Акционерное общество «Национальная платежная корпорация Национального Банка Республики Казахстан»

Утвержден
решением Правления
АО «НПК»
от «23» 04 2024 года
(протокол № 8)

Структура и порядок формирования транспортных сообщений в платежных системах Казахстана

Рег. № 55

г. Алматы

Оглавление

Глава 1. Введение ---- 4
Глава 2. Область применения ---- 4
Глава 3. Термины и определения ---- 4
Глава 4. Бизнес-слой. Структура бизнес-сообщений ---- 5
Глава 5. Слой транспортировки сообщений ---- 6
Глава 6. Структура конверта сообщения ---- 6
Глава 7. Прикладной слой ---- 7
Глава 8. Подписание и проверка ЭЦП бизнес-сообщений ---- 8
Параграф 1. Основная часть сообщения ---- *8*
Параграф 2. Подписание сообщения ---- *8*
Параграф 3. Проверка ЭЦП сообщений ---- *9*
Глава 9. Сжатие, шифрование, расшифровка и восстановление сообщений ----10
Параграф 1. Сжатие и шифрование сообщения ----*10*
Параграф 2. Расшифровка и восстановление сообщения ----*11*
Глава 10. Подписание ЭЦП транспортного сообщения ----11
Глава 11. Параметры маршрута транспортного сообщения ----11
Приложение 1 ----12

Глава 1. Введение

1. Структура и порядок формирования транспортных сообщений в платежных системах Казахстана (далее – Порядок) содержит требования по реализации обмена сообщениями в соответствии с международным стандартом ISO 20022 «Финансовые услуги – Универсальная схема сообщений для финансовой отрасли» (Financial services - Universal financial industry message scheme) (далее – стандарт ISO 20022).

2. В соответствии с положениями документа ISO 20022-6 «Характеристики транспортировки сообщений» (ISO 20022-6 «Message transport characteristics») стандарта ISO 20022 обмен данными выполняется в следующих слоях (далее - Слой):

1) бизнес-слой – самый верхний слой, в котором определены правила и сценарии обмена бизнес-сообщениями, а также структуры бизнес-сообщений, используемых в процессах обмена в рамках конкретных моделей;

2) слой транспортировки сообщений – слой, в котором определены правила обмена электронными сообщениями, независимо от бизнес-слоя.

3. Порядок определяет требования по обмену сообщениями в рамках платежных систем (Межбанковская система переводов денег, Система межбанковского клиринга и Система массовых электронных платежей) в каждом из указанных выше слоев. Соблюдение требований обеспечивает функциональную совместимость (интероперабельность) взаимодействующих в рамках платежных и информационных систем, поддерживающих рекомендации стандарта ISO 20022. Требования к форматам сообщений бизнес-слоя определены во внутренних документах, регламентирующих порядок обмена электронными платежными и информационными сообщениями, и не входят в данный документ.

Глава 2. Область применения

4. Порядок рекомендован к использованию техническими специалистами (разработчиками и администраторами) информационного и программного обеспечения, информационных систем и техническими консультантами при организации информационного взаимодействия между банками и их клиентами - юридическими лицами.

Глава 3. Термины и определения

5. В Порядке применяются следующие термины и определения:

1) бизнес-сообщение – электронное сообщение стандарта ISO 20022, предназначенное для передачи прикладных данных между участниками информационного взаимодействия;

2) система доставки сообщений – механизм, обеспечивающий принятие, транспортировку и доставку транспортных сообщений между участниками информационного взаимодействия;

3) транспортное сообщение – электронный конверт, в который вложено бизнес-сообщение на участке передачи между: клиентом и платежной

системой; клиентом и клиентом. Эти сообщения дополнительно содержат метаданные (информацию о сообщении и его маршрутизации);

4) участник информационного взаимодействия – субъект, который создает, обрабатывает, принимает или отправляет электронные сообщения;

5) base64 – стандарт кодирования последовательности байт в строку символов ASCII и обратно;

6) ЭЦП – электронная цифровая подпись, набор электронных цифровых символов, созданный средствами электронной цифровой подписи по алгоритму СТ РК ГОСТ Р 34.10-2015 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и подтверждающий достоверность электронного документа, его принадлежность и неизменность содержания.

Глава 4. Бизнес-слой. Структура бизнес-сообщений

6. В бизнес-слое обмен данными реализуется путем передачи бизнес-сообщений. Бизнес-сообщение представляет собой совокупность бизнес-заголовка и содержимого сообщения.

7. Бизнес-сообщения содержат только бизнес-данные и не должны содержать информацию о системе доставки сообщений, механизмах адресации, отправки, передачи или получения сообщений, а также прочую информацию, специфичную для использования в слое транспортировки сообщения. Бизнес-сообщения должны содержать всю информацию, необходимую для их корректной интерпретации участниками информационного взаимодействия, и быть понятны вне контекста транспортного конверта.

8. Бизнес-сообщения представлены в виде XML-документов и должны соответствовать соответствующим XSD-схемам и правилам заполнения документов.

9. Бизнес-сообщение имеет следующую структуру:

```
<Envelope>
    <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
        <!-- Содержимое заголовка Бизнес-сообщения -->
    </AppHdr>
    <Document xmlns="urn:iso:std:iso:20022:tech:xsd:xxx.nnn.nnn.nn">
        <!-- Содержимое документа -->
    </Document>
<Envelope>
```

10. В качестве заголовка бизнес-сообщения используется структура Business Application Header (AppHdr). Структура заголовка бизнес-сообщения и порядок ее заполнения для целей использования в платежной системе установлен во внутреннем документе, регламентирующем структуру платежных сообщений в платежных системах Казахстана (далее - Структура платежных сообщений).

Глава 5. Слой транспортировки сообщений

11. Обмен данными в слое транспортировки сообщений выполняется с использованием транспортных сообщений, в которые вложены бизнес-сообщения. Структура транспортных сообщений определена Главой 6 Порядка. Примеры сообщений отображены в Приложении 1 к Порядку.

12. Обмен транспортными сообщениями и бизнес-сообщениями выполняется по следующему сценарию:

1) отправитель формирует бизнес-сообщение;

2) отправитель упаковывает сформированное бизнес-сообщение в транспортное сообщение;

3) отправитель отправляет транспортное сообщение получателю;

4) получатель принимает транспортное сообщение;

5) получатель производит техническую проверку транспортного сообщения;

6) система доставки сообщений формирует извещение об успешном приеме/ошибке приема сообщения.

13. Процедуры вложения (распаковки) транспортного сообщения включают в себя операции в строго последовательном прямом (обратном) порядке:

1) подписания (проверки подписи) ЭЦП бизнес-сообщения;

2) сжатия и шифрования (расшифровывания и восстановления) бизнес-сообщения;

3) подписания ЭЦП транспортного сообщения;

4) установка (извлечение) параметров маршрута транспортного сообщения в (из) заголовки (-ов) HTTP/ MQ API.

Правила выполнения указанных процедур описаны в Главах 7, 8 и 9 Порядка.

14. Отправитель может отправлять одно транспортное сообщение только одному получателю.

15. Недопустимо изменение содержимого бизнес-сообщения при его обработке системами доставки сообщений.

Глава 6. Структура конверта сообщения

16. При описании структуры и правил формирования транспортного сообщения используются спецификации, указанные в Таблице 1 Описания.

Таблица 1. Используемые спецификации

Краткое наименование	Полное наименование
REST	Representational State Transfer. Предоставление услуг внешним пользователям посредством API должно осуществляться с помощью программных интерфейсов на базе архитектурного стиля REST
API	Application Programming Interface

XML-binaryOptimized Packaging	XML-binary Optimized Packaging. W3C Recommendation 25 January 2005. http://www.w3.org/TR/2005/REC-xop10-20050125
XML Encryption 1.1	XML Encryption Syntax and Processing Version 1.1. W3C Recommendation 11 April 2013 https://www.w3.org/TR/xmlenc-core/#sec-Usage
XML 1.0	Extensible Markup Language (XML) 1.0 (Fifth Edition). W3C Recommendation 26 November 2008. http://www.w3.org/TR/2008/REC-xml-20081126
GZIP compression	Обеспечивает сжатие без потерь, иными словами, исходные данные можно полностью восстановить при распаковке. Основанный на алгоритме DEFLATE
СТ РК ГОСТ Р 34.10-2015	Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи
СТ РК ГОСТ Р 34.11-2015	Информационная технология. Криптографическая защита информации. Функция хэширования
ГОСТ 28147-89	Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования
ТУМАР-CSP	Программное средство криптографической защиты информации, предназначенное для авторизации, обеспечения конфиденциальности, гарантии неизменности и контроля целостности информации

17. Транспортный конверт сообщения имеет следующую структуру:

```
<body>
<EncryptedData>
        <CipherData>
        <!-- Преобразованное бизнес-сообщение -->
        </CipherData>
        <ds:Signaturexmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        </ds:Signature>
</EncryptedData>
</body>
```

18. При формировании электронных сообщений используется кодировка UTF-8 (Unicode Transformation Format).

Глава 7. Прикладной слой

19. В качестве протокола передачи данных прикладного слоя участниками информационного взаимодействия выбирается один из протоколов, обеспечивающий требуемые характеристики доставки сообщений, определяемые в бизнес-слое.

Рекомендуется использовать следующие протоколы:

1) HTTPS: Hypertext Transfer Protocol - HTTP/1.1 (RFC 2616) совместно со спецификацией HTTP Over TLS (RFC 2818);

2) Протокол обмена сообщениями Apache Kafka версии 2.8. Для отправки сообщений Producer API, для получения сообщений - Consumer API.
Спецификация Javadoc:

https://kafka.apache.org/28/javadoc/org/apache/kafka/clients/producer/package - summary.html,

https://kafka.apache.org/28/javadoc/org/apache/kafka/clients/consumer/package-summary.html.

Спецификация .Net: https://github.com/confluentinc/confluent-kafka-dotnet.

Глава 8. Подписание и проверка ЭЦП бизнес-сообщений

Параграф 1. Основная часть сообщения

20. Бизнес-сообщение можно условно разделить на две части:

1) Заголовок бизнес-сообщения <AppHdr> – содержит информацию о сообщении и ЭЦП;

2) Бизнес-часть сообщения <Document> – содержит смысловую часть сообщения.

21. Заголовок бизнес-сообщения содержит информацию:

1) об отправителе и получателе;

2) о системе отправителя и системе получателя,

3) ЭЦП сообщения;

4) иную информацию, описанную в Структуре платежных сообщений.

ЭЦП сообщения содержит элементы данных, которые позволяют обеспечить целостность и подлинность сообщения. В данной части сообщения указывается только одна ЭЦП. Выработка и проверка ЭЦП осуществляется в порядке, установленном законодательством Республики Казахстан.

Бизнес-часть сообщения подписывается в обязательном порядке. Структура заголовка бизнес-сообщения и правила ее заполнения для целей использования в платежной системе определены Структурой платежных сообщений. Бизнес-часть сообщения содержит смысловую информацию сообщения, например, информацию о переводе определенной суммы денег с соблюдением определенных условий или информацию о движении денег по счетам, направляемую банком своему клиенту.

Параграф 2. Подписание сообщения

22. Подписание бизнес-части сообщения осуществляется посредством XML-подписи (XML-Signature) по стандарту XML-Signature Syntax and Processing (XMLDSIG). Рекомендация «XML — Signature Syntax and Processing» определяет, что подпись и информация о ней должны содержаться в элементе <Signature>, который в нашем случае включает следующие части:

1. CanonicalizationMethod;
2. SignatureMethod;
3. DigestMethod;
4. DigestValue;
5. SignatureValue;
6. KeyInfo;

7. Object.

Данные подписываются, применяя алгоритм подписания ECGOST34310. Полученный результат помещается в заголовок бизнес-сообщения: AppHdr +Sgntr.

Согласно стандарту XML Advanced Electronic Signatures (XAdES) в элемент <Signature> должен добавляться дополнительный элемент <SigningTime> для передачи времени формирования ЭЦП. Данный элемент должен быть расположен в следующей иерархии.

Signature
+ Object
++ QualifyingProperties
+++ SignedProperties
++++ SignedSignatureProperties
+++++ SigningTime

Значение этого элемента должно быть представлено в виде строки со значением времени формирования ЭЦП в формате “ YYYY-MM-DDThh:mm:ss”.

Параграф 3. Проверка ЭЦП сообщений

23. Проверка подлинности ЭЦП сообщения осуществляется следующим образом:

1) извлекается регистрационное свидетельство из структуры заголовка бизнес-сообщения:

AppHdr
+Sgntr
++Signature
++KeyInfo
+++X509Data
++++X509Certificate

2) извлеченное регистрационное свидетельство проверяется на то, что действительно выпущено АО «Национальная платежная корпорация Национального Банка Республики Казахстан»;

3) проверяется вся цепочка сертификатов до корневого;

4) проверяется срок действия ключа;

5) проверяется валидность ключа (не отозван);

6) проверяются политики использования ключа (для ЭЦП должны присутствовать политики Digital Signature, Non-Repudiation);

7) проверяются политики сертификатов OID. При отсутствии необходимой политики выдается ошибка и сообщение не направляется в целевую систему;

8) проверяется subject, он должен соответствовать имени терминала отправителя, в противном случае выдается ошибка;

9) проверяется действительность электронной подписи и время подписания сообщения ЭЦП;

10) проверяется целостность бизнес-сообщения.

Глава 9. Сжатие, шифрование, расшифровка и восстановление сообщений

Параграф 1. Сжатие и шифрование сообщения

24. Сжатие бизнес-сообщения осуществляется посредством технологии GZIP, которая основана на алгоритме сжатия без потерь Deflate, использующем комбинацию алгоритмов LZ77 и Хаффмана. Бизнес-сообщение сжимается и результат передается на шифрование.

25. Шифрование сжатого бизнес-сообщения проводится с использованием библиотек предоставляемого программным средством криптографической защиты информации «ТУМАР-CSP».

26. Для шифрования используются регистрационные свидетельства получателя сообщения, извлеченных из LDAP. Поиск производится путем поиска в LDAP субъекта по DN - фактически полное имя записи. DN строится из иерархической структуры: «C» (Country Name), «O» (Organization Name), «CN» (Common Name), например, C=KZ, O=AO «Национальная платежная корпорация Национального Банка Республики Казахстан», CN= VTEST.KISC0005. Где CN – имя получателя, полученного в заголовке технического сообщения.

Из полученного массива данных в LDAP извлекается массив данных по ключу «userCertificate» - пул регистрационных свидетельств. Из полученного пула регистрационных свидетельств строится массив из ключей «Шифрование ключей, Шифрование данных (30)». Данный массив регистрационных свидетельств используется для шифрования Бизнес-сообщения.

27. Полученный результат преобразуется в Base64 и помещается в значение элемента <CipherValue> транспортного сообщения. «CN» из сертификата получателя сообщения записывается в значение элемента <KeyName>. Сжатое и зашифрованное бизнес-сообщение (encrypted-data) располагается в элементе <CipherValue>:

```
<EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Type="http://www.w3.org/2001/04/xmlenc#Element">
   <EncryptionMethod
Algorithm="http://www.w3.org/2001/04/xmlenc#gost34310gost34311" />
 <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>

<ds:KeyName>VTEST.KISC0005</ds:KeyName>
 </ds:KeyInfo>
   <CipherData>
    <CipherValue>
     <!-- encrypted-data -->
    </CipherValue>
   </CipherData>
</EncryptedData>
```

Параграф 2. Расшифровка и восстановление сообщения

28. Шифрованное и сжатое бизнес-сообщение из элемента «CipherValue» преобразуется из формата Base64. Расшифровка полученных данных проводится с использованием библиотек предоставляемого программным средством криптографической защиты информации «ТУМАР-CSP».

29. Полученные на этапе расшифровки массив восстанавливается методом декомпрессии, используя технологию GZIP.

30.Восстановленное сообщение является бизнес-сообщением с утвержденной структурой, представляет собой совокупность бизнес-заголовка и содержимого сообщения.

Глава 10. Подписание ЭЦП транспортного сообщения

31. Подписание транспортного сообщения осуществляется посредством XML-подписи (XML-Signature) по стандарту XML-Signature Syntax and Processing (XMLDSIG). Порядок постановки ЭЦП аналогичный описанному процессу в Параграфе 2 Главы 8 Порядка.

Подписывается элемент <EncryptedData> со всем его содержимым. Полученный в результате постановки ЭЦП элемент <Signature> вместе с элементом <EncryptedData> упаковывается в элемент транспортного конверта <Body> для отправки в транспортную среду.

Глава 11. Параметры маршрута транспортного сообщения

32. Идентификаторы отправителя и получателя, записываемые в заголовок HTTP/MQ-протокола, приведены в Таблице № 2.

Таблица 2. Идентификаторы отправителя, системы отправителя, получателя и система доставки сообщений

Идентификатор	**Описание**	Обязательное
SENDER	Идентификатор (терминал) отправителя	Да
RECIPIENT	Идентификатор (терминал) получателя	Да
BIZMSGID	Идентификатор сообщения	Да
RELATEDBIZMSGID	Идентификатор предыдущего сообщения	Да

Приложение 1
к Структуре и порядку формирования транспортных сообщений
в платежных системах Казахстана

Примеры сообщений

1) Пример бизнес-сообщения, без подписи документа, до сжатия и шифрования:

```
<Envelope>
  <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
    <Fr>
...
    </Fr>
<To>
...
    </To>
    <BizMsgIdr>BMID_0000000001</BizMsgIdr>
    <MsgDefIdr>pacs.008.001.08</MsgDefIdr>
    <CreDt>2021-06-01T10:30:00+06:00</CreDt>
    <Prty>NORM</Prty>
  </AppHdr>
  <Document xmlns="urn:iso:std:iso:20022:tech:xsd:pacs.008.001.08">
    <FIToFICstmrCdtTrf>
      <GrpHdr>
        <MsgId>MSGID_0000000001</MsgId>
            ...
      </GrpHdr>
        <CdtTrfTxInf>
...
      </CdtTrfTxInf>
    </FIToFICstmrCdtTrf>
  </Document>
</Envelope>
```

2) Пример бизнес-сообщения с электронной подписью, до сжатия и шифрования:

```
<Envelope>
  <AppHdr xmlns="urn:iso:std:iso:20022:tech:xsd:head.001.001.01">
    <Fr>
...
    </Fr>
<To>
...
    </To>
    <BizMsgIdr>BMID_0000000001</BizMsgIdr>
    <MsgDefIdr>pacs.008.001.08</MsgDefIdr>
    <CreDt>2021-06-01T10:30:00+06:00</CreDt>
    <Prty>NORM</Prty>
    <Sgntr>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
    <ds:SignedInfo>
    <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/TR/2001/RECxml-c14n-20010315"/>
    <ds:SignatureMethod
  Algorithm="http://www.w3.org/2001/04/xmldsigmore#gost34310-gost34311"/>
    <ds:Reference URI="">
    <ds:Transforms>
    <ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#envelopedsignature"/>
```

```
          <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
20010315#WithComments"/>
          </ds:Transforms>
          <ds:DigestMethod
Algorithm="http://www.w3.org/2001/04/xmldsigmore#gost34311"/>
          <ds:DigestValue>dacd7+…4WuBpdu8=</ds:DigestValue>
          </ds:Reference>
          </ds:SignedInfo>
          <ds:SignatureValue>9/yx…gHA==</ds:SignatureValue>
          <ds:KeyInfo>
          <ds:X509Data>
          <ds:X509Certificate>…4EgE=</ds:X509Certificate>
          </ds:X509Data>
          </ds:KeyInfo>
          <ds:Object>
            <QualifyingProperties>
              <SignedProperties Id="SignedProperties">
                <SignedSignatureProperties>
                  <SigningTime>2024-02-05T21:11:17</SigningTime>
                </SignedSignatureProperties>
              </SignedProperties>
            </QualifyingProperties>
          <ds:Object>
          </ds:Signature>
          </Sgntr>
        </AppHdr>
        <Document xmlns="urn:iso:std:iso:20022:tech:xsd:pacs.008.001.08">
          <FIToFICstmrCdtTrf>
            <GrpHdr>
              <MsgId>MSGID_0000000001</MsgId>
                  ...
            </GrpHdr>
              <CdtTrfTxInf>
     ...
              </CdtTrfTxInf>
          </FIToFICstmrCdtTrf>
        </Document>
      </Envelope>
```

3) Пример транспортного сообщения в зашифрованном виде с ЭЦП:

```
    <Body>
     <EncryptedData xmlns="http://www.w3.org/2001/04/xmlenc#"
     xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
     Type="http://www.w3.org/2001/04/xmlenc#Element">
         <EncryptionMethod
     Algorithm="http://www.w3.org/2001/04/xmlenc#gost34310-gost34311" />
      <ds:KeyInfo xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
            <ds:KeyName>VTEST.KISC0005</ds:KeyName>
      </ds:KeyInfo>
         <CipherData>
           <CipherValue>
             <!-- encrypted-data -->
           </CipherValue>
         </CipherData>
         <ds:Signature>
         </ds:Signature>
     </EncryptedData>
    </Body>
```