Die Zentralbank der Genossenschaftlichen FinanzGruppe setzt auf CORONIC Sicherheitstechnologie

Mit der DZ BANK AG hat sich die Zentralbank der Genossenschaftlichen FinanzGruppe für ein technisches Verfahren von CORONIC zum Schutz von Kreditkarten Bezahlvorgängen im Internet entschieden. Die Kieler App SIGN soll künftig unter dem Namen VR-SecureCARD den Versand der Transaktionsnummer (TAN) bei Bezahlvorgängen im Internet übernehmen. Damit folgt die DZ BANK einer Entscheidung der Bundesanstalt für Finanzaufsicht (BaFin), die im Rahmen der Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI) auf eine Verbesserung der Sicherheitsverfahren bei Online-Bezahlvorgängen mit Kreditkarten gedrungen hat.

Kiel/Frankfurt, den 4. April 2017 – Das Bezahlen mit der Kreditkarte beim Online-Shopping ist einfach und bequem. Man gibt die Kartennummer an, klickt auf O.K. und der Bezahlvorgang ist abgeschlossen. Wenn allerdings ein Krimineller an die Kreditkarten-Daten kommt, kann er problemlos selber Waren im Internet bestellen und die Kosten trägt der bestohlene Kartenbesitzer. Aus diesem Grund gibt es seit vielen Jahren bei allen deutschen Banken, die Kreditkarten an ihre Kunden herausgeben, das sogenannte 3D-Secure-Verfahren. Hierbei wird zu jedem Bezahlvorgang zusätzlich eine Transaktionsnummer (TAN) generiert, die per SMS auf das Handy des Kreditkartenbesitzers geschickt wird - genauso wie beim klassischen Online-Banking mit mobiler TAN.

Die „SMS per Mobilfunk“ ist eine Technik der frühen Neunzigerjahre. Damals wurde auf Verschlüsselung und Sicherheit wenig Wert gelegt, so dass heute quasi jede App auf dem privaten Smartphone den Inhalt der TAN-Nachricht auslesen und manipulieren kann. Auch im aktuellen BITKOM-Leitfaden zum Online-Banking wird die SMS-TAN als unsicher eingestuft. Dieser Umstand hat das Bundesamt für Finanzdienstleistungen (BaFin) dazu bewogen, von den Kreditkarten ausgebenden Banken eine Verbesserung des 3D-Secure-Verfahrens zu verlangen: die nach dem Online-Einkauf per Kreditkarte verschickte TAN soll künftig nicht mehr via Mobilfunk-SMS sondern kryptografisch gesichert in eine spezielle TAN-App der Bank übermittelt werden, so die Finanzaufsicht.

Mit dem Produkt SIGN hat die CORONIC GmbH schon länger eine Anwendung im Portfolio, die den neuen Anforderungen der Finanzaufsicht genügt. Jetzt hat sich mit der DZ BANK AG die Zentralbank der Genossenschaftlichen FinanzGruppe dafür entschieden, bei der sicheren

Übermittlung der TAN auf die SIGN-Technologie der Kieler Sicherheitsexperten zu setzen. Das Produkt wird von der DZ BANK in Frankfurt zentral unter dem eigenen Namen „VR-SecureCARD“ vermarktet. „Wir freuen uns, ab sofort allen Kreditkarten-Kunden die neue VR-SecureCARD App über die App-Stores von Google und Apple zur Verfügung stellen zu können“, sagt Christian Bartsch, Produktmanager für Kreditkarten bei der DZ BANK.

Für die Endkunden ist die neue Anwendung nicht nur sicherer, sondern auch schnell und bequem zu handhaben. Aber auch für die einsetzende Bank ergeben sich große Vorteile, denn die CORONIC Technologie basiert auf einer sogenannten virtuellen Handynummer. Dadurch kann die Bank technisch die gleichen, etablierten SMS-Schnittstellen und -Prozesse wie bisher verwenden. Für das Banksystem sieht die CORONIC App wie ein normales Handy mit einer normalen Telefonnummer aus. „Dieser technische Kniff macht die Umstellung innerhalb der Bank zu einem Kinderspiel“, sagt Dr. Frank Bock, Geschäftsführer der CORONIC GmbH in Kiel. Dies ist auch ein weiterer Vorteil für die Kreditkarten-Kunden: sie geben weiter ihre Handynummer bei der Bank an, nur eben jetzt eine virtuelle. Es ändert sich also fast nichts.

Infoblock zu VR-SecureCARD

Die DZ BANK AG als Herausgeber von Kreditkarten der Genossenschaftlichen FinanzGruppe bietet mit VR-SecureCARD eine App-basierte Authentifizierung für sichere Kreditkartenzahlungen. Karteninhaber der angeschlossenen Genossenschaftsbanken können damit eine, wahlweise per Fingerabdruck oder persönlichem Kennwort, geschützte App zur MaSI-konformen E-Commerce Bezahlung nutzen. Die App wird allen Karteninhabern angeboten und kann über den Internetauftritt der jeweiligen Bank des Karteninhabers registriert werden.

Hintergrundinformationen zur CORONIC TAN-App SIGN:

Online-Banking gibt es seit über 15 Jahren, stets mit einer Authentifizierung des Nutzers über die Kontonummer und das Passwort (PIN) sowie der Autorisierung jeder einzelnen Überweisung durch eine Transaktionsnummer, die so genannte TAN. Die TAN wird von der Bank meist per SMS aufs Handy des Kunden geschickt. Das ist zwar für den Kunden bequem, für die Bank jedoch teuer (SMS-Kosten) und sicherheitstechnisch nicht mehr zeitgemäß, denn die Mobilfunk-SMS ist eine Technologie der 90er Jahre. Exakt das gleiche Verfahren, wie es hier für das Online-Banking beschrieben wurde, gibt es unter dem Namen 3D-Secure auch für Internet-Bezahlvorgänge mit der Kreditkarte. Auch hier wird eine klassische Mobilfunk-SMS mit einer TAN versendet. Es lag daher nahe, die TAN nicht auf diese veraltete Weise über den Telekom-Provider zu versenden, sondern sie direkt via Internet an eine besonders geschützte TAN-App auf das Smartphone zu übermitteln. Die deutschen Sparkassen haben für diesen Vorgang vor zwei Jahren den rechtlich geschützten Begriff pushTAN™ geprägt. Nach einer Novellierung der sogenannten Mindestanforderungen an die Sicherheit von Internetzahlungen (MaSI) durch die Bundesanstalt für Finanzaufsicht (BaFin) ist ein solches kryptografisch gesichertes TAN-

Verfahren jetzt auch für alle Internet-Bezahlvorgänge mit der Kreditkarte zur Vorschrift geworden. Heute gibt es auf dem Markt einige artverwandte Softwarelösungen zum Versenden der TAN-Nachricht. Meist geschieht dies über die cloud- bzw. push-Dienste von Google und Apple. Technisch sind die Ansätze zur Ablösung der alten SMS sehr ähnlich: Zweikanaltrennung, Datentresor und starke Verschlüsselung machen push-Apps schnell und sicher. Das eigentliche Problem für die Banken ist aber nicht die Funktion der App, sondern der große Aufwand bei der Umstellung der Banksysteme vom klassischen SMS-Versand auf das neue push-Format. Genau hier setzt die push-App SIGN aus dem Hause CORONIC an. Sie simuliert für die Kommunikation mit dem Banksystem eine so genannte virtuelle Handynummer. Dadurch kann das Rechenzentrum der Bank die gleichen, alten SMS-Schnittstellen und -Prozesse wie bisher verwenden. Für das Banksystem wirkt die neue CORONIC push-App wie ein normales Handy mit einer normalen Telefonnummer. Dieser Trick macht die technische Umstellung im Rechenzentrum zu einem Kinderspiel. Die virtuelle Handynummer erlaubt die bestehenden Banksysteme ohne Anpassungen weiterzuverwenden und ist auch für den Bankkunden transparent und einfach. Der Kunde kann seine neue virtuelle Handynummer genauso nutzen wie die alte Handynummer.

Die CORONIC GmbH wurde 2003 von Dipl.-Inf. Andreas Harder und Dr. Frank Bock in Kiel gegründet. Das Unternehmen wurde für seine technische Innovationskraft von der Europäischen Union ausgezeichnet und gewann verschiedene Technologiepreise. CORONIC beschäftigt 24 Mitarbeiter, die sich mit der Sicherheit und Härtung von Bankprozessen im Internet beschäftigen. Das Unternehmen ist Marktführer bei der Trojaner-Abwehr und dem Verhindern von Phishing-Angriffen auf die Computer von Privatkunden bei deutschen Banken. Zu den Kunden des Unternehmens gehören über 900 In- und Ausländische Banken und Versicherungen sowie internationale Konzerne wie T-Systems, Heidelberger Druckmaschinen oder Airbus.

Pressekontakt: Frank Bock, CORONIC GmbH, Schauenburgerstraße 116, 24118 Kiel, Tel.: +49 (0)431 530 237 - 0, E-Mail: info@coronic.de, Web: www.coronic.de

Bild VR-SecureCARD App der DZ Bank