APIs für Kontoabfragen und Banktransaktionen

Miteinander reden

Christian Kirsch

Ab Mitte 2019 müssen Banken in der EU anderen Firmen eine API anbieten, mit der diese auf Konten von Privatkunden zugreifen können. Schon heute gibt es einige solcher Schnittstellen, nicht nur von Banken.

Am Anfang stand in Deutschland HBCI. Das „Home Banking Computer Interface“ definierte ein Protokoll für den Zugriff auf Bankkonten via Internet. Seine erste praxisrelevante Version, 2.0.1, erschien 1998 und setzte voll auf Sicherheit: Kunden mussten ihre Transaktionen mit einem Schlüssel freigeben, der auf einem externen Medium gespeichert war. Anfangs nutzte man Disketten und Chipkarten dafür, später USB-Sticks.

PIN-TAN statt Chipkarte

Was Firmen wegen ihrer Ansprüche an Sicherheit schätzten, kam bei Privatkunden wegen der Umständlichkeit kaum an. 2002 öffnete sich HBCI mit Version 3 für das damals bereits im Web übliche PIN-TAN-Verfahren und firmiert seitdem als FinTS (Financial Transaction Services). Heutzutage bieten gut 2000 hiesige Banken eine FinTS-Schnittstelle mit PIN-TAN-Absicherung der Transaktionen. Bekannteste Ausnahme ist die Commerzbank, die beim externen Schlüsselmedium blieb.

Was bislang eine deutsche Besonderheit war, ist ab 2019 verpflichtend für alle Banken in der EU: Sie müssen eine Schnittstelle anbieten, über die Dritte Kontodaten von Privatkunden lesen und Überweisungen auslösen können. Wohlgemerkt: Dafür ist das Einverständnis des Kontoinhabers nötig, an dessen Authentifizierung hohe Ansprüche gestellt werden. Neben „Wissen“ (PIN) und „Besitz“ (Smartphone, Chipkarte) kommt der Faktor „Inhärenz“ hinzu, der dem Kunden körperlich eigen sein muss – also etwa ein Fingerabdruck. Onlinetransaktionen muss man künftig mit zwei dieser drei Faktoren autorisieren, die voneinander unabhängig sind. Diese und einige andere Vorschriften sind Teil der Zweiten Payment Service Directive (PSD2), die seit Anfang 2018 in allen EU-Mitgliedsstaaten gilt [1]. (Siehe ix.de/ix1803086, [a]; auch die weiteren mit Buchstaben bezeichneten Referenzen beziehen sich auf diese Liste mit Webadressen.) Bis auf das Auslösen von Überweisungen sieht sie jedoch keine von Dritten veranlassbaren Transaktionen vor – Daueraufträge, Lastschriftrückgaben et cetera bleiben also außen vor.

Anders als in Deutschland wird es allerdings auf absehbare Zeit keine einheitliche Banking-API für die Europäische Union geben. Die PSD2 schreibt lediglich deren Vorhandensein vor, äußert sich jedoch nicht zur konkreten Ausgestaltung. Ein Regulatory Technical Standard (RTS, [b]), den die Europäische Bankenaufsicht (EBA) im Auftrag der EU-Kommission definiert hat, enthält ebenfalls keine API-Spezifikation. Er unterscheidet zwischen der Schnittstelle „Online-Banking“ (also der Webanwendung) und einer „dedizierten“ Schnittstelle. Letztere kann eine Bank anbieten, sie muss es aber nicht. Das Interesse an so einer Programmier-API ist aber bei Banken wie anderen Firmen groß, etwa bei den neu auf den Markt drängenden Fintechs (siehe Kasten).

Eigentlich möchten alle eine API

Fintechs wollen klarerweise möglichst einfach auf die Bankkonten zugreifen können. Das ist mit einer definierten API gewährleistet, nicht jedoch mit dem Auslesen der Webseite (Screen Scraping), die die Bank ihren Kunden online präsentiert. Denn deren Struktur und Aussehen kann sich häufig ändern. Umgekehrt erlaubt eine klar beschriebene Schnittstelle den Banken nicht nur Kontrolle über den Zugriff auf die Kundendaten, wie ihn die PSD2 vorsieht. Sie können zudem mit geeigneten Funktionen neue kostenpflichtige Dienste anbieten.

Obwohl auf den ersten Blick alte und neue Player mit einer Programmierschnittstelle besser fahren, gab es bei den Diskussionen um den RTS heftige Debatten zwischen Banken und Verbraucherschützern einer- sowie Fintechs andererseits. Letztere befürchteten, Geldinstitute könnten absichtlich langsame und unzuverlässige APIs bereitstellen, um die Wettbewerber zu behindern. Deshalb wollten sie das Screen Scraping als Fallback festgeschrieben sehen. Dagegen sprachen sich Banken und Verbraucherschützer aus und verwiesen auf die dem Kunden dabei verloren gehende Datenhoheit. Denn beim Screen Scraping lässt sich praktisch nicht verhindern, dass ein Dritter alle im Webbrowser angezeigten Informationen abruft und sich durch sämtliche Daten klickt. Wichtiger dürfte

für Banken jedoch sein, dass auch sie bei dieser Technik die Kontrolle über ihre Kundendaten einbüßen. Sie bevorzugen leicht zu monetarisierende Programmierschnittstellen.

Das demonstriert etwa die Deutsche Bank mit ihrer Ende 2017 vorgestellten API [c]. Sie erlaubt noch keine Zahlungsvorgänge, sondern enthält nur Funktionen, die Transaktionen und Metadaten liefern. Zu letzteren gehört die Information, ob der Kontoinhaber volljährig ist oder ob regelmäßig mindestens eine vorgegebene Summe eingeht. Nutzen darf die REST-Schnittstelle nur, wer sein Projekt vorher von der Bank hat prüfen lassen. Kunden authentifizieren sich prinzipiell auf einer von ihr ausgelieferten Webseite und müssen dort der Verwendung ihrer Daten ausdrücklich und en détail zustimmen. Nutzer der Schnittstelle erhalten also keinen Zugriff auf die Anmeldedaten.

Was eine Anwendung tun darf, definiert dann die Schnittmenge aus von der Deutschen Bank für die App generell und vom einzelnen Kunden gestatteten Funktionen. Die iOS-App „FinanzGuru“ des Start-ups dwins GmbH zeigt, welche Art von Diensten sich das Geldinstitut vorstellt: Die Software wertet Überweisungen und Lastschriften aus und ermittelt daraus Vorschläge, wo der Kontoinhaber Geld sparen kann. Das betrifft zum Beispiel Mobilfunk- und Versicherungsverträge. Aus den Zahlungsterminen versucht FinanzGuru zudem die Vertragslaufzeit zu ermitteln und rechtzeitig auf eine mögliche Kündigung hinzuweisen.

Zusammenarbeit statt Konkurrenz

Auf Kooperation mit anderen Firmen setzt ebenfalls die Hamburger Sutor Bank. Mit ihrer „Startup-Plattform“ [d] wendet sie sich gezielt an Fintechs, die die gesamte Palette an Bankdienstleistungen benötigen. Die Bank sieht ihr Angebot als „Backbone“ für die Newcomer und bietet etwa eine Fondsdepot-Verwaltung für Partner wie den Roboadvisor Growney an. Dabei kommt ihr zugute, dass sie über alle notwendigen Zulassungen für das Bankgeschäft in Deutschland verfügt. Fintechs, die mit der Bank kooperieren, brauchen sich deshalb nicht selbst um diese aufwendige Zulassung zu kümmern. Die Sutor-API bietet Funktionen unter anderem für den Zugriff auf Spar-, Giro- und Depotkonten. Eine Kooperation existiert auch mit dem Innogy-Start-up „Share & Charge“, das per Blockchain „smarte“ Verträge zwischen Anbietern und Nutzern von Ladestationen für E-Autos verwaltet und abrechnet.

Was für die Banken naheliegt, nämlich jeweils eine eigene Schnittstelle zu ihren Diensten anzubieten, ist für Fintechs und Hersteller von Anwendungen weniger reizvoll: Sie müssten ihre Software für jede Ziel-Bank anpassen. Wer möglichst bankenneutral arbeiten will, kann sich bei diversen Lieferanten von Schnittstellen bedienen, die im Wesentlichen alle (deutschen) Institute anbinden. Auf Protokollebene ähneln sich diese Interfaces und die der Banken: Die Daten fließen in der Regel über eine REST-API in Form von JavaScript-Objekten im JSON-Format.

In Deutschland gibt es solche Multi-Banken-APIs unter anderem von BANKSapi, Figo, Subsembly und finAPI. Sie setzen intern FinTS ein oder verwenden Screen Scraping, wenn diese Schnittstelle

Fintechs: Alter Wein und Innovation

Digitale Finanzdienstleister, sogenannte Fintechs, sind ein Liebling von Politikern und Massenmedien. Sie gelten als „innovativ“ sowie „digital“ und vor allem sind sie hip, weil sie wie einst David gegen die als übermächtiger Goliath porträtierten Banken stehen. Schaut man jedoch ein bisschen genauer hin, erinnert manches Fintech eher an die Geschichte von des Kaisers neuen Kleidern.

Da sind etwa die Firmen mit „Roboadvisor“-Diensten: Sie investieren automatisch mithilfe von „Algorithmen“, angeblich für Investoren günstiger und einfacher als andere Anbieter. Tatsächlich handelt es sich jedoch in der Regel nur um eine Art Dachfonds von ETFs (Exchange Traded Funds), zusammengestellt nach der Risikoneigung und Renditeerwartung des Kunden. Ähnliches gibt es als Dachfonds gemanagter Fonds seit Jahren von Investmentgesellschaften. ETFs sind zwar im Prinzip preiswerter als verwaltete („managed“) Fonds, doch an diesem Vorteil nagen die nicht gerade niedrigen Kosten der Roboadvisor. Zudem gibt es, Robo hin, Algorithmus her, selbstverständlich keine Garantie auf Erfolg oder Kapitalerhalt. Wie bei Banken und traditionellen Fonds trägt der Kunde das Risiko und der Anbieter kassiert die sicheren Gebühren.

Ähnlich alten Wein verkaufen andere Fintechs in neuen Schläuchen, etwa digitales Forderungsmanagement oder Bonitätsprüfungen für Ratenkäufe.

Daneben existieren wirklich neuartige Angebote, wie von vermietet.de: Die Firma wertet automatisch Kontodaten von Vermietern aus, um zum Beispiel säumige Mietzahler rechtzeitig zu entdecken und das Zusammenstellen der Nebenkosten zu erleichtern. Allerdings liegen Details wie Namen der Mieter sowie die zugehörige Wohnungsgröße, -lage und -miete in der Cloud von finAPI. Vermieter müssen sich daher fragen, ob sie einer jungen Firma hinsichtlich des Datenschutzes trauen, gerade in Anbetracht der neuen EU-Datenschutzrichtlinie.

Ebenfalls zu Recht dürfte sich Fintiba [k] mit dem Wort „innovativ“ schmücken. Die Firma bedient eine Marktnische, die früher die Deutsche Bank beherrschte: Studenten aus einem Nicht-EU-Land müssen vor Studienbeginn in Deutschland eine bestimmte Summe auf ein Sperrkonto einzahlen. Allerdings war es nicht eben leicht, so ein Konto aus einem weit entfernten Land einzurichten – das PostIdent-Verfahren gibt es eben nur in Deutschland.

Fintiba bietet für die Kontoeröffnung das Identifizieren per Video-Chat an, was dank Internet fast überall auf der Welt möglich ist. Das Führen des Kontos selbst übernimmt die Sutor Bank.

nicht existiert. Unterschiede gibt es vor allem im Funktionsumfang und in der technischen Umsetzung. Gemeinsam sind allen APIs Methoden zur Authentifizierung des Kunden, zur Abfrage seiner Kontenliste und der Umsätze. Und auch das Auflösen von Überweisungen ist mit allen APIs möglich. Das reicht, wenn man nur die in der PSD2 vorgesehenen Funktionen Kontoinformation und Zahlungsauslösung braucht.

Mehr Komfort dank PSD2-API

Solche auf PSD2 zugeschnittenen Schnittstellen bieten unter anderem Figo [e] und BANKSapi [f] an. Ihre Partner sind Fintechs, die die APIs unter anderem für elektronische Fakturierung inklusive Forderungsmanagement nutzen, damit einen digitalen, einfachen Kontowechsel durchführen oder Versicherungsverträge verwalten.

Darüber hinaus geht das Angebot von Subsembly, zu dem ein „Bank-Access-Server“ gehört [g]. Er ist in .NET geschrieben, läuft lokal beim Kunden auf dem Betriebssystem seiner Wahl und spricht mit Banken neben FinTS das im Geschäftsbereich verbreitete Protokoll EBICS (siehe unten). Dabei verlassen die Konto- und Transaktionsdaten nie das Unternehmen des Kunden, der den Server unter anderem in Kombination mit Buchhaltungs- und Finanzprogrammen für Kontoabgleich und Zahlungskontrolle nutzt. Daneben gibt es eine „XS2A-API“ (Access to Account), die FinTS nutzt und bei Bedarf auf Screen Scraping zurückgreift. Sie enthält die üblichen Zahlungsfunktionen und ist Kernstück der Banking4-Apps von Subsembly.

Noch einen Schritt weiter geht finAPI: Die Firma bietet neben einer Banking-API ein Data Warehouse [h]. Es aggregiert Daten aus verschiedenen Quellen und bereitet sie auf. So füllt die Software nach Möglichkeit leere Felder. Sie ist auch in der Lage, Transaktionen auf Wunsch zu kategorisieren. Anders als bei Subsembly liegen die Kundendaten in einer Cloud, und der Dienst fragt regelmäßig im Hintergrund Transaktionen ab – vorausgesetzt, der Kontoinhaber hat seine Zugangsdaten dauerhaft dort hinterlegt. Verpflichtend ist weder dies noch die Nutzung des Data Warehouse. Ein Anwendungsfall ist laut finAPI etwa die vereinfachte Kreditbearbeitung: Statt eine Schufa-Auskunft abzuwarten, könne ein Kunde der kreditgebenden Bank den (lesenden) Zugriff auf sein Girokonto gestatten. Auch die Plattform vermietet.de setzt auf die finAPI, um Mieteingänge automatisch zu kontrollieren und Zahlungsausgänge zu kategorisieren. Banken können ihrerseits die Schnittstelle von finAPI einbinden, um ihre Daten und Dienste Dritten zugänglich zu machen.

EU-weite Schnittstelle am Horizont

An einer Banking-API arbeitet neben Banken und Unternehmen auch die Berlin Group [i]. An dem Konsortium beteiligen sich (Stand Anfang 2018) nicht nur die deutschen, sondern auch polnische, rumänische, niederländische, litauische und irische Bankenverbände sowie europäische Geldinstitute wie die französische Société Générale und die italienische UniCredit sowie Visa und Mastercard. Die Gruppe will eine PSD2-konforme Schnittstelle spezifizieren, die das Abfragen von Transaktionen und das Auslösen von Überweisungen vereinheitlicht. Eine erste Version der „NextGen PSD2“ soll Anfang Februar 2018 erscheinen.

Im Gespräch äußerten sich Banken wie Firmen hoffnungsvoll, dass diese Schnittstelle ihre Arbeit erleichtern werde. Sie würde erstmals das Anbinden nicht deutscher Banken ermöglichen und damit das Geschäftsfeld von Fintechs deutlich erweitern. Etwas Ähnliches gibt es für Geschäftskonten bereits länger mit EBICS (Electronic Internet Communications Standard). Auf dieses Protokoll setzen bislang jedoch nur deutsche, französische und Schweizer Banken. Zu hoffen wäre, dass die PSD2-API der Berlin Group tatsächlich EU-weite Verbreitung findet. (js@ix.de)

Christian Kirsch

ist freier IT-Journalist und arbeitete mehrere Jahre lang als Redakteur bei *iX*.

Literatur

[1] Christian Kirsch; Onlinebanking; Meine API, deine API, keine API; EU-Regulierung zu Zahlungsdiensten; *iX* 10/2017, S. 102

Alle Links: ix.de/ix1803086