

## Gerätewechsel von SecureGo bzw. Umstellung auf SecureGo

Sehr geehrte Kundin, sehr geehrter Kunde,  
mit dieser Anleitung erläutern wir Ihnen die Vorgehensweise beim Gerätewechsel von SecureGo. Bitte installieren Sie zunächst die SecureGo-App.

SecureGo QR-Code für iOS



SecureGo QR-Code für Android



Das SecureGo-Verfahren kann in Kombination mit der VR Banking-App ebenso wie das Online-Banking über unsere Internetseite bzw. Onlinebankingsoftware genutzt werden. Ein höheres Sicherheitsniveau wird durch die Nutzung von zwei Geräten (PC und Smartphone bzw. Tablet) erreicht.

VR-Banking-App  
QR-Code für iOS

App für iPhone



VR-Banking-App  
QR-Code für Android

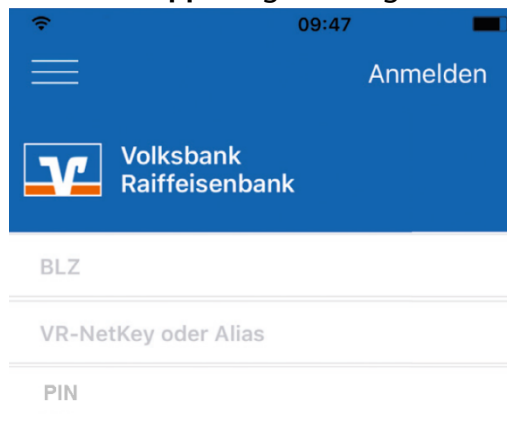
VR-BankingApp



VR-Banking-App  
QR-Code für iPad



### 1. SecureGo-App - Registrierung zum SecureGo-Verfahren



The screenshot shows the registration screen of the SecureGo app. At the top, there is a blue header with the Volksbank Raiffeisenbank logo and the text 'Anmelden'. Below the header, there are three input fields: 'BLZ', 'VR-NetKey oder Alias', and 'PIN'. The time '09:47' is visible in the top right corner of the screen.

Starten Sie die zuvor installierte SecureGo-App.


Als nächstes geben Sie die Bankleitzahl **72090000** und Ihre persönliche **VR-NetKey-Nummer** ein.

Des Weiteren geben Sie Ihre persönliche VR-NetKey PIN ein und tippen auf **Anmelden**.

Abbrechen Kennwort Sichern

Mit diesem Kennwort melden Sie sich künftig an der App an.


Anmeldekennwort

..... 

Anmeldekennwort wiederholen

.....

Kennwortstärke



Die SecureGo-App muss aus Sicherheitsgründen mit einem Anmeldekennwort versehen werden.

- Mindestens 1 Großbuchstabe
- Mindestens 1 Kleinbuchstabe
- Mindestens 1 Ziffer
- Mind. 8 Zeichen, max. 20 Zeichen

Neben den Mindestanforderungen sind auch die am Smartphone/Tablet verfügbaren Sonderzeichen möglich, damit erhöht sich die Kennwortstärke.

11:21 92%

VR-SecureGo


Bankleitzahl: 69968602 VR-NetKey: 147386022

Die SecureGo App muss zuerst registriert und anschließend freigeschaltet werden.

Bitte beachten Sie, dass für SecureGo Gebühren anfallen können. Informationen finden Sie im Preis- und Leistungsverzeichnis.

Nach Freischaltung der App:  
- mobileTAN nicht mehr nutzbar  
- Sm@rt-TAN plus weiterhin nutzbar

Zustimmung zu den Sonderbedingungen

 Sonderbedingungen


App registrieren

Stimmen Sie den Sonderbedingungen zu und tippen Sie auf **App registrieren**. Dadurch wird die sicherheitstechnische Bindung zwischen Ihrem Smartphone/Tablet, der VR-SecureGo-App und Ihrem VR-NetKey hergestellt.



Hinweis

Sie haben die App VR-SecureGo erfolgreich registriert. Die App-ID lautet 8AXTVKN3. Für die Freischaltung der App erhalten Sie Ihren Freischaltcode per Post zugesendet. Nach Erhalt können Sie dann in einem zweiten Schritt Ihre SecureGo-App freischalten.



Ihren persönlichen Freischaltcode erhalten Sie dann per Post.

## 2. SecureGo-App - SecureGo aktivieren

Der Freischaltcode wird Ihnen mit der Post zugestellt.

Ihr Freischaltcode für SecureGo:

VR-NetKey: 234706363

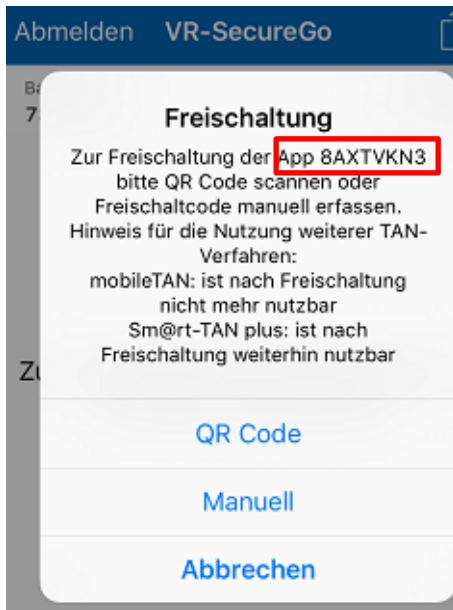
Inhaber: Max Mustermann

Folgenummer: 89

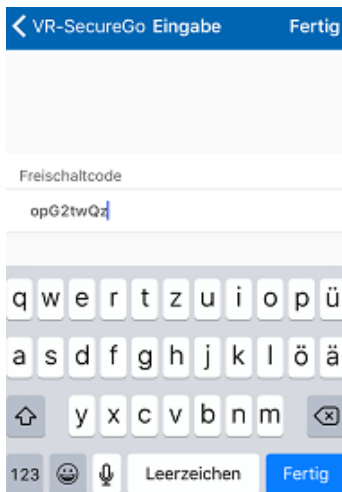
Kundennummer: 0123456789

Freischaltcode für die App.-ID.: **8AXTVKN3**

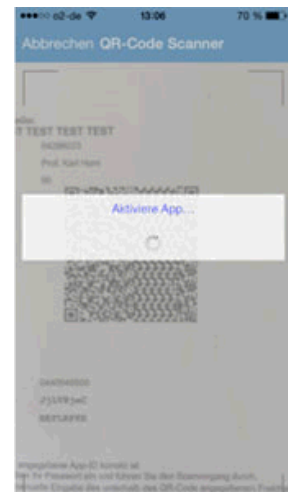




Für die Eingabe **starten Sie die SecureGo-App** und geben Ihr **Anmeldekennwort** ein. In der nachfolgenden Maske muss die angezeigte App-ID mit der Angabe im Freischaltcode übereinstimmen.



Der Freischaltcode kann entweder als QR-Code eingelesen oder manuell eingegeben werden.



Nach erfolgreicher Freischaltung ist die SecureGo-App auf Ihrem vorherigen mobilen Endgerät deaktiviert und kann nicht mehr genutzt werden.

### Bitte beachten Sie nachfolgende Sicherheitshinweise SecureGo bzw. VR-Banking-App

- Ihre VR Bank Augsburg-Ostallgäu eG versendet grundsätzlich keine E-Mails, in denen Kunden dazu aufgefordert werden, ihre Kontodaten, Online-Banking Zugangsdaten oder SecureGo Freischaltcodes einzugeben. Reagieren Sie nicht auf solche E-Mail-Anfragen und löschen Sie diese sofort.
- Beziehen Sie Ihre Apps nur aus sicheren und vertrauenswürdigen Quellen, zum Beispiel iTunes oder GooglePlay Store.
- Achten Sie auf die Herstellerbezeichnung bei den Apps, zum Beispiel „Fiducia & GAD IT AG“ für VR-SecureGo.
- Halten Sie das Betriebssystem Ihres Smartphones bzw. Tablets immer auf dem aktuellen Stand.
- Verwenden Sie stets die aktuelle Version der jeweiligen App.
- Kontrollieren Sie regelmäßig Ihre Kontoauszüge und informieren Sie bei Unregelmäßigkeiten sofort Ihre kontoführende Bank.

- Sperren Sie Ihren Online-Banking-Zugang sofort, wenn Ihnen etwas verdächtig vorkommt.
- Öffnen Sie keine E-Mails oder SMS unbekannter Herkunft mit Anhängen oder Download-Links.
- Sie können auch mittels Drittanbietern auf Ihr Girokonto zugreifen und diese beauftragen, für Sie Zahlungen auszulösen oder Kontoinformationen abzurufen. Da diese Drittanbieter nunmehr gesetzlich reguliert und beaufsichtigt werden, dürfen Sie Ihre Online-PIN und -TAN bei einem von Ihnen gewählten Drittanbieter verwenden. Sofern Sie Drittanbieter nutzen, empfehlen wir Ihnen, diese sorgfältig auszuwählen.
- Stellen Sie eine Internetverbindung nur über vertrauenswürdige Netze her, insbesondere bei unbekanntem Netzwerken wie zum Beispiel öffentlichen WLANs.
- Geben Sie Passwörter nur unbeobachtet ein.
- Wichtig: Bitte überprüfen Sie zu Ihrer Sicherheit bei jeder Transaktion die Daten in der Push-Nachricht, die Sie erhalten haben. In der Push-Nachricht werden Ihnen der Betrag und die IBAN des Empfängers angezeigt. Sollte hier etwas nicht passen, geben Sie die TAN-Nummer NICHT ein, brechen Sie den Vorgang ab und kontaktieren Sie Ihren Berater.