

# Kosten senken, Sicherheit erhöhen, Zukunft gestalten

*Sichere Authentifizierung als Grundlage für neue digitale Banking-Angebote.* Immer mehr Menschen tätigen ihre Bankgeschäfte vom PC oder Smartphone aus. Gleichzeitig wachsen in Deutschland die Bedenken in der Bevölkerung. Laut einer Studie des Marktforschungsinstituts Puls halten 45 Prozent der befragten 1.100 deutschen Bankkunden Mobile Banking für unsicher.



*Autor:*  
*Claudius van der Meulen,*  
VP Business Development Europe  
bei Entersakt

Schlechte Voraussetzungen für die Digitalisierung, die von allen Banken massiv vorangetrieben wird. Immer mehr Leistungen sollen vom Kunden im „Self-Service“ über den PC oder mobile Endgeräte getätigt werden, so dass die kostenintensiven stationären Bankfilialen nach und nach abgebaut werden können. Diese Entwicklung zeichnet sich bereits seit einigen Jahren ab und ist nicht aufzuhalten. Aber wie erfolgreich wird der Umbau zur „Bank der Zukunft“ sein, wenn die Kunden nicht mitziehen? Auch Kunden, die seit Jahren gewohnt sind, von ihrem PC Online-Banking Transaktionen durchzuführen oder Online-Shopping Angebote zu nutzen, haben bei der Abwicklung von Geldgeschäften mit mobilen Endgeräten ein schlechtes Gefühl: Sind meine Login-Daten auch wirklich sicher? Was passiert, wenn meine Zugangs-Informationen in die falschen Hände gelangen? Eine Angst, die nicht unbegründet ist, wenn man die weltweit steigende Zahl des Betrugs mit elektronisch abgegriffenen Passwörtern oder Kreditkarten-Daten betrachtet.

Eine nachhaltige Entwicklung bei der Digitalisierung und beim Mobile Banking kann es nur geben, wenn Finanzdienstleister es schaffen, beim Kunden Vertrauen in die

Sicherheit der mobilen Apps aufzubauen. Welche Optionen hat eine Bank hier? Welche Lösung ist für die Zukunft die Beste? Statische Passwort-Verfahren können es nicht sein. Sie haben sich als anfällig erwiesen und entsprechen auch nicht mehr den aktuellen Vorschriften der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). In deren Mindestanforderungen für die Sicherheit von Internet-Zahlungen (MaSI) wird eine „starke“ Authentifizierung verlangt. Diese Forderung wird durch die neuen PSD2-Vorschriften, die spätestens ab 2018 angewendet werden müssen, noch einmal verschärft.

Alle Finanzinstitute sind auf der Suche nach der richtigen Lösung. Dabei hängen sie vielfach noch der überholten Vorstellung nach, dass Komplexität gleichzeitig Sicherheit bedeutet. Nur: Der Kunde akzeptiert keine komplizierten Sicherheitsvorschriften. Er will sich eigentlich überhaupt nicht mit Sicherheitsthemen beschäftigen. Darum soll sich die Bank kümmern. Nur ist ein wirklich wasserdichtes Authentifizierungssystem nun mal nicht ohne die Mitwirkung des Verbrauchers umzusetzen. Dieser verlangt nach einem System, das für ihn möglichst einfach und komfortabel in der Anwendung ist und Sicherheit quasi nebenbei liefert. Widersprechen sich Anforderungen der Banken an ein hochsicheres System und die Wünsche der Kunden nach einer sicheren aber trotzdem einfachen, benutzerfreundlichen Lösung? „An keinem einzigen Punkt müssen Sie für wirklich sicheres Online- oder Mobilebanking bei der Benutzerfreundlichkeit Kompromisse eingehen“, verspricht Schalk Nolte, CEO

von Entersakt, dem Spezialisten für sichere Authentifizierungslösungen. Das Unternehmen hat eine Lösung entwickelt, die beide Seiten zufriedenstellt und gehört damit zu den global führenden Technologieanbietern für Authentifizierung und Sicherheit von mobilen Apps. Entersakt-Technologie schützt heute bereits die Transaktionen von zwölf Millionen Kunden weltweit.

## *Authentifizierung mit nur einem mobilen Endgerät?*

Entersakt nutzt ausschließlich das mobile Endgerät des Kunden zur Authentifizierung von Transaktionen. Dabei wird zunächst das Endgerät mittels eines individuellen digitalen Zertifikats eindeutig identifiziert und anschließend die Transaktion verifiziert. Das Anstoßen und die anschließende Verifizierung erfolgen bei einer vom Smartphone aus getätigten Transaktion zwar über ein Gerät, in jedem Fall aber über zwei separate, mit neuester PKI-Technologie (PKI = Public Key Infrastructure) verschlüsselte Kommunikationskanäle. Kunden bestätigen Transaktionen per Knopfdruck über ihre Mobilgeräte: „Annehmen“ oder „Ablehnen“. Diese „Out-of-Band“-Multifaktor-Authentifizierung, die ohne Browser-Kommunikation auskommt, erhöht die Sicherheit erheblich und erfüllt gleichzeitig die gesetzlichen Bestimmungen einer „starken Authentifizierung“ der MaSI und von PSD2.

Seit 2016 arbeiten in Großbritannien auch die Privatbank Coutts und in Deutschland Pluscard für Transaktionen der Sparkassen-Kreditkarten mit der Entersakt App. ■