

Онлайн-банкинг с использованием pushTAN

Настройка pushTAN

Предварительные условия для пользования pushTAN:

- У вас есть смартфон или планшет (Android или iOS/Apple)
- Ваш консультант активировал для вашего счёта процедуру pushTAN
- Вы получили для первичного доступа имя пользователя и/или ID-код, а также, если вы заключаете новый договор, то вы получили стартовый PIN-код и регистрационное письмо

Порядок действий следующий:

Активация приложения на вашем смартфоне или планшете

1. Установите приложение „S-pushTAN“ из магазина приложений вашего смартфона (Google Play / App Store).

2. Запустите приложение S-pushTAN, нажмите „Jetzt einrichten“ [„Настроить“] и разрешите приложению отправлять вам уведомления. Подтвердите действие нажатием на „Erlauben“ [„Разрешить“] и установите для приложения надёжный пароль.

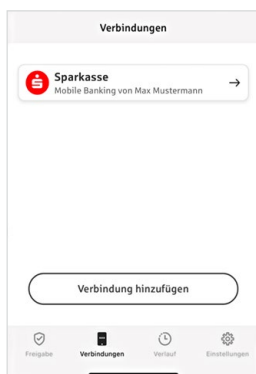
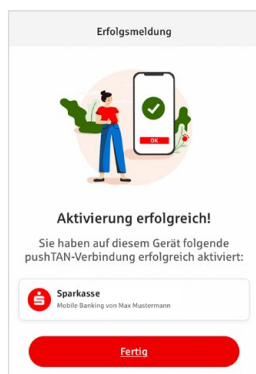
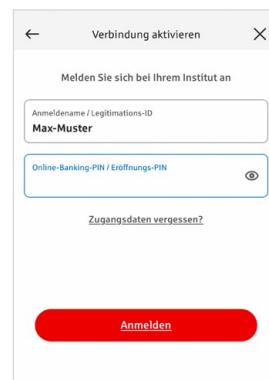
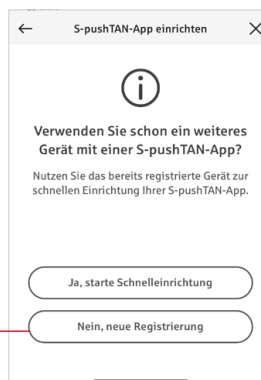
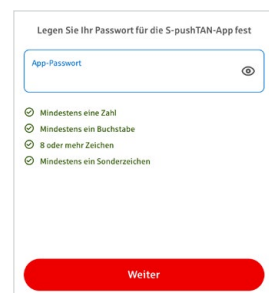
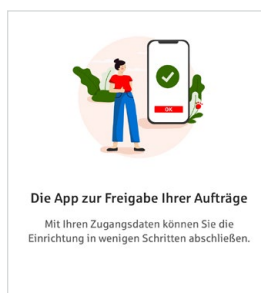
Пароль должен состоять не менее чем из 8 символов (цифры, буквы и один специальный знак).

На следующем этапе вы можете решить, хотите ли вы разблокировать приложение с помощью биометрической функции, например Face ID, или с помощью пароля.

3. Нажмите „Nein, neue Registrierung“ [„Нет, новая регистрация“], затем „Ja, Registrierungsdaten vorhanden“ [„Да, регистрационные данные доступны“].

Чтобы активировать соединение, отсканируйте QR-код из письма про регистрацию с помощью камеры смартфона.

Затем подтвердите свою личность, введя данные доступа к онлайн-банкингу.



Новые клиенты

Если вы являетесь новым клиентом, введите после этого новый PIN-код в качестве своего личного PIN-кода.

После того, как система подтвердит ваш новый PIN-код, вы сможете пользоваться услугами в полном объеме.

Вы увидите подтверждение успешной активации соединения pushTAN.

На вкладке „Соединения“ [„Verbindungen“] приведены ваши сохраненные соединения pushTAN, и вы можете

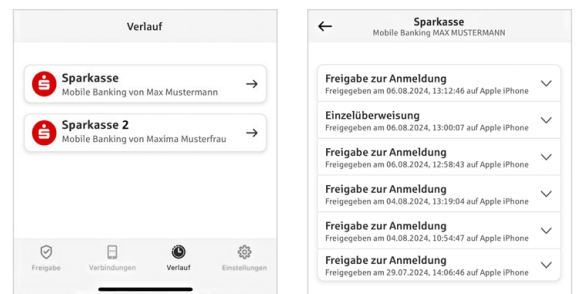
„S-pushTAN“ – приложение для одобрения платежей и подтверждения личности

Кстати: с помощью приложения „S-pushTAN“ вы сможете:

- подтверждать платежные операции в онлайн-банкинге
- подтверждать карточные интернет-платежи (уровень безопасности 3D Secure) по банковским картам Sparkasse и кредитным картам Sparkasse
- подтверждать свою личность при обращении к нам по телефону

История выдачи подтверждений

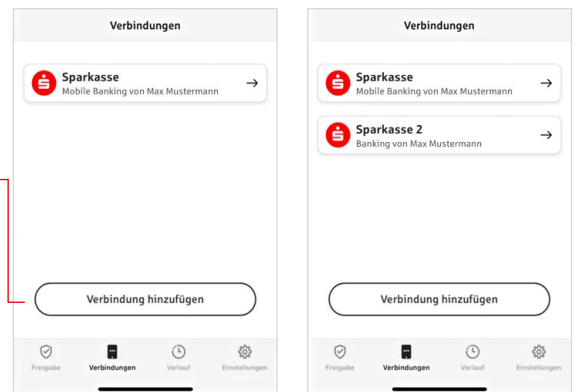
Вы можете просмотреть свои одобрения задним числом в приложении pushTAN в разделе «История» [„Verlauf“].



Добавлять соединения pushTAN

Для того, чтобы добавить другие соединения pushTAN, например, соединения других банков Sparkasse, войдите в приложение „S-pushTAN“.

1. Щелкните на пункте „Соединения“ [„Verbindungen“], а затем на пункте „Добавить соединение“ [„Verbindung hinzufügen“].
2. Действуйте в ранее описанном порядке, чтобы настроить соединение pushTAN. Повторного присвоения пароля для приложения не требуется.
3. После успешной настройки вам будет показано новое соединение pushTAN.pushTAN.



Управление соединениями pushTAN

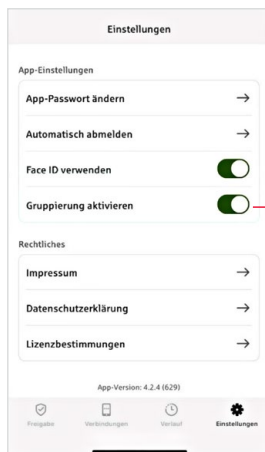
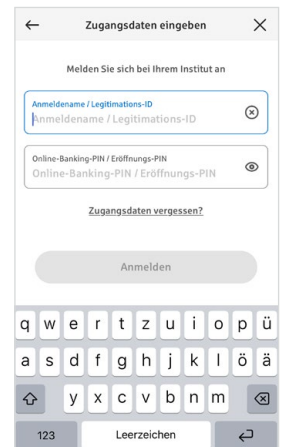
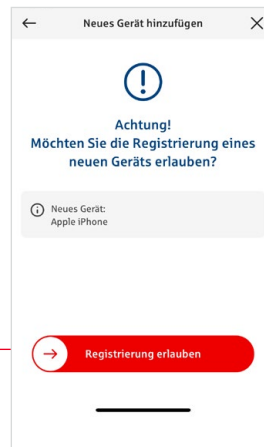
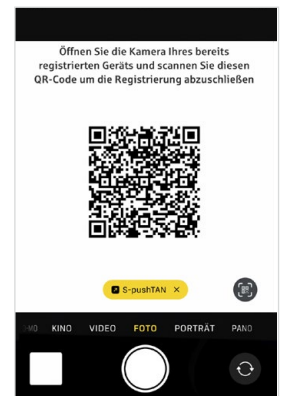
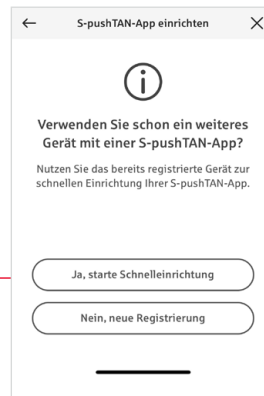
В разделе „Соединения“ [„Verbindungen“] вы можете управлять своими зарегистрированными соединениями pushTAN: активировать функцию Face-ID, блокировать соединение, управлять вашими устройствами и задавать конфигурацию групп рассылки.

Добавить новое устройство

(Bluetooth должен быть активирован на обоих устройствах)

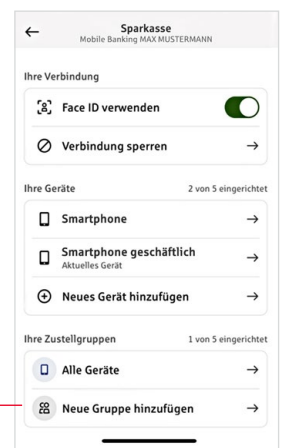
Способы соединения с pushTAN также могут быть зарегистрированы на нескольких устройствах. Чтобы добавить еще одно устройство, войдите в приложение „S-PushTAN“ на новом устройстве. Нажмите „Ja, starte Schnelleinrichtung“ [„Да, запустить быструю настройку“], затем нажмите „Weiter“ [„Далее“].

1. Создайте QR-код, который соединит два устройства друг с другом.
2. Отсканируйте QR-код с помощью специального приложения на вашем старом устройстве. Приложение S-pushTAN запустится автоматически. Выберите способ соединения, который вы хотите настроить на новом устройстве.
Как только на экране появится ваше новое устройство, смахните кнопку „Registrierung erlauben“ [„Разрешить регистрацию“] слева направо. Подтвердите свою личность с помощью пароля для приложения или ваших биометрических данных.
3. Введите данные доступа к онлайн-банкингу на новом устройстве.
Все зарегистрированные устройства отображаются в разделе „Ваши устройства“ [„Ihre Geräte“].



Конфигурирование групп

Если вы используете функцию pushTAN на нескольких устройствах, вы можете задать конфигурацию групп. В разделе „Настройки“ [„Einstellungen“] активируйте функцию „Активировать группировку“ [„Gruppierung aktivieren“]. Затем перейдите в пункте „Соединения“ [„Verbindungen“] в соответствующее соединение pushTAN. С помощью функции „Добавить новую группу“ [„Neue Gruppe hinzufügen“] выполнить конфигурацию.



Пользование pushTAN в онлайн-банкинге

Для подтверждения платежных операций на нашем веб-сайте на компьютере или в приложении на смартфоне/планшете, соблюдайте следующий порядок действий:

1. Авторизуйтесь на нашем веб-сайте (www.sparkasse-hannover.de) или запустите свое банковское приложение.
2. Введите данные для желаемой платежной операции (например, перечисление денег) и подтвердите ввод.
3. Перейдите в приложение „S-pushTAN“. После ввода пароля S-pushTAN вам будут показаны данные платежной операции.

Сверьте показанные данные со своими.

→ Тип распоряжения

→ Номер IBAN получателя

→ Сумма

→ Дата

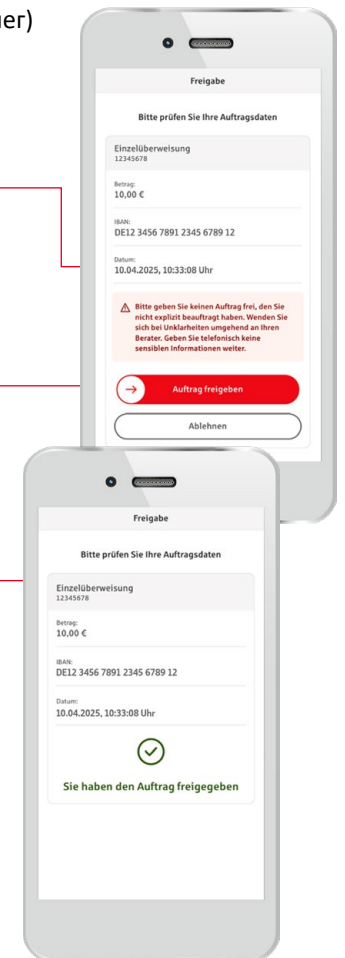
В случае расхождений следует немедленно прервать процесс и обратиться к консультанту или в наш центр по работе с клиентами.

4. Если данные совпадают, подтвердите платеж, проведя пальцем по кнопке „Auftrag freigeben“ вправо.

Разблокируйте устройство с помощью биометрических функций, например Face ID.

Вы сразу увидите уведомление о подтверждении операции.

Указание: Всегда обновляйте приложение „S-pushTAN“ и операционную систему своего смартфона.



Контакт

У вас появились вопросы касательно онлайн-банкинга?

Мы охотно проконсультируем вас в личной беседе.

Sparkasse Hannover
Raschplatz 4
30161 Hannover

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

Положение об отказе от ответственности

Настоящее руководство составлено в соответствии с текущим уровнем знаний и предназначено для обслуживания клиентов. Возможные отклонения в изображениях не являются предметом ответственности Sparkasse или авторов. Ответственно за ущерб, которые может быть понесен, не принимается.

Stand: 04/2025 BFG © e-liberate GmbH, Lüneburg

Указания для усиления безопасности в интернете

Прежде чем пользоваться онлайн-банкингом или расплачиваться вашей кредитной картой в интернете, посвятите несколько минут ознакомлению с нижеследующими важными сведениями.

В интернет – во всеоружии

Если соблюдать важные основные правила, можно в значительной мере защитить себя от атак из интернета. Пояснения на тему распознавания попыток мошенничества и повышения безопасности вашего компьютера и доступа в интернет, а также важные указания по выявленным попыткам мошенничества вы найдете по адресу

www.sparkasse-hannover.de/sicherheit

- Регулярно обновляйте операционную систему и используемые программы.
- Не в коем случае не работайте со своего компьютера в статусе администратора.
- Пользуйтесь брандмауэром и антивирусной программой, поддерживайте их всегда в актуальном состоянии.
- По окончании операций через интернет всегда очищайте память браузера и кэш-память.
- Ни в коем случае не производите банковские операции или онлайн-покупки через чужой вай-фай.
- Не сохраняйте личных данных доступа на чужих порталах, не сообщайте их третьим лицам.
- Следите за тем, чтобы онлайн-сделки производились только через закодированное соединение.
- Для онлайн-банкинга и покупок в интернете всегда вводите интернет-адрес вручную.
- Не открывайте файлов, вложенных в электронные письма от неизвестных отправителей.
- Никогда не отвечайте на электронные письма и телефонные звонки с запросами подтвердить платежные операции.

Никто из сотрудников банка Sparkasse не потребует от вас назвать свои данные для доступа к онлайн-банкингу – ни в электронном письме, ни по факсу, ни по телефону, ни лично.

Безопасный онлайн-банкинг и платежи в интернете

Необходимо в обязательном порядке соблюдать эти правила:

Лучше: сохранять бдительность

Проведя пальцем по кнопке „Auftrag freigeben“ или введя TAN, перевод обычно подтверждается с вашего счета. Не забывайте об этом, когда вас просят предоставить ваши банковские реквизиты, подтвердить платежную операцию или ввести TAN, если вы не хотите производить эту транзакцию.

Будьте недоверчивы

Если происходит что-нибудь странное, лучше всего прервать действие, как только появились сомнения. Ваш банк Sparkasse, например, никогда не просит подтвердить платежные операции и не требует ввода TAN для участия в лотереях, обновлений системы безопасности или для предполагаемых возвратов платежей.

Тщательно: проверять данные

На дисплее вашего генератора TAN или мобильного телефона отображаются важные данные платежной операции, Если отображаемые данные не соответствуют желаемой платежной операции, немедленно прервите процесс.

Важно: безопасный ввод данных

При вводе данных доступа к онлайн-банкингу: всегда обращать внимание, появился ли в браузере символ замка.

Всегда: быть внимательным

Регулярно проверять операции по своему счету. Это можно сделать как в онлайн-банкинге, так и путем распечатки выписок со счета. Только так вы можете своевременно выявить неправомерные снятия средств, пока не истек срок для претензии.

Ввести ограничения: дневной лимит

Установите дневной лимит для транзакций в онлайн-банкинге. С помощью установления вашего личного лимита вы ограничите возможность несанкционированного доступа.

В случае сомнений: заблокировать доступ

Если у вас возникли подозрения, что при пользовании услугами банкинга что-то не так: заблокируйте свой доступ.

Для этого обращайтесь в свой филиал Sparkasse или по круглосуточному телефону экстренной блокировки 116 116 – на территории Германии бесплатно. Звонить по телефону экстренной блокировки можно также из-за рубежа.