Zeitschrift für
Zahlungsverkehr und Kartendienstleistungen

cards

cartes

Karten

D 25079
Fritz Knapp Verlag
Frankfurt am Main
28. Jahrgang
10. Februar 2017
ISSN 0937-597 X

Digitaler Sonderdruck aus 1-2017

Rechtsfragen im Payment-Business

Online-Shopping: Sicherheit und Bequemlichkeit verbinden

Von Thomas Blaß, Thomas Fromherz und Claudius van der Meulen

Online-Shopping: **Sicherheit** und **Bequemlichkeit** verbinden

Von Thomas Blaß, Thomas Fromherz und Claudius von der Meulen

Komplizierte Sicherheitsverfahren im Online-Handel werden vom Kunden nicht akzeptiert. Der Sparkassen-Prozessor Pluscard hat deshalb mit zwei Dienstleistern ausgehend von 3-D-Secure eine neue Lösung implementiert, die auf eine App-basierte dynamische Authentifzierung setzt. Damit sollen Bequemlichkeit und Sicherheit verbunden werden. Red.

Der Online-Handel boomt und ersetzt zunehmend den stationären Handel. So plant beispielsweise die US-Kaufhaus-Gruppe Macy`s, hundert (etwa 15 Prozent) ihrer Filialen zu schließen, und konzentriert stattdessen ihre Ressourcen im Rahmen der Omnichannel-Strategie verstärkt auf Online- und Mobile-Shopping-Kanäle. Letztes Jahr wurde eines von vier britischen Pfund am Black Friday (25. November) online ausgegeben und Amazon erklärte 2016 zum besten Weihnachtsgeschäft aller Zeiten. In Deutschland schließt Gerry Weber einen Teil seiner Filialen und treibt erfolgreich seine Digitalisierungsstrategie voran. Auch bei anderen klassischen deutschen Einzelhändlern wie Douglas oder Thalia investieren die Verantwortlichen verstärkt in Omnichannel-Konzepte und sichern damit den wirtschaftlichen Erfolg ihrer Unternehmen.

Der Zuwachs im Online-Handel hat aber auch eine Kehrseite: Verbraucher müssen ihre persönlichen Daten bei immer mehr Online-Marktplätzen eingeben und steigern damit die Anfälligkeit für Betrug. Meist haben Kunden ein ungutes Gefühl: Sind meine Login-Daten auch wirklich sicher, was passiert, wenn meine Kreditkarten-Informationen in die falschen Hände gelangen? Eine Angst, die nicht unbegründet ist, wenn man die weltweit steigende Zahl des Betrugs mit abgegriffenen Kreditkarten-Daten betrachtet. Neben dem eigentlichen Kartendiebstahl werden heute vermehrt Karteninformationen mittels elektronischer Methoden gestohlen und missbraucht.

Sicherheit ohne Mitwirkung des Kunden?

Hier müssen Banken und Kreditkartenherausgeber reagieren, um das Vertrauen der Kunden in die Sicherheit von Online-Transaktionen zu erhalten und den Kunden ein sicheres Online-Einkaufserlebnis zu gewährleisten.

Das Problem dabei: Der Verbraucher will sich nicht mit Sicherheitsthemen beschäftigen. Darum soll sich die Bank kümmern. Komplizierte Verfahren werden nicht akzeptiert, sondern verhindern im Zweifelsfall sogar einen Online-Kauf. Nur ist ein wirklich wasserdichtes Sicherheitssystem nun einmal nicht ohne die Mitwirkung des Kunden umzusetzen. Der Kunde verlangt also nach einem System, das für ihn möglichst einfach und komfortabel in der Anwendung ist und Sicherheit quasi nebenbei liefert.

Dazu kommt, dass bisherige Authentifizierungsverfahren mit statischen oder dynamischen Passwörtern über das Internet den geltenden rechtlichen Ansprüchen nicht mehr entsprechen. Es fehlt hier der geforderte „zweite Faktor".

Zwei-Faktor-Authenitifizierung

Im Mai 2015 hat die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) eine neue Reihe von Mindestanforderungen für die Sicherheit von Internetzahlungen (MaSI) veröffentlicht. Die BaFin verlangt eine „starke" Authentifizierung. Genau das fordert auch die neue Zahlungsdienstleistungsrichtlinie der Europäischen

Zu den Autoren

Thomas Blaß, Abteilungsleiter Markt Innen, PLUSCARD Service-Gesellschaft für Kreditkarten-Processing mbH, Saarbrücken; **Dr. Thomas Fromherz**, Head of Payment & Card Services, Netcetera, Zürich; **Claudius van der Meulen**, VP Business Development Europe, Entersekt Europe, Geldermalsen (NL)

Union, kurz PSD2 (Payment Service Directive 2), die ab 2018 auch nach nationalem Recht für alle Finanzinstitute verpflichtend wird und die MaSI-Richtlinien noch einmal verschärft. Danach müssen mindestens zwei der folgenden Elemente für den Authentifizierungsprozess einer Bank vorhanden sein, um sich als „stark" zu qualifizieren:

- Wissen – etwas, das der Benutzer kennt (zum Beispiel Passwort, PIN, ID-Nummer),
- Besitz – etwas, das der Benutzer besitzt (zum Beispiel Token oder Chipkarte),
- Inhärenz – etwas, das nur vom Benutzer kommen kann (ein biometrisches Merkmal, zum Besipiel Fingerabdruck oder Iris-Scan)

Eine weitere Voraussetzung ist, dass mindestens eines dieser Elemente nicht wiederverwendbar und nicht replizierbar sein darf.

Ausgangspunkt 3-D-Secure

Wie kann ein solches System aussehen, das höchste Sicherheitsstandards berücksichtigt, gleichzeitig die gesetzlichen Vorgaben erfüllt und so einfach und benutzerfreundlich ist, dass es vom Kunden auch akzeptiert und genutzt wird? Vor dieser Frage stand auch die Pluscard.

Seit August 2015 organisiert der Prozessor sein Kreditkartenportfolio über das mandantenfähige 3DS-System von Netcetera, das in der Schweiz betrieben wird und die Sicherheitsanforderungen von nach PCI DSS erfüllt. So lag es nahe, auch die Realisierung einer sicheren Zahlungslösung für den Online-Einkauf der Sparkassenkunden gemeinsam durchzuführen. Ziel war es nicht nur, dafür zu sorgen, dass die neuesten rechtlichen Vorschriften eingehalten werden, sondern den Anwendern die höchste verfügbare Sicherheit und das beste Nutzererlebnis anzubieten.

Zunächst führte Pluscard gemeinsam mit dem Dienstleister eine 3-D-Secure-Authentifizierung für die Kreditkartennutzer ein. Das seit 2001 bestehende 3-D-Secure-Protokoll hat sich als Sicherheitsmaßnahme bewährt. Online-Shopper erkennen und vertrauen den etablierten Verfahren beim Kauf im Internet „Verified by Visa" und „Mastercard Secure Code". Beide basieren auf diesem Protokoll.

Dynamische Authentifizierung via App

Um das System noch sicherer, vor allem aber deutlich benutzerfreundlicher zu gestalten, wurde das Produkt 3DS DYN für die dynamische Authentifizierung implementiert und dabei die Sicherheitstechnologie des südafrikanischen Unternehmens Entersekt eingebunden. Dabei wurde die auf der Transakt-App von Entersekt basierende Technologie in den etablierten Authentifizierungsprozess von Pluscard integriert und bietet damit Sicherheit und Benutzerfreundlichkeit. Das Ergebnis ist die S-ID-Check-App.

Kreditkartennutzer können nun mit einem Klick in der App ihre Zahlungen bestätigen. Damit werden nun Online-Zahlungen per Kreditkarte mit einer extrem sicheren und dabei trotzdem nutzerfreundlichen Adaptierung von 3-D-Secure geschützt. Unsichere Passwörter gehören der Vergangenheit an. Das Verfahren wurde als zusätzliche Sicherheitsebene für den Internethandel entwickelt. Damit kann der Online-Kreditkartenbetrug, bei dem die Karte nicht physisch vorhanden sein muss, deutlich reduziert werden.

Wenn ein solcher App-Nutzer eine Shopping-Transaktion auf einer E-Commerce-Website initiiert, die Kreditkartenzahlung mit dem 3-D-Secure-Verfahren anbietet, erhält er eine Push-Nachricht mit den Zahlungsdetails auf seinem mobilen Endgerät.

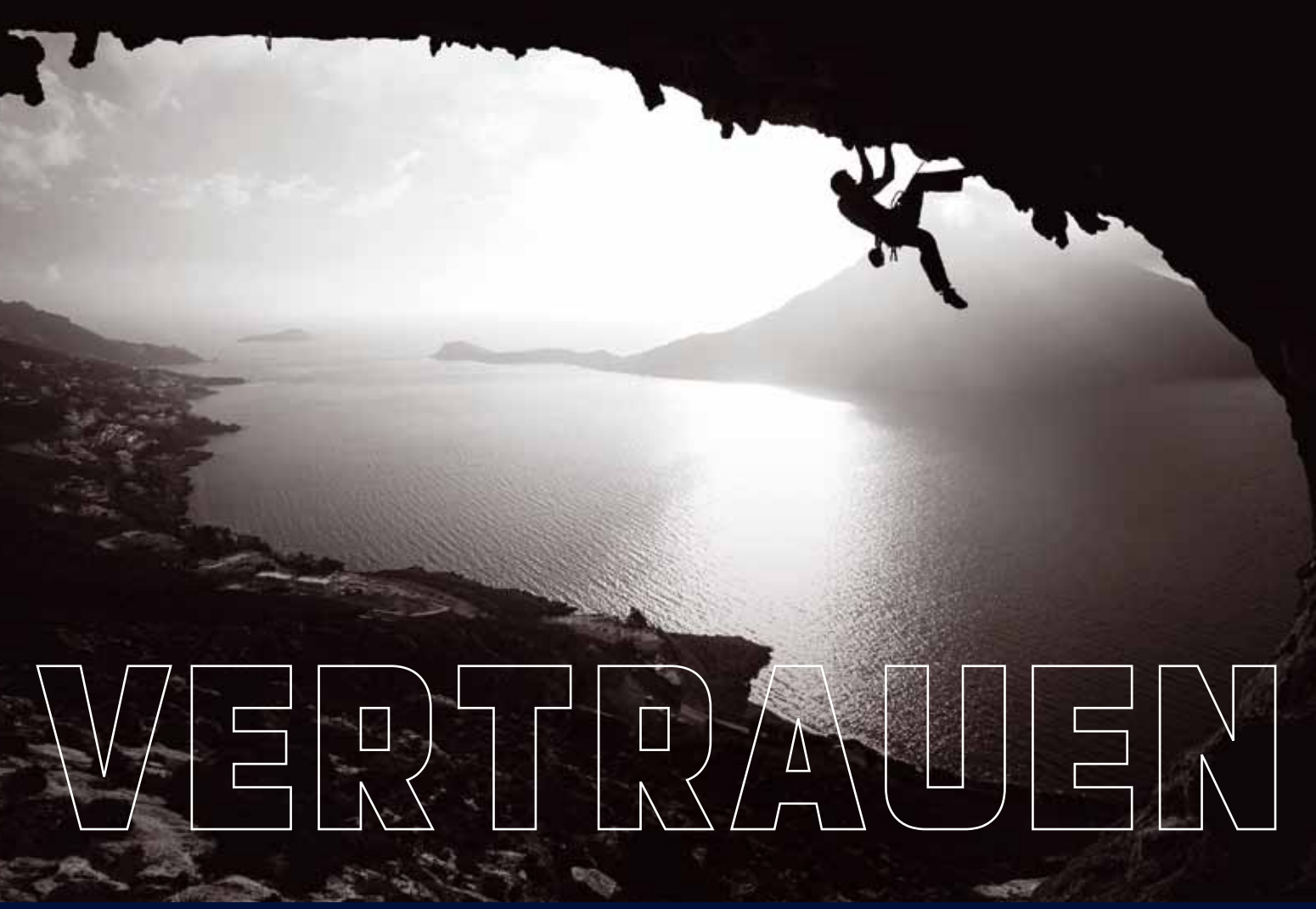
Alles, was der Nutzer tun muss, ist, die Zahlung innerhalb der App und damit außerhalb eines anfälligen Webbrowsers durch Antippen der Antwort „Bestätigen" zu genehmigen oder die Zahlung zu beenden, indem er auf „Abbrechen" tippt. Letzteres verhindert einfach und effektiv, dass ungewollt betrügerische Transaktionen vom Kunden bestätigt werden. Der Käufer muss sich weder an sein Kennwort erinnern, das er eventuell seit längerer Zeit nicht verwendet hat, noch auf eine Textnachricht mit einem Code warten, bevor er den Einkauf abschließen kann.

Die Technologie nutzt dazu digitale Zertifikate und State-of-the-Art PKI(Public Key Infrastructure)-Verschlüsselungstechnologie, um das Endgerät zu identifizieren und die Transaktion zu verifizieren. Das Anstoßen und die anschließende Verifizierung erfolgen auch bei einer vom Smartphone aus getätigten Transaktion in jedem Fall über zwei separate, verschlüsselte Kommunikationskanäle.

Gesetzliche Bestimmungen der MaSi erfüllt

Die Verbraucher bestätigen Einkäufe per Knopfdruck über ihre Mobilgeräte. Diese „Out-of-Band"-Multifaktor-Authentifizierung, die ohne Browser-Kommunikation auskommt, erhöht die Sicherheit erheblich und erfüllt gleichzeitig die gesetzlichen Bestimmungen der MaSI.

Die Kooperation der drei Partner hat es in diesem Fall ermöglicht, sowohl den Anforderungen der Regulierungsbehörden als auch der Verbraucher gerecht zu werden. Für die Sparkassen-Kreditkarte ist eine Sicherheitslösung auf dem neuesten Stand der Technik entstanden. Die Sparkassenkunden profitieren von einer benutzerfreundlichen Lösung, die nicht nur Sicherheit bietet, sondern auch dafür sorgt, dass Online-Transaktionen schnell und einfach durchgeführt und nicht abgebrochen werden.



Entersekt

Online-Banking und digitaler Zahlungsverkehr. **Vertrauen ist die Basis für eine erfolgreiche Zukunft.**

Entersekt unterstützt Banken und Finanzinstitutionen weltweit beim Aufbau innovativer digitaler Services, denen Kunden zu 100 % vertrauen können.

Mit Transakt™ wird Online- und Mobile-Banking ganz einfach, sicher und nutzerfreundlich. Ob als Software Development Kit (SDK) oder als App.

Mit Transakt™ von Entersekt erschließen Sie das volle Potenzial des digitalen Bankings.

Für zufriedene und loyale Kunden.

- Push-basiert
- Multi-Faktor-Authentifizierung
- Hochsichere Out-of-Band-Technologie
- Erfüllt alle regulatorischen Anforderungen inklusive PSD2

fido U2F™ Certified

entersekt.com