

# Інтернет-банкінг з pushTAN

## Налаштувати pushTAN

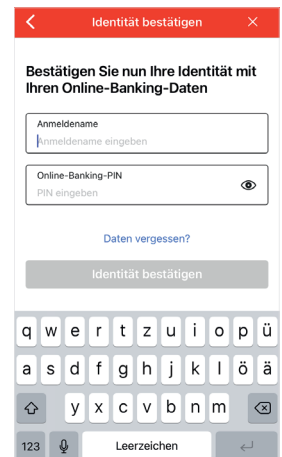
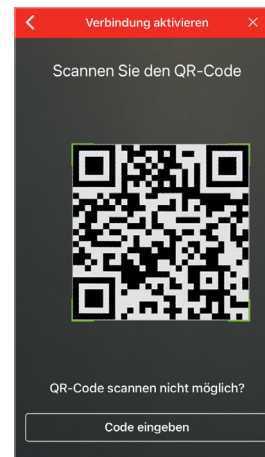
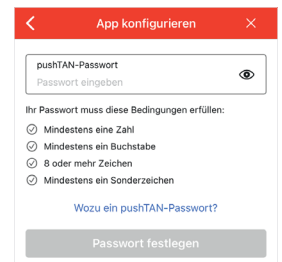
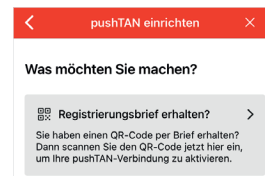
### Попередні умови для pushTAN:

- Ви маєте смартфон або (Android або iOS/Apple)
- Ваш консультант активував ваш рахунок для використання методу pushTAN
- Ви маєте дані для першого доступу, а саме, ім'я користувача або код легітимації, а також (у випадку нового договору) стартовий PIN-код та реєстраційний лист

Послідовність дій наступна:

### 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» та натисніть клавішу „Jetzt einrichten“ / „Registrierungsbrief erhalten“ («Налаштувати зараз» / «Реєстраційного листа отримано»). Підтвердіть вказівки клавішею „Weiter“ («Далі»), після чого виберіть собі надійний пароль. Пароль повинен складатися мінімум з 8 знаків (цифри, літери та один спеціальний символ).
3. За допомогою камери вашого смартфона відскануйте код QR з реєстраційного листа. Після цього вам буде запропоновано засвідчити свою особу шляхом введення своїх даних доступу до інтернет-банкінгу. Потім ви отримуєте підтвердження активації pushTAN.



### Зміна PIN-коду інтернет-банкінгу

4. Якщо ви новий клієнт, змініть стартовий PIN-код на свій власний PIN-код.

Щойно новий PIN-код буде підтверджений системою, ви будете в змозі користуватися усіма послугами, які ми пропонуємо.

## Використання pushTAN в інтернет-банкінгу

Щоб дати доручення у нашій інтернет-філії на комп'ютері або в дорозі за допомогою смартфона або планшета, дотримуйтесь наступної послідовності дій:

1. Увійдіть до нашої інтернет-філії ([www.sk-westerwald-sieg.de](http://www.sk-westerwald-sieg.de)) та запустіть застосунок банкінгу.
2. Введіть дані відповідного платіжного доручення (наприклад, переказ грошей) та підтвердіть це доручення.
3. Перейдіть до застосунку «S-pushTAN». Щойно ви введете свій пароль до S-pushTAN, ви побачите дані платіжного доручення.

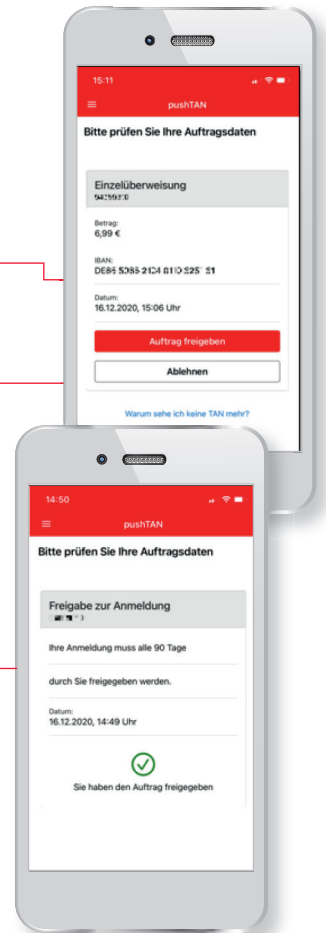
Звірте дані платіжного доручення з тими даними, які були вамі введені.

- |                       |        |
|-----------------------|--------|
| ■ Тип доручення       | ■ Сума |
| ■ Код IBAN отримувача | ■ Дата |

Якщо виявлені розбіжності, негайно скасуйте операцію та зверніться до свого консультанта або до нашого сервісного центру.

4. Якщо дані співпадають, підтвердіть платіж, для чого слід натиснути кнопку „Auftrag freigeben“ (Дозволити операцію). Відразу після цього ви отримаєте підтвердження прийому платіжного доручення до виконання.

Вказівка: Завжди підтримуйте застосунок «S-pushTAN» та операційну систему свого смартфона/планшета у актуальному стані.



## Контакт

Чи залишилися у вас ще запитання по темі «Інтернет-банкінг»  
 Мы охоче проконсультуємо вас у особистій бесіді.

### Sparkasse Westerwald-Sieg

Bismarckstraße 16  
 56470 Bad Marienberg

Телефон: +49 2661/620-0  
[info@skwws.de](mailto:info@skwws.de)  
[www.sk-westerwald-sieg.de](http://www.sk-westerwald-sieg.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. Мы не беремо на себе жодної відповідальності за будь-який збиток, який стався.

## Вказівки щодо підвищення рівня безпеки в інтернеті

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

### Готовий 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.sk-westerwald-sieg.de/sicherheit](http://www.sk-westerwald-sieg.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 кеш-пам'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 інтернет-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 інтернет-банкінгу – ані електронною поштою, ані факсом, ані телефоном, ані в особистій бесіді.**

### Безпечний інтернет-банкінг та платежі в інтернеті

Необхідно в обов'язковому порядку дотримуватись наступних вимог:

#### Краще: бути обережним

Натисканням кнопки „Auftrag freigeben“ (Дозволити операцію) або введенням TAN зазвичай підтверджується переказ грошей з вашого рахунку. 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: Перевірити дані

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

#### Приховано: безпечне введення

Безпечно вводити дані Завжди звертайте увагу на те, чи видно у браузері символ замка.

#### Завжди: зберігати увагу

Регулярно перевіряйте обіг коштів на вашому рахунку. Перевіряти слід інтернет-банкінг та витяги з вашого рахунку. Лише так можна своєчасно і у належні строки виявити несанкціоноване зняття коштів.

#### Обмежити: ліміт коштів за день

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

#### Якщо виникли сумніви: заблокувати доступ

Если 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.