Instructies voor de eerste registratie in OnlineBanking

met de TAN-procedure "VR SecureGo plus"

1. Vereisten om aan de slag te gaan met OnlineBanking

Dit is uw uitgangssituatie

U heeft het OnlineBanking contract al getekend en wilt in de toekomst de Push-TAN procedure "VR SecureGo plus" gebruiken. Om te beginnen, ontvangt u van ons twee aparte brieven, met de volgende informatie/toegangsgegevens:

- **VR-NetKey** (gebruikersnaam voor OnlineBanking)
- **PIN** (wachtwoord voor OnlineBanking, niet te verwarren met de pincode voor bankpas of creditcard)

2. Begint u met het instellen van de VR SecureGo plus app

Stap 1: Download de app

Download de VR SecureGo plus app van uw app-store naar uw smartphone. Deze app heeft u nodig om een TAN te genereren voor het bevestigen van alle transacties. U kunt installatie van de app ook uitvoeren met onderstaande QR-code.

Sta pushberichten en cameratoepassingen toe op uw smartphone.

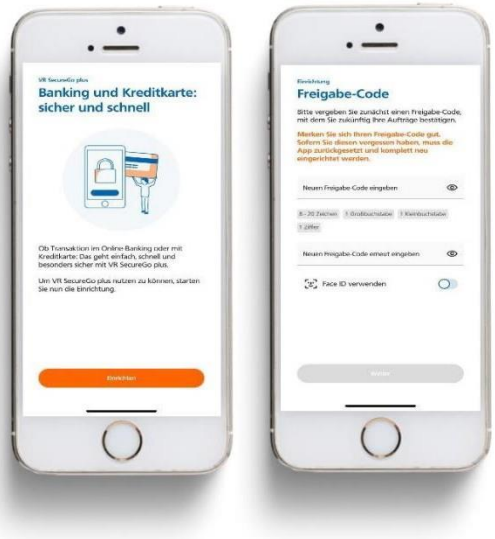
Opmerking: U kunt VR SecureGo plus maximaal op drie mobiele apparaten tegelijk gebruiken (bijv. smartphone en tablet).

Stap 2: Registratie in de VR SecureGo plus app

Open de app en wijs uzelf een individuele goedkeuringscode toe.

Opmerkingen over het samenstellen van de goedkeuringscode:

- tenminste één hoofdletter
- tenminste één kleine letter
- tenminste één cijfer
- een woordlengte van minimaal 8 tekens (max. 20 tekens)



Belangrijk: u heeft uw **individuele goedkeuringscode (Freigabe** nodig bij het **bevestigen van toekomstige opdrachten** in de VR SecureGo plus app.

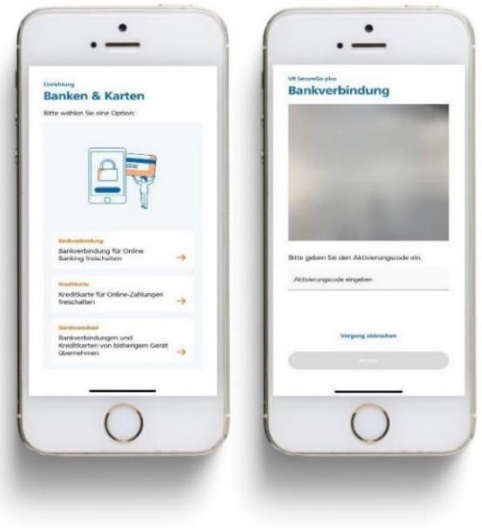
Volksbank Gronau-Ahaus eG

Instructies voor het activeren van Online-Banking

met de Push-TAN procedure "VR SecureGo plus"

Stap 3: Registratie in de VR SecureGo plus app

Selecteer in het Menu: "Bankgegevens voor OnlineBanking ontgrendelen" en scan vervolgens de activeringscode vanuit de begeleidende brief of voer deze handmatig in.

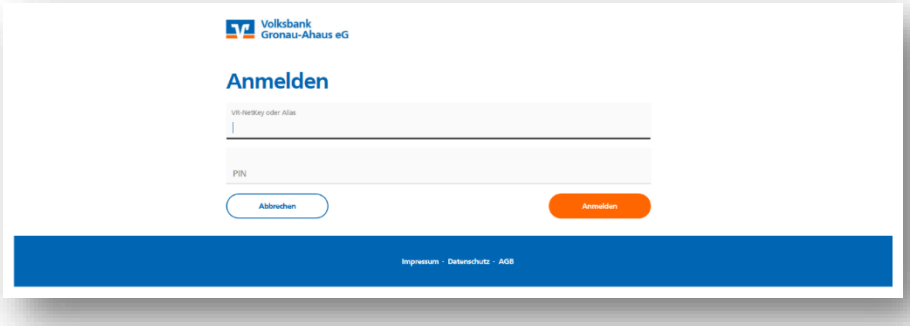


3. Verder gaan met de eerste registratie in OnlineBanking

Stap 1: Eerst keer aanmelden bij OnlineBanking

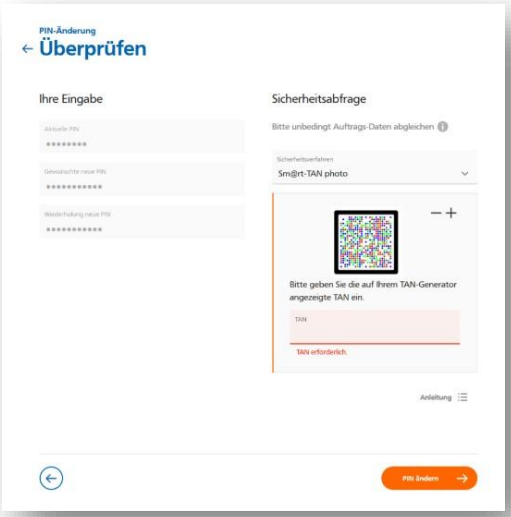
Om u voor de eerste keer aan te melden bij OnlineBanking, gaat u naar het internetadres “www.vbga.de“ in de **internetbrowser op uw computer/laptop**. Klik op de knop "Inloggen" rechtsboven op de pagina. Klik daarna op “Inloggen Rekening / Depot” (Let op: Vanaf 30 november 2021 wordt de naam gewijzigd in “VR OnlineBanking”).

Voer in het bovenste veld uw persoonlijke VR-NetKey in. Voer in het veld "PIN" uw PIN in. Beide toegangsgegevens vindt u in de twee brieven die u heeft ontvangen. Klik nu op "Aanmelden".



Stap 2: Wijzigen eerste PIN

In het veld "Gewenste nieuwe PIN" voert u op de computer/laptop een geheel vrij door u te kiezen PIN (= wachtwoord) in . Houdt u a.u.b. rekening met de PIN-regels en herhaal de door u gewenste PIN in het veld "Herhaal nieuwe PIN". Klik op "Invoer controleren".



Belangrijk: Deze **PIN** geeft u voortaan elke keer in, als u zich aanmeldt bij OnlineBanking via uw computer of in de VR Banking app.

U ontvangt in de VR SecureGo plus app een bericht om uw PIN te bevestigen.

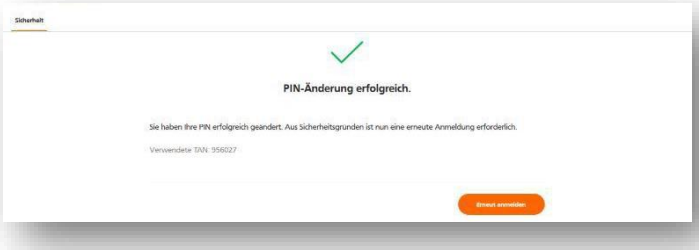
Volksbank Gronau-Ahaus eG

Instructies voor het activeren van Online-Banking

met de Push-TAN procedure "VR SecureGo plus"

Stap 3: Opnieuw aanmelden

In de volgende stap vraagt het systeem u om u opnieuw aan te melden bij OnlineBanking. Klik op "Opnieuw aanmelden" en voer uw VR-NetKey en uw nieuwe PIN (= wachtwoord) in.



Stap 4: De VR Banking app instellen

Download de VR Banking app vanuit uw app store en installeer hem op uw smartphone. Installeren is ook mogelijk met behulp van de hier afgebeelde QR-codes:

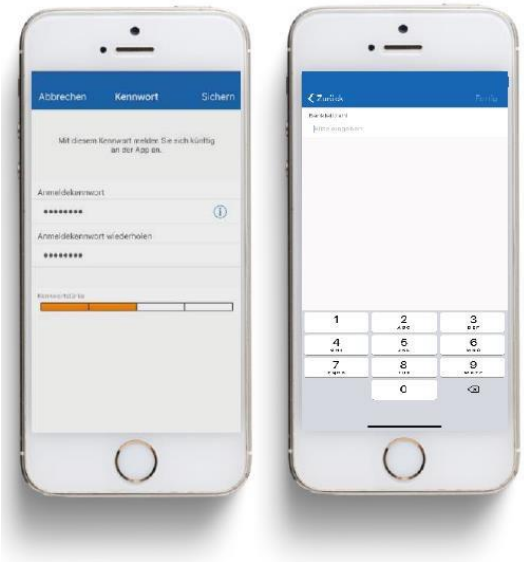
Sta pushmeldingen en cameratoepassingen toe.

Stap 5: Registreren in de VR Banking app

Open de app en wijs uzelf een app-wachtwoord toe voor de VR Banking app.

Opmerking over het kiezen van het inlogwachtwoord:

- tenminste 8 en maximaal 20 tekens lang
- tenminste één cijfer
- een hoofdletter en een kleine letter



Daarna vult u onze Bankcode **40164024** in. Voer nu uw VR-NetKey en de gewijzigde PIN in, die u heeft opgeslagen bij de tweede stap "Eerste PIN wijzigen".

Belangrijk: **Elke keer dat u inlogt** in der VR Banking app, heeft u uw **individuele inlogwachtwoord** nodig.

Tip: Wilt u Touch/Face ID op uw smartphone gebruiken, dan kunt u dit activeren om ermee in te loggen in de app.

Om in de toekomst gebruik te kunnen maken van OnlineBanking, heeft u de volgende toegangsgegevens nodig:

1. VR-NetKey voor OnlineBanking via computer of app
2. PIN voor OnlineBanking via Homepage (en eventueel ook voor de VR Banking app)
3. Inlogwachtwoord voor de VR Banking app
4. Goedkeuringscode voor de VR Secure-Go plus app

Volksbank Gronau-Ahaus eG

Instructies voor het activeren van Online-Banking

met de Push-TAN procedure "VR SecureGo plus"

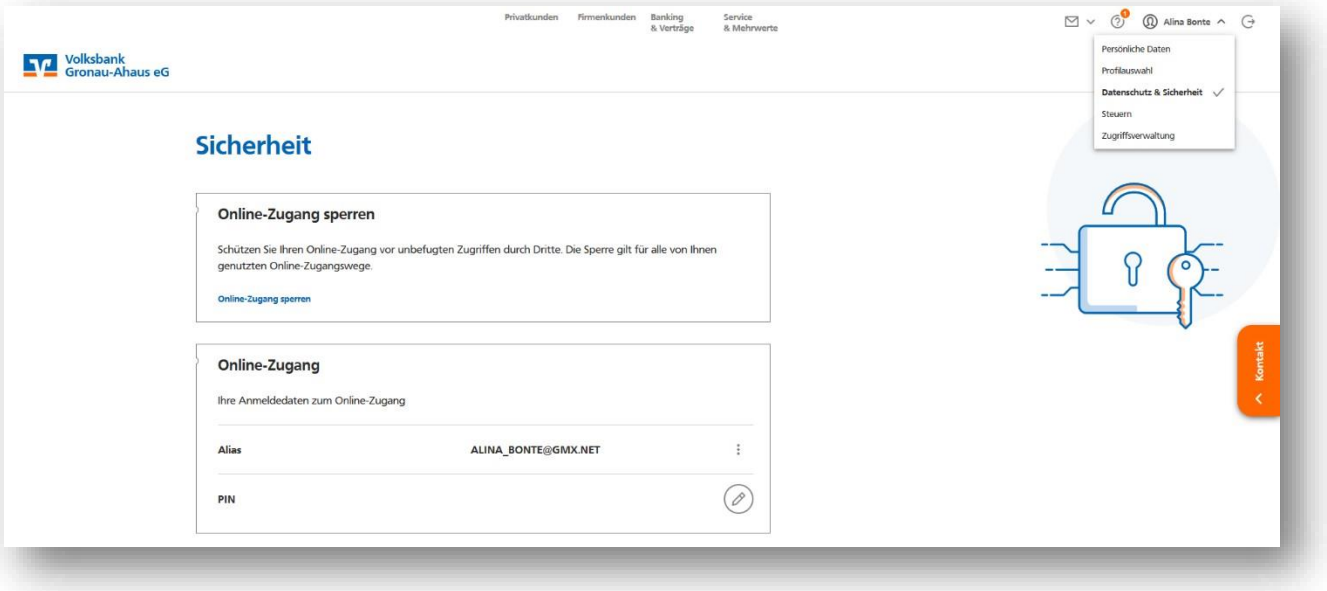
4. Meer tips voor OnlineBanking

Tip 1: stel een persoonlijke alias in

Indien gewenst, kunt u in plaats van de VR-NetKey kiezen voor een persoonlijke alias (gebruikersnaam). Open hiervoor het "Kop"-symbool en klik vervolgens op “Gegevensbescherming en -beveiliging". Klik vervolgens op de drie punten in het Alias-gebied.

Voer op de volgende pagina uw gewenste nieuwe alias in en herhaal dit in het onderste veld. Met "Wijzigen" beëindigt u het proces.

U kunt nu met de alias die u zojuist heeft ingesteld - in combinatie met uw persoonlijke PIN - inloggen bij OnlineBanking.



Tip 2: eBanking-software gebruiken

Gebruik in uw software/app altijd uw VR-NetKey. Een alias wordt daar niet geaccepteerd.

Tip 3: Mobiel bankieren met de VR Banking app

Banktransacties snel en veilig uitvoeren terwijl u onderweg bent

Met de VR Banking app heeft u altijd een overzicht van uw financiën, waar u ook bent. Controleer eenvoudig het saldo op uw rekening of de transacties met uw creditcard, of doe een overboeking.

Instructies voor het activeren van Online-Banking

met de Push-TAN procedure "VR SecureGo plus"

Uw voordelen

- **Geschikt voor meerdere banken:** Beheer van al uw rekeningen – ongeacht bij welke bank u een rekening heeft; toegang tot de rekeningsaldi van HBCI-geactiveerde rekeningen en overschrijvingen van alle geïntegreerde rekeningen
- **Gemak en veiligheid:** optimale beveiliging door inloggen met aanmeldwachtwoord of vingerafdruk
- **Brokerage:** portefeuilleoverzicht met realtime koersen, actueel nieuws en ad hoc nieuws, alsook de mogelijkheid om effecten te kopen of te verkopen (orderboek)

De functies

- Financieel overzicht met transactiegegevens (inclusief creditcardtransacties) en mutaties op al uw rekeningen
- Facturen eenvoudig fotograferen en de overschrijving automatisch laten invullen met Scan2Bank
- Automatisch pushberichten of meldingen per sms ontvangen bij gebruik van de creditcard
- Overzicht van uw producten bij de ondernemingen van het coöperatieve financiële netwerk Volksbanken Raiffeisenbanken (online financiële status)
- Overschrijvingen uitvoeren, doorlopende opdrachten instellen of verwijderen
- Makkelijk filialen en geldautomaten vinden in Duitsland
- Postvak - als centraal en veilig toegangskanaal voor online communicatie tussen u en uw Volksbank Gronau-Ahaus

Tip 4: VR SecureGo plus overzetten naar een nieuw apparaat

Het proces van het overzetten naar een ander apparaat is hetzelfde als het proces voor de eerste installatie en registratie. U kunt de activering echter direct voltooien met een TAN-code.

Als u geen TAN-code meer ontvangt of kunt aanmaken, heeft u een nieuwe activeringscode van ons nodig om stap 1 en 2 te herhalen. Neemt u in dat geval contact met ons op!

Heeft u buiten onze openingstijden nog vragen over OnlineBanking?

Ons ServiceFiliaal helpt u bij vragen over OnlineBanking graag telefonisch verder, van maandag tot en met vrijdag van 8:00 bis 18:00 uur, op **02562 914-0**.

Volksbank Gronau-Ahaus eG

5. Belangrijke veiligheidsinstructies

Controleer de echtheid van de website van de bank

Zorg ervoor dat u er zeker van bent, dat u ook daadwerkelijk op de website van de bank bent. Voer elke keer dat u naar de webpagina gaat, via uw toetsenbord, het internetadres van uw bank in. Als u bij het inloggen om een TAN-code wordt gevraagd, dan is het zeker dat u zich op **een vervalste pagina** bevindt**!** Over het algemeen zijn pagina's, waarvan het adres met een nummer en niet met een domeinnaam begint, verdacht (bijv. http://1357.246.579/...) of pagina's, waarbij in het adres de naam van uw financiële instelling alleen is "ingebouwd" (bijv. http://Voorbeeldbank.Domeinnaam.nl).

Kies uw inloggegevens zorgvuldig en ga er voorzichtig mee om

Als bij OnlineBanking wachtwoorden gebruikt worden, kies dan moeilijk te raden combinaties van letters en cijfers. Scherm wachtwoorden en toegangsgegevens zoals PIN en TAN-codes altijd af tegen toegang door derden en sla dergelijke gegevens in geen geval op - ook niet in de wachtwoordmanager!

Gebruik OnlineBanking zoveel mogelijk uitsluitend vanaf uw eigen apparaten

Bijzondere voorzichtigheid is geboden bij computers die publiekelijk toegankelijk zijn, zoals in internetcafés. Log iedere keer uit, nadat u OnlineBanking gebruikt heeft (“Uitloggen”) en verwijder na het voltooien van banktransacties de cache van uw computer. Selecteer hiervoor in Internet Explorer "Internetopties" in het menu "Extra". Klik in het gedeelte "Tijdelijke internetbestanden" op de opdracht "Bestanden verwijderen" - Zorg ervoor dat de optie "Alle offline inhoud verwijderen" is aangeklikt! Bij Netscape vindt u de betreffende commando's in de browserbalk, onder "Bewerken" in de "Instellingen" onder "Geavanceerd". Klik in Firefox op "Extra" in de browserbalk en vervolgens op "Instellingen". De optie om de cache te wissen vindt u daar onder "Gegevensbescherming".

Gebruik alleen programma's, afkomstig van een betrouwbare bron

Over het algemeen moet u oppassen, dat u geen software van dubieuze of onveilige bronnen op uw computer opslaat. Deze kunnen schadelijke programma's, zoals spyware, bevatten, die uw apparaat bespioneren. Tot de gevaarlijke tools horen bijvoorbeeld enkele surfturbo's, die het mogelijk maken dat vreemden meelezen.

Bescherm uw pc tegen onbevoegde toegang.

Maak gebruik van de mogelijkheden die uw besturingssysteem biedt om uw harde schijf te beschermen: u kunt bijvoorbeeld een wachtwoord definiëren dat wordt gevraagd bij het opstarten van het systeem of door de screensaver.

Gebruik de nieuwste antivirussoftware en firewalls.

De programma's ter bescherming tegen infecties op internet worden voortdurend bijgewerkt. Zorg ervoor, dat u de updates altijd downloadt en installeert vanaf de website van uw softwareleverancier.

Pas de nieuwste beveiligingsupdates voor uw besturingssysteem toe

Steeds opnieuw treden er beveiligingslekken op in besturingssystemen, die door de updates weer worden gedicht. Zorg er daarom voor, dat u regelmatig de patches downloadt en installeert vanaf de website van de fabrikant.

Veiligheidsinstructies voor instellingen en downloads

- Haal uw app's alleen uit veilige en betrouwbare bronnen, bijvoorbeeld de Apple App Store of de GooglePlay Store.
- Let op de aanduiding van de fabrikant "Atruvia AG".
- Zorg ervoor dat het besturingssysteem van uw smartphones of tablets altijd up-to-date is.
- Gebruik altijd de nieuwste versies van de betreffende app of het programma.

Controleer regelmatig uw rekeningbewegingen

Als u iets ziet dat volgens u niet klopt, dan moet u zo snel mogelijk reageren en contact opnemen met uw bank.

Spreek met uw bank een limiet af voor dagelijkse geldbewegingen in OnlineBanking

Door samen met uw bank een maximumbedrag in te stellen, zorgt u ervoor dat fraudeurs geen grote bedragen van uw rekening kunnen afschrijven.

Reageer niet op phishingmails!

Uw bank zal u nooit per e-mail vragen om vertrouwelijke gegevens zoals PIN, TAN-code, goedkeuringscode of rekeningnummer te verstrekken. Als u dergelijke berichten ontvangt, informeer dan onmiddellijk uw bank en volg zeker niet de instructies in de e-mail op.

Houd er rekening mee, dat Volksbank Gronau-Ahaus

- GEEN proefoverdrachten laat doorvoeren.
- GEEN geldovermakingen laat doorvoeren.
- U NOOIT zal vragen om binnen ons online filiaal een demo-account te openen of er op in te loggen .

Blokkeer uw toegang tot internetbankieren meteen, als u iets verdachts vindt.

Dit kunt u doen door de bank te bellen, of door de bijbehorende functie in het venster OnlineBanking te gebruiken.

Nog meer veiligheid - Informatie voor uw bescherming

Nog meer informatie over het onderwerp veiligheid vindt u op onze website, onder het kopje: **Banking & Service – Beveiliging.** Hier vindt u belangrijke informatie over phishing-aanvallen en Trojaanse paarden bij OnlineBanking, plus informatie over hoe u uzelf kunt beschermen.