Februar 2021

Hannoversche Volksbank

VR Aktuell

EIN THEMA. VIELE FACETTEN.

Onlinebanking optimal nutzen

1 ***EINFACHER ZUGANG***
VERFAHREN FÜR JEDEN EINSATZZWECK

2 ***SICHERE VERWENDUNG***
SICHERHEITS- UND ANWENDUNGSTIPPS

3 ***SCHNELLE BEZAHLUNG***
ZAHLUNGSDIENSTE SINNVOLL NUTZEN

Bankgeschäfte per Mausklick oder Touchscreen

Banking, wo und wann Sie wollen

So gut wie alle Geldangelegenheiten lassen sich heute jederzeit und an jedem Ort online erledigen. Mobile Apps und zuverlässige Sicherheitsverfahren machen das Onlinebanking zum täglichen sicheren Begleiter. Es ergänzt die Informations- und Handelsangebote im Internet um die Möglichkeit, Waren und Dienste komfortabel elektronisch zu bezahlen und die Finanzen zu verwalten. Mit dem Onlinebanking können Zahlungen an Internethändler über verschiedene Schnittstellen ganz einfach ausgelöst und Daten für andere Dienste zur Verfügung gestellt werden. Zudem können Sie viele weitere Services Ihrer Bank oder der angeschlossenen genossenschaftlichen Finanzdienstleister nutzen.

Das Online-Konto: der Schlüssel zu digitalen Angeboten

Über 85 Prozent der Internetnutzer in Deutschland verwenden bereits Onlinebanking. Um den Vorgang immer reibungsloser zu gestalten und die Möglichkeiten weiter zu verbessern, investieren die Volksbanken und Raiffeisenbanken stetig in ihre Online-Angebote, moderne Sicherheitsverfahren, intelligente Betrugserkennung und verstärkte Kundenaufklärung. Das Online-Konto wird zum universellen Schlüssel für die Angebote der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken sowie anderer Unternehmen. Diese Ausgabe von VR Aktuell zeigt, wie Sie ins Onlinebanking einsteigen, wie Sie es sicher nutzen und wie Sie Zugriffe auf die neue Zahlungsschnittstelle effektiv kontrollieren können.

1 EINFACHER ZUGANG
VERFAHREN FÜR JEDEN EINSATZZWECK

Online-Zugang per VR-NetKey

Die Grundlage und eindeutige Anmeldekennung für das Onlinebanking bei jeder Volksbank und Raiffeisenbank ist der VR-NetKey. Kunden erhalten diesen nach ihrer Zustimmung zu den Online-Nutzungsbedingungen. Zur einfacheren Anmeldung im Onlinebanking kann ein frei wählbarer Benutzername vergeben werden. Mit diesem können Kunden sich auf die von ihnen gewünschte Weise mit dem Onlinebanking verbinden. Die meisten wählen eines der TAN-Verfahren: Smart-TAN, SecureGo oder mobileTAN. Diese Verfahren benötigen keine stationäre Installation und sind für alle Zugangskanäle geeignet.

Als Zugang stehen den Kunden der Volksbanken und Raiffeisenbanken die mobile VR-BankingApp sowie das VR-Web-Banking kostenlos zur Verfügung. Alternativ können sie eine beliebige Finanzsoftware nutzen, die dem FinTS-Standard entspricht, zum Beispiel die VR-NetWorld Software.

Aufträge und Zahlungen mit zwei Faktoren absichern

Aufträge und Zahlungen im Onlinebanking sowie auch Kartenzahlungen im Internet müssen prinzipiell mit einer sogenannten starken Kundenauthentifizierung abgesichert werden. Das heißt: Sie müssen durch zwei unabhängige Faktoren vom Kunden autorisiert werden. Hierfür erhält der Kunde eine persönliche Online-PIN (erster Faktor) und eines der TAN-Verfahren (zweiter Faktor). Bei Zahlungen geringer Beträge kann die Bank unter Umständen auf den zweiten Faktor verzichten. Auch beim Anmelden muss mindestens alle 90 Tage zusätzlich zur PIN eine TAN eingegeben werden.

Sicherheitsverfahren freischalten

Bevor Kunden zum ersten Mal das VR-Web-Banking nutzen können, muss ein TAN-Verfahren als zweiter Authentifikationsfaktor registriert sein. Bei Smart-TAN ist das besonders einfach: Die Bank schaltet hierfür die girocard frei, die jeder üblicherweise zu seinem Konto bekommt. Der Chip der girocard enthält einen TAN-Generator. Zum Anzeigen der TAN sollte man noch über einen Smart-TAN Leser verfügen, aber auch chipTAN Leser der Sparkassen können verwendet werden.

Wer sein Smartphone zur Authentifikation nutzen möchte, installiert die VR-SecureGo App über den Link auf der Seite seiner Bank. An diese App kann die Bank dann die TAN zur Freigabe schicken. Um sicherzugehen, dass es sich dabei auch um das richtige Smartphone handelt, muss die installierte App zuvor verifiziert werden. Hierfür erstellt die App bei der ersten Verwendung einen Freischaltcode und sendet ihn an die Nutzer. Mit diesem kann die App dann – wie mit einer TAN – freigeschaltet werden.

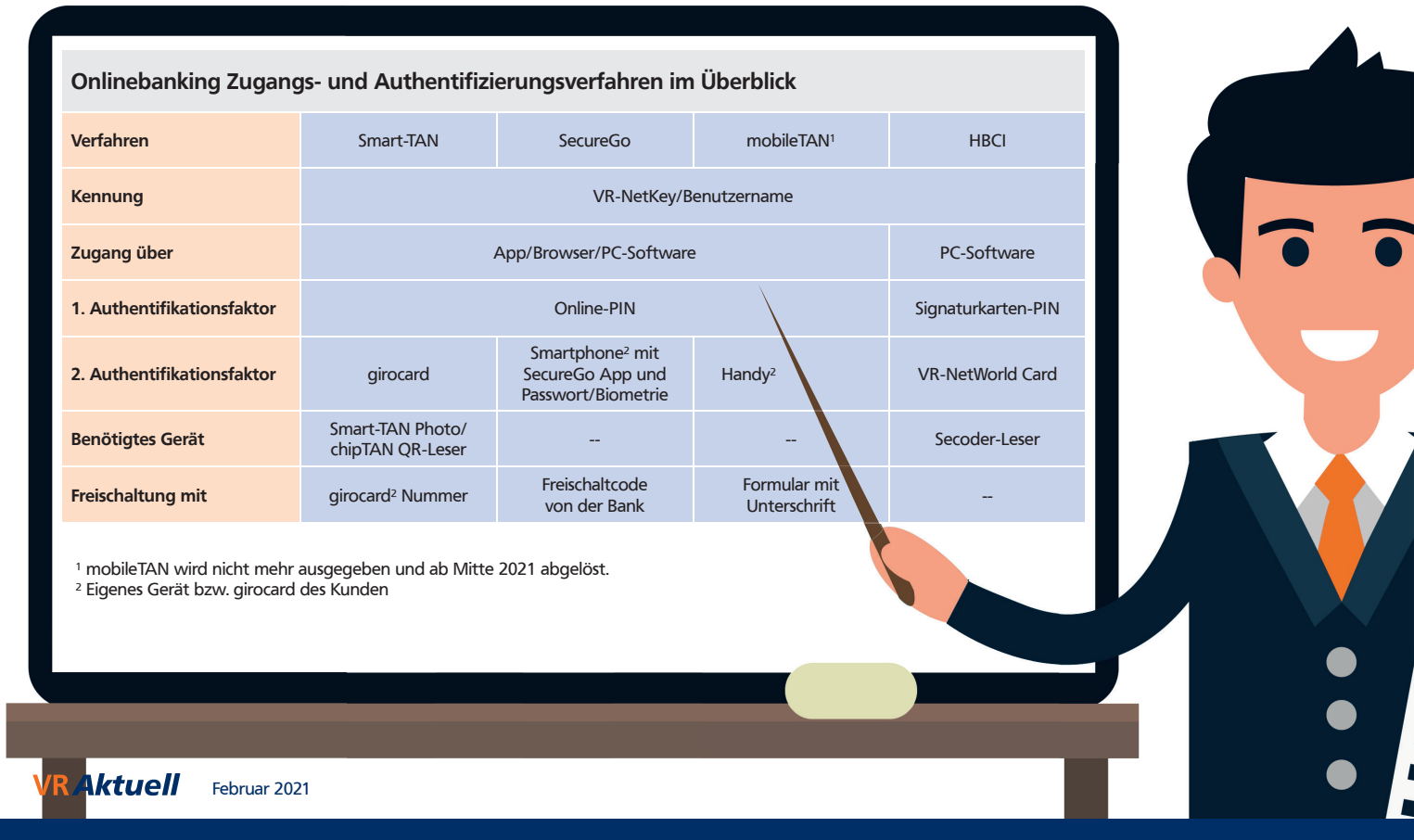
TAN-Verfahren wechseln oder erweitern

Kunden können in den meisten Fällen auch im VR-Web-Banking unter „Banking > Service > Online-Banking > TAN-Verwaltung“ selbst ein neues TAN-Verfahren freischalten oder auf ein anderes wechseln. Über „Smart-TAN plus anmelden“ kann dort die von der Bank zur Verfügung gestellte girocard als TAN-Generator aktiviert werden. Smart-TAN und SecureGo können gleichzeitig registriert und genutzt werden. Ist das Verfahren mobileTAN registriert, wird es dabei automatisch gelöscht, da es veraltet ist und nicht mehr angewandt werden sollte.

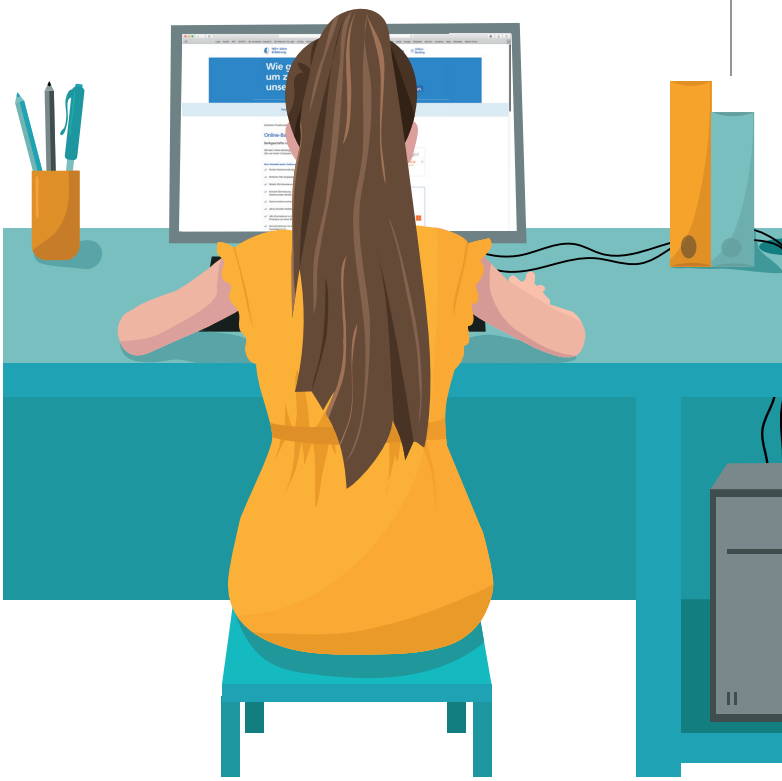
Onlinebanking Zugangs- und Authentifizierungsverfahren im Überblick

Verfahren	Smart-TAN	SecureGo	mobileTAN[1]	HBCI
Kennung	VR-NetKey/Benutzername			
Zugang über	App/Browser/PC-Software			PC-Software
1. Authentifikationsfaktor	Online-PIN			Signaturkarten-PIN
2. Authentifikationsfaktor	girocard	Smartphone[2] mit SecureGo App und Passwort/Biometrie	Handy[2]	VR-NetWorld Card
Benötigtes Gerät	Smart-TAN Photo/ chipTAN QR-Leser	--	--	Secoder-Leser
Freischaltung mit	girocard[2] Nummer	Freischaltcode von der Bank	Formular mit Unterschrift	--

[1] mobileTAN wird nicht mehr ausgegeben und ab Mitte 2021 abgelöst.
[2] Eigenes Gerät bzw. girocard des Kunden



2 SICHERE VERWENDUNG
SICHERHEITS- UND ANWENDUNGSTIPPS



Aufträge stets prüfen

Die Sicherheitsverfahren beim Onlinebanking unterscheiden sich in der Art ihrer Technik. In der Bedienung sind sie jedoch grundsätzlich gleich. Diese läuft stets in vier Schritten ab:

1. Auftrag im Onlinebanking erfassen und „Weiter" drücken.
2. Bei Smart-TAN Photo: TAN-Leser mit girocard vor Farbcode-Grafik halten und Farbcode scannen.
   Bei SecureGo: Smartphone entsperren und SecureGo App mit Passwort oder Biometrie öffnen.
3. Im Display des Lesers oder Smartphones Auftragsart, Empfänger-IBAN und Betrag mit den beabsichtigten Daten vergleichen und mit „O. K." bestätigen.
4. TAN übertragen und „Ausführen" drücken.

Schritt 3 ist dabei entscheidend: Auf dem Kartenleser oder Smartphone wird genau angezeigt, was die Bank ausführen wird. Die Daten im Display sollten daher stets nur mit den beabsichtigten Auftragsdaten zum Beispiel aus der Original-Rechnung oder dem Auftrag verglichen werden. Niemals sollte das Display mit Daten auf dem PC oder Tablet verglichen werden, denn deren Anzeigen könnten von anderen Programmen manipuliert worden sein. Nach dem Befehl „Ausführen" ist ein Zurückholen oder Widerrufen des Auftrags prinzipiell nicht mehr möglich.

Vorsicht vor Betrug

Smart-TAN Photo, SecureGo und HBCI mit VR-NetWorld Card sind alle gleichermaßen sicher. Aufträge können stets nur von der Person ausgeführt werden, die im Besitz der zum Konto gehörigen Authentifizierungsverfahren ist. Betrüger suchen sich daher andere Wege, um an das Geld von Kunden zu kommen, so etwa über unglaubwürdige Sonderangebote unbekannter Händler im Internet. Die Kunden erhalten dann meist nicht die bestellte oder gar keine Ware.

Sogenannte Phishing-E-Mails sind den meisten Internetnutzern oft schon bekannt. Die Links und Anhänge in diesen Phishing-E-Mails können den PC nachhaltig schädigen, indem etwa sensible Daten gelöscht oder verschlüsselt werden. In anderen Fällen wird in diesen E-Mails um die Eingabe der Online-PIN und einiger TANs gebeten, mit denen sich die Betrüger dann Geld vom jeweiligen Konto holen. Die Phishing-E-Mails haben gefälschte Absender-Adressen von vertrauenswürdigen Unternehmen oder Personen, teilweise sogar von Banken, ohne dass diese etwas gegen den Missbrauch ihrer Namen unternehmen oder den Versand solcher Phishing-E-Mails verhindern können. Daher sollten sie stets sofort gelöscht werden.

Einige Betrüger rufen die Kunden sogar direkt an, um sie zu überreden, private Zugangsdaten zu verraten. So bieten angebliche Service-Mitarbeiter von Microsoft an, den PC zu untersuchen, oder angebliche Bankangestellte fordern Nutzer unter einem Vorwand dazu auf, eine Testüberweisung vorzunehmen, um die Funktion des jeweiligen Kontos zu überprüfen oder wiederherzustellen.

Alle Funktionen des Onlinebankings wurden bereits von der Bank umfassend geprüft. Eine Hilfe durch die Nutzer ist nicht erforderlich. Testüberweisungen gibt es nicht und Mitarbeiter einer Bank werden niemals nach der Onlinebanking-PIN oder einer TAN fragen. Auch wenn ein unerwarteter Betrag auf dem Konto eingeht, sollten Kunden diesen niemals an eine IBAN zurücküberweisen, die ihnen ein freundlicher Anrufer oder eine E-Mail nennt. Solche fehlgeleiteten Beträge stammen oft aus illegalen Geschäften. Besteht der Verdacht, dass es sich um Betrugsversuche handeln könnte, sollte man sich stets zuerst an seine Bank wenden.

Gut zu wissen

Beim Onlinebanking sind Verbraucher gegen Missbrauch gut geschützt. Hält der Kunde seine Sorgfaltspflichten ein, ist die Selbstbeteiligung für Schäden auf 50 Euro begrenzt. Nicht autorisierte Zahlungen werden innerhalb eines Bankarbeitstags auf das Konto zurückerstattet. Im Notfall ist das Onlinebanking unverzüglich bei der Bank oder über die kostenlose Sperrrufnummer 116 116 zu sperren.

3 SCHNELLE BEZAHLUNG
ZAHLUNGSDIENSTE SINNVOLL NUTZEN

Neue Zahlungsdienstleister bekommen Zugang zu Girokonten

Seit einiger Zeit gibt es im Internet vermehrt sogenannte Zahlungsauslöse- und Kontoinformationsdienste. Zahlungsauslösedienste werden vor allem als Bezahlmöglichkeit in Webshops von Händlern angeboten. Hier kann man einen solchen Dienst beauftragen, um eine Zahlung vom Onlinekonto aus per Online-PIN und TAN auszulösen. Kontoinformationsdienste bieten an, alle Umsätze eines Online-Kontos auszulesen, etwa um die Kontostände mehrerer Zahlungskonten bei verschiedenen Banken aufzubereiten, Bonitätsaussagen für weitere Dienste wie Kredite zu bieten oder die Ausgaben zu durchsuchen, um neue Angebote machen zu können.

Aber keine Sorge: Die Bank gewährt solchen Zahlungsauslöse- oder Informationsdiensten nur dann Zugang zu einem Online-Konto, wenn der Kunde die Erlaubnis dafür gegeben sowie dem Dienst seinen VR-NetKey, seine Online-PIN und eine gültige TAN übermittelt hat.

Kontrollmöglichkeiten für die Kontozugriffe

Damit Kunden den Überblick darüber behalten, welchen Diensten sie die Erlaubnis für den Zugriff auf ihr Onlinebanking erteilt haben, wurden neue Kontrollmöglichkeiten eingebaut. Denn: Kontoinformationsdienste können bis zu 90 Tage lang die Kontoumsätze lesen. Zahlungsauslösedienste können regelmäßige Zahlungen anlegen, die weiter ausgeführt werden müssen. Im VR-Web-Banking zeigt der Bereich „Banking > Service > Konten und Verträge > Zugriffsverwaltung“ sämtliche bei der Bank eingegangenen Aktionen von Zahlungsdiensten. Hier kann man sehen, welche Erlaubnisse erteilt wurden und welche Aktivitäten ein Dienst ausgelöst hat. Will man eine Erlaubnis zurücknehmen, ist dies in der Zugriffsverwaltung sehr leicht möglich.

Wenn es wider Erwarten einmal einen Betrug bei einer Zahlung mit einem Zahlungsdienstleister geben sollte, etwa weil ein falscher Betrag abgebucht wurde oder der Händler sein Geld nicht bekommen hat, sollte der Kunde dies sowohl dem Zahlungsdienstleister als auch seiner Bank anzeigen. Diese werden den Schaden dann gemeinsam beheben.

Herausgeber und verantwortlich für den Inhalt dieser Ausgabe:
Bundesverband der Deutschen Volksbanken und Raiffeisenbanken · BVR, Berlin
Leitung/Chefredaktion: Tim Zuchiatti, BVR – Kommunikation und Öffentlichkeitsarbeit
Autor: Dr. Olaf Jacobsen, BVR
Co-Autor: Dr. Christian Koch, BVR
Objektleitung: Manuela Nägel, DG VERLAG, Leipziger Str. 35, 65191 Wiesbaden,
E-Mail: mnaegel@dgverlag.de
Verlag und Vertrieb: Deutscher Genossenschafts-Verlag eG, vertreten durch den Vorstand: Peter Erlebach (Vorsitzender), Franz-J. Köllner und Marco Rummer, Leipziger Str. 35, 65191 Wiesbaden

Gestaltung und Redaktion: hundertzwölf . agentur für kommunikation GmbH, Wielandstraße 17, 60318 Frankfurt am Main
Herstellung: Görres-Druckerei und Verlag GmbH, Niederbieberer Str. 124, 56567 Neuwied
Bildnachweis: BVR, shutterstock