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

Anforderungen an eine Datenschnittstelle für Drittdienste

Finale Version

A. Hintergrund

Die Novellierung der Zahlungsdiensterichtlinie (PSD 2) sieht vor, dass sogenannte dritte Zahlungsdienstleister Zugang zu Bankdienstleistungen erhalten können. In Artikel 98 wird angekündigt, dass hierzu technische Standards zur Authentifizierung und Kommunikation entwickelt werden sollen.
Die Deutsche Kreditwirtschaft (DK) kann diesen Prozess mit ihren Erfahrungen aus dem Bereich der Standardisierung bankfachlicher Schnittstellen unterstützen. Die DK ist bereits Herausgeber verschiedener Schnittstellenstandards für den Privat- und Firmenkundenbereich, die teilweise zusammen mit den französischen Banken entwickelt wurden und in Frankreich, Deutschland und der Schweiz im Einsatz sind.

B. Vorgehensweise

Die DK schlägt eine mindestens zweistufige Vorgehensweise zur Abstimmung einer PSD 2 konformen Schnittstelle für dritte Zahlungsdienstleister vor. Zum jetzigen Zeitpunkt sollten zuerst die Anforderungen an eine neu zu schaffende Schnittstelle für PSP definiert werden, die im Folgenden gemeinsam mit allen Marktteilnehmern abgestimmt und verabschiedet werden. Denn die Interessenlage der einzelnen Marktteilnehmer ist derzeit noch zu uneinheitlich, um schon

konkrete Vorschläge vorlegen zu können. Besonders wichtig ist daher, dass der Prozess der Schnittstellendefinition für alle Beteiligten transparent ist.
Wenn bzgl. der grundsätzlichen Anforderungen und Rahmenbedingungen Einigkeit erzielt wurde, sollte auf dieser Basis in einem zweiten Schritt eine konkrete technische Ausprägung erarbeitet werden.

C. Anforderungen an eine Datenschnittstelle für Drittdienste

Nachfolgend sind die aus Sicht der DK wesentlichen Anforderungen genannt, wobei folgende Teilgebiete zu unterscheiden sind:

- Organisatorische Abläufe
- (Bank-)Fachlichkeit und Autorisierung
- Technische Abwicklung
- Authentifizierung

C.1 O - Anforderungen an organisatorische Abläufe

O1	Es darf für die technische Kommunikation nur eine einzige Schnittstelle geben, die europaweit standardisiert und für alle Drittdienste und Anwendungsszenarien einheitlich ist. Es kann weder den Banken zugemutet werden, für verschiedene Drittdienste unterschiedliche Schnittstellen unterstützen zu müssen, noch den Drittdiensten zugemutet werden, für die einzelnen Mitgliedsländer unterschiedliche Bankzugänge zu implementieren. Neben dieser einen Datenschnittstelle zu Drittanbietern muss es auch möglich sein, dass Banken darüber hinaus ihre eigenen Schnittstellen definieren und nutzen können, z. B. für eigene Services im bilateralen Verhältnis mit dem Kunden.

O2	Die Definition der Schnittstelle muss in einem transparenten Prozess durch die betroffenen Marktteilnehmer (Drittdienste, Zahlungsdienstleister) erfolgen. Eine proprietäre Spezifikation durch Dritte (z. B. BSI, ENISA) könnte dazu führen, dass nicht-marktgerechte Anforderungen zu erfüllen sind. Geeignet wäre aus Sicht der DK hierfür z. B. das aktuelle New Work Proposal der ISO ISO/TC 68/SC 2.
O3	Die Governance, d. h. Pflege und Weiterentwicklung der Schnittstelle, sollte durch eine zentral beauftragte neutrale Stelle erfolgen (z. B. ISO, CEN, ETSI). Die Anwender (dritte Zahlungsdienstleister und Kreditinstitute) sollten mittels eines standardisierten Change-Request-Verfahrens die Möglichkeit haben, Anforderungen an die Schnittstelle zu formulieren, die im Rahmen eines transparenten Prozesses bearbeitet werden.
O4	Die Schnittstelle darf ausschließlich für Berechtigte (d. h. zugelassene dritte Zahlungsdienstleister) zugänglich sein; diese müssen sich bei jedem Dialogaufbau bzw. jeder Serviceanfrage legitimieren.
O5	Es muss ein formaler Prozess bei einer neutralen Instanz zur Registrierung bzw. Lizenzierung von Drittdiensten aufgesetzt werden. Dieser muss für alle Beteiligten transparent sein, mit eindeutigen Kriterien, welche Voraussetzungen erfüllt sein müssen, um registriert zu werden bzw. eine Lizenz zu bekommen. Hierzu gehören auch zu erfüllende Sicherheitsanforderungen. Alle teilnehmenden und lizenzierten Drittdienste müssen in einer europaweit übergreifenden Registrierungsinfrastruktur geführt werden. Separate Register pro Land, auf die jede europäische Bank zugreift, wären nicht praktikabel. ASPSPs sollten bei Bedarf ebenfalls die Rolle eines Drittanbieters einnehmen können. Aufgrund der für Banken bereits geltenden Regularien wird davon ausgegangen, dass die geforderten Voraussetzungen dort als erfüllt gelten. Für den technischen Nachweis der Legitimation eines Drittanbieters („Anbieterkennung“) wird ein zertifikatsbasierter Ansatz empfohlen. Die Zertifikate sollten im Rahmen einer vertrauenswürdigen Zertifikatsinfrastruktur z. B. auf Basis von TSLs (Trustservice Status List) ausgestellt werden, d. h. der Zahlungsdienstleister muss sich darauf verlassen können, dass es sich bei einem Nutzer, der sich mit einem Zertifikat an der Schnittstelle anmeldet, um einen zugelassenen dritten Zahlungsdienstleister gemäß PSD 2 handelt. Hierzu gehört z. B. die Überprüfung signierter Zertifikate online oder mittels Sperrlisten und der Aufbau einer Private Key Infrastructure auf Basis von Trust-Centern. Auch müssen ggf. Kontoberechtigungen im Vorfeld geprüft werden.

	Trust Center müssen ohne vorhandene vertragliche Beziehung zwischen ASPSP und PSP betrieben werden können. Zusätzlich wären im Rahmen entsprechender Policies noch festzulegen: Aktualisierung, Service Level (Verfügbarkeit), Neuzulassung, Sperren. Abhängig von den rechtlichen Anforderungen an Dritte (z. B. Datenschutz) müssten Zulassungsverfahren bzw. Erklärungen der PSPs definiert werden.
O6	Es wird eine zentrale Liste aller Kreditinstitute und eine Adresse der Erreichbarkeit (IP-Adressen, URLs) benötigt, so dass Drittdienstleister die Institute ansprechen können. Alternativ kann diese Information je nach Ausgestaltung der Schnittstelle auch über den Kunden an den Dritten durchgereicht werden.
O7	Im Rahmen des Registrierungsprozesses (siehe O5) erhält der Drittanbieter eine eindeutige „Anbieterkennung", die ihn als PSD 2 konformen Anbieter ausweist und mit der er sich bei den entsprechenden europäischen Zahlungsdienstleistern legitimieren kann. Der Zahlungsdienstleister muss im Rahmen des eigenen Risikomanagements prüfen, ob das Zertifikat gültig ist und nicht widerrufen wurde.
O8	Die Schnittstelle soll architektonisch aus getrennten Schichten aufgebaut sein, die funktional und vom Rollenmodell voneinander unabhängig sind. Ein beispielhaftes Modell könnte folgendermaßen aussehen: 1. Eine Transportschicht definiert die technische Abwicklung und somit die grundlegende Kommunikation (Verbindungsaufbau, Serviceanfrage/-antwort, Fehlerprotokollierung, Sicherheitsverfahren etc.). 2. Eine Sicherheitsschicht beinhaltet die verwendeten Verfahren für Authentifizierung und Vertraulichkeit. In ihr enthalten sind auch Managementfunktionen für die Authentifizierungsinstrumente der Kunden, die in direkter Kommunikation zwischen Kunde und Kreditinstitut abgewickelt werden, also nicht Inhalt der neu zu definierenden Schnittstelle sind. 3. In einer Anwendungsschicht ist die Autorisierung enthalten und es werden die bankfachlichen Daten transportiert. Hiermit soll erreicht werden, dass eine Änderung der bankfachlichen Formate oder die Definition neuer bankfachlicher Geschäftsvorfälle keine Auswirkungen auf andere Schichten hat.

	4. Eine Präsentationsschicht kann sich auf der Seite des Drittanbieters befinden, d. h. dort würde entschieden, wie die Daten auf dem Endgerät des Kunden angezeigt werden.
O9	Der nutzbare Funktionsumfang der Schnittstelle muss auf das gesetzliche Minimum beschränkt werden können. So darf die im Erwägungsgrund 51a genannte Ausnahme – für Zahlungen mit geringem Risiko (bspw. Kleinbetragszahlungen am POS) weniger strenge Sicherheitsanforderungen anzuwenden – nicht als allgemein gültige Regel definiert werden. Dies ist heute eine individuelle Entscheidung jeder Bank auf Basis von entsprechenden Risikovorgaben. Gleichwohl muss die Schnittstelle so aufgebaut sein, dass sie bei Bedarf auf Institutsebene fachlich leicht erweitert werden kann. Somit könnten ggf. zukünftige PSD-Erweiterungen berücksichtigt werden. Es darf nicht sein, dass die technische Beschaffenheit der Schnittstelle die Fachlichkeit einschränkt und bei Erweiterungen hohe Investitionen in Umsetzungen erzeugt.
O10	Kontoinformationsdienst: Banken können, basierend auf ihrem Risikomanagement und einer Vereinbarung mit dem Kunden, lesenden Kontenzugriff auch ohne starke Authentifizierung anbieten.
O11	Deckungsabfragedienst / Herausgeber von Zahlungsinstrumenten (Drittkartenherausgeber): Es ist zu prüfen, in welchem Detailgrad der Kontoinhaber über Deckungsabfragen informiert werden muss? Informiert wird lediglich über Zeitpunkt der Abfrage, Höhe der abgefragten Summe sowie die gegebene Antwort durch den ASPSP und die PIISP-Identität. Es muss noch geklärt werden, wie die Rückantwort an den PIIS aussieht. Eine Auskunft auf Existenz des Kunden und des Kontos sollte vermieden werden.
O12	Eindeutigkeit der Schnittstelle Die Schnittstelle muss so stringent spezifiziert sein, dass es keine Mehrdeutigkeiten oder Auslegungen geben kann. Auch müssen die technischen Parameter und Protokolle so eindeutig sein, dass ein Drittanbieter mithilfe seiner Anbieterkennung und Kenntnis der Adressinformationen (z. B. URL) ohne weitere Abstimmungen eine Verbindung zum Zahlungsdienstleister aufbauen und zugelassene Services nutzen kann.
O13	Versionsfähigkeit Die Schnittstelle muss so konzipiert werden, dass sie eine Versionsverwaltung auf Protokollebene erlaubt, d. h. dass anhand von eindeutigen Versionsinformationen innerhalb des Protokolls eine Kommunikation auf unterschiedlichen Versionen möglich ist. Zudem muss ein versionsneut-

	raler Zugang – z. B. über einen speziellen XML-Namespace – vorgesehen werden, über den alle standardisierten und freigegebenen Protokollversionen abrufbar sein sollen. Damit kann eine fehlerfreie Kommunikation zwischen jedem beliebigen Drittanbieter und jeder Bank ermöglicht werden.

C.2 B - Anforderungen aus Sicht der Bankfachlichkeit

B1	Für die Übermittlung bankfachlicher Daten sollte auf bestehende normierte Standards zurückgegriffen werden (ISO 20022, SEPA pain, camt). Ggf. müssen für die Formate spezielle Belegungsrichtlinien definiert werden, damit Drittdienste nur die für sie benötigten Informationen erhalten.
B2	Die Schnittstelle sollte ein Berechtigungskonzept beinhalten, mit dem gesteuert wird, welche Arten von Geschäftsvorfällen für einen Drittdienst zulässig sind. Bspw. muss gewährleistet sein, dass Zahlungsauslösedienste keine Umsatzdaten abrufen können.
B3	Für jeden Servicebereich darf es nur ein oder mehrere exakt definierte Datenaustauschformate geben, bspw. sind einem Zahlungsauslösedienst nur vordefinierte Zahlungsformate zuzuordnen. Mit einem Kontoinformationsdienst werden nur Datenaustauschformate für Kontoinformationen verknüpft.
B4	Das Schnittstellenprotokoll sollte Möglichkeiten für die Übertragung von bankfachlichen Steuerungsinformationen (IBAN, BIC) außerhalb der Standardformate bieten, um z. B. Routinginformationen zu erhalten, ohne das gesamte bankfachliche Format lesen zu müssen.
B5	Die Schnittstelle sollte die Möglichkeit bieten, dass Zahlungsdienstleister die Art und den Umfang der für Drittdienste angebotenen Services sowie die Parameter des jeweiligen Services dem Drittdienst z. B. im Rahmen des Dialogaufbaus mitteilen können, um so dem Drittdienst zu erlauben, diese Informationen für die Kommunikation zu berücksichtigen.[1]
B6	Ein kontoführendes Institut darf für den Kunden bei eine generelle Blacklist einrichten können, wenn dieser nicht über Drittdienste kommunizieren möchte.

[1] z.B. sollte ein Zahlungsdienstleister einem Kontoinformationsdienst vorab mitteilen können, für wie viele Tage rückwirkend Kontoumsatzinformationen bereitgestellt werden.

C.3 T - Anforderungen an die technische Abwicklung

T1	Die Schnittstelle sollte auf gängigen Internet-Standards basieren (z. B. XML, XML Schema, XML Signature, Web Services, JSON oder REST-API).
T2	Die Schnittstelle sollte einen service- und dialogorientierten Betrieb ermöglichen: • In einem serviceorientierten Betrieb kann eine Serviceanfrage innerhalb eines Request-/Response-Zyklus erfolgen. Ein Beispiel hierfür sind Zahlungsauslösedienste. Für einen serviceorientierten Betrieb müssen die technischen und fachlichen Rahmenbedingungen im Vorfeld ausgetauscht worden sein, da diese während des Prozesses nicht ausgetauscht werden können. • Im dialogorientierten Betrieb können im Rahmen einer Initialisierung spezielle Parameter für diesen Dialog ausgehandelt werden. Diese gelten dann für die Serviceanfrage, die innerhalb des Dialoges erfolgt. Kontoinformationsdienste können z. B. dialogorientiert sein.
T3	Im dialogorientierten Betrieb muss es möglich sein, die Eigenschaften der Schnittstelle in Form von Parametern auszutauschen. Damit können einem Drittanbieter abhängig von seiner Anbieterkennung unterschiedliche Services angeboten werden.
T4	Die Betriebssicherheit der technischen Schnittstelle muss gewährleistet sein, d. h. es muss anhand des Protokollverhaltens für den Drittanbieter eindeutig erkennbar sein, ob eine Serviceanfrage ausgeführt wurde oder nicht. Zusätzlich müssen bei Ablehnungen fachliche Informationen geliefert werden, wie der Fehler behoben werden kann. Insbesondere muss klar erkennbar sein, ob eine zurückgewiesene Serviceanfrage unverändert wieder eingereicht werden soll, oder nicht.
T5	Wiedereinreichungskontrolle Falls Serviceanfragen in unveränderter Weise wiederholt eingereicht werden, muss dies auf Protokollebene erkennbar sein, so dass es nicht zu Mehrfachverfügungen kommen kann.
T6	Fragmentierung Bei Serviceanfragen, wie z. B. Kontoinformationsdiensten, können die erzeugten Serviceantworten ggf. mehrere Megabyte groß sein. Daher müssen auf Protokollebene Möglichkeiten existieren, um die Antwortnachrich-

	ten in definierten Teilstücken übertragen zu können.
T7	Fehlerbehandlung Das Schnittstellenprotokoll muss über eine transparente Fehlerbehandlung verfügen. Es müssen eindeutige Fehler bzw. Fehlerklassen definiert sein, mit deren Hilfe ein Dritter auf eindeutige Weise automatische Fehlerbehandlungsroutinen auslösen kann, ohne z. B. die Antwortnachricht textuell auswerten zu müssen. Fehlerklassen wie Information, Warnung und Fehler sollten eine Erstanalyse für Dritte ermöglichen.
T8	Die kommunikationstechnische Anbindung von Drittdiensten erfolgt über Internet-Protokolle.

C.4 S - Anforderungen an die Sicherheit (Authentifizierung und Vertraulichkeit)

S1	Das konkrete Sicherheits- bzw. Authentifizierungsverfahren muss für die Schnittstelle transparent sein, d. h. mit der Festlegung auf ein Schnittstellenformat sollen die Nutzer der Schnittstelle nicht auf eine bestimmte Art der Authentifizierung festgelegt werden. Damit soll erreicht werden, dass die Schnittstelle möglichst unabhängig von den seitens der unterschiedlichen Kreditinstitute verwendeten Authentisierungsverfahren ist. Die Auswertung erfolgt in vor- bzw. nachgelagerten Systemen. Hiermit ist es möglich, trotz unterschiedlichster Authentisierungsverfahren der einzelnen Zahlungsdienstleister dieselbe Schnittstelle zu verwenden.
S2	Statische personalisierte Zugangsdaten (PSC, z. B. statische Passworte) oder biometrische Daten eines PSU sollen nicht missbraucht werden können. Die EBA sollte innovative Lösungen vorschreiben, bei denen ein Kunde seine PSC keinem Dritten mitteilen muss.
S3	PSPs sollten nur die ASPSP-eigenen Authentifizierungsverfahren verwenden dürfen. Letztlich liegt die Primärhaftung bei den ASPSPs. Die Nutzung bestehender Verfahren für Authentifizierung des PSP erfolgt nach Verfügbarkeit der Verfahren beim ASPSP. Ausnahme: Falls ein Institut entscheidet, ein Verfahren nicht mehr via Online Banking anzubieten, da es bspw. die Sicherheitsanforderungen nicht mehr erfüllt, kann es während einer Übergangsphase dazu führen, dass die Authentifizierungsverfahren im Online Banking und in der PSD2

	Schnittstelle nicht einheitlich sind.
S4	Das Schnittstellenprotokoll muss in der Lage sein, sowohl 1-Schritt-Request-/Response-Verfahren als auch 2-Schritt-Challenge-/Response-Verfahren abwickeln zu können. Ein 1-Schritt-Verfahren wäre z. B. für einen Kontoinformationsdienst denkbar, der als Request die konkrete Anforderung inkl. Legitimation des Dienstleisters sendet und als Response die gewünschten Daten zurück erhält. Ein 2-Schritt-Verfahren wäre z. B. bei einem Zahlungsauslösedienst ab einer bestimmten Risikoklasse gegeben, bei der auf Basis des eingereichten Zahlungsauftrags eine Bestätigung der auftragsrelevanten Daten (Challenge) gefordert wird, was dann z. B. zu einem kontextbasierten Einmalpasswort führt.
S5	Sicherheitsverfahren sind soweit zu abstrahieren und zu kapseln, dass diese über eindeutige Kennungen und ggf. Profile beschrieben werden können. Eine solche Kennung identifiziert eindeutig ein Sicherheitsverfahren und die zughörigen Prozesse bei beiden Schnittstellenpartnern. So könnten z. B. unter Profilnamen „SEC1, SEC2 …" unterschiedliche Signatur-, Padding- und Hashverfahren zusammengefasst sein. Das Aushandeln eines geeigneten Verfahrens zwischen Drittanbieter und Bank würde dann nur auf Basis der Profilnamen stattfinden, was die Komplexität der Datenschnittstelle verringern hilft.
S6	Für die Verschlüsselung der Daten zwischen dem Dritten und dem Zahlungsdienstleister ist eine Standardverschlüsselung wie TLS mit aktuellen Kryptomechanismen zu verwenden, um die Vertraulichkeit der Daten zu gewährleisten.