

Онлайн-банкинг с использованием pushTAN

Настройка pushTAN

Предварительные условия для пользования pushTAN:

- У вас есть смартфон или планшет (Android или iOS/Apple)
- Ваш консультант открыл вам доступ к счету с помощью pushTAN
- Вы получили для первичного доступа имя пользования или идентификатор для подтверждения полномочий, а также, если вы заключаете новый договор, то вы получили стартовый PIN-код и регистрационное письмо

Порядок действий следующий:

Предоставление доступа из приложения на вашем смартфоне или планшете

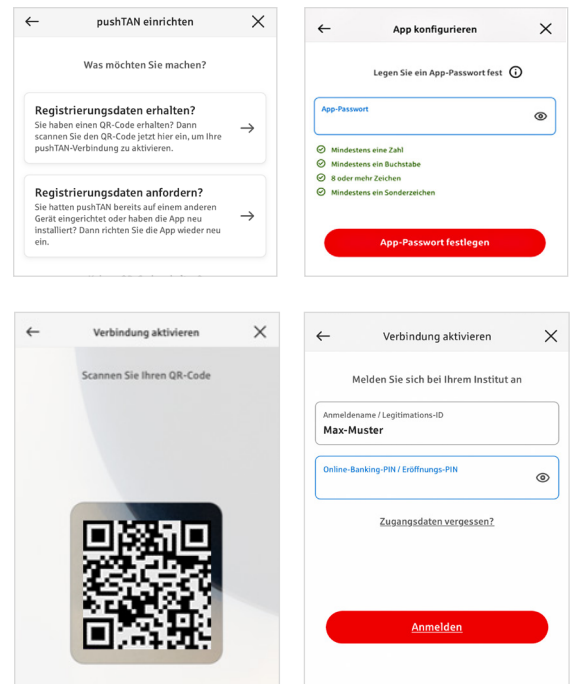
1. Установите приложение „S-pushTAN“ из магазина приложений вашего смартфона (Google Play / App Store).
2. Запустите приложение „S-pushTAN“ и нажмите на клавишу „Jetzt einrichten“ / „Registrierungsdaten erhalten“ («Настроить сейчас» / «Получить регистрационное письмо»). Подтвердите инструкции клавишей „Weiter“ («Дальше»), после чего задайте надежный 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.

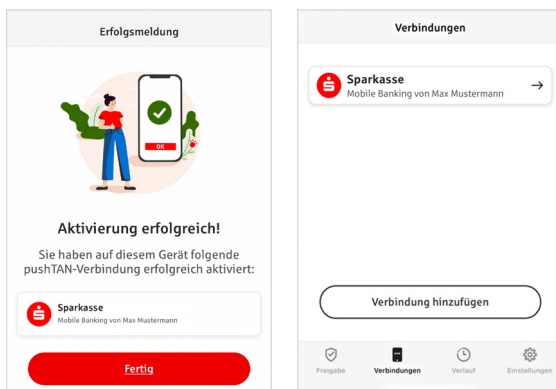
3. С помощью камеры смартфона отсканируйте QR-код из регистрационного письма. Затем от вас потребуется подтвердить свою личность вводом данных для доступа к онлайн-банкингу.

В завершение поступит подтверждение успешной активизации соединения pushTAN.



Изменение кода PIN для онлайн-банкинга

4. 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 услугой в полном объеме.

На вкладке «Соединения» („Verbindungen“) приведены ваши сохраненные соединения pushTAN, и вы можете управлять ими.

„S-pushTAN“ –

приложение для выдачи разрешений и подтверждения идентичности

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

- давать разрешения на выполнение банковских поручений в онлайн-банкинге
- осуществлять платежи с помощью карт в интернете (уровень безопасности 3D Secure) по банковским картам Sparkasse и кредитным картам Sparkasse*
- подтверждать свою идентичность при обращении к нам по телефону*

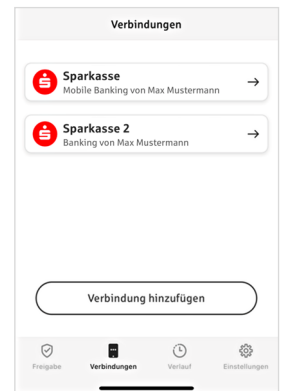
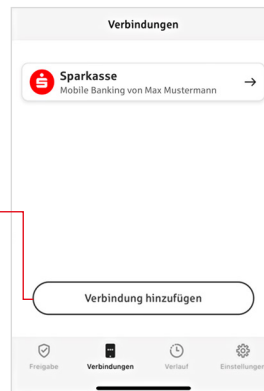
История выпуска

Вы можете просмотреть свои одобрения задним числом в разделе История.

добавлять соединения pushTAN

Для того, чтобы добавить другие соединения pushTAN или 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.



* Доступность может различаться.

Управление соединениями pushTAN

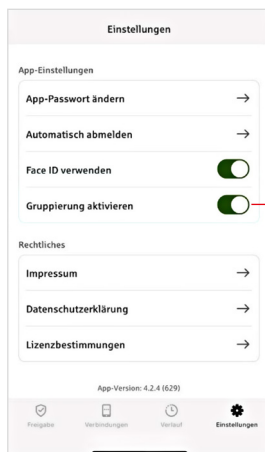
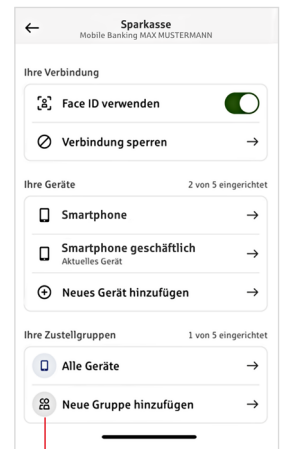
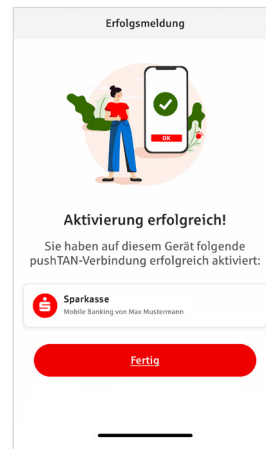
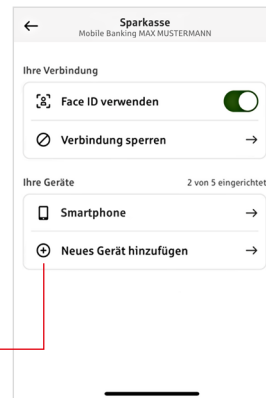
В разделе «Соединения» („Verbindungen“) вы можете управлять своими зарегистрированными соединениями pushTAN: активировать функцию Face-ID, блокировать соединение, управлять вашими устройствами и задавать конфигурацию групп рассылки.

Добавить новое устройство

Соединения pushTAN можно регистрировать также на нескольких устройствах. Для добавления другого устройства (например, планшета), войдите в приложение „S-pushTAN“ на устройстве [A] с помощью существующего соединения.

1. Щелкните на пункте «Соединения» („Verbindungen“), а затем на соединении pushTAN, которым вы хотите пользоваться на другом устройстве.
2. Выберите пункт «Добавить новое устройство („Neues Gerät hinzufügen“) и следуйте инструкциям, пока не будет показан QR-код.
3. На новом устройстве [B] уже установлено приложение „S-pushTAN“. Запустите приложение, выберите пункт «Получить регистрационные данные» („Registrierungsdaten erhalten“) и следуйте вышеприведенным инструкциям, чтобы настроить соединение pushTAN. Используйте QR-код, показанный на устройстве [A].

Выберите среди ваших устройств все те, которые уже зарегистрированы.



Конfigurирование 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 отдачи распоряжений в нашем интернет-филиале на компьютере или находясь в пути, с помощью смартфона или планшета, соблюдайте следующий порядок действий:

1. Войдите в наш интернет-филиал (www.kreissparkasse-heinsberg.de) или запустите свое банковское приложение.
2. Введите данные для желаемого распоряжения (например, перечисление денег) и подтвердите ввод.
3. Перейдите в приложение „S-pushTAN“. После ввода пароля S-pushTAN вам будут показаны данные платежного распоряжения.

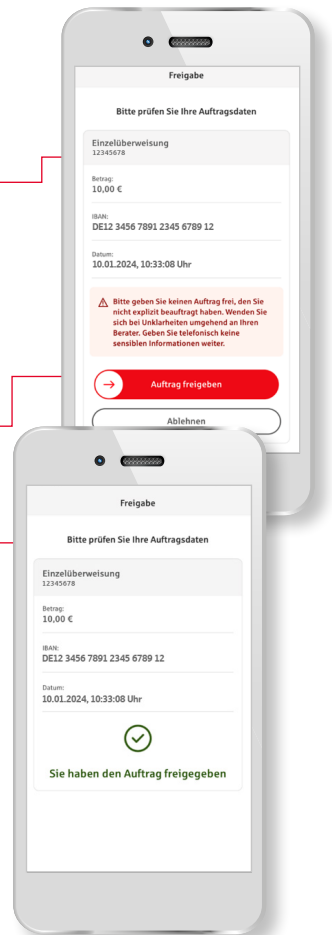
Сверьте показанные данные со своими.

- 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. Или разблокируйте устройство с помощью биометрических функций, например Face ID.
Вам немедленно поступит сообщение о приеме распоряжения к исполнению.

Указание: постоянно поддерживайте приложение „S-pushTAN“ и операционную систему своего смартфона (планшета) в актуальном состоянии.



Контакт

У вас появились вопросы касательно онлайн-банкинга?
Мы охотно проконсультируем вас в личной беседе.

Kreissparkasse Heinsberg

Dr.-Eberle-Platz 1
41812 Erkelenz

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

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 посягательств 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.kreissparkasse-heinsberg.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.
- Не отвечайте на электронные письма, содержащие запрос вашей конфиденциальной информации, либо предложение перейти по ссылке.

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.

Безопасные услуги онлайн-банкинга 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 от вас спрашивают о ваших банковских реквизитах или требуют их предоставить, дать разрешение на выполнение поручения 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, как правило, никогда не спрашивает о данных вашего платежного поручения и не требует ввода TAN для участия в азартных играх, для обновлений с целью безопасности или для предполагаемых возвратах платежей.

Тщательно: проверять данные

На дисплее вашего генератора TAN или мобильного телефона отображаются важные данные платежного распоряжения, Если отображаемые данные не соответствуют вашему распоряжению, немедленно прервите процесс.

Сосредоточенно: безопасно вводить данные

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

Всегда: сохранять внимание

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. В пределах ваших собственных границ пользования вы вправе ограничивать несанкционированный доступ.

В случае сомнений: заблокировать доступ

Если у вас возникли подозрения, что при использовании 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.