**ПОРЯДОК ОФОРМЛЕНИЯ ДОКУМЕНТОВ C ИСПОЛЬЗОВАНИЕМ СТАНДАРТА ISO20022 ПРИ ОБМЕНЕ ФИНАНСОВЫМИ СООБЩЕНИЯМИ МЕЖДУ ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» И КЛИЕНТАМИ (далее – Порядок)**

**Оглавление**

[**1.** **Общие положения** 2](#_Toc163649675)

[**2.** **Перечень используемых типов сообщений** 2](#_Toc163649676)

[**3.** **Статусная схема платежных документов** 2](#_Toc163649677)

[**4.** **Передача вложенных файлов** 3](#_Toc163649678)

[**5.** **Требования к электронной подписи (ЭП)** 3](#_Toc163649679)

[**6.** **История изменений Порядка** 7](#_Toc163649680)

1. **Общие положения**
	1. Настоящий Порядок определяет правила оформления в электронном виде расчетных и иных документов (далее – ЭД) в формате ISO20022 при обмене финансовыми сообщениями между ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК» (далее – Банк) и клиентом Банка - юридическим лицом (далее – Клиент).
	2. Настоящий Порядок разработан в соответствии с требованиями законодательства Российской Федерации, нормативными актами Банка России, внутренними документами Банка и Рекомендациями Российской Национальной Ассоциации SWIFT для передачи финансовых сообщений.
	3. Настоящий Порядок используется при обслуживании Клиентов на основании договора о дистанционном обслуживании, заключенного в соответствии с Правилами электронного документооборота и дистанционного банковского обслуживания клиентов – юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством Российской Федерации порядке частной практикой, в ПАО «МОСКОВСКИЙ КРЕДИТНЫЙ БАНК».
2. **Перечень используемых типов сообщений**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | **Таблица 1** |
| **Вид****сообщения** | **Вид ЭД** | **Направление** | **Комментарии** |
| **Pain.001** | Платежное поручение  | Клиент -> Банк | Правила оформления приведены в Приложении № 1 к настоящему Порядку |
| Распоряжение на перевод в иностранной валюте (валютный перевод)  | Клиент -> Банк | Правила оформления приведены в Приложении № 2 к настоящему Порядку |
| Распоряжение на списание средств с транзитного валютного счета | Клиент -> Банк | Правила оформления приведены в Приложении № 3 к настоящему Порядку |
|  |  |  |  |
| **Pain.002** | Ответная квитанция Банка о статусе ЭД | Банк -> Клиент | Правила приведены в Приложении № 4 к настоящему Порядку |
|  |  |  |  |
| **Auth.025** | Справка о подтверждающих документах | Клиент -> Банк | Правила оформления приведены в Приложении № 5 к настоящему Порядку |
| **Auth.024** | Информация о коде вида операции | Клиент -> Банк |
|  |  |  |  |
| **Camt.060** | Запрос выписки | Клиент -> Банк | Правила оформления приведены в Приложении № 6 к настоящему Порядку |
| **Camt.053[[1]](#footnote-1)** | Выписка по счету | Банк -> Клиент |
| **Camt.054** | Уведомление об операции | Банк -> Клиент |

1. **Статусная схема платежных документов**

|  |  | **Таблица 2** |
| --- | --- | --- |
| **№ п/п** | **Код** | **Статус ЭД/сообщения** |
| 1 | RCVD | Получено |
| 2 | RJCT | Отклонено |
| 3 | ACTC | Принято, проверены подлинность и формат |
| 4 | ACSC | Исполнено |
| 5 | ACSP | Принято к исполнению |
| 6 | ACCP | Принято, проверены реквизиты плательщика |

В ответных квитанциях о статусах распоряжения о переводе денежных средств (платежного документа) Клиента всегда должен быть заполнен реквизит «Статус сообщения/ЭД». Детализация может быть указана в реквизите «Комментарий к статусу».

1. **Передача вложенных файлов**

Передача вложенных файлов реализуется в соответствии с рекомендациями по использованию формата:

* приложенный бинарный файл передается в виде отдельного файла в его исходном формате;
* в XML-документе (в теге …/Attchmnt/URL) указывается ссылка (имя) приложенного файла;
* в XML-документе (в теге …/Attchmnt/LkFileHash) заполняется хэш файла;
* для обеспечения синхронной передачи документа и приложенных к нему файлов они помещаются и передаются получателю в виде ZIP архива;
* архиву присваивается имя XML файла с добавлением расширения “.zip”;
* для исключения проблем с кодировкой на разных платформах имена всех файлов в ZIP архиве должны представляться в кодировке UTF-8;
* для обеспечения уникальности имени приложенного файла к исходному имени файла добавляется идентификатор отправителя, дата и время формирования сообщения;
* для упрощения идентификации файлов внутри ZIP архива к имени приложенных файлов добавляется префикс "attach\_".

Алгоритм формироания электронной подписи (ЭП) при наличии приложений к XML-документу не изменяется: подписывается все содержимое XML-документа, включая хэши вложений.

Структура пакета из XML-файла с приложенным документом:



1. **Требования к электронной подписи (ЭП)**
	1. **Описание ЭП**

Все ЭД подписываются единообразно, независимо от версии типового сообщения стандарта ISO20022, используемого при их создании. ЭП помещается в секцию SplmtryData. Подписанный ЭД представляет собой Document, в котором добавлена секция SplmtryData, содержащая одну или несколько ЭП.

Таким образом подписанный ЭД представляет тег верхнего уровня Document, в него вложен тег (DocumentSpecificTag), наименование которого зависит от типа ЭД (тег CstmrCdtTrfInitn для pain.001, тег BkToCstmrStmt для camt.053 и т.п). Внутри этого тега расположена секция SplmtryData, содержащая одну или несколько ЭП.

<Document>

 <DocumentSpecificTag>

 …содержимое документа…

 <SplmtryData>

 …подписи…

 </SplmtryData>

 </DocumentSpecificTag >

</Document>

ЭП поставляется под всем ЭД, за исключением тега SplmtryData содержащего блок ЭП.

Структура секции SplmtryData приведена в Таблице 3.

|  |  |  |
| --- | --- | --- |
|  |  | **Таблица 3** |
| **Наименование секции /поля** | **Режим** | **Описание поля** |
| SplmtryData  | [1..1] | Секция для размещения произвольных данных |
| Envlp  | [1..1] | Секция, содержащая произвольный блок данных |
| SgntrSt  | [1..1] | Секция для размещения ЭП |
| Signature  | [1..n] | ЭП по стандарту XML Signature |

* 1. **Требования к формированию ЭП**
1. При наличии в подписываемом ЭД секции SplmtryData, содержащей блок ЭП, данная секция должна быть исключена из ЭД, подлежащего подписанию.
2. Перед подписанием ЭД должен быть трансформирован (каноникализирован) согласно документу **Canonical XML 1.0** <https://www.w3.org/TR/xml-c14n.html>. Метод каноникализации - <http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments>.
3. Для ЭД, полученного после шагов a), b), ЭП генерируется в формате XML Digital Signature согласно документу **XML Signature Syntax and Processing** <https://www.w3.org/TR/xmldsig-core/> с применением алгоритмов ГОСТ 34.11-2012.
4. Полученная структура ЭП размещается в ЭД в теге /Document/DocumentSpecificTag/SplmtryData/Envlp/SgntrSt/Signature. В случае если в ЭД уже есть одна или несколько ЭП, полученная ЭП размещается в дополнительном теге /Document/DocumentSpecificTag/SplmtryData/Envlp/SgntrSt/Signature
5. При наличии в подписываемом ЭД секции SplmtryData, содержащей бизнес-данные (//Document/DocumentSpecificTag/SplmtryData), для подписи создается новая секция SplmtryData.
6. Результирующий документ представляет собой подписанный ЭД.
7. Количество ЭП в итоговом ЭД не ограничено.
	1. **Требования к проверке ЭП**
8. Для проверки ЭП применяется весь ЭД за исключением секции SplmtryData, содержащей блок ЭП. Данная секция должна быть исключена из ЭД при проверке ЭП.
9. Перед проверкой ЭД должен быть трансформирован (каноникализирован) согласно документу **Canonical XML 1.0** <https://www.w3.org/TR/xml-c14n.html>. Метод каноникализации - <http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments>
10. Для ЭД, полученного после шагов a), b), ЭП в формате XML Digital Signature проверяется согласно документу **XML Signature Syntax and Processing** <https://www.w3.org/TR/xmldsig-core/> с применением алгоритмов ГОСТ 34.11-2012.
	1. **Формирование ЭП**

Формирование ЭП под ЭД должно выполняться по следующему алгоритму действий:

1. **Подготовка ЭД к подписанию**

Если в документе есть секция SgntrSt:

* сохранить в оперативную память секцию SplmtryData, содержащую секцию SgntrSt с ранее проставленными ЭП;
* удалить секцию SplmtryData из ЭД;
* результатом является ЭД без секции SplmtryData и сохраненная секция SplmtryData.

Если в ЭД нет секции SgntrSt результатом является исходный ЭД.

1. **Каноникализация ЭД**

Перед подписанием ЭД, подготовленный на шаге 1, должен быть обработан (каноникализирован) в порядке, предусмотренном п. 5.2 настоящего Порядка.

1. **Формирование ЭП под ЭД**

ЭП под ЭД, который является результатом выполнения шага 2, формируется соответствующим вызовом криптопровайдера с передачей ему на вход ЭД и контейнера закрытого ключа.

ЭП в формате XML Digital Signature генерируется в соответсвии с требованиями, указанными в п. 5.2 настоящего Порядка.

При формироании ЭП должны использваться действующие алгоритмы криптографических преобразований, встроенные в СКЗИ «КриптоПро CSP» и «КриптоПро Java CSP».

1. **Размещение ЭП в секцию SplmtryData.**

Если на шаге 1 был оставлен исходный ЭД, для первой ЭП:

* создать новую секцию SplmtryData;
* в секции Signature указать атрибут ID = 0 и разместить в ней ЭП.

Если на шаге 1 была сохранена секция SplmtryData, содержащая ЭП:

* в сохраненной секции SplmtryData найти секцию Signature с максимальным значением атрибута ID (N);
* в сохраненной секции SplmtryData добавить секцию Signature с атрибутом ID = N+1, разместить в ней ЭП;
* добавить обновленную секцию SplmtryData в ЭД.

Если требуется поставить несколько ЭП, надо повторить шаги 2-4 нужное количество раз.

* 1. **Проверка ЭП под ЭД**
1. Сохранить в оперативную память все ЭП из секции SplmtryData;
2. Удалить из ЭД секцию SplmtryData, содержащую ЭП;
3. Выполнить процедуру каноникализации согласно требованиям, указанным в п. 5.3 Настоящего Порядка.
4. Для каждой ЭП из хранилища модуля формирования и проверки ЭП на основании серийного номера и имени издателя извлекается сертификат ключа проверки ЭП (открытого ключа).
5. В случае отсутствия сертификата, будет сформирована ошибка проверки ЭП под ЭД.
6. Проводится проверка валидности сертификата, извлеченного из хранилища:
* проверка наличия сертификата в списке отозванных сертификатов. Если сертификат находится в списке отозванных, то сертификат некорректный. При этом будет сформирована ошибка проверки ЭП под ЭД;
* окончание срока действия сертификата. Если срок действия сертификата закончился, то сертификат считается некорректным. При этом будет сформирована ошибка проверки ЭП под ЭД;
* проверка принадлежности сертификата издателя списку доверенных сертификатов издателей Банка. Если сертификат выпущен сертификатом издателя, не входящим в список доверенных издателей Банка, то сертификат считается некорректным. При этом будет сформирована ошибка проверки ЭП под ЭД.
1. Для каждой ЭП в процедуру проверки передается:
* ЭД, подготовленный на шаге 2;
* сертификат ключа проверки ЭП (открытого ключа);
* ЭП в формате XML Digital Signature.

Для проверки ЭП должны использоваться алгоритмы ГОСТ Р 34.11-2012). Модуль должен использовать действующие алгоритмы криптографических преобразований, встроенные в СКЗИ «КриптоПро CSP» и «КриптоПро Java CSP».

1. В случае выявления нарушенной ЭП формируется соответствующее сообщение об ошибке.
2. Для данных с успешно проверенной ЭП формируется успешный результат проверки ЭП.
3. **История изменений Порядка**

|  |  |  |
| --- | --- | --- |
| **Документ** | **Дата** | **Описание изменения** |
| **Версия 1.0** | **26.02.2020** | **Утверждение первой редакции Порядка** |
| **Версия 1.1** | **02.04.2020** | **Уточнения по описанию полей сообщения pain.002** |
| **Версия 1.2** | **17.08.2020** | **Уточнения по порядку формирования ЭП и используемых ГОСТах** |
| **Версия 1.2** | **17.08.2020** | **Добавлены тэги для указания внутреннего клиентского номера расходной операции в сообщении pain.001** |
| **Версия 1.2** | **17.08.2020** | **Добавлены тэги для отражения клиентского номера расходной операции и уникальный номер транзакции в выписке (сообщение camt.053)** |
| **Версия 1.3** | **07.02.2022** | **Добавлен блок SplmtryData используемый для передачи ЭП подписанта документа со стороны Банка (сообщение camt.053)** |
| **Версия 1.4** | **25.03.2022** | **Уточнения по описанию полей сообщения pain.002** |
| **Версия 1.5** | **17.10.2022** | **Уточнения по описанию полей сообщения pain.001** |
| **Версия 1.6.**  | **01.06.2024** | **Описание форматов выненесно в отдельные приложения.** **Выполнены уточнение по описанию полей. Добавлено описание на английском языке** |

1. *Сообщение camt 053, полученное до времени, установленного договором о дистанционном обслуживании как время предоставления выписки о движении денежных средств по счету Клиента, может содержать не окончательную информацию об операциях по счету, балансе счета* [↑](#footnote-ref-1)