

# FinTS

## Financial Transaction Services

Schnittstellenspezifikation

Echtzeitbenachrichtigungen

Herausgeber:

Bundesverband deutscher Banken e.V., Berlin

Deutscher Sparkassen- und Giroverband e.V., Bonn/Berlin

Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e.V., Berlin

Bundesverband Öffentlicher Banken Deutschlands e.V., Berlin

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

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

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

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

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

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

---

## **Versionsführung**

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

Name	Organisation	Datum	Version	Dokumente	Anmerkungen
Mindnich	SIZ	16.12.2021	3.0 Final Version	FinTS 3.0_Echtzeitbenachrichtigungen-16-12-2021-final_version.docx	Erste von der DK verabschiedete Version

Grau dargestellte Spezifikationsteile sind aus Sicht der Spezifikation obsolet, können aber aus Migrationsgründen noch verwendet werden. Die Entscheidung hierüber ist institutsspezifisch.

## **Änderungen gegenüber der Vorversion**

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

lfd. Nr.	Kapitel	Kapitelnummer	Ken-nung <sup>1</sup>	Art <sup>2</sup>	Beschreibung
1					
2					

---

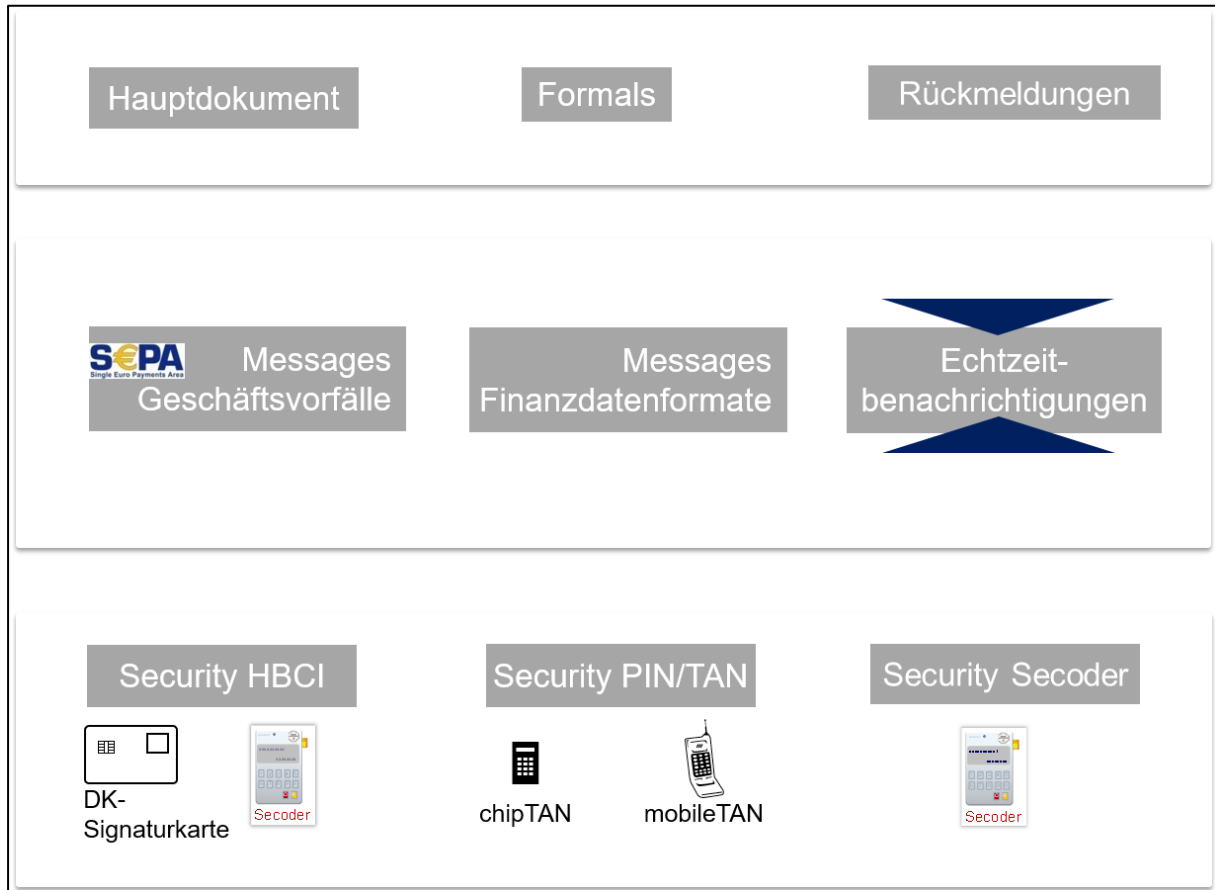
<sup>1</sup> nur zur internen Zuordnung

<sup>2</sup> F = Fehler; Ä = Änderung; K = Klarstellung; E = Erweiterung

---

## Dokumentenstruktur

Das vorliegende Dokument steht in folgendem Bezug zu den anderen Bänden der FinTS V3.0 Spezifikation:



Inhaltsverzeichnis

<b>Versionsführung .....</b>	<b>ii</b>
<b>Änderungen gegenüber der Vorversion .....</b>	<b>ii</b>
<b>Dokumentenstruktur .....</b>	<b>iii</b>
<b>A. Einführung .....</b>	<b>5</b>
<b>B. Technische Architektur des Verfahrens .....</b>	<b>6</b>
B.1 Nutzung des WebSocket-Protokolls für Echtzeitbenachrichtigungen .....	6
B.2 Daten für den clientseitigen Verbindungsaufbau .....	7
B.2.1 Erweiterung der Bank- und Userparameterdaten (BPD / UPD) .....	7
B.2.2 Szenarien für die Nutzung von Push-Services.....	8
B.2.2.1 Basisfunktionalitäten für Push-Services bei DK-TAN- Verfahren DecoupledPush.....	8
B.2.2.2 HKPUR mit Token .....	10
B.2.3 Geschäftsvorfälle zur Registrierung und De-Registrierung von Kundenprodukten .....	11
B.2.3.1 Geschäftsvorfall HKPUR zur Registrierung für die Nutzung von Push-Services.....	11
B.2.3.2 Geschäftsvorfall HKPUA zur Änderung von registrierten Push-Services / Token-Aktualisierung.....	13
B.2.3.3 Registrierte FinTS-Kundenprodukte für Push-Services .....	17
B.2.3.4 FinTS-Kundenprodukte für Push-Services de- registrieren .....	19
B.3 Headerbeschreibung für den HTTPS-Handshake .....	21
<b>C. Struktur von Echtzeitbenachrichtigungen .....</b>	<b>23</b>
C.1 Avisierung neuer Daten im FinTS-Banksystem .....	23
C.2 Allgemeine Informationen .....	26
<b>D. Abgrenzung FinTS Sphäre – WebSocket-Verbindung .....</b>	<b>28</b>
D.1 Beispiele für das Zusammenspiel der verschiedenen Sphären .....	28
D.1.1 Beispiel: Aufbau einer einmal gültigen WebSocket- Verbindung.....	29
D.1.1.1 Ablaufbeschreibung.....	29
D.1.1.2 Verhalten bei Störungen .....	30
D.1.2 Beispiel: Längerfristiger Aufbau einer WebSocket- Verbindung.....	31
D.2 Aktionen auf Kreditinstitutsseite .....	32
D.3 Aktionen auf Kundenseite .....	33
<b>E. Data Dictionary .....</b>	<b>34</b>

---

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: A
Kapitel: Einführung Abschnitt: Nutzung des WebSocket-Protokolls für	Stand: 16.12.2021	Seite: 5

## A. EINFÜHRUNG

Im Zusammenhang mit der Einführung des PIN/TAN-Decoupled-Verfahrens ergibt sich die Notwendigkeit dem Kundensystem mitzuteilen, dass die Freigabe eines Auftrags erfolgt ist.

Durch den FinTS-Standard der Deutschen Kreditwirtschaft wird eine sichere Übertragung von Zahlungen, Kontoinformationen etc. gewährleistet. Als Client-Server-Verfahren konzipiert geht die Initiative zur Übertragung immer von der Kunden- bzw. der Client-Seite aus. Kunden schicken Zahlungen und/oder holen Daten ab. Die Bankseite schickt niemals initiativ Daten an den Kunden. Für die gewünschte Echtzeit-Benachrichtigung von Kunden bedeutet dies, dass Kunden über FinTS aktiv nachfragen müssten, ob entsprechende Informationen zur Abholung bereitstehen. Dies führt unweigerlich zu der Situation, dass FinTS-Kundensysteme in regelmäßigen kurzen Zeitabständen die Bank-Server abfragen (Polling), was zur Überlastung der Banksysteme aufgrund des hohen und dabei überflüssigen Kommunikations-Overheads führen kann. Um dies zu verhindern, könnte es eine Lösung sein, FinTS derart zu verändern, dass über FinTS aktiv Informationen (Push-Service) an Kunden übertragen werden können. Eine solche Lösung würde aber bedeuten, dass die Banken aktiv FinTS-Verbindungen in die Kundensphäre aufbauen müssten, was eine Fülle von zu lösenden Sicherheitsfragen nach sich ziehen würde und zu einer komplexen bankseitigen Administration von FinTS-Kundensystemen führt.

Um einerseits eine komplexe und grundlegende Änderung des FinTS-Standards zu vermeiden und andererseits zu verhindern, dass vermehrt institutsindividuelle Lösungen zur Übermittlung von Echtzeitinformationen geschaffen werden, die nicht miteinander kompatibel sind, hat sich die Deutsche Kreditwirtschaft dazu entschlossen, eine Standardisierung auf Basis der Kombination zweier systemisch unabhängiger Verfahren zu schaffen. Hierzu soll es einerseits bei der Nutzung des sicheren und etablierten FinTS-Verfahrens zur Abholung von bankfachlichen Daten bleiben, zum anderen aber moderne Webtechnologie genutzt werden, um die FinTS-Abholung durch den Kunden eventgesteuert triggern zu können. Hierzu wird der etablierte Internetstandard „WebSocket“ genutzt, der einen von der Clientseite aufgebauten und mittels TLS gesicherten einmal oder längerfristig verwendbaren bidirektionalen Kanal zwischen Kunde und Bank bietet, über den die Banken die Zurverfügungstellung (Bereitstellung zur Abholung) von Echtzeitinformationen avisieren können. Kundenseitig können dann die bankfachlich relevanten Echtzeitinformationen über das bewährte FinTS-Protokoll sicher zum Kunden übertragen werden.

Der oben beschriebene Lösungsansatz bietet ein Zusammenspiel von etablierten Internetstandards mit dem FinTS-Standard der Deutschen Kreditwirtschaft zur sicheren Übermittlung von Echtzeitbenachrichtigungen an Kunden. In erster Linie ist dieses Verfahren für die Übermittlung der erfolgten Freigabe eines Auftrags durch den Kunden im Rahmen des Decoupled-Verfahren vorgesehen, welches das Kundensystem in Echtzeit über die erfolgte Freigabe eines zuvor eingereichten Auftrags informiert. Das Verfahren ist aber darüber hinaus geeignet, auch weitere zukünftige Geschäftsprozesse zu unterstützen, die die Übermittlung von Echtzeitbenachrichtigungen erfordern.

Das Design der im Folgenden näher spezifizierten Lösung bietet aufgrund der systemischen Trennung von FinTS- und WebSocket-Funktionalität und die enge Anlehnung an die bereits vorhandene Lösung des EBICS-Standards grundsätzlich die Möglichkeit der Nutzung vorhandener IT-Infrastrukturen sowohl in der Bank- als auch in der Kundensphäre. Die sichere FinTS-

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Nutzung des WebSocket-Protokolls für	Stand: 16.12.2021	Seite: 6

Infrastruktur wird hierbei unverändert für die Übermittlung der sensiblen bankfachlichen Daten genutzt.

## **B. TECHNISCHE ARCHITEKTUR DES VERFAHRENS**

### **B.1 Nutzung des WebSocket-Protokolls für Echtzeitbenachrichtigungen**

Für die Möglichkeit, serverseitig Nachrichten an einen Client zu schicken (Push-Funktionalität) wird das wss-Protokoll verwendet. Die konkrete Beschreibung des wss-Protokolls findet sich in RFC 6455<sup>1</sup>.

Während der Server bei einer HTTPS-Verbindung auf Anfragen eines Clients reagiert (Client Request / Server Response), öffnet der Client beim WebSocket-Protokoll die (bzw. eine) Verbindung zum Server. Der Server kann dann diese offenbleibende Verbindung dazu verwenden, aktiv (d.h. ohne einen konkreten Request des Clients) Informationen an den Client zu liefern. Das Verfahren ist grundsätzlich bidirektional, d.h. der Client kann auch Antworten senden. Für den hier beschriebenen Anwendungsfall werden allerdings nur Nachrichten vom Server an den Client geschickt. Zur sicheren Datenübertragung wird die Internetverschlüsselung TLS verwendet (wss-Verbindung).

Die Anzahl der Sessions (Verbindungen) eines Kunden mit seiner Bank ist grundsätzlich nicht beschränkt. Mehrere Sessions sind zum Beispiel bei getrennten Kundensystemen erforderlich. Sollte ein Kunde zum Zeitpunkt des Versands einer Nachricht keine geöffnete Verbindung haben, dann entscheidet die Bank, ob sie aufgelaufene Push-Nachrichten sendet, sobald unterbrochene Verbindungen wieder verfügbar sind.

---

<sup>1</sup> <https://tools.ietf.org/html/rfc6455>

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 7

## B.2 Daten für den clientseitigen Verbindungsaufbau

Um eine wss-Verbindung zum Server aufzubauen, müssen dem Client die notwendigen Verbindungsdaten mitgeteilt werden.

Eine Möglichkeit für FinTS-Kundensysteme ist das Abholen der Daten im Rahmen der Dialoginitialisierung und eines Registrierungsgeschäftsvorfalles. Den Banken steht es aber prinzipiell frei, die Zugangsdaten auch über alternative Kanäle den Kunden mitzuteilen. Für den betrachteten initialen Anwendungsfall handelt es sich jedoch um FinTS-Kunden, daher ist die Nutzung der sicheren FinTS-Kommunikation zur Übermittlung von Zugangsdaten sinnvoll.

### B.2.1 Erweiterung der Bank- und Userparameterdaten (BPD / UPD)

Ob ein Kreditinstitut Push-Funktionalitäten anbietet, erkennt das Kundenprodukt in den Bankparameterdaten am Vorhandensein des Geschäftsvorfallparametersegments HIPURS („Registrierung für die Nutzung von Push-Services“, vgl. Kapitel B.2.3).

Die Unterstützung von HKPUR in der UPD weist darauf hin, dass durch den Kunden gezielt Geschäftsvorfälle für Push-Services registriert werden können.

Es ergeben sich somit folgende Kombinationen:

	UPD	HKPUR nicht vorhanden	HKPUR vorhanden
BPD			
HIPURS nicht vorhanden		Push-Services werden vom Kreditinstitut nicht unterstützt	---
HIPURS vorhanden		Push-Basisfunktionalitäten werden unterstützt (s. Kapitel B.2.2.1)	Push-Basisfunktionalitäten werden unterstützt (s. Kapitel B.2.2.1) Push-Funktionalitäten inklusive Registrierung werden unterstützt (s. Kapitel B.2.2.2)



Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 8

## B.2.2 Szenarien für die Nutzung von Push-Services

Aus den in Kapitel B.2.1 aufgeführten Kombinationen von HIPURS und HKPUR sowie den daraus entstehenden Möglichkeiten, ein Token an das Kundenprodukt zu übermitteln, resultieren zwei unterschiedliche Szenarien, um an alle Daten für den clientseitigen Verbindungsaufbau zu gelangen.

Die in diesem Kapitel aufgeführten Szenarien beschreiben lediglich die Ablaufschritte, die ein Kundenprodukt in die Lage versetzen, Push-Services zu nutzen. Beispiele für den vollständigen Ablauf bei Verwendung von Push-Services befinden sich in Kapitel D.1

### B.2.2.1 Basisfunktionalitäten für Push-Services bei DK-TAN-Verfahren DecoupledPush

Für dieses Szenario gelten folgende Voraussetzungen:

- Kreditinstitut und Kundenprodukt unterstützen Push-Funktionalitäten
- In der BPD ist das Parametersegment HIPURS vorhanden
- Es wird HKTAN  $\geq 7$  genutzt
- In den „Verfahrensparametern Zwei-Schritt-Verfahren“ im HITANS ist das DE „DK TAN-Verfahren“ mit „DecoupledPush“ belegt. Dieses TAN-Verfahren wird vom Kundenprodukt unterstützt und ist zur Nutzung ausgewählt.

Beispiel Dialoginitialisierung:

Bereits im Rahmen der Dialoginitialisierung kann eine starke Kundenauthentifizierung notwendig sein. Der Ablauf gestaltet sich hier im Detail wie folgt:

Ablaufschritte:

1. Dialoginitialisierung inkl. HKTAN
2. In der Kreditinstitutsnachricht ist HIPURS in der BPD vorhanden. Der FinTS-Client kann dieser die WebSocket-URL des Instituts entnehmen. Es ist für dieses Szenario unerheblich, ob HKPUR für den Kunden in der UPD unterstützt wird. Das Kreditinstitut übermittelt in seiner Antwort den Rückmeldecode 3090, welcher ein im Kontext der Dialoginitialisierung einmal gültiges Token beinhaltet.

➔ WebSocket-URL **und** Token für einen einmaligen clientseitigen Verbindungsaufbau sind nun verfügbar.



Für die weiteren Beispiele im Dokument wird davon ausgegangen, dass eine Dialoginitialisierung in jedem Fall erfolgreich ist. Auf die Nennung des HKTAN im Rahmen der Dialoginitialisierung wird daher im weiteren Verlauf des Dokuments verzichtet.

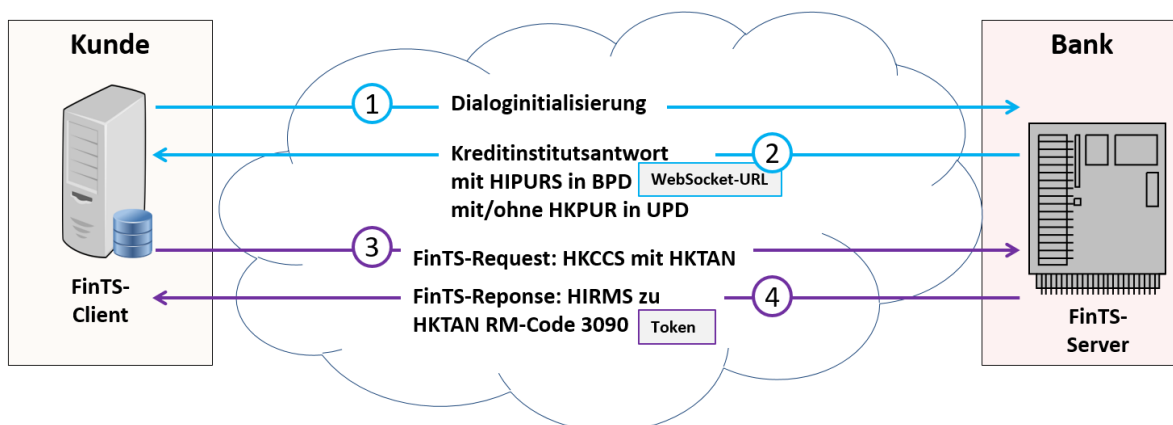
Beispiel Einzelüberweisung:

Financial Transaction Services (FinTS)	Version:	Kapitel:
Dokument: Echtzeitbenachrichtigungen in FinTS	3.0-FV	B
Kapitel: Technische Architektur des Verfahrens	Stand:	Seite:
Abschnitt: Daten für den clientseitigen Verbindungsaufbau	16.12.2021	9

Abläufe beim Einreichen eines vom Kunden freizugebenden Auftrags am Beispiel einer Einzelüberweisung. Es gelten dieselben Voraussetzungen wie in oben aufgeführt.

Ablaufschritte:

1. Dialoginitialisierung
2. In der Kreditinstitutsnachricht ist HIPURS in der BPD vorhanden. Der FinTS-Client kann dieser die WebSocket-URL des Instituts entnehmen. Es ist unerheblich, ob HKPUR für den Kunden in der UPD unterstützt wird.
  - ➔ Die WebSocket-URL ist damit bekannt. Zum clientseitigen Verbindungsaufbau fehlt ein Token.
3. Der Kunde löst z.B. eine TAN-pflichtige Einzelüberweisung aus.
4. Das Kreditinstitut übermittelt in seiner Antwort den Rückmeldecode 3090, welcher ein im Kontext des Geschäftsvorfalles einmal gültiges Token beinhaltet.
  - ➔ WebSocket-URL **und** Token für einen einmaligen clientseitigen Verbindungsaufbau sind nun verfügbar.



Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 10

### B.2.2.2HKPUR mit Token

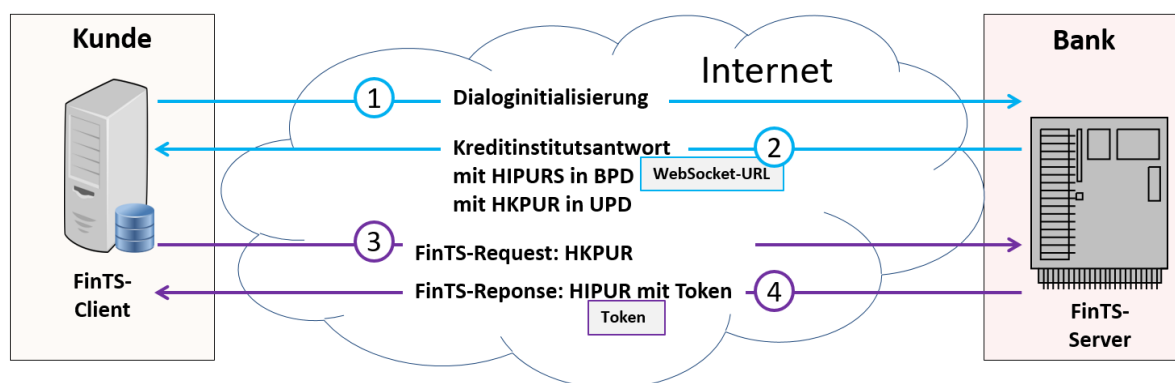
Für dieses Szenario gelten folgende Voraussetzungen:

- Kreditinstitut und Kundenprodukt unterstützen Push-Funktionalitäten
- In der BPD ist das Parametersegment HIPURS vorhanden
- HKPUR ist in der UPD vorhanden

Ablaufschritte:

1. Dialoginitialisierung
2. In der Kreditinstitutsnachricht ist HIPURS in der BPD vorhanden. Der FinTS-Client kann dieser die WebSocket-URL des Instituts entnehmen. In der UPD ist HKPUR für den Kunden verfügbar. Eine explizite Registrierung von Geschäftsvorfällen für Push-Services ist damit möglich.
  - ➔ Die WebSocket-URL ist damit bekannt. Zum clientseitigen Verbindungsaufbau fehlt ein Token.
3. Der Kunde registriert sich mit Hilfe des Geschäftsvorfalles HKPUR für Push-Services für diverse Geschäftsvorfälle, darunter z.B. HKISS.
4. In der Kreditinstitutsantwort befindet sich ein Token. Ebenso beinhaltet sie ggf. Informationen zum Gültigkeitsende der Möglichkeit zum mehrfachen Aufbau der WebSocket-Verbindung mittels dieses Tokens.
  - ➔ WebSocket-URL und Token für einen längerfristigen clientseitigen Verbindungsaufbau sind nun verfügbar

Die übermittelten Daten für den Verbindungsaufbau können unmittelbar genutzt werden. Eine Verwendung für Push-Services bei DK-TAN-Verfahren „DecoupledPush“ ist nicht erlaubt. Das bedeutet, dass HKTAN nicht mittels HKPUR registriert werden darf. HKTAN nutzt immer die Basisfunktionalitäten für Push-Services (s. Kapitel B.2.2.1).



Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 11

## B.2.3 Geschäftsvorfälle zur Registrierung und De-Registrierung von Kundenprodukten

### B.2.3.1 Geschäftsvorfall HKPUR zur Registrierung für die Nutzung von Push-Services

Realisierung Bank: optional

Realisierung Kunde: optional

#### a) Kundenauftrag

##### ◆ Format

Name: Push-Services Registrierung  
 Typ: Segment  
 Segmentart: Geschäftsvorfall  
 Kennung: HKPUR  
 Bezugssegment: -  
 Version: 1  
 Sender: Kunde

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	1	DEG			M	1	
2	Produktbezeichnung	1	DE	an	..25	M	1	
3	Produktversion	1	DE	an	..5	M	1	
4	<a href="#">Name des Herstellers</a>	1	DE	an	..35	M	1	
5	<a href="#">Eindeutige Bezeichnung des Kundensystems</a>	1	DE	an	..32	M	1	
6	<a href="#">Segmentkennung Registrierung</a>	1	DE	an	..5	M	..99	It BPD: „Segmentkennung Registrierung“

##### ◆ Belegungsrichtlinien

#### Produktbezeichnung, Produktversion, Name des Herstellers

Die Datenelemente sind verpflichtend mit aussagekräftigen Informationen über das verwendete Kundenprodukt, nicht eine ggf. verwendete interne FinTS-/HBCI-Bibliothek, zu füllen. Die Produktregistrierungsnummer aus dem Registrierungsverfahren der Deutschen Kreditwirtschaft ist nicht zu verwenden.

#### Segmentkennung Registrierung

Es ist eine Segmentkennung aus den in der BPD angebotenen registrierungsfähigen Geschäftsvorfällen einzustellen.



HKTAN ist automatisch durch die Auswahl des DK TAN-Verfahrens „DecoupledPush“ registriert. Eine weitere Registrierung durch HKPUR ist nicht erlaubt. (s. Kapitel B.2.2.1)

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 12

## b) Kreditinstitutsrückmeldung

### ◆ Beschreibung

### ◆ Format

Name: Push-Services Registrierung rückmelden  
 Typ: Segment  
 Segmentart: Geschäftsvorfall  
 Kennung: HIPUR  
 Bezugssegment: HKPUR  
 Version: 1  
 Anzahl: 1  
 Sender: Kreditinstitut

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	1	DEG			M	1	
2	<a href="#">Token Push-Service</a>	1	DE	an	..80	M	1	
3	<a href="#">Gültigkeitsende Token</a>	1	DEG	tsp	#	O	1	
4	<a href="#">Segmentkennung Registrierung</a>	1	DE	an	..5	M	..99	

### ◆ Belegungsrichtlinien

#### Token Push-Service

Das Token ist nur auf das Kundenprodukt bezogen, von dem aus die Registrierung vorgenommen wurde.



Für jedes Kundenprodukt muss eine eigene Registrierung für Push-Services durchgeführt werden. Der Umfang der registrierten Geschäftsvorfälle kann sich daher - je nach Vorlieben des Kunden - von Kundenprodukt zu Kundenprodukt unterscheiden.

#### Gültigkeitsende Token

Ist das Feld nicht belegt, gilt das Token unbegrenzt.



Ein ablaufendes Token ist über den Geschäftsvorfall „Änderung von registrierten Push-Services“ (HKPUA) zu aktualisieren.

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 13



Eine Nichtbelegung des Gültigkeitsdatums wird nicht empfohlen.

#### ◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
0020	Push-Services wurden registriert
9210	Auftrag abgelehnt – Bezeichnung des Kundensystem bereits vergeben

#### c) Bankparameterdaten

##### ◆ Format

Name: Push-Services Registrierung Parameter  
 Typ: Segment  
 Segmentart: Geschäftsvorfall  
 Kennung: HIPURS  
 Bezugssegment: HKVVB  
 Version: 1  
 Sender: Kreditinstitut

Nr.	Name	Ver- sion	Typ	For- mat	Län- ge	Sta- tus	An- zahl	Restriktionen
1	Segmentkopf	1	DEG			M	1	
2	Maximale Anzahl Aufträge	1	DE	num	..3	M	1	
3	Anzahl Signaturen mindestens	1	DE	num	1	M	1	0, 1, 2, 3
4	Sicherheitsklasse	1	DE	code	1	M	1	0, 1, 2, 3, 4
5	<a href="#">Parameter Push-Services Registrierung</a>	1	DEG			M	1	

#### B.2.3.2 Geschäftsvorfall HKPUA zur Änderung von registrierten Push-Services / Token-Aktualisierung

Dieser Geschäftsvorfall dient einerseits dazu, Änderungen an bereits registrierten Push-Services vorzunehmen, und andererseits, ein bereits vorhandenes Token zu aktualisieren.

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 14



Dieser Geschäftsvorfall ist nicht TAN-pflichtig.

Realisierung Bank: optional

Realisierung Kunde: optional

## a) Kundenauftrag

### ◆ Format

Name: Änderung von registrierten Push-Services

Typ: Segment

Segmentart: Geschäftsvorfall

Kennung: HKPUA

Bezugssegment: -

Version: 1

Sender: Kunde

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	1	DEG			M	1	
2	<a href="#">Token Push-Service</a>	1	DE	an	..80	M	1	
3	Produktbezeichnung	1	DE	an	..25	O	1	
4	Produktversion	1	DE	an	..5	O	1	
5	<a href="#">Name des Herstellers</a>	1	DE	an	..35	O	1	
6	<a href="#">Eindeutige Bezeichnung des Kundensystems</a>	1	DE	an	..32	M	1	
7	<a href="#">Segmentkennung Registrierung</a>	1	DE	an	..5	O	..99	lt. BPD HIPURS: „Segmentkennung Registrierung“

### ◆ Belegungsrichtlinien

#### Token Push-Service

Es ist das vorhandene Token einzustellen.

#### Produktbezeichnung, Produktversion, Name des Herstellers

Die Datenelemente sind mit aussagekräftigen Informationen über das verwendete Kundenprodukt, nicht eine ggf. verwendete interne FinTS-/HBCI-Bibliothek, zu füllen. Die Produktregistrierungsnummer aus dem Registrierungsverfahren der Deutschen Kreditwirtschaft ist nicht zu verwenden.

#### Segmentkennung Registrierung

Es sind Segmentkennungen aus den in der BPD für den Geschäftsvorfall „Push-Services Registrierung“ angebotenen registrierungsfähigen Geschäftsvorfällen einzustellen. Eine Registrierung gilt immer für alle laut BPD unterstützten Segmentversionen eines Geschäftsvorfalles. Die Änderung von Registrierungen wird immer durch das Überschreiben der bisher registrierten Geschäftsvorfälle vorgenommen. Es muss immer ein vollständiger Satz der für Push-Services registrierten und zu registrierenden Segmentkennungen eingereicht werden.

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 15

Fehlt dieses Datenelement in der Änderung von registrierten Push-Services so entspricht dies einer De-Registrierung.



Es bietet sich kundenproduktseitig an, die bis dahin registrierten Geschäftsvorfälle in der Eingabemaske als „ausgewählt“ vorbelegt anzuzeigen.



HKTAN ist automatisch durch die Auswahl des DK TAN-Verfahrens „DecoupledPush“ registriert. Eine weitere Registrierung durch HKPUR ist nicht erlaubt. (s. Kapitel B.2.2.1)



## b) Kreditinstitutsrückmeldung

### ◆ Beschreibung

### ◆ Format

Name: Änderung von registrierten Push-Services rückmelden  
 Typ: Segment  
 Segmentart: Geschäftsvorfall  
 Kennung: HIPUA  
 Bezugssegment: HKPUA  
 Version: 1  
 Anzahl: 1  
 Sender: Kreditinstitut

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	1	DEG			M	1	
2	<a href="#">Token Push-Service</a>	1	DE	an	..80	C	1	N: „Segmentkennung Registrierung“ nicht belegt M: sonst
3	<a href="#">Gültigkeitsende Token</a>	1	DEG	tsp	#	C	1	N: „Token Push-Service“ nicht belegt O: sonst
4	<a href="#">Segmentkennung Registrierung</a>	1	DE			O	..99	

### ◆ Belegungsrichtlinien

#### Token Push-Service

Das Token ist nur auf das Kundenprodukt bezogen, von dem aus die Änderung vorgenommen wurde.



Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 16



Für jedes Kundenprodukt muss eine eigene Änderung für Push-Services durchgeführt werden. Der Umfang der registrierten Geschäftsvorfälle kann sich daher - je nach Vorlieben des Kunden - von Kundenprodukt zu Kundenprodukt unterscheiden.

### Gültigkeitsende Token

Ist das Feld nicht belegt, gilt das Token unbegrenzt.



Eine Nichtbelegung des Gültigkeitsdatums wird nicht empfohlen.

### ◆ Ausgewählte Beispiele für RückmeldungsCodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
0020	Registrierte Push-Services wurden geändert
0020	Push-Services wurden de-registriert
9210	Auftrag abgelehnt – Kundensystem nicht für Push-Services registriert

### c) Bankparameterdaten

#### ◆ Format

Name: Änderung von registrierten Push-Services Parameter  
 Typ: Segment  
 Segmentart: Geschäftsvorfall  
 Kennung: HIPUAS  
 Bezugssegment: HKVVB  
 Version: 1  
 Sender: Kreditinstitut

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	1	DEG			M	1	
2	Maximale Anzahl Aufträge	1	DE	num	..3	M	1	
3	Anzahl Signaturen mindestens	1	DE	num	1	M	1	0, 1, 2, 3
4	Sicherheitsklasse	1	DE	code	1	M	1	0, 1, 2, 3, 4

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 17

### B.2.3.3 Registrierte FinTS-Kundenprodukte für Push-Services

Mit Hilfe dieses Geschäftsvorfalles kann sich ein Benutzer alle Kundenprodukte anzeigen lassen, die er für Push-Services registriert hat.

Realisierung Bank: optional

Realisierung Kunde: optional

#### a) Kundenauftrag

##### ◆ Format

Name: Registrierte FinTS-Kundenprodukte für Push-Services anzeigen  
 Typ: Segment  
 Segmentart: Geschäftsvorfall  
 Kennung: HKPRB  
 Bezugssegment: -  
 Version: 1  
 Sender: Kunde

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	1	DEG			M	1	
2	Maximale Anzahl Einträge		DE	num	..4	C	1	>0 O: „Eingabe Anzahl Einträge erlaubt“ (BPD) = „J“ N: sonst
3	Aufsetzpunkt	1	DE	an	..35	C	1	M: vom Institut wurde ein Aufsetzpunkt rückgemeldet N: sonst

#### b) Kreditinstitutsrückmeldung

Für jedes registrierte Kundenprodukt wird ein Segment zurückgeliefert.

##### ◆ Format

Name: Registrierte FinTS-Kundenprodukte für Push-Services rückmelden  
 Typ: Segment  
 Segmentart: Geschäftsvorfall  
 Kennung: HIPRB  
 Bezugssegment: HKPRB  
 Version: 1  
 Anzahl: n  
 Sender: Kreditinstitut

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	1	DEG			M	1	
2	Produktbezeichnung	1	DE	an	..25	M	1	
3	Produktversion	1	DE	an	..5	M	1	
4	<a href="#">Name des Herstellers</a>	1	DE	an	..35	M	1	

Financial Transaction Services (FinTS)				Version: 3.0-FV		Kapitel: B	
Dokument: Echtzeitbenachrichtigungen in FinTS							
Kapitel: Technische Architektur des Verfahrens				Stand: 16.12.2021		Seite: 18	
Abschnitt: Daten für den clientseitigen Verbindungsaufbau							

5	<a href="#">Eindeutige Bezeichnung des Kundensystems</a>	1	DE	an	..32	M	1	
---	--	---	----	----	------	---	---	--

◆ **Ausgewählte Beispiele für RückmeldungsCodes**

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
9210	Keine registrierten FinTS-Kundenprodukte vorhanden

**c) Bankparameterdaten**

◆ **Format**

Name: Registrierte FinTS-Kundenprodukte für Push-Services anzeigen Parameter  
Typ: Segment  
Segmentart: Geschäftsvorfall  
Kennung: HIPRBS  
Bezugssegment: HKVVB  
Version: 1  
Sender: Kreditinstitut

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	1	DEG			M	1	
2	Maximale Anzahl Aufträge	1	DE	num	..3	M	1	
3	Anzahl Signaturen mindestens	1	DE	num	1	M	1	0, 1, 2, 3
4	Sicherheitsklasse	1	DE	code	1	M	1	0, 1, 2, 3, 4
5	<a href="#">Parameter registrierte FinTS-Kundenprodukte anzeigen</a>	2	DEG			M	1	

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 19

### B.2.3.4 FinTS-Kundenprodukte für Push-Services de-registrieren

Mit Hilfe dieses Geschäftsvorfalles kann ein Benutzer Kundenprodukte, die er für Push-Services registriert hat, de-registrieren. Er hat somit die Möglichkeit Registrierungen für Push-Services von zentraler Stelle aus zu löschen (z.B. für bereits deinstallierte oder nicht mehr verwendete Kundenprodukte).



Dieser Geschäftsvorfall ist TAN-pflichtig.

Realisierung Bank: optional

Realisierung Kunde: optional

#### a) Kundenauftrag

##### ◆ Format

Name: FinTS-Kundenprodukte für Push-Services de-registrieren

Typ: Segment

Segmentart: Geschäftsvorfall

Kennung: HKPRL

Bezugssegment: -

Version: 1

Sender: Kunde

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Segmentkopf	1	DEG			M	1	
2	<a href="#">Eindeutige Bezeichnung des Kundensystems</a>	1	DE	an	..32	M	1	

#### b) Kreditinstitutsrückmeldung

##### ◆ Beschreibung

Es werden keine Datensegmente zurückgemeldet.

##### ◆ Ausgewählte Beispiele für Rückmeldungscodes

Code	Beispiel für Rückmeldungstext
0010	Auftrag entgegengenommen
0020	Kundenprodukt wurden de-registriert
9210	Kein gültiges Kundensystem des Kunden

#### c) Bankparameterdaten

##### ◆ Beschreibung

Geschäftsvorfallspezifische Parameter existieren nicht.

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Daten für den clientseitigen Verbindungsaufbau	Stand: 16.12.2021	Seite: 20

◆ **Format**

Name: FinTS-Kundenprodukte für Push-Services de-registrieren Parameter  
Typ: Segment  
Segmentart: Geschäftsvorfall  
Kennung: HIPRLS  
Bezugssegment: HKVVB  
Version: 1  
Sender: Kreditinstitut

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	<a href="#">Segmentkopf</a>	1	DEG			M	1	
2	<a href="#">Maximale Anzahl Aufträge</a>	1	DE	num	..3	M	1	
3	<a href="#">Anzahl Signaturen mindestens</a>	1	DE	num	1	M	1	0, 1, 2, 3
4	<a href="#">Sicherheitsklasse</a>	1	DE	code	1	M	1	0, 1, 2, 3, 4

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Headerbeschreibung für den HTTPS-Handshake	Stand: 16.12.2021	Seite: 21

### B.3 Headerbeschreibung für den HTTPS-Handshake

Prämisse: Auf Grund der hohen Kompatibilität mit den verschiedenen Programmiersprachen (Java, Javascript,..) und High Level Frameworks wie Spring-Boot, sollte bei der Übermittlung der Credentials auf http-Basic Authentication RFC 2617<sup>2</sup> zurückgegriffen werden.

Dort wird der folgende Header definiert:

Authorization: Basic <base64encoded Credential>

Das Credential besteht üblicherweise aus User:Passwort.

Anhand des BPD-Parameters „Benutzerkennung verwenden“ aus HIPURS wird dem Kundenprodukt mitgeteilt, ob für „User“ die FinTS-Benutzerkennung zur Erzeugung des Credentials verwendet werden soll.

Sollen die Benutzerkennung und das Token verwendet werden („Benutzerkennung verwenden“=J), wird das Credential aus den Key-Values von User=BENUTZERKENNUNG und Passwort=TOKEN (aus „Token Push-Service“ bzw. dem „Rückmeldungstext“ aus der Rückmeldung mit Rückmeldungscode 3090) in der Form

BENUTZERKENNUNG:TOKEN gebildet (vergl. Kapitel B.2).

Bei einer Benutzerkennung mit dem Wert von z.B. 26314255 und einem Token mit dem Wert von z.B. „550e8400-e29b-11d4-a716-446655440000“ ergibt sich für den Header:

- ➔ Credential = 26314255:550e8400-e29b-11d4-a716-446655440000
- ➔ base64encoded Credential=  
MjYzMTQyNTU6NTUwZTg0MDAtZTI5Yi0xMWQ0LWE3MTYtNDQ2NjU1NDQwMDAw
- ➔ **Authorization: Basic**  
**MjYzMTQyNTU6NTUwZTg0MDAtZTI5Yi0xMWQ0LWE3MTYtNDQ2NjU1NDQwMDAw**

Soll nur das Token und keine Benutzerkennung verwendet werden („Benutzerkennung verwenden“=N), wird das Credential aus den Key-Values von User=NOTPROVIDED und Passwort=TOKEN (aus „Token Push-Service“ bzw. dem „Rückmeldungstext“ aus der Rückmeldung mit Rückmeldungscode 3090) in der Form

NOTPROVIDED:TOKEN gebildet (vergl. Kapitel B.2).

Bei einem Token mit dem Wert von z.B. „550e8400-e29b-11d4-a716-446655440000“ ergibt sich für den Header:

- ➔ Credential = NOTPROVIDED:550e8400-e29b-11d4-a716-446655440000

---

<sup>2</sup> <https://tools.ietf.org/html/rfc2617>

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: B
Kapitel: Technische Architektur des Verfahrens Abschnitt: Headerbeschreibung für den HTTPS-Handshake	Stand: 16.12.2021	Seite: 22

- base64encoded Credential=  
Tk9UUFJPVkie-  
RUQ6NTUwZTg0MDAtZTI5Yi0xMWQ0LWE3MTYtNDQ2NjU1NDQwMDAw
  
  - **Authorization: Basic**  
**Tk9UUFJPVkie-**  
**RUQ6NTUwZTg0MDAtZTI5Yi0xMWQ0LWE3MTYtNDQ2NjU1NDQwMDAw**
-

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: C
Kapitel: Struktur von Echtzeitbenachrichtigungen Abschnitt: Avisierung neuer Daten im FinTS-Banksystem	Stand: 16.12.2021	Seite: 23

## C. STRUKTUR VON ECHTZEITBENACHRICHTIGUNGEN

Echtzeitbenachrichtigungen, die innerhalb einer wss-Session an den Kunden geliefert werden, sind im JSON-Format kodiert.

Zu unterscheiden sind zwei Klassen von Nachrichten:

1. Die Avisierung neuer Daten auf dem FinTS-Server sowie
2. Allgemeine Informationen (Broadcast-Nachrichten) für Kunden

Die Inhalte und Struktur im JSON-Format sind in den folgenden Unterkapiteln beschrieben. Alle Werte in der JSON-Datei sind Zeichenketten (UTF-8).

### C.1 Avisierung neuer Daten im FinTS-Banksystem

Ebene	Name	Beschreibung	Erläuterungen	Kardinalität
1	MCLASS	Nachrichtenklasse als Array mit den Schlüsselinformationen NAME VERS TIMESTAMP		[1..1]
2	NAME	Name der Nachrichtenklasse	Für die hier vorliegende Klasse immer „FINTS“	[1..1]
2	VERS	Formatversion der vorliegenden Nachrichtenklasse	Diese Spezifikation startet für Klasse „FinTS“ mit „1.0“	[1..1]
2	TIMESTAMP	Zeitpunkt der Lieferung	Im dem Fall, dass keine aktive wss-Verbindung zum Kunden verfügbar ist, die Daten jedoch bei Verfügbarkeit noch nachgeliefert werden sollen, ist dies der Zeitpunkt des ersten Bereitstellungsversuches der Bankseite. Das Format ist ISO DateTime mit Zeitzone UTC.	[1..1]
1	TRANSACTION	Aufführung von Geschäftsvorfalls-Informationen als Arrays	Geschäftsvorfall, zu dem Informationen zur Abholung bereitstehen	[0..1]
2	MESSAGEID	Nachrichten-ID	Eindeutige Kennung zur ausgelieferten Nachricht	[0..1]
2	SEGMENTID	Segmentkennung	Segmentkennung des Geschäftsvorfalls, für den Push-Services bereitstehen	[1..1]
2	EXECUTE	Geschäftsvorfall ausführen J/N	Gibt an, ob der Geschäftsvorfall sofort ausgeführt werden muss (bei HKTAN).	[0..1]



Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: C
Kapitel: Struktur von Echtzeitbenachrichtigungen Abschnitt: Avisierung neuer Daten im FinTS-Banksystem	Stand: 16.12.2021	Seite: 24

Ebene	Name	Beschreibung	Erläuterungen	Kardinalität
2	ADDINFO	Zusätzliche Informationen als Array	Enthält zusätzliche Informationen z.B. zur Erleichterung von Abfragen	[0..1]
3	DATAELEMENT	Feldname im Geschäftsvorfall	Angabe des Feldnamens im Geschäftsvorfall. Es sind - sofern dort verfügbar - die Bezeichnungen aus dem Data Dictionary aus „ZKA-TAN-Generator Belegungsrichtlinien für das chipTAN-Verfahren“ zu verwenden.	[1..1]
3	DATA	Inhalt des Feldes	Entsprechende inhaltliche Befüllung	[1..1]
2	LANG	Sprache des Freitextes	Angabe des zweistelligen Länderkürzels, wenn nicht belegt ist DE gültig.	[0..1]
2	SUBJECT	Betreff	Betreff zur Freitextnachricht. Wenn vorhanden, muss das Feld dem Kunden angezeigt werden. (max. 80 Zeichen)	[0..1]
2	FREE	Freitextnachricht	Die Übertragung sicherheitsrelevanter Informationen ist nicht zulässig. Datenschutz ist zu beachten. Wenn vorhanden, muss das Feld dem Kunden angezeigt werden. (max. 2048 Zeichen)	[0..1]

### Beispiel

1:

Freigabe eines Auftrags auf einem anderen Gerät des Kunden erfolgt

```
{
  "MCLASS": [
    {
      "NAME": "FINTS",
      "VERS": "1.0",
      "TIMESTAMP": "2021-05-13T12:21:50Z"
    }
  ],
  "TRANSACTION": [
    {
      "MESSAGEID": "47110815",
      "SEGMENTID": "HKTAN",
      "EXECUTE": "J"
    }
  ]
}
```

### Beispiel

2:

Neue Umsätze und ein Payment Status Report zu Echtzeitüberweisungen des Kunden

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: C
Kapitel: Struktur von Echtzeitbenachrichtigungen Abschnitt: Avisierung neuer Daten im FinTS-Banksystem	Stand: 16.12.2021	Seite: 25

```

{
  "MCLASS": [
    {
      "NAME": "FINTS",
      "VERS": "1.0",
      "TIMESTAMP": "2021-05-13T12:21:50Z"
    }
  ],
  "TRANSACTION": [
    {
      "MESSAGEID": "47081511",
      "SEGMENTID": "HKCAZ",
      "EXECUTE": "N",
      "ADDINFO": [
        {
          "DATAELEMENT": "IBAN",
          "DATA": "DE18940594210019609759"
        }
      ],
      "LANG": "DE",
      "FREE": "Es liegen neue Umsätze vor."
    },
    {
      "MESSAGEID": "08154711",
      "SEGMENTID": "HKISS",
      "EXECUTE": "N",
      "ADDINFO": [
        {
          "DATAELEMENT": "IBAN",
          "DATA": "DE18940594210019609759"
        }
      ],
      "LANG": "DE",
      "FREE": "Es liegt ein neuer SEPA-Instant Payment Sammelzahlung Status vor."
    }
  ]
}

```

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: C
Kapitel: Struktur von Echtzeitbenachrichtigungen Abschnitt: Allgemeine Informationen	Stand: 16.12.2021	Seite: 26

## C.2 Allgemeine Informationen

Ebene	Name	Beschreibung	Erläuterungen	Kardinalität
1	MCLASS	Nachrichtenklasse als Array mit den Schlüsselinformationen NAME VERS TIMESTAMP		[1..1]
2	NAME	Name der Nachrichtenklasse	Für die hier vorliegende Klasse immer „INFO“	[1..1]
2	VERS	Formatversion der vorliegenden Nachrichtenklasse	Diese Spezifikation startet für Klasse „INFO“ mit „1.0“	[1..1]
2	TIMESTAMP	Zeitpunkt der Lieferung	Im dem Fall, dass keine aktive wss-Verbindung zum Kunden verfügbar ist, die Daten jedoch bei Verfügbarkeit noch nachgeliefert werden sollen, ist dies der Zeitpunkt des ersten Bereitstellungsversuches der Bankseite Das Format ist ISO DateTime mit Zeitzone UTC.	[1..1]
1	INFO	Freitextnachrichten als Array mit den Schlüsselinformationen MESSAGEID LANG SUBJECT FREE	Das Array muss FREE enthalten.	[1..1]
2	MESSAGEID	Nachrichten-ID	Eindeutige Kennung zur ausgelieferten Nachricht	[0..1]
2	LANG	Sprache des Freitextes	Angabe des zweistelligen Länderkürzels. Wenn nicht belegt, ist DE gültig.	[0..1]
2	SUBJECT	Betreff	Betreff zur Freitextnachricht. Wenn vorhanden, muss das Feld dem Kunden angezeigt werden. (max. 80 Zeichen)	[0..1]
2	FREE	Freitextnachricht	Die Übertragung sicherheitsrelevanter Informationen ist nicht zulässig. Datenschutz ist zu beachten. Wenn vorhanden, muss das Feld dem Kunden angezeigt werden. (max. 2048 Zeichen)	[1..1]

Beispiel

Beispiel für eine allgemeine Information

3:

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: C
Kapitel: Struktur von Echtzeitbenachrichtigungen Abschnitt: Allgemeine Informationen	Stand: 16.12.2021	Seite: 27

```
{
  "MCLASS": [
    {
      "NAME": "INFO",
      "VERS": "1.0",
      "TIMESTAMP": "2021-03-25T12:25:34Z"
    }
  ],
  "INFO": [
    {
      "MESSAGEID": "08471115",
      "LANG": "DE",
      "SUBJECT": "Wartungsarbeiten",
      "FREE": "Der FinTS-Service ist am 30.10.2021 von 03:00 – 04:00 Uhr wegen Wartungsarbeiten
nur eingeschränkt verfügbar."
    }
  ]
}
```

Financial Transaction Services (FinTS)	Version:	Kapitel:
Dokument: Echtzeitbenachrichtigungen in FinTS	3.0-FV	D
Kapitel: Abgrenzung FinTS Sphäre – WebSocket-Verbindung	Stand:	Seite:
Abschnitt: Beispiele für das Zusammenspiel der verschiedenen	16.12.2021	28

## D. ABGRENZUNG FINTS SPHÄRE – WEBSOCKET-VERBINDUNG

Über die WebSocket-Verbindung kann ein FinTS-Kunde in Echtzeit über neu auf dem FinTS-Banksystem bereitstehende Daten informiert werden (vergleiche Kapitel C.1).

Die WebSocket-Verbindung ist somit eine Ergänzung der FinTS-Kommunikation, sie ist allerdings vom FinTS-Verfahren technisch vollkommen getrennt. Insbesondere dürfen keine FinTS-Inhalte oder generell inhaltlich sensible Daten (z. B. die IBAN bei Überweisungen und gleichzeitig dazugehörige Beträge) übertragen werden.

### D.1 Beispiele für das Zusammenspiel der verschiedenen Sphären

Der Aufbau der WebSocket-Verbindung ist in den folgenden Beispielen mit den einzelnen Aktionen nach zeitlichem Ablauf durchnummeriert und für die verschiedenen Sphären in unterschiedlichen Farben dargestellt:

FinTS:

- blau (Dialoginitialisierung)
- lila (Tokenübermittlung)

WebSocket: rot

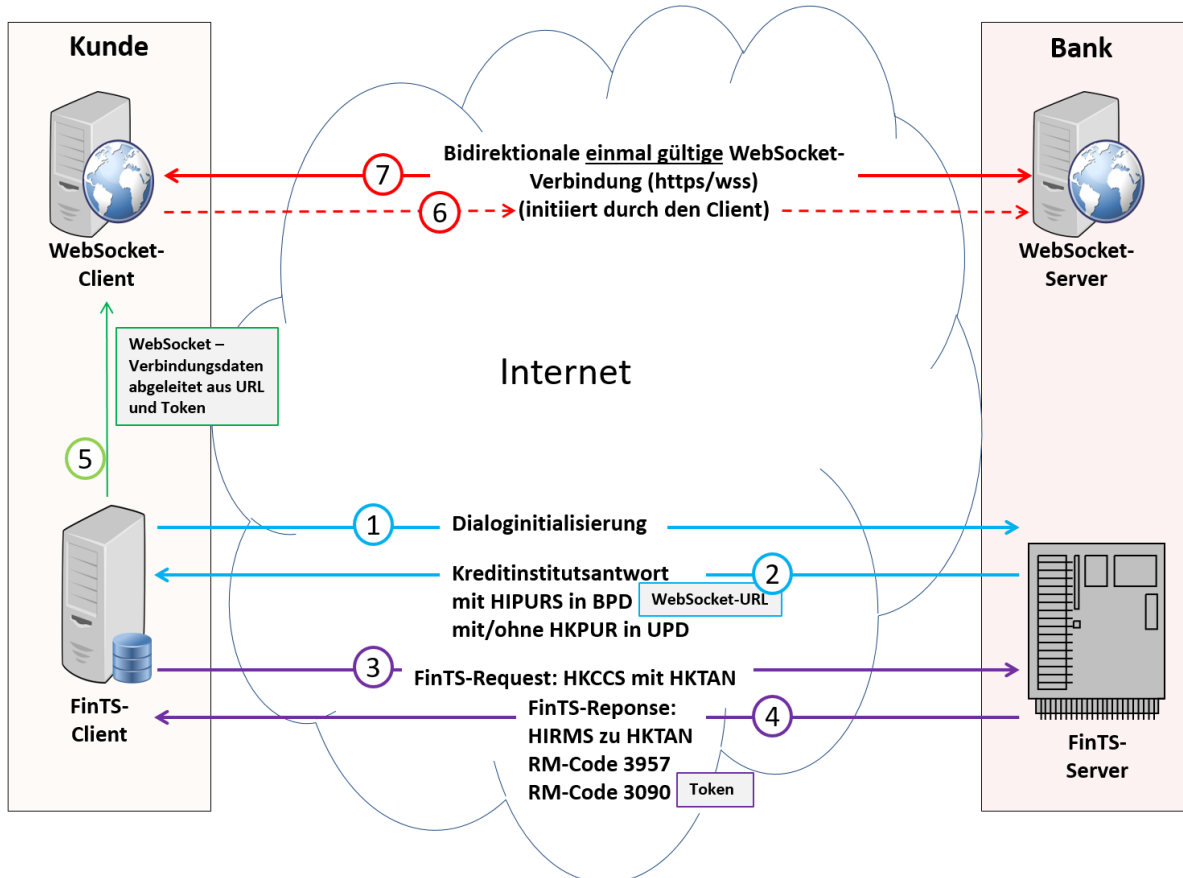
Zusammenspiel WebSocket und FinTS in der Kreditinstituts- bzw. Kundensphäre: grün

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: D
Kapitel: Abgrenzung FinTS Sphäre – WebSocket-Verbindung Abschnitt: Beispiele für das Zusammenspiel der verschiedenen	Stand: 16.12.2021	Seite: 29

## D.1.1 Beispiel: Aufbau einer einmal gültigen WebSocket-Verbindung

### D.1.1.1 Ablaufbeschreibung

Das Beispiel entspricht dem Szenario „Basisfunktionalitäten für Push-Services“ bei DK-TAN-Verfahren „DecoupledPush“ (vergl. B.2.2.1). Es gelten die dort beschriebenen Voraussetzungen.

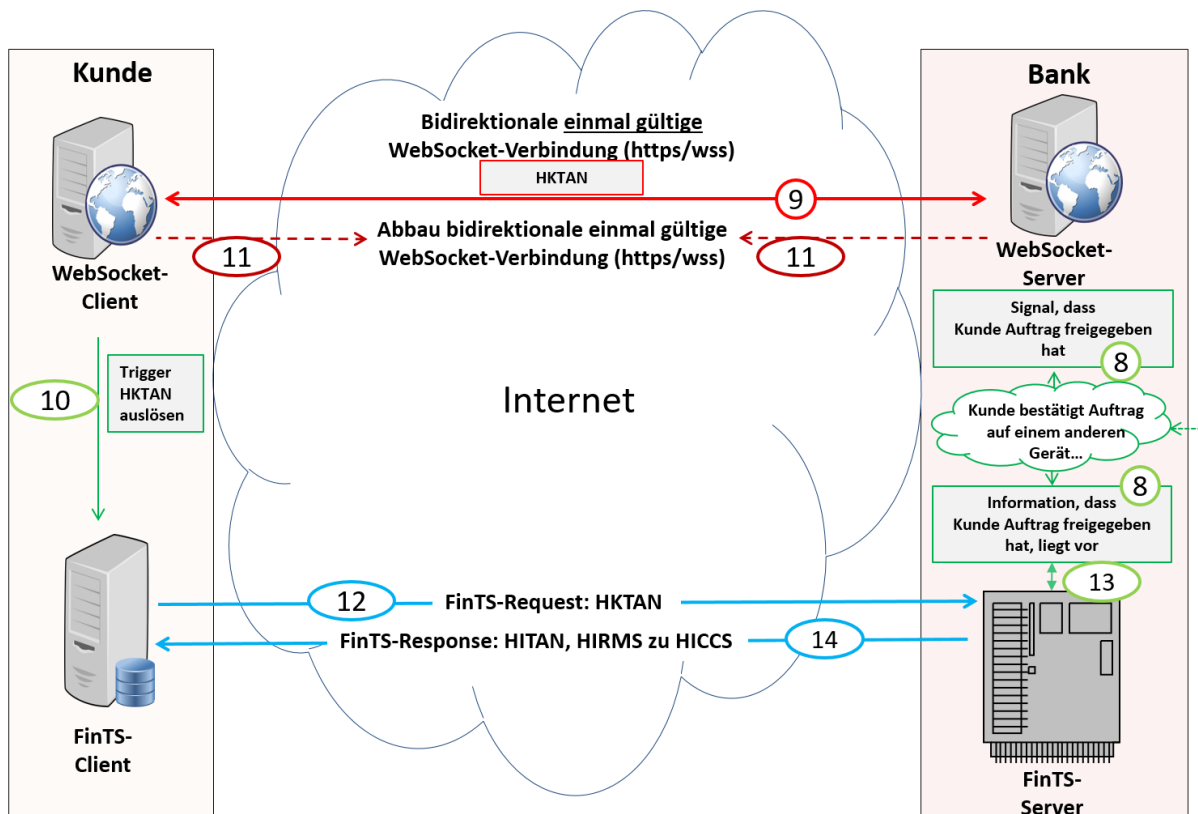


Durch den RM-Code 3957 wird das Kundenprodukt aufgefordert, auf eine Push-Nachricht des Instituts zu warten.

Die folgende Grafik zeigt die Auslösung eines HKTAN im DecoupledPush-Verfahren.

Auch hier sind die einzelnen Aktionen nach zeitlichem Ablauf durchnummeriert und für die verschiedenen Sphären in unterschiedlichen Farben dargestellt:

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: D
Kapitel: Abgrenzung FinTS Sphäre – WebSocket-Verbindung Abschnitt: Beispiele für das Zusammenspiel der verschiedenen	Stand: 16.12.2021	Seite: 30



## D.1.1.2 Verhalten bei Störungen

### D.1.1.2.1 Kunde bestätigt noch vor Aufbau der WebSocket-Verbindung

Es besteht die Möglichkeit, dass ein Kunde einen Auftrag bereits auf einem anderen Gerät freigegeben hat, während die WebSocket-Verbindung noch nicht initiiert wurde bzw. gerade im Aufbau befindlich ist. Das Kreditinstitut hat in diesem Falle die aufgelaufene Push-Nachricht zu puffern, bis die WebSocket-Verbindung steht.

Die Push-Nachricht darf allerdings gelöscht werden, wenn eine WebSocket-Verbindung endgültig nicht zustande gekommen ist, weil das Kundenprodukt bereits Statusabfragen mit TAN-Prozess=S sendet. (s. Kapitel D.1.1.2.2)

### D.1.1.2.2 Die WebSocket-Verbindung kommt nicht zustande

Für den Fall, dass zwar vom Kundenprodukt ein Token über RM-Code 3090 empfangen wurde, sich aber eine WebSocket-Verbindung auch nach mehreren Versuchen nicht einrichten lässt, ist davon auszugehen, dass ein länger andauernder Fehler im Verbindungsaufbau vorliegt.

Um das Kundenprodukt nicht weiter zu blockieren, darf nach Ablauf einer gewissen Zeitspanne, die durch den BPD-Parameter „Polling im Fehlerfall nach“ im HIPURS vorgegeben wird, der RM-Code 3957 „Auf Push-Nachricht warten“ übergangen werden.

Dem Kundenprodukt ist ab dann erlaubt, Statusabfragen mit TAN-Prozess=S zu senden. Sowohl Kundenprodukt als auch Kreditinstitut verhalten sich dann so, als sei das gewählte DK TAN-Verfahren „Decoupled“ und nicht mehr „DecoupledPush“. Das bedeutet, dass das Kreditinstitut nach Ablauf der Zeitspanne als Antwort auf den HKTAN

Financial Transaction Services (FinTS)	Version:	Kapitel:
Dokument: Echtzeitbenachrichtigungen in FinTS	3.0-FV	D
Kapitel: Abgrenzung FinTS Sphäre – WebSocket-Verbindung	Stand:	Seite:
Abschnitt: Beispiele für das Zusammenspiel der verschiedenen	16.12.2021	31

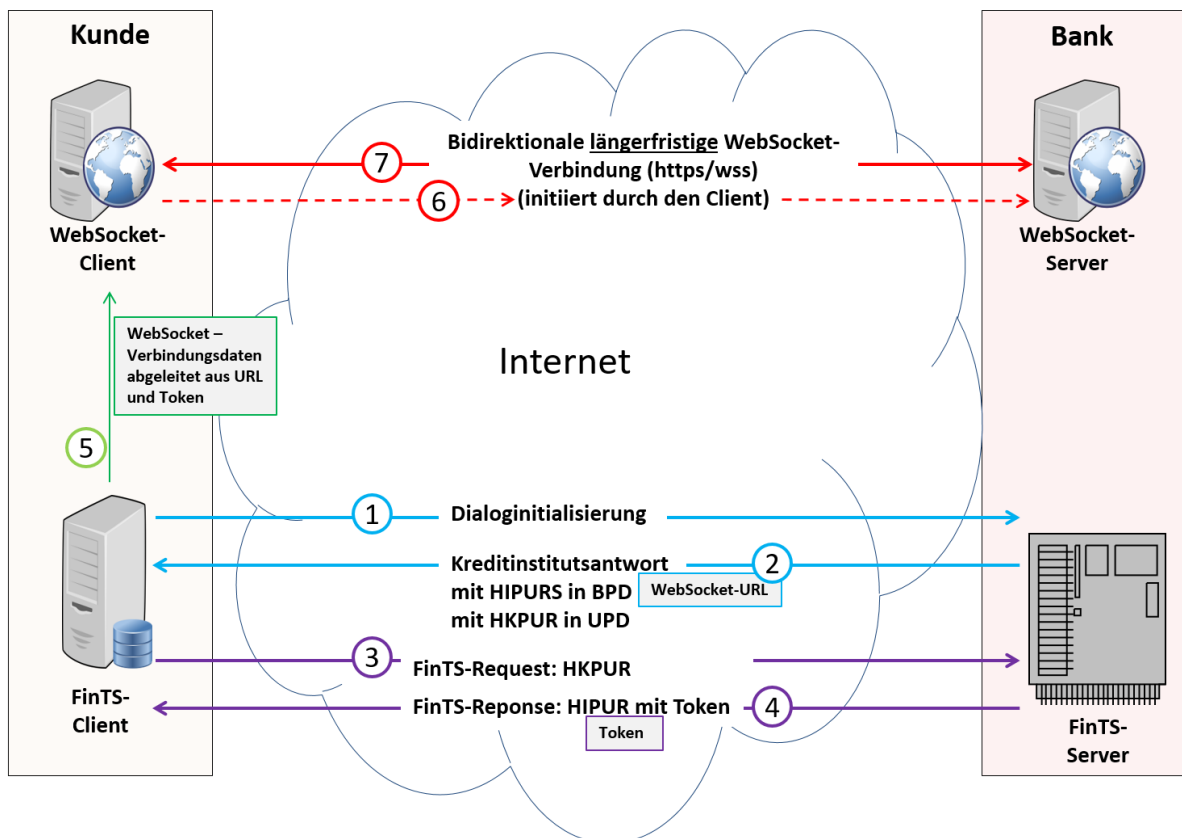
im TAN-Prozess=S nicht mehr erneut die RM-Codes 3957 sowie 3090 als Antwort senden darf. Nach Ausführung der ersten Statusabfrage mit TAN-Prozess=S treten auch die Vorgaben aus HITANS für das DK TAN-Verfahren „Decoupled“ in Kraft.

### D.1.2 Beispiel: Längerfristiger Aufbau einer WebSocket-Verbindung

Der längerfristige Aufbau einer WebSocket-Verbindung wird durch die Verwendung des HKPUR mit gleichzeitiger Anforderung eines Tokens ermöglicht (vergl. B.2.2.2). Es gelten die dort beschriebenen Voraussetzungen (s. B.2.2.1)

„Längerfristig“ heißt in diesem Zusammenhang, dass das Token nicht nur einmal gültig ist, aber durch sein eventuell vorgegebenes Gültigkeitsende beschränkt wird. Während seiner Gültigkeit kann das Token durchgehend genutzt werden. Eine WebSocket-Verbindung auf Basis dieses Tokens kann, im Gegensatz zu einer Verbindung auf Basis eines einmal gültigen Tokens, bestehen bleiben.

Die einzelnen Aktionen sind nach zeitlichem Ablauf durchnummeriert und für die verschiedenen Sphären in unterschiedlichen Farben dargestellt:

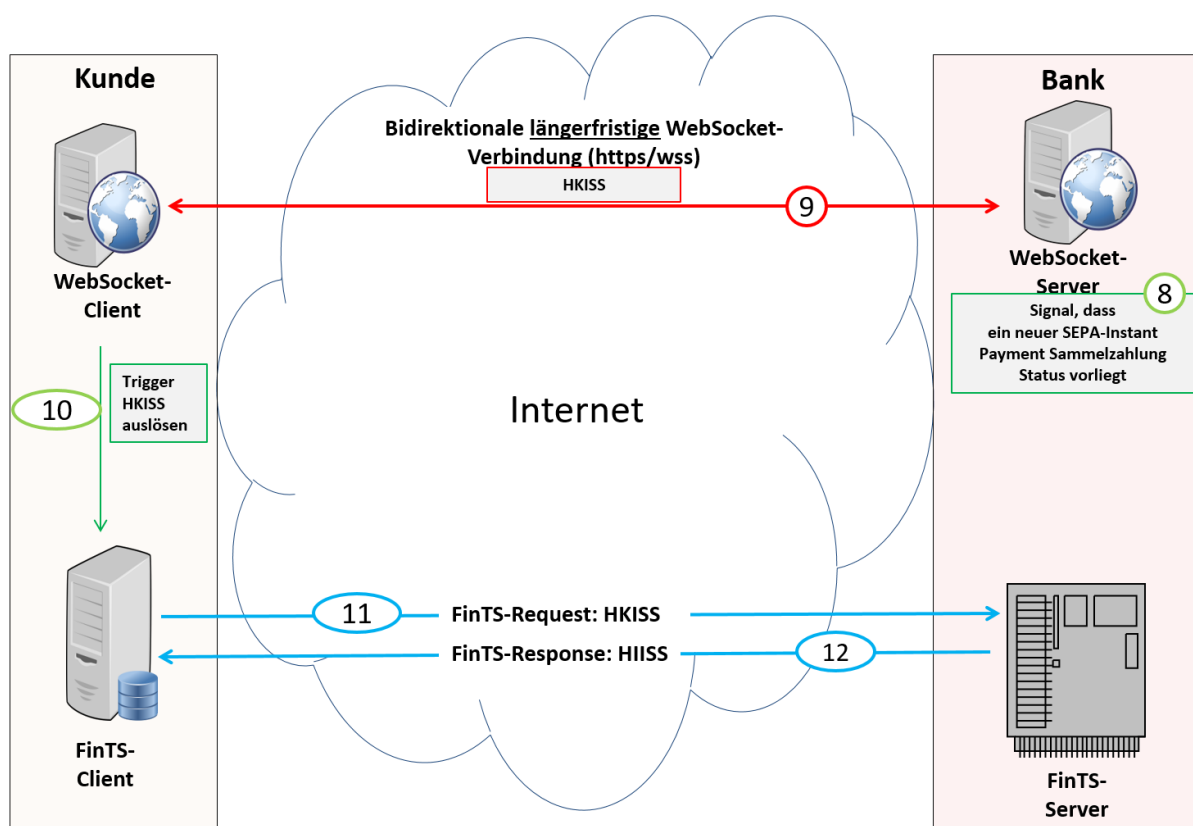


Die folgende Grafik zeigt als Beispiel eine Auslösung eines SEPA-Instant Payment Sammelzahlung Status-Abfrage.

Auch hier sind die einzelnen Aktionen nach zeitlichem Ablauf durchnummeriert und für die verschiedenen Sphären in unterschiedlichen Farben dargestellt:



Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: D
Kapitel: Abgrenzung FinTS Sphäre – WebSocket-Verbindung Abschnitt: Aktionen auf Kreditinstitutsseite	Stand: 16.12.2021	Seite: 32



## D.2 Aktionen auf Kreditinstitutsseite

Das Institut, das den Echtzeitbenachrichtigungsservice anbieten möchte, muss mindestens das Parametersegment HIPURS in der BPD liefern. Je nach Funktionsumfang muss es den Rückmeldecode 3090 und/oder HKPUR sowie die für Push-Services registrierbaren Geschäftsvorfälle in der UPD anbieten.

Die wss-Zugangs-Daten müssen für die beschriebene Verwendung je nach Funktionsumfang für den Rückmeldecode 3090, das Parameter- und ggf. das Antwortsegment des HKPUR erstellt werden können, um sie dann durch den FinTS-Server bereitzustellen. Die Bankseite muss die N potenziellen WebSocket-Verbindungen für ihre M Kunden verwalten können. Die entsprechenden Anmeldetoken müssen ebenfalls verwaltet werden, insbesondere muss eine eindeutige interne Zuordnung zum richtigen Kunden und dessen Kundenprodukten erfolgen.

Zudem erstellt die Bank JSON-Nachrichten, wenn neue Daten auf dem FinTS-Server verfügbar sind oder allgemeine Informationen schnell an den Kunden gesendet werden sollen.

Vorgaben für den Umgang mit Störungen im Ablauf sind zu beachten. Das DK TAN-Verfahren „Decoupled“ ist als „Fallback“-Verfahren zu unterstützen, wenn das TAN-Verfahren „DecoupledPush“ angeboten wird. (s. Kapitel D.1.1.2)

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: D
Kapitel: Abgrenzung FinTS Sphäre – WebSocket-Verbindung Abschnitt: Aktionen auf Kundenseite	Stand: 16.12.2021	Seite: 33

### D.3 Aktionen auf Kundenseite

Das Kundenprodukt eines Kunden, der Echtzeitbenachrichtigungen erhalten möchte, muss die Rückmeldecodes 3090 und 3957 verarbeiten bzw. HKPUR ausführen können. Ebenso muss es Geschäftsvorfälle durchführen können, die durch HKPUR für Push-Services registriert werden dürfen.

Insbesondere muss sein System die zurückgelieferten Informationen aus HIPURS und HIPUR bzw. Rückmeldecode 3090 verstehen und daraus eine entsprechende WebSocket-Verbindung aufbauen können.

Zudem muss das Kundensystem die Push-Nachrichten aus der WebSocket-Verbindung verstehen und entsprechende Aktionen ableiten können (insbesondere Trigger für entsprechende Dialog-Requests in FinTS).

Vorgaben für den Umgang mit Störungen im Ablauf sind zu beachten. Das DK TAN-Verfahren „Decoupled“ ist als „Fallback“-Verfahren zu unterstützen, wenn das TAN-Verfahren „DecoupledPush“ angeboten wird. (s. Kapitel D.1.1.2)

Financial Transaction Services (FinTS) Dokument: Echtzeitbenachrichtigungen in FinTS	Version: 3.0-FV	Kapitel: E
Kapitel: Data Dictionary Abschnitt: Aktionen auf Kundenseite	Stand: 16.12.2021	Seite: 34

## E. DATA DICTIONARY

---

### Benutzerkennung verwenden

Gibt an, ob die Benutzerkennung für die Credential-Erzeugung mitverwendet werden soll.

Typ: DE  
Format: jn  
Länge: #  
Version: 1

### Eindeutige Bezeichnung des Kundenystems

Symbolischer Name des verwendeten Kundensystems. Dieser Name wird vom Kunden vergeben (z.B. Laptop) und erleichtert ihm die Identifikation.

Typ: DE  
Format: an  
Länge: ..32  
Version: 1

### Gültigkeitsende Token

Gültigkeitsende für den Aufbau der wss-Verbindung mittels Zugangstoken. Bei Abbruch der Verbindung kann diese mit dem Sicherheitstoken erneut gestartet werden, so lange das Gültigkeitsende nicht erreicht ist.

Typ: DEG  
Format: tsp  
Länge: #  
Version: 1

### Name des Herstellers

Dieses Element enthält den Firmennamen des FinTS-Kundenproduktherstellers.

Typ: DE  
Format: an  
Länge: ..35  
Version: 1

### Parameter registrierte FinTS-Kundenprodukte für Push-Services

Auftragsspezifische Bankparameterdaten für den Geschäftsvorfall „Registrierte FinTS-Kundenprodukte für Push-Services“.

---

Financial Transaction Services (FinTS)		Version:	Kapitel:
Dokument: Echtzeitbenachrichtigungen in FinTS		3.0-FV	E
Kapitel: Data Dictionary		Stand:	Seite:
Abschnitt: Aktionen auf Kundenseite		16.12.2021	35

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	Eingabe Anzahl Einträge erlaubt	1	DE	jn	#	M	1	

Typ: DEG  
Format:  
Länge:  
Version: 1

### Parameter Push-Services Registrierung

Auftragsspezifische Bankparameterdaten für den Geschäftsvorfall „Push-Services Registrierung“.

Nr.	Name	Version	Typ	Format	Länge	Status	Anzahl	Restriktionen
1	<a href="#">WebSocket-URL</a>	1	DE	an	..256	M	1	
2	<a href="#">Polling im Fehlerfall nach</a>	1	DE	num	..2	M	1	>0
3	<a href="#">Benutzerkennung verwenden</a>	1	DE	jn	#	M	1	
4	<a href="#">Segmentkennung Registrierung</a>	1	DE			O	..99	

Typ: DEG  
Format:  
Länge:  
Version: 1

### Polling im Fehlerfall nach

Dieses Feld gibt an, nach welchem Zeitraum eine Statusabfrage durch das Kundenprodukt zulässig ist, wenn der Versuch des Aufbaus einer WebSocket-Verbindung immer wieder scheitert. (s. Kapitel D.1.1.2)

Der Wert wird in Sekunden angegeben und gilt ab dem Zeitpunkt des Empfangs des Tokens.

Typ: DE  
Format: num  
Länge: ..2  
Version: 1

### Segmentkennung Registrierung

Segmentkennung eines Geschäftsvorfalles, für den Push-Services angeboten werden und für den sich ein Kunde registrieren möchte. Zum Abonnieren allgemeiner Informationen (s. Kapitel C.2) ist das Feld mit dem Wert „INFO“ zu belegen.

Financial Transaction Services (FinTS)		Version:	Kapitel:
Dokument:	Echtzeitbenachrichtigungen in FinTS	3.0-FV	E
Kapitel:	Data Dictionary	Stand:	Seite:
Abschnitt:	Aktionen auf Kundenseite	16.12.2021	36

Typ: DE  
 Format: an  
 Länge: ..5  
 Version: 1

### Token Push-Service

Im Zeitraum der Gültigkeit verwendbares Passwort für den wss-Verbindungsaufbau.

Anforderung ist, dass das Token pro Banksystem eindeutig ist.

Es wird empfohlen, eine UUID (Version 4, d.h. Zufallszahl) gemäß RFC 4122<sup>1</sup> mit der Länge von 16 Bytes zu verwenden.

Typ: DE  
 Format: an  
 Länge: ..80  
 Version: 1

### WebSocket-URL

WebSocket-URL zur Etablierung einer WebSocket-Verbindung. Die Angabe erfolgt inklusive des Dienstbezeichners (z.B. 'https://').

Typ: DE  
 Format: an  
 Länge: ..256  
 Version: 1

---

<sup>1</sup> <https://tools.ietf.org/html/rfc4122>