

Онлайн-банкінг з pushTAN

Налаштувати pushTAN

Попередні умови для pushTAN:

- Ви маєте смартфон або планшет (Android або iOS/Apple)
- Ваш консультант активував для вашого рахунку процедуру pushTAN
- Ви отримали дані для першого доступу, а саме ім'я користувача та/або ID-код, а також, у випадку нового договору, стартовий PIN-код та реєстраційний лист

Ваші наступні дії:

Активация застосунку на вашому смартфоні або планшеті

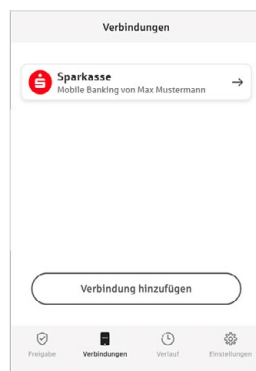
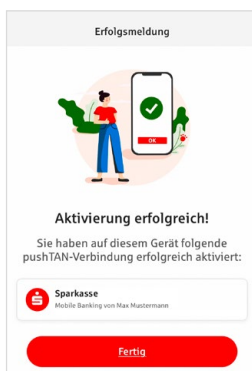
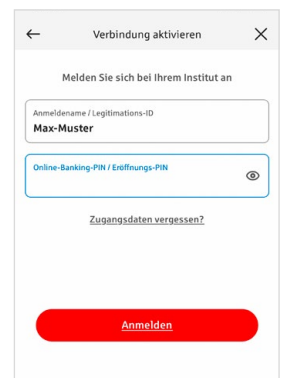
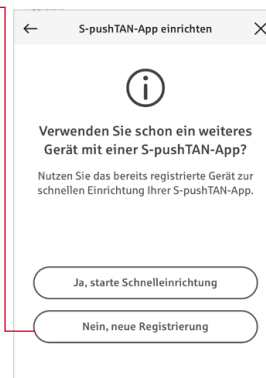
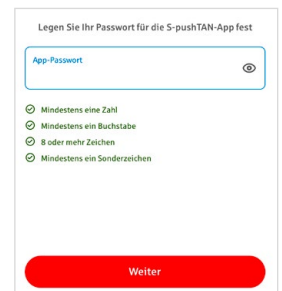
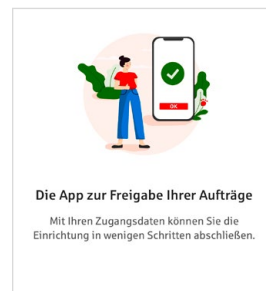
1. Встановіть застосунок „S-pushTAN“ з магазину застосунків вашого смартфона (Google Play / App Store).
2. Запустіть застосунок „S-pushTAN“, натисніть „Jetzt einrichten“ [„Налаштувати“] та дозвольте застосунку надсилати вам сповіщення. Підтвердьте дію натисканням на „Erlauben“ [„Дозволити“] та встановіть для застосунку надійний пароль. Пароль повинен складатися мінімум з 8 знаків (цифри, літери та один спеціальний символ).

На наступному кроці ви можете вирішити, чи хочете ви розблокувати додаток за допомогою біометричної функції, наприклад, Face ID, або за допомогою пароля.

3. Натисніть „Nein, neue Registrierung“ [„Ні, нова реєстрація“], потім „Ja, Registrierungsdaten vorhanden“ [„Так, реєстраційні дані доступні“]. Щоб активувати з'єднання, відскануйте QR-код із листа про реєстрацію за допомогою камери смартфона. Потім підтвердьте свою особу, ввівши дані доступу до онлайн-банкінгу.

Нові клієнти:

Як новий клієнт, змініть стартовий PIN-код на свій власний PIN-код. Після того, як новий PIN-код буде підтверджений системою, у вас буде можливість користуватися усіма запропонованими послугами.



Ви побачите підтвердження успішної активації з'єднання pushTAN.

У вкладці „З'єднання“ [„Verbindungen“] можна знайти свої pushTAN-з'єднання і керувати ними.

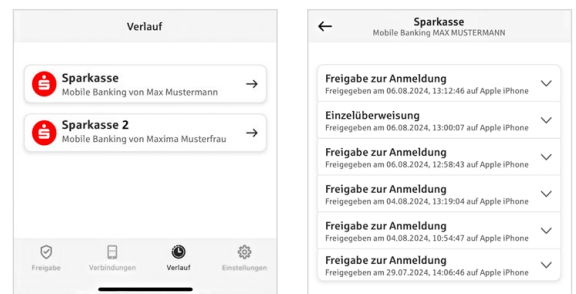
„S-pushTAN“ – Додаток для затвердження платіжних операцій та підтвердження особи

До речі: З додатком „S-pushTAN“ Ви можете:

- Затверджувати платіжні операції в онлайн-банкінгу
- Затверджувати карткові платежі в Інтернеті (3D Secure) за допомогою карток Sparkasse та кредитних карток Sparkasse
- Підтверджувати свою особу під час телефонних розмов з нами

Історія видачі затверджень

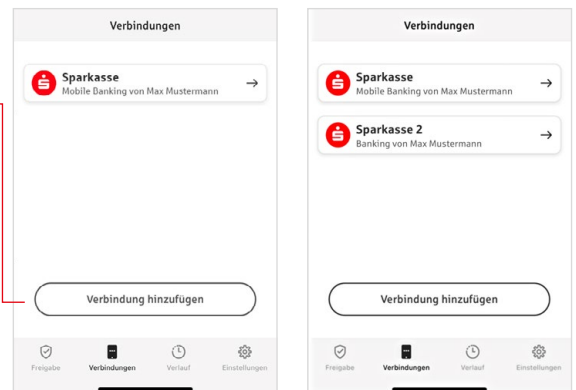
Ви можете переглянути видані вами затвердження ретроспективно в розділі „Історія“ [„Verlauf“].



Додати ще одне з'єднання pushTAN

Щоб додати інші з'єднання pushTAN, наприклад, з іншими відділеннями Sparkasse, увійдіть у додаток „S-pushTAN“.

1. Натисніть на „З'єднання“ [„Verbindungen“], а потім на „Додати з'єднання“ [„Verbindung hinzufügen“].
2. Щоб налаштувати з'єднання pushTAN, виконайте дії, описані вище.
Не обов'язково призначати новий пароль для додатку.
3. Після успішного налаштування відобразиться нове з'єднання pushTAN.



Керувати з'єднаннями pushTAN

Ви можете керувати зареєстрованими з'єднаннями pushTAN у розділі „З'єднання“ [„Verbindungen“]: активувати Face ID, блокувати з'єднання, керувати пристроями та налаштовувати групи доставки.

Додати ще один пристрій

(Bluetooth має бути активований на обох пристроях)

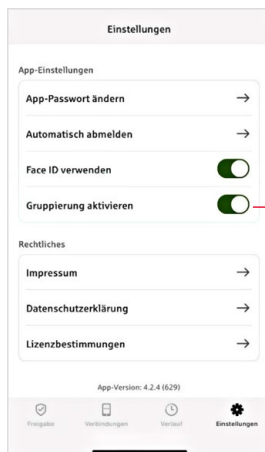
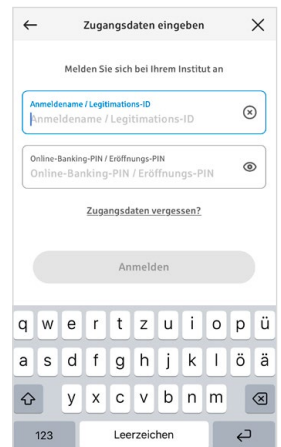
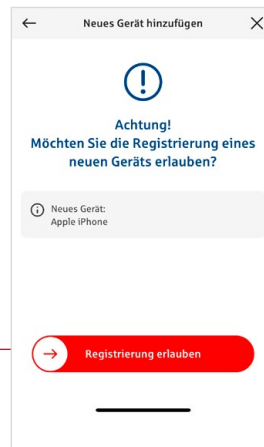
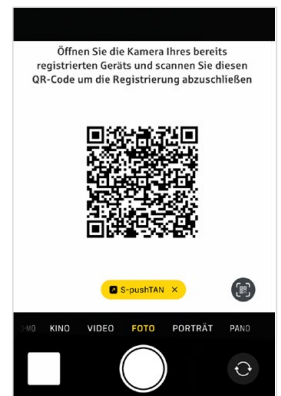
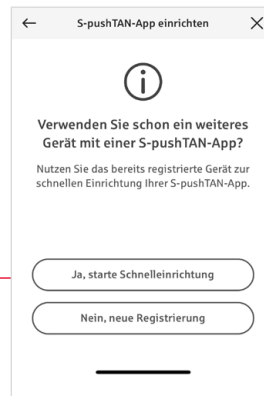
Способи з'єднання з pushTAN також можуть бути зареєстровані на декількох пристроях. Щоб додати ще один пристрій, увійдіть у застосунок „S-PushTAN“ на **новому пристрої**. Натисніть „Ja, starte Schnelleinrichtung“ [„Так, запустити швидке налаштування“], потім натисніть „Weiter“ [„Далі“].

1. Створіть QR-код, який з'єднає два пристрої один з одним.
2. Відскануйте QR-код за допомогою спеціального застосунку на вашому старому пристрої. Застосунок S-pushTAN запуститься автоматично. Виберіть спосіб з'єднання, який ви хочете налаштувати на новому пристрої.

Щойно на екрані з'явиться ваш новий пристрій, змахніть кнопку „Registrierung erlauben“ [„Дозволити реєстрацію“] зліва направо. Підтвердьте свою особу за допомогою пароля для застосунку або ваших біометричних даних.

3. Введіть дані доступу до онлайн-банкінгу на новому пристрої.

Усі зареєстровані пристрої відображаються у розділі „Ваші пристрої“ [„Ihre Geräte“].



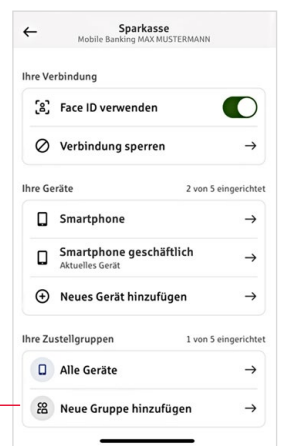
Налаштувати групи

Якщо Ви використовуєте з'єднання pushTAN на декількох пристроях, можна налаштувати групи.

Активуйте функцію „Активувати групування“ [„Gruppierung aktivieren“] в розділі „Налаштування“ [„Einstellungen“].

Потім перейдіть до відповідного з'єднання pushTAN у розділі „З'єднання“ [„Verbindungen“].

Використовуйте функцію „Додати нову групу“ [„Neue Gruppe hinzufügen“], щоб виконати конфігурацію.



Використання pushTAN в онлайн-банкінгу

Для затвердження платіжних операцій на нашому веб-сайті на комп'ютері або у застосунку в смартфоні/планшеті, ваші дії наступні:

1. Авторизуйтеся на нашому веб-сайті (www.sparkasse-hannover.de) або запустіть застосунок банкінгу.
2. Введіть дані для проведення бажаної операції (наприклад, переказ грошей) та підтвердьте їх.
3. Перейдіть до застосунку „S-pushTAN“. Після введення вашого S-pushTAN паролю, на екрані з'являться дані по операції.

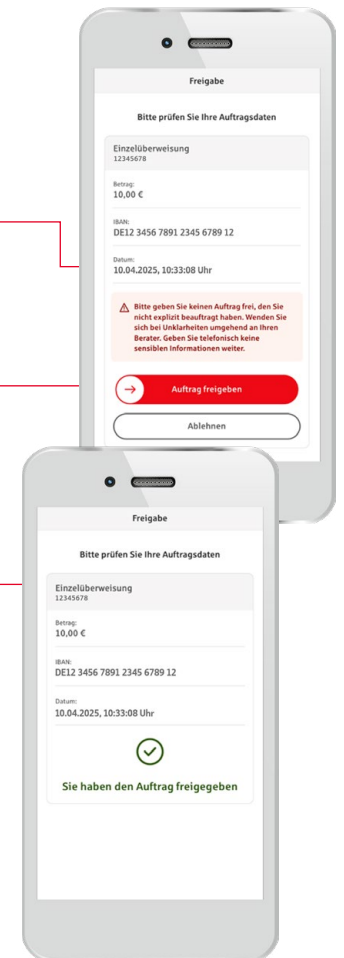
Будь-ласка, перевірте, чи платіжні дані на екрані співпадають з тими, що ви вказали раніше.

- | | |
|----------------|-----------------------|
| → Тип операції | → Код IBAN отримувача |
| → Сума | → Дата |

У разі виявлення розбіжностей негайно скасуйте операцію та зверніться до свого консультанта або до нашого сервісного центру.

4. Якщо дані збігаються, підтвердьте платіж, провівши кнопку „Auftrag freigeben“ вправо. Розблокуйте за допомогою біометричної функції, наприклад, Face ID. Відразу після цього ви отримаєте сповіщення про затвердження операції.

Вказівка: Завжди оновлюйте застосунок „S-pushTAN“ та операційну систему свого смартфона/планшета.



Контакт

Чи залишилися у вас ще запитання по темі онлайн-банкінг?
Ми охоче проконсультуємо вас в особистій бесіді.

Sparkasse Hannover
Raschplatz 4
30161 Hannover

Телефон: +49 511 3000-2288
info@sparkasse-hannover.de
www.sparkasse-hannover.de

Відмова від відповідальності

Ця інструкція складена на базі актуальної інформації та надана як послуга сервісу. Банк Sparkasse та автори інструкції не несуть відповідальності за можливі відхилення від цього тексту. Ми не беремо на себе жодної відповідальності за будь-який понесений збиток.

Вказівки щодо підвищення рівня безпеки в інтернеті

Перш ніж користуватись послугою онлайн-банкінгу або застосовувати вашу кредитну карту в інтернеті, присвятіть кілька хвилин часу наступній важливій інформації.

Готовність до інтернету

Той, хто дотримується найважливіших базових вимог, може значною мірою захистити себе від атак з інтернету. Роз'яснення щодо виявлення спроб шахрайства та щодо захисту вашого комп'ютера та доступу до інтернету, а також важливу інформацію щодо актуальних спроб шахрайства ви знайдете за адресою

www.sparkasse-hannover.de/sicherheit

- Регулярно оновлюйте операційну систему та програми, якими ви користуєтесь.
- Не працюйте на своєму комп'ютері з правами адміністратора.
- Користуйтеся брандмауером та антивірусною програмою та тримайте їх завжди у актуальному виді.
- Після фінансових транзакцій в інтернеті завжди виконуйте очищення історії браузера та кешпам'яті.
- Ні в якому разі не виконуйте жодних банківських транзакцій та покупок в інтернеті через чужу бездротову мережу вай-фай.
- Не залишайте жодної особистої інформації на чужих порталах, а також не передавайте її третім особам.
- Слідкуйте за тим, щоб фінансові транзакції в інтернеті виконувались завжди через кодоване з'єднання.
- Для онлайн-банкінгу та покупок в інтернеті вводіть інтернет-адресу завжди тільки вручну.
- Ніколи не відкривайте файлів-додатків до електронних листів від невідомих відправників.
- Ні в якому разі не виконуйте вимог, які ви отримали електронною поштою або телефоном щодо підтвердження платіжних операцій.

Жоден співробітник Sparkasse не вимагатиме від вас розголошення даних доступу до онлайн-банкінгу – ані електронною поштою, ані факсом, ані телефоном, ані в особистій бесіді.

Безпечний онлайн-банкінг та платежі в інтернеті

Необхідно в обов'язковому порядку дотримуватись наступних вимог:

Краще: бути обережним

Переказ з вашого рахунку зазвичай підтверджується, проводячи пальцем по кнопці „Auftrag freigeben“ або ввівши TAN. Не забувайте про це, якщо в вас питають або від вас вимагають назвати свої банківські реквізити, дозволити виконання операції або ввести TAN, а ви при цьому не давали доручення на операцію.

Бути недовірливим

Якщо відбувається щось незвичне, у разі будь-яких сумнівів краще скасувати операцію. Зокрема, ваш банк Sparkasse ніколи не спитає у вас про дозвіл на виконання операції або не запропонує ввести TAN для участі в лотереях, оновлення в цілях безпеки та немовби повернення якихось коштів на ваш рахунок.

Ретельно: перевіряти дані

На дисплеї вашого генератора TAN або мобільного телефону ви побачите найважливіші дані платіжної операції. Якщо дані на дисплеї не співпадають з даними вашого доручення, скасуйте операцію.

Приховано: безпечне введення

Коли ви вводите дані доступу до онлайн-банкінгу: завжди звертайте увагу на те, чи видно у браузері символ замка.

Завжди: зберігати увагу

Регулярно перевіряйте обіг коштів на вашому рахунку. Це можна зробити у онлайн-банкінгу або роздрукувавши виписку по рахунку. Лише так можна своєчасно і у належні строки виявити несанкціоноване зняття коштів.

Обмежити: щоденний ліміт

Встановіть щоденний ліміт для ваших транзакцій онлайн-банкінгу. Встановлюючи особисті межі користування коштами, ви обмежуєте можливості для несанкціонованого доступу.

Якщо виникли сумніви: заблокувати доступ

Якщо у вас виникли підозри, що с користуванням послугами банкінгу щось не так: заблокуйте доступ. Для цього звертайтеся безпосередньо до відділення Sparkasse або зателефонуйте за цілодобовим безкоштовним номером 116 116 з будь-якої точки Німеччини. Телефон блокування рахунку доступний також із-за кордону.