„Biometrie und Besitz verdrängen Karte & PIN/TAN“

Strategien und Lösungsansätze für ein Banking-Ökosystem nach der PSD2

CORONIC
Software & Security

Verzeichnisse

0.1 Inhaltsverzeichnis

0.2 Abbildungsverzeichnis

Über Autor und Inhalt

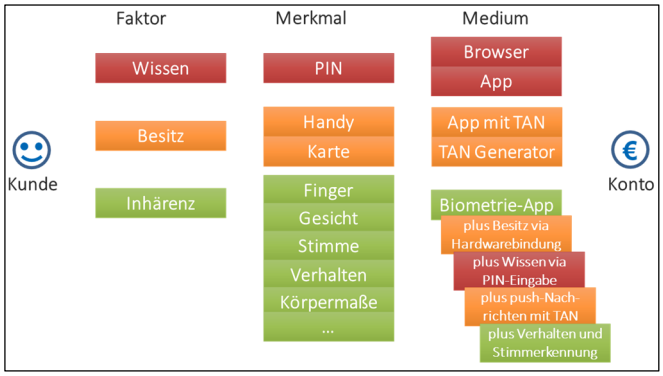
Mein Name ist Frank Bock, ich habe ursprünglich einmal Atomphysik studiert, aber wie Sie sehen, bin ich in der IT gelandet. Ich bin geschäftsführender Gesellschafter der CORONIC GmbH und wir beschäftigen uns seit 16 Jahren mit Sicherheitsprodukten und Authentifizierungsverfahren für Banken. Über 900 Banken im In- und Ausland setzen unsere Produkte im Online-Banking ein. Im Moment wird unsere Branche gerade dereguliert und die PSD2 wird sicher nicht der letzte Schritt in diese Richtung sein. Wem nicht ganz klar ist, was Deregulierung für Banken bedeutet, kann sich gerne daran erinnern, dass es einmal ein staatliches Monopol auf den Postverkehr, die Telekommunikation oder auf die Stromversorgung gegeben hat.

Zeit also, sich Gedanken über die Zukunft der Banken zu machen. Wo entwickeln sich die Systeme hin, was ist technologisch möglich und was wird uns strategisch wie technisch abverlangt? Da auch ich keine Kristallkugel besitze, habe ich mich entschieden in den folgenden Ausführungen hauptsächlich Ideen und Lösungsansätze zu vermitteln, die uns und unsere Kunden im Moment bewegen. Es geht dabei sowohl um strategische Ansätze für das Banking in der Zeit nach der PSD2, als auch um die richtigen technologischen Entscheidungen für die nähere Zukunft.

Ich hoffe, dass ich damit einigen von uns weiterhelfen kann, zumindest jedoch Diskussionen und Gedanken beflügele, die unsere Branche einen Schritt voranbringen. Sagen Sie mir gerne Ihre Meinung, ich verspreche auch zu antworten: frank.bock@coronic.de

1 Zusammenfassung

Während die meisten noch über die PSD2 sprechen, ist die zentrale Frage eigentlich: was kommt danach? Kann man die nächste Regel erahnen oder zumindest bereits heute technisch in eine Richtung gehen, die auch zukunftssicher bezüglich einer möglichen PSD3 ist? Wie immer in unsicheren Situationen hilft ein Blick zurück: Banken haben Authentifizierungssysteme, die sich längs der Kundenprodukte entwickeln. Sicherheitsverfahren wie TAN, photo, Flicker und push sind jeweils einzeln in die App, den Browser oder den PC-Client integriert. Spätestens jetzt, wo die Regulatoren „unendlich viele“ neue Merkmale für das Banking freigegeben haben, wird klar, dass ein „weiter so“ nicht funktioniert. Viele Finanzdienstleister sind gerade dabei eine Authentifizierungsstrategie zu entwickeln und beschäftigen sich mit Themen wie FIDO, yes, VERIMI oder der Vereinheitlichung von Schnittstellen für ID[1]-Prozesse. Noch ist nicht wirklich klar, wer das Rennen macht, aber klar ist: es braucht eine zentralisierte ID-Strategie, die unabhängig von Kundenprodukten den Zugang zu denselben steuern und autorisieren wird. Das Zielbild einer solchen Strategie kann dabei durchaus fordernd formuliert werden:



- Keine separate Hardware mehr (nur noch Smartgeräte oder Software des Kunden)
- Mutige halten die Chipkarte auch für eine Hardware!
- Keine Wissenselemente mehr (denn der Kunde ist vergesslich)
- Keine (transaktionsbasierten) Kosten mehr für Banken und Kunden

Schwierig wird es dann erst bei der Ausformulierung der Strategie und der konkreten Umsetzung, also der Frage nach den ersten (technischen) Schritten: Mit welcher Technologie wollen wir die Zukunft bestreiten und wie sieht das erste Pilotprojekt aus? Dafür bietet sich die Biometrie als der große vereinheitlichende Faktor an. Zum einen verfügt Biometrie über deutlich mehr Merkmale, als dies die Bestandsfaktoren (Wissen & Karte) bisher ermöglicht haben. Zum anderen ist die Umsetzung von Biometrie in Form einer zentralen ID-App in der Lage die Altverfahren zu integrieren. Ein Besitzmerkmal in Form einer Hardwarebindung ist genauso in die ID-App integrierbar wie die heute im Einsatz befindliche push-Technologie. Damit werden Biometrie und Besitz zum natürlichen Anker für das Banking-Ökosystem nach der PSD2. Beide Faktoren als Team bieten Lösungsräume für Online-Banking, Brokerage und das Versicherungsportal oder kurz: für jede starke Kundenauthentifizierung. Wenn man noch ein paar technische Details im RTS beachtet und die Faktoren in zwei getrennte Ausführungsumgebungen implementiert, lassen sich sogar beide Faktoren in einer einzigen App unterbringen. Genau in dieser Konstellation können Biometrie und Besitz dann tatsächlich Karte und PIN/TAN verdrängen – bequemer, schneller, besser und dabei stets regulatorikkonform.

[1] Identitäts-Prozess: Verfahren, in denen der Nutzer authentifiziert wird.

2 Strategien für die Zeit nach der PSD2

Rahmen, Regeln und Vorgaben ändern sich andauernd, das ist der Lauf der Zeit. Ja klar, es hat Banken und Finanzdienstleister in den letzten Jahren relativ hart getroffen. Und selbstverständlich ist der größte Stolperstein, die Umsetzung der PSD2, auf der Zielgeraden. Auch hier gilt sicher wie beim Fußball: nach der PSD2 ist vor der PSD3 - so sehen es zumindest die Pessimisten in der Branche. Und so sehr wir bei Betrachtung der Jahre seit 2008 einen pessimistischen Blick in der Finanzszene nachvollziehen können, so unnötig ist er tatsächlich. Man neigt einfach dazu, vor lauter Problemen und Risiken nicht mehr auf die Chancen zu schauen. Die Chancen, die sich gerade jetzt durch den ersten europaweiten Regulierungsrahmen für Finanzdienstleister zwangsläufig ergeben. Gerade für die deutschen Banken, Sparkassen und Versicherungen ist diese Chance in ganz Europa am größten. Unsere Prozesse und Lösungen waren seit jeher dicht dran an den neuen Vorgaben, die die EU nun für alle verbindlich festgeschrieben hat. Die zentrale Frage ist also nicht „was kommt da auf uns zu“, sondern vielmehr „welche Möglichkeiten ergeben sich für uns danach“ - strategisch, wie auch technologisch.

2.1 Der Status Quo im Banking

Es gibt in Deutschland zwar einen ganzen Zoo von Authentifizierungsmaßnahmen für Login und Überweisung, aber anders als in der sonstigen EU sind diese bei den Banken hinreichend gleich. Würde man den deutschen Endkunden fragen, wer die TAN erfunden hat, so würde die Antwort wahrscheinlich „Angela Merkel“ lauten. Ich hoffe, Sie erkennen in diesem kleinen Spaß das große Potenzial des deutschen Bankensystems: Man hat sich in den Gremien auf einheitliche Standards und Abläufe geeinigt, auch wenn es davon immer noch zu viele gibt (und sie sich ehrlicherweise im Detail auch etwas unterscheiden). Damit ist nicht so sehr gemeint, dass die SMS-basierte TAN einmal mobileTAN, mTAN, oder smsTAN heißt, sondern dass Freischaltprozesse, Prozesse beim Gerätewechsel und die Einbindung in den Überweisungsprozess bei jeder Bank unterschiedlich verlaufen. Gleiches ließe sich für photo-, chip- oder push-Verfahren ausführen. Wenn man so mag, haben wir eine abgestimmte, ähnliche Basis von technologisch gleichartigen Authentifizierungsverfahren. Dies jedoch in nahezu unendlich vielen Integrationsvarianten, was sowohl die Interoperabilität als auch den kundenfreundlichen Einsatz von Omnikanalstrategien schwierig macht. Ich weiß, der Plan war ja positiv an das ganze heranzugehen und daher: letzten Endes ist auch eine leicht heterogene Basis besser als gar keine Basis.

Abbildung 1 "Kleine Auswahl von Bankverfahren"

2.1.1 Authentifizierung als Aufgabe der Kundenprodukte

Die Frage nach der Integration in die banküblichen Überweisungsverfahren führt allerdings gleich zur nächsten Herausforderung: Integration bedeutet bei fast jeder Bank Integration in das jeweilige Kundenprodukt. SMS, push, photo - alles individuell integriert in das browserbasierte Online-Banking und dann genau die gleichen Verfahren nochmal individuell integriert in den PC-Client und dann noch einmal alles in die App und als letztes in die stationären Automaten. Authentifizierung war in Deutschland schon immer eine Aufgabe des Kundenproduktes. Das Kundenprodukt ist meist einer Abteilung zugeordnet und so gibt es heute in fast allen Rechenzentren ein trautes nebeneinanderher von individuellen Implementierungen der bestehenden Authentifizierungsverfahren in die unterschiedlichen Kundenprodukte. Dieser technische Trend der vergangenen Jahre hat sich gewissermaßen in den organisatorischen und hierarchischen Strukturen der Banken nachgebildet. Zuständigkeit für Online-Banking getrennt von der Zuständigkeit für PC-Clients, von der für Apps und von der für SB- und Geldautomaten. So ist die Welt, in der wir uns heute alle bewegen.

Zu dieser Vielfalt an unterschiedlichen Authentifizierungsmöglichkeiten für unterschiedliche Kundenprodukte kommen jetzt mindestens drei neue Spieler hinzu: die Stimme, der Fingerabdruck, das Gesicht und vielleicht auch das Verhalten. Und dummerweise sind die drei nur die ersten Vertreter einer neuen Art, es werden weitere Inhärenzfaktoren folgen. Und alle können als eigenständiger Faktor für eine starke Kundenauthentifizierung genutzt werden. Bleibt man in der „alten Welt“ und bei den „alten Regeln“, werden alle zusätzlichen Faktoren in alle Kundenprodukte als neue Authentifizierungsmöglichkeiten integriert. Wir führen also viermal die Integration von vier verschiedenen Faktoren in mindestens drei unterschiedlichen Kundenprodukten durch, was die ehedem große Heterogenität weiter ausbauen würde. Rein taktisch ist dies der richtige Zeitpunkt, um über eine Neuausrichtung sowohl der Verbindung von Kundenprodukt und Authentifizierungsverfahren als auch der Auswahl der „sinnvollen Faktoren“ für eine starke Kundenauthentifizierung nachzudenken.

Abbildung 2 "Implementierung jedes Faktors in jedem Kundenprodukt"

2.2 Die Sonderrolle der Biometrie

Um vor all der integrativen Vielfalt nicht den Überblick zu verlieren, lohnt es sich einen Schritt zurückzutreten. Blickt man auf die Faktoren, mit denen Authentifizierung stattfindet oder auch auf die Medien, über die diese umgesetzt wird, so lichtet sich die alte Welt. Im Prinzip gibt es das klassische Wissensmerkmal, das in über 90 % der Fälle als PIN ausgestaltet wurde und es gibt das klassische Besitzmerkmal, das entweder die Chipkarte selbst oder aber ein mit der Push-App verbundenes Smartphone ist. An dieser Stelle betritt dann die europäische Regulatorik das Rampenlicht: wir bekommen einen neuen Faktor, der hier den „Straßennamen“ Biometrie bekommen soll.

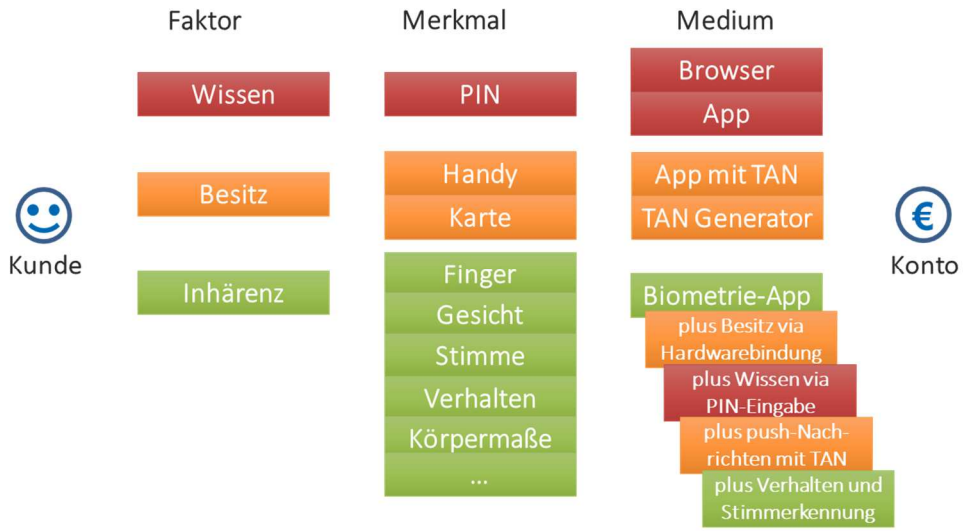


Abbildung 3 "Verteilung der PSD-konformen Faktoren und Merkmale auf die Medien"

Das erste, was beim Blick auf die Abbildung 3 ins Auge fällt, ist, dass der neue Faktor mehr als nur ein Merkmal hat. Ganz im Gegenteil, er kann 10 oder mehr Merkmale besitzen (Iris, Venen, Herzschlag, Pigmentierung, Gang, Körpermaße, …). Vor dem Hintergrund der aktuellen technologischen Landschaft auf Endkundenseite sind (erst mal) allein die Merkmale Stimme, Finger, Gesicht und Verhalten umsetzbar. Nichtsdestotrotz ließe sich die Kette der Merkmale beliebig verlängern. Schon grafisch fällt also auf, dass bei Biometrie mehr drin ist (grün), als die alte Welt (rot, gelb) jemals im Angebot hatte. Ein kurzes Gespräch mit dem Datenschutzbeauftragten wird die meisten davon überzeugen, dass eine Überprüfung der biometrischen Daten (gleich welcher Art) nur möglich ist, solange das Datum nicht die Hemisphäre des Kunden verlässt. Damit sind biometriebasierte Merkmale nur überprüfbar in einer (Smart-)Hardware, die der Kunde selber mitbringt. Ganz folgerichtig taucht hier dann auch das Wort von der Biometrie-App zum ersten Mal auf, die, anders als ihre Kollegen in der alten Welt, den Zugriff auf viele verschiedene Merkmale ermöglicht.

Die Umsetzung als App hat aber noch eine zweite Konsequenz: es lassen sich auch andere Faktoren integrieren. Der Besitz, genauso wie es in der Push-App gemacht wird und das Wissen, genauso wie es in der Banking-App gemacht wird. Damit hat die Biometrie-App die Fähigkeit, die gesamte alte Authentifizierungswelt in Form von Software unter ihrer Hoheit neu zu ordnen. Ehrlicherweise muss man natürlich zugestehen, dass auch die bestehende Push-App

(oder Banking-App) die neuen biometrischen Merkmale unter sich vereinen könnte, aber dann hätten wir im Prinzip nur den Namen der App gewechselt, die Aussage bliebe die gleiche.

2.2.1 Von FIDO, yes, VERIMI, MobileConnect & Co.

Was aber ist nun die technische Struktur für die neuen ID- und Authentifizierungsprozesse, wie sie uns zukünftig alle begleiten werden? Ich setze dabei mal stillschweigend voraus, dass keiner Lust hat, die einzelnen biometrischen Merkmale in alle bestehenden Kundenprodukte zu integrieren, wie es die Abbildung 2 als schlechtes Beispiel unterstellt. Im Prinzip klingt die Lösung ganz einfach: wir brauchen einen zentralen Authentifizierungsprozess für alle Kundenprodukte. An dieser Stelle teilen sich dann sprachlich die Welten: die einen sprechen von ihrem zentralen Authentifizierungssystem, die anderen von einem zentralen ID-Server, die Dritten von definierten Schnittstelle, um alle Identifikationsprozesse zentral im Banksystem zu integrieren. In diesem Punkt sind die Sorgen (der Pessimisten) sowie die Ideen und Wünsche (der Optimisten) in den Banken sogar einmal deckungsgleich mit denen der großen IT-Konzerne. Auch Google, Amazon und Co. haben ein Login-Problem und ein Online-Einkauf-Problem. Auch hier hat der zweite Faktor die Kundenkommunikation nicht gerade erleichtert und daher gibt es Ansätze, um gemeinsam Normen für Schnittstellen zu etablieren, wie sie zum Beispiel die Fido Allianz vorschlägt.

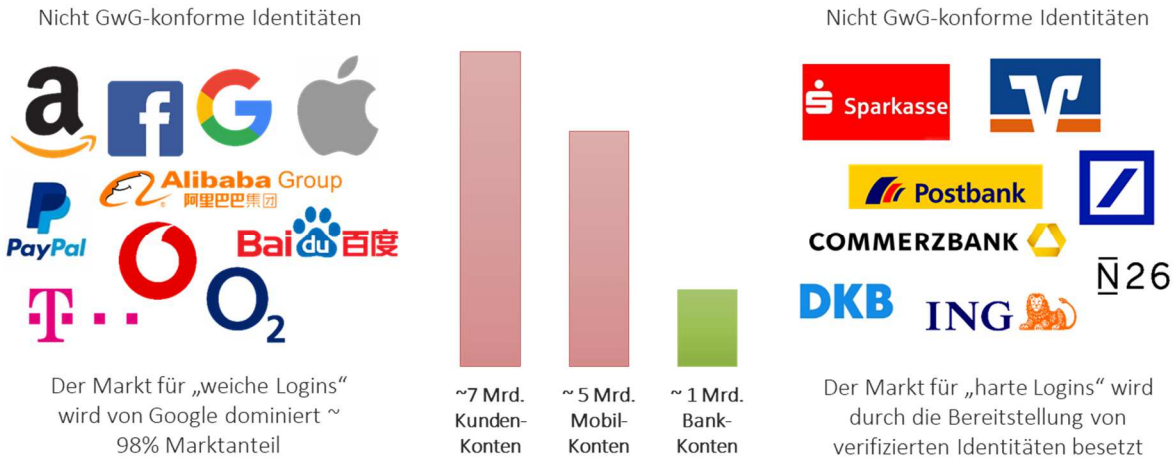


Abbildung 4 "Verifizierte Identitäten sind das Alleinstellungsmerkmal der Banken"

Banken sollten an dieser Stelle umsichtig sein, denn FIDO hat zwar eine PSD2-Spezifikation herausgebracht (Ende 2018), aber der Umsetzungskern der FIDO-Architektur ist das Login bzw. der Online-Einkauf. Leider beides in einem Kontext, der kein Dynamic Linking kennt. Und das ist auch nur das kleinere Problem, denn alle neuen ID-Dienste der großen US-Konzerne verfügen nur über nicht verifizierte Identitäten. Platt gesagt hängt die Identität an einer E-Mail-Adresse und nicht an einem (mit Ausweis) identifizierten echten Kunden. Das Login, das daraus resultiert, kann man bestenfalls als „weiches Login“ bezeichnen. Die Transaktion, die daraus resultiert, reicht bestenfalls zum Schuhe kaufen im Internet. Nicht so bei den Banken. Sie verfügen über verifizierte Identitäten. Diese sind nutzbar für „harte Logins“, in denen der Kunde tatsächlich identifiziert wird. Mit Hilfe eines zweiten Faktors können sie wie eine nor-

male rechtsgültige Unterschrift eingesetzt werden (nach erfolgter eIDAS-Zertifizierung[2]). Ehrlicherweise sollte man die großen Telcos auch nicht vergessen, die mit MobileConnect ähnliches im Sinn haben. Auch sie haben jedoch keine GwG[3]-konformen Identitäten und bezüglich des Kundenvertrauens deutlich das Nachsehen gegenüber den Banken.

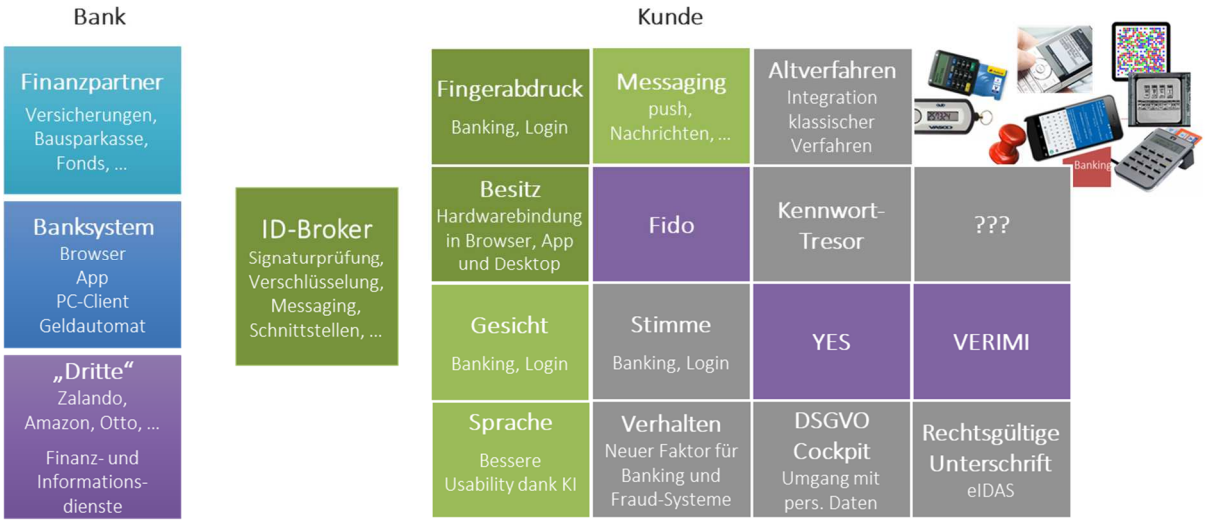


Abbildung 5 "ID- und Authentifizierung-Dashboard[4]"

Nichtsdestotrotz schadet es uns Banken nicht, den Blickwinkel noch mehr auf Kundenfokus umzustellen, denn das haben die großen IT-Konzerne uns wirklich voraus. Unser Augenstern ist nach wie vor das Banksystem, ihm gelten 95 % unserer Aufmerksamkeit. Rechts und links des Weges sind vielleicht noch ein paar Finanzgruppenpartner, Versicherungen oder Bausparkassen zu integrieren und … ach ja, dann gibt es da natürlich auch noch Dinge wie Zalando und Amazon. Aus Sicht des Endkunden steht unsere Welt auf dem Kopf. Der Kunde interagiert zu 95% unten links in der Abbildung 5. Dort wo er seine Waren und Dienstleistungen bestellt. Und er sagt „ach ja, da gibt es auch noch Online-Banking“. In diesem Umfeld unterschiedlicher Brennpunkte gilt wie immer: Schuster bleib bei deinen Leisten. Die Banken sollten ihre Schnittstellen zum Online-Banking und zu den Finanzpartnern selbst im Griff haben, um langfristig nicht zum Bereitsteller einer Überweisungsinfrastruktur degradiert zu werden. Gleichzeitig sollten sie aber auch ihre Kunden fest im Blick haben und denen auch den Zugriff auf den Hauptteil ihrer Lebenswirklichkeit ermöglichen (also die Login- und Shopping-Systeme Dritter). Und vor allem sollten wir uns darüber bewusstwerden, welche Macht wir besitzen, denn faktisch verfügt jeder Deutsche über eine verifizierte Identität bei seiner Bank. Man kann diesen Punkt gar nicht deutlich genug betonen, denn nachdem die PSD2 uns die Hoheit über die Umsätze genommen hat, ist dies der einzig verbleibende Schatz, der noch in unseren Kundendaten steckt. Optimisten fangen am besten jetzt an ihn zu nutzen … bevor die PSD3 ihn in ein paar Jahren auch noch wegnimmt. Daher kann die Umsetzung zwar gerne mithilfe Dritter oder

[2] Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im EU Binnenmarkt
[3] Geldwäschegesetz
[4] „Grüne Elemente“ hat CORONIC bei Kunden im Einsatz, „Graue“ sind technisch heute schon umsetzbar.

aber auf Basis von fremden Spezifikationen erfolgen, aber zumindest die Schnittstellen zum Banksystem sollten in eigener Hoheit und Verantwortung bleiben.

2.3 Eine neue Ausrichtung für Technik und Management

Die Frage der richtigen Abgrenzung ist an dieser Stelle wirklich spannend. Welche Schnittstellen beschreibt man selbst? Wo bleibt die Bank der Herr ihrer Prozesse und wo setzt sie lieber auf internationale Standards oder Partner? Die Darstellung in Abbildung 5 ist daher sehr bewusst als ein Netzwerk aus unterschiedlichen funktionalen Kacheln angelegt. Hier können unterschiedliche Dienste mit unterschiedlichen Authentifizierungsverfahren über eine zentrale Schnittstelle zum Banksystem kommunizieren. Man sollte auch im Auge behalten, dass die alten organisatorischen Strukturen von Banken sich an den alten technischen Möglichkeiten orientiert haben. Wenn das hier auch der Fall werden sollte, stellt sich die Frage nach der „ID-Abteilung“, der zentralen Ausrichtung für diesen Bereich und der Integration der neuen ID-Prozesse in die allgemeine Bankstrategie. Das mag strategisch wie technisch einfach klingen, ist es aber in den meisten Fällen nicht.

Technisch sind bisher alle Authentifizierungssysteme von Banken davon ausgegangen, dass an irgendeiner Stelle Kontextinformationen (Kennwort, Alias, Anmeldename, PIN, TAN, …) in ein Kundenprodukt (Browser, App, PC-Client, Automat) eingegeben und im Backend geprüft werden. In der neuen Welt gibt es einen zentralen „ID-Dienst“, der eine zentrale Schnittstelle für alle Kundenprodukte bereitstellt. Keine ganz einfache Neuausrichtung für die Kollegen in der IT-Strategie, denn zum ersten Mal erfolgt der Authentifizierungsprozess „gewissermaßen hintenrum“ und nicht mehr direkt an der Benutzeroberfläche. Bezüglich der Organisationsentwicklung bietet sich (fast) das gleiche Bild. Einfach eine neue Abteilung gründen und die Zuständigkeiten neu sortieren wird nicht funktionieren.

2.3.1 Die Politik der kleinen Schritte

Der eine große strategische Wurf ist aus heutiger Sicht schon deswegen kaum darstellbar, weil noch nicht abzusehen ist, welche Technologien sich für Authentifizierungsprozesse in der Zukunft durchsetzen. Heute jedoch ist die Verbreitung von Biometriesensoren auf Smartgeräten sehr hoch und weiter stark steigend. Auch die Akzeptanz der Kunden für Fingerabdruck-basierte Lösungen liegt laut einer aktuellen PwC-Studie[5] mit 37% höher als bei jedem anderen Verfahren. Aber wirklich wissen, wie die Welt in fünf Jahren tickt, können wir natürlich nicht. Vollständig klar ist nur, dass die Banken auf einem Schatz an verifizierten Identitäten sitzen, dass sie weiterhin zentral die Hoheit über den Transfer von Geld besitzen, dass es ein zentralisiertes ID-System geben wird und, dass dieses idealerweise mehrere Faktoren in mehreren Kundenprodukten in immer gleicher Art und Weise zur Authentifizierung verarbeiten kann.

Soweit der Blick der Optimisten. Wir wollen aber natürlich auch die Pessimisten nicht vergessen. Sie bedauern ihre Hoheit über die Umsätze verloren zu haben, fühlen sich bedrängt vom Markteintritt der ID-Dienstleister und können am Horizont fremde Anbieter von Vertrauens- und Bezahldiensten erkennen, die ihnen den Markt streitig machen. Natürlich ist beides wahr

[5] Biometrische Authentifizierungsverfahren, PwC 11/2018

und natürlich kann beides passieren, aber wie schon gesagt, sind die Voraussetzungen, gerade der deutschen Finanzdienstleister, derzeit gut, dass sie den Wettlauf gewinnen können.

Eine Frage stellt sich nur: was sind die ersten Schritte in diesem Marathon? Nimmt man alles zusammen, was heute bekannt ist, so bietet sich Biometrie in der Ausprägung Fingerabdruck oder Gesichtserkennung als Ultima Ratio für den ersten Schritt an. Sie erfüllt den RTS[6], kann bestehende push-TAN- oder auch Karten-basierte Prozesse ersetzen und wird damit zum idealen Experimentierfeld für die Neuausrichtung der Bankstrukturen – organisatorisch wie technologisch. Es verbleibt allein die Frage nach den Kunden, die keine eigene Smarthardware besitzen. Hier kommt das gute alte Besitzmerkmal für starke Kundenauthentifizierung am Desktop zum Einsatz. Diesmal jedoch in Form einer gehärteten Softwarelösung, denn eine per USB oder Bluetooth angebundene Hardwarekomponente am Desktop will ja eigentlich keiner mehr haben. Als Spoiler für die technisch Interessierten: wenn Sie genau wissen wollen, wie Besitz und Biometrie auf Smartgeräten und Desktop sinnvoll implementiert werden kann und warum es statthaft ist, mit diesen beiden Faktoren auch am Desktop eine starke Kundenauthentifizierung durchzuführen, lesen Sie einfach weiter im Abschnitt 3.2.1. Es gibt für das biometrische Verfahren bereits eine Konformitätsfreigabe von SRC[7] in Bonn, ein DAkks[8]-Zertifikat, das Produkt ist im Piloteinsatz bei einer deutschen Bankengruppe und ja, man kann damit tatsächlich auf PIN und TAN und Chipkarte verzichten … wenn man es denn will.

2.3.2 Unser Zielbild

Das weitere Vorgehen bezüglich der Strategie kennen Sie im Prinzip: Bestandsanalyse für Strategie und Technologie machen, neues Zielbild definieren, als ersten Umsetzungsschritt eine Lösung für das Bankverfahren auf biometrischer Basis durchdeklinieren und dann aus den Unterschieden zwischen Zielbild und aktueller Wirklichkeit die nächsten Schritte ableiten. Wahrscheinlich sind die Zielbilder bei den meisten gar nicht so unterschiedlich:

> Wir wollen keine separate Hardware mehr (sondern nur noch Smartgeräte oder Software, die der Kunde sowieso benutzt),
> Die Optimisten unter uns halten auch die Chipkarte für eine Hardware,
> Wir wollen idealerweise auf Wissenselemente komplett verzichten (denn der Kunde neigt zum Vergessen),
> Die Verfahren sollten zentral und einheitlich über alle Kundenprodukte in gleicher Art funktionieren (Wagemutige könnten die Idee entwickeln, dass dies via DK[9] bei allen deutschen Banken ähnlich aussehen sollte),
> Und zuletzt darf das Ganze nichts mehr kosten (keine transaktionsbasierten Kosten für SMS oder Push oder separate Hardwarebausteine).

[6] Regulatory Technical Standards on strong customer authentication and secure communication
[7] Security Resarch & Consulting GmbH - Zertifikatsnummer SRC.00034.RTS.04.2019
[8] Deutsche Akkreditierungsstelle - Zertifiziert nach DIN EN ISO/IEC 17065 Richtlinie 2015/2366 (PSD2)
[9] Die Deutsche Kreditwirtschaft (DK) ist eine zentrale Einrichtung der deutschen Kreditinstitute

Wir haben solche Prozesse bereits bei namhaften Marktteilnehmern durchlaufen. Das beginnt bei der Authentifizierungsstrategie und endet bei Technik und Umsetzung. Wir freuen uns daher stets, wenn Sie sich mit Ihren Fragen an uns richten: frank.bock@coronic.de

3 Technische Lösungsräume von Besitz und Biometrie

In den letzten Abschnitten haben wir uns eher mit grundsätzlichen Betrachtungen zum Thema ID- und Authentifizierungsstrategie beschäftigt. Herausgekommen ist im Wesentlichen, dass man etwas ändern muss und dass Biometrie mit weitem Abstand der interessanteste Faktor ist, um als erster Umsetzungskandidat zu dienen. Hier stellen wir jetzt die einzelnen technischen Schritte vor, mit denen wir bei CORONIC die hausintern „Mittelbare Biometrie“ genannte Technologie umgesetzt haben. Das Verfahren hat im Herbst 2018 eine offizielle Konformitätsbestätigung der Firma SRC in Bonn erhalten. Alle dargestellten Lösungen für die Biometrie-App sind also BaFin- und RTS-konform. Bei konkretem Umsetzungsinteresse stellen wir das Gutachten auf Nachfrage gerne zur Verfügung, hier einmal kurz ein Zitat aus der Zusammenfassung:

> *„Der vorliegende Bericht weist nach, dass das Konzept Mittelbare Biometrie von CORONIC die aufsichtsrechtlichen Anforderungen aus dem RTS für die Freischaltung des Verfahrens, für das Login mit PIN und das Login ohne PIN sowie für die Transaktionsautorisierung erfüllt. Schließlich werden auch Prozesse zur Gerätemigration mit QR-Code und mit Migrationscode vollumfänglich als konform zum RTS eingestuft.“*

3.1 Technische Voraussetzungen für Biometrie am Smartgerät

Da nicht alle von uns tief in der Technik stecken, zunächst ein paar einleitende Worte - der Experte kann gerne ein Kapitel weiter springen. Auf Kundenseite wird ein Smartgerät (Handy, Tablet, Laptop) vorausgesetzt, dass über einen Biometriesensor verfügt. Dieser kann entweder eine Implementierung für Fingerabdrücke (Fingerprint) oder aber eine für Gesichtserkennung (FaceID) besitzen.

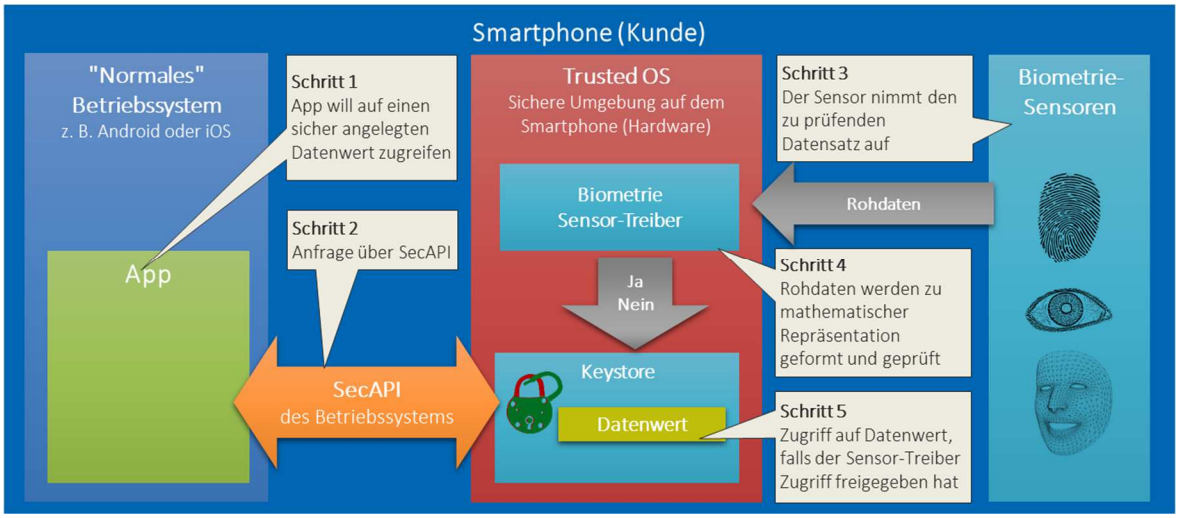


Abbildung 6 "Funktionsweise von Smartphone, TrustedOS und Biometriesensor"

Das normale mobile Betriebssystem, auf dem wir unsere Anwendung starten, ist nur ein Teil des Smartgerätes. Neben dem Standard-Betriebssystem gibt es eine im folgenden TrustedOS genannte Betriebssystemkomponente, die vom restlichen Betriebssystem entkoppelt ist. Sie kann nur über eine spezielle Schnittstelle angesprochen werden. Nur dieses gesicherte, hardwarenahe TrustedOS hat die Möglichkeit auf die Biometriesensoren zuzugreifen.

Um es sprachlich einfacher zu halten, werden wir uns im weiteren Verlauf auf den Fingerabdruck einschränken, technologisch ist die Umsetzung bei Apple-Geräten mit Gesichtserkennung identisch, die Aussagen sind also analog für iOS und Android gültig. Wird ein Fingerabdruckscan ausgelöst, werden die biometrischen Daten in eine mathematisch nicht umkehrbare Repräsentanz des Fingerabdruckes verwandelt. Man kann sich das am besten vorstellen wie der Hash eines eingegebenen Kennwortes. Zu dieser mathematischen Repräsentanz wird ein Schlüssel im TrustedOS abgelegt. Das TrustedOS sorgt dafür, dass dieser Schlüssel gebunden ist an das Gerät, die App (zum Beispiel die Biometrie-App) und an die vom Nutzer registrierten Fingerabdrücke. Eine Veränderung der Fingerabdrücke, zum Beispiel das Hinzufügen eines zusätzlichen Abdrucks, wird bemerkt. Die Spezifikationen der Hersteller Google und Apple für die biometrischen Sensoren geben eine Mindesterkennungsrate von 1:50.000 vor. Damit ist das System bezüglich der Erkennungsrate in der Größenordnung einer fünfstelligen Zahlen-PIN angesiedelt und erfüllt die gleichen Anforderungen, wie sie für die wissensbasierten Faktoren (zum Beispiel die PIN) verlangt werden. Nach wenigen Fehlversuchen wird die Funktion der Biometrie eingeschränkt und man muss sie erneut via Smartphone-PIN oder einem zuvor vergebenen Kennwort freischalten.

Für die nicht-technischen Leser noch ein Bild zur Interpretation der technischen Vorgänge: wenn Sie in Ihrem normalen Alltag den Fingerabdrucksensor am Smartphone verwenden, zum Beispiel, um eine App zu öffnen, wird der Fingerabdruck nur als eine Art Kennwortersatz verwendet. Bei der Mittelbaren Biometrie passiert mehr. Es geht darum, das tatsächliche biometrische Datum zu prüfen, ohne dass man Zugriff auf „ein Foto der Fingerkuppe“ hat (denn das gestattet das TrustedOS nicht). Man kann sich das im Prinzip wie bei einem Indizienprozess vor Gericht vorstellen. Die Tat wurde nicht gefilmt, es gibt keine direkten Tatzeugen, aber eine Reihe von beweiskräftigen indirekten Indizien. Diese Indizienbeweise sind bei der Mittelbaren Biometrie unterschiedliche kryptografische Schlüssel- und Signaturvorgänge, die den Nachweis erbringen, dass „bei der Überweisung von Herrn Meyer auch tatsächlich der Fingerabdruck von Herrn Meyer zugegen war“.

3.2 Login und Überweisen in einer App

Das Ziel steht im Prinzip schon in der Überschrift. Wir wollen Login-Vorgänge und Überweisungen in einer einzigen App ausführen - ohne TAN, ohne PIN und ohne Chipkarte.

3.2.1 Der Freischaltungsprozess

Als Beispiel haben wir den Freischaltprozess für die Biometrie-App gewählt. Das Sequenzdiagramm startet entweder, wenn eine Bank sich entscheidet eine neue Biometrie-App auszurollen oder aber, wenn eine bestehende Push- oder Banking-App um die Biometriefunktion erweitert wird. In jedem Fall müssen erst einmal RTS-konform die Freigaben für die Nutzung der

Biometrie sichergestellt werden, daher heißt die App hier schlicht und ergreifend Freigabe-App. Einer der interessantesten Punkte ist der Start des ganzen Prozesses im Punkt „A“. Die Freischaltung startet mit der Eingabe der Kontoverbindung und der PIN. Eine Implementierung in das Online-Banking oder die Eingabe von Daten in einem zweiten System sind nicht nötig. Die App kann freigeschaltet werden „allein aus der App heraus“.

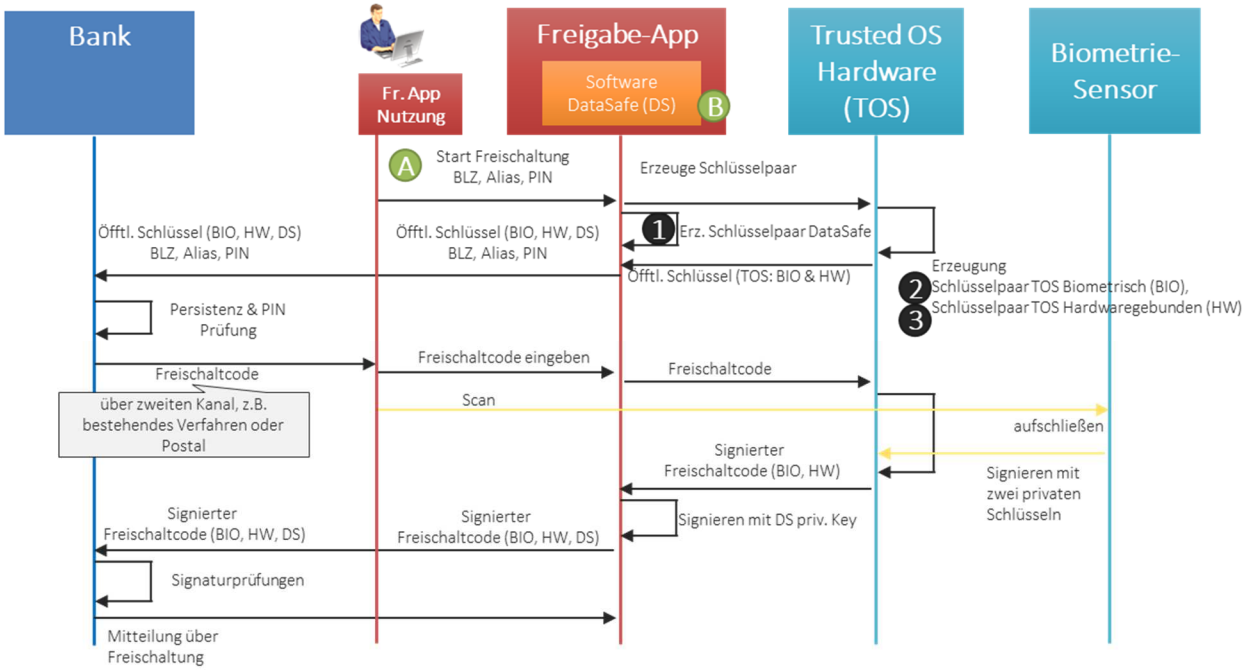


Abbildung 7 "Sequenzdiagramm zur Mittelbaren Biometrie"

Die App erzeugt zunächst in der gehärteten CORONIC Software Umgebung „B“ (DataSafe) ein Schlüsselpaar „1“ (DS). Das ist gebunden an die Gerätehardware des Handys, den Nutzer und dessen Konto (Alias/Anmeldename). Dann meldet sich die App beim TrustedOS und lässt dort zwei weitere unabhängige Schlüsselpaare erzeugen. Das eine Schlüsselpaar „2“ (BIO) ist konnotiert mit der Biometrie des Nutzers, dem biometrischen Datum des Nutzers und dem Konto. Das zweite Schlüsselpaar „3“ (HW) ist konnotiert mit der Hardware des TrustedOS und dem Konto. Die Mehrfachbenutzung unterschiedlicher gesicherter Ausführungsumgebungen (TrustedOS und Datasafe) wird später noch wichtig, weil wir so verschiedene PSD2-Faktoren in verschiedenen Ausführungsumgebungen gleichzeitig verfügbar machen. Es ist keine zweite App und kein zweites Gerät notwendig, denn die RTS-Bedingungen der Kanaltrennung sind erfüllt und auch die Möglichkeit „mit einem Hack beide Faktoren auszuhebeln“ ist nicht gegeben, da die eine Ausführungsumgebung Hardware-basiert ist und die andere Software-basiert.

An die Bank zurückgeliefert werden jetzt drei öffentliche Schlüssel (BIO, HW, DS) sowie die zugehörigen Credentials (PIN, Alias bzw. „Kontonummer“). Auf Bankseite findet eine Persistenzprüfung und die Kontrolle der PIN statt. Über einen zweiten, unabhängigen Weg wird dann ein Freischaltcode an den Kunden gesendet. Dieser Weg kann ein Brief sein, kann aber auch jedes beliebige vorher existente Altverfahren sein (zum Beispiel ein TAN-Prozess). Der Freischaltcode wird an drei unterschiedlichen Stellen (DS, BIO, HW) dreimal in zwei unterschiedlichen Ausführungsumgebungen (DS, TrustedOS) mit drei PSD2-Faktoren (Besitz-TrustedOS, Biometrie, Besitz-DS) signiert. Der signierte Freischaltcode kehrt zurück zur Bank. Diese

kann drei Signaturprüfungen durchführen und kennt damit drei zusätzliche PSD2-Faktoren, die der Kunde künftig nutzen kann. Will man weiter die PIN verwenden, stünde mit „Wissen“ noch ein vierter Faktor zur Verfügung. Wirklich brauchen würde man ihn aber nicht, denn schon zwei Faktoren reichen für eine starke Kundenauthentifizierung. Dieser Prozess wurde von SRC in Bonn geprüft und hat die volle und uneingeschränkte Konformitätsfreigabe für alle drei eingesetzten Faktoren bekommen.

> *„Wir kennen die Firma CORONIC als technischen Dienstleister für Banken und Zahlungsverkehr und haben ihre Konzepte aus dem Biometrie-Bereich auf rechtliche Konformität hin überprüft. Das Unternehmen hat hier eine elegante technische Lösung präsentiert.“*
>
> Sandro Amendola, SRC GmbH

Interessanterweise ist dieses Konzept ausbaufähig. Sobald die großen US-Konzerne nicht nur Spracherkennung, sondern auch Stimmerkennung auf ihren Smartgeräten im Angebot haben, steht ein fünfter PSD2-konformer Faktor zur Verfügung. Schon heute umsetzbar ist eine Variante mit Verhaltenserkennung (sechster Faktor). Auch an eine Unterschrift, die der Kunde direkt auf dem Smartphone durch Fingerwischen erzeugt, ließe sich als zusätzliches Inhärenzmerkmal etablieren (sieben). Wir haben an dieser Stelle absichtlich zwei gegensätzliche Verhaltensmerkmale benannt. Während „die Art, wie der Kunde das Smartphone bedient und hält“ im Hintergrund überprüft werden kann, ist „das Abverlangen einer Finger-Unterschrift“ ein aktiver Prozess. Er verlangt dem Nutzer Aufmerksamkeit ab und bietet damit eine höhere gefühlte Sicherheit für den Kunden. Diese beiden Verhaltensmerkmale stehen sich im Prinzip genauso gegenüber wie Besitz und Biometrie. Besitz kann still und leise im Hintergrund kontrolliert werden, Biometrie erfordert ein aktives Handeln des Nutzers. Damit stünden sieben PSD2-Faktoren in zwei unterschiedlichen Ausführungsumgebungen zu Verfügung. Die Vielfalt und Unterschiedlichkeit der Faktoren kann im Fraudsystem der Bank benutzt werden, um unterschiedliche Risiken oder Überweisungshöhen abzubilden. Im Zweifel können mehrere Faktoren, zusätzliche Faktoren oder einzelne Faktoren doppelt erhoben werden, um im Nutzerkontext mehr Sicherheit zu generieren.

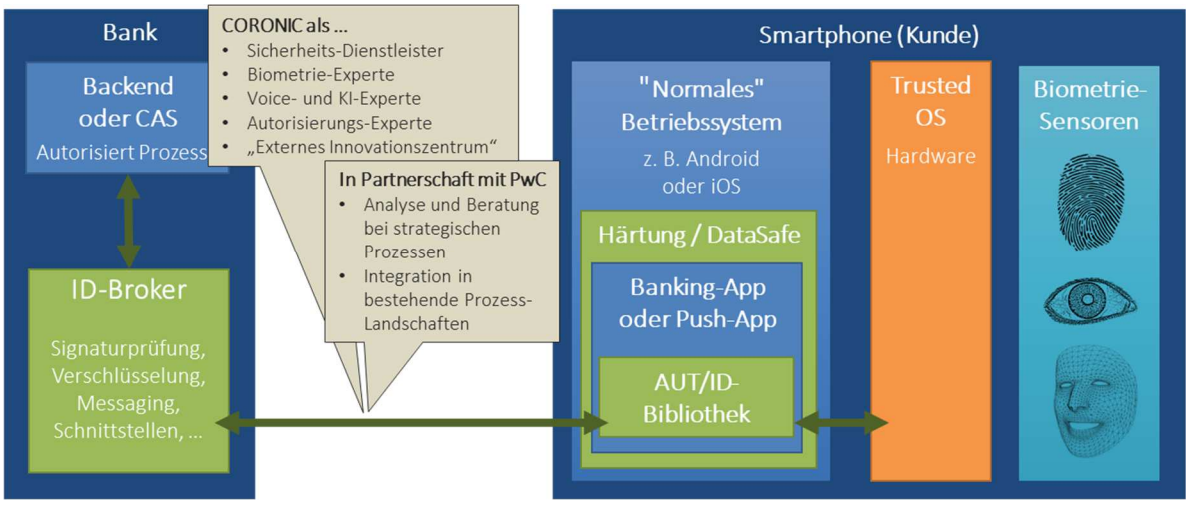


Abbildung 8 "Upgrade einer Bestands-App durch CORONIC ID-Bibliothek"

Abbildung 8 zeigt, wie die Biometriefunktionen und die DataSafe-Technologie in Bestandsanwendungen, wie die Push-App oder die Banking-App integriert werden können. Damit stehen auch „Altfaktoren“ auf Basis von TAN-Nachrichten weiter zur Verfügung.

Der Freischaltprozess ist natürlich nur einer von vielen Prozessen, die die Banken auf Basis der neuen gesetzlichen Regelungen alle durchdeklinieren müssen. Es geht weiter mit …

> Gerätemigration mit Migrationscode (QR oder Text)
> Gerätemigration ohne Migrationscode (NFC)
> Login ohne PIN
> Login mit PIN
> Transaktionsautorisierung ohne TAN
> Transaktionsautorisierung mit TAN
> Gerätedeaktivierung
> Mehrfachbetrieb von Geräten

… aber das würde den Rahmen des Dokumentes sicher sprengen.

An dieser Stelle noch ein Hinweis für die nicht ganz so Technik-Verliebten: dargestellt wurden die technischen und regulatorikkonformen Möglichkeiten der Mittelbaren Biometrie. Auch wenn man jetzt Login und Überweisung in einer App machen darf, heißt das nicht, dass Sie das in Ihrer Bank tun müssen. Wie Sie die gegebenen Möglichkeiten verwenden, die Sicherheitslage bewerten oder aber konkrete Umsetzungen für Ihre Kundenprodukte planen, bleibt natürlich Ihnen überlassen.

3.2.2 Maximale Nutzung der Mittelbaren Biometrie

Im Prinzip ist bezüglich der Technologie und der Konformität alles gesagt worden. Aber wenn man jetzt seiner Fantasie freien Lauf lässt, lassen sich folgende Aussagen treffen:

> Biometrie- und Besitz-Banking verbessert die Usability und kann andere Faktoren im Banking ersetzen
> Biometrie- und Besitz können als zusätzlicher Faktor die Sicherheit im Banking verbessern (Fraud-Analyse)
> Biometrie- und Besitz-Apps können zusätzlich die „alten Faktoren“ Wissen (PIN) und Besitz (TAN) integrieren
> Damit ist Konto-Login in der Banking-App ohne die 90-Tage-TAN möglich
> Bei Überweisungen in der Banking-App kann das Abtippen der TAN durch den Fingerabdruck in der Biometrie-App (oder push-App) ersetzt werden
> Bei Online-Überweisung im Browser kann das Abtippen der TAN durch den Fingerabdruck in der Biometrie-App ersetzt werden
> Am PC-Client können Besitz und Biometrie die push-App oder die Chipkarte samt Lesegerät ersetzen
> Die Kombination "Besitz plus Biometrie" kann prinzipiell immer wie "PIN plus Chipkarte" agieren
> Login und Überweisung kann immer in einer App erfolgen

> Die nicht ganz so Mutigen können auch schrittweise erst auf die TAN, dann auf die PIN und erst ganz zum Schluss auf die Chipkarte verzichten
> Letzteres geht auch am Geldautomaten!
> Das Vorgehen ist technologisch offen für neue Faktoren und kann sich so stets den veränderten Gegebenheiten im Nutzerverhalten und der Sicherheitslage anpassen
> Wenn Sie Ihre verifizierten Kunden-Identitäten eIDAS-zertifizieren lassen, können Sie mit der Mittelbaren Biometrie-App rechtsgültige Unterschriften unter Verträge setzen (Versicherungsvertrag, Kaufvertrag, Kraftfahrzeug, …)
> Letzteres befähigt Ihre Kunden überall Verträge auf dem eigenen Smartphone zu unterschreiben (oder auch im Browser)

Richtig interessant wird das Ganze aber erst dann, wenn das Speichern der PIN in push-App, Banking App oder PC-Client tatsächlich verboten wird. Dann verlieren alle Altverfahren den Wissensfaktor und haben keinen als Ersatz in petto – das kann Besitz und Biometrie nicht passieren.

3.3 PSD2-Browser – Online-Banking ohne TAN

Bevor wir die Zukunft allzu rosig färben, müssen wir noch mal einen Schritt zurückgehen (die Pessimisten werden sich freuen): was ist mit den Kunden, die kein Smartphone haben oder kein Smartphone wollen oder ein Smartphone haben, aber ohne Biometriesensoren? Da gibt‘s nur zwei Möglichkeiten: entweder sie bleiben bei den Altverfahren oder aber man findet eine Möglichkeit die neuen Verfahren am Desktop nutzbar zu machen. Der Desktop ist schon deswegen ein interessantes Objekt, weil bei den meisten Banken zwar das Gros der Kunden mobil ist („ist mein Geld noch da“) aber immer noch am Desktop seine Überweisung macht („finde ich sicherer und übersichtlicher“). Wir brauchen also eine starke Kundenauthentifizierung am Desktop und im Prinzip ist sie im Abschnitt 3.2.1 bereits beschrieben worden: Das CORONIC Security Framework, die gehärtete Systemumgebung (DataSafe), die in Abbildung 7 zur Nutzung des zusätzlichen Besitzfaktors im Konformitätsbericht eingesetzt wurde, steht auch für Desktopsysteme (Windows und Macintosh) zur Verfügung. Man braucht auf dem Desktop nur eine eigene App, die auch über einen gehärteten DataSafe verfügt, und die gleiche Geschichte kann noch einmal erzählt werden. Dazu bietet sich ein Bank-Browser mit Besitzmerkmal an, den wir in dieser Kapitelüberschrift erst einmal als „PSD2-Browser“ bezeichnet haben.

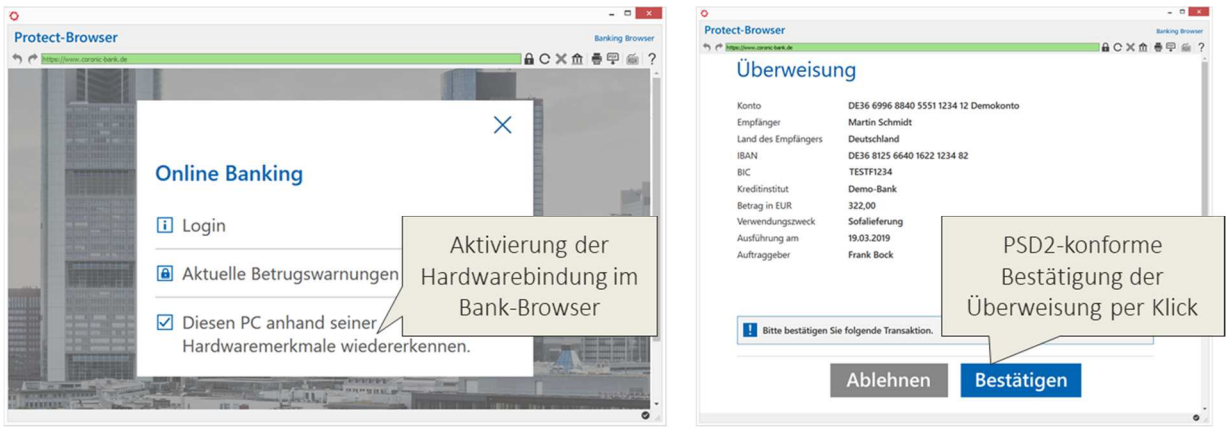


Abbildung 9 "Der PSD2-Browser am Desktop: Banking ohne TAN"

Das Ganze sieht dann so aus, dass der Kunde beim Login im Online-Banking (ähnlich wie bei der Anmeldung bei Amazon) einen zusätzlichen Haken vorfindet, mit dem er die Hardwarebindung im Browser aktivieren kann. Dazu wird ein Freigabeprozess durchlaufen, in dem analog zu den obigen Ausführungen mithilfe einer TAN das Besitzmerkmal am PC verankert wird. Danach ist dieses neue PSD2-Merkmal im Browser nutzbar. Der Besitz-Faktor kann dann sowohl die 90-Tage-Login-TAN im Browser-Banking ersetzen als auch für Überweisungen ganz ohne TAN-Eingabe genutzt werden.

Da die neueren Macbooks und Windows Laptops inzwischen mit Biometriesensoren und Kameras ausgerüstet sind, lassen sich auch biometrische Merkmale auf den PC übertragen. Bei Windows 10 unterstützt an dieser Stelle die Hello API (falls eine Webcam vorhanden ist), die eine Faktor-taugliche Gesichtserkennung anbieten kann, ähnlich wie das iPhoneX.

3.4 Der PC-Client mit Besitzmerkmal

Nachdem wir jetzt im Geiste schon ein Besitzmerkmal auf dem PC verankert haben, ist der nächste Schritt nur noch eine Kleinigkeit. Gerade die im Geschäftskundenbereich häufig eingesetzten Kundenprodukte über FinTS oder HBCI können um ein softwarebasiertes Besitzmerkmal auf Basis einer gehärteten Ausführungsumgebung ergänzt werden. Dazu ließe sich entweder die gesamte Banking-Software am PC härten oder aber eine zusätzliche zweite gesicherte PC-App aufspielen. Diese kann dann sowohl das Besitzmerkmal verankern, als auch die sichere Visualisierung im Überweisungsprozess gewährleisten. Damit kann auf die Nutzung von Secodern oder Chipkartenlesegeräten am PC durch den Besitzfaktor verzichtet werden. Das erhöht die Usability im Geschäftskundenumfeld nachhaltig. Am besten nachvollziehen kann das, wer schon mal bei einem Auftrag mit mehreren Sammlern 20-, 40- oder 60-mal am Kartenleser auf „OK“ klicken musste.

4 Mehrwertdienste und Marktchancen

Dies ist nun ausschließlich ein Abschnitt für die Optimisten. Die Pessimisten lassen ja kein gutes Haar an der Regulatorik und der PSD2. Für uns Optimisten ist das anders, in den Änderungen und Vorschriften stecken auch Chancen und Mehrwerte, man muss sie nur finden und zu nutzen wissen.

4.1 Usability über alles

Die Mehrwerte liegen in diesem Fall auch ganz offen auf der Hand: der richtige und strukturierte Einsatz der neuen Faktoren für eine starke Kundenauthentifizierung führt zu einem enormen Gewinn in der Usability. Die Bedienung wird einfacher, schlanker, schneller und vor allem weniger fehleranfällig. Das freut ganz besonders die Kollegen im Kunden-Servicecenter oder im IT-Support, bei denen sich immer noch ein großer Teil der Anfragen aus „Sidekicks der TAN-Nutzung“ speist: „ich habe mein Konto gesperrt“, „ich habe die richtige TAN eingegeben und trotzdem funktioniert es nicht“, „ich habe ein neues Handy gekauft“, „können Sie meinen Account wieder freischalten“. Für viele von uns ist das ein unangenehmer (aber leider großer) Teil ihres Alltags. Über die bisweilen wirklich extrem umständlichen Prozesse beim Gerätewechsel (neues Handy) möchte ich hier gar nicht sprechen. Heute ist es fast der Standard, dass

man sich beim Neueinrichten einer Push-App die Finger bricht. Von den folgenden Aufwänden im IT-Support mal ganz zu schweigen. Bisher musste es so kompliziert sein, sagte zumindest die Security, aber jetzt gibt es die Möglichkeit die Authentifizierung eleganter, bequemer und weniger fehleranfällig zu gestalten.

Ich möchte hier noch einmal für eine große Vereinheitlichung der Überweisung die Lanze brechen. Stellen Sie sich eine Welt vor, in der sich alle mit Besitz anmelden und mit Biometrie überweisen (oder andersherum). Wir hätten eine einheitliche Art des Umgangs über alle Banken hinweg. Die Kunden würden wirklich wissen, was genau passiert und hätten nicht bei jeder Bank und jedem Anbieter ein anderes Verfahren zu erlernen. Diese starke Heterogenität führt übrigens auch dazu, dass der Kunde immer genau das macht, was ihm die Nutzeroberfläche sagt und dahinter steckt nicht selten ein Phisher. Da auch die großen IT-Konzerne in Richtung Biometrie zielen, bietet sich tatsächlich die Chance, einen einheitlichen Zugang zum Konto und einen einheitlichen Transfer von Geld zu gestalten - zumindest was die Prozessführung aus Benutzersicht angeht. Kurz und gut, wir werden die typischen Fallstricke von „ich habe meine PIN Nummer vergessen“, „ich kenne meinen Alias nicht mehr“, „wo finde ich denn meine Kennung“ oder „wie war noch mein Anmeldename“ alle los, denn das Smartphone, das eigene Gesicht und den eigenen Finger hat der Kunde stets dabei.

4.2 Struktur- und Kosteneffizienz

Neben diesen an der Usability orientierten Argumenten gibt es natürlich auch noch die strukturellen Vorteile, die sich für unsere Aufbauorganisation ergeben. Eine Zentralisierung der ID-Systeme ist natürlich erst einmal ein großer Aufwand für alle Kundenprodukte. Danach werden die Dinge aber nicht mehr N-Mal in jedem Produkt gemacht, sondern nur noch 1-mal an zentraler Stelle:

> Das ist klassisches Einsparpotenzial in den Prozessen und beim Personal
> Die Zahl der Umsetzungsfehler wird stark reduziert (man sollte Software sowieso nur einmal schreiben)
> Der wichtigste Punkt ist die erhöhte Geschwindigkeit: schneller neue Faktoren implementieren, schneller am Markt sein, all das ist mit einem zentralisierten ID-System deutlich besser zu erreichen
> Neue Marktoptionen und Geschäftsmodelle für Banken durch verifizierte Identitäten (und einmal weniger die Sorge nur noch Infrastrukturanbieter für Dritte zu sein)

Und als letztes noch ein kleiner Hinweis für diejenigen, die von den Support-Aufwänden bei der Gerätemigration betroffen sind: nichts kann schlimmer sein als ein neues Handy, wenn es darum geht eine Push-App vom alten Handy auf das neue Handy zu übertragen. Auch hier obsiegen Biometrie und Besitz, denn sie haben automatisch zwei Faktoren, um diesen Übergang direkt „von Gerät zu Gerät“ durchzuführen - ohne dass man Prozesse im Backend der Bank dafür anpassen muss.

4.3 Beispielrechnungen

Aber auch für die Kaufleute unter uns, die gerne zuerst auf messbare Zahlen schauen, gibt es Rechnungen, die jeden freuen:

> Was kostet die Neuausstattung des Kunden mit TAN-Generatoren?
> Was kostet die Karten-Grundausstattung, die alle paar Jahre auf uns zukommt?

Oder wer lieber „kleinere“ Zahlen mag …

> Viermal im Jahr die 90-Tage-Login-TAN kostet zwischen 8 und 20 Cent (je nachdem, ob man push oder SMS verwendet) und es gibt 50 Millionen Bankkunden in Deutschland.
> Das gleiche Rechenbeispiel auch noch einmal für die Überweisung: wir überweisen 2 bis 4 Mal pro Monat, an zwölf Monaten, das sind dann zwischen 0,75 € (push) und 1,75 € (SMS) pro Jahr. Multiplizieren Sie das mit der Zahl Ihrer Online-Kunden und Sie wissen, wie groß die „kleinen“ Einspareffekte sind.

Die beiden letzten Rechenbeispiele funktionieren natürlich sowohl beim Einsatz von Biometrie in der App, wie auch beim Einsatz von Besitz im Browser. Natürlich auch bei Besitz in der App oder Biometrie am PC – also eigentlich immer.

Denken Sie auch noch einmal daran, dass wir über die Biometrie eine Art Eingangsbestätigung für an den Kunden versendete Dokumente erzeugen können. Zur Not auch im Range einer rechtlich bindenden Unterschrift.

> Wie viele Kunden und Kontoinformationen gehen bei Ihnen im Hause noch per Post an den Endkunden, weil die Juristen den Postweg als zwingend empfinden?
> Wie viele AGB-Änderungen oder Anpassungen des Kontomodells werden immer noch per Briefpost versendet, obwohl wir eine einfache Möglichkeit hätten die Dokumente auszuliefern und den Empfang zu bestätigen?

4.4 Ein kurzes Fazit

All das sind interessanterweise Einspareffekte, wie sie sich zwangsläufig aus dem Abschnitt 2.3.2 „Unser Zielbild“ ergeben. Dort hatten wir gesagt, wir wollen keine extra Geräte, sondern nur noch Software und Smarthardware, die der Kunde sowieso nutzt und wir wollen das Ganze bitte kostenneutral. Alle genannten Kosteneinsparungen sind schlicht und ergreifend das Resultat dieser guten Zielformulierung … und deren sinnvoller Umsetzung.