



Konzeption und Umsetzung von Open Banking-Plattformen





Ausgangslage

Veränderte Kundenbedürfnisse und verhaltene Reaktionen der etablierten Banken hierauf haben in den vergangenen Jahren zu einem starken Wachstum der FinTech-Branche geführt. In den großen Finanzzentren (z.B. London), aber auch abseits davon (z.B. in Berlin), haben sich große FinTech-Hubs entwickelt. Gleichzeitig haben sich Plattformbanken als Dienstleister für FinTechs positioniert, die den regulierten Teil der Dienstleistung abdecken (z.B. Wirecard Bank, Fidor Bank, solarisBank). In diesen Ökosystemen entstehen fokussierte Produkt- und Prozessinnovationen für den Finanzsektor in kurzer Zeit mit geringem Ressourceneinsatz (verglichen mit der Einführung neuer Produkte und Services bei etablierten Banken).

Inzwischen binden Banken zunehmend FinTech-Innovationen ein und bauen eigene Innovationslabore und „Digitalfabriken“ auf, um Innovationsprozesse zu beschleunigen und die eigene Wettbewerbsposition zu stärken. Die Entwicklung von Innovationen erfolgt dabei häufig in geschützten Sandboxes mit gelockerten IT-Anforderungen im Vergleich zur produktiven Core Banking IT der Banken.

Für FinTechs sowie die in den Sandboxes der Banken entstehende Innovationen gilt gleichermaßen die Herausforderung, dass diese mittelfristig an die etablierten, produktiven Core Banking-Systeme angebunden oder in diese integriert werden müssen, um beispielsweise Zugriff auf Kunden- und Kontodaten zu erhalten.

Folgende Ansätze hierzu haben sich etabliert:

- **Whitelabeling** in beide Richtungen (Bank bietet FinTech regulierte Banking-Services an/FinTech bietet Bank innovative Lösungen z.B. per Mobile App oder im Online-Banking an), nur einer der Akteure tritt aktiv gegenüber dem Kunden auf und aggregiert eigene Services sowie Services weiterer Parteien
- **Akquisition** eines FinTechs mit passender Innovation durch Bank bzw. Übernahme der Innovation aus der bank-eigenen Sandbox in die produktive Umgebung
- **Partnering/Kooperationen**, wobei beide Partner gegenüber dem Kunden auftreten (z.B. integrierter Produktabschlussprozess über Kreditvermittlungsplattform). FinTechs profitieren hierbei insbesondere vom Zugang zum regulatorischen Know-how der Bank sowie der großen Kundenbasis der Banken, die Banken von der höheren Innovationsgeschwindigkeit der FinTechs

Herausforderung

Alle genannten Ansätze stellen neue Anforderungen an die Core Banking-Architektur der Banken.

Zunächst ist eine weitere Öffnung der Bankarchitektur für die Anbindung/Integration von Services externer Dienstleister, die ggf. nicht den bisher etablierten

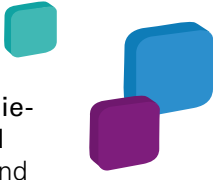
Standards entsprechen (im Gegensatz zu traditionellen Dienstleistern mit langjähriger Historie in der Branche), zu ermöglichen. Diese wird teilweise auch durch den Gesetzgeber (Stichwort: PSD2) forciert, um den Marktzugang für neue Wettbewerber zu erleichtern und Innovationskräfte zu fördern. Hier gelten mit der Umsetzung bis September 2019 harte Zieltermine.

Dies bedeutet insbesondere eine Veränderung des Fokus von internen, funktional-technisch orientierten Schnittstellen hin zu extern angebotenen Business Services, die flexibel kombiniert und ausgetauscht werden können. Dieser veränderte Fokus ist in der IT-Architektur abzubilden. Insbesondere bei öffentlichen Schnittstellen, die im Rahmen einer Open Banking-Strategie für externe Entwickler geöffnet werden, sind neue Formen der Governance, aber auch des Supports notwendig. Es sind z.B. Regelwerke für die Nutzung der Schnittstelle, Zustimmungspflichten des Kunden und Datenschutzkonformität zu entwickeln und technisch umzusetzen.

Zudem sind neue Konzepte für die Sicherheit dieser Schnittstellen zu erarbeiten, um klassische Angriffsvektoren wie Denial-of-Service-Angriffe, unberechtigte Datenzugriffe und Datenmanipulationen zu reduzieren. Ziel sollte eine möglichst starke Entkopplung der API-Schicht von der restlichen Architektur sein, um gleichzeitig die Sicherheit der Kernsysteme nicht zu kompromittieren sowie die Ausfallsicherheit zu erhöhen. Am Markt angebotene API-Management-Lösungen können für die technische Umsetzung dieser Herausforderungen eine Option sein. Aus strategischer Sicht ist im Hinblick auf Skill-Aufbau und Erhöhung der Agilität jedoch auch die interne Entwicklung eines API-Managements, insbesondere des entsprechenden Lifecycle- und Release-Managements und einer API-Plattform-Architektur zu überprüfen. Auch die steigende Systemlast in Kernbanksystemen durch erhöhte, schlechter steuerbare Zugriffszahlen über APIs ist zu berücksichtigen und muss in der Architektur- und Infrastrukturkonzeption, beispielsweise durch Umsetzung als skalierbare Microservices auf einer Cloud-Plattform, möglichst früh angegangen werden.

Neben der Öffnung der Architektur selbst haben sich auch die Anforderungen an die Geschwindigkeit der Integration und die Austauschbarkeit von externen Services in den vergangenen Jahren deutlich erhöht. Treiber ist wiederum die Notwendigkeit, neue Kundenbedürfnisse schnell erfüllen zu können und gleichzeitig eine zu große Abhängigkeit von einzelnen Dienstleistern zu vermeiden.

Die Vision geht soweit, dass beispielweise ein Kunde sich Zusatzleistungen, wie den passenden Analyseservice für das Depot per „Plug and Play“ aussuchen und aktivieren kann. Die Anforderung der Modularität und Konfigurierbarkeit reicht somit



bis in den Kundenkanal. Um diese Modularität zu erreichen und auch intern agil neue Anwendungen entwickeln, integrieren und ggf. extern als Whitelabel-Lösung anbieten zu können, sind auch interne Schnittstellen – soweit sinnvoll – von technischen Punkt-zu-Punkt-Verbindungen zwischen Anwendungen auf eine zentrale Integrationsarchitektur umzustellen.

Bei gesteigerter Offenheit, Modularität und Flexibilität der IT-Architektur ist weiterhin sicherzustellen, dass die Anforderungen an die Sicherheit und Stabilität der Lösungen den Anforderungen der Bank im Core Banking-Bereich entsprechen – dies gilt sowohl für interne Innovationen aus der digitalen Fabrik sowie für FinTech-Innovationen, die häufig in einem deutlich lockeren regulatorischen Umfeld entwickelt werden und häufig nicht den strengen Anforderungen der Bankenaufsicht an die IT, die insbesondere in den Mindestanforderungen an das Risikomanagement (MaRisk) sowie den zuletzt veröffentlichten Bankaufsichtsrechtlichen Anforderungen an die IT (BAIT) geregelt werden, entsprechen.

Der Ansatz vom KPMG

Wir helfen unseren Mandanten, ein zukunftsfähiges API-Management und einen API-Architektur-Layer als Basis für Open Banking aufzubauen und entsprechend der geltenden regulatorischen Anforderungen an die bestehende Core Banking-Architektur anzubinden. Hierbei bieten wir Hilfestellung von der fachlichen Konzeption bis zur Begleitung der Umsetzung und iterativen Weiterentwicklung mit agilen Ansätzen.

Unser Vorgehen gliedert sich in 5 eigenständige, aber aufeinander aufbauende Phasen und zwei parallele Umsetzungsstränge für die API-Management-Plattform sowie konkrete API Use Cases auf der Plattform, die wir parallel zur Plattform iterativ weiterentwickeln. Abhängig vom aktuellen Umsetzungsstand innerhalb der Organisation können wir somit den konkreten Ansatzpunkt für unser Vorgehensmodell definieren und dieses auf die individuellen Bedürfnisse anpassen.

Der Startpunkt in **Phase 1** ist hierbei die **Entwicklung einer Vision und Verankerung in der Organisation**. Hierbei ist das Ziel eine zukunftsfähige Strategie, die klare, messbare Ziele definiert, die mit Open Banking erreicht werden sollen (z.B. Vertrieb neuer, bepreisbarer Zusatzservices von Dritten an 10% der Retail-Kunden). Als erweiterte Basis sind die zu erstellenden fachlichen und technischen Konzepte des Open Banking-Ansatzes generell (z.B. Sicherheitskonzept, Konzept für den EU-DSGVO-konformen Umgang mit Daten im Open Banking-Kontext, Berücksichtigung der Anforderungen der MaRisk und BAIT) sowie für die API-Management-Plattform (als technischem „Enabler“ von Open Banking) zu sehen, die Ausgangspunkt für das anschließende Design bzw. die Auswahl der Plattform sind.

In **Phase 2** werden die **Lösungsoptionen basierend auf der Ist-Architektur identifiziert und in eine Ziel-Architektur überführt**. Hierbei sind Make-, Buy- oder Use-Entscheidungen zu treffen und geeignete Technologien auszuwählen. Unsere vielfach erprobte KPMG-Methodik für die Softwareauswahl stellt in Kombination mit unserer Kenntnis der relevanten Anbieter und Produkte im Bereich API-Management/API-Gateways und unserer Unabhängigkeit sicher, dass wir die beste mögliche Lösung für Sie identifizieren. Mit vielen Produkten (auch Open Source) haben wir dabei bereits konkrete Implementierungserfahrungen, die wir in den Auswahlprozess einbringen. Auf Basis dieser Lösungsauswahl konkretisieren wir gemeinsam mit Ihnen bei Bedarf den Entwicklungsprozess und die Architektur-Details der API-Management-Plattform. Dabei stellen wir sicher, dass diese konform zur übergreifenden Core Banking-Architektur sowie den spezifischen regulatorischen Anforderungen (z.B. PSD2) ist und unsere Better Practices, insbesondere im Hinblick auf Zukunftsfähigkeit, Flexibilität, Sicherheit, Verfügbarkeit und Compliance, berücksichtigt. Zu nennen sind hier u.a. weitgehende Entkopplung der Services, Load-Balancing, Clustering/Sharding der Services und, soweit möglich, Umsetzung als selbstheilende Services.

In der darauf folgenden **Umsetzung (Phase 3)** wird das API-Management in die Governance-Strukturen der Organisation integriert. Dies beinhaltet u.a. die Konzeption und Einführung von Reporting- und Monitoring-Prozessen für die API-Management-Schicht (z.B. Einbettung in das Reporting zu schwerwiegenden Sicherheitsvorfällen an die Aufsicht) sowie den Onboarding-Prozess für neue APIs und API-Konsumenten. Darüber hinaus werden Prozesse zur Überprüfung der Wirksamkeit der Sicherheitsmaßnahmen (bspw. Penetrationstests) definiert und etabliert. Nebenläufig erarbeiten wir gemeinsam mit Ihnen ein Betriebs- und Supportmodell und bereiten den Roll-out vor.

Die letzte Phase in der initialen Entwicklung der Plattform stellt der **Roll-out und Go-Live dar (Phase 4)**. Zentral hierbei sind neben dem technischen Roll-out der Kommunikationsplan und die Etablierung der definierten Prozesse rund um die Plattform. Nur so können die relevanten internen und externen Stakeholder und zukünftigen Nutzer der Plattform (wie z.B. externe Entwickler, interne Fachbereiche und FinTechs) aktiviert werden und die Plattform zu einem Erfolg werden.

Nach erfolgreichem Start (üblicherweise mit einzelnen produktiven APIs) erfolgt ein **kontinuierlicher Optimierungs- und Innovationsprozess (Phase 5)**, der Feature-Nachfragen, Performance-Probleme oder grundsätzliche Änderungen angeht. In diesem Prozess werden die vorangegangenen Phasen iterativ durchlaufen um API-Strategie, -Architektur und -Umsetzung kontinuierlich weiterzuentwickeln.

Vorgehensmodell Umsetzung Open Banking-Plattformen



	initial			On-going	
Plattform Delivery	“Long Term” Strategie <ul style="list-style-type: none"> Entwicklung der übergreifenden Open Banking-Plattform Entwicklung eines validen Business-Case für den Betrieb der Plattform Treffen grundlegender Entscheidungen (<i>“make-or-buy”</i>) 	Design & Ideate <ul style="list-style-type: none"> Identifikation relevanter Systeme und Datenquellen Definition notwendiger generischer Plattform-Funktionalitäten Gap-Analyse zum As-Is Definition von Architekturmustern für API-Integration Definition Ziel-Architektur der Plattform und neuer Architektur-Komponenten Sourcing ext. Komponenten Entwicklung eines externen fachl. Datenmodells 	Implementierung & Testing <ul style="list-style-type: none"> Generelle Anpassungen in der Integrationsschicht Integration neuer Komponenten der Architektur (z.B. API-Management Lösung) Definition Betriebsmodell mit Fachbereichen & IT Entwicklung Partnermodell Unterstützung bei der Entwicklung der Kommunikations- und Trainingspläne Entwicklung eines Release-Modells für kontinuierliche Integration neuer Use-Cases, Partner und Schnittstellen 	Pilotierung & Roll-Out <ul style="list-style-type: none"> Start Pilotierungsphase (bspw. <i>“Family & Friends”</i>-Modell für Angestellte, Hackathon mit Sandbox-Plattform, Start mit internen API Konsumenten) und Vorbereitung des Roll-Outs Roll-Out der Plattform 	Betrieb & Innovation <ul style="list-style-type: none"> Fokus: Überführung in robusten, optimierten Plattform-Betrieb Kontinuierliches Monitoring sicherheits- und performance-relevanter Parameter Laufende Optimierung der Plattform-Managements
	API Delivery	<ul style="list-style-type: none"> Evaluierung vorhandener Paradigmen für Implementierung der Open Banking-Plattform Identifikation Kernkompetenzen und Daten als Basis für Use Cases / APIs 	<ul style="list-style-type: none"> Definition initialer Use Cases und notw. APIs Erweiterung ext. Datenmodell Frühe Einbindung potenzieller Partner 	<ul style="list-style-type: none"> Etablierung agiler API-Delivery-Teams Technische Umsetzung APIs inkl. Anbindung weiterer interner Systeme & Datenquellen Iterative Entwicklung API-Policies & Standards 	<ul style="list-style-type: none"> Deployment erster APIs auf produktiver Plattform Start des Feedback-Prozesses mit API-Konsumenten (ext. Entwickler-Community)

Quelle: KPMG in Deutschland, 2018

Mehrwert für den Kunden

Durch den ganzheitlichen Ansatz von KPMG ist sichergestellt, dass wir den gesamten Lebenszyklus von der Ausarbeitung einer Strategie, über die Planung und Realisierung der Umsetzung bis zur Wartung und iterativen Weiterentwicklung der Plattform sowie einzelner APIs unterstützen können. Unser internationales Expertennetzwerk ermöglicht die Teilhabe an den aktuellsten technologischen Entwicklungen und garantiert, dass jederzeit der richtige Ansprechpartner für konkrete Fragestellungen zur Verfügung steht.

Zudem stellt KPMG sicher, dass alle Projektergebnisse aktuellen und absehbaren regulatorischen Anforderungen genügen und durch unsere Erfahrung aus diversen Projekten die aktuellsten Better Practices Verwendung finden. Wir machen Ihre Core Banking-Architektur fit für die digitale Zukunft und stellen die umfassende Berücksichtigung der PSD2-Anforderungen zum Access-to-Account sicher.

Kontakt

KPMG AG Wirtschaftsprüfungsgesellschaft
The SQUAIRE/Am Flughafen
60549 Frankfurt

Andreas Reuß

Partner, Financial Services
T +49 69 9587-4193
areuss@kpmg.com

Sebastian Schwittay

Manager, Financial Services
T +49 69 9587-4167
sschwittay@kpmg.com

www.kpmg.de

www.kpmg.de/socialmedia



Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation. Unsere Leistungen erbringen wir vorbehaltlich der berufsrechtlichen Prüfung der Zulässigkeit in jedem Einzelfall.

© 2018 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind eingetragene Markenzeichen von KPMG International.



Weitere Informationen zu den Herausforderungen der Digitalisierung für Core-Banking-Architekturen finden Sie auch in unserem Whitepaper „Core-Banking-Architektur zukunftssicher gestalten“