ООО «Цифровой Платеж»
115088, г. Москва, ул. Шарикоподшипниковская, д.1, помещ.10/5
ОГРН 1137746565934
ИНН/ КПП 7714909651/ 772301001
www.sendy.land , тел. +7(495) 969-29-32

У Т В Е Р Ж Д Е Н О
Приказом Генерального директора
ООО «Цифровой Платеж»
от «15» июля 2025 г. № 12/1-1

Введено в действие с 15.07.2025

ПРАВИЛА

электронного документооборота в системе трансграничных переводов денежных средств (СТПДС)

Москва, 2025

Оглавление

Перечень сокращений

ИБ	–	информационная безопасность
ПЭП	–	простая электронная подпись
УНЭП	–	усиленная неквалифицированная электронная подпись
СТПДС	–	система трансграничных переводов денежных средств
ЭДО	–	электронный документооборот
ЭП	–	электронная подпись

1. Общие положения

1.1. Настоящие «Правила электронного документооборота в системе трансграничных переводов денежных средств (СТПДС)» разработаны в целях реализации требований законодательства Российской Федерации регулирующего отношения в области использования электронных подписей при использовании Сервиса.

1.2. Настоящие Правила устанавливают порядок получения ключей ЭП, использования ЭП в ходе обмена электронными сообщениями при информационно-технологическом взаимодействии между участниками электронного взаимодействия при осуществлении Операций в Сервисе.

1.3. Настоящие Правила обязательны для всех Клиентов, принявших Пользовательское соглашение в отношении мобильного приложения «Sendy».

1.4. Стороны признают юридическую силу электронных подписей, используемых в Сервисе, равнозначной собственноручным подписям Сторон.

1.5. Стороны соглашаются с порядком получения ключей электронной подписи, создания и проверки электронных подписей, установленным настоящими Правилами, и взаимно признают подписи, используемые ими в Сервисе.

1.6. Стороны соглашаются с тем, что в ходе электронного взаимодействия не создается сертификат ключа проверки электронной подписи. Соответствие электронной подписи признакам неквалифицированной электронной подписи, а также принадлежность ключа проверки электронной подписи конкретному участнику электронного взаимодействия обеспечивается механизмами Сервиса.

1.7. В Сервисе используются простая электронная подпись и усиленная неквалифицированная электронная подпись, при этом:

1) ПЭП применяется для подтверждения принадлежности ключа проверки УНЭП конкретному Клиенту;

2) УНЭП применяется для подтверждения авторства электронного сообщения.

2. Термины и определения

Клиент – физическое лицо, принявшее условия Пользовательское соглашение в отношении мобильного приложения «Sendy».

Ключ электронной подписи (закрытый, секретный ключ) – уникальная последовательность символов, предназначенная для создания электронной подписи.

Ключ проверки электронной подписи (открытый ключ) – уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи (далее – проверка электронной подписи).

Ключи – ключ электронной подписи и ключ проверки электронной подписи.

Операция – действия, осуществляемые в мобильном приложении Sendy в рамках использования сервиса СТПДС в целях осуществления перевода денежных средств.

Оператор Платежной системы «Sendy» (Оператор) – ООО «Цифровой платеж» (ОГРН: 1137746565934, ИНН: 7714909651) (регистрационный номер в Банке России №0035 от 30.09.2014).

Перевод денежных средств (Перевод) – действия оператора по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению Получателю денежных средств Плательщика.

Плательщик – физическое лицо, по распоряжению которого осуществляется Перевод денежных средств, предоставляющее денежные средства для осуществления такого Перевода.

Получатель – физическое лицо, в пользу которого направлен Перевод денежных средств.

Простая электронная подпись – электронная подпись, которая посредством использования кода подтверждает факт формирования электронной подписи Участником электронного взаимодействия.

Система (Программный комплекс СТПДС) – программный комплекс, позволяющий оказывать услуги по технологическому взаимодействию между Клиентом и оператором по переводу денежных средств. Система включает в себя мобильное приложение «Sendy» и Сервис «Sendy».

Сервис «Sendy» (Сервис) – программно-аппаратный комплекс Оператора, обеспечивающий информационно-технологическое взаимодействие между участниками электронного взаимодействия при осуществлении Операций в целях осуществления Переводов.

Стороны (участники электронного взаимодействия) – Оператор, Клиенты.

Усиленная неквалифицированная электронная подпись – электронная подпись, которая:

1) получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

2) позволяет определить лицо, подписавшее электронное сообщение;

3) позволяет обнаружить факт внесения изменений в электронное сообщение после момента его подписания;

4) создается с использованием средств электронной подписи.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и, которая используется для определения лица, подписывающего информацию.

3. Порядок получения и использования простой электронной подписи

3.1. В качестве ключа простой электронной подписи используется код, который генерируется Сервисом и направляется Клиенту посредством SMS-сообщения при регистрации Клиента.

3.2. ПЭП используется для подтверждения авторства электронного сообщения, содержащего открытый ключ УНЭП Клиента. Указанное электронное сообщение формируется мобильным приложением «Sendy» и направляется Оператору автоматически в ходе регистрации Клиента.

3.3. При получении электронного сообщения от Клиента Сервис автоматически проверяет подлинность ПЭП. На основании результатов проверки Сервисом принимается решение о регистрации ключа проверки УКЭП Клиента (открытого ключа УКЭП Клиента).

4. Порядок получения и использования усиленной неквалифицированной электронной подписи

Устанавливается следующий порядок получения и использования усиленной неквалифицированной электронной подписи:

4.1. Получение ключей УНЭП Оператора.

4.1.1. Оператор самостоятельно генерирует ключи своей УНЭП.

4.1.2. Закрытый ключ Оператора сохраняется в Сервисе.

4.1.3. Открытый ключ Оператора сохраняется в дистрибутиве мобильного приложения «Sendy» и устанавливается в хранилище ключевой информации устройства Клиента непосредственно в ходе инсталляции мобильного приложения.

4.2. Получение ключей УНЭП Клиента.

4.2.1. Ключи УНЭП Клиента генерируются в ходе установки мобильного приложения «Sendy» на устройство Клиента с использованием механизмов устройства Клиента.

4.2.2. Ключи УНЭП Клиента устанавливаются (записываются) в хранилище ключевой информации устройства Клиента непосредственно в ходе инсталляции мобильного приложения «Sendy» с использованием механизмов устройства Клиента.

4.2.3. Открытый ключ Клиента в ходе регистрации Клиента в Сервисе направляется Оператору с использованием механизмов мобильного приложения «Sendy». Авторство электронного сообщения, содержащего открытый ключ УНЭП Клиента, подтверждается ПЭП Клиента.

4.2.4. При получении сообщения от Клиента Сервис проверяет корректность ПЭП Клиента. При подтверждении корректности ПЭП Сервис сохраняет открытый ключ УНЭП Клиента и регистрирует соответствие конкретного открытого ключа УНЭП конкретному Клиенту.

4.3. Использование УНЭП.

4.3.1. УНЭП Клиента и Оператора используются в ходе обмена электронными сообщениями, содержащими в том числе служебную информацию, необходимыми для осуществления Операций с использованием Сервиса. При этом:

1) закрытые ключи участников ЭДО применяются для автоматического наложения ЭП на отправляемые электронные сообщения;

2) открытые ключи участников ЭДО используются для автоматической проверки авторства и целостности полученных электронных сообщений.

4.4. Подтверждение подлинности (корректности) ЭП.

4.4.1. Подтверждение подлинности ПЭП обеспечивается Сервисом за счет сверки кода, направленного Клиенту при его регистрации, с кодом, поступившем с устройства Клиента при его регистрации. В случае соответствия кодов ПЭП признается корректной.

4.4.2. Подтверждение подлинности УНЭП обеспечивается Сервисом при одновременном выполнении следующих условий:

1) с помощью криптографических средств подтверждено отсутствие изменений, внесенных в электронное сообщение после его подписания, установлен ключ проверки УНЭП, соответствующий ключу УНЭП, который использовался для создания электронной подписи;
2) ключ проверки УНЭП совпадает с ключом проверки, принадлежащим участнику электронного взаимодействия, отправившему электронное сообщение;
3) участник обмена не отзывал (не аннулировал) свой ключ проверки УНЭП.

5. Обеспечение безопасности при обмене электронными сообщениями

5.1. Обеспечение безопасности ПЭП обеспечивается за счет:

1) обеспечения конфиденциальности ключа ПЭП Клиентом до конца процедуры регистрации;
2) разграничения доступа к устройству Клиента, исключающего вмешательство неуполномоченных лиц в процедуру получения/ использования ключа ПЭП;
3) разграничения доступа к серверным компонентам Сервиса, исключающего вмешательство неуполномоченных лиц в процедуру генерации/ отправки/ проверки ключа ПЭП;
4) обеспечения конфиденциальности ключа ПЭП при передаче Клиенту за счет шифрования средствами мобильной телефонной связи;
5) обеспечения конфиденциальности ключа ПЭП при передаче Оператору за счет шифрования средствами, встроенными в мобильное приложение, Сервис, операционную систему приложения Клиента;
6) проведения специальной оценки соответствия, подтверждающей исполнение регуляторных требований в области защиты информации[1].

5.2. Обеспечение безопасности закрытого ключа УНЭП обеспечивается за счет:

1) разграничения доступа к устройству Клиента с закрытым ключом, исключающего доступ к закрытому ключу неуполномоченных лиц;
2) разграничения доступа к серверным компонентам Сервиса с закрытым ключом, исключающего доступ к закрытому ключу неуполномоченных лиц;
3) проведения специальной оценки соответствия, подтверждающей исполнение регуляторных требований в области защиты информации.

5.3. Обеспечение безопасности электронных сообщений обеспечивается за счет использования средств шифрования, обеспечивающих конфиденциальность, контроль авторства и неизменности электронных сообщений (шифрование информации при передаче по открытым каналам связи и механизмы электронной подписи).

[1] Соответствие по требованиям к оценочному уровню доверия не ниже, чем ОУД4, предусмотренного пунктом 7.6 раздела 7 национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013

6. Плановая смена ключей УНЭП

6.1. Плановая смена ключей УНЭП не предусматривается.

7. Внеплановая смена ключей УНЭП

7.1. Внеплановая смена ключей Клиента осуществляется за счет повторного прохождения процедуры регистрации.

7.2. Внеплановая смена ключей Оператора осуществляется за счет обновления мобильного приложения Клиента.

8. Отзыв ключей УНЭП

8.1. Отзыв ключей Клиента осуществляется при внеплановой смене ключей УНЭП за счет блокировки возможности осуществления переводов и повторного прохождения процедуры регистрации.

9. Приостановление работ Клиентом в системе денежных переводов

9.1. В ходе приостановки работы Клиента в СТПДС ключи УНЭП не отзываются, после возобновления работы могут использоваться ранее выпущенные ключи.

10. Прекращение работ Клиентом в системе денежных переводов

10.1. В ходе прекращения работы Клиента в СТПДС ключи УНЭП отзываются (удаляются) в момент удаления мобильного приложения. При возобновлении работ требуется повторное прохождение процедуры регистрации.

11. Разбор конфликтных ситуаций

11.1. Споры и разногласия, возникающие между участниками при использовании системы электронного документооборота в Сервисе, применении средств шифрования и электронной подписи, решаются путем переговоров между участвующими в конфликте Сторонами.

11.2. Непосредственно платежные документы/ поручения в Сервисе не формируются и не хранятся. Сервис предназначен исключительно для организации технологического взаимодействия между Клиентом и оператором по переводу денежных средств, непосредственно осуществляющим перевод денежных средств. Исходя из данной особенности разбор конфликтных ситуаций заключается исключительно в определении принадлежности конкретного ключа ЭП конкретному Клиенту.

11.3. В случае возникновения конфликтной ситуации между участниками ЭДО по поводу принадлежности ЭП, которую не удается решить путем переговоров между Сторонами ЭДО, Оператор организует проведение технической экспертизы.

11.4. В целях расследования спорной ситуации Оператор создает специальную комиссию, в которую входит равное количество представителей от каждой из Сторон, но не более 2-х человек. По инициативе каждой из Сторон (и с согласия другой Стороны) в состав комиссии могут включаться независимые эксперты, но не более 2-х человек.

11.5. Разбор конфликтной ситуации заключается в доказательстве принадлежности или не принадлежности ключей ЭП конкретному Участнику электронного взаимодействия.

11.6. Разбор конфликтных ситуаций, связанных с простой электронной подписью.

11.6.1. Разбор конфликтной ситуации основывается на анализе регистрационной информации о ходе генерации кода регистрации и отправке его Клиенту, а также информации о полученном Оператором электронном сообщении, содержащем открытый ключ Клиента, подписанным с помощью ПЭП (кода регистрации).

11.6.2. Источником эталонной информации о ключе ПЭП является база данных Оператора.

11.6.3. В ходе проверки комиссия сверяет информацию о коде активации из эталонного источника с данными компонента СТПДС, осуществляющего сверку кодов в ходе регистрации Клиента.

11.6.4. В случае совпадения ключей ЭП (кода, отправленного Клиенту и кода, полученного от Клиента в ходе его регистрации) – комиссия делает вывод о необоснованности претензий и завершает работу.

11.6.5. В случае несовпадения ключей ЭП – комиссия делает вывод об обоснованности претензий. Целесообразность дальнейшей работы комиссии решается Сторонами в ходе дальнейших переговоров и расследовании выявленного инцидента ИБ.

11.7. Разбор конфликтных ситуаций, связанных с усиленной неквалифицированной электронной подписью.

11.7.1. Разбор конфликтной ситуации основывается на математических свойствах алгоритмов несимметричных криптографических преобразований, которые заключаются в использовании двух взаимосвязанных криптографических ключей (ключевая пара в составе закрытого ключа ЭП и открытого ключа проверки ЭП) и гарантии невозможность подделки значения ЭП любым лицом, не обладающим секретным криптографическим ключом ключевой пары, либо невозможности генерации (определения) закрытого ключа на основе открытого ключа.

11.7.2. Для разбора конфликтных ситуаций комиссия использует специальные программные средства Оператора, информацию из баз данных Оператора, содержащую открытый ключ УКЭП.

11.7.3. В случае обоснованной необходимости комиссия (в соответствии с настоящими Правилами) может проверить корректность ПЭП, которая использовалась при регистрации открытого ключа УНЭП Клиента.

11.7.4. Проверка подтверждения подлинности УНЭП осуществляется специальными программными средствами Оператора (на основе утверждения п.11.7.1.), которые выдают заключение о корректности ключей УНЭП.

11.7.5. В случае подтверждения принадлежности ключей конкретных ключей ЭП конкретному клиенту – комиссия делает вывод о необоснованности претензий и завершает работу.

11.7.6. В случае если проверка УНЭП дала отрицательный результат – комиссия делает вывод об обоснованности претензий. Целесообразность дальнейшей работы комиссии решается Сторонами в ходе дальнейших переговоров и расследовании выявленного инцидента ИБ.