App-basierte Sicherheitsverfahren im Online-Banking

Dokumentversion: 1.1

Datum: 11.01.2017

Weitere Informationen: Dr. Hubertus von Poser

hubertus.von.poser@ppi.de

Vorwort

Smartphones bestimmen zu einem großen Teil, wie wir unser privates und geschäftliches Umfeld organisieren. Nicht nur die Art und Weise wie wir miteinander kommunizieren hat sich durch die Verbreitung dieser Geräte maßgeblich verändert, auch das Angebot an elektronischen Dienstleistungen ist in den vergangenen Jahren enorm gewachsen. Hohe Datentransferraten und nahezu flächendeckende Verfügbarkeit von Mobilfunkverbindungen ermöglichen eine ortsunabhängige Nutzung zu jeder Zeit. In 2016 nutzen rund 70 Mio. Menschen das Internet. Smartphones werden von fast 50 Mio. Menschen in Deutschland verwendet.

Elektronische Bankdienstleistungen, insbesondere Zahlungen, bilden hierbei einen Nutzungsschwerpunkt, bei dem ein Smartphone als zentrales Steuerungsinstrument und Authentifikationsmedium eingesetzt werden kann. Bei der Nutzung ist aus Sicht der Finanzwirtschaft stets zwischen Nutzerfreundlichkeit und Sicherheit abzuwägen.

Die PPI-Studie App-basierte Sicherheitsverfahren im Online-Banking beleuchtet diesen Aspekt im Detail und gibt einen Überblick über die in Deutschland verwendeten Sicherheitsverfahren.

Wir wünschen eine angenehme Lektüre.

PPI AG Informationstechnologie, Dezember 2016

Dokumentversion 1.1, 11.01.2017

Inhaltsverzeichnis

1 Zusammenfassung

Die rasante Entwicklung des Marktes der Smartphones und Applets dominiert immer mehr die Anwendungslandschaft und verdrängt zunehmend Desktop- und browserbasierte Anwendungen. Moderne Apps sind einfach zu bedienen, auf praktischen Nutzen ausgerichtet und bestimmen mehr und unser tägliches Leben. Dies hat auch große Auswirkungen auf Online-Banking- und Payment-Anwendungen, von denen gleichermaßen ein mehr an Usability und der Verzicht auf zusätzliche Hardware erwartet wird. Parallel dazu setzen Regulierungsmaßnahmen wie die Zahlungsdiensterichtlinie PSD2 neue Rahmenbedingungen für den Einsatz von Zahlungsverkehrsanwendungen.

In diesem Spannungsfeld haben nahezu alle Banken und Sparkassen in den letzten Monaten und Jahren App-basierte Authentifizierungs-Apps entwickelt und auf den Markt gebracht, um schnell und sicher Zahlungen auslösen und Überweisungen durchführen zu können. Vor dem Hintergrund noch nicht endgültig definierter Sicherheitsanforderungen – die Überführung der europäischen Zahlungsdiensterichtlinie PSD2 in nationales Recht ist erst für den Einsatz in 2018 geplant – wurden von den App-Herstellern unterschiedliche Philosophien gewählt, um die Symbiose aus Benutzerfreundlichkeit und Einhaltung der zu erwartenden Sicherheitsvorschriften optimal lösen zu können.

Diese Studie soll Ihnen dabei helfen, die Grundzüge und Gemeinsamkeiten von heute im Markt befindlicher App-basierten Authentifizierungslösungen zu verstehen und die Unterschiede der einzelnen Produkte einordnen zu können.

Dokumentversion 1.1, 11.01.2017

2 Motivation / Eigenschaften App-basierter Verfahren

Der Bereich der Smartphones und Tablets dominiert seit Jahren mit hohen Steigerungsraten den Markt und verdrängt Desktop- und browserbasierte Anwendungen im professionellen Bereich aber auch im Alltag immer mehr. Gerade bei alltäglichen Prozessen wie Bezahlvorgängen besitzen diese Geräte den entscheidenden Vorteil der Mobilität, weshalb auch neue Bezahlverfahren und Online-Banking-Anwendungen vermehrt durch die Bankkunden genutzt werden. Speziell in diesem Bereich kommt der Frage der sicheren Authentifizierung eine immer größere Bedeutung zu, da hier die Ausgewogenheit zwischen ausreichender Sicherheit und möglichst hoher Benutzerfreundlichkeit entscheidend ist.

2.1 Online-Banking-Sicherheitsverfahren

Gerade beim Faktor der Mobilität und Convenience aber hatte die Kreditwirtschaft lange Zeit keine Antwort parat. So wiesen die etablierten Online-Banking-Sicherheitsverfahren gravierende Nachteile im mobilen Bereich auf. Die im Rahmen der Deutschen Kreditwirtschaft genannten und bei den Banken und Sparkassen verbreitet eingesetzten Verfahren sind chipTAN und mobileTAN (vgl. [1]). Listen-basierte Verfahren wie iTAN sind zwar noch bei einigen Instituten im Portfolio, spielen jedoch prozentual aufgrund ihrer Schwächen im Sicherheitsbereich keine Rolle mehr für den mobilen Einsatz – wo sie zudem unter Usability-Gesichtspunkten keine Alternative darstellen.

Bleiben also nur chipTAN und mobileTAN als Alternativen. Beide Verfahren unterstützen eine Zwei-Faktor-Authentifizierung durch Verwendung der Online-Banking-PIN als „Wissen“ und der girocard bzw. der SIM-Karte im Smartphone als „Besitz“. Somit sind beide Verfahren konform zur starken Kundenauthentifizierung, wie sie in den aktuell diskutierten regulatorischen Vorgaben (siehe Kapitel 2.4) gefordert wird. Zudem werden beide Verfahren als „kontextbasiert“ bezeichnet, da die wichtigen auftragsbezogenen Daten in die TAN Berechnung mit einfließen. In den regulatorischen Vorgaben gilt hierfür der Begriff „dynamic linking“.

Hinweis: als „Online-Banking-Applikation“ werden in diesem Kontext sowohl fest am Desktop installierte Finanzmanagementprogramme wie z. B. StarMoney, VRNetWorld oder Wiso „Mein Geld“ als auch mobile Banking-Apps wie Sparkasse-App, VR-Banking-App oder Outbank verstanden. Hierzu gehören auch browserbasierte Banking-Portalanwendungen auf dem Desktop oder Smartphone / Tablet.

2.1.1 Das chipTAN- / Sm@rtTAN-Verfahren

Mit dem Begriff „chipTAN“ oder im Genossenschaftsbereich auch „Sm@rtTAN optic“ werden Verfahren bezeichnet, bei denen die auftragsbezogenen Daten wie z. B. Empfänger-IBAN und Betrag bei einer SEPA-Überweisung über eine optische Kopplung an ein chipTAN-Lesegerät mit optischen Sensoren übertragen werden, in dem eine girocard steckt.

Dazu wird von der Online-Banking-Applikation eine animierte Schwarzweißgraphik, in der die Informationen kodiert sind, am Bildschirm angezeigt. Der Benutzer hält nun sein chipTAN-Lesegerät mit der Leiste von fünf optischen Sensoren einige Sekunden lang vor die animierte Grafik, bis die Übertragung beendet ist und das erste Datenpärchen im Display des Lesers erscheint. Nach Bestätigung dieser Daten wird durch die TAN-Generator-Applikation auf der girocard eine auftragsbezogene TAN berechnet, die dann dem Kunden auf dem Display des chipTAN-Lesers angezeigt wird. Dieser kann die errechnete TAN nun in seiner Online-Banking-Applikation eintippen und sich damit für den gewünschten Auftrag authentifizieren.

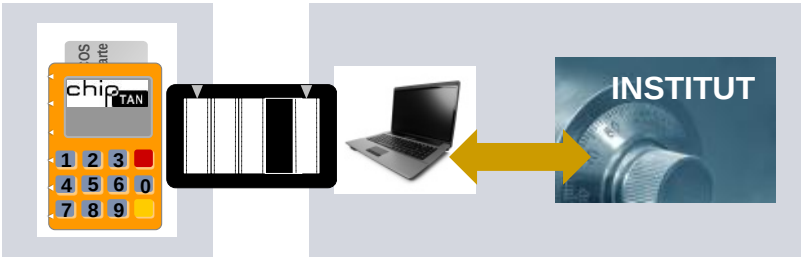

Abbildung 1: chipTAN-Verfahren

Das chipTAN-Verfahren wurde durch die Deutsche Kreditwirtschaft standardisiert, um einen Markt für solche chipTAN-Leser zu schaffen, die dann multibankfähig eingesetzt werden können. Aktuell sind Produkte der Hersteller Gemalto, Kobil, REINER SCT und Vasco am Markt vertreten. Mit einem dieser chipTAN-Leser können Online-Banking-Anwendungen bei allen Instituten, die chipTAN einsetzen, verwendet werden.

Obwohl chipTAN als eines der sichersten Verfahren für Online-Banking bezeichnet werden darf, ist es für den Einsatz im mobilen Bereich eher schlecht geeignet. Nicht nur die Anzahl der Komponenten – außer dem Smartphone selbst wird noch der chipTAN-Leser und die girocard benötigt – auch das Handling mit dem Positionieren des Lesers auf dem Smartphone-Display zum abscannen der animierten Grafik ist alles andere als handlich. Somit bildet das chipTAN-Verfahren nur eine Nische für diejenigen Kunden, die aufgrund der hohen Sicherheit des Verfahrens die Unzulänglichkeiten bei der Usability in Kauf nehmen.

2.1.2 Das mobileTAN- / smsTAN-Verfahren

Das mobileTAN- / mTAN- bzw. im Sparkassenbereich smsTAN-Verfahren nutzt eine physische Trennung der Übertragungskanäle. Parallel zur Online-Banking-Applikation z. B. auf dem Desktop, die mit dem Institut über Internet verbunden ist, wird auf dem Telefonkanal eine SMS übermittelt, die wieder die auftragsbezogenen Daten und hier auch die im Institut errechnete TAN enthält. Nach Erhalt der SMS muss der Kunde diese Daten prüfen und bei deren Korrektheit die TAN in seine Online-Banking-Applikation übernehmen und damit den Auftrag freigeben.

Abbildung 2: das mobileTAN-Verfahren

Obwohl die Handhabung beim mobileTAN-Verfahren vergleichsweise einfach ist, scheidet es aus einem anderen Grund für die mobile Nutzung aus: in den Sicherheitsbestimmungen der Deutschen Kreditwirtschaft wurde festgelegt, dass der Betrieb einer Banking-App zusammen mit der SMS auf einem Gerät nicht gestattet ist.

Dies ist auch nachvollziehbar, da die SMS-Applikation im Betriebssystem des Mobiltelefons komplett ungeschützt und durch Angreifer somit verhältnismäßig leicht zu manipulieren ist. Somit scheidet das mobileTAN-Verfahren für die mobile Nutzung generell aus.

2.1.3 Fazit zu den Online-Banking-Sicherheitsverfahren

Diese kurze Betrachtung zeigt, dass sich aus Sicht des mobilen Einsatzes für die Banken und Sparkassen ein Problem auftat, das man versuchte auf verschiedene Art zu lösen. Ein erster Weg führt über die Erhöhung der Mobilität beim chipTAN-Verfahren. Hier sind inzwischen erste Produkte am Markt, welche z. B. die Verbindung zwischen der Banking-App und dem chipTAN-Leser über Bluetooth herstellen, was die Usability stark erhöht, die Notwendigkeit der drei Komponenten Smartphone / chipTAN-Leser / Karte aber nicht beheben kann, da diese ja das hohe Sicherheitsniveau garantieren. Diese Lösungen haben somit für sicherheitsbewusste Kunden ihren Stellenwert, stehen hier aber nicht im Fokus der Betrachtung.

Das Zielszenario hat die klare Vorgabe, dass außer dem mobilen Device keine zusätzliche Hardwarekomponente benötigt wird, das so entstehende Konstrukt aber bei optimaler Mobilität und Convenience maximal sicher sein soll. Auch müssen natürlich die regulatorischen Vorgaben wie die starke Kundenauthentifizierung und dynamic linking erfüllt werden. Das Ergebnis sind die im Folgenden dargestellten App-basierten Verfahren, von denen jedes eine eigene Philosophie verfolgt und versucht, den benötigten Kompromiss zwischen Sicherheit, Regulatorik und Benutzerfreundlichkeit optimal zu erreichen.

2.2 Einsatzszenarien

Für eine strukturierte Betrachtung der verschiedenen App-Verfahren werden zunächst drei generelle Einsatzszenarien und ihre Eigenschaften beschrieben, auf die sich die einzelnen Lösungen im Abschnitt 3 immer zurückführen lassen.

Alle drei Szenarien haben gemeinsam, dass sie über einen speziellen Authentifizierungsserver mit einer Authentifizierungs-App kommunizieren. Wie diese Serverinstanz physisch in das jeweilige Online-Banking-System eingebunden wird, ist an dieser Stelle unerheblich, da nur der „logische Kanal“ zum mobilen Device für die vorliegende Betrachtung relevant ist. Die sogenannte „logische Kanaltrennung“ ist ein Hilfskonstrukt, das ausdrücken soll, dass die beiden beteiligten Apps auf irgendeine Weise voneinander isoliert betrieben werden. Dies kann wie bei getrennten Geräten in Szenario 1 eine physische Kanaltrennung ähnlich mobileTAN sein. Beim Betrieb auf einem einzigen Device müssen jedoch spezielle Vorkehrungen in der Software geschaffen werden, um eine vergleichbare Isolierung der beiden Apps zu erhalten.

2.2.1 Szenario 1 – Betrieb auf getrennten Geräten über zwei physische Kanäle

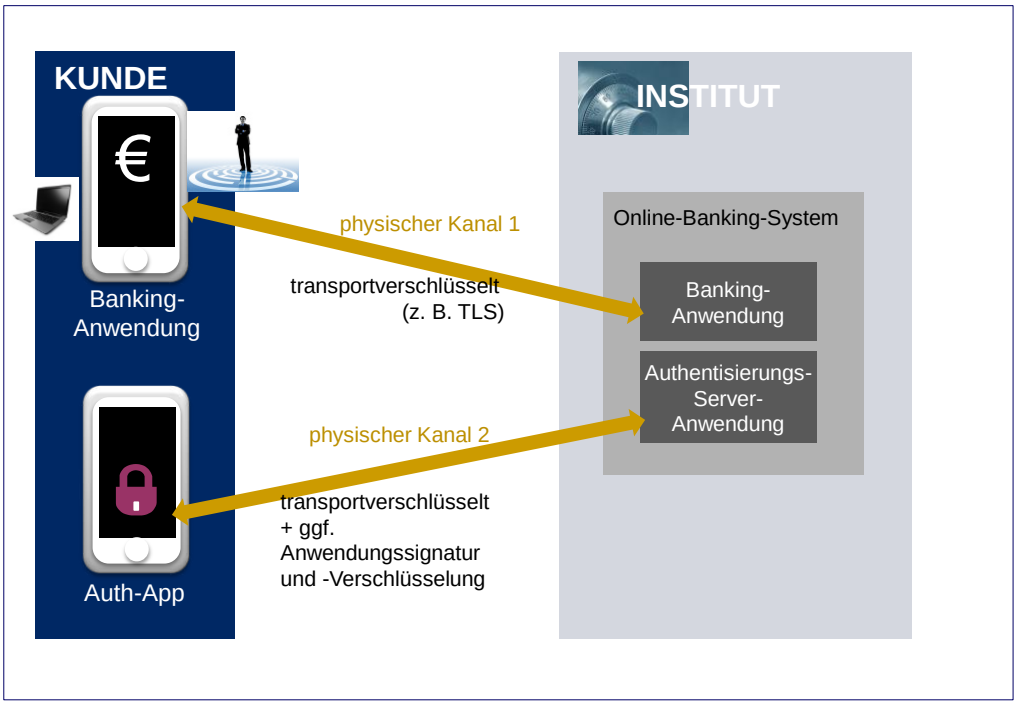

Abbildung 3: Szenario 1 - Zwei getrennte Geräte mit zwei physischen Kanälen

Verfahren, die eine Authentisierungs-App in einem eigenen mobilen Gerät wie einen Sicherheitstoken nutzen, ohne dass die zugehörige Banking-Applikation auf dem gleichen Endgerät betrieben werden kann, werden als Szenario 1 zusammengefasst.

Die Banking-Anwendung kann hierbei z. B. eine Desktop-Anwendung, eine mobile App oder ein browserbasiertes Portal sein. Zur Freigabe eines Auftrags wird der Kunde aufgefordert, die Authentisierungs-App auf dem dafür registrierten Device zu starten; dort werden die auftragsbezogenen Daten angezeigt und nach der Bestätigung durch den Kunden wird eine TAN oder Signatur erzeugt. Diese wird bei einigen Varianten gleich über den Authentisierungskanal automatisch zum Institut übertragen und mit dem offenen Auftrag synchronisiert, so dass für einen Benutzer z. B. die Eingabe einer TAN entfällt.

Szenario 1 kann somit die Usability gegenüber chipTAN / mobileTAN erhöhen, wobei das Sicherheitsniveau von der Robustheit der Authentifizierungs-App abhängt. Als Alternative für mobiles Banking im engeren Sinn kann es jedoch nicht gewertet werden, da in jedem Fall zwei Geräte benötigt werden.

2.2.2 Szenario 2 – Betrieb auf einem Gerät mit zwei logisch getrennten Apps

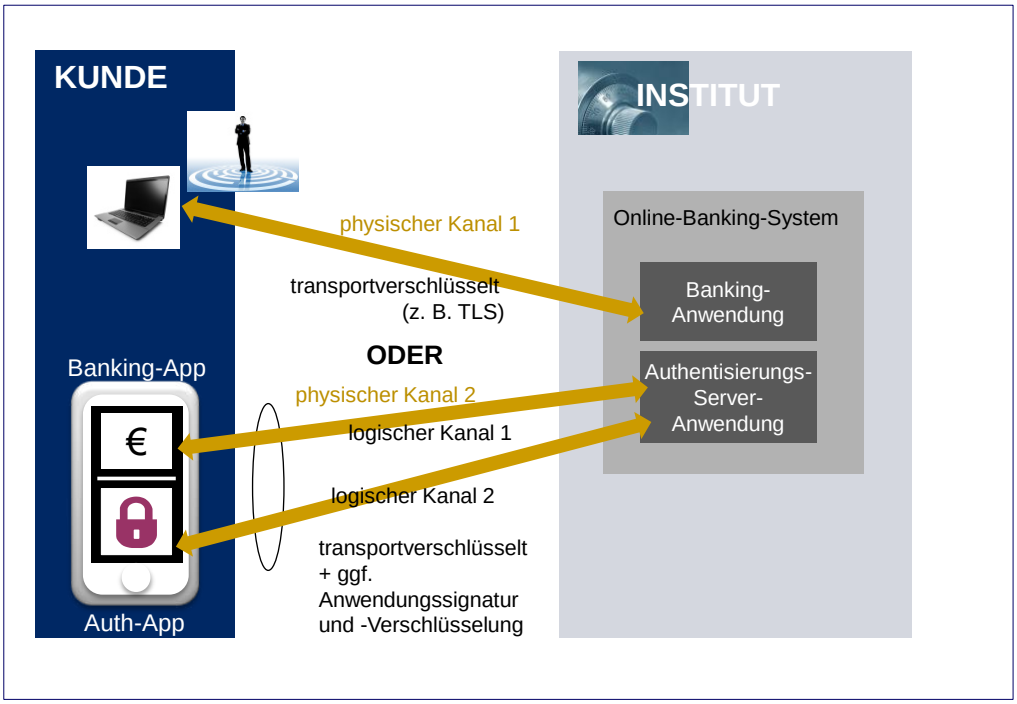

Abbildung 4: Szenario 2 - Ein Gerät und zwei logisch getrennte Kanäle

Szenario 2 ist die aktuell gängigste Art für die Umsetzung von App-basierten Verfahren. Es setzt auf der Wirkungsweise von Szenario 1 auf, ergänzt dieses jedoch um die Option, dass nun Banking-App und Authentifizierungs-App auf demselben Endgerät betrieben werden können. Dadurch wird grundsätzlich die Forderung erreicht, dass für die Abwicklung von mobilen Online-Banking-Transaktionen kein zusätzliches Device benötigt wird.

Da der Betrieb beider Apps in einer Ablaufumgebung zusätzliche Angriffsrisiken birgt, müssen zusätzliche Vorkehrungen getroffen werden, um diese zu minimieren. Diese Anforderungen werden aktuell durch neue europäische regulatorische Maßnahmen artikuliert, wie sie in Abschnitt 2.4 genauer beschrieben werden.

Generell wird den Risiken eines solchen Betriebs durch folgende Maßnahmen begegnet und oft auch als logische Kanaltrennung bezeichnet:

1. Schutz der verwendeten kryptografischen Schlüssel
2. Schaffen eines HW-Bezugs (auch als „Device Identity“ bezeichnet), um die Kopierbarkeit der Schlüssel auf andere Endgeräte zu unterbinden
3. Isolieren der Banking- und Authentifizierungs-App, um gegenseitige Zugriffe zu vermeiden
4. Erkennen von Manipulationen an Betriebssystem oder Apps

Die Liste dieser Maßnahmen ist kurz, jedoch sind diese nur schwer umsetzbar, da es sich bei diesem Szenario um ein reines Softwaresystem ohne zusätzliche Hardware handelt. Während die Verwendung von Signaturen und Verschlüsselung zwischen Authentifizierungs-App und –Server leicht zu bewerkstelligen ist, sind die restlichen Punkte beliebig komplex und stark abhängig von den Betriebssystemen (z. B. Android oder iOS) und den Sicherheitsstrategien der jeweiligen Hersteller. Auch die Erkennung von Betriebssystems-Manipulationen wie Rootings oder Jailbreaks ist stark der Dynamik des Marktes der Mobilgeräte unterworfen, was eine ständige Beobachtung und Justierung der Authentifizierungs-Apps erfordert. Trotz aller Anstrengungen bleiben App-basierte Lösungen nicht unangreifbar, wobei es sich bei bisher bekannt gewordenen und in den Medien gezeigten Angriffen nur um die Kompromittierung einzelner Geräte unter Laborbedingungen handelte.

Andererseits geht es aber bei der Bewertung der Sicherheit auch nicht um die Möglichkeit eines erfolgreichen Angriffs generell, sondern nur um den benötigten Aufwand, ein solches Verfahren zu knacken. Dies ist ein gängiges Vorgehen, da es absolute Sicherheit ohnehin nicht geben kann und die Zuverlässigkeit somit immer von dem Verhältnis der einzusetzenden kriminellen Energie zur Kompromittierung des Gesamtsystems abhängt.

Zudem ist für eine Beurteilung der Sicherheit eines solchen App-basierten Sicherheitssystems immer die Begutachtung einer speziellen Implementierung eines Verfahrens notwendig, da Aussagen zu den abstrakten Prozessen nicht ausreichen.

2.2.3 Szenario 3 – Betrieb auf einem Gerät in einer App

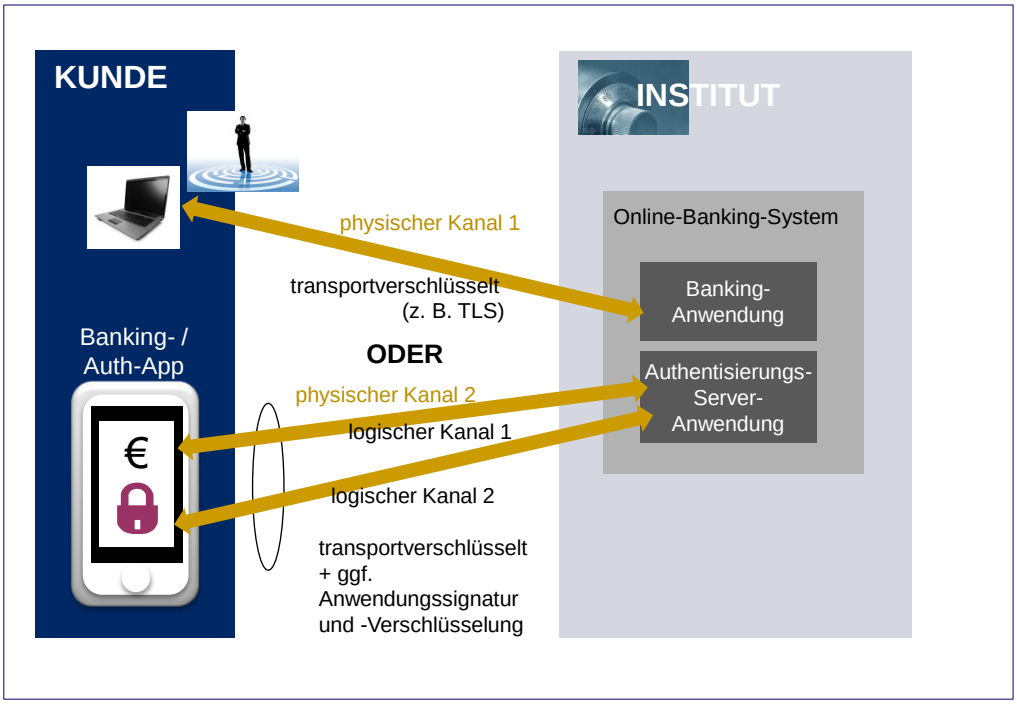

Abbildung 5: Szenario 3 - Logische Kanaltrennung und eine App

Szenario 3 perfektioniert Szenario 2 nochmals aus Sicht der Usability, da ein Benutzer nun auch keine zwei unterschiedlichen Apps mehr zu bedienen braucht, sondern die Erfassung und Authentifizierung von Aufträgen in einer Umgebung erfolgen kann.

Während dies für eine reine App-Umgebung aus Benutzersicht optimal ist, gestaltet sich die Verwendung dieser zentralen App z. B. zur Authentifizierung von Aufträgen in einer parallelen Desktop-Anwendung als schwieriger, da die Authentifizierung nun als Einzelpunkt in der Gesamtanwendung versteckt und daher oft schlecht zu finden ist.

Daher findet dieses Szenario vornehmlich in rein mobilen Szenarien ohne solche Anwendungswechsel Verwendung.

Aus Sicherheitssicht ist eine Entkopplung der fachlichen Anwendung und Authentifizierung nun nicht mehr gegeben, weshalb nur noch die restlichen Kriterien für eine Härtung der Anwendung herangezogen werden können. Somit ist die Bewertung der Sicherheit eines solchen Systems noch kritischer als unter Szenario 1 oder 2.

2.3 Registrierung

Da Authentifizierungs-Apps den Benutzer bzw. sein Smartphone / Tablet gegenüber dem Institut als „Besitz“ authentifizieren sollen, muss zunächst ein sicherer Ausgangszustand geschaffen werden. Hierzu gibt es bei allen Verfahren einen Registrierungs- bzw. Freischaltprozess, der einmal durchlaufen werden muss, um die Authentifizierungs-App dann im Online-Banking nutzen zu können. Dieser Prozess läuft im Allgemeinen folgendermaßen ab:

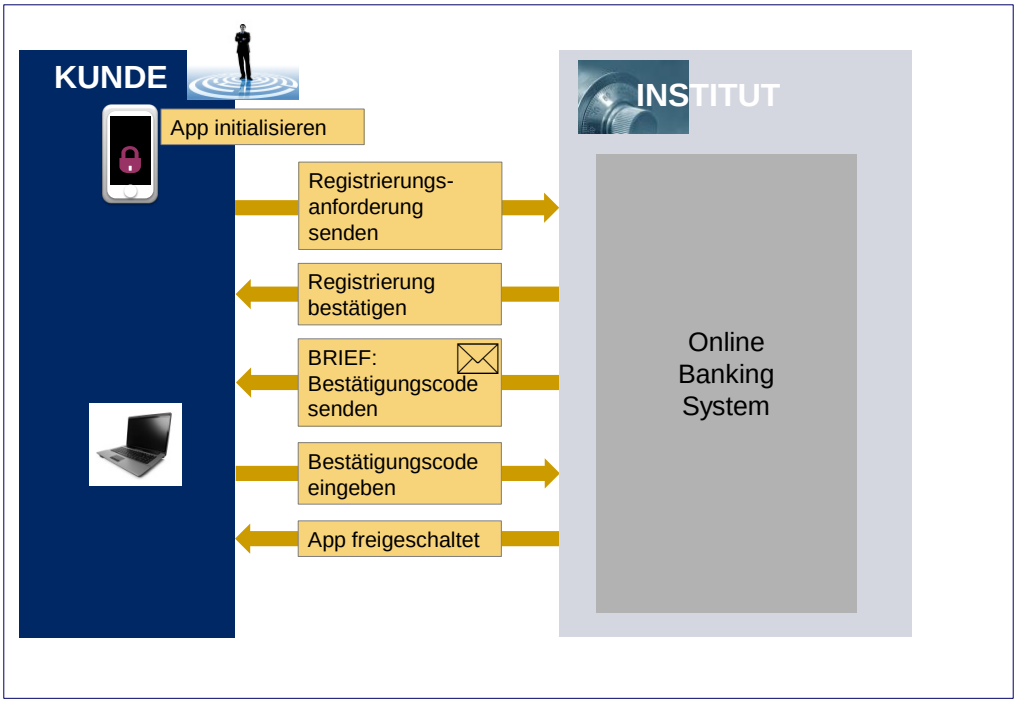

Abbildung 6: Registrierung / Freischaltung der Authentifizierungs-App

Zunächst wird die Authentifizierungs-App aus dem jeweiligen App-Store geladen und auf dem Gerät installiert. Beim ersten Aufruf wird gängigerweise ein Passwort vergeben, das auch in die Generierung der für den späteren Betrieb benötigten kryptografischen Schlüssel mit einfließt.

Je nach konkretem Verfahren wird in der Authentifizierungs-App oder im Internet-Banking-Portal die Registrierung angestoßen. Im Institut wird die Registrierung vorgemerkt und bestätigt. Parallel dazu wird ein Bestätigungscode meist auf postalischem Weg an den Benutzer gesendet.

Nach Erhalt des Briefes gibt der Benutzer den dort angedruckten Bestätigungscode meist im Internet-Banking-Portal des Instituts ein. Nach dessen erfolgreicher Prüfung wird die Authentifizierungs-App freigeschaltet und kann genutzt werden.

Die Registrierungs- / Freischaltverfahren der einzelnen Verfahren weichen teilweise von dem gezeigten Ablauf ab. Auf diese Abweichungen wird bei der Beschreibung der einzelnen Verfahren eingegangen.

2.4 Sperren von Authentifizierungs-Apps

Bei Gefahr des Missbrauchs bieten alle Institute Möglichkeiten an, den Online-Banking-Zugang z. B. über die zentrale Sperrhotline 116 116 zu sperren. Sperrmöglichkeiten für die Authentifizierungs-Apps existieren teilweise über die Internet-Banking-Portale.

Bei Authentifizierungs-Apps, die mit einem Zugangspasswort versehen sind, führt die Eingabe von Fehleingaben zum Sperren der App und teilweise auch zum Löschen der kryptografischen Schlüssel. Die Anzahl der Fehlversuche ist anwendungsabhängig und die Reaktionen im Fall des Sperrens meist nicht offengelegt.

2.5 Regulatorische Rahmenbedingungen

Aufgrund der zunehmenden Bedeutung befassen sich auch die Gesetzgeber und Aufsichtsbehörden seit Jahren mit der Sicherheit im Internet-gestützten Zahlungsverkehr. Aktuell relevant sind hierbei die durch die Bundesanstalt für Finanzdienstleitungen (BaFin) herausgegebenen „Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)“. Diese sind seit dem 5. November 2015 in Kraft und bilden die Basis für Prüfungen durch die Bankenaufsicht.

Parallel hierzu fand auch eine Überarbeitung der Zahlungsdiensterichtlinie „Payment Service Directive (PSD 2)“ statt. Diese trat im Januar 2016 in Kraft und befindet sich nun bis 2018 in der Umsetzung in nationales Recht.

Beide regulatorischen Vorgaben verwenden den Begriff der „Starken Kundenauthentifizierung“. Aufgrund der komplexen Zusammenhänge und der bedeutenden Auswirkungen sowohl auf die Sicherheit als auch auf die Einsatzszenarien befindet sich die konkrete Ausgestaltung dieser starken Kundenauthentifizierung im Rahmen der PSD 2 derzeit noch in der Konkretisierungsphase durch die European Banking Authority (EBA).

Für eine Beurteilung der App-basierten Sicherheitsverfahren ist daher momentan die Ausführung des MaSI-Rundschreibens relevant, die sich aber mit den Aussagen in der aktuellen Kommentierungsversion des „Regulatory Technical Standard (RTS)“ der EBA deckt:

„Starke Kundenauthentifizierung ist im Sinne dieses Rundschreibens ein Verfahren, das auf der Verwendung zweier oder mehrerer der folgenden Elemente basiert, die als Wissen, Besitz und Inhärenz kategorisiert werden:

i) etwas, das nur der Nutzer weiß, z. B. ein statisches Passwort, ein Code, eine persönliche Identifikationsnummer,

ii) etwas, das nur der Nutzer besitzt, z. B. ein Token, eine Smartcard, ein Mobiltelefon,

iii) eine Eigenschaft des Nutzers, z. B. ein biometrisches Charakteristikum, etwa ein Fingerabdruck.

Außerdem müssen die gewählten Elemente unabhängig voneinander sein, d. h. die Verletzung eines Elements darf keinen Einfluss auf das andere bzw. die anderen haben. Mindestens eines der Elemente sollte nicht wiederverwendbar und nicht reproduzierbar (die Inhärenz ausgenommen) sein und nicht heimlich über das Internet entwendet werden können.

Das starke Authentifizierungsverfahren sollte so gestaltet sein, dass die Vertraulichkeit der Authentifizierungsdaten gewahrt bleibt.“

Quelle: Rundschreiben 4/2015 der BaFin vom 5.5.2015 [2]

Für die praktische Umsetzung speziell der starken Kundenauthentifizierung auf Basis von Besitz, Wissen und Inhärenz hat die Bankenaufsicht in einem FAQ-Dokument mit letztem Stand vom 24.06.2016 die Rahmenbedingungen für die Umsetzung der MaSI-Anforderungen nochmals konkretisiert und dabei unter Punkt 4b „Wie sind App-basierte Sicherungsverfahren in Bezug auf starke Kundenauthentifizierung zu sehen?“ Aussagen zum Einsatz von App-basierten Verfahren gemacht. Im Vordergrund stehen hierbei Einsatzszenarien mit dem Betrieb von Banking-App und Authentifizierungs-App auf einem Gerät, wie sie in den Abschnitten 2.2.2 und 2.2.3 beschrieben sind. Diese Einsatzszenarien werden durch die MaSI ausdrücklich nicht untersagt, sondern dem Risikomanagement des Instituts unterstellt.

Speziell für den Betrieb auf einem Gerät werden durch die BaFin beispielhaft Maßnahmen genannt, um das Risiko zu minimieren. Diese entsprechen i. W. den in Abschnitt 2.2 gemachten Aussagen zu den Anforderungen an die Härtung von Sicherheitssystemen auf Basis von Authentifizierungs-Apps.

1. Sandboxing/Nutzung von vertrauenswürdiger Anwendungsumgebung
2. Ausgiebige Prüfung von Software auf Manipulationsmöglichkeiten
3. Verwendung von Device-Identity-Lösungen
4. Ausschluss der Nutzung von Geräten, die „jail-broken“ sind
5. Aufklärung des Kunden über die etwaigen Risiken

Quelle: MaSI FAQ der BaFin vom 24.6.2016 [3]

Zum besseren Verständnis hier eine Erläuterung dieser beispielhaften Anforderungen:

1. Sandboxing / Nutzung von vertrauenswürdiger Anwendungsumgebung

Unter „Sandboxing“ ist zum einen die generelle Kapselung einer App in einer Betriebssystemumgebung zu verstehen. Im Speziellen ist hier aber auch die Entkopplung von der Banking-App gemeint. Betriebssysteme bieten hierfür Vorkehrungen an, aber auch Möglichkeiten, auf sicherem Wege zwischen zwei bekannten Apps zu kommunizieren, um z. B. eine TAN zu übergeben.

Unter vertrauenswürdiger Anwendungsumgebung sind aber auch Vorkehrungen zum Signieren und Verschlüsseln der Daten zwischen dem Authentifizierungsserver im Institut und der Authentifizierungs-App auf dem Endgerät des Kunden zu verstehen.

Der wichtigste Punkt jedoch – gerade, wenn von Signatur und Verschlüsselung die Rede ist – ist die sichere Ablage des Schlüsselmaterials, damit gerade diese gesicherten Strecken nicht aufgebrochen und manipuliert werden können.

2. Ausgiebige Prüfung von Software auf Manipulationsmöglichkeiten

An dieser Stelle kann keine ausführliche Darstellung erfolgen, auf welche Weise die Ablaufumgebung unter Android und iOS geprüft werden kann. Es gibt zahlreiche Möglichkeiten, sowohl die eigenen Apps auf Manipulationen zu prüfen als auch Betriebssystemfunktionen zu überwachen. All diese Vorkehrungen befinden sich unter der Kontrolle der Hersteller Google und Apple und sind ständigem Wandel unterworfen. Auch können diese teilweise z. B. durch Softwarelücken in den Betriebssystemen mit entsprechendem Aufwand von Angreifern umgangen werden. Daher müssen diese betriebssystemnahen Funktionen in den Apps permanent überwacht und auf den neuesten Stand gebracht werden, um den gewünschten Schutzeffekt zu erzielen.

3. Verwendung von Device-Identity-Lösungen

Eine gefährliche Angriffsmöglichkeit stellt das Kopieren von Programmen und Daten und die Ausführung in einer anderen Umgebung dar. Davon sind nicht nur Backup-Konzepte betroffen, bei denen z. B. keine kryptografischen Schlüssel mit kopiert werden dürfen, sondern auch mutwillige Kopiervorgänge durch Angreifer. Umgangen werden kann dies durch eine Bindung der Authentifizierungssoftware an das jeweilige Endgerät durch Einbinden von verfügbaren HW-Informationen wie MAC- oder IP-Adresse, Geräteseriennummern usw. Leider sind nur die wenigsten dieser HW-Informationen inzwischen durch die Betriebssysteme noch abgreifbar, wodurch eine HW-Bindung erschwert, aber nicht komplett verhindert wird.

4. Ausschluss der Nutzung von Geräten, die „jail-broken“ sind

Grundsätzlich funktionieren die unter 1 bis 3 aufgezeigten Maßnahmen nur, wenn das Betriebssystem nicht durch Rooting (Android) oder Jailbreaks (iOS) modifiziert wurde. Diese Manipulationen am eigentlichen Betriebssystem sind oft auch genutzte Tools, um den Funktionsumfang des Smartphones/Tablets zu erweitern. Andererseits sind diese Eingriffe nicht kontrollierbar und für eine sichere Ausführungsumgebung, wie sie für Online-Banking benötigt wird, nicht akzeptabel. Daher gilt im Allgemeinen, dass das Gerät beim Start der Authentifizierungs-App auf Hinweise von Rootings oder Jailbreaks hin untersucht wird. Wird ein solcher Hinweis gefunden, beendet sich die App gängigerweise mit einem Hinweis und verweigert ihren Dienst.

Auch hier gilt wieder die Maßgabe, dass das Erkennen von solchen Manipulationen höchst dynamisch und von der Version des Betriebssystems abhängig ist, so dass auch hier ein ständiges Beobachten und Nachjustieren erforderlich ist. Dies wird speziell im Android-Bereich noch erschwert durch Produkte, die Jailbreak-Technologien nutzen, um offizielle Funktionserweiterungen in ihre Geräte zu integrieren. Solche Produkte werden dann ggf. als gejailbreakt erkannt und von der Erkennungsroutine abgelehnt, was natürlich zu Unmut bei den entsprechenden Kunden führt. Somit ist also bei diesem Thema viel Fingerspitzengefühl gefragt.

5. Aufklärung des Kunden über die etwaigen Risiken.

Eine geeignete Kommunikation mit den Kunden ist die Basis für einen verantwortungsvollen Umgang mit App-basierten Verfahren. Sie müssen über die gezeigten Risiken informiert werden, ohne sie dadurch aber von der Nutzung abzuschrecken. Je mehr ein Institut in die Härtung der eigenen App-Lösung investiert, desto selbstbewusster kann auch die Kommunikation sein. Letztlich steht dahinter auch die Botschaft, wie das Institut im Falle eines monetären Schadens mit der Kundschaft verfährt. Einige Institute bieten hier Kontomodelle mit Versicherungen an, um das verbleibende Restrisiko abzudecken.

2.6 Konsequenzen für die Umsetzung

Wie in den Abschnitten 2.2 und 2.4 aufgezeigt, erfordert die Absicherung und Härtung App-basierter Verfahren einen großen Aufwand für die jeweiligen Implementierungen und eine laufende Beobachtung der Sicherheitslage. Es muss im Gefahrenfall schnell reagiert werden können, um Programmupdates bereit zu stellen, die aber dann auch von den Nutzern zeitnah aktiviert werden müssen. Dies stellt hohe technische, finanzielle und organisatorische Anforderungen an den Betrieb einer App-basierten Lösung.

Bei all den aufgezeigten Risiken darf man jedoch nicht vergessen, dass die gezeigten Angriffe nur mit großem Aufwand umzusetzen sind und sich nach heutigem Wissensstand nur gegen ein spezielles Endgerät richten, ein Flächenangriff gegen ein App-Verfahren selbst also bisher nicht zur Diskussion steht.

Dem gegenüber stehen die großen Vorteile des optimalen Zuschnitts eines solchen Verfahrens auf den mobilen Markt, was App-basierte Lösungen momentan konkurrenzlos dastehen lässt. Somit sollen die im nächsten Kapitel gezeigten Marktlösungen eher das Anwendungsspektrum als die Sicherheitsthematik beleuchten, da zudem die Sicherheitskonzepte der Lösungen ohnehin nicht offengelegt sind.

3 App-basierte Verfahren am Markt

Nach diesen Vorbemerkungen nun zu den konkret angebotenen App-basierten Verfahren am Markt. In den nächsten Abschnitten werden folgende Bankprodukte vergleichend dargestellt:

Produkt	Anbietende Institute
appTAN	Hypovereinsbank Unicredito
BestSign mobil	Postbank
BV-appTAN	Bank-Verlag
Photo-TAN	Deutsche Bank, Commerzbank
pushTAN	Sparkassen-Finanzgruppe
QR-TAN	1822direkt
SmartSecure	ING DiBa
VR-SecureGo	Volks- und Raiffeisenbanken Süd
VR-SecureSIGN	Volks- und Raiffeisenbanken Nord

Kriterien

Alle dargestellten Verfahren erfüllen nach Aussagen der jeweiligen Banken die Anforderungen nach starker Kundenauthentifizierung (sie bilden also den Faktor „Besitz“ im Rahmen der Zwei-Faktor-Authentifizierung ab, wobei als Faktor „Wissen“ die Online-Banking-PIN verwendet wird) und dynamic linking. Auch die in Kapitel 2.4 dargestellten fünf Anforderungen an die Umsetzung werden als erfüllt vorausgesetzt, obwohl bei den wenigsten Lösungen konkrete Beschreibungen für die Umsetzungen vorliegen, was aber auch nachvollziehbar ist. Daher werden für die folgende Gegenüberstellung der App-basierten Verfahren eher Kriterien zugrunde gelegt, die Unterschiede im Benutzerverhalten und in der Funktionalität beschreiben.

Kriterium	Bedeutung
Positionierung	Es werden Aussagen getroffen, ob mit der Einführung des App-basierten Verfahrens andere Sicherheitsverfahren abgelöst werden, oder ob es sich um ein zusätzliches Verfahren handelt.
Registrierung	Es wird beschrieben, ob das App-basierte Verfahren über einen per Post übermittelten Registrierungsbrief freigeschaltet wird, oder ob die Freischaltung online erfolgt.

Kriterium	Bedeutung
App-Passwort	Beschreibung, ob beim Start der Authentifizierungs-App eine Passworteingabe erfolgen muss.
TAN-/Signatur-Übertragung	Es wird dargelegt, ob der Benutzer die TAN manuell eingeben muss bzw. in welchen Fällen sie automatisch übertragen wird.
Beantragung	Beschreibung des Beantragungs- und Freischaltungsprozesses für Bestandskunden
Mehrere Geräte oder Bankverbindungen	Aussagen zu folgenden Fragen: ■ Können einem Benutzer mehrere Geräte zugeordnet werden? ■ Wie findet ein Gerätewechsel statt (z. B. bei einem neuen SmartPhone)? ■ Können mit einem Gerät mehrere Benutzer / Bankverbindungen verwaltet werden?
Einsatz von zusätzlicher Hardware	Hinweis, ob das Verfahren alternativ auch mit einer Hardware-Komponente betrieben werden kann.

3.1 appTAN (Hypovereinsbank Unicredito)

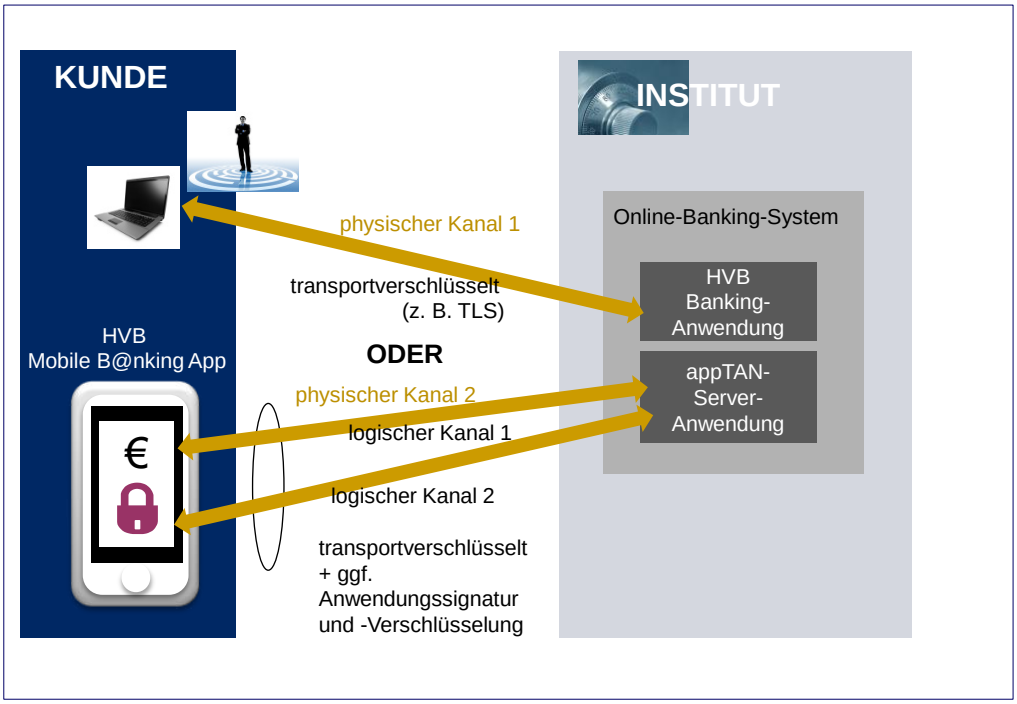

Abbildung 7: appTAN (Hypovereinsbank Unicredito)

Verfahrenssteckbrief

Kriterium	Eigenschaften appTAN
Institute	Hypovereinsbank Unicredito
Geräte	Smartphones und Tablets
Betriebssysteme	Android, iOS
Hersteller	keine Angabe
Szenario	Szenario 3 – in HVB Mobile B@nking integriert
Positionierung	löst iTAN und mobileTAN ab
Registrierung	per Registrierungsbrief (postalisch oder Filiale)
App-Passwort	nein
TAN-Übertragung	Ja, zu HVB Direct B@nking und Mobile B@nking
Kosten für den Kunden	kostenlos

Unterstützte Vertriebskanäle

- Internet-Banking-Portal: ja, HVB Direct B@nking
- Mobile Banking: ja, HVB Mobile B@nking App, limitiert auf 1.000 EUR
- Apps vom Markt: nein
- FinTS-Kundenprodukte: nein, nur HBCI oder iTAN

Beantragung

Bestandskunden können die appTAN über das bestehende iTAN- oder mobileTAN-Verfahren im HVB Direct B@nking oder Mobile B@nking beantragen und durch Eingabe einer TAN mit dem bestehenden Verfahren absichern.

Der Registrierungsbrief enthält einen 6-stelligen Freischaltcode, der im HVB Direct B@nking eingegeben werden muss.

Mehrere Geräte oder Bankverbindungen

Es kann nur ein Gerät als Besitzfaktor registriert werden, wobei der Zugriff nicht durch ein Passwort geschützt ist. Bei einem Wechsel muss das bestehende Smartphone / Tablet deaktiviert und das neue Gerät neu registriert werden.

Es sind Verbindungen zu maximal 10 HVB Direct-B@nking-Nummern möglich.

Einsatz von zusätzlicher Hardware

Nein

3.2 BestSign mobil (Postbank)

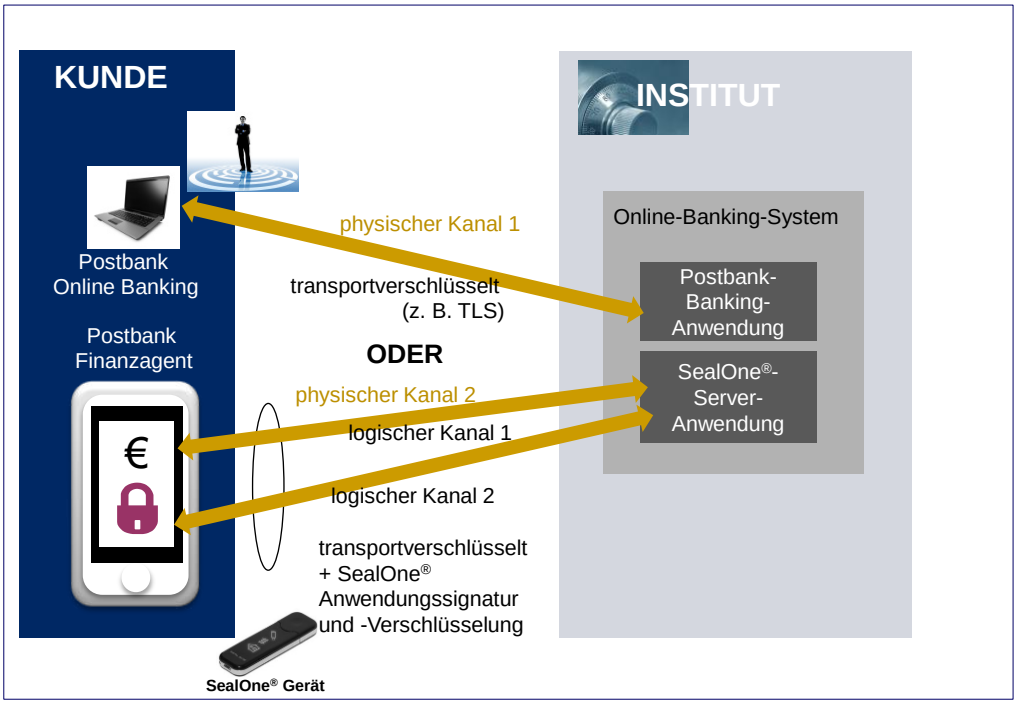

Abbildung 8: BestSign mobil (Postbank)

Verfahrenssteckbrief

Kriterium	Eigenschaften BestSign mobil
Institute	Postbank
Geräte	Smartphones und Tablets
Betriebssysteme	Android, iOS, Windows Phone
Hersteller	SealOne®
Szenario	Szenario 3 – Betrieb in einer gemeinsamen App
Positionierung	zusätzliches Sicherheitsverfahren
Registrierung	per Registrierungsbrief (postalisch)
App-Passwort	BestSign-Passwort, min. 4 Stellen oder TouchID
Signatur-Übertragung	Ja, zum Postbank Online-Banking und Finanzassistent
Kosten für den Kunden	kostenlos

Unterstützte Vertriebskanäle

- Internet-Banking-Portal: ja, Postbank Online-Banking
- Mobile Banking: ja, Postbank Finanzassistent
- Apps vom Markt: FinTS Banking-Apps
- FinTS-Kundenprodukte: Ja

Beantragung

Bestandskunden können BestSign mobil nach der Initialisierung des Postbank Finanzagenten auf dem Smartphone / Tablet über das Postbank Online-Banking beantragen. Dabei wird eine von der App generierte SealOne-ID im Online-Banking eingetragen. Anschließend wird ein Registrierungsbrief mit einem Aktivierungscode und der SealOne-ID per Post versendet.

Der im Brief enthaltene Aktivierungscode muss dann im Online-Banking eingegeben werden. Damit ist diese App auf diesem Gerät aktiviert.

Mehrere Geräte oder Bankverbindungen

Es können mehrere Geräte aktiviert werden, die nach Eingabe des jeweiligen BestSign-Passworts bzw. der TouchID als Besitzfaktor eingesetzt werden können. Die Beantragung eines neuen Gerätes kann mit einem aktiven BestSign-Gerät oder beim Berater erfolgen.

Es sind Verbindungen zu maximal 3 Postbank-Benutzern möglich.

Einsatz von zusätzlicher Hardware

Ja, SealOne® Gerät

3.3 BV-appTAN (Bank-Verlag)

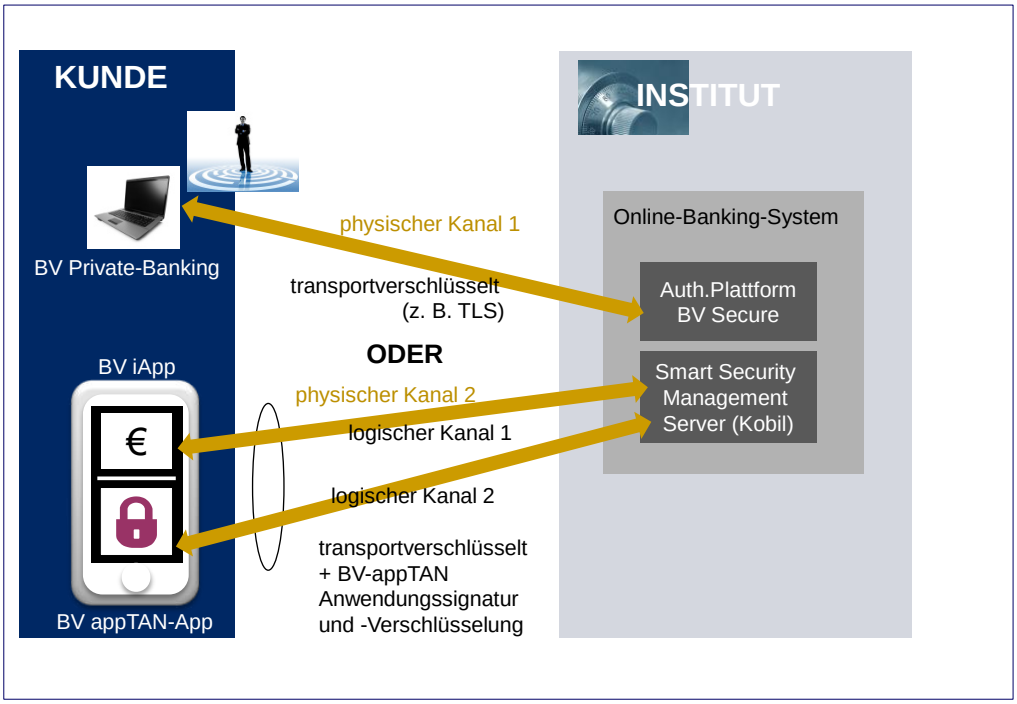

Abbildung 9: BV-appTAN (Bank-Verlag)

Verfahrenssteckbrief

Kriterium	Eigenschaften BV-appTAN
Institute	an Bank-Verlag angeschlossene Institute
Geräte	Smartphones und Tablets
Betriebssysteme	Android, iOS
Hersteller	Kobil
Szenario	Szenario 2 – Betrieb mit zwei logischen Kanälen
Positionierung	Bank-spezifisch
Registrierung	per Aktivierungsbrief (postalisch)
App-Passwort	Ja
TAN-Übertragung	Keine Angabe
Kosten für den Kunden	Bank-spezifisch

Unterstützte Vertriebskanäle

- Internet-Banking-Portal: ja, BV Private-Banking
- Mobile Banking: ja, BV iApp
- Apps vom Markt: nein
- FinTS-Kundenprodukte: nein

Beantragung

Bestandskunden können die BV-appTAN im BV Private-Banking beantragen.

Der Aktivierungsbrief enthält einen Freischaltcode, der im BV Private-Banking eingegeben werden muss.

Mehrere Geräte oder Bankverbindungen

Keine Angaben.

Einsatz von zusätzlicher Hardware

Nein

3.4 Photo-TAN (Commerzbank, Deutsche Bank)

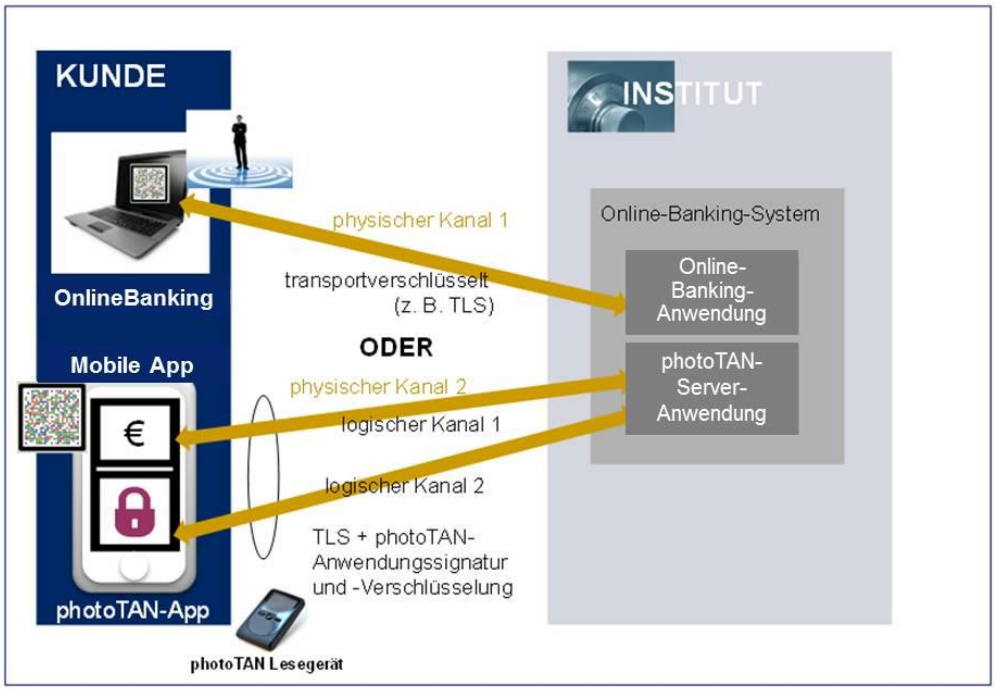

Abbildung 10: Photo-TAN (Commerzbank, Deutsche Bank)

Verfahrenssteckbrief

Kriterium	Eigenschaften Photo-TAN
Institute	Commerzbank, Comdirect, Deutsche Bank
Geräte	Smartphones und Tablets
Betriebssysteme	Android, iOS, Blackberry
Hersteller	Vasco
Szenario	Szenario 2 – Betrieb mit zwei logischen Kanälen
Positionierung	zusätzliches Verfahren
Registrierung	per Registrierungsbrief (postalisch)
App-Passwort	nein
TAN-Übertragung	Ja, zu DB Meine Bank
Kosten für den Kunden	kostenlos

Unterstützte Vertriebskanäle

- Internet-Banking-Portal: ja, DB OnlineBanking
- Mobile Banking: ja, DB Meine Bank
- Apps vom Markt: FinTS Banking-Apps
- FinTS-Kundenprodukte: Ja

Beantragung

Bestandskunden können PhotoTAN im DB OnlineBanking beantragen. Anschließend wird ein Aktivierungsschreiben mit einer Photo-TAN-Grafik per Post versendet. Dieses Aktivierungsschreiben ist benutzerbezogen, d. h. es kann für die Verwaltung von bis zu 8 Geräten verwendet werden.

Als nächstes muss die PhotoTAN-App aus dem jeweiligen Appstore geladen und installiert werden. Mithilfe dieser photoTAN-App wird die PhotoTAN-Grafik aus dem Aktivierungsschreiben fotografiert und ein 12-stelliger Aktivierungscode angezeigt. Dieser muss dann im Online-Banking eingegeben werden. Auf der Bestätigungsseite erscheint eine neue photoTAN. Nach dem Scannen wird die erste 7-stellige photoTAN generiert. Nach Eingabe dieser TAN im DB OnlineBanking und der Bestätigung in der photoTAN-App ist dieses Gerät aktiviert.

Mehrere Geräte oder Bankverbindungen

Es können bis zu 8 Geräte aktiviert werden, die ohne Verwendung eines Passworts als Besitzfaktor eingesetzt werden können. Die Beantragung eines neuen Gerätes kann mit einem aktiven TAN-Verfahren im DB OnlineBanking erfolgen. Nach der Aktivierung eines neuen Gerätes mit dem bereits vorliegenden Aktivierungsschreiben wird dieses nach 72 Stunden aktiv.

Es ist nur die Verbindung zu einem DB-Benutzer möglich.

Einsatz von zusätzlicher Hardware

Ja, photoTAN Lesegerät

3.5 pushTAN (Sparkassen, DKB)

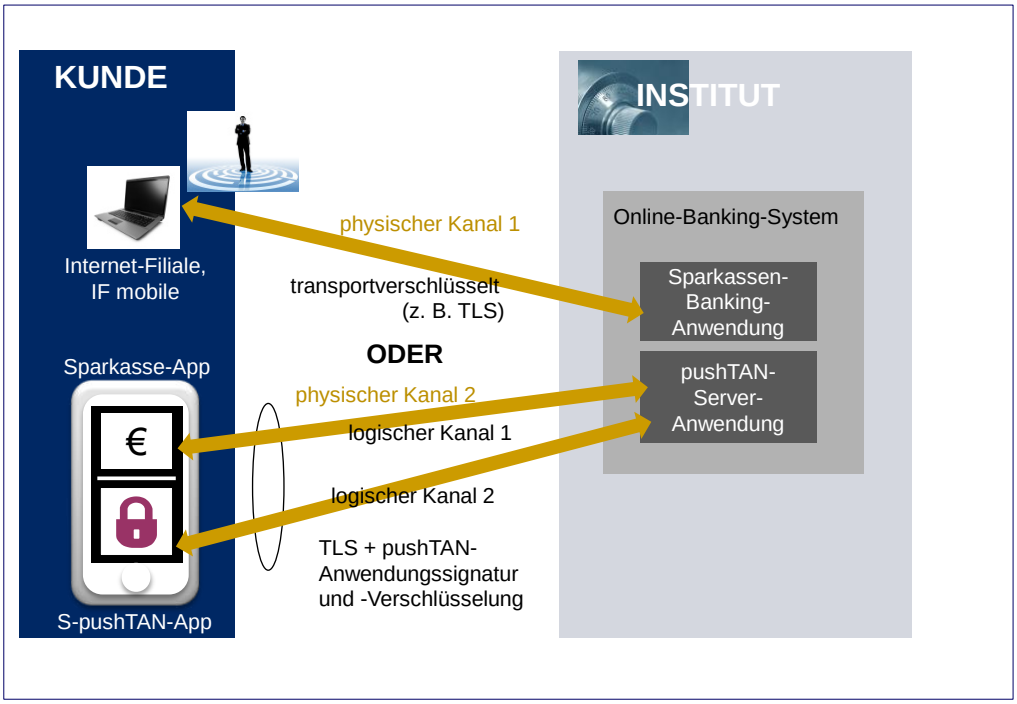

Abbildung 11: pushTAN (Sparkassen)

Verfahrenssteckbrief

Kriterium	Eigenschaften pushTAN
Institute	Sparkassen, DKB
Geräte	Smartphones und Tablets
Betriebssysteme	Android, iOS
Hersteller	Star Finanz
Szenario	Szenario 2 – Betrieb mit zwei logischen Kanälen
Positionierung	zusätzliches Legitimationsverfahren oder Ersatz
Registrierung	Registrierungsbrief (postalisch oder Filiale)
App-Passwort	ja, mindestens 8 Stellen (Ziffern, Buchstaben, Sonderzeichen)
TAN-Übertragung	ja, zu Sparkasse, Sparkasse+
Kosten für den Kunden	Sparkassen-spezifisch

Unterstützte Vertriebskanäle

- Internet-Banking-Portal: ja, Internet-Filiale, Internet-Filiale mobile
- Mobile Banking: ja, Sparkassen-App
- Apps vom Markt: FinTS Banking-Apps
- FinTS-Kundenprodukte: Ja

Beantragung

Bestandskunden können pushTAN in der Internet-Filiale und Internet-Filiale mobile beantragen. Anschließend wird ein Registrierungsbrief mit einem QR-Code per Post versendet oder in der Filiale ausgehändigt.

Als nächstes muss die S-pushTAN-App aus dem jeweiligen Appstore geladen und installiert werden. Bei der Initialisierung muss ein Zugangspasswort vergeben werden. Mithilfe der S-pushTAN-App wird der QR-Code aus dem Registrierungsbrief gescannt und ein 6-stelliger Freischaltcode angezeigt. Dieser muss dann in der Internet-Filiale bzw. Internet-Filiale mobile eingegeben werden. Nach erfolgreicher Prüfung des Freischaltcodes ist die S-pushTAN-App für dieses Gerät aktiviert.

Mehrere Geräte oder Bankverbindungen

Es können maximal 2 Geräte freigeschaltet werden die nach Eingabe des jeweiligen pushTAN-Passworts als Besitzfaktor eingesetzt werden können. Die Beantragung eines neuen Gerätes kann mit einem aktiven TAN-Verfahren in der Internet-Filiale und Internet-Filiale mobile erfolgen. Für das neue Gerät wird ein neuer Registrierungsbrief verschickt.

Es sind Verbindungen zu mehreren Sparkassen-Benutzern möglich.

Einsatz von zusätzlicher Hardware

Nein

3.6 QR-TAN (1822direkt)

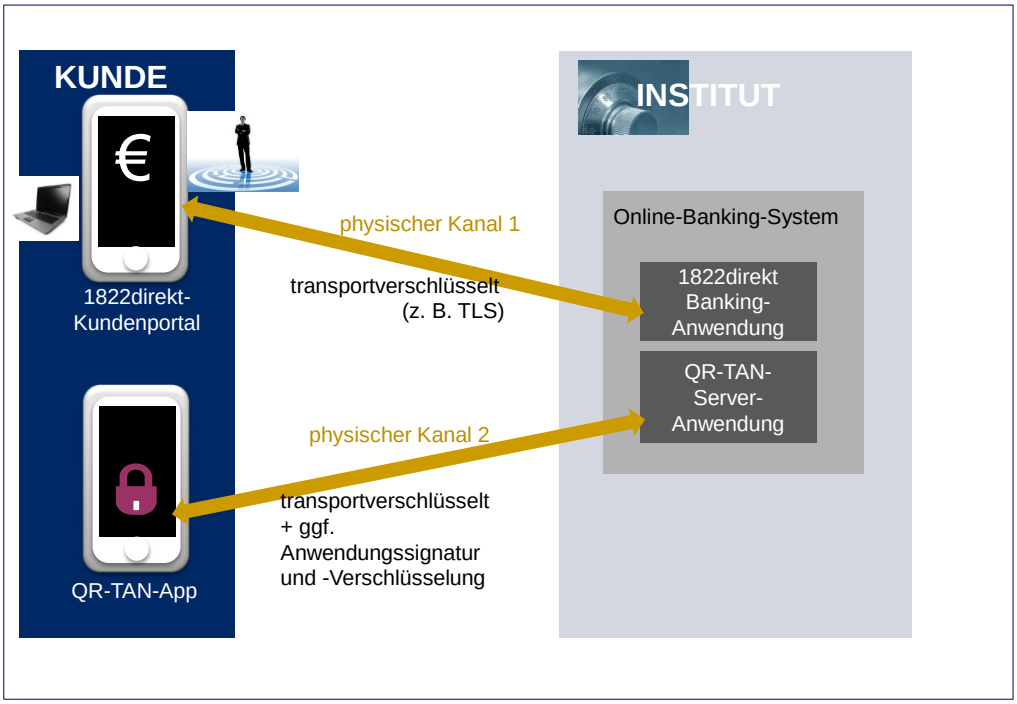

Abbildung 12: QR-TAN (1822direkt)

Verfahrenssteckbrief

Kriterium	Eigenschaften QR-TAN
Institute	1822direkt
Geräte	Smartphones (Mobilfunknummer benötigt)
Betriebssysteme	Android, iOS
Hersteller	
Szenario	Szenario 1 – Betrieb mit zwei Geräten
Positionierung	löst iTAN und mTAN ab
Registrierung	per Registrierungsbrief (postalisch)
App-Passwort	Ja
TAN-Übertragung	Ja, zum 1822direkt Kundenportal
Kosten für den Kunden	kostenlos

Unterstützte Vertriebskanäle

- Internet-Banking-Portal: ja, 1822direkt Kundenportal
- Mobile Banking: ja, 1822direkt Banking-App
- Apps vom Markt: nein
- FinTS-Kundenprodukte: nein

Beantragung

Bestandskunden können QR-TAN durch Verwendung einer TAN des bestehenden iTAN- oder mTAN-Verfahrens im 1822direkt Kundenportal oder per Telefonbanking beantragen. Anschließend wird ein Registrierungsbrief mit einem QR-Code und einer Aktivierungs-TAN per Post versendet.

Als nächstes muss die QR-TAN-App aus dem jeweiligen Appstore geladen und installiert werden. Bei der Initialisierung muss ein Zugangspasswort vergeben werden. Mithilfe der QR-TAN-App wird der QR-Code aus dem Registrierungsbrief gescannt und ein 6-stelliger Freischaltcode angezeigt. Dieser muss dann im 1822direkt Kundenportal eingegeben werden. Nach erfolgreicher Prüfung des Freischaltcodes wird dieser noch mit der Aktivierungs-TAN aus dem Brief bestätigt. Damit ist die QR-TAN-App für dieses Gerät aktiviert.

Mehrere Geräte oder Bankverbindungen

Pro Benutzer kann nur ein Gerät freigeschaltet werden, das nach Eingabe des Passworts als Besitzfaktor eingesetzt werden kann. Bei einem Gerätewechsel kann mit einem bestehenden TAN-Verfahren die Beantragung eines neuen Registrierungsbriefes im Kundenportal erfolgen. Das alte Gerät wird mit der Freischaltung des neuen Gerätes deaktiviert.

Es ist nur die Verbindung zu einem 1822direkt-Benutzer möglich.

Einsatz von zusätzlicher Hardware

Nein

3.7 SmartSecure (ING DiBa)

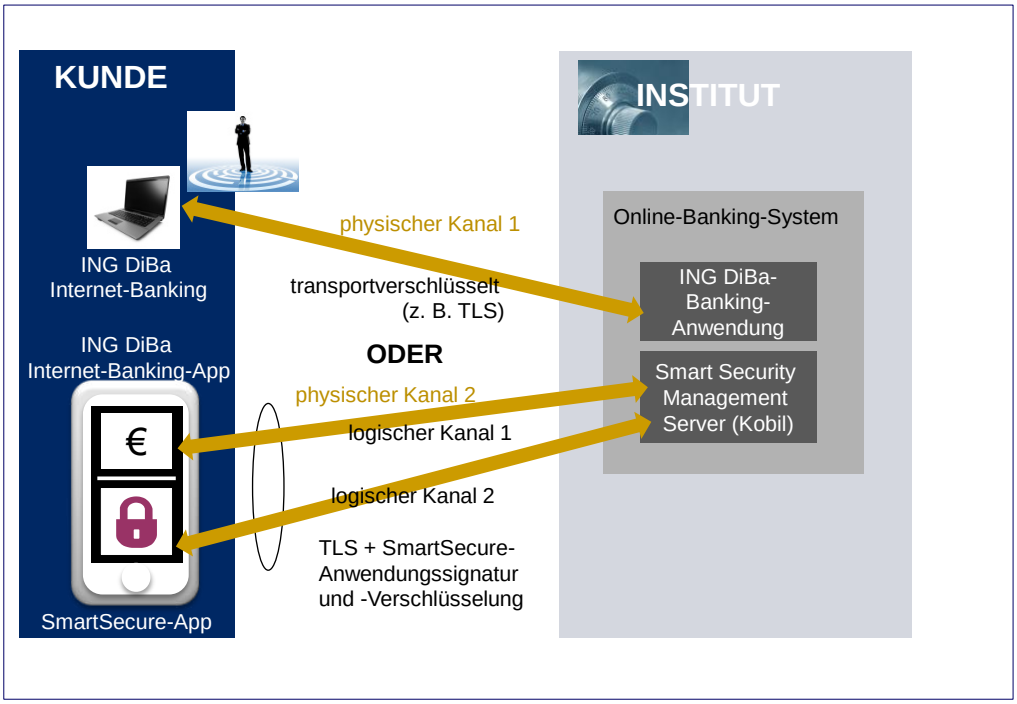

Abbildung 13: SmartSecure (ING DiBa)

Verfahrenssteckbrief

Kriterium	Eigenschaft
Name	SmartSecure
Institute	ING DiBa
Geräte	Smartphones (Mobilfunknummer benötigt)
Betriebssysteme	Android, iOS
Hersteller	Kobil
Szenario	Szenario 2 – Betrieb mit zwei logischen Kanälen
Positionierung	löst iTAN ab
Registrierung	online: Eingabe der Mobilfunknummer im Internet-Banking und TAN des bestehenden Verfahrens
App-Passwort	Ja
TAN-Übertragung	Ja, zum ING DiBa Internet-Banking und der Internet-Banking-App

Kriterium	Eigenschaft
Kosten für den Kunden	kostenlos

Unterstützte Vertriebskanäle

- Internet-Banking-Portal: ja, ING DiBa Internet-Banking
- Mobile Banking: ja, ING DiBa Internet-Banking App
- Apps vom Markt: nein
- FinTS-Kundenprodukte: nein

Beantragung

Bestandskunden können SmartSecure im ING DiBa Internet-Banking direkt aktivieren. Dazu muss die SmartSecure-App aus dem jeweiligen Appstore geladen und installiert werden. Im Registrierungsprozess wird die Mobilfunknummer für SmartSecure festgelegt. Es erfolgt die Freigabe mit einer TAN des bestehenden Verfahrens. Auf der Bestätigungsseite wird ein QR-Code angezeigt, der mit der SmartSecure-App fotografiert wird. Damit ist SmartSecure für dieses Mobiltelefon aktiviert.

Mehrere Geräte oder Bankverbindungen

Es kann maximal ein Gerät aktiviert werden, das nach Eingabe des Passworts als Besitzfaktor eingesetzt werden kann. Die Beantragung eines neuen Gerätes kann mit dem aktivierten SmartSecure Gerät erfolgen. Nach Scannen des QR-Code mit dem neuen Gerät ist dieses dann aktiv und das alte Smartphone deaktiviert.

Es ist nur die Verbindung zu einem ING DiBa-Benutzer möglich.

Einsatz von zusätzlicher Hardware

Nein

3.8 VR-SecureGo (Volks- und Raiffeisenbanken Süd)

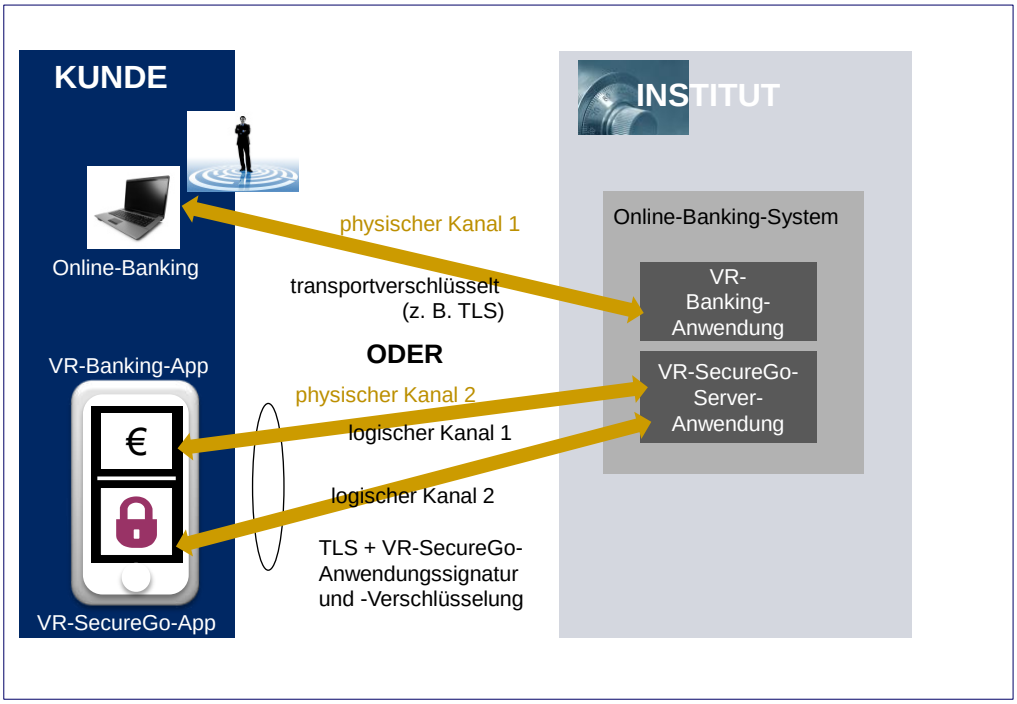

Abbildung 14: VR-SecureGo (Volks- und Raiffeisenbanken Süd)

Verfahrenssteckbrief

Kriterium	Eigenschaften VR-SecureGo
Institute	Volks- und Raiffeisenbanken Süd
Geräte	Smartphones und Tablets
Betriebssysteme	Android, iOS
Hersteller	Fiducia & GAD IT
Szenario	Szenario 2 – Betrieb mit zwei logischen Kanälen
Positionierung	löst mobileTAN ab
Registrierung	per Registrierungsbrief (postalisch)
App-Passwort	ja, 8 – 20 Stellen (Ziffern, Groß- und Kleinbuchstaben)
TAN-Übertragung	Ja, zur VR-Banking-App
Kosten für den Kunden	VR-Bank-spezifisch

Unterstützte Vertriebskanäle

- Internet-Banking-Portal: ja, Online-Banking
- Mobile Banking: ja, VR-Banking-App
- Apps vom Markt: ja
- FinTS-Kundenprodukte: ja

Beantragung

Bestandskunden können VR-SecureGo über die VR-SecureGo-App beantragen. Hierzu muss als erstes die VR-SecureGo-App aus dem jeweiligen Appstore geladen und installiert werden. Bei der Initialisierung muss ein Zugangspasswort vergeben werden. Dann werden der gewünschte VR-NetKey und die zugehörige Online-Banking-PIN erfasst und über den Authentifizierungskanal zum Institut gesendet. Im Online-Banking kann dann ein Registrierungsbrief beantragt werden. Dieser wird per Post versendet und enthält einen QR-Code mit den Registrierungsdaten.

Nach Auswertung des QR-Code aus dem Registrierungsbrief mit der VR-SecureGo-App wird ein Freischaltcode angezeigt. Dieser muss dann im Online-Banking eingegeben werden. Nach erfolgreicher Prüfung des Freischaltcodes ist die VR-SecureGo-App für dieses Gerät aktiviert.

Mehrere Geräte oder Bankverbindungen

Es kann maximal 1 Gerät aktiviert werden, das nach Eingabe des Passworts als Besitzfaktor eingesetzt werden kann. Die Beantragung eines neuen Gerätes kann mit dem aktivierten VR-SecureGo Gerät erfolgen. Es wird ein neuer Registrierungsbrief versendet. Nach Freischaltung des neuen Geräts ist dieses dann aktiv und das alte Smartphone / Tablet deaktiviert.

Es ist die Verbindung zu mehreren VR-NetKey-Benutzern möglich.

Einsatz von zusätzlicher Hardware

Nein

3.9 VR-SecureSIGN (Volks- und Raiffeisenbanken Nord)

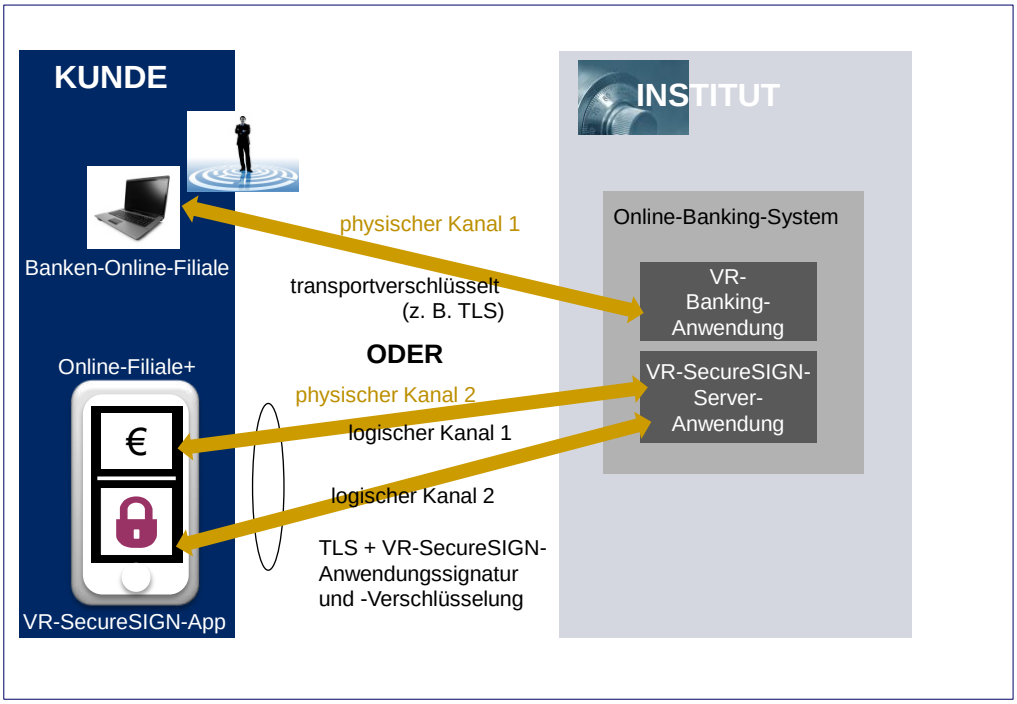

Abbildung 15: VR-SecureSIGN (Volks- und Raiffeisenbanken Nord)

Verfahrenssteckbrief

Kriterium	Eigenschaft VR-SecureSIGN
Institute	Volks- und Raiffeisenbanken Nord
Geräte	Smartphones und Tablets
Betriebssysteme	Android, iOS
Hersteller	Coronic
Szenario	Szenario 2 – Betrieb mit zwei logischen Kanälen
Positionierung	löst mobileTAN ab
Registrierung	per Registrierungsbrief (postalisch)
App-Passwort	Ja
TAN-Übertragung	Ja, zur Online-Filiale+
Kosten für den Kunden	VR-Bank-spezifisch

Unterstützte Vertriebskanäle

- Internet-Banking-Portal: ja, Banken-Online-Filiale
- Mobile Banking: ja, Online-Filiale+
- Apps vom Markt: ja
- FinTS-Kundenprodukte: ja

Beantragung

Bestandskunden können VR-SecureSIGN über die VR-SecureSIGN-App beantragen und freischalten. Hierzu muss als erstes die VR-SecureSIGN-App aus dem jeweiligen Appstore geladen und installiert werden. Bei der Initialisierung muss ein Zugangspasswort vergeben werden. Dem Smartphone / Tablet wird eine virtuelle Handynummer zugeordnet. Anschließend werden die Bankleitzahl, die gewünschte VR-Kennung und die zugehörige Online-Banking-PIN erfasst und über den Authentifizierungskanal zum Institut gesendet. Dies löst den Postversand eines Registrierungsbriefes aus, der einen Freischaltcode als Text und QR-Code enthält. Der Freischaltcode wird nach Erhalt des Registrierungsbriefes ebenfalls in der VR-SecureSIGN-App eingegeben. Damit ist die Freischaltung abgeschlossen und die VR-SecureSIGN-App für diese virtuelle Handynummer aktiviert.

Mehrere Geräte oder Bankverbindungen

Es kann maximal 1 Gerät aktiviert werden, das nach Eingabe des App-Passworts als Besitzfaktor eingesetzt werden kann. Die Beantragung eines neuen Gerätes kann mit dem aktivierten VR-SecureGo Gerät erfolgen. Es wird ein neuer Registrierungsbrief versendet. Nach Freischaltung des neuen Geräts ist dieses dann aktiv und das alte Smartphone / Tablet deaktiviert.

Es ist die Verbindung zu mehreren VR-Kennungen möglich.

Einsatz von zusätzlicher Hardware

Nein

4 Fazit

Die Gegenüberstellung der App-basierten Verfahren zeigt, dass das Smartphone / Tablet als Authentifizierungsinstrument Einzug in die Banken- und Sparkassenwelt gehalten hat. Die einzelnen Lösungen unterscheiden sich vom Funktionsumfang teilweise deutlich, jedoch lassen sich alle auf die eingangs gezeigten drei Szenarien zurückführen.

Da alle vorgestellten Produkte sich im Rahmen der regulatorischen Anforderungen bewegen müssen, sollten die kritischen Sicherheitsfragen geklärt und entsprechende Härtungsmaßnahmen erfolgt sein. Somit ist die Deutsche Kreditwirtschaft im Bereich der mobilen Absicherung von Online-Banking-Transaktionen am Markt repräsentativ vertreten.

Die Zukunft wird jedoch erst zeigen, wie robust die einzelnen Anwendungslösungen gegen reale Angriffe sind bzw. als Softwarelösungen sein können. Heutige Angriffsszenarien unter Laborbedingungen bieten keine repräsentativen Aussagen, lassen jedoch bereits erkennen, dass sich ein stetiger Wettlauf zwischen Angriffsmustern und Härtungsmaßnahmen ergeben wird, dem sich die Hersteller der Authentisierungs-Apps stellen werden müssen.

Dokumentversion 1.1, 11.01.2017

Literaturverzeichnis

[1] DK-Kompendium Online-Banking-Sicherheit
Februar 2014
Die Deutsche Kreditwirtschaft

[2] Rundschreiben 4/2015 (BA) – Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI)
05.05.2015
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

[3] Häufige Fragen zum Rundschreiben 4/2015 (BA)
24.06.2016
Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)

[4] Payment Service Directive (PSD) 2
28.09.2015
Europäisches Parlament und Rat

[5] Consultation Paper – PSD2 Regulatory Technical Standard (RTS)
12.08.2016
European Banking Authority

Abkürzungsverzeichnis

BaFin	Bundesanstalt für Finanzaufsicht
EBA	European Banking Authority
MaSI	Mindestanforderungen an die Sicherheit von Internet-Zahlungen
PSD2	Payment Service Directive 2
RTS	Regulatory Technical Standard der EBA

Abbildungsverzeichnis

PPI AG

Moorfuhrtweg 13
22301 Hamburg
Tel.: +49 40 227433-0
Fax: +49 40 227433-333

E-Mail: info@ppi.de
Internet: www.ppi.de

Dokumentversion 1.1, 11.01.2017