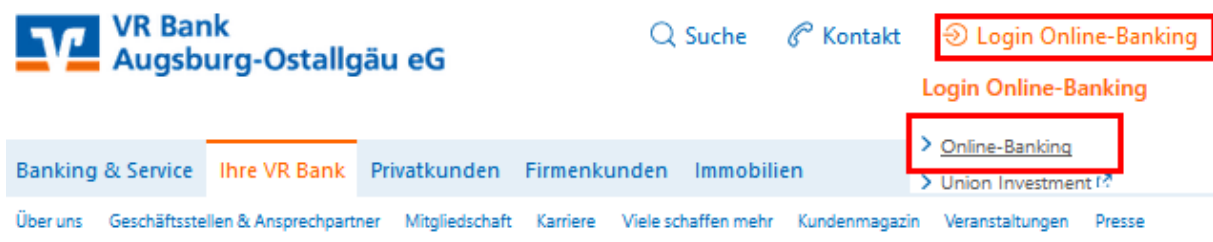


## Erstanmeldung im Online-Banking mit Sm@rt-TAN photo

Sehr geehrte Kundin, sehr geehrter Kunde,  
mit dieser Anleitung erläutern wir Ihnen die Vorgehensweise bei der Erstanmeldung in Ihrem Online-Banking mit dem Sm@rt-TAN photo-Verfahren. Das Verfahren kann sowohl in Kombination mit unserer VR-Banking-App sowie das Online-Banking über unsere Internetseite genutzt werden.

Bitte wählen Sie auf unserer Homepage [www.vrbank-a-oal.de](http://www.vrbank-a-oal.de) rechts oben den Button „Login Online-Banking“ aus und klicken Sie auf den Unterpunkt „Online-Banking“.



Als nächstes geben Sie bitte Ihren VR-NetKey und Ihre PIN-Nummer ein und klicken Sie auf den Button „Anmelden“.


### Anmeldung

VR-NetKey oder Alias:

PIN:

Jetzt werden Sie aufgefordert, Ihre vorgegebene PIN in eine persönliche PIN zu ändern.

### Erst-PIN-Änderung

 Wir begrüßen Sie recht herzlich in unserer Online-Anwendung. Aus Sicherheitsgründen ist es erforderlich, die Ihnen vorliegende Erst-Zugangs-PIN in Ihre persönliche PIN zu ändern.

Aktuelle PIN:

Gewünschte neue PIN (mind. 5, max. 20 Stellen):

Wiederholung neue PIN:

Geben Sie zunächst bei „Aktuelle PIN“ die PIN-Nummer ein, die Sie per Post erhalten haben. Anschließend erfassen Sie eine neue PIN mit nachfolgenden Kriterien und wiederholen die Eingaben. Nach erfolgreicher Eingabe bestätigen Sie diese mit **Eingabe prüfen**.

- Mind. 8, max. 20 Stellen
- Die PIN muss entweder rein numerisch sein oder min. einen Großbuchstaben und eine Ziffer enthalten.

Erlaubter Zeichensatz:

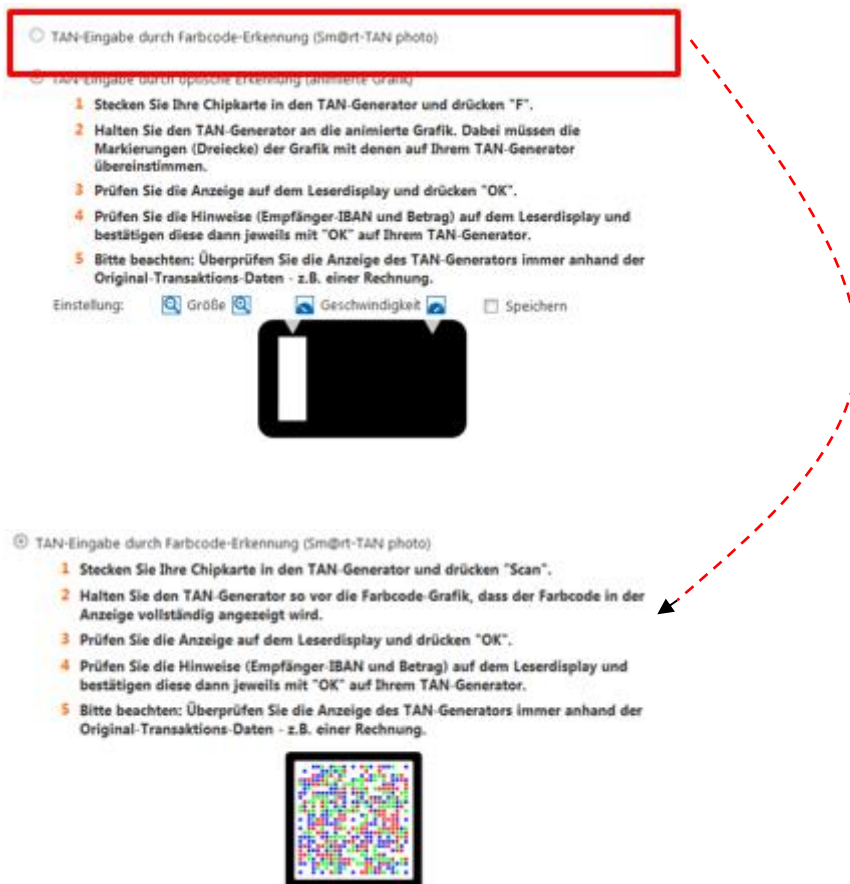
- Buchstaben (a-z und A-Z, incl. Umlaute und ß) und Ziffern (0-9)
- Die Sonderzeichen @ ! % & / = ? \* + ; : , . \_ -

Wichtig

Die selbst gewählte VR-NetKey PIN wird zu jeder Anmeldung im Online-Banking benötigt.

Die Änderung der PIN muss mit einer TAN-Nummer bestätigt werden.

Wechseln Sie hier wie angezeigt auf den Eintrag „TAN-Eingabe durch Farbcode-Erkennung (Sm@rt-TAN photo)“:




TAN-Eingabe durch Farbcode-Erkennung (Sm@rt-TAN photo)

TAN-Eingabe durch optische Erkennung (animierte Grafik)


- 1 Stecken Sie Ihre Chipkarte in den TAN-Generator und drücken "F".
- 2 Halten Sie den TAN-Generator an die animierte Grafik. Dabei müssen die Markierungen (Dreiecke) der Grafik mit denen auf Ihrem TAN-Generator übereinstimmen.
- 3 Prüfen Sie die Anzeige auf dem Leserdisplay und drücken "OK".
- 4 Prüfen Sie die Hinweise (Empfänger-IBAN und Betrag) auf dem Leserdisplay und bestätigen diese dann jeweils mit "OK" auf Ihrem TAN-Generator.
- 5 Bitte beachten: Überprüfen Sie die Anzeige des TAN-Generators immer anhand der Original-Transaktions-Daten - z.B. einer Rechnung.

Einstellung:  Größe  Geschwindigkeit  Speichern



TAN-Eingabe durch Farbcode-Erkennung (Sm@rt-TAN photo)

- 1 Stecken Sie Ihre Chipkarte in den TAN-Generator und drücken "Scan".
- 2 Halten Sie den TAN-Generator so vor die Farbcode-Grafik, dass der Farbcode in der Anzeige vollständig angezeigt wird.
- 3 Prüfen Sie die Anzeige auf dem Leserdisplay und drücken "OK".
- 4 Prüfen Sie die Hinweise (Empfänger-IBAN und Betrag) auf dem Leserdisplay und bestätigen diese dann jeweils mit "OK" auf Ihrem TAN-Generator.
- 5 Bitte beachten: Überprüfen Sie die Anzeige des TAN-Generators immer anhand der Original-Transaktions-Daten - z.B. einer Rechnung.





Nun stecken Sie Ihre VR-BankCard in den TAN-Generator und drücken Sie „Scan“. Sie positionieren die Kamera des TAN-Generators dabei so, dass der vollständige Farbcode im Bildschirm erkennbar ist.



Folgen Sie nun den angezeigten Anweisungen des Bildschirms. Bei erfolgreicher Übertragung wechselt die Anzeige Ihres TAN-Generators auf „Service Funktionen“. Bitte mit „OK“ auf dem TAN-Generator bestätigen. Anschließend zeigt der TAN-Generator die TAN für die PIN-Änderung. Bitte geben Sie diese TAN wieder in das entsprechende Feld ein und klicken dann auf „OK“.

Nach einer erneuten Anmeldung steht Ihnen nun Ihr Online-Banking zur Verfügung.

## Information zu: Erst-PIN-Änderung

Sie haben Ihre PIN erfolgreich geändert, aus Sicherheitsgründen ist nun eine erneute Anmeldung erforderlich.

[Erneut anmelden](#)


 Verwendete TAN: 718145  
 Der Vorgang wurde ausgeführt.

### Sm@rt-TAN photo als Standard-TAN-Verfahren definieren:

Für die Umstellung wählen Sie den Menüpunkt „Service“ und wechseln in den Unterpunkt „My eBanking“. Im Abschnitt „Individuelle TAN Eingabe für Sm@rt-TAN plus festlegen“ wählen Sie den Abschnitt „TAN-Eingabe durch Farbcode-Erkennung (Sm@rt-TAN photo)“ und speichern diese Eingabe.

[Banking](#) [Brokerage](#) [UnionDepot](#) [Postfach](#)

[Übersicht](#) [Umsatzanzeige](#) [Zahlungsaufträge](#) [Finanzmanager](#) [Angebote](#) [Service](#)

[> Banking](#) [> Service](#) [> Online-Banking](#) [> My eBanking](#) 

## My eBanking

### Individuelle TAN-Eingabe für Sm@rt-TAN plus festlegen

Mit dieser Funktion haben Sie die Möglichkeit, eine Standardanzeige für TAN-pflichtige Geschäftsvorfälle (z.B. einer Überweisung) festzulegen.

1. Wählen Sie eine der angebotenen Möglichkeiten für die TAN-Eingabe aus.
2. Legen Sie ggf. die Grafikgröße für die optische Erkennung fest.
3. Klicken Sie auf [Speichern].

- TAN-Eingabe durch Farbcode-Erkennung (Sm@rt-TAN photo)
- TAN-Eingabe durch manuelle Erfassung
- TAN-Eingabe durch optische Erkennung (animierte Grafik)

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

- 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.
- Ihre VR Bank Augsburg-Ostallgäu eG wird Sie nie per E-Mail zu etwas auffordern, bei dem Sie die Zugangsdaten zu Ihrem Konto eingeben müssten, zum Beispiel für eine Sicherheitsüberprüfung oder für eine Rücküberweisung. Reagieren Sie nicht auf solche E-Mail-Anfragen und löschen Sie diese sofort.
- 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.