pushTAN: Initial setup

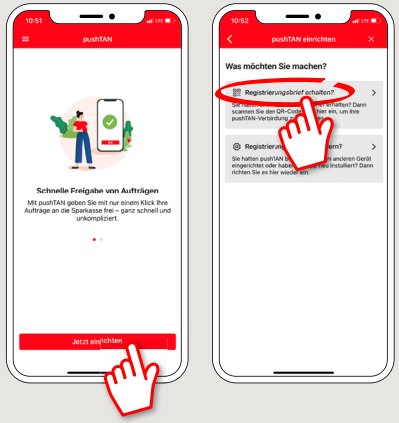
www.sparkasse-hanau.de/pushtan

Sparkasse Hanau

Only start the registration process described below when you have received the registration letter and your access data for online banking (opening PIN and login name).
If you have changed your previous procedure to pushTAN, you will keep your previous access data. Otherwise you will receive a separate PIN letter in the post containing your new access data.

1 Install the S-pushTAN app on your smartphone.

2 Start the app and tap "**Jetzt einrichten**" → „**Registrierungsbrief erhalten**" → "**Weiter**" → "**Weiter**" to allow push notifications.

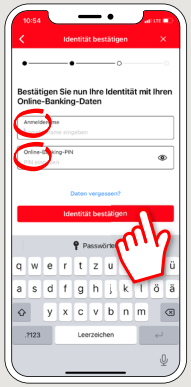


3 In the next step, you assign a password for the app and confirm this by re-entering it.

Then select whether you want to open the app using TouchID or FaceID.

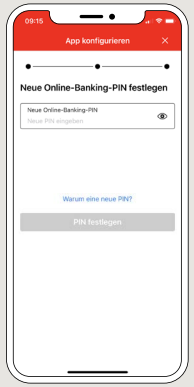
4 Now allow the app to access your camera to scan the QR code in the registration letter.

5 In the next step, enter your access data for online banking.

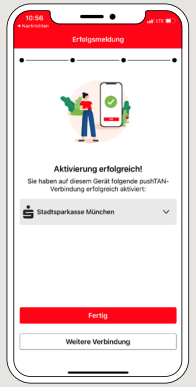


6 If you have received your initial access data for online banking from us, it is now necessary to change the PIN you have been given. Type in your new PIN and confirm by re-entering it.

Remember the PIN well!
You need this PIN for banking via App „Sparkasse" and via our website www.sparkasse-hanau.de



7 Your pushTAN connection has now been successfully set up!



DO YOU HAVE ANY QUESTIONS ABOUT pushTAN?

Central service call number: You can contact us under **06181 298-0 Mon – Fri from 8 am – 7 pm**.

Further information and FAQs about pushTAN is available at: **www.sparkasse-hanau.de/pushtan**

Sparkasse Hanau | Am Markt 1 | 63450 Hanau | Telefon: 06181 298-0 | E-Mail: info@sparkasse-hanau.de | www.sparkasse-hanau.de

november 2022

Sparkasse Hanau
phone: +49 6181 298-0
www.sparkasse-hanau.de

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-hanau.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.