

Інтернет-банкінг з pushTAN

Налаштувати pushTAN

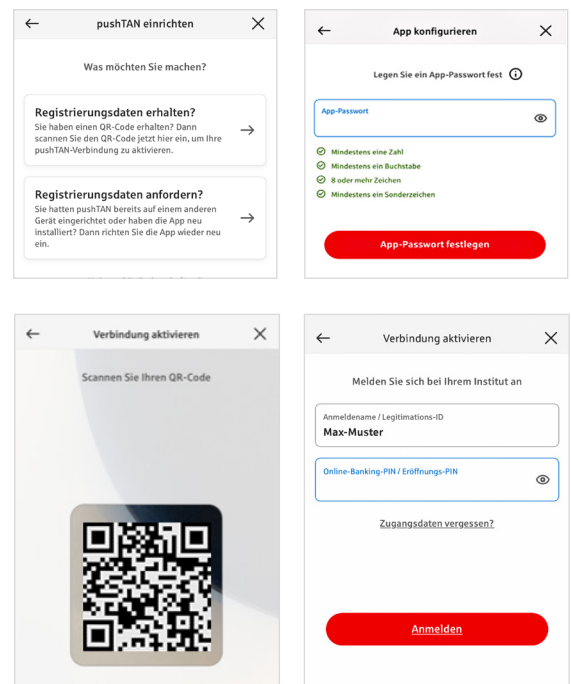
Попередні умови для pushTAN:

- Ви маєте смартфон або планшет (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 легітимізації а також у випадку нового договору стартовий PIN-код та реєстраційний лист

Ваші наступні дії:

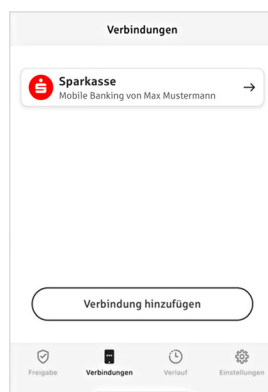
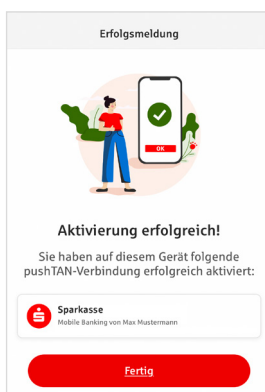
Активация застосунку на вашому смартфоні або планшеті

1. Встановіть застосунок «S-pushTAN» з магазину застосунків вашого смартфона (Google Play / App Store).
2. Запустіть застосунок «S-pushTAN» та натисніть клавішу «Jetzt einrichten» / «Registrierungsdaten erhalten» («Налаштувати зараз» / «Реєстраційного листа отримано»). Підтвердьте вказівки, натиснувши «Weiter» («Далі»), після чого створіть собі 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. За допомогою камери вашого смартфона відскакуйте QR код з реєстраційного листа. Після цього вам буде запропоновано підтвердити свою особу шляхом введення своїх даних доступу до інтернет-банкінгу. У разі успішної активації pushTAN - з'єднання, ви отримаєте підтвердження.



Зміна PIN-коду інтернет-банкінгу

4. 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.

У вкладці «З'єднання» («Verbindungen») можна знайти свої pushTAN-з'єднання і керувати ними.

«S-pushTAN» – Додаток для авторизації та підтвердження особи

До речі: З додатком «S-pushTAN» Ви можете:

- Авторизувати замовлення в онлайн-банкінгу
- Авторизувати карткові платежі в Інтернеті (3D Secure) за допомогою карток Sparkassen-Card та кредитних карток Sparkasse*
- Підтверджувати свою особу під час телефонних розмов з нами*

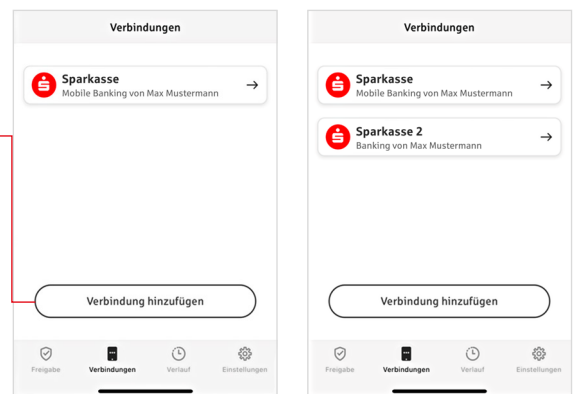
Історія випусків

Ви можете переглянути свої схвалення ретроспективно в розділі «Історія».

Додати ще одне з'єднання pushTAN

Щоб додати інші з'єднання pushTAN, наприклад, з іншими ощадними касами, увійдіть у додаток «S-pushTAN».

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



* Доступність може змінюватися

Керувати з'єднаннями pushTAN

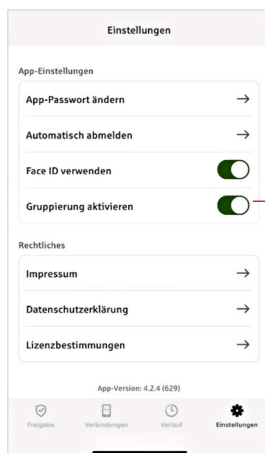
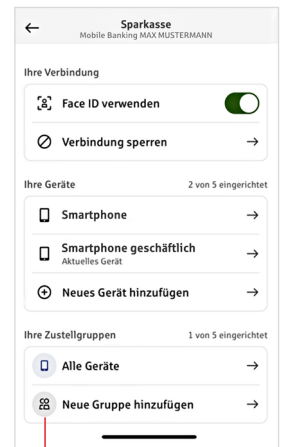
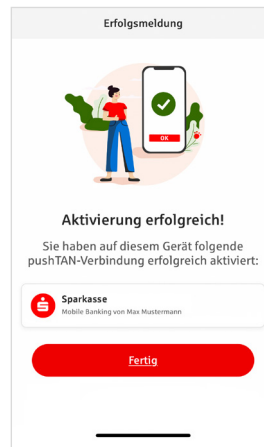
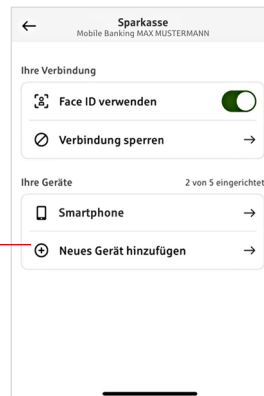
Ви можете керувати зареєстрованими підключеннями pushTAN у розділі «З'єднання (Verbindungen)»: Активувати Face ID, блокувати з'єднання, керувати пристроями та налаштовувати групи доставки.

Додати ще один пристрій

З'єднання pushTAN можна зареєструвати на декількох пристроях. Щоб додати ще один пристрій (наприклад, планшет), увійдіть у додаток «S-pushTAN» на пристрої [A] з наявним з'єднанням.

1. Натисніть на «З'єднання (Verbindungen)», а потім на з'єднання pushTAN, яке Ви хочете використовувати на іншому пристрої.
2. Виберіть «Додати новий пристрій (Neues Gerät hinzufügen)» і дотримуйтеся інструкцій, доки не відобразиться QR-код.
3. Ви вже встановили додаток «S-pushTAN» на новий пристрій [B]. Запустіть додаток, виберіть «Отримати реєстраційні дані (Registrierungsdaten erhalten)» і дотримуйтеся наданих вище інструкцій, щоб налаштувати з'єднання pushTAN. Скористайтеся QR-кодом, який відображається на пристрої [A].

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 «Налаштування (Einstellungen)».

Використовуйте функцію «Додати нову групу (Neue Gruppe hinzufügen)», щоб виконати конфігурацію.

Використання pushTAN в інтернет-банкінгу

Щоб користуватися послугами доступними у нашій інтернет-філії на комп'ютері або смартфоні / планшеті, ваші дії наступні:

1. Зареєструйтесь у нашій інтернет-філії (www.kreissparkasse-heinsberg.de) та запустіть застосунок банкінгу.
2. Введіть дані для проведення бажаної операції (наприклад, переказ грошей) та підтвердьте її.
3. Перейдіть до застосунку «S-pushTAN». Після введення вашого S-pushTAN паролю, на екрані з'являться дані по операції.

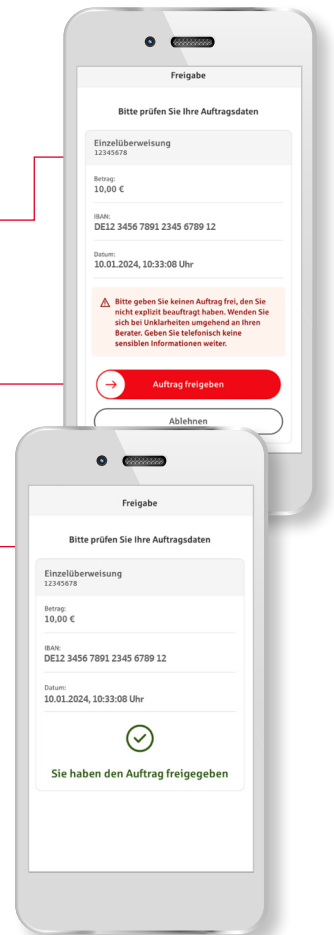
Будь-ласка, перевірте показані на екрані дані операції на відповідність даним, які введені вами.

- Тип операції
- Сума
- Код IBAN отримувача
- 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. Або розблокувати за допомогою біометричної функції, наприклад, Face ID. Відразу після цього ви отримаєте підтвердження прийому операції 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?
Ми охоче проконсультуємо вас в у особистій бесіді.

Kreissparkasse Heinsberg

Dr.-Eberle-Platz 1
41812 Erkelenz

Телефон: +49 2451 600
info@kskhs.de
www.kreissparkasse-heinsberg.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 інтернет-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.kreissparkasse-heinsberg.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

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 платіжного доручення. Якщо дані на дисплеї не співпадають з даними вашого доручення, скасуйте операцію.

Приховано: безпечне введення

Коли ви вводите дані доступу до інтернет-банкінгу: 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: щоденний ліміт

Встановіть щоденний ліміт для ваших транзакцій інтернет-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.