Anleitung für die Erstanmeldung im OnlineBanking

mit dem TAN Verfahren „VR SecureGo plus“

1. Voraussetzungen für den Ersteinstieg beim OnlineBanking

Das ist Ihre Ausgangssituation

Sie haben den OnlineBanking-Vertrag bereits unterschrieben und möchten zukünftig das Push-TAN Verfahren „VR SecureGo plus“ nutzen. Zunächst erhalten Sie von uns zwei separate Briefe, mit den nachfolgenden Informationen/Zugangsdaten:

- **VR-NetKey** (Benutzername für OnlineBanking)
- **PIN** (Passwort für OnlineBanking, nicht zu verwechseln mit PIN für girocard oder Kreditkarte)

2. Starten Sie mit der Einrichtung der VR SecureGo plus App

Schritt 1: Download der App

Bitte laden Sie die VR SecureGo Plus App aus ihrem App-Store auf Ihr Smartphone. Diese App benötigen Sie zur Generierung einer TAN zur Bestätigung aller Transaktionen. Die Installation können Sie ebenfalls mit dem nachfolgenden QR-Code durchführen.

Bitte lassen Sie Push-Nachrichten und Kameraanwendungen zu.

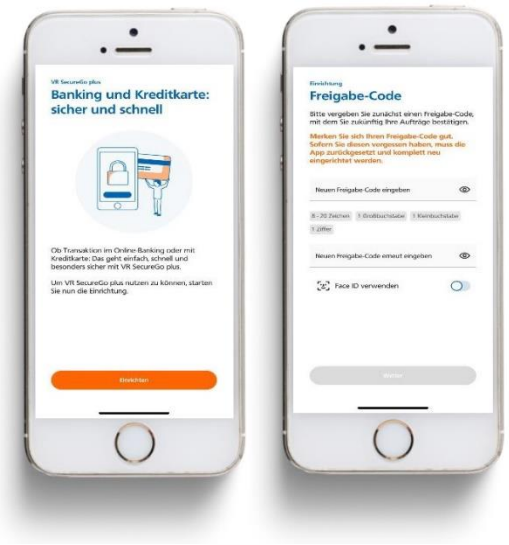
Hinweis: Sie können bis zu drei mobile Endgeräte (z.B. Smartphone und Tablet) gleichzeitig für VRSecureGo plus registrieren.

Schritt 2: Anmeldung in der VR SecureGo plus App

Öffnen Sie die App und vergeben Sie sich einen individuellen Freigabe-Code.

Hinweise zur Vergabe des Freigabe-Codes:

- mindestens ein Großbuchstabe
- mindestens ein Kleinbuchstabe
- mindestens eine Ziffer
- eine Kennwortlänge von mindestens 8 Zeichen (max. 20 Zeichen)



Wichtig: Ihren **individuellen Freigabe-Code** benötigen Sie bei der **Bestätigung zukünftiger Aufträge** in der VR SecureGo plus App.

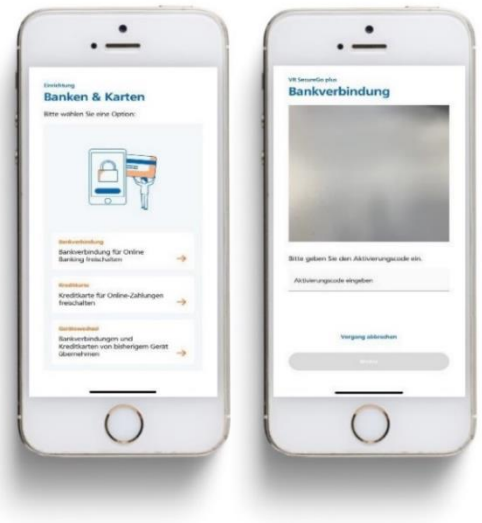
Volksbank Gronau-Ahaus eG

Anleitung für die Freischaltung des Online-Bankings

mit dem Push-TAN Verfahren „VR SecureGo plus“

Schritt 3: Registrierung in der VR SecureGo plus App

Wählen Sie im Menü „Bankverbindung für OnlineBanking freischalten“ und scannen Sie anschließend den Aktivierungscode im Anschreiben oder geben Sie ihn manuell ein.

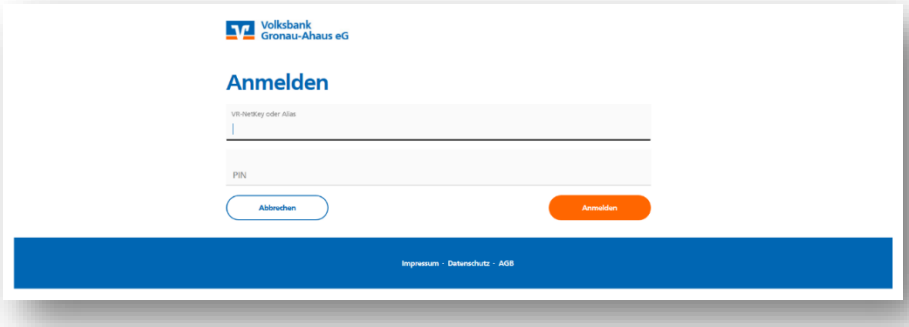


3. Weiter mit der Erstanmeldung im OnlineBanking

Schritt 1: Erstanmeldung im OnlineBanking

Für die Erstanmeldung im OnlineBanking rufen Sie die Internet-Adresse „www.vbga.de“ im **Internet-Browser auf Ihrem Computer/Laptop** auf. Klicken Sie rechts oben auf der Seite auf den Button „Login“. Danach klicken Sie bitte auf „Login Konto/ Depot“ (Hinweis: Ab dem 30.11.2021 wird die Bezeichnung in „VR OnlineBanking geändert).

In das obere Feld geben Sie bitte Ihren persönlichen VR-NetKey ein. In das Feld „PIN“ geben Sie bitte Ihre PIN ein, beide Zugangsdaten finden Sie auf den zwei erhaltenen Briefen. Klicken Sie nun auf „Anmelden“.

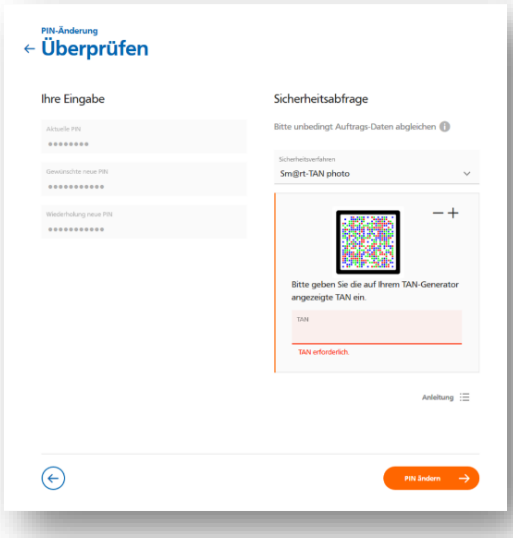


Schritt 2: Erst-PIN Änderung

Im Feld „gewünschte neue PIN“ geben Sie bitte eine von Ihnen frei gewählte PIN (= Passwort) am Computer / Laptop ein. Beachten Sie bitte die PIN-Regeln und wiederholen Sie die Eingabe Ihrer gewünschten PIN im Feld „Wiederholung neue PIN“. Klicken Sie bitte auf „Eingaben prüfen“.

Wichtig: Diese **PIN** geben Sie zukünftig bei **jeder Anmeldung** im OnlineBanking über Ihren Computer oder in der VR Banking App ein.

Für die Bestätigung Ihrer PIN erhalten Sie eine Nachricht in der VR SecureGo plus App.



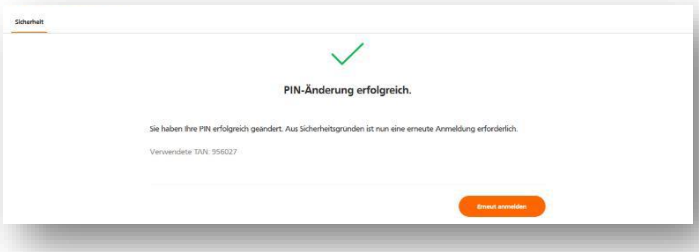
Volksbank Gronau-Ahaus eG

Anleitung für die Freischaltung des Online-Bankings

mit dem Push-TAN Verfahren „VR SecureGo plus“

Schritt 3: Erneut anmelden

Im nächsten Schritt fordert das System Sie dazu auf, sich neu im OnlineBanking anzumelden. Klicken Sie bitte auf „erneut anmelden“ und geben Sie Ihren VR-NetKey und Ihre neue PIN (= Passwort) ein.



Schritt 4: Einrichtung VR Banking App

Bitte laden Sie die VR Banking App in Ihrem App-Store herunter und installieren diese auf Ihrem Smartphone. Die Installation ist auch mittels der hier abgebildeten QR-Codes möglich:

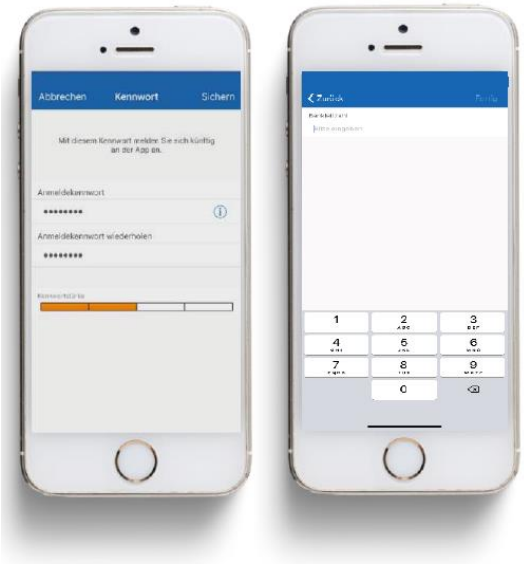
Bitte lassen Sie Push-Benachrichtigungen und Kameraanwendungen zu.

Schritt 5: Anmeldung in der VR Banking App

Öffnen Sie diese App und vergeben Sie sich ein App-Passwort für die VR Banking App.

Hinweis zur Vergabe des Anmeldekennworts:

- mind. 8 und max. 20 Zeichen lang
- mind. eine Ziffer
- einen Groß- und einen Kleinbuchstaben



Danach geben Sie unsere Bankleitzahl **40164024** ein. Jetzt geben Sie noch Ihren VR-NetKey und die geänderte PIN ein, die Sie sich im 2. Schritt „Erst-PIN Änderung“ vergeben haben.

Wichtig: Ihr **individuelles Anmeldekennwort** benötigen Sie bei **jeder Anmeldung** in der VR Banking App.

Tipp: Falls Sie auf Ihrem Smartphone Touch/Face ID verwenden, können Sie diese auch für die Anmeldung in der App aktivieren.

Folgende Zugangsdaten benötigten Sie zukünftig für die Nutzung des OnlineBankings:

1. **VR-NetKey** für OnlineBanking via Computer oder App
2. **PIN** für OnlineBanking via Homepage (und eventuell auch für die VR Banking App)
3. **Anmeldekennwort** für VR Banking App
4. **Freigabe-Code** für VR Secure-Go plus App

Volksbank Gronau-Ahaus eG

Anleitung für die Freischaltung des Online-Bankings

mit dem Push-TAN Verfahren „VR SecureGo plus“

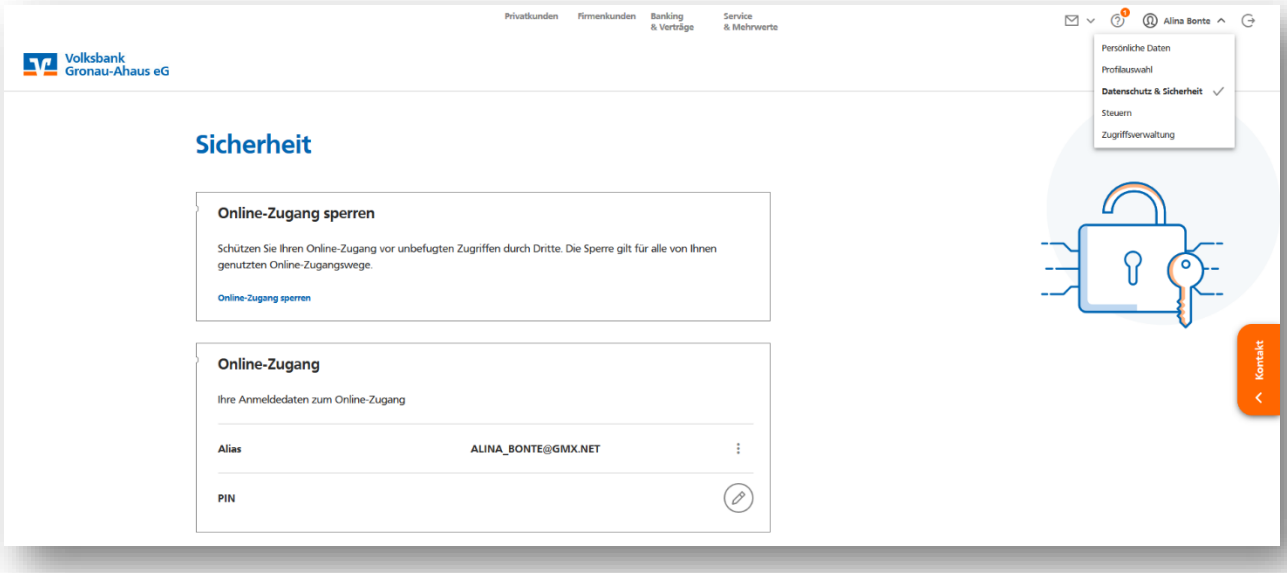
4. Weitere Tipps im OnlineBanking

Tipp 1: Einrichtung eines persönlichen Alias

Sofern gewünscht, können Sie sich statt des VR-NetKey einen persönlichen Alias (Benutzername) vergeben. Hierzu öffnen Sie das „Kopf“ Symbol und klicken dann „Datenschutz & Sicherheit“ an. Anschließend klicken Sie auf die drei Punkte im Bereich Alias.

Auf der nächsten Seite tragen Sie bitte Ihren gewünschten neuen Alias ein und wiederholen diesen im unteren Feld. Mit „Ändern“ beenden Sie den Vorgang.

Ab sofort können Sie sich im OnlineBanking mit dem eben eingerichteten Alias sowie Ihrer individuellen PIN einloggen.



Tipp 2: Nutzung einer eBanking-Software

Bitte hinterlegen Sie in Ihrer Software/App immer Ihren VR-NetKey. Ein Alias wird dort gegebenenfalls nicht akzeptiert.

Tipp 3: Mobiles Banking mit der VR Banking App

Bankgeschäfte auch unterwegs schnell und sicher erledigen

Mit der VR-Banking App haben Sie an jedem Ort Ihre Finanzen im Blick. Prüfen Sie problemlos Kontostände, die Umsätze Ihrer Kreditkarte oder veranlassen Sie eine Überweisung.

Anleitung für die Freischaltung des Online-Bankings

mit dem Push-TAN Verfahren „VR SecureGo plus“

Ihre Vorteile

- **Multibankenfähig**: Verwaltung Ihrer gesamten Konten – egal bei welcher Bank bzw. Bankengruppe Sie diese führen; Zugriff auf die Kontostände von HBCI-fähigen Konten und Überweisungen von allen eingebundenen Konten
- **Komfort und Sicherheit:** optimale Sicherheit durch Login mit Anmeldekennwort oder Fingerprint
- **Brokerage:** Depotübersicht mit Realtime-Kursen, aktuelle News und Ad-hoc-Nachrichten sowie die Möglichkeit, Wertpapiere zu kaufen oder zu verkaufen (Orderbuch)

Die Funktionen

- Finanzübersicht mit Umsatzdetails (auch Kreditkartenumsätze) und Kontobewegungen Ihrer gesamten Konten
- Rechnungen einfach abfotografieren und die Überweisung automatisch ausfüllen lassen mit Scan2Bank
- Automatische Push-Benachrichtigung bzw. Benachrichtigung per SMS bei Einsatz der Kreditkarte
- Übersicht Ihrer Produkte von Unternehmen der Genossenschaftlichen FinanzGruppe Volksbanken Raiffeisenbanken (Online-Finanzstatus)
- Überweisungen durchführen, Daueraufträge einrichten oder löschen
- Geschäftsstellen und Geldautomaten innerhalb Deutschlands finden
- Postfach als zentraler und sicherer Eingangskanal für die Online-kommunikation zwischen Ihnen und Ihrer Volksbank Gronau-Ahaus

Tipp 4: VR SecureGo plus auf ein neues Gerät umziehen

Der Prozess bei einem Gerätewechsel und der für die erstmalige Installation bzw. Registrierung sind identisch. Sie können die Freischaltung allerdings mit einer TAN direkt abschließen.

Wenn Sie keine TAN mehr empfangen oder erstellen können, dann benötigen Sie von uns einen neuen Aktivierungscode, um die Schritte 1 und 2 zu wiederholen. In diesem Fall nehmen Sie bitte Kontakt mit uns auf.

Haben Sie noch Fragen zum OnlineBanking außerhalb unserer Öffnungszeiten?

Unsere ServiceFiliale unterstützt Sie gerne bei Fragen zum OnlineBanking telefonisch von Montags bis Freitags von 8:00 Uhr bis 18:00 Uhr unter **02562 914-0**.

5. Wichtige Sicherheitshinweise

Prüfen Sie die Echtheit der Bank-Website
Achten Sie darauf, dass Sie auch tatsächlich auf der Seite Ihrer Bank sind. Geben Sie die Internetadresse Ihrer Bank bei jedem Einstieg erneut über die Tastatur ein. Wenn Sie beim Login nach einer TAN gefragt werden, befinden Sie sich mit Sicherheit auf einer **gefälschten Seite!** Generell verdächtig sind Seiten, deren Adresse mit einer Nummer und keinem Domain-Namen beginnt (z. B.: http://1357.246.579/...) oder Seiten, in deren Adresse der Name Ihres Geldinstituts nur „eingebaut" ist (z. B.: http://Musterbank.Domainname.de).

Wählen Sie Zugangsdaten sorgfältig aus und gehen Sie vorsichtig damit um
Wenn beim Online-Banking Passwörter zum Einsatz kommen, dann wählen Sie schwer zu erratende Buchstaben-/Zahlenkombinationen. Schützen Sie Kennwörter und Zugangsdaten wie PIN und TAN vor dem Zugriff Dritter und speichern Sie solche Kennungen keinesfalls ab - auch nicht im Passwort-Manager!

Betreiben Sie Online-Banking soweit möglich nur von eigenen Geräten aus
Vorsicht ist insbesondere bei öffentlich zugänglichen Computern wie etwa in Internetcafés geboten. Melden Sie sich nach jeder Online-Banking-Sitzung ab („Logout") und löschen Sie nach der Beendigung von Banktransaktionen den Zwischenspeicher (Cache) Ihres Computers. Im Internetexplorer wählen Sie dazu die „Internetoptionen" im Menü „Extras". Im Abschnitt „Temporäre Internetdateien" betätigen Sie nun den Befehl „Dateien löschen" - achten Sie darauf, dass die Option „Alle Offlineinhalte löschen" angeklickt ist! Bei Netscape finden Sie die betreffenden Befehle in der Browserleiste unter „Bearbeiten" in den „Einstellungen", und zwar unter „Erweitert". Bei Firefox klicken Sie in der Browserleiste auf „Extras" und dann auf „Einstellungen". Die Möglichkeit, den Cache zu löschen, finden Sie dort unter „Datenschutz".

Setzen Sie nur Programme aus vertrauenswürdiger Quelle ein
Generell sollten Sie darauf achten, keine Software aus unseriösen oder unsicheren Quellen auf Ihrem Computer zu speichern. Diese können mit schädlichen Programmen wie etwa Spyware versehen sein, die Ihr Gerät ausspionieren. Zu den gefährlichen Tools zählen beispielsweise einige Surf-Turbos, die das Mitlesen durch Fremde ermöglichen.

Schützen Sie Ihren PC vor unerlaubten Zugriffen.
Nutzen Sie die Möglichkeiten, die Ihr Betriebssystem für den Schutz Ihrer Festplatte vorsieht: Definieren Sie beispielsweise ein Passwort, das beim Starten oder auch vom Bildschirmschoner abgefragt wird.

Setzen Sie aktuelle Virenschutzsoftware und Firewalls ein.
Die Programme zum Schutz vor Infektionen im Internet werden laufend aktualisiert. Stellen Sie sicher, dass Sie die Updates immer von den Seiten Ihres Softwareanbieters herunterladen und installieren.

Spielen Sie aktuelle Sicherheitsupdates für Ihr Betriebssystem ein
Immer wieder treten in Betriebssystemen Sicherheitslücken auf, die durch Aktualisierungen geschlossen werden. Sie sollten daher darauf achten, die Patches regelmäßig von der Internetseite der Hersteller herunter zu laden und zu installieren.

Sicherheitshinweise für Einstellungen und Downloads

- Beziehen Sie Ihre Apps nur aus sicheren und vertrauenswürdigen Quellen, zum Beispiel aus dem Apple App Store oder aus dem GooglePlay Store.
- Achten Sie auf die Herstellerbezeichnung „Atruvia AG".
- Halten Sie das Betriebssystem Ihres Smartphones bzw. Tablets immer auf dem aktuellen Stand.
- Verwenden Sie stets die aktuelle Version der jeweiligen App bzw. des Programms.

Überprüfen Sie regelmäßig Ihre Kontenbewegungen

Falls Ihnen etwas unschlüssig erscheint, sollten Sie so schnell wie möglich reagieren und sich mit Ihrer Bank in Verbindung setzen.

Vereinbaren Sie mit Ihrer Bank ein Limit für tägliche Geldbewegungen beim Online-Banking

Durch einen gemeinsam mit Ihrem Kreditinstitut fixierten Höchstbetrag können Sie sicherstellen, dass Betrüger nicht unbemerkt hohe Summen von Ihrem Konto abbuchen.

Reagieren Sie nicht auf Phishing-Mails!

Ihre Bank fordert Sie niemals per E-Mail dazu auf, vertrauliche Daten wie PIN, TAN, Freigabe-Code oder Kontonummer bekannt zu geben. Falls Sie derartige Nachrichten erhalten, informieren Sie Ihre Bank darüber - aber folgen Sie keinesfalls den in der E-Mail enthaltenen Anweisungen.

Bitte beachten Sie, dass die Volksbank Gronau-Ahaus

- KEINE Testüberweisungen durchführen lässt.
- KEINE Rücküberweisungen durchführen lässt.
- Sie NIEMALS dazu auffordern wird, ein Demo-Konto innerhalb unserer Online-Filiale zu eröffnen oder sich in eines einzuloggen.

Sperren Sie Ihren Online-Banking-Zugang, wenn Ihnen etwas verdächtig vorkommt.

Das können Sie entweder telefonisch bei der Bank erledigen oder über die entsprechende Funktion im OnlineBanking-Fenster.

Noch mehr Sicherheit – Informationen zu Ihrem Schutz

Noch mehr Informationen zum Thema Sicherheit finden Sie auf unseren Internetseiten unter der Rubrik: **Banking & Service – Sicherheit**. Hier finden Sie wichtige Hinweise zu Phishing-Attacken und Trojanern im Online-Banking und Informationen dazu, wie Sie sich schützen können.