

Subsembly FinTS Server



Produktinfo

VORLÄUFIG
(ohne Gewähr)

Dieses Dokument ist urheberrechtlich geschützt. Eine Weitergabe des Dokuments oder Auszügen daraus darf, egal in welcher Form, nur mit ausdrücklicher Genehmigung der Subsembly GmbH erfolgen. Die Übergabe des Dokuments begründet keinen Anspruch auf Lizenz.

Es wurden alle Anstrengungen unternommen um die Richtigkeit des Dokuments sicher zu stellen. Subsembly GmbH übernimmt jedoch keine Garantie hinsichtlich der Richtigkeit oder Vollständigkeit. Die Tauglichkeit oder Eignung für einen bestimmten Zweck wird nicht gewährleistet. Die enthaltenen Informationen können ohne besondere Ankündigung geändert werden. Ein Rechtsanspruch ist hieraus nicht ableitbar.

Copyright © 10. Mai. 2019 Subsembly GmbH.

Inhaltsverzeichnis

1 Überblick.....	3
2 Starke Kundenauthentifizierung (SCA).....	5
3 Merkmale.....	7
3.1 Backend-Integration.....	7
3.2 Systemvoraussetzungen.....	8
3.3 Implementierungsumfang.....	8
4 Weitere Informationen.....	10
4.1 Spezifikationen.....	10

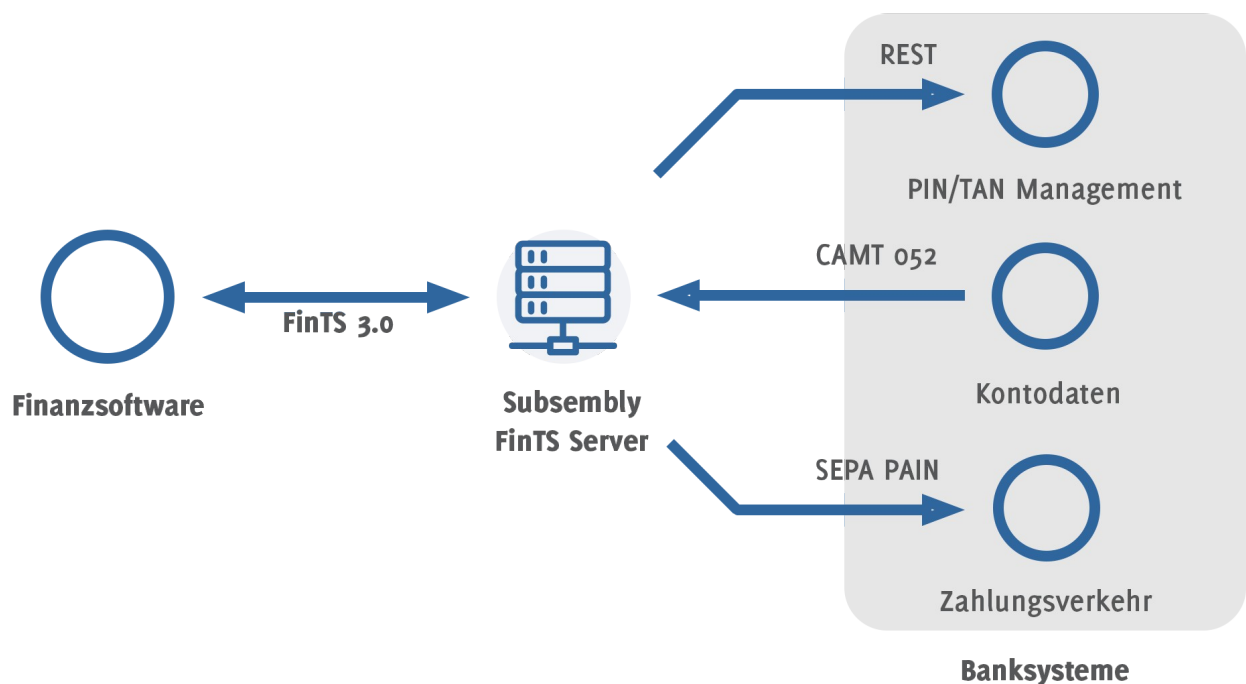
1 Überblick

FinTS steht für *Financial Transaction Services* und ist die von der Deutschen Kreditwirtschaft (DK) verbindlich spezifizierte Kundenschnittstelle für Finanzsoftware.

Der **Subsembly FinTS Server** ist ein plattformneutrales, vollständig auf Basis von .NET Core realisiertes, Servermodul für die Implementierung des FinTS Standards bei Kreditinstituten. Die Software ist als Standardprodukt realisiert und kann mit minimalem Aufwand in eine vorhandene Online-Banking-Infrastruktur einer Bank integriert werden.

Auf der Kundenseite bietet der Subsembly FinTS Server eine Internet-Schnittstelle gemäß der aktuellen FinTS 3.0 Spezifikation einschließlich der neuesten Erweiterungen zur sicheren Kundenauthentifizierung (SCA). Damit erfüllt der Subsembly FinTS Server bereits heute die ab dem 14.09.2019 verbindlichen Anforderungen nach PSD2.

Bankseitig werden die durch das Online-Banking bereits vorhandenen Schnittstellen zur Benutzerverwaltung, Authentifizierung, Kontoinformation und Abwicklung des Zahlungsverkehrs angebunden. Der Subsembly FinTS Server selbst speichert keinerlei Bestandsdaten sondern fungiert ausschließlich als Protokollgateway. Dies stellt eine erhebliche Erleichterung für Betrieb und Wartung des Subsembly FinTS Servers dar und erlaubt die Nutzung von Cloud-Diensten wie Microsoft Azure.



Auf Basis des Subsembly FinTS Servers betreibt Subsembly ein *Subsembly FinTS Dummy* Testsystem für Entwicklung, Test und Validierung von FinTS Kundensystemprodukten. Mit Hilfe des Subsembly FinTS Dummy können Entwickler von FinTS Kundenprodukten schon jetzt die ab dem 14.09.2019 wirkende starke Kundenauthentifizierung implementieren und testen. Das Verhalten unter verschiedenen Testszenarien kann wiederholt und ohne Risiko ausführlich getestet werden.

2 Starke Kundenauthentifizierung (SCA)

Der Subsembly FinTS Server implementiert bereits die von PSD2 für den Zugriff auf Zahlungsverkehrskonten geforderte starke Kundenauthentifizierung. Hierbei gibt es verschiedene Konfigurationsmöglichkeiten.

SCA optional In diesem Modus erzwingt der Subsembly FinTS Server niemals eine starke Kundenauthentifizierung per HKTAN6. Dennoch kann sich ein Kundensystem mit HKTAN6 anmelden und erhält als Antwort immer eine TAN-Ausnahme. In diesem Modus ist der Subsembly FinTS Server kompatibel mit alter FinTS Kundensystemsoftware ohne SCA und mit neuer FinTS Kundensystemsoftware mit SCA.

Bietet ein Institut lediglich den Zugriff auf Nicht-Zahlungsverkehrskonten an, so kann dieser Modus sinnvoll sein.

SCA erforderlich Ein Standarddialog kann nur mit HKTAN6 in der Dialoginitialisierung eröffnet werden. Ohne HKTAN6 wird der Dialog sofort mit dem Rückmeldecode 9075 abgebrochen.

Basierend auf Zeitstempel, Benutzerkennung und Kundensystem-ID kann für eine Anmeldung mit SCA auch eine TAN-Ausnahme generiert werden, zum Beispiel wenn eine SCA nur alle 90 Tage durchgeführt werden soll.

In diesem Modus ist für spezielle Administrative Vorgänge (Abruf TAN-Verfahren, PIN/TAN-Verwaltung, Synchronisierung) dennoch eine Anmeldung ohne SCA möglich.

SCA ab ... erforderlich Der gewählte Modus ist abhängig vom eingestellten Kalenderdatum. Vor dem eingestellten Kalenderdatum ist SCA optional, danach ist sie zwingend erforderlich. Dies ermöglicht eine vollautomatische Umstellung zum Stichtag 14.09.2019.

Ein laufender FinTS Dialog im Subsembly FinTS Server befindet sich grundsätzlich in einer von drei Authentifizierungsebenen. Parallel dazu kann für jeden Geschäftsvorfall eine von fünf erforderlichen Authentifizierungsebenen festgelegt werden.

Anonym Es ist keinerlei Kundenauthentifizierung erforderlich. Es können nur

anonyme Geschäftsvorfälle, wie zum Beispiel eine Gastmeldung, ausgeführt werden.

PIN-Authentifizierung

Der Kunde ist lediglich durch seine PIN authentifiziert. Eine SCA wurde noch nicht durchgeführt, bzw. ist nicht erforderlich. In dieser Authentifizierungsebene ist beispielsweise der Abruf eines Wertpapierdepots möglich. In dieser Authentifizierungsebene werden vom Subsembly FinTS Server niemals UPD an das Kundensystem übermittelt.

SCA-Authentifizierung

Der Kunde ist durch eine starke Authentifizierung authentifiziert. Dies gilt auch bei einer SCA TAN-Ausnahme, z.B. bei Anmeldung innerhalb von 90 Tagen. Dies ist z.B. die Voraussetzung für die Übermittlung der UPD an das Kundensystem.

TAN teilweise erforderlich

Hiermit zeigt ein Geschäftsvorfall an, dass eine geschäftsvorfallsbezogene TAN erforderlich sein kann. Der Dialog selbst muss zuvor mindestens mit einer PIN des Kunden authentifiziert worden sein. Eine TAN-Ausnahme ist nur mit SCA möglich, zum Beispiel bei Überweisungen von Kleinstbeträgen.

TAN immer erforderlich

Hiermit zeigt ein Geschäftsvorfall an, dass immer eine geschäftsvorfallsbezogene TAN erforderlich ist. Der Dialog selbst muss zuvor mindestens mit einer PIN des Kunden authentifiziert worden sein.

3 Merkmale

Der Subsembly FinTS Server wird von Subsembly als sofort installierbares System zusammen mit einem umfangreichen Entwicklerkit ausgeliefert. Der Entwicklerkit ermöglicht eine selbständige Integration und den Betrieb des Subsembly FinTS Servers ausschließlich mit eigenen Ressourcen. Gerne ist Subsembly bei Implementierung und Betrieb behilflich, oder kann dies auch komplett für Sie übernehmen.

3.1 Backend-Integration

Der Subsembly FinTS Server ist ein sofort installierbares Standardprodukt und zeichnet sich durch eine besonders einfache Backend-Integration aus. Hierzu definiert der Subsembly FinTS Server einige wenige, einfache Programmcode-Schnittstellen welche bankseitig implementiert (programmiert) werden müssen. Zur weiteren Vereinfachung liefert Subsembly bereits Beispielimplementierungen dieser Schnittstellen als C# Quellcode aus. Auf dieser Basis kann die Integration durch das Kreditinstitut selbst, oder durch unsere Mitarbeiter zügig umgesetzt werden.

Üblicherweise existieren die für die Integration erforderlichen Schnittstellen zum Kernsystem der Bank bereits durch das Browser basierte Internetbanking. Der Subsembly FinTS Server wird im Normalfall einfach an diese Schnittstellen angekoppelt. Besonders einfach ist die Integration wenn die Bank bereits eine offene REST API zur Verfügung stellt, welche vom Subsembly FinTS Server genutzt werden kann.

Grundsätzlich müssen durch das Online-Banking-Backend, oder durch zusätzliche Implementierung, folgende Dienste für den Subsembly FinTS Server zur Verfügung gestellt werden:

- Benutzerverwaltung mit zugehöriger Berechtigungsstruktur.
- Verwaltung und Prüfung der Online-Banking-PIN der Benutzer.
- Verwaltung der unterstützten TAN-Verfahren, Erstellen von TAN-Challenges und die TAN-Prüfung im Zusammenhang mit den Auftragsdaten.
- Bereitstellen allgemeiner Kontoinformationen für den jeweiligen Benutzer. (Geschäftsvorfall HKUPD)

- Bereitstellen von Kontoumsatzdaten im CAMT 052/053 oder SWIFT MT-940 Format. Hierbei müssen die Kontoumsatzdaten für mindestens die letzten 90 Tage bereitgestellt werden. (Geschäftsvorfälle HKCAZ und/oder HKKAZ)
- Entgegennehmen von vorvalidierten Zahlungsaufträgen im SEPA PAIN Format. (Alle SEPA Zahlungsverkehrsgeschäftsvorfälle)
- Optional: Bereitstellung von Wertpapierdepotbeständen im SWIFT MT-535 Format (Geschäftsvorfall HKWPD)
- Eine Anbindung weiterer Geschäftsvorfälle ist jederzeit möglich.

3.2 Systemvoraussetzungen

Der Subsembly FinTS Server ist ein reines Protokollgateway und speichert keinerlei bankfachlichen Kunden- oder Kontodaten. Es werden ausschließlich die für den laufenden Betrieb und für die korrekte Realisierung des FinTS Protokolls erforderlichen, transienten Zustandsdaten in wenigen Datenbanktabellen abgelegt.

Der Subsembly FinTS Server nutzt und benötigt die Microsoft .NET Core 2.1 Laufzeitumgebung welche von Microsoft für Windows, macOS und verschiedene Linux Distributionen kostenlos zur Verfügung gestellt wird. Ausführliche Informationen über Microsoft .NET Core finden Sie auf <https://www.microsoft.com/net>.

.NET Core ist sehr performant, skalierbar und ermöglicht sehr kurze Antwortzeiten.

3.3 Implementierungsumfang

Der Subsembly FinTS Server implementiert ausschließlich FinTS 3.0 nach der jeweils aktuellen Spezifikation. Ältere FinTS/HBCI-Versionen werden nicht unterstützt, da diese spätestens ab dem 14.09.2019 durch die neuen PSD2 Anforderungen obsolet sind.

Weitere Festlegungen der Implementierung sind:

- Es werden ausschließlich PIN/TAN basierte Sicherheitsverfahren unterstützt. Schlüsseldateien (RDH/RAH) oder Chipkarten (RDH/RAH/DDV) werden nicht unterstützt.
- Für alle TAN-Verfahren wird ausschließlich die TAN-Prozessvariante 2 unterstützt.
- Es wird ausschließlich die Dialogsprache "Deutsch" unterstützt. Weitere Sprachen sind auf Wunsch möglich.
- Ein Benutzer wird ausschließlich durch seine Benutzerkennung identifiziert. Eine zusätzliche Kunden-ID ist nicht erforderlich.

Folgende Administrative Geschäftsvorfälle werden direkt durch den Subsembly FinTS Server, basierend auf der Back-End-Integration behandelt:

- HKIDN / HKVVB im Rahmen der Dialoginitialisierung
- HKUPD zum Abruf der verfügbaren Konten. Wird implizit vom HKVVB aufgerufen, kann aber auch individuell im Rahmen eines Dialogs aufgerufen werden.
- HKTAN im Rahmen des 2-Schritt-TAN-Prozesses
- HKPIN Automatische Erzeugung eines gültigen HIPINS-BPD-Segments
- HKSYN, ausschließlich für die Synchronisierung der Kundensystem-ID
- HKTAB zum Abruf der verfügbaren TAN-Medien
- HKEND zur Dialogbeendigung

Im Rahmen der Back-End-Integration können beliebige bankfachliche Geschäftsvorfälle umgesetzt werden.

4 Weitere Informationen

4.1 Spezifikationen

Deutsche Kreditwirtschaft / FinTS:

<https://die-dk.de/zahlungsverkehr/electronic-banking/fints/>

<https://www.hbci-zka.de/>

Microsoft .NET Core 2.1:

<https://www.microsoft.com/net/download/dotnet-core/2.1>