FinTS PIN/TAN inkl. Zwei-Schritt-Verfahren, Rel. 2005-06-21
- Befundliste -

	FinTS PIN/TAN V3.0 mit Zwei-Schritt-Verfahren (Final Version)						
lfd. Nr.	**Beschreibung**	**Kapitel**	**Seite**	**Art**	**durch**	**Kommentar**	**Status**
1	Es sollte vermieden werden, dass bei dem dargestellten Prozess ein Zwischenschritt mit HKTAN, TP=3 benötigt wird	B.2.1.2.1	S.20	E	Finanz_ IT	Es wird ein zusätzlicher Ablauf definiert, der diesen Zwischenschritt einspart. Dabei es sollte nicht die Reihenfolge der Signaturblöcke zur Steuerung verwendet werden.	angenommen
2	„Die für den Kunden zugelassenen Geschäftsvorfälle HIPINS, HKTAN und die Geschäftsvorfälle für das PIN/TAN-Management sind im Segment HIUPD mitzuteilen." Beim Segment HIPINS handelt es sich um keinen Geschäftsvorfall (da es u.a. kein HKPIN-Segment gibt). Er sollte daher auch nicht im HIUPD-Segment genannt werden.	B.1	S.13 6.SP	F	PPI	Fehler wird behoben	angenommen
3	Bei Prozessvariante 1 darf der Parameter „Auftrags-Hashwertverfahren" in HITANS nicht mit „0" (nicht unterstützt) belegt werden! Diese Voraussetzung sollte jeweils in den Ausgangszustand der Ablaufbeschreibungen aufgenommen werden. Außerdem sollte dieser Hinweis auch im Data Dictionary bei der DE „Auftrags-Hashwertverfahren" aufgenommen werden.	B.2.1.1 + B.2.1.1.1	S.16 + S.17	K	PPI	Klarstellung wird eingefügt. Betroffen ist auch TAN-Prozess 4 (siehe Punkt 30)	angenommen

FinTS PIN/TAN inkl. Zwei-Schritt-Verfahren, Rel. 2005-06-21
- Befundliste -

lfd. Nr.	Beschreibung	Kapitel	Seite	Art	durch	Kommentar	Status
5	„Ablauf bei synchroner Eingabe von Mehrfach-TANs mit Prozessvariante 1“: Es ist unklar, ob alle Benutzer dasselbe konkrete Zwei-Schritt-Verfahren benutzen müssen oder ob jeder Benutzer ein anderes konkretes Verfahren derselben Prozessvariante nutzen darf. Die Auftragseinreichung (Schritt 4a) würde im letzteren Fall drei Signaturköpfe mit unterschiedlichen Belegungen der DE „Sicherheitsfunktion, kodiert“ enthalten (z.B. 1. Benutzer = 991, 2. Benutzer = 992, 3. Benutzer = 993). Ist das so gewollt? Falls ja, dann könnte auch die Restriktion „Alle Benutzer müssen dasselbe konkrete Zwei-Schritt-Verfahren verwenden“ in Kapitel B.2.1.2.1 (auf Seite 20) entfallen.	B.2.1.1.1	S.17	#	PPI	Die Restriktion „Alle Benutzer müssen dasselbe konkrete Zwei-Schritt-Verfahren verwenden“ in Kapitel B.2.1.2.1 (auf Seite 20) kann entfallen.	angenommen
7	„Ablauf bei zeitversetzter Eingabe von Mehrfach-TANs mit Prozessvariante 2, dialogübergreifend“: Die Beschreibung des Ausgangszustands (3. Spiegelpunkt) ist nicht richtig: „Die Dialoginitialisierung ist erfolgt; der erste Benutzer hat dort durch entsprechende Belegung des DE „Sicherheitsfunktion, kodiert“ ein konkretes Zwei-Schritt-Verfahren für den *ersten* Dialog gewählt *und damit die Prozessvariante für den gesamten Ablauf festgelegt* .“	B.2.1.2.2	S.22	K	PPI	Es erfolgt eine Korrektur dahingehend, dass eine Mischung der Verfahren zulässig ist	in Arbeit
8	„Initialisierungsprozess bei Einsatz der Banken-Signatur bei HITAN“, Schritt 2: In einer anonymen Dialoginitialisierung kann aufgrund des fehlenden Signaturkopfes HNSHK eine Belegung mit Sicherheitsprofil „PIN-1“ und „Sicherheitsfunktion kodiert“=“999“ nicht erfolgen. Der Teilsatz „mit Sicherheitsprofil PIN-1 und Sicherheitsfunktion, kodiert=999 für Einschrittverfahren“ ist daher zu streichen.	B.2.1.3	S.24	F	PPI	Fehler wird behoben. Grund: bei anonymer Dialoginitialisierung existiert kein Signaturkopf	in Arbeit

FinTS PIN/TAN inkl. Zwei-Schritt-Verfahren, Rel. 2005-06-21
- Befundliste -

lfd. Nr.	Beschreibung	Kapitel	Seite	Art	durch	Kommentar	Status
10	Rückmeldungscode 3920: Laut Beschreibung ist das Ein-Schritt-Verfahren nicht mehr nur institutsweit über das Parametersegment HITANS (DE „Einschritt-Verfahren erlaubt“) konfigurierbar, sondern für jeden Benutzer über die „zugelassenen Zwei-Schritt-Verfahren für den Benutzer“. Leider stimmt somit die Überschrift zum Rückmeldungscode 3920 nicht mehr mit den Inhalten überein.	B.3.1	S.34	K	PPI	Klarstellung: "zugelassene Verfahren für den Benutzer (Ein- und Zwei-Schritt)"	angenommen
12	„TAN-Liste freischalten im Zwei-Schritt-Verfahren mit Prozessvariante 1“: Aus der Beschreibung wird nicht deutlich, dass für die TAN aus der alten TAN-Liste eine Challenge per HKTAN mitBelegung gemäß TAN-Prozess=1 angefordert werden muss. Der in diesem Schritt eingereichte Auftrags-Hashwert des Segments HKTLF muss bereits die TAN aus der neuen TAN-Liste und die neue TAN-Listennummer umfassen.	B.7.1.3.1. 1	S.46	K	PPI	Es wird eine entsprechende Klarstellung erfolgen	angenommen
13	„TAN-Liste freischalten im Zwei-Schritt-Verfahren mit Prozessvariante 2“, Grauer Kasten: Zum besseren Verständnis für den Kunden, soll bei TAN-Prozess=2 in HITAN die zu verwendende TAN-Listennummer angegeben werden. Ist hier vielleicht die Prozessvariante 2 gemeint?! Bei der Auftragseinreichung und beim Senden der Challenge für die TAN aus der alten Liste werden HKTAN und HITAN aber gemäß TAN-Prozess=4 belegt (d.h. ohne TAN-Listennummer)!	B.7.1.3.1. 2	S.47	K	PPI	Korrektur: Es muss 'Prozess-Variante' heissen	angenommen
15	DE „Maximale Länge des TAN-Eingabewertes im Zwei-Schritt-Verfahren“ und C, S. 81, DEG „Verfahrensparameter Zwei-Schritt-Verfahren“: Bei der DE „Maximale Länge des TAN-Eingabewertes im Zwei-Schritt-Verfahren“ müsste die Längenangabe „..2“ (statt „2“) sein.	C	S.68	F	PPI	Der Fehler wird behoben	angenommen

FinTS PIN/TAN inkl. Zwei-Schritt-Verfahren, Rel. 2005-06-21
- Befundliste -

lfd. Nr.	Beschreibung	Kapitel	Seite	Art	durch	Kommentar	Status
16	DE „Maximale Länge des Rückgabewertes im Zwei-Schritt-Verfahren“ und C, S. 81, DEG „Verfahrensparameter Zwei-Schritt-Verfahren“: Bei der DE „Maximale Länge des Rückgabewertes im Zwei-Schritt-Verfahren“ müsste die Längenangabe „..3“ (statt „3“) sein.	C	S.68	F	PPI	Der Fehler wird behoben	angenommen
17	DE „Mehr als ein TAN-pflichtiger Auftrag pro Nachricht erlaubt“ und C, S. 70, DEG „Parameter Zwei-Schritt-TAN-Einreichung“: Die DE „Mehr als ein TAN-pflichtiger Auftrag pro Nachricht erlaubt“ steht im Widerspruch zu den Aussagen in dem ersten grauen Kasten auf Seite 42 („..., dass eine Nachricht entweder nur einen einzelnen Geschäftsvorfall enthält für den eine TAN erforderlich ist, oder nur solche Geschäftsvorfälle, für die keine TAN erforderlich ist“). Außerdem ist unklar, wie bei mehr als einem TAN-pflichtigen Auftrag pro Nachricht eine Zuordnung der TANs in den Signaturabschlüssen bzw. der HKTANs/HITANs zu den Aufträgen erfolgen soll.	C	S.69	#	PPI	S. 42 bezieht sich auf PIN/TAN-Management - eine weitere Spezifikation erfolgt nicht. Es besteht die Forderung, den Parameter generell zu entfernen (siehe Punkt 44)	in Arbeit
18	DE „Sicherheitsfunktion, kodiert“: In der Spalte „Segment“ der Tabelle müsste statt „Rückmeldungsparameter Px“ besser „Verfahrensparameter Zwei-Schritt-Verfahren“ stehen. Sollte sich die Anmerkungen auf die Rückmeldungsparameter beim Rückmeldungscode 3290 beziehen, dann ist die Angabe „Px“ (mit x=1..98) falsch, da maximal 10 Parameter angegeben werden können.	C	S.74	F	PPI	Der Fehler wird behoben; es sind nur die Parameter P1 bis P9 möglich, keine 98.	angenommen
21	Die Beispieldialoge in den Anlagen verwenden für die Segmente HNSHK und HNVSK die falschen Segmentversionen (nämlich die aus HBCI 2.2). Daher fehlt in den Beispieldialogen auch die DEG „Sicherheitsprofil“.	D.3	S.85	F	PPI	Der Fehler wrid behoben: Fehler bestand bereits in der Original FinTS V3.0	angenommen

FinTS PIN/TAN inkl. Zwei-Schritt-Verfahren, Rel. 2005-06-21
- Befundliste -

lfd. Nr.	Beschreibung	Kapitel	Seite	Art	durch	Kommentar	Status
23	Es fehlt ein Hinweiskasten, dass das Zwei-Schritt-Verfahren unter HBCI 2.2 „analog“ umgesetzt werden kann und soll.			K	PPI	Ist Inhalt der "Festlegungen zum PIN/TAN-Interface mit Zwei-Schritt-Verfahren", das beim SIZ erhältlich ist	angenommen
24	Wie soll bei Prozessvariante 2 (Schritt 2b bei Einfach-TAN bzw. Schritt 4b bei Mehrfach-TAN) in den Antwortnachrichten und Rückmeldungen auf das Auftragssegment die DE „Bezugssegment“ (Segmentnummer des Auftragssegments in der Kundennachricht) belegt werden? Bislang bezieht sich das Bezugssegment immer auf die unmittelbar vorausgehende Nachricht! Durch den Abläufe bei Prozessvariante 2 wird die Auftragsnachricht aber nicht unmittelbar vorher geschickt, sondern ggf. sogar in einem anderen Dialog. Der Kernel benötigt diese Information für die Zuordnung der Rückmeldungen zu den Aufträgen.	B.2.1.2 + B.2.1.2.1	S.19 + S.21	K	PPI	siehe auch Punkt Nr. 37. Die Aufträge sollten unter einer 'Auftragsreferenz' abgelehnt werden. Das Bezugssegment kann aus den beschriebenen Gründen nicht verwendet werden.	angenommen
27	Übersicht Nachrichtenaufbau: Bei Unterstützung der Banken-Signatur muss der Kunde in die Dialoginitialisierung (mindestens) ein HKISA-Segment einstellen und in der Antwortnachricht erhält er 0-2 HIISA-Segmente zurück.	D.2	S. 84	E	PPI	Klarstellung in der Tabelle D.2 erfolgt	angenommen
28	Banken-Signatur: Soll die Banken-Signatur auch in Verbindung mit den Abläufen bei Mehrfach-TANs unterstützt werden?	B.2.1.3	S.23	K	PPI	Klarstellung: es wird eine entsprechende Anmerkung im Kapitel Bankensignatur eingefügt	angenommen
29	Optionale Banken-Signatur bei HITAN und Prozessvariante 2: Klarstellung, dass in Schritt 1b ein HITAN mit Belegung gemäß TAN-Prozess=4 gesendet wird.	B.2.1.3	S.26	K	PPI	Klarstellung: es wird ergänzt, dass es sich um TAN-Prozess=4 handelt.	angenommen

FinTS PIN/TAN inkl. Zwei-Schritt-Verfahren, Rel. 2005-06-21
- Befundliste -

lfd. Nr.	Beschreibung	Kapitel	Seite	Art	durch	Kommentar	Status
30	Segmentbeschreibung HITAN: Die DE „Auftrags-Hashwert“ muss auch bei TAN-Prozess=4 belegt werden dürfen (vgl. optionale Banken-Signatur bei HITAN und Prozessvariante 2). Die Belegungsrichtlinie sollte ergänzt werden, dass bei optionaler Banken-Signatur bei Prozessvariante 2 bei der Auftragseinreichung (Schritt 1b) der Auftrags-Hashwert vom Institut zu berechnen ist.	B.2.3	S.31	#	PPI	Klarstellung: Entfernen des TAN-Prozess=4 aus der Bedingung (Conditional). Die Belegungsrichtlinie wird entsprechend erweitert.	angenommen
31	Zeitüberwachung bei synchroner Eingabe von Mehrfach-TANs: Der zweite Teilsatz „Das Zeitfenster muss berücksichtigen, dass zwei oder drei Benutzer in separaten Dialogen eine Challenge erhalten und die daraus resultierenden TANs in einem abschließenden Dialog des letzen Benutzers zur Auftragseinreichung synchron übertragen (vgl. Kapitel B.2.1).“ bezieht sich eindeutig und ausschließlich auf die TAN-Prozessvariante 1. Eine synchrone Eingabe von Mehrfach-TANs kann es nun aber auch bei TAN-Prozessvariante 2 geben. Insoweit sollte der Teilsatz entfernt oder umformuliert werden.	B.2.2.3.1	S.28	F	PPI	Korrektur: Der Teilsatz wird entfernt, der gesamte Absatz etwas abstrahiert, da es sich nicht um Inhalt der Spezifikation handelt.	angenommen
33	Klarstellung, dass es nicht vorgesehen ist, das die Prozesse überlappend laufen. Falls ja, wird ggf. nur der letzte Auftrag ausgeführt und die anderen TANs entwertet.	B.1	S. 14	K	SI	Klarstellung, dass alle Prozesse nur exakt wie beschrieben umzusetzen sind. Eigene Derivate sind nicht erlaubt.	angenommen
34	Es muss bei HKTLF möglich sein, in allen Fällen aus mehreren freizuschaltenden TAN-Listen wählen zu können.	B.7.1.3	S. 48	E	Finanz_ IT	Der Punkt ist noch unklar und wird durch das SIZ geprüft.	in Arbeit
35	Ergänzen eines neuen Verbrauchskennzeichens 12: "TAN verbraucht durch Falscheingabe", wenn ein Kunde eine Index-Anfrage falsch beantwortet	D	S. 77	E	SI	Erweiterung: Ergänzen weiterer TAN-Verbrauchskennzeichen für IZV, AZV, …	angenommen

FinTS PIN/TAN inkl. Zwei-Schritt-Verfahren, Rel. 2005-06-21
- Befundliste -

lfd. Nr.	Beschreibung	Kapitel	Seite	Art	durch	Kommentar	Status
36	Klarstellung, dass sich der Auftragshashwert vom ersten bit des Segmentkopfes bis zum letzten bit des Trennzeichens erstreckt	D	S. 62	K	GAD, SIZ	Klarstellung, dass in die Berechnung des Auftragshashwerts der Bereich vom ersten bit des Segmentkopfes bis zum letzten bit des Trennzeichens eingeht.	angenommen
37	Schritt 2b: Klarstellung, dass sich alle HIRMSe in der letzten Antwort bei Prozessvariante 2 auf den Auftrag selbst beziehen, auch die HIRMSe auf die TAN-Einreichung mit HKTAN. Klarstellung, dass in der Antwort auch explizite Kreditinstitutsantworten, z. B. HIDAE enthalten sein können	B.2.1.2	S. 19	K	GAD, SIZ	Schritt 2b: Klarstellung, dass sich alle HIRMSe in der letzten Antwort bei Prozessvariante 2 auf den Auftrag selbst beziehen, auch die HIRMSe auf die TAN-Einreichung mit HKTAN. Klarstellung, dass in der Antwort auch explizite Kreditinstitutsantworten, z. B. HIDAE enthalten sein können	angenommen
38	Ggf. Klarstellung, dass auch bei rein PIN-pflichtigen Aufträgen ein konkretes Zwei-Schritt-Verfahren im Signaturkopf angegeben werden muss.	B.5.2	S. 37	K	GAD, SIZ	Klarstellung: es muss (wie bisher) ein gültiges Verfahren analog BPD verwendet werden, auch bei rein PIN-pflichtigen Aufträgen.	angenommen
39	Aufnahme der BEN in der Rückantwort in HKTAN	B.2.3	S. 29	E	WS	Erweiterung: die BEN wird als letztes Feld in HITAN ergänzt, optional, an ..99	angenommen
40	Auftragsreferenz bei HKTAN/HITAN muss für TAN-Prozess 1 und 4 "O" sein, damit auch bei Prozessvariante 1 Challenges übertragen werden können.	B.2.3	S. 29	E	GAD	Eine entsprechende Korrektur wird in der GV-Beschreibung vorgenommen.	angenommen

FinTS PIN/TAN inkl. Zwei-Schritt-Verfahren, Rel. 2005-06-21
- Befundliste -

lfd. Nr.	Beschreibung	Kapitel	Seite	Art	durch	Kommentar	Status
42	Im Segment HITAN muss das Feld "Auftragsreferenz" bei Variante 2, 3 und 4 belegt werden. Bei Variante 1 muss das Feld belegt werden, wenn in HKTAN das Feld belegt war. Konkret: Die Auftragsreferenz soll unabhängig von der Prozessvariante durch das Banksystem vergeben werden. Ist das Feld in HITAN belegt, so muss das Kundenprodukt bei den folgenden HKTAN-Segmenten das Feld ebenfalls mit dem gesendeten Wert belegen.	B.2.1.2	S. 19	F	GAD	siehe auch Punkt 30. eine Klarstellung erfolgt analog Beschreibung.	angenommen
43	Belegung der DE "TAN-Zusatzinformationen" mit GV-Code und Challenge	B.2.3	S. 30	E	GAD	Klarstellung in den Belegungsrichtlinien: abhängig vom konkreten Zwei-Schritt-Verfahren wird diese Beschreibung strukturiert, wie in der entsprechenden Spezifikation beschrieben.	angenommen
44	Der Parameter "mehrere TAN-pflichtige Aufträge pro Nachricht" soll entfallen, da die Komplexität dann nicht mehr handhabbar ist.	D	S.70	Ä	SIZ	Klärung BdB	in Arbeit