# Ich sehe was, das du nicht siehst

## Die Realität von Mobilebanking zwischen allgemeinen und rechtlichen Anforderungen

Vincent Haupert[1], Gaston Pugliese[2]

**Abstract:** Kürzlich hat die Europäische Kommission die Technischen Regulierungsstandards im Rahmen der Zahlungsdiensterichtlinie II vorgelegt. Sie regeln unter anderem auch die Anforderungen an die starke Kundenauthentifizierung, die für digitale Zahlungsvorgänge zumindest eine Zwei-Faktor-Authentifizierung vorschreiben.

Der Beitrag setzt sich mit den rechtlichen Vorgaben auseinander, indem zunächst allgemeine Anforderungen formuliert werden, ehe darauf eingegangen wird, ob und wie Transaktionen auf nur einem mobilen Endgerät diesen Anforderungen genügen können. Hierbei wird die Transaktionssicherheit der Ein-Gerät-Authentifizierung anhand von smsTAN- und App-basierten Mobilebankingverfahren mittels allgemeiner wie auch rechtlicher Anforderungen bewertet. Es zeigt sich, dass die vorherrschenden Plattformen Android und iOS die Anforderung an ein unkopierbares Besitzelement bereits heute erfüllen können, während eine sichere Anzeige weiter eine Zukunftsaufgabe bleibt, gerade auch, weil der Gesetzgeber klare Anforderungen versäumt hat.

**Keywords:** Mobilebanking; Onlinebanking; Compliance; PSD2; RTS; Trusted Path; Secure Display

## 1 Einleitung

Die Europäische Bankenaufsicht (EBA) hat im Rahmen ihres Mandats zur Ausarbeitung der Technischen Regulierungsstandards (RTS) der Zahlungsdiensterichtlinie II (PSD2) auf ihr Diskussionspapier einen Rekord von 224 Rückmeldungen zu vermelden [EBA17]. Schon allein die Tatsache, dass ein Regulierungsvorhaben der EBA noch nie so viel Resonanz erzeugt hat, zeigt bereits die Tragweite der im Januar 2018 in Kraft getretenen Richtlinie.

Besonders kontrovers wurden die Anforderungen an die starke Kundenauthentifizierung diskutiert, die auch Einfluss darauf haben, welche Legitimierungsverfahren die Banken zukünftig noch einsetzen dürfen, bzw. welche Anforderungen an neue Verfahren zu stellen sind. Daraus ergeben sich auch unmittelbare Auswirkungen auf die Kunden, da diese unter Umständen nicht nur ihre Legitimierungsverfahren wechseln, sondern auch Verhaltensweisen ändern müssen. Bis vor Kurzem war vor allem unklar, ob die bereits verfügbaren App-basierten Mobilebankinglösungen der Kreditinstitute mit dem Inkrafttreten der RTS noch konform wären, haben die Institute in den vergangenen Jahren doch beträchtliche Ressourcen in deren Entwicklung und Vermarktung investiert.

Lehrstuhl für Informatik 1 (IT-Sicherheitsinfrastrukturen), Department Informatik, Technische Fakultät, Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Martensstraße 3, 91058 Erlangen, Deutschland
[1] vincent.haupert@cs.fau.de
[2] gaston.pugliese@cs.fau.de

doi:10.18420/sicherheit2018_13

Mobilebanking meint im Unterschied zum Onlinebanking, dass Transaktionen von ein und demselben mobilen Endgerät durchgeführt werden können. Ein solches Vorgehen stellt im Vergleich zu allen bisherigen Legitimierungsverfahren im Onlinebanking einen Bruch dar, da sie eine physikalische Trennung der Authentifizierungselemente immer als inhärentes Sicherheitsmerkmal verstanden haben. Mit dem Aufkommen von Smartphones haben sich die Voraussetzungen scheinbar geändert, da nahezu jede Bank von Rang und Namen ein Verfahren zum Mobilebanking anbietet.

Obwohl auch die finale Fassung der Europäischen Kommission [COM17] vom 27. November 2017 einigen Interpretationspielraum lässt, kann sie als Entscheidung zugunsten des Status Quo und somit auch der Banken gewertet werden. Der vorliegende Beitrag setzt sich mit den finalen Voraussetzungen an die starke Kundenauthentifizierung auseinander. Hierzu werden zunächst allgemeine Voraussetzungen an die Sicherheit von digitalen Transaktionen formuliert, um im nächsten Abschnitt die Anforderungen der RTS zu skizzieren. An diesen allgemeinen und rechtlichen Anforderungen werden dann SMS- und App-basierte Mobilebankingansätze jeweils gemessen. Den Abschluss bildet ein Ausblick darauf, wie digitale Transaktionen zukünftig über nur ein Smartphone sicher abgewickelt werden können, sowie eine Zusammenfassung unserer Ergebnisse.

## 2 Allgemeine Anforderungen an die Sicherheit digitaler Transaktionen

In diesem Abschnitt sollen allgemeine Anforderungen formuliert werden, die die Sicherheit digitaler Transaktionen aus Nutzersicht beschreiben. Der Begriff *digitale Transaktion* abstrahiert ganz bewusst von den geläufigen Bezeichnungen *Onlinebanking* und *Mobilebanking* und meint jedwede Aktion, die über einen digitalen Kanal abgewickelt wird und eine Zustandsüberführung herbeiführt. Es sei darauf hingewiesen, dass dies auch Aktionen abseits des prototypischen Beispiels der elektronischen Überweisung einschließt, insofern sie Änderungen an den Kernattributen des Kontos herbeiführen.

Für die Sicherheit von digitalen Transaktionen sind die beiden folgenden Eigenschaften maßgeblich:

1. Eine digitale Transaktion wird nur genau dann durchgeführt, wenn sie vom Nutzer willentlich ausgeführt wurde.
2. Eine vom Nutzer willentlich ausgeführte digitale Transaktion ist manipulationsfrei.

Hierbei fordert 1, dass ein Zugriff auf die am Transaktionsprozess beteiligten Authentifizierungselemente nicht, bzw. nur in solch einer Art und Weise durch unautorisierte Dritte möglich ist, dass keine digitalen Transaktionen durchgeführt werden können. Weiter fordert 2, dass auch dann, wenn ein unautorisierter Dritter keinen direkten Zugriff auf die Authentifizierungselemente im Sinne von 1 erlangen kann, es ihm nicht möglich ist, eine Transaktion für den Nutzer transparent zu manipulieren. Aus dieser Anforderung folgt auch, dass zumindest eines der am digitalen Transaktionsprozess beteiligten Geräte über einen *Trusted Path* verfügt. Hiermit ist ein geschützter, vertrauenswürdiger Kanal gemeint, der

zumindest Authentizität bzgl. der zum Zwecke der Durchführung der digitalen Transaktion ein- und ausgegebenen Daten garantiert, sodass eine sichere Verifikation und Bestätigung durch den Nutzer möglich ist [WW17; Zh12].

## 3 Rechtliche Anforderungen an die Sicherheit digitaler Transaktionen

Dieser Abschnitt beschäftigt sich mit den Technischen Regulierungsstandards (RTS) der Europäischen Kommission vom 27. November 2017 [COM17], die auf dem Standardentwurf der EBA vom 23. Februar 2017 [EBA17] beruhen. Insofern es binnen drei Monaten seitens des Europäischen Parlaments oder des Rats keine Einwände gibt, tritt die Verordnung mit der Veröffentlichung im Amtsblatt der Europäischen Union in Kraft, gilt jedoch erst 18 Monate später.

### 3.1 Anforderungen an die Authentifizierungselemente

Die PSD2 fordert ganz allgemein, dass die Authentifizierung zumindest zwei Elemente aus den Kategorien Wissen, Besitz und Inhärenz umfasst. Die Anforderungen an die einzelnen Elemente sind weitgehend intuitiv: So sollten Maßnahmen ergriffen werden, die dem Risiko, dass ein unautorisierter Dritter das Wissenselement in Erfahrung bringt oder das Besitzelement replizieren kann, nach Möglichkeit vollumfänglich entgegenwirken. Ebenso muss es vermieden werden, dass ein als Inhärenz kategorisiertes Authentifizierungselement in unautorisierte Hände gelangt. Im Unterschied zu Wissens- und Besitzelementen ist das Anwenden eines inhärenten Authentifizierungselements regelmäßig mit einem heuristischen Prozess verbunden, der durch eine gewisse Fehlerrate charakterisiert wird. Folgerichtig ist diese Fehlerrate zumindest auf einem sehr niedrigen Niveau zu halten. Ferner sollen die Hard- und Software des entsprechenden Geräts auch sicherstellen, dass ein Inhärenzelement nicht unrechtmäßig verwendet werden kann.

### 3.2 Authentifizierungscode, dynamische Verknüpfung und Unabhängigkeit

Neben den Bedingungen an die einzelnen Elemente setzen die RTS auch noch einen Authentifizierungscode, eine dynamische Verknüpfung, sowie die Unabhängigkeit der Elemente voraus. Der Authentifizierungscode ist dabei mit einer Transaktionsnummer (TAN), wie sie seit jeher aus dem Onlinebanking bekannt ist, vergleichbar. Im Zusammenspiel mit der dynamischen Verknüpfung muss der Authentifizierungscode zumindest in Abhängigkeit zu Empfänger und Betrag einer Transaktion stehen. Die Anforderung an die dynamische Verknüpfung der Transaktion geht aber noch weiter: Nicht nur müssen dem Zahlungsauslöser zu jeder Phase des Transaktionsprozesses Empfänger und Betrag sichtbar gemacht werden, sondern es müssen auch solche Sicherheitsmaßnahmen ergriffen werden, die dafür Sorge tragen, dass die Vertraulichkeit, Authentizität und Integrität der angezeigten Transaktionsdaten nicht verletzt wird.

Schlussendlich soll die Unabhängigkeit der Elemente sicherstellen, dass die Kompromittierung eines der Authentifizierungselemente nicht auch die Kompromittierung eines oder mehrerer der anderen Elemente nach sich zieht. Zu diesem Zweck sollen Authentifizierungselemente, wann immer sie durch ein Mehrzweckgerät realisiert werden, in getrennten sicheren Ausführungsumgebungen durch Softwaremaßnahmen gekapselt werden. Ferner sollen Maßnahmen ergriffen werden, die sicherstellen, dass keine Software- oder Gerätemodifikationen stattgefunden haben, weder durch unautorisierte Dritte, noch durch den Nutzer selbst. Werden Modifikationen festgestellt, dann sollen die daraus resultierenden Konsequenzen eingedämmt werden.

### 3.3 Vergleich zu den allgemeinen Anforderungen

Im Unterschied zu unseren allgemeinen Anforderungen, sind die soeben geschilderten rechtlichen Voraussetzungen deutlich spezifischer. Auch fordert die PSD2 explizit eine Mehr-, jedoch mindestens eine Zwei-Faktor-Authentifizierung. Obwohl diese Vorgabe aus Sicht der IT-Sicherheit zweifelsohne sinnvoll ist, folgt sie aus unseren Anforderungen nicht zwangsläufig, insofern beide Bedingungen erfüllt sind.

Dennoch lassen sich die Anforderungen durch die PSD2, bzw. die ihr zugehörigen RTS, jeweils unseren allgemeinen Voraussetzungen an die Sicherheit zuordnen. So entsprechen die Anforderungen an die Authentifizierungselemente, den Authentifizierungscode und die Unabhängigkeit weitgehend unserer Vorgabe, dass die Elemente durch einen unautorisierten Dritten nicht zugreifbar sein dürfen. Die Anforderung an die dynamische Verknüpfung der Transaktion geht sogar noch weiter als unsere Forderung nach Manipulationsfreiheit. Während wir nur einen Trusted Path voraussetzen, damit dem Zahler eine lückenlose Transaktionsverifikation möglich ist, fordert die PSD2 neben Authentizität auch Integrität und Vertraulichkeit. In unserer Anforderung kommt die Integrität nicht vor, da diese vom Nutzer zu prüfen ist. Einzige Voraussetzung ist, dass ein Nutzer auch genau das bestätigt bzw. nicht bestätigt, was ihm dargestellt wird. Obwohl Vertraulichkeit zweifelsfrei ein erstrebenswertes Gut ist, das in der Praxis stets gewahrt werden sollte, spielt sie für die technische Transaktionssicherheit eine untergeordnete Rolle.

## 4 Bewertung von SMS- und App-basierten Mobilebankingverfahren

Nachdem die allgemeinen sowie rechtlichen Anforderungen geklärt sind, setzen wir uns im Folgenden damit auseinander, ob diese in der Praxis des Mobilebankings eingehalten werden können. Wie eingangs beschrieben, sind mit Mobilebanking Transaktionen gemeint, die auf nur einem Gerät stattfinden. In der Realität moderner Smartphones qualifizieren sich unter den gebräuchlichen Legitimierungsverfahren nur das smsTAN- sowie App-basierte Verfahren, die laut einer repräsentativen Umfrage aus dem Jahre 2016 von 36% bzw. 5 – 8%[3]

[3] Die Spannweite resultiert aus der separat erfassten Verwendung des photoTAN-Verfahrens. Das photoTAN-Verfahren wird sowohl als dediziertes Gerät als auch als App-basiertes Verfahren angeboten. Die Studie gibt jedoch keinen genaueren Aufschluss darüber, welche Anteile auf welche Ausprägung entfallen. Die Hardwarevariante wäre ihren Eigenschaften nach eher dem chipTAN-Verfahren zuzuordnen.

der Bevölkerung verwendet werden [NB16]. Der Rest entfällt auf das chipTAN- bzw. iTAN-Verfahren, die beide jedoch nicht durch ein einziges Gerät abgebildet werden.

### 4.1 Angreifermodell

Obwohl gerade die allgemeinen Anforderungen hinreichende und notwendige Bedingungen für die theoretische Sicherheit von Transaktionen sind, können sie in der Praxis der Transaktionssicherheit digitaler Bankgeschäfte nur durch ein entsprechendes Angreifermodell bewertet werden. Die Schwierigkeit besteht darin, ein solches Angreifermodell zu wählen, das die in der Wirklichkeit herrschenden Umstände möglichst gut widerspiegelt [HHF17]. Zu diesem Zweck stellen wir die folgenden Bedingungen an das Angreifermodell, die unseren formalen Anforderungen gegenübergestellt werden:

1. Ein Angreifer hat keinen physischen Zugriff auf die Authentifizierungselemente.
2. Der Nutzer kommt seiner Sorgfaltspflicht nach, sodass der digitale Transaktionsprozess von seiner Seite regelkonform erfolgt.
3. Der Angriff enthält zumindest eine technische Komponente, basiert also nicht ausschließlich auf der Täuschung des Nutzers im Sinne von *Social Engineering*.

Im Folgenden wird ferner davon ausgegangen, dass die Transaktionsauslösung und -bestätigung auf ein und demselben Smartphone stattfindet. Hierbei wird ein System der beiden vorherrschenden Plattformen Android und iOS angenommen. Die Transaktionsauslösung kann dabei entweder aus dem Browser oder einer eigenen Banking-App erfolgen. Während dieser Vorgang für das smsTAN-Verfahren zwingend ist, muss die Bestätigung der Transaktion nicht zwangsläufig durch eine separate App erfolgen, sondern kann auch von derselben App durchgeführt werden, die bereits zur Transaktionsauslösung verwendet wurde.

### 4.2 Die smsTAN und die Geräteevolution

Beim smsTAN-Verfahren wird dem Nutzer eine TAN samt Empfänger und Betrag über den Mobilfunk zugestellt, die dann nach erfolgreicher Verifikation der Transaktionsdetails manuell in den transaktionsauslösenden Kanal zu übertragen ist. Als das smsTAN-Verfahren 2003 eingeführt wurde [DP03], waren die die SMS-empfangenden Geräte noch merklich in ihrer Funktionalität eingeschränkt, weshalb sie heute in der Vorherrschaft der Smartphones als Featurephones bezeichnet werden. Ihre primären Aufgaben waren das Telefonieren und das Senden und Empfangen von SMS. Beide Aufgabenfelder sind auf modernen Smartphones deutlich in den Hintergrund gerückt. Dennoch existiert die gleiche Funktionalität auch heute noch auf den mobilen Endgeräten und wird auch nach wie vor von einer SIM-Karte abgewickelt. Hierbei hat die sie tragende Hardware eine Veränderung weg von den Spezialgeräten der Featurephones, hin zu den Mehrzweckgeräten moderner Smartphones

vollzogen. Zu den wesentlichen Neuerungen von Smartphones zählen die quasi immer verfügbare Internetverbindung sowie ein Ökosystem aus verschiedenen Apps, die eine bestimmte Funktionalität bereitstellen.

Bei den Featurephones sorgte die fehlende Internetfähigkeit unter der Verwendung des smsTAN-Verfahrens noch implizit dafür, dass zwei unterschiedliche Geräte an der Transaktionsdurchführung beteiligt waren. Mit dem Aufkommen von Smartphones wurde diese implizite Gerätetrennung aufgehoben, weil es jetzt theoretisch möglich war, Transaktionen von ein und demselben Gerät durchzuführen. Es ist unmittelbar begreifbar, dass dieser Zustand zu einer Absenkung des Sicherheitsniveaus führte und man sich jetzt sogar wieder einem Bedrohungsszenario gegenübersah, das es mit der Einführung des smsTAN-Verfahrens gerade zu bekämpfen galt: nämlich die Infektion mit Schadsoftware [CT09]. Im Vergleich zum iTAN-Verfahren hatte sich die Situation sogar noch verschlechtert: Während die reine Infektion des Nutzercomputers nur dazu genutzt werden konnte, Transaktionen transparent zu manipulieren, war durch die Verwendung des smsTAN-Verfahrens auf einem Smartphone sogar das eigenständige Ausführen beliebiger Transaktionen durch entsprechende Schadsoftware zu beliebigen Zeitpunkten denkbar.

Dieser Umstand ist auch der Deutschen Kreditwirtschaft (DK) nicht verborgen geblieben. Die DK ist ein Interessensverbund eines Großteils der öffentlich-rechtlichen, genossenschaftlich und privat organisierten Banken. Auch die DK, damals noch als Zentraler Kreditausschuss bekannt, wollte dieser neuen Entwicklung Rechnung tragen und schrieb schon 2008 für die Verwendung des smsTAN-Verfahrens zwei Geräte vor [ZKA08]. Dies begründete sie damit, dass die Sicherheit von Transaktionen maßgeblich davon abhängt, dass „man sich der Technik der Übertragung über zwei unterschiedliche Kanäle“ bedient. Demnach müsse Mobilebanking mit dem smsTAN-Verfahren „in den Kundenbedingungen für das Online-Banking explizit ausgeschlossen“ werden [DK].

Diese Vorgabe führt dazu, dass den Kunden, die sich mit ihrem Smartphone über den Browser oder die Banking-App des Kreditinstituts anmelden, die Möglichkeit, Überweisungen zu tätigen, ausgeblendet wird, insofern sie das smsTAN-Verfahren bei einer Bank verwenden, die direkt oder indirekt in der DK organisiert ist. Obwohl diese Regelung zunächst sinnvoll und konsequent erscheint, stellt sich durch sie kein Sicherheitsgewinn, sondern nur ein Verlust an Benutzerfreundlichkeit ein. Dem Nutzer wird nämlich nicht untersagt, beispielsweise seinen Kontostand über den mobilen Browser oder die Banking-App zu überprüfen. Um Zugang zu diesem zu erhalten, muss der Kunde jedoch seine Zugangsdaten eingeben. Sollte das Handy durch eine entsprechende Schadsoftware infiziert sein, kann diese die Zugangsdaten mitschneiden. Der Angreifer unterliegt jedoch nicht den gleichen Restriktionen wie der Nutzer: Oft erkennt der Bankenserver anhand des User-Agents des Browsers oder durch ein bestimmtes Protokoll der Banking-App, dass sich der Nutzer über ein mobiles Endgerät Zugang zu seinem Konto verschafft. Eine Schadsoftware könnte nun ohne Weiteres z. B. den User-Agent seiner HTTP(S)-Anfragen so aussehen lassen, dass der Bankenserver den Nutzer an einem Desktop-Computer vermutet. In Folge wäre die Vorgabe, zwei Geräte zu verwenden, erfüllt und eine Transaktionsauslösung mit Bestätigung über das smsTAN-Verfahren wird möglich. Da sich die Schadsoftware aber in Wirklichkeit auf

dem Smartphone befindet, kommt die via SMS zugestellte TAN dennoch auf dem gleichen Endgerät an. Ein Angreifer kann somit beliebige Transaktionen tätigen, wenn es ihm gelingt, dass Gerät zu kompromittieren.

Gerade die rasant steigende Komplexität der ersten Smartphones sorgte auch für die ersten Schadensfälle [Dm14]. Die SIM-Karte, die letztendlich dafür verantwortlich ist, die SMS entgegenzunehmen, blieb uns jedoch bis heute erhalten und hat somit die Geräteentwicklung vom Spezial- zum Mehrzweckgerät ohne merkliche Änderungen auf Seiten des Geräts mitgemacht. Es ist zwar richtig, dass es in der Vergangenheit immer wieder erfolgreiche Angriffe auf die technische Infrastruktur der SMS gegeben hat [Mu13; Re16; RKH16; SZ17b] und dass sogar neuere Mobilfunkstandards nicht nur alte Sicherheitsprobleme schließen, sondern auch neue schaffen [Tu16]. Dennoch wurde die Sicherheit des smsTAN-Verfahrens gerade durch den Betrieb auf einem Mehrzweckgerät erodiert.

### 4.3 App-basierte Verfahren

Bei den App-basierten Methoden haben sich verschiedene Verfahren herausgebildet. Allen gemein ist jedoch, dass die für die Transaktionsverifikation benötigten Daten nicht direkt über den Mobilfunk, sondern über ein IP-basiertes Protokoll übertragen werden. Im Gegensatz zum smsTAN-Verfahren ist hierfür nicht zwangsläufig eine SIM-Karte notwendig, obwohl auch eine Abwicklung über das Internetangebot des Mobilfunkanbieters möglich ist. Für das App-basierte Verfahren ist dies jedoch transparent. Der Unterschied der einzelnen App-basierten Verfahren liegt in ihrer Ausprägung (eine oder zwei Apps) und ihres Rückkanals (online oder offline bzw. manuell). Obwohl die seit jeher herrschende Zwei-Faktor-Authentifizierung im Onlinebanking stets eine TAN beinhaltet hat, erwächst aus der Zahlenfolge per se kein Sicherheitsgewinn, da sie semantisch wertlos ist. Sie ist vielmehr ein Artefakt derer Verfahren, die keinen digitalen Rückkanal bieten. Aus diesem Grund fordern App-basierte Verfahren zunehmend nicht mehr, dass die TAN manuell in den transaktionsauslösenden Kanal übertragen wird, bzw. verzichten komplett auf eine für den Nutzer sichtbare TAN.

Der Blick in die Finanzbranche lässt erkennen, dass großes, in jedem Fall aber größeres, Vertrauen in die Sicherheit von Smartphones herrscht, als das bei stationäre Computer und Notebooks der Fall ist. Bis vor Kurzem wäre es noch undenkbar gewesen, alle am Transaktionsprozess beteiligten Authentifizierungselemente über ein und dasselbe Gerät abzubilden, ohne dass dem ein entscheidender Sprung in Sachen Hardware- und Softwaresicherheit vorangegangen wäre, der diesem einschneidenden Schritt Rechnung getragen hätte. Nichtsdestotrotz sind die hierbei entstandenen und entstehenden Verfahren mittlerweile allesamt so ausgelegt, dass sie auch für das Nutzungsszenario des Mobilebankings geeignet sind. Ruft man sich den vorhergehenden Abschnitt und die Aussage der DK bzgl. der Verwendung des smsTAN-Verfahrens auf nur einem Gerät in Erinnerung, überrascht dieses Vorgehen.

Ein genauerer Blick auf das smsTAN-Verfahren offenbart heute große Ähnlichkeiten zu App-basierten Verfahren, besonders zu solchen, die über zwei eigenständige Apps realisiert

sind. Dies ist darauf zurückzuführen, dass die Funktionalität, die die SMS darstellt, ebenfalls über eine App erfolgt. Die Unterschiede liegen vor allem bei den fehlenden Garantien bzgl. des Zustellwegs und bei der Tatsache, dass die SMS-empfangende App nicht von der zugehörigen Bank stammt. Obwohl es richtig ist, dass die App-basierten Verfahren der Kreditinstitute den Schutzzielen der Authentizität, Vertraulichkeit und Integrität besser Rechnung tragen, bleibt die für das smsTAN-Verfahren aufgestellte Argumentation der DK, dass Transaktionsauslösung und -bestätigung nicht auf einem Gerät erfolgen dürfen, gültig.

### 4.4 Bewertung

Im Kern lassen sich für sicheres Mobilebanking auf dem Smartphone in Bezugnahme auf unsere allgemeinen und die rechtlichen Anforderungen an die Transaktionssicherheit die folgenden notwendigen Voraussetzungen formulieren:

1. Das Besitzelement lässt sich unter praktischen Gesichtspunkten nicht replizieren, sodass eine autonome Inbetriebnahme ausgeschlossen ist.
2. Das Smartphone garantiert Verifizierbarkeit der Transaktionsdetails, sodass die dem Nutzer dargestellten Daten auch denen entsprechen, die der Bank vorliegen, sollte der Nutzer die Transaktion freigeben.

Nachdem unsere allgemeinen Voraussetzungen keine Vertraulichkeit vorschreiben, die Sicherheit eines Wissenselements, wie es im heutigen Mobilebanking üblich ist, jedoch ausschließlich auf Vertraulichkeit fußt, werden wissensbasierte Authentifizierungselemente als kompromittiert betrachtet. Da die RTS hier weiter gehen, unser Angreifermodell jedoch auch nicht-technische Angriffe erlaubt, insofern diese nicht ausschließlich vorkommen, kann auch im Rahmen der rechtlichen Voraussetzungen die Annahme getroffen werden, dass das Wissenselement – in der Regel Benutzername und Passwort – nicht mehr nur dem autorisierten Nutzer bekannt ist.

Im Bezug auf die in 1 geforderte Nichtkopierbarkeit des Besitzelements ergeben sich für die SMS- und App-basierten Verfahren unterschiedliche Situationen. Das smsTAN-Verfahren erfüllt diese Voraussetzung, weil die SIM-Karte letztendlich ein Mikroprozessor ist, dessen Replikation aus der Ferne ohne physikalischen Zugriff ausgeschlossen ist. Es ist zwar richtig, dass es in der Vergangenheit schon Situationen gegeben hat, in denen sich Kriminelle Zugriff auf eine Ersatzkarte des Nutzers verschaffen konnten, dies erfolgte jedoch fernab des Verantwortungsbereichs des Nutzers [SZ17a]. Die Nichtkopierbarkeit im Sinne von 1 bleibt hiervon unberührt.

Für App-basierte Verfahren kann keine derart pauschale Aussage getroffen werden, da die theoretischen Möglichkeiten zur Aufrechterhaltung von praktischer Nichtkopierbarkeit auf den aktuell eingesetzten Smartphones zwischen unmöglich, mäßig und vollständig reichen. Grundsätzlich ist die Ausgangssituation fundamental anders als bei einer SIM-Karte, welche bereits ab ihrer Entgegennahme personalisiert ist. Die App-basierten Legitimierungsverfahren müssen aber zuerst über einen Einrichtungsprozess personalisiert werden, da alle

Apps aus den offiziellen Bezugsquellen zunächst gleich sind. Die im Rahmen des Einrichtungsprozesses hinterlegten Daten werden oft lediglich in einem privaten, App-eigenen Verzeichnis abgelegt. Dieses Vorgehen zieht eine triviale Eins-zu-Eins-Kopierbarkeit nach sich: Werden die nach der Installation angelegten Daten kopiert und auf einem anderen Gerät wiederhergestellt, ergibt sich der gleiche Zustand auf dem Ziel- wie auf dem Quellgerät. Daraus folgt auch, dass die App auf dem Zielgerät in einem registrierten Zustand verwendet werden kann. Diese Situation versuchen die herausgebenden Banken freilich zu vermeiden, indem sie eine Gerätebindung einführen.

Um eine Gerätebindung herzustellen, kann die App zum Beispiel auf *Fingerprinting* zurückgreifen. Zu diesem Zweck liest die App während des ersten Starts – oder auch während des Registrierungsprozesses – verschiedene Umgebungswerte aus, die dann auch in den privaten App-Daten gespeichert werden. Diese Werte werden nun periodisch, z. B. beim Start der App, erneut abgerufen und mit den Werten verglichen, die zuvor gespeichert wurden. Weichen die Werte ab, schließt der Algorithmus zur Umsetzung der Gerätebindung unter Umständen darauf, dass die App-Instanz kopiert wurde. Die Schwierigkeit an diesem Vorgehen liegt daran, möglichst viele Werte zu verwenden, die sowohl einzigartig als auch stabil sind. Es hat sich gezeigt, dass die Hersteller hier einen eher defensiven Ansatz bevorzugen und nur wenige, dafür aber stabile und einzigartige, Werte verwenden [HM18]. Das führt aber auch dazu, dass sie durch statische und dynamische Analyse relativ leicht bestimmt werden können, um so die Gerätebindung zu umgehen.

Eine adäquate Variante Gerätebindung herzustellen, ist die Verwendung von speziellen Hardwarebausteinen in aktuellen Smartphones, mit denen asymmetrische Kryptographie möglich ist. Wichtig ist, dass die so erstellten privaten Schlüssel den gesicherten Bereich niemals verlassen. Auf diese Art kann selbst dann der private Schlüssel nicht extrahiert werden, wenn das komplette Betriebssystem bis hin zum Kernel-Level kompromittiert ist. Eine stabile Verfügbarkeit von solchen Verfahren ist seit Android 6 (hardwaregestützter KeyStore) und seit iOS 9 (KeyChain mit Secure Enclave) gegeben. Um nun Gerätebindung unter solchen Umständen zu erreichen, müssen die am Authentifizierungsprozess als Besitzelemente beteiligten Apps im Registrierungsprozess ein asymmetrisches Schlüsselpaar generieren und den öffentlichen Schlüssel an die Stelle weitergeben, die die Antworten der App letztendlich bearbeitet. Von diesem Punkt an versieht das Besitzelement alle ausgebenden Daten mit einer Signatur, die von der entgegennehmenden Stelle – z. B. dem Bankserver – stets zuerst geprüft wird. Durch dieses Vorgehen werden zwar keine Aussagen über die gesendeten Daten gemacht, es kann aber zumindest sichergestellt werden, dass eine Nachricht von einem bestimmten Gerät stammt. Es zeigt sich also, dass sich Punkt 1 – unter bestimmten Voraussetzungen – auch auf aktuellen Smartphones unter Verwendung App-basierter Verfahren erfüllen lässt. Die Voraussetzungen unter Android erfüllen zum 8. Februar 2018 bereits 57,7% [An], während es unter iOS sogar mindestens 93% sind [Ap].

Eine ganz andere Situation stellt sich aber für Anforderung 2 ein, die eine sichere Anzeige in dem Sinne fordert, dass der Nutzer genau das sieht, was er gegenüber der Bank dann auch bestätigt. Für die smsTAN stellt schon der Transportweg eine Herausforderung dar, da zumindest den vermittelnden Stellen der Klartext vorliegt und auch keine Garantien bzgl.

der Authentizität gewährleistet werden [Re16]. Es wäre also denkbar, dass der Inhalt der SMS bereits vor Zustellung auf dem Smartphone manipuliert wurde. Bei den App-basierten Verfahren kann die Authentizität relativ einfach hergestellt werden, indem z. B. auf TLS zurückgegriffen wird.

Ist die SMS jedoch einmal auf dem Gerät eingegangen, unterscheiden sich die weiteren Voraussetzungen im Vergleich zu App-basierten Verfahren nicht mehr. Als nächstes müssen dem Nutzer die Transaktionsdetails dargestellt werden, damit er deren Richtigkeit überprüfen kann. Hierfür ist es zwingend notwendig, dass die dargestellten Daten zum einen dem entsprechen, was empfangen wurde, und zum anderen auch nicht mehr verändert werden können, wenn die Transaktionsverifikation vom Nutzer abgeschlossen wurde. Es wurde in der Vergangenheit mehrmals gezeigt, dass solche Garantien insbesondere unter Android aktuell nicht existieren. So ist es einem Angreifer aktuell möglich, die ein- und ausgegebenen Daten zu modifizieren, wenn ein Angreifer Kontrolle über die App oder das Betriebssystem erlangt [Ha17; HM16; HM18]. Unter Android haben Fratantonio et al. erst kürzlich Wege gefunden, um auch innerhalb des vorgeschriebenen Rechtemodells volle Kontrolle über die Benutzerschnittstelle zu erlangen [Fr17].

## 5 Zusammenfassung und Ausblick

In diesem Beitrag haben wir allgemeine Anforderungen an die Sicherheit von digitalen Transaktionen formuliert und diese den rechtlichen Voraussetzungen im Rahmen der Zahlungsdiensterichtlinie II (PSD2) gegenübergestellt. Dabei zeigte sich, dass sich die rechtlichen Anforderungen im Kern mit unseren allgemeinen Voraussetzungen vereinen lassen. Hierbei wurden mit dem Blick auf das Mobilebanking insbesondere die Nichtkopierbarkeit und die sichere Anzeige als notwendige Bedingungen für sichere Transaktionen auf nur einem mobilen Endgerät ermittelt. Die Bewertung ergab, dass sich die Anforderung an die Nichtkopierbarkeit bereits jetzt gut realisieren lässt. Die Voraussetzung einer sicheren Anzeige, die verhindert, dass ein Nutzer andere Daten bestätigt, als ihm angezeigt werden, bleibt jedoch ein ungelöstes Problem.

Und obwohl wir die Anforderung der Technischen Regulierungsstandards (RTS) bzgl. der dynamischen Verknüpfung so auffassen, dass eine sichere Anzeige gewährleistet werden muss, scheint der Entwicklungsverlauf der RTS eher darauf hinzudeuten, dass es sich hierbei doch nicht um eine strikte Vorgabe handelt. So zeigt der finale Entwurf nicht nur, dass nun keine separaten vertrauenswürdigen Ausführungsumgebungen (TEE) gefordert werden, sondern die EBA stellt auch klar, dass sie es nicht für nötig hält, dass die verschiedenen Authentifizierungselemente über unterschiedliche Geräte abgebildet werden [EBA17].

Wir sind der Auffassung, dass eine Forderung nach einer TEE, wie sie bereits heute in allen Smartphones vorhanden ist, die Entwicklung einer gemeinsamen Betriebssystemschnittstelle signifikant beschleunigt hätte. Stattdessen wird auch in Zukunft Schadsoftware noch auf absehbare Zeit Verstecken spielen können.

## Literatur


[An] Android Developers: Dashboards: Platform versions, URL: https://developer.android.com/about/dashboards/index.html, Stand: 08. 02. 2018.

[Ap] Apple Inc.: App Store - Support - Apple Developer, URL: https://developer.apple.com/support/app-store/, Stand: 08. 02. 2018.

[COM17] Europäische Kommission: Delegierte Verordnung (EU) der Kommission zur Ergänzung der Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates durch technische Regulierungsstandards für eine starke Kundenauthentifizierung und für sichere offene Standards für die Kommunikation, Nov. 2017, URL: https://ec.europa.eu/transparency/regdoc/rep/3/2017/DE/C-2017-7782-F1-DE-MAIN-PART-1.PDF.

[CT09] Bachfeld, D.: Mit guten Karten: Sicher bezahlen im Internet. c't 19/26, S. 92–95, 2009.

[DK] Die Deutsche Kreditwirtschaft: mobileTAN, URL: https://die-dk.de/zahlungsverkehr/electronic-banking/mobiletan, Stand: 14. 12. 2017.

[Dm14] Dmitrienko, A.; Liebchen, C.; Rossow, C.; Sadeghi, A.: On the (In)Security of Mobile Two-Factor Authentication. In: Financial Cryptography and Data Security - 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers. S. 365–383, 2014, URL: https://doi.org/10.1007/978-3-662-45472-5_24.

[DP03] Deutsche Postbank AG: Online Durchstarten mit Postbank direkt: Neues Finanzportal im Internet / Premiere für die mobileTAN in Deutschland, Nov. 2003, URL: https://www.postbank.de/postbank/pr_presseinformation_2003_11284.html, Stand: 14. 12. 2017.

[EBA17] European Banking Authority: Final Report Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), Feb. 2017, URL: https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf.

[Fr17] Fratantonio, Y.; Qian, C.; Chung, S. P.; Lee, W.: Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop. In: 2017 IEEE Symposium on Security and Privacy, SP 2017, San Jose, CA, USA, May 22-26, 2017. S. 1041–1057, 2017, URL: https://doi.org/10.1109/SP.2017.39.

[Ha17] Haupert, V.: Die fabelhafte Welt des Mobilebankings, 34th Chaos Communication Congress, 34c3: tuwat, Leipzig, Germany, December 27-30, 2017, Chaos Computer Club e.V., Dez. 2017, URL: https://doi.org/10.5446/34946.

[HHF17] Hoffmann, J.; Haupert, V.; Freiling, F.: Anscheinsbeweis und Kundenhaftung beim Online-Banking. Zeitschrift für das gesamte Handels- und Wirtschaftsrecht (ZHR) 181/5, S. 780–816, 2017.

[HM16] Haupert, V.; Müller, T.: Auf dem Weg verTAN: Über die Sicherheit App-basierter TAN-Verfahren. In: Sicherheit 2016: Sicherheit, Schutz und Zuverlässigkeit, Beiträge der 8. Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), 5.-7. April 2016, Bonn. S. 101–112, 2016.

[HM18] Haupert, V.; Müller, T.: On App-based Matrix Code Authentication in Online Banking. In (Furnell, S.; Mori, P.; Camp, O., Hrsg.): Proceedings of the 4th International Conference on Information Systems Security and Privacy, ICISSP 2018, Funchal, Madeira, Portugal, February 22-24, 2018. S. 149–160, 2018, ISBN: 978-989-758-282-0, URL: https://doi.org/10.5220/0006650501490160.

[Mu13] Mulliner, C.; Borgaonkar, R.; Stewin, P.; Seifert, J.: SMS-Based One-Time Passwords: Attacks and Defense - (Short Paper). In: Detection of Intrusions and Malware, and Vulnerability Assessment - 10th International Conference, DIMVA 2013, Berlin, Germany, July 18-19, 2013. Proceedings. S. 150–159, 2013, URL: https://doi.org/10.1007/978-3-642-39235-1_9.

[NB16] norisbank GmbH: norisbank-Umfrage zum Thema Online-Banking, Nov. 2016, URL: https://www.norisbank.de/ueberuns/presseinformation-norisbank-umfrage-online-banking-ein-viertel-der-deutschen-nutzt-veraltetes-tan-verfahren.html, Stand: 13. 12. 2017.

[Re16] Reaves, B.; Scaife, N.; Tian, D.; Blue, L.; Traynor, P.; Butler, K. R. B.: Sending Out an SMS: Characterizing the Security of the SMS Ecosystem with Public Gateways. In: IEEE Symposium on Security and Privacy, SP 2016, San Jose, CA, USA, May 22-26, 2016. S. 339–356, 2016, URL: https://doi.org/10.1109/SP.2016.28.

[RKH16] Rao, S. P.; Kotte, B. T.; Holtmanns, S.: Privacy in LTE networks. In: Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications, MobiMedia 2016, Xi'an, China, June 18-20, 2016. S. 176–183, 2016, URL: http://dl.acm.org/citation.cfm?id=3021417.

[SZ17a] Freiberger, H.; Martin-Jung, H.: Die Tücken der TAN. Süddeutsche Zeitung 73/102, Mai 2017.

[SZ17b] Tanriverdi, H.; Zydra, M.: SMS von gestern Nacht. Süddeutsche Zeitung 73/101, Mai 2017.

[Tu16] Tu, G.; Li, C.; Peng, C.; Li, Y.; Lu, S.: New Security Threats Caused by IMS-based SMS Service in 4G LTE Networks. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016. S. 1118–1130, 2016, URL: http://doi.acm.org/10.1145/2976749.2978393.

[WW17] Weiser, S.; Werner, M.: SGXIO: Generic Trusted I/O Path for Intel SGX. In: Proceedings of the Seventh ACM on Conference on Data and Application Security and Privacy, CODASPY 2017, Scottsdale, AZ, USA, March 22-24, 2017. S. 261–268, 2017, URL: http://doi.acm.org/10.1145/3029806.3029822.

[Zh12] Zhou, Z.; Gligor, V. D.; Newsome, J.; McCune, J. M.: Building Verifiable Trusted Path on Commodity x86 Computers. In: IEEE Symposium on Security and Privacy, SP 2012, 21-23 May 2012, San Francisco, California, USA. S. 616–630, 2012, URL: https://doi.org/10.1109/SP.2012.42.

[ZKA08] Zentraler Kreditausschauss: Mindestsicherheitsanforderungen an die mobile TAN, Apr. 2008, URL: https://die-dk.de/media/files/Mindestsicherheitsanforderungen_mobileTAN_V1_20110621.pdf.

**Danksagungen**: Wir danken Prof. Dr.-Ing. Felix Freiling für hilfreiche Diskussionen sowie den zahlreichen Gutachtern, die ausführliche und wertvolle Verbesserungsvorschläge geliefert haben. Diese Arbeit entstand im Rahmen des von der DATEV eG geförderten Forschungsprojekts „Softwarebasierte Härtungsmaßnahmen für mobile Applikationen“.