung einer TAN im Zwei-Schritt-Verfahren, also auch bei Mehrfach-TANs in einem Dialog.

II.4.3.2.1 Zeitüberwachung bei zeitversetzten Mehrfach-TANs

Die maximale Dauer, die ein eingereichter Auftrag für die Übermittlung weiterer TANs aufbewahrt wird, unterliegt bei zeitversetzter Einreichung einer separaten Zeitüberwachung für jeden Benutzer. Wird dieses Zeitfenster überschritten und der Auftrag wurde inzwischen auf Institutsseite gelöscht, so wird dies in der Auftragsantwort zu *Verteilte Signatur leisten (DistSigsSign)* über die Rückmeldecodes 9210 „Auftrag abgelehnt – Kein eingereichter Auftrag gefunden“ bzw. 9210 – „Auftragsreferenz ist unbekannt“ signalisiert.

Die Aufbewahrungsdauer von Aufträgen mit Mehrfach-TANs bei zeitversetzter Eingabe entspricht den Regelungen bei FinTS Statusprotokollen (vgl. [Formals], *Abschnitt III.2*), kann institutsindividuell jedoch auch bis zu einem Jahr betragen.

II.5 Erweiterung der Rückmeldungscodes

Bei Verwendung des PIN/TAN-Verfahrens können spezielle Rückmeldecodes vom Kreditinstitut zurückgemeldet werden, die rein PIN/TAN-spezifisch sind und nicht direkt mit dem zugehörigen Geschäftsvorfall in Verbindung stehen. Es handelt sich hierbei um die folgenden Codes:

- **Erfolgsmeldungen**

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
0020	PIN-Sperre erfolgreich
0020	PIN-Sperre aufgehoben
0020	PIN geändert
0030	Auftrag empfangen – Sicherheitsfreigabe erforderlich
0900	TAN gültig
0901	PIN gültig

- **Warnungen und Hinweise**

Code	Beispiel für Rückmeldungstext
3075	Starke Authentifizierung ab dem … erforderlich
3076	Keine starke Authentifizierung erforderlich
3910	TAN wurde nicht verbraucht
3913	TAN wurde verbraucht
3916	PIN muss wegen erstmaliger Anmeldung zwangsweise geändert werden
3918	Kompetenz nicht ausreichend – weitere TAN erforderlich
3920	Zugelassene Ein- und Zwei-Schritt-Verfahren für den Benutzer (+ Rückmeldungsparameter)
3931	PIN gesperrt. Entsperren mit GV „PIN-Sperre aufheben“ möglich
3931	TAN-Generator gesperrt. Führen Sie ggf. eine TAN-Gen.-Synchronisation durch
3932	Bitte führen Sie zunächst eine PIN-Änderung durch
3933	TAN-Generator gesperrt, Synchronisierung erforderlich Kartennummer ##########
3934	Bitte eine Karte für die Verwendung mit chipTAN zulassen
3935	Bitte eine Karte für die Verwendung mit chipTAN zulassen
3939	mobileTAN-Freischaltung erforderlich. SMS-Freischaltcode wurde versendet
3940	Zur PIN-Änderung stehen folgende TAN-Medien zur Verfügung: ##########
3941	Zur PIN-Änderung stehen folgende Rufnummern zur Verfügung: ##########
3950	Die Selbstumstellung auf ein anderes Sicherheitsverfahren ist möglich
3951	Die Selbstumstellung auf ein anderes Sicherheitsverfahren ist erforderlich
3952	<Rückmeldung des erfolgten Prozesschrittes der Selbstumstellung>
3960 - 3999	Individuell

- **Fehlermeldungen**

Code	Beispiel für Rückmeldungstext
9075	Dialog abgebrochen - starke Authentifizierung erforderlich
9210	Auftrag abgelehnt – Auftragsdaten inkonsistent. Eingereichter Auftrag gelöscht
9210	Auftrag abgelehnt – Zwei-Schritt-TAN inkonsistent. Eingereichter Auftrag gelöscht
9210	Auftrag abgelehnt – Kein eingereichter Auftrag gefunden
9210	Auftrag abgelehnt – Auftragsreferenz ist unbekannt
9210	Auftrag abgelehnt – Kompetenz nicht ausreichend

Code	Beispiel für Rückmeldungstext
9210	Auftrag abgelehnt – Auftragsdaten inkonsistent. Eingereichter Auftrag gelöscht
9931	Teilnehmersperre durchgeführt, Entsperren nur durch Kreditinstitut
9939	Freischalten der Mobilfunknummer für mobileTAN nicht möglich
9941	TAN ungültig
9942	PIN ungültig
9942	neue PIN ungültig
9943	TAN bereits verbraucht
9951	Zeitüberschreitung im Zwei-Schritt-Verfahren – TAN ungültig
9955	Ein-Schritt-TAN-Verfahren nicht zugelassen
9991	chipTAN nicht zulässig bei Benutzerkennung für iTAN

Dies ist nur ein Auszug der möglichen Rückmeldungscodes beim PIN/TAN-Verfahren. Eine vollständige und aktuelle Beschreibung befindet sich in [RM-Codes].

II.5.1 Beschreibung spezieller Rückmeldungen im Zwei-Schritt-Verfahren

Rückmeldungscode 0030: Auftrag empfangen – Sicherheitsfreigabe erforderlich

Mit dem Rückmeldungscode 0030 als Antwort auf den Geschäftsvorfall *Einreichen eines Auftrags zur verteilten Signatur (DistSigsSubmit)* bzw. auch *Verteilte Signatur leisten (DistSigsSign)* zur Challenge-Anforderung wird der zweite Schritt eines Zwei-Schritt-Verfahrens eingeleitet. Als Folge auf diesen Rückmeldecode darf ausschließlich ein Geschäftsvorfall *Verteilte Signatur leisten (DistSigsSign)* mit der zugehörigen TAN übermittelt und keine neue Auftragseinreichung eingeleitet werden. Unabhängig davon können PIN-pflichtige Geschäftsvorfälle, die keine TAN erfordern zwischen den beiden Prozess-Schritten bearbeitet werden.

Rückmeldungscode 3075 / 9075:

- **Starke Authentifizierung ab dem … erforderlich bzw.**
- **Dialog abgebrochen - starke Authentifizierung erforderlich**

Diese Rückmeldungen werden verwendet, wenn ein Institut durch Belegen des Elements *SCARequired* mit *2* oder *3* in der BPD eine starke Kundenauthentifizierung fordert, das Kundenprodukt diese jedoch nicht durchführt. Diese Möglichkeit einer schwachen Authentifizierung kann – solange zulässig – parallel zur starken Authentifizierung unterstützt werden. Durch Verwendung des Rückmeldungscode *3075 „Starke Authentifizierung ab dem … erforderlich“* kann der Benutzer auf den Wegfall der schwachen Authentifizierung hingewiesen werden. Nach Ablauf dieser Frist kann eine Dialoginitialisierung mit schwacher Authentifizierung durch den Rückmeldungscode *9075 „Dialog abgebrochen - starke Authentifizierung erforderlich“* abgewiesen werden. Der Rückmeldungscode *9075* muss in Kombination mit Code *9800* auftreten.

Rückmeldungscode 3076: Keine starke Authentifizierung erforderlich

Der Rückmeldungscode 3076 wird verwendet, wenn ein Institut durch Belegen des Elements *SCARequired* mit *2* oder *3* in der BPD informiert, dass eine starke Kundenauthentifizierung unterstützt wird. Im Rahmen des Zwei-Schritt-Verfahrens bei Initialisierung und Auftragseinreichung dient dieser RM-Code dazu, das Kundenprodukt nach der Einreichung in Schritt 1a zu informieren, dass die Eingabe der PIN als Wissensfaktor ausreichend ist und aufgrund einer in PSD2 definierten Ausnahme

keine starke Kundenauthentifizierung erforderlich ist. Die Verarbeitung wird mit Schritt 2b (Bestätigung der Auftragseinreichung) fortgesetzt. Somit wird der `RM-` *Code 3076* situationsbezogen alternativ zu *RM-Code 0030* verwendet.

Rückmeldungscode 3920: Zugelassene Ein- und Zwei-Schritt-Verfahren für den Benutzer (+ Rückmeldungsparameter)

Der Rückmeldungscode 3920 dient dazu, dem Kundenprodukt im Rahmen der Initialisierungsantwort die für den Benutzer zugelassenen Zwei-Schritt-Verfahren mitzuteilen, falls diese über die UPD nicht übermittelt werden können. Hierzu werden in den Rückmeldungsparametern entsprechend den zugelassenen Verfahren („900“ bis „997“) aus der BPD für den Benutzer zugelassene Zwei-Schritt-Verfahren transportiert.

Das Kundenprodukt muss – unabhängig vom gewählten Verfahren in „Sicherheitsfunktion, kodiert“ – bei jeder Initialisierung die vom Institut in der UPD bzw. mit dem Rückmeldungscode 3920 übermittelten Werte prüfen, gegen gespeicherte Informationen vergleichen und diese ggf. aktualisieren.
Sollte das Kundenprodukt in der Initialisierungsnachricht ein Verfahren wählen, das für den Benutzer nicht bzw. nicht mehr zugelassen ist, so beendet das Kreditinstitut den Dialog mit Rückmeldungscode 9800 in Kombination mit Code 3920 und meldet die aktuell zugelassenen Verfahren in den Rückmeldungsparametern.

Rückmeldungscode 3934 bzw. 3935: Bitte eine Karte zur Verwendung mit chipTAN zulassen (+ Rückmeldungsparameter)

Die Rückmeldungscodes 3934 und 3935 veranlassen das Kundenprodukt, auf Basis des Geschäftsvorfalls *TAN-Generator / TAN-Liste an- bzw. ummelden (ChangeTANGenerator)* eine gültige Karte für das chipTAN-Verfahren im laufenden Dialog anzumelden. Die Rückmeldungsparameter P1 und P2 enthalten pro Rückmeldung verpflichtend eine „Kartennummer“ (Format „id“) und die zugehörige *Bezeichnung des TAN-Mediums (..32)*.

Bei Verwendung des Rückmeldungscode 3934 ist das Anstoßen des Geschäftsvorfalls *TAN-Generator / TAN-Liste an bzw. ummelden (ChangeTANGenerator)* verpflichtend.

Beim Rückmeldungscode 3935 ist das Initiieren der Kombination *Anzeigen der verfügbaren TAN-Medien (DisplayTANGeneratorList)* und *TAN-Generator / TAN-Liste an bzw. ummelden (ChangeTANGenerator)* optional.

Rückmeldungscode 9210:

- **Auftragsreferenz / Auftrags-ID ist unbekannt bzw.**
- **Auftrag abgelehnt – kein eingereichter Auftrag gefunden**

Diese Rückmeldung kann folgende Ursachen haben:

- Die eingereichte Auftrags-ID (DistSigsID) wird im Auftragsbestand nicht gefunden, da das Element auf dem Weg vom Kreditinstitut zum Kunden und wieder zurück verfälscht wurde.

- Ein zugehöriger Auftrag, der mehrere TANs erfordert, hat den maximalen Aufbewahrungszeitraum überschritten und wurde vom Institut gelöscht.
- Ein zugehöriger Auftrag, der mehrere TANs erfordert, wurde über einen anderen Vertriebsweg (außerhalb FinTS) autorisiert und ist inzwischen verarbeitet.

Das Kreditinstitut sollte den wirklichen Grund für diese Rückmeldung in das Statusprotokoll einstellen, damit der Kunde sich später ggf. dort informieren und den Auftrag kundenseitig entsprechend weiter bearbeiten kann.

II.6 Bankfachliche Anforderungen

Es gelten die in [HBCI], Abschnitt *II.4 Bankfachliche Anforderungen* aufgeführten Regelungen. Abweichend hierzu gilt:

- **Zu signierende Nachrichten**

  Wie auch beim Sicherheitsverfahren HBCI ist die Signatur von Kreditinstitutsnachrichten optional. Da der Benutzer in seiner Auftragsnachricht das anzuwendende Signaturverfahren vorgibt, darf das Kreditinstitut jedoch nicht mit einem HBCI-Sicherheitsverfahren antworten. Es sendet daher ein entsprechendes Segment Antwort auf eine PIN/TAN-Signatur zurück (siehe [Syntax]).

- **Doppeleinreichungskontrolle**

  Im PIN/TAN-Verfahren werden keine Signatur-IDs benötigt, da hier die TAN deren Aufgabe übernimmt und durch sie eine Doppeleinreichung verhindert wird.

II.7 Bankparameterdaten zum PIN/TAN-Verfahren

Realisierung Kreditinstitut: verpflichtend, falls Geschäftsvorfälle mit PIN/TAN-Absicherung angeboten werden
Realisierung Kundenprodukt: optional

Für die Verwendung des PIN/TAN-Verfahrens müssen dem Kundenprodukt spezielle Daten im Rahmen der BPD-Segmentfolge übermittelt werden. So ist beispielsweise anzugeben, welche Geschäftsvorfälle über PIN/TAN abgesichert werden dürfen und für welche davon eine TAN erforderlich ist. Des Weiteren werden hier Längenangaben für PIN und TAN sowie die kreditinstitutsspezifischen Belegungsvorschriften für Benutzerkennungs- und Kunden-ID-Felder in Textform übermittelt.

Hierfür existiert das Segment *Parameterdaten PIN/TAN*, welches die oben beschriebenen Daten aufnehmen kann. Die hier aufgeführten Geschäftsvorfälle dürfen vom Benutzer in über PIN/TAN abgesicherte Nachrichten eingestellt werden, sofern sie in den BPD und UPD als generell erlaubt hinterlegt sind. Alle übrigen Geschäftsvorfälle können mit dem PIN/TAN-Interface nicht verwendet werden.

Im Segment *SecurityMethodParam/OTPTransactions* können Parameterdaten abgelegt werden, die unabhängig vom verwendeten PIN/TAN-Verfahren gelten. So können Geschäftsvorfälle, die eine TAN über ein beliebiges PIN/TAN-Verfahren erfordern, dort abgelegt werden. Geschäftsvorfälle, die nur mit Zwei-Schritt-TAN-Verfahren zugelassen sind, werden im Segment *SecurityMethodParam/SupportedMethod/OTP/BusinessTransAllowed* aufgelistet.

Sollen die in [Formals], Abschnitt *III.7 Verteilte Signaturen* beschriebenen Abläufe auch mit dem PIN/TAN-Verfahren möglich sein, so müssen die zugehörigen Geschäftsvorfälle für die Abwicklung verteilter Signaturen im Segment *Parameterdaten PIN/TAN* hinterlegt sein. Auch die Geschäftsvorfälle, die verteilt signiert werden sollen, müssen dort hinterlegt sein.

II.8 Userparameterdaten zum PIN/TAN-Verfahren

Realisierung Kreditinstitut: verpflichtend, falls Geschäftsvorfälle mit PIN/TAN-Absicherung angeboten werden
Realisierung Kundenprodukt: optional

Bei Verwendung des PIN/TAN-Verfahrens werden dem Kundenprodukt in *UserParamData/GenericUserParam/AllowedSecurityMethod/OTP/fintstype:Option* die für ihn erlaubten Zwei-Schritt-TAN-Verfahren mitgeteilt.

II.9 Sicherheitstechnische Abläufe

Bei Verwendung des PIN/TAN-Verfahrens sind alternativ zu den in [HBCI] beschriebenen Signatur-Segmenten andere Segmente in die Nachricht einzustellen, die die für das PIN/TAN-Verfahren notwendigen Daten aufnehmen können. In einer Benutzernachricht ist dies ein Segment PIN/TAN-Signatur und in einer Kreditinstitutsnachricht ein Segment Antwort auf eine PIN/TAN-Signatur (siehe auch [Syntax]).

II.9.1 PIN/TAN-Signatur

Analog zu den in Kapitel [HBCI], Abschnitt *II.5.1 Signatur-Segment* beschriebenen Signaturen lassen sich die in PIN/TAN-Signatur-Segmenten enthaltenen Informationen in allgemeine und verfahrensspezifische Informationen aufteilen:

Zu den allgemeinen Informationen gehören:

- Rolle des Signierenden
- Zeitstempel

Zu den für PIN/TAN-spezifischen Informationen gehören:

- Kreditinstitutskennung
- Benutzerkennung
- Kundensystemkennung
- PIN (optional)
- TANs (optional; nur in Benutzernachrichten zulässig)
- Referenzen auf die über TAN abzusichernden Teile der FinTS-Nachricht
- Challenges (bei Zwei-Schritt-TAN-Verfahren)

♦ **Belegungsrichtlinien**

Rolle des Signierenden

Es gelten die gleichen Regeln wie in [HBCI], Abschnitt *II.5.1 Signatur-Segment* beschrieben.

Kundensystemkennung

Die Kundensystemkennung ist für das PIN/TAN-Verfahren optional. Sie kann verwendet werden, um eine eindeutige Identifizierung eines Dialogs im Rahmen der Synchronisierung der letzten Nachrichtennummer zu ermöglichen (siehe dazu Hinweistext in [Formals], Abschnitt *III.3 Synchronisierung*). Eine Kundensystemkennung kann wie im Sicherheitsverfahren HBCI mit einer Synchronisierungsnachricht angefordert werden.

TAN und Referenz

Zu jeder TAN ist in der Signatur eine Referenz enthalten. Die Referenz bezeichnet denjenigen Teil der Nachricht, auf den sich die TAN bezieht.

Bei der Verwendung der PIN/TAN-Signatur als Botensignatur bezieht sich die PIN implizit auf die gesamte Nachricht. Wenn eine TAN angegeben ist,

muss sie auf den kompletten Nachrichtenkörper mit allen Aufträgen bezogen sein.

Bei einer Verwendung als Auftragssignatur bezieht sich die PIN implizit auf alle Aufträge des Auftragsteils, die TANs müssen jeweils einem Auftrag des Auftragsteils zugeordnet sein.

Falls mehrere Aufträge in einer Nachricht transportiert werden, ist bei der Verwendung von TANs Folgendes zu bedenken:

Wenn nicht erwünscht ist, dass mehrere Aufträge mit derselben TAN versehen werden, ist die Angabe einer TAN in der Botensignatur nicht sinnvoll, denn diese bezieht sich per Definition auf alle enthaltenen Aufträge. Statt dessen werden die TANs im Rahmen einer oder mehrerer Auftragssignaturen angegeben.

Ist hingegen gewollt, dass mehrere Aufträge mit derselben TAN versehen werden, so besteht entweder die Möglichkeit, die TAN in der Botensignatur anzugeben und somit alle Aufträge mit dieser TAN zu signieren, oder aber in einer oder mehreren Auftragssignaturen die gleiche TAN mit Referenzen auf unterschiedliche Aufträge anzugeben und somit gezielt bestimmte Aufträge mit derselben TAN zu versehen.

II.9.2 Antwort auf eine PIN/TAN-Signatur

Mit dem Segment Antwort auf eine PIN/TAN-Signatur können vom Kreditinstitut PIN und TANs bestätigt und optional Bestätigungsnummern für verbrauchte TANs zurück gemeldet werden.

- PIN (optional)

♦ **Belegungsrichtlinien**

PIN

Hier kann die PIN aus der PIN/TAN-Signatur zurückgespiegelt werden.

II.9.3 Verschlüsselung im PIN/TAN-Verfahren

Im PIN/TAN-Verfahren ist eine Verschlüsselung nach kryptographischen Verfahren aus [HBCI] nicht möglich. Stattdessen ist zwischen Benutzer und Kreditinstitut beim Nachrichtentransport eine Transportverschlüsselung einzusetzen, um so den Inhalt der Nachrichten gegenüber Dritten zu schützen.

Es ist zu beachten, dass die zwischen Benutzer und Kreditinstitut ausgetauschten Nachrichten aus FinTS-Protokollsicht unverschlüsselt sind, obwohl eine personalisierte Kommunikation stattfindet. Dass die Nachrichten bei ihrem Transport transportverschlüsselt waren, kann ihnen nicht angesehen werden. Dennoch darf dies nicht zu einer Ablehnung der Nachrichten führen. Vielmehr ist eine unverschlüsselte Nachricht, die über einen transportverschlüsselten Kanal das Kundensystem bzw. das Kreditinstitut erreicht, immer wie eine Botenverschlüsselte Nachricht zu betrachten.

II.9.4 Komprimierung im PIN/TAN-Verfahren

Eine Komprimierung ist auch im PIN/TAN-Verfahren möglich, dafür werden die gleichen Mechanismen eingesetzt wie bei Komprimierung in Kombination mit Sicherheitsmechanismen nach [HBCI].

II.10 PIN/TAN-Management

Alle Geschäftsvorfälle zum PIN/TAN-Management enthalten explizit die Angabe eines Benutzers. Bei direkter Kommunikation eines Kunden mit dem Kreditinstitut muss mindestens eine PIN/TAN-Signatur dieses Benutzers als Herausgebersignatur (*II.9.1 PIN/TAN-Signatur* mit Rolle ISS) vorhanden sein, die sich auf diesen Auftrag bezieht. Die PIN ist dabei zwingend erforderlich, falls zusätzlich eine TAN verlangt wird, ist dies in der Beschreibung des Geschäftsvorfalls vermerkt. 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 [Formals], Abschnitt *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.


Da diese Geschäftsvorfälle in UPD und BPD aufgeführt sind (vgl. auch [Formals], Abschnitt *V. USER-PARAMETERDATEN (UPD)*, [Formals], Abschnitt *IV. BANKPARAMETERDATEN (BPD)*), kann das Kreditinstitut prinzipiell eine minimale Signaturanzahl von ‚0' für einen Geschäftsvorfall 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.

Details zum Aufbau der im Folgenden beschriebenen Geschäftsvorfälle finden sich in [Syntax].

Die Geschäftsvorfälle zum PIN/TAN-Management sollten vom Kundenprodukt immer in einem geschlossenen Kommunikationskontext, d. h. in separaten Nachrichten in einer separaten Kommunikation geschickt werden, da ansonsten eine gezielte Verarbeitung nicht gewährleistet werden kann und somit ein exaktes Wissen, ab wann z. B. eine PIN-Änderung gültig ist, nicht besteht.

Grundsätzlich werden alle vom Benutzer übermittelten TANs, wenn möglich, aus Sicherheitsgründen entwertet („verbrannt").

Damit der Benutzer Informationen darüber erhält, dass eine von ihm verwendete TAN aufgrund des Abbruchs der Verarbeitung eines Geschäftsvorfalles nicht verbraucht wurde, ist vom Kreditinstitut eine entsprechende Rückmeldung zu diesem Geschäftsvorfall zu erzeugen. Ist diese Rückmeldung eingestellt worden, kann vom Benutzer die gleiche TAN noch einmal verwendet werden.

Wird vom Kreditinstitut nicht gemeldet, dass die übermittelte TAN weiterhin gültig ist, muss die Benutzerseite davon ausgehen, dass die TAN verbraucht wurde. Dies gilt auch dann, wenn der zugehöri-

ge Geschäftsvorfall aufgrund von Fehlern nicht ausgeführt wurde.

II.10.1 Verwalten der Online-Banking-PIN

II.10.1.1 Online-Banking-PIN ändern

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional
XML-Schema ChangePIN-1.xsd

a) Benutzerauftrag

Dieser Geschäftsvorfall bewirkt das Ändern der Online-Banking-PIN (im Folgenden als „PIN“ bezeichnet). Zum Ändern der PIN ist im Segment PIN/TAN-Signatur die alte PIN und optional eine TAN erforderlich; der Geschäftsvorfall selbst enthält die neue PIN.

Folgende Ereignisse können Auslöser zum Ändern der PIN sein:

- Erstzugang zum Online-Banking – hier ist die vom Kreditinstitut vergebene Initial-PIN durch eine persönliche PIN zu ersetzen.

  Dazu wird bei der Initialisierung vom Kreditinstitut der Code 3916 („PIN muss wegen erstmaliger Anmeldung zwangsweise geändert werden“) zurück gemeldet. Der Benutzer muss als ersten Auftrag zwingend eine PIN-Änderung senden.

- Auf Wunsch des Benutzers
- Zwangsänderung bei Verdacht auf Kompromittierung

Die Abläufe zur Durchführung einer PIN-Änderung im Kontext der starken Kundenauthentifizierung befinden sich in den Abschnitten II.4.2.1.1 (Erstzugang) und II.4.2.1.2 (Zwangsänderung).

Hinweis: mit Einführung der starken Kundenauthentifizierung muss eine PIN-Änderung obligatorisch mit einer TAN authentifiziert werden. Hierzu muss der Geschäftsvorfall *PIN-Änderung* als TAN-pflichtig deklariert sein.

b) Kreditinstitutsrückmeldung

♦ **Erläuterungen**

Es werden keine Datensegmente zurückgemeldet.

♦ **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	PIN geändert
9942	neue PIN ungültig

c) Bankparameterdaten

Geschäftsvorfallspezifische Parameter existieren nicht.

Sperren der Online-Banking-PIN

Es ist zu unterscheiden zwischen Sperren, die vom Kreditinstitut automatisch durch eine mehrfach falsche Benutzereingabe veranlasst werden, und Sperren, die bewusst vom Benutzer initiiert werden.

II.10.1.2 Sperre bei mehrmaliger Falscheingabe

Bei jedem Erhalt einer falsch signierten Nachricht für einen noch nicht gesperrten Benutzer (z. B. falsche PIN oder ungültige TAN) wird der jeweilige Fehlbedienungszähler (PIN oder TAN) erhöht. Nach Überschreiten des vom Kreditinstitut vorgegebenen Wertes wird eine Sperre vorgenommen. Eine erfolgte Sperre wird dem Benutzer per Rückmeldungscode mitgeteilt.

Sofern das Kreditinstitut dies zulässt, ist bei Benutzer-initiierten Sperren eine Entsperrung mit Hilfe des Geschäftsvorfalls „PIN-Sperre aufheben“ (siehe *II.10.1.4 Online-Banking-PIN-Sperre aufheben*) möglich. Die Sperre hat in diesem Fall vorläufigen Charakter. Es wird der Rückmeldungscode **3**931 verwendet, damit ein Kundenprodukt für das Versenden der Entsperrung den Dialog weiterhin offen halten kann.

Falls die Sperre hingegen nur vom Kreditinstitut aufgehoben werden kann (endgültige Sperre), wird der Rückmeldungscode **9**931 verwendet

Der Umfang der Sperre ist kreditinstitutsabhängig und kann dem Benutzer im Rahmen der Rückmeldung detaillierter mitgeteilt werden.

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
3931	Vorläufige Sperre liegt vor. Entsperren mit GV „PIN-Sperre aufheben“ möglich
9931	Online-Zugang gesperrt, Entsperren nur durch Kreditinstitut
9931	SB-Zugang gesperrt, Entsperren nur durch Kreditinstitut
9931	Konto gesperrt, Entsperren nur durch Kreditinstitut
9931	PIN gesperrt, Entsperren nur durch Kreditinstitut

II.10.1.3 Online-Banking-PIN sperren

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional
XML-Schema BlockPIN-1.xsd

a) Benutzerauftrag

Dieser Geschäftsvorfall bewirkt eine Sperre durch den Benutzer. Der Umfang der Sperre ist kreditinstitutsabhängig und kann dem Benutzer im Rahmen der Rückmeldung detaillierter mitgeteilt werden. Benutzer-initiierte Sperren werden jedoch gängigerweise als vorläufige Sperren behandelt, da es dem Benutzer auch freistehen sollte z. B. während eines Urlaubs selbst seinen Online-Banking-Zugang zu sperren.

Das Sperren des Online-Banking-Zugangs durch den Benutzer erfordert analog zu den HBCI-RAH-Signaturverfahren die Eingabe einer gültigen PIN, selbst wenn diese kompromittiert sein sollte. Diese wird im Segment PIN/TAN-Signatur eingestellt.

Der Geschäftsvorfall selbst enthält keine weiteren Daten.

b) Kreditinstitutsrückmeldung

- **Erläuterungen**

  Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	PIN-Sperre erfolgreich
0020	Konto-Sperre erfolgreich
0020	Sperre erfolgreich. Zur Entsperrung wenden Sie sich bitte an Ihr Kreditinstitut

Code	Beispiel für Rückmeldungstext
3931	Vorläufige Sperre liegt vor. Entsperren mit GV „PIN-Sperre aufheben“ möglich

c) Bankparameterdaten

Geschäftsvorfallspezifische Parameter existieren nicht.

II.10.1.4 Online-Banking-PIN-Sperre aufheben

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional
XML-Schema RevokePINBlock-1.xsd

a) Benutzerauftrag

Dieses Segment bewirkt das Aufheben einer PIN-Sperre. Wurde eine Online-Sperre auf ein Konto gelegt (z. B. durch mehrmalige Eingabe einer falschen PIN), kann das Konto durch die Eingabe der richtigen PIN und einer gültigen TAN wieder entsperrt werden (PIN und TAN befinden sich im Segment PIN/TAN-Signatur).

Der Geschäftsvorfall selbst enthält keine weiteren Daten.

Da bei gesperrter PIN im Regelfall keine weitere Kommunikation möglich ist, kann dieser Geschäftsvorfall nur angeboten werden, wenn das Kreditinstitut nach einer PIN-Sperre weitere Kommunikationen mit der gesperrten PIN zulässt, sofern in diesen nur der Geschäftsvorfall „PIN-Sperre aufheben“ gesendet wird. Siehe dazu auch *II.10.1.2 Sperre bei mehrmaliger Falscheingabe*.

In der Regel wird kreditinstitutsseitig nur ein einziger Versuch zur Aufhebung der PIN-Sperre zugelassen. Schlägt dieser fehl, kann nur das Kreditinstitut entsperren.

b) Kreditinstitutsrückmeldung

- **Erläuterungen**

  Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	PIN-Sperre aufgehoben

c) Bankparameterdaten

Geschäftsvorfallspezifische Parameter existieren nicht.

II.10.1.5 Online-Banking-PIN prüfen

Um eine PIN prüfen zu lassen, wird dem Benutzer kein spezieller Geschäftsvorfall bereitgestellt. Vielmehr ist diese PIN-Prüfung innerhalb der Initialisierung implizit vom Kreditinstitut durchzuführen. Der Benutzer hat somit analog zu *0*

TAN prüfen und „verbrennen“ die Möglichkeit, eine Initialisierungsnachricht ohne Auftragsteil zu senden. Die PIN wird dann an das Kreditinstitut übermittelt und kann dort geprüft werden. Die Ergebnisse der Prüfung werden vom Kreditinstitut als zusätzliche Returncodes innerhalb der Initialisierungsantwort zurückgemeldet.

♦ **mögliche Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0901	PIN gültig
9942	PIN ungültig

II.10.2 Management chipTAN, mobileTAN und bilaterale Verfahren

II.10.2.1 TAN-Verbrauchsinformationen anzeigen #2

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional
XML-Schema TANDisplay-2.xsd

a) Benutzerauftrag

Dieses Segment bewirkt die Anzeige der verbrauchten TANs des Benutzers für einen bestimmten Zeitraum.

Der Geschäftsvorfall selbst enthält keine weiteren Daten.

♦ **Belegungsrichtlinien**

Gültig ab, Gültig bis

Die übliche Angabe im Format JJMM muss in diesem Fall auf ein existierendes Datumsformat umgesetzt werden (z. B. Gültig bis „9912“ wird umgesetzt in „19991231“).

b) Kreditinstitutsrückmeldung

♦ **Beschreibung**

Das Response-Segment enthält für den gewählten Zeitraum eine DEG mit den zugehörigen Informationen. Diese umfassen mindestens das TAN-Verbrauchskennzeichen. Jeweils optional können darüber hinaus die TANs und nähere Informationen zu den TANs selbst enthalten sein.

♦ **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	Auftrag ausgeführt

c) Bankparameterdaten

Name: TAN-Verbrauchsinformationen anzeigen Parameter
Tagname: *TANListDisplay_2_Par*

II.10.2.2 Anzeige der verfügbaren TAN-Medien #4 und #5

Bei Segmentversion #5 wird gegenüber der Vorgängerversion #4 in der Kundennachricht durch das Datenelement *TAN-Medium-Klasse #4* die Unterstützung von bilateral vereinbarten Verfahren möglich.

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional
XML-Schema DisplayTANGeneratorList-4.xsd
DisplayTANGeneratorList-5.xsd

a) Benutzerauftrag

Dem Benutzer wird eine Übersicht über seine verfügbaren TAN-Medien für chipTAN und mobileTAN angezeigt.

Der Kunde muss auch im Hinblick auf das TAN-Zwei-Schritt-Verfahren wissen, welches Medium er verwenden darf. Hierzu werden ihm seine verfügbaren Medien (Kartennummern bzw. Telefonbezeichnungen) mit ihrem aktuellen Status angezeigt. Es wird dahingehend unterschieden, ob das Medium „Verfügbar“ oder „Aktiv“ ist. Folgekarten werden bei TAN-Generatoren separat mit eigenen Kennzeichen versehen, da mit der „Aktivierung“ der Folgekarte die aktuelle Karte für die TAN-Generierung gesperrt wird.

Status	Erläuterungen
Verfügbar	Das Medium kann genutzt werden, muss aber zuvor folgendermaßen aktiv gemeldet werden: TAN-Generator: mit *TAN-Generator an- bzw. ummelden* Mobiltelefon mit *Mobilfunkverbindung freischalten*
Aktiv	Das Institut zeigt an, dass es eine TAN-Prüfung gegen dieses Medium vornimmt.
Verfügbare Folgekarte	Das Medium kann mit dem Geschäftsvorfall *TAN-Generator an- bzw. ummelden* aktiv gemeldet werden. Die aktuelle Karte kann dann nicht mehr genutzt werden.
Aktiv Folgekarte	Mit der ersten Nutzung der Folgekarte wird die zurzeit aktive Karte gesperrt.

Anmerkung: Wenn ein Institut mehrere Medien in dem Status „Aktiv“ verwalten kann, dann muss beim Zwei-Schritt-Verfahren dem Institut zuvor mit dem Geschäftsvorfall *TAN-Medium an- bzw. ummelden* mitgeteilt werden, welches Medium für die Signatur des Geschäftsvorfalles verwendet werden soll.

b) Kreditinstitutsrückmeldung

- **Erläuterungen**

  Es wird ein Datensegment zurückgemeldet.

- **Belegungsrichtlinien**

  TAN-Medium-Liste

  Darf nur belegt werden, wenn für den Kunden ein TAN-Medium verfügbar / nutzbar ist.

  Beim mobileTAN-Verfahren (TAN-Medium-Klasse=“M“) muss entweder das Datenelement „Mobiltelefonnummer“ oder „Mobiltelefonnummer verschleiert“ angegeben werden.

  Bei bilateral vereinbarten Verfahren (TAN-Medium-Klasse=“B“) muss das Datenelement *Option* angegeben werden. Die *Option* beinhaltet den Wert für das bilateral vereinbarte Verfahren in der DEG *SecurityMethodParam*.

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	Auftrag verarbeitet

c) Bankparameterdaten

Geschäftsvorfallspezifische Parameter existieren nicht.

II.10.2.3 TAN-Medium an- bzw. ummelden #2 und #3

Bei Segmentversion #3 wird gegenüber der Vorgängerversion #2 in der Kundennachricht durch das Datenelement *TAN-Medium-Klasse #4* die Unterstützung von bilateral vereinbarten Verfahren möglich.

Realisierung Kreditinstitut:	verpflichtend, wenn chipTAN unterstützt wird
Realisierung Kundenprodukt:	optional
XML-Schema	ChangeTANGenerator-2.xsd ChangeTANGenerator-3.xsd

a) Benutzerauftrag

Mit Hilfe dieses Geschäftsvorfalls kann der Benutzer seinem Kreditinstitut mitteilen, welches Medium (Chipkarte, TAN-Generator oder bilateral vereinbart) er für die Autorisierung der Aufträge per TAN verwenden wird.

Welches Medium gerade aktiv ist, kann mit Hilfe des Geschäftsvorfalls *TAN-Medium anzeigen Bestand* bzw. für Detailinformationen zur Karte auch *Kartenanzeige anfordern* (siehe [Messages], *Abschnitt III.6.2*) durch den Kunden erfragt werden.

Der Kunde entscheidet selbst, welches seiner verfügbaren TAN-Medien er verwenden möchte.

chipTAN-Verfahren:
Steht beim chipTAN-Verfahren ein Kartenwechsel an, so kann der Kunde mit diesem Geschäftsvorfall seine Karte bzw. Folgekarte aktivieren. Kann der Kunde mehrere Karten verwenden, dann kann mit diesem GV die Ummeldung auf eine andere Karte erfolgen. Das Kreditinstitut entscheidet selbst, ob dieser GV TAN-pflichtig ist oder nicht.

♦ **Belegungsrichtlinien**

Gültig ab, Gültig bis

Die übliche Angabe im Format JJMM muss in diesem Fall auf ein existierendes Datumsformat umgesetzt werden (z. B. Gültig bis „9912“ wird umgesetzt in „19991231“).

Kartenart

Die Eingabe der Kartenart wird über den BPD-Parameter *Eingabe Kartenart zulässig* gesteuert. Ist dieser Parameter auf *J* gesetzt, enthält das BPD-Segment auch die DEG *gültige Kartenarten*.

b) Kreditinstitutsrückmeldung

♦ **Erläuterung**

Allgemeine Kreditinstitutsnachricht ohne Datensegmente

♦ **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	An- bzw. Ummeldung erfolgreich
9935	An- bzw. Ummeldung fehlgeschlagen

Code	Beispiel für Rückmeldungstext
9935	Kartennummer unbekannt
9935	Karte als TAN-Medium nicht zugelassen – bitte wenden Sie sich an Ihr Institut

c) Bankparameterdaten

Name: TAN-Medium an-/ummelden Parameter
Tagname: *ChangeTANGenerator_2_Par*
ChangeTANGenerator_3_Par

II.10.2.4 TAN-Generator Synchronisierung

Realisierung Kreditinstitut: verpflichtend, wenn chipTAN unterstützt wird
Realisierung Kundenprodukt: optional
XML-Schema SynchronizeTANGenerator-1.xsd

a) Benutzerauftrag

Mit diesem Geschäftsvorfall ist eine explizite Synchronisierung eines TAN-Generators nach chipTAN-Standard [HHD] möglich. Im Regelfall erfolgt die Synchronisierung implizit, d. h. das Hintergrundsystem führt aufgrund eines Vergleichs des in der TAN übermittelten Zählers (ATC) und des hintergrundseitig geführten Zählers eine automatische Synchronisierung durch. Falls aufgrund eines zu starken Divergierens dieser beiden Zähler eine implizite Synchronisierung nicht mehr möglich ist, muss der Kunde eine explizite Synchronisierung veranlassen.

Um die Synchronisierung durchführen zu können, muss der Kunde den aktuellen ATC im TAN-Generator zur Anzeige bringen und zusammen mit der zugehörigen TAN an das Kreditinstitut übermitteln. Diese TAN wird zusammen mit der PIN im Segment *PIN/TAN-Signatur* übertragen.

Da bei der vierten Falscheingabe der TAN-Generator kreditinstitutsseitig gesperrt wird, sollte das Kundenprodukt den Kunden spätestens nach der dritten Ablehnung einer TAN zu einer expliziten Synchronisierung auffordern, da in diesem Fall zu vermuten ist, dass der Fehler nicht auf einer Falscheingabe des Kunden, sondern auf einem Synchronisierungsproblem beruht.

b) Kreditinstitutsrückmeldung

- **Erläuterung**

  Allgemeine Kreditinstitutsnachricht ohne Datensegmente

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	Synchronisierung erfolgreich
3931	TAN-Generator gesperrt, Synchronisierung erforderlich
3933	TAN-Generator gesperrt, Synchronisierung erforderlich Kartennummer ##########
9931	TAN-Generator gesperrt
9931	Online-Zugang gesperrt

c) Bankparameterdaten

Name: TAN-Generator Synchronisierung
Tagname: *SynchronizeTANGenerator_1_Par*

II.10.2.5 Mobilfunkverbindung registrieren #2 und #3

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional
XML-Schema RegisterMobilePhoneConnection-2.xsd,
RegisterMobilePhoneConnectionNoFee-2.xsd
RegisterMobilePhoneConnection-3.xsd,
RegisterMobilePhoneConnectionNoFee-3.xsd

a) Benutzerauftrag

Mit diesem Geschäftsvorfall kann ein Kunde seine Mobilfunkverbindung registrieren.


Dieser Geschäftsvorfall kann auch mit der Bezeichnung *Mobilfunkverbindung registrieren ohne Entgelte* verwendet werden. Damit ist es möglich, den Geschäftsvorfall mit unterschiedlicher Belegung des Parameters *Abbuchungskonto erforderlich* in der BPD zur Verfügung zu stellen und damit über die UPD eine kundenspezifische Abrechnung der SMS-Kosten zu erreichen.

Die Segmentversion #3 beinhaltet gegenüber der #2 das Element *TAN-Medium-Klasse* zur Unterstützung von bilateral vereinbarten Verfahren.

♦ **Belegungsrichtlinien**

Mobiltelefonnummer

Es muss die Mobiltelefonnummer verwendet werden, die mit dem Institut für die Nutzung von mobileTAN vereinbart ist. Es sind nur Ziffern inklusive führender Nullen erlaubt und es gilt die nationale Schreibweise für Telefonnummern, z. B. 0170/1234567 oder (0170) 1234567.

Das Kundensystem sollte den Kunden bei der Eingabe eines korrekten Telefonnummern-Formates unterstützen.

Falls der Prozess vorsieht, dass die Registrierung der Mobiltelefonnummer zuvor auf alternativem Weg erfolgen muss, können nur im Vorfeld vereinbarte Rufnummern verwendet werden. Das Institut muss in diesem Fall die Existenz einer entsprechenden Vereinbarung prüfen.

b) Kreditinstitutsrückmeldung

- **Erläuterungen**

  Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	Auftrag verarbeitet
9939	MobileTAN-Mobilrufnummer nicht zur Registrierung zugelassen
9939	Format der mobileTAN-Mobilrufnummer nicht korrekt
9939	MobileTAN-Mobilrufnummer bereits registriert

c) Bankparameterdaten

Name: Mobilfunkverbindung registrieren Parameter
Tagname: *RegisterMobilePhoneConnection_2_Par*
RegisterMobilePhoneConnectionNoFee_2_Par
RegisterMobilePhoneConnection_3_Par
RegisterMobilePhoneConnectionNoFee_3_Par

II.10.2.6 Mobilfunkverbindung freischalten #2 und #3

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional
XML-Schema ActivateMobilePhoneConnection-2.xsd
ActivateMobilePhoneConnection-3.xsd

a) Benutzerauftrag

Mit Hilfe dieses Geschäftsvorfalls kann ein Kunde seine zuvor registrierte Mobilfunkverbindung freischalten.

Die Segmentversion #3 beinhaltet gegenüber der #2 das Element *TAN-Medium-Klasse* zur Unterstützung von bilateral vereinbarten Verfahren (vergleiche [Syntax], Abschnitt III.7.4 *PIN/TAN*).

b) Kreditinstitutsrückmeldung

- **Erläuterungen**

  Es werden keine Datensegmente zurückgemeldet.

- **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	Mobiltelefon für mobileTAN freigeschaltet
9939	mobileTAN-Mobilrufnummer kann nicht freigeschaltet werden
3939	mobileTAN-Freischaltung erforderlich. SMS-Freischaltcode wurde versendet

c) Bankparameterdaten

Geschäftsvorfallspezifische Parameter existieren nicht.

II.10.2.7 Mobilfunkverbindung ändern #2 und #3

Realisierung Kreditinstitut:	optional
Realisierung Kundenprodukt:	optional
XML-Schema	ChangeMobilePhoneConnection-2.xsd, ChangeMobilePhoneConnectionNoFee-2.xsd ChangeMobilePhoneConnection-3.xsd, ChangeMobilePhoneConnectionNoFee-3.xsd

a) Benutzerauftrag

Mit Hilfe dieses Geschäftsvorfalls kann ein Kunde seine Mobilfunkverbindung bzw. die damit verbundenen Informationen ändern.

Dieser Geschäftsvorfall kann auch mit der Bezeichnung *Mobilfunkverbindung ändern ohne Entgelte* verwendet werden. Damit ist es möglich, den Geschäftsvorfall mit unterschiedlicher Belegung des Parameters *Abbuchungskonto erforderlich* in der BPD zur Verfügung zu stellen und damit über die UPD eine kundenspezifische Abrechnung der SMS-Kosten zu erreichen.

Die Segmentversion #3 beinhaltet gegenüber der #2 das Element *TAN-Medium-Klasse* zur Unterstützung von bilateral vereinbarten Verfahren (vergleiche [Syntax], Abschnitt III.7.4 *PIN/TAN*).

♦ **Belegungsrichtlinien**

Bezeichnung des TAN-Mediums alt

Es muss die vereinbarte Bezeichnung einer bestehenden und frei geschalteten Mobiltelefonnummer verwendet werden.

b) Kreditinstitutsrückmeldung

♦ **Erläuterungen**

Es werden keine Datensegmente zurückgemeldet.

♦ **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	Auftrag verarbeitet
9939	MobileTAN-Mobilrufnummer nicht zur Registrierung zugelassen
9939	Format der mobileTAN-Mobilrufnummer nicht korrekt
9939	MobileTAN-Mobilrufnummer bereits registriert
9939	alte mobileTAN-Mobilfunknummer existiert nicht oder ist nicht freigeschaltet

c) Bankparameterdaten

Name: Mobilfunkverbindung ändern Parameter
Tagname: *ChangeMobilePhoneConnection_2_Par*
ChangeMobilePhoneConnectionNoFee_2_Par
ChangeMobilePhoneConnection_3_Par
ChangeMobilePhoneConnectionNoFee_3_Par

II.10.2.8 Deaktivieren / Löschen von TAN-Medien #1 und #2

Realisierung Kreditinstitut: optional
Realisierung Kundenprodukt: optional
XML-Schema DeactivateDeleteTANMedium-1.xsd
DeactivateDeleteTANMedium-2.xsd

a) Benutzerauftrag

Mit Hilfe dieses Geschäftsvorfalls kann ein Kunde ein aktives bzw. verfügbares TAN-Medium deaktivieren oder löschen.

Deaktivieren, bewirkt eine Statusänderung von „aktiv“ nach „verfügbar“ für das gewählte TAN-Medium.

Beim Löschvorgang wird das entsprechende TAN-Medium gänzlich von der Liste der TAN-Medien genommen. Dieser Vorgang kann nicht mehr rückgängig gemacht werden.

♦ **Belegungsrichtlinien**

TAN-Medium-Klasse

Es muss die zu deaktivierende / zu löschende TAN-Medium-Klasse angegeben werden. Bei Angabe von TAN-Medium-Klasse“G“ wird die als aktiv definierte Kombination aus TAN-Generator und Karte gelöscht bzw. deaktiviert. Bei TAN-Medium-Klasse=„M“ muss die Angabe der Bezeichnung des TAN-Mediums erfolgen.

Das Kundensystem sollte den Kunden darauf hinweisen, wenn er versuchen will, das letzte im Bestand des Kundensystems bekannte TAN-Medium zu deaktivieren oder zu löschen.

Die Segmentversion #2 beinhaltet gegenüber der #1 das Element TAN-Medium-Klasse zur Unterstützung von bilateral vereinbarten Verfahren (vergleiche [Syntax], Abschnitt III.7.4 PIN/TAN).

b) Kreditinstitutsrückmeldung

♦ **Erläuterungen**

Es werden keine Datensegmente zurückgemeldet.

♦ **Ausgewählte Beispiele für Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0020	Auftrag verarbeitet
9958	Deaktivieren / Löschen für TAN-Medium nicht möglich
9958	TAN-Medium nicht bekannt

c) Bankparameterdaten

Geschäftsvorfallspezifische Parameter existieren nicht.

II.10.2.9 TAN prüfen und „verbrennen“

Um eine TAN prüfen und verbrennen zu lassen, wird dem Benutzer kein spezieller Geschäftsvorfall bereitgestellt. Vielmehr hat er die Möglichkeit, in einer Initialisierungsnachricht ohne Auftragsteil neben der PIN zusätzlich auch eine TAN mitzuschicken. Diese wird an das Kreditinstitut übermittelt und kann dann von diesem geprüft und entwertet werden. Die Ergebnisse der Prüfung und des Verbrennens werden vom Kreditinstitut als zusätzliche Returncodes innerhalb der Initialisierungsantwort zurückgemeldet.

- **mögliche Rückmeldungscodes**

Code	Beispiel für Rückmeldungstext
0900	TAN gültig
9941	TAN ungültig
3913	TAN wurde verbraucht