

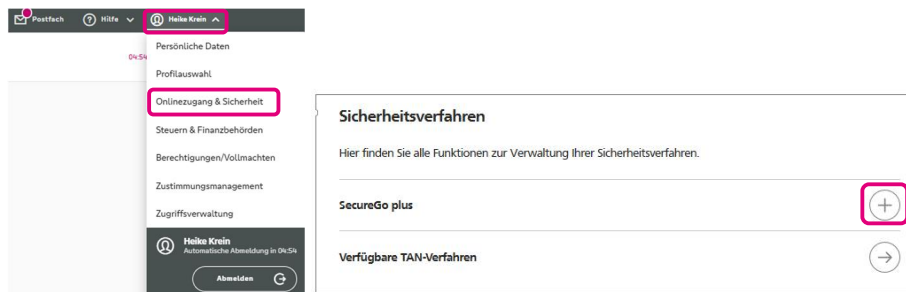
Umstellung auf das PIN/TAN-Verfahren mit VR-SecureGo plus

Gehen Sie beim Onlinebanking auf Nummer sicher – und machen Sie es sich noch bequemer, denn mit der neuen **VR SecureGo plus App** geben Sie Transaktionen ganz einfach frei. Sie benötigen lediglich ein Smartphone oder Tablet, auf dem die VR-SecureGo plus-App installiert ist. Sie können dieses Sicherheitsverfahren in Verbindung mit unserer Online-Filiale, der **VR Banking App** bzw. einem Zahlungsverkehrsprogramm nutzen.

Bitte prüfen Sie die angezeigten Daten auf Richtigkeit und bestätigen Sie den Vorgang mit dem von Ihnen gewählten Freigabe-Passwort (ggf. biometrisches Merkmal). Bestätigen Sie niemals Daten, deren Ausführung Sie nicht wünschen.

Aktivierungscode anfordern

Melden Sie sich bitte über www.dkm.de **Zum OnlineBanking** an. Klicken Sie im Bereich **Onlinezugang & Sicherheit** beim **Sicherheitsverfahren** auf das **+ Zeichen** bei SecureGo plus und anschließend auf **+ Gerät hinzufügen**.



Wählen Sie aus, wofür das Gerät genutzt werden soll (Online-Banking und ggf. Online Kartenzahlung). Stimmen Sie anschließend den Sonderbedingungen zu und akzeptieren Sie die Preise (b.a.W. ist die Verwendung kostenlos). Vergeben Sie anschließend einen Gerätenamen und wählen Sie **Weiter**. Bestätigen Sie dieses mit einer TAN, die Sie über ihr bisheriges TAN-Medium erhalten.

SecureGo plus - Geräteverwaltung
← **Gerät hinzufügen**

Wie soll das Gerät heißen?

Gewünschter Geräte Name: 10/35

Regeln für den Gerätenamen:
Der Gerätename muss aus mindestens 5 Zeichen bestehen und kann maximal 35 Zeichen lang sein. Zulässig sind alle Buchstaben, Ziffern und die Sonderzeichen: - _ . @.

Wie wollen Sie den Aktivierungscode erhalten?

☒ Online anzeigen

☐ Per Post

Bitte laden Sie sich die VR SecureGo plus App auf Ihr Smartphone.

Installation für Android

Installation für iOS

Wichtiger Sicherheitshinweis
Ihre Bank wird Sie niemals nach Ihren Zugangsdaten wie PIN, TAN, Freischaltcode, Aktivierungscode oder Entsperrcode fragen. Weder per E-Mail, SMS, telefonisch, noch persönlich. Geben Sie Ihre Zugangsdaten niemals weiter. Wenn Sie dazu aufgefordert werden, setzen Sie sich bitte umgehend mit uns in Verbindung.

← Abbrechen Weiter →

Installation der VR-SecureGo plus App



Laden Sie VR-SecureGo plus über den App-Store auf ihr Smartphone oder Tablet. Die App ist für Systeme mit Android und iOS verfügbar.

Klicken Sie auf **Einrichten**, legen Sie ein individuelles **Freigabe-Passwort** fest und bestätigen Sie dieses. Mit dem Passwort können Sie künftig Transaktionen freigeben. Dieser muss einen Kleinbuchstaben, einen Großbuchstaben und 1 Ziffer enthalten, sowie aus 8 Zeichen bis 20 Zeichen bestehen. Aktivieren Sie ggf. **Biometrie verwenden** und wählen Sie aus, ob Sie Diagnosedaten teilen möchten oder nicht. Um für Freigaben eine Pushmitteilung zu bekommen, erlauben Sie bitte den Erhalt von Mitteilungen der VR SecureGo plus App.

Wählen Sie nun **Aktivierungscode einscannen**. Erlauben Sie den Zugriff auf die Kamera. Scannen Sie anschließend den Aktivierungscode, den Sie mit getrennter Post erhalten haben und klicken auf **Weiter**. Die Aktivierung ist damit abgeschlossen!

So nutzen Sie die VR SecureGo plus App

- Sie führen eine TAN-pflichtige Transaktion, z.B. eine Überweisung im Online-Banking durch.
- Sie erhalten eine Push-Nachricht auf Ihr Smartphone, dass ein Auftrag zur Freigabe vorliegt. (Hinweis: Sind mehrere Geräte für VR SecureGo plus registriert (maximal drei), erhalten Sie die Nachricht auf allen Geräten gleichzeitig.)
- Bitte prüfen Sie die angezeigten Daten auf Richtigkeit und bestätigen Sie den Vorgang mit dem von Ihnen gewählten Freigabe-Passwort (ggf. biometrisches Merkmal).
- Sie erhalten eine Bestätigung, dass die Transaktion ausgeführt wurde.

Sicherheitstipps und Hinweise

Allgemeine Sicherheitshinweise

Bitte halten Sie auf Ihrem PC Browser und Betriebssystem stets auf dem aktuellen Stand und beachten Sie die Sicherheitshinweise auf unserer Internetseite www.dkm.de/sicherheitstipps.

Weiterführende Informationen und ausführliche Anleitungen finden sie auf unserer Homepage www.dkm.de im Bereich Privatkunden / Banking und auf den Seiten des Bundesamtes für Sicherheit in der Informationstechnik (<https://www.bsi-fuer-buerger.de>).

Vorsicht mit vertraulichen Daten

Gut zu wissen: Wir werden Sie niemals, erst recht nicht per Mail nach vertraulichen Kontodaten fragen, oder Sie auffordern PIN und TAN außerhalb des Bankings einzugeben. Diese Mails sind immer gefälscht!

Sperrmöglichkeiten

Im Bereich **Datenschutz & Sicherheit - Online-Zugang sperren** haben Sie die Möglichkeit Ihren Online-Zugang sofort zu sperren. Bitte beachten Sie, dass die Sperre für alle von Ihnen genutzten Online-Zugangswege gilt und dass Sie die Sperre selbst nicht wieder aufheben können.