

# Online banking with pushTAN

## Setting up pushTAN

### What you need for pushTAN:

- A smartphone or tablet (Android or iOS/Apple)
- Your customer support agent at the bank has activated the pushTAN procedure for your account
- You have received your initial access data, registration name and/or Legitimation ID, and if yours is a new contract, your Start PIN and registration letter

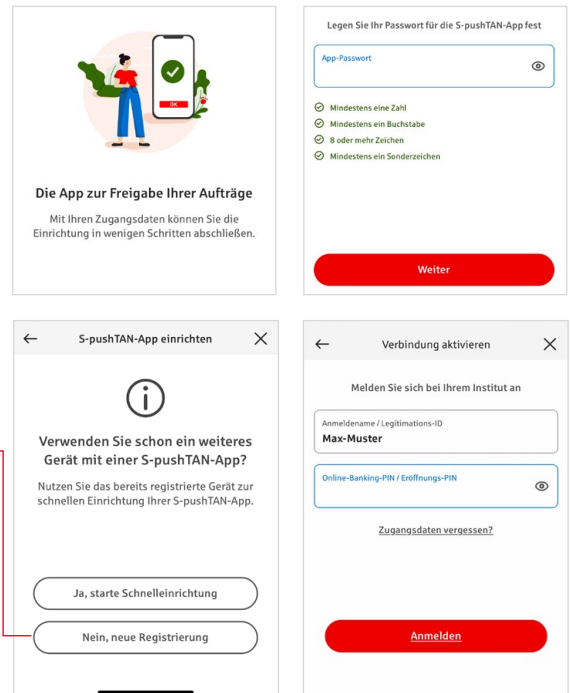
If you have all that, proceed as follows:

### Activating the app on your smartphone or tablet

1. Install the “S-pushTAN” app onto your device from your App Store (Google Play/App Store).
2. Start the “S-pushTAN” app, click on “Jetzt einrichten” [“Set up now”], and allow the app to send you notifications. Confirm the instructions with “Erlauben” [“Permit”] and then set a secure password for the app.

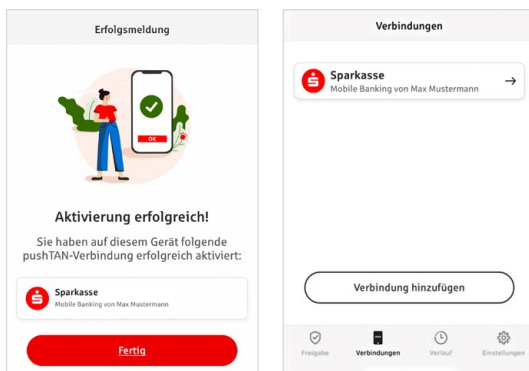
The password must have at least 8 characters (comprising numbers, letters and one special character). In the next step, you can decide whether you want to unlock the app with a biometric feature such as Face ID or with the help of the password.

3. First, click on “Nein, neue Registrierung” [“No, new registration”] and then on “Ja, Registrierungsdaten vorhanden” [“Yes, registration data on file”]. Scan the QR code on the registration letter with your smartphone camera in order to activate the connection. Then, you will be asked to confirm your identity by entering your online banking access data.



### Changing your online banking PIN

4. If you are a new customer, then change the Start PIN that was issued to you into your own personal PIN that you can remember well.



Once the system confirms your new PIN you can enjoy the benefits of all the products and services we offer.

You can find and manage your pushTAN connections using the “Verbindungen” (Connections) tab.

## ”S-pushTAN” – The app for approvals and identity confirmations

### By the way:

You can use the „S-pushTAN“ app to:

- Approve orders in online banking
- Approve card payments on the Internet (3D Secure) with the Sparkassen Card and Sparkassen credit cards
- Confirm your identity when calling us by phone

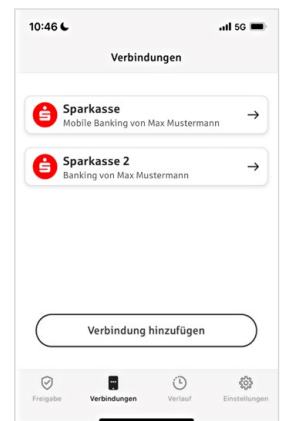
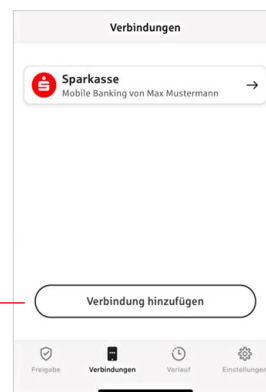
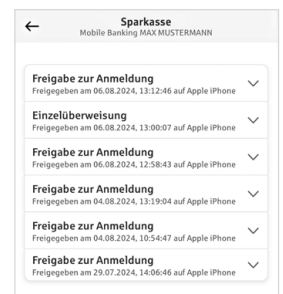
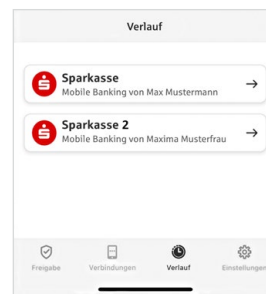
## Approval history

You can view your approvals retrospectively under „Verlauf“.

## Add another pushTAN connection

To add further pushTAN connections, e.g. from other Sparkassen, log in to the „S-pushTAN“ app.

1. Click on „Verbindungen“ and then on „Verbindung hinzufügen“.
2. Proceed as described above to set up the pushTAN connection.  
No new password is required for the app.
3. After successful setup, the new pushTAN connection will be displayed.



## Manage pushTAN connections

You can manage your registered pushTAN connections under „Verbindungen“:  
Activate the Face ID, block the connection, manage your devices and configure the delivery groups.

### Add another device

(Bluetooth must be activated on both devices)

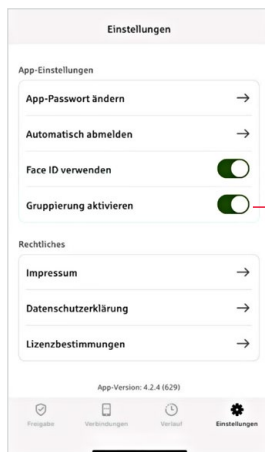
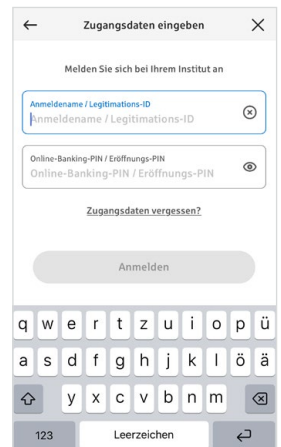
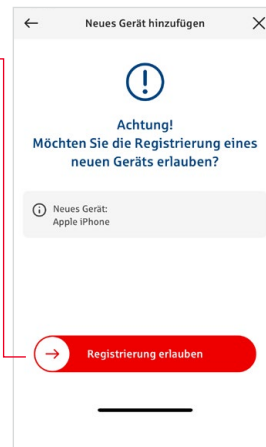
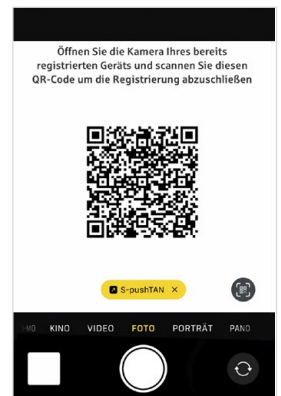
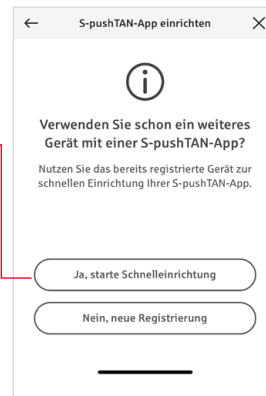
pushTAN connections can also be registered on numerous devices. In order to add an additional device, log into the “S-PushTAN” app on the new device. Click on “Ja, starte Schnelleinrichtung” [“Yes, begin quick setup”] and then on “Weiter” [“Continue”].

1. Now, create the QR code that connects the two devices with one another.
2. Scan the QR code with the photo app of your old device. Your S-pushTAN app will start automatically. Select the connection that you want to set up on the new device.

As soon as your new device is shown, swipe the “Registrierung erlauben” [“Permit registration”] button from left to right. Confirm with the app password or your biometric feature.

3. You will then be asked to enter your online banking access data on the new device.

All registered devices are displayed under „Ihre Geräte“.



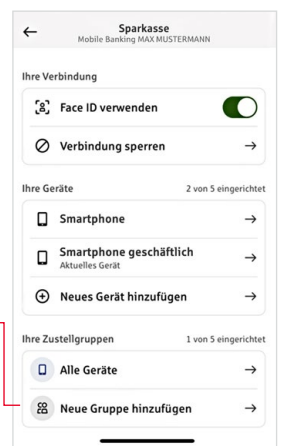
### Configure groups

If you use your pushTAN connection on multiple devices, you can configure groups.

Activate the „Gruppierung aktivieren“ function in „Einstellungen“.

Then go to the corresponding pushTAN connection under „Verbindungen“.

Use the „Neue Gruppe hinzufügen“ function to carry out the configuration.





---

## Tips for more security on the internet

Before you do online banking or use your credit card on the internet, please take a few minutes to consider the following important matters.

### Fit for the internet

You can largely protect yourself against attacks coming from the internet by observing the following basic rules. You can find explanations on how to recognise attempted frauds, how to secure your computer and its access to the internet, and important information on current fraudulent activity on the internet at

[www.sparkasse-hannover.de/sicherheit](http://www.sparkasse-hannover.de/sicherheit)

- Regularly update your operating system and the programs you use.
- Do not work with administrator rights on your computer.
- Use a firewall and a virus scanner, and keep them up to date.
- Always delete your browser history and cache after doing business on the internet.
- Never do your banking or make online purchases using someone else`s wireless network.
- Do not store personal access data in third-party portals, and do not give your data to others.
- Make sure you only do online business through an encrypted connection.
- Always enter the IP address manually when doing online banking or buying something online.
- Do not open attachments in e-mails from e-mail addresses not known to you.
- Never respond to e-mail or telephone requests to confirm payment orders.

**No Sparkasse employee will ever ask you for your online-banking access data – neither by e-mail, by fax, by telephone nor in person.**

### Safe online banking and payments on the internet

Always follow these rules:

#### Be careful

Swiping the button „Auftrag freigeben“ or entering a TAN usually confirms a transfer from your account. Do not forget this if you are asked for your bank details or to place an order without actually wanting to do so.

#### Be suspicious

If something seems strange to you, we recommend you abort the transaction. For instance, your Sparkasse will never ask you to place orders for lotteries, security updates or supposed return transfers of money.

#### Check your data carefully

The main order data will be shown on the display, your TAN generator or mobile phone. If the information shown is not the same as on your order, cancel the transaction.

#### Enter your data safely

When entering your log-in data for online banking, make sure the padlock symbol is displayed in your browser.

#### Be alert

Regularly check the transactions in your account, through your account statements or in online banking. That is the only way to recognise unauthorised transactions in time to stop them.

#### Set daily limits

Set a daily maximum amount that can be transferred from your online account. This limits the possibilities of unauthorised access.

#### When in doubt: block your access

If you suspect that something is wrong with your banking application, block your access to it. To do so, contact your Sparkasse or call the Germany-wide free emergency account-blocking telephone number 116 116. That number also works if you are not in Germany.