

**ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)**

**Унифицированные форматы
электронных банковских сообщений**

**ЗАЩИТА ЭЛЕКТРОННЫХ СООБЩЕНИЙ
(Пакетов ЭС)**

Версия 2017.4.0

Москва

2017

Содержание

1. ЗАЩИТА ЭЛЕКТРОННЫХ СООБЩЕНИЙ (ПАКЕТОВ ЭС).....	3
1.1 Область применения	3
1.2 Требования по защите электронных сообщений (пакета ЭС)	3
2. ЗАЩИТА ЭЛЕКТРОННЫХ СООБЩЕНИЙ (ПАКЕТОВ ЭС) НА ПРИКЛАДНОМ УРОВНЕ	5
2.1 Область применения	5
2.2 Требования по защите электронных сообщений (пакета ЭС) с помощью ЗК	6
2.3 Правила формирования и проверки ЗК	10
3. ЗАЩИТА ЭЛЕКТРОННЫХ СООБЩЕНИЙ (ПАКЕТОВ ЭС) С ПОМОЩЬЮ КА	11
3.1 Область применения	11
3.2 Требования по защите ЭС (пакета ЭС) с помощью КА	12
3.3 Правила формирования и проверки КА	16
3.4 Шифрование	17
3.5 Сжатие.....	17

1. Защита электронных сообщений (пакетов ЭС)

1.1 Область применения

В настоящем разделе приведено описание правил оформления, формирования и проверки КА и защитного кода для унифицированных форматов электронных банковских сообщений для обмена электронными сообщениями подразделений Банка России с кредитными организациями и другими клиентами Банка России, расположенными на территории Российской Федерации, при осуществлении безналичных расчетов в валюте Российской Федерации.

Процедура разрешения разногласий при обмене электронными сообщениями состоит в доказательстве неизменности отправленного сообщения при доставке до получателя, основанном на применении средств контроля целостности и подтверждения авторства сообщений, предоставленных отправляющей и получающей сторонами в установленном порядке. В связи с этим необходимым требованием при использовании УФЭБС является передача сообщения получателю в том виде, в котором оно было подписано отправителем. Для защиты электронного сообщения с учетом данного требования используется КА.

Дополнительно ЭС (пакет ЭС) может быть защищено на технологическом уровне, для чего в состав реквизитов ЭС (пакета ЭС) может быть включен защитный код. В связи с тем, что защита пакета ЭС, а также отдельных электронных сообщений в составе пакета защитным кодом является элементом технологической защиты, требование передачи ЭС (пакета ЭС) получателю в том виде, в котором оно было защищено ЗК отправителем, не является необходимым. Однако алгоритм вычисления защитного кода принимает на вход двоичные данные, следовательно, подписываемое ЭС (пакет ЭС) необходимо привести к единому виду, имеющему в любом случае на любой платформе одинаковое двоичное представление. Электронные сообщения представляют собой XML-документы, поэтому для того, чтобы привести подписываемое и проверяемое ЭС (пакет ЭС) к одному виду, необходимо использовать алгоритмы, предназначенные для обработки XML-документов. Для приведения XML-документа к единому виду, имеющему в любом случае на любой платформе одинаковое двоичное представление, консорциум W3C рекомендует использовать алгоритм канонизации. Дополнительное преобразование (нормализация), позволяющее удалить лишнюю информацию из XML-документа, позволяет формировать ЗК только по значащим данным, что дает возможность защиты информации без учета особенностей разметки.

1.2 Требования по защите электронных сообщений (пакета ЭС)

Необходимость защиты ЭС (пакетов ЭС) в расчетной системе Банка России с помощью КА определена нормативными документами Банка России.

Защита ЭС (пакета ЭС), создаваемого в подразделении Банка России, с помощью защитного кода (ЗК) также определена нормативными документами Банка России.

Примечание – В применении к документу «Временные требования по обеспечению безопасности технологий обработки электронных платежных документов в системе Центрального банка Российской Федерации» от 03.04.1997 № 60 в настоящем документе под защитным кодом (ЗК) понимается КА обработки.

В ТУ Банка России может быть организована работа по вариантам защиты ЭС (пакета ЭС) с помощью КА и ЗК (см.таблицу 1). Первый вариант может быть использован только для защиты ЭС, передаваемых из КО/ОК в подразделение Банка России. При всех вариантах защиты применение КА является обязательным для пакета ЭС и ЭС без оформления в пакет.

Количество КА и ЗК на ЭС (пакете ЭС), которые **передаются** при обмене с КО/ОК, зависит от варианта защиты (см.таблицу 1). При описании вариантов защиты ЭС (пакета ЭС) с помощью КА и ЗК использовались условные обозначения (см.таблицу 2).

Таблица 1 – Количество КА и ЗК на ЭС при обмене с КО/ОК в зависимости от варианта защиты

Вариант	ЭС	Подписываемые данные	Кол-во КА	Кол-во ЗК
1 ¹⁾	пакет ЭС	пакет ЭС	[1]	—
		каждое ЭС в составе пакета ЭС	—	—

Вариант	ЭС	Подписываемые данные	Кол-во КА	Кол-во ЗК
	ЭС ²⁾	ЭС	[1]	—
2	пакет ЭС	пакет ЭС	[1]	[1]
		каждое ЭС в составе пакета ЭС	—	—
	ЭС ²⁾	ЭС	[1]	[1]
3	пакет ЭС	пакет ЭС	[1]	—
		каждое ЭС в составе пакета ЭС	—	n×[1]
	ЭС ²⁾	ЭС	[1]	[1]
¹⁾ Вариант 1 допустим только для защиты ЭС, формируемых в КО/ОК и ДОФР ²⁾ ЭС без оформления в пакет				

Т а б л и ц а 2 – Условные обозначения, использованные при описании вариантов защиты ЭС (пакета ЭС) с помощью КА и ЗК

Обозначение	Описание
[1]	Обязателен один и только один экземпляр КА или ЗК.
—	КА или ЗК не применяется
n×[1]	Один ЗК на каждое ЭС в пакете (n – количество ЭС в составе пакета)

В качестве средства криптографической защиты информации используется **СКАД «Сигнатура»**.

2. Защита электронных сообщений (пакетов ЭС) на прикладном уровне

В состав реквизитов ЭС может быть включен защитный код. При этом защита пакета ЭС или отдельных электронных сообщений в составе пакета ЭС защитным кодом является элементом технологической защиты.

В данном разделе приводятся правила оформления ЗК в XML-документе, определены защищаемые ЗК части XML-документа.

2.1 Область применения






В настоящем разделе приведено описание правил оформления, формирования и проверки защитного кода, применяемого в рамках УФЭБС для обмена электронными сообщениями подразделений Банка России с кредитными организациями и другими клиентами Банка России, расположенными на территории Российской Федерации, при осуществлении безналичных расчетов в валюте Российской Федерации.

Электронные сообщения представляют собой XML-документы, причем требование передачи ЭС (пакета ЭС) получателю в том виде, в котором оно было защищено ЗК отправителем, не является необходимым. Однако алгоритм вычисления защитного кода принимает на вход двоичные данные, следовательно, подписываемое ЭС (пакет ЭС) необходимо привести к единому виду, имеющему в любом случае на любой платформе одинаковое двоичное представление. Для приведения XML-документа к единому виду, имеющему в любом случае на любой платформе одинаковое двоичное представление, консорциум W3C рекомендует использовать алгоритм **канонизации**. Алгоритм канонизации XML-документов [XML-c14n] приводит XML-документ к форме, позволяющей определить логическую эквивалентность данного XML-документа другому XML-документу в канонической форме. Чтобы определить, являются ли два XML-документа логически эквивалентными, необходимо канонизировать каждый XML-документ согласно правилам канонизации, определенным W3C, и сравнить их канонические формы, сопоставляя байт за байтом. Если обе канонические формы содержат одинаковую последовательность байт, значит, соответствующие XML-документы являются логически эквивалентными.

Правила канонизации позволяют получить двоичное представление XML-документа, не зависящее от парсера и операционной платформы, однако не учитывают специфики УФЭБС. Например, канонизация XML-документа не предполагает удаления узлов со вспомогательной информацией, в то время как при электронном обмене в системе безналичных расчетов узлы со вспомогательной информацией (команды обработки; комментарии) не используются, т.е. информация, содержащаяся в них, игнорируется. Таким образом, при обработке информации из XML-документа применяется лишь часть узлов, а все прочие просто игнорируются. Дополнительное преобразование (**нормализация**), позволяющее удалить лишнюю информацию из XML-документа, позволяет формировать ЗК только по значащим данным, что дает возможность защиты информации без учета особенностей разметки. Формирование ЗК только по значащим данным без учета особенностей разметки конкретного первоначального экземпляра XML-документа позволяет проверить подписанное ЭС (пакет ЭС) независимо от формата его хранения (исходный XML-документ или восстановленный из реляционных данных).

Схемы обработки ЗК представлены на рисунках ниже (см. рисунок 1, рисунок 2). При построении схем использовались условные обозначения (см. таблица 3).

Таблица 3 – Условные обозначения, используемые при построении схем обработки ЗК

Обозначение	Описание	Обозначение	Описание
	Процесс		Объект
	XML-документ, отвечающий требованиям [XML]		Движение между состояниями объекта
			Передача объекта процессу

2.2 Требования по защите электронных сообщений (пакета ЭС) с помощью ЗК

2.2.1 Пространства имен

Для данной версии настоящего документа используются пространства имен:

“urn:cbr-ru:dsig:v1.1” (префикс **dsig**).

П р и м е ч а н и е — префикс пространства имен не несет смысловой нагрузки и используется только для привязки имен элементов и атрибутов к названию пространства имен.

2.2.2 Структура и синтаксис защитного кода

Реквизит со значением ЗК может быть добавлен в состав реквизитов любого ЭС (пакета ЭС). Реквизит со значением ЗК представлен элементом из пространства имен “urn:cbr-ru:dsig:v1.1”, который может быть добавлен перед первым дочерним элементом ЭС (пакета ЭС). Описание реквизита со значением ЗК представлено в таблице ниже (см. т а б л и ц а 4). Номер реквизита «0» говорит о том, что реквизит должен предшествовать реквизиту с номером «1» из состава реквизитов ЭС.

Т а б л и ц а 4 – Реквизит ЭС со значением ЗК

Описание реквизита	Тип реквизита	Кратность
0.Значение ЗК (any namespace="urn:cbr-ru:dsig:v1.1")	Элемент, содержащий значение ЗК	[0..n]

П р и м е ч а н и е — данная нотация не описывает структуру реквизита со значением ЗК.

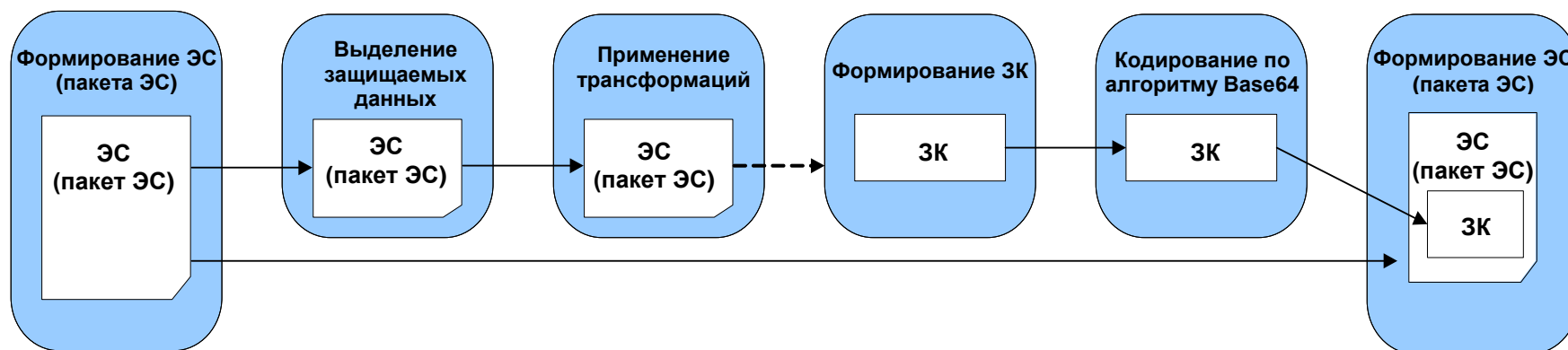


Рисунок 1 – Схема формирования ЗК

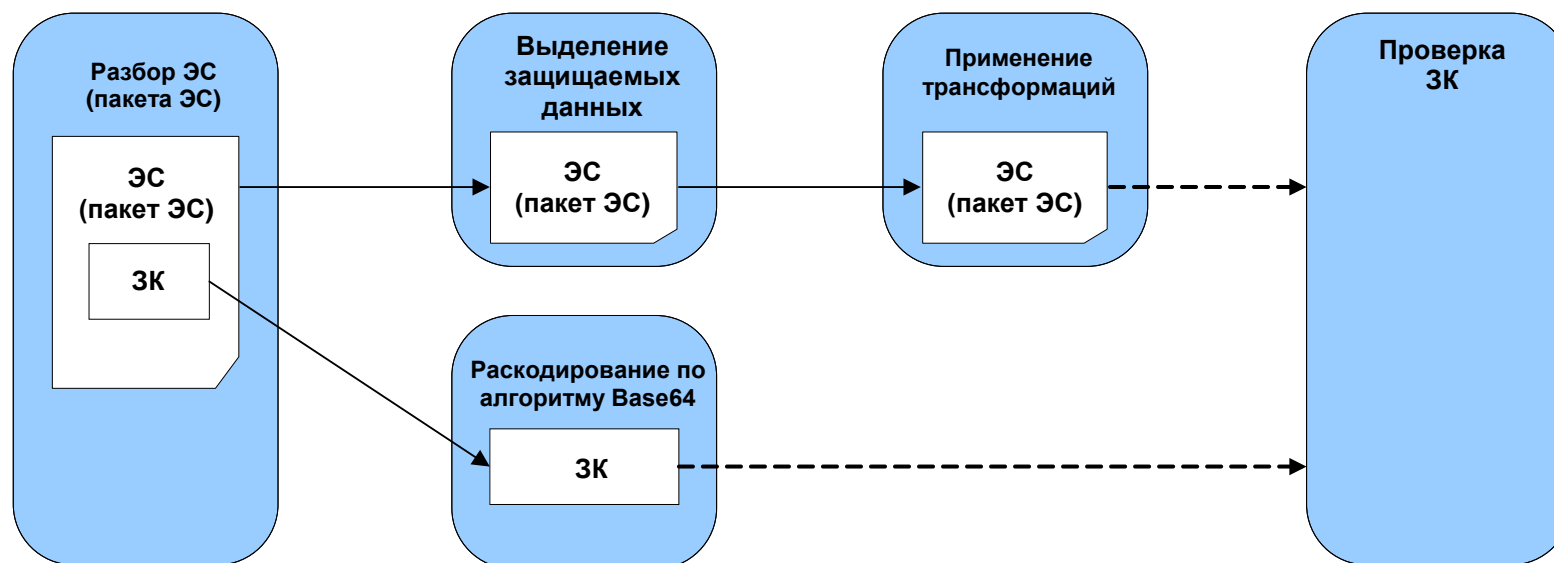


Рисунок 2 – Схема проверки ЗК

Структурно реквизит со значением ЗК представлен элементом **dsig:SigValue**, в который помещается значение ЗК, рассчитываемое по алгоритму, указанному в профиле параметров защиты ЭС (пакета ЭС) с помощью ЗК (см. таблица 6). Значение ЗК приводится в формате, с которым работает используемое СКЗИ. Перед помещением в элемент dsig:SigValue значение ЗК кодируется по алгоритму [base64]. Структура элемента со значением ЗК представлена в таблице ниже (см. таблица 5).

Пространства имен

“urn:cbr-ru:dsig:v1.1” (префикс dsig)

“http://www.w3.org/2001/XMLSchema” (префикс xsd)

Т а б л и ц а 5 – Реквизиты элемента со значением ЗК

Описание реквизита	Тип реквизита	Кратность
0.Значение ЗК (dsig:SigValue)	xsd:base64Binary	[0..n]

Пример – оформление значения ЗК:

```
<dsig:SigValue xmlns:dsig="urn:cbr-ru:dsig:v1.1">
RpxoZ6vnUXn9/nTSC9rkqeWtlNYTc+RxWZ5JbdFW6Vlg+ULhx7uDJFPRIIdqxXJnIugF2xzlpGjCtmh
4hz9tLAg==</dsig:SigValue>
```

2.2.3 Профиль параметров защиты ЭС (пакета ЭС) с помощью ЗК

В документе, описывающем обмен электронными сообщениями между сторонами при осуществлении расчетов через расчетную сеть Банка России (в договоре обмена) оговаривается порядок применения защиты ЭС (пакетов ЭС) с помощью ЗК. Защита ЭС (пакетов ЭС) с помощью ЗК применяется в соответствии с профилем параметров защиты ЭС (пакета ЭС) с помощью ЗК (см. таблица 6). Профиль защиты ЭС (пакета ЭС) с помощью ЗК содержит перечень спецификаций и алгоритмов, применяемых для приведения ЭС (пакета ЭС) к виду, обеспечивающему его защиту системой криптографической защиты информации путем простановки и проверки ЗК. Шаблон также определяет перечень и порядок трансформаций ЭС (пакета ЭС) перед операцией формирования и проверки ЗК.

Т а б л и ц а 6 – Профиль параметров защиты ЭС (пакета ЭС) с помощью ЗК

Алгоритм	Идентификатор
Трансформации ЭС (пакета ЭС)	
Преобразование ЭС (пакета ЭС) для приведения к нормализованному виду	urn:cbr-ru:dsig:v1.1#normalization
Канонизация XML без комментариев [XML-c14n]	https://www.w3.org/TR/xml-c14n
Кодирование ЭС (пакета ЭС)	
Алгоритм кодирования Base64	не используется
Кодирование значения ЗК	
Алгоритм кодирования Base64	http://www.ietf.org/rfc/rfc2045#base64

Криптографическая защита файлов с ЭС должна обеспечиваться на основе использования СКЗИ, имеющих сертификат или временное разрешение ФСБ, либо временное разрешение Банка России.

2.2.4 Ссылка на подписываемые данные

Место расположения элемента из пространства имен “urn:cbr-ru:dsig:v1.1” внутри ЭС (пакета ЭС) однозначно определяет ту часть ЭС (пакета ЭС) которая должна быть защищена: **ЗК** всегда **защищает родительский элемент** (включая все его дочерние элементы и атрибуты) по отношению к элементу со значением ЗК (за исключением всех **дочерних элементов** первого уровня по отношению к корню ЭС (пакета ЭС), **содержащих значения ЗК**):

– В ЭС, не оформленном в пакет, ЗК защищает весь ЭС, за исключением всех дочерних элементов первого уровня по отношению к корню ЭС, содержащих значения ЗК.

- В ЭС в составе пакета ЗК защищает весь ЭС, за исключением всех дочерних элементов первого уровня по отношению к корню ЭС, содержащих значения ЗК.
- В пакете ЭС ЗК защищает весь пакет ЭС, за исключением всех дочерних элементов первого уровня по отношению к корню пакета ЭС, содержащих значения ЗК.

Ниже (см.рисунок 3) представлена иллюстрация, показывающая подписываемые данные при формировании ЗК (для ЭС в составе пакета, а также пакета ЭС).

2.2.5 Преобразования для выделения данных, защищаемых ЗК

При **формировании** ЗК для выделения данных, защищаемых ЗК, выполняются следующие действия:

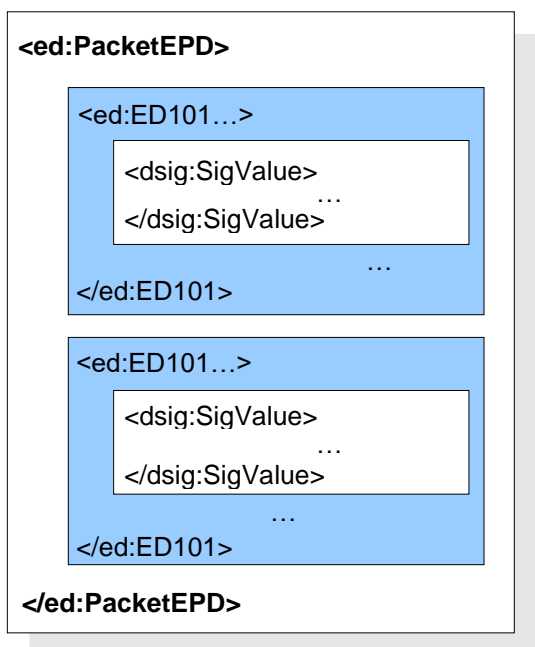
- Формируется XML-документ, корневым элементом которого является элемент, содержащий подписываемое ЭС (пакет ЭС) (со всеми его дочерними элементами и атрибутами).
- Из корневого элемента удаляются все элементы dsig:SigValue, являющиеся дочерними элементами первого уровня, если они есть.

Примечание – Элементы dsig:SigValue, являющиеся элементами первого уровня по отношению к корню подписываемой части ЭС (пакета ЭС), могут существовать в подписываемой части ЭС (пакета ЭС) в том случае, если подписываемая часть ЭС (пакета ЭС) уже защищена ЗК.

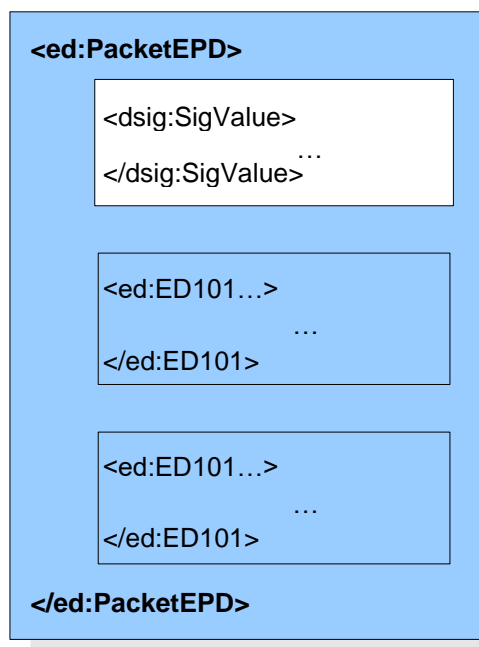
При **проверке** ЗК для выделения данных, защищаемых ЗК, выполняются следующие действия:

- Формируется XML-документ, корневым элементом которого является родительский элемент по отношению к элементу dsig:SigValue со значением проверяемого ЗК (со всеми его дочерними элементами и атрибутами).
- Из корневого элемента удаляются все элементы dsig:SigValue, являющиеся дочерними элементами первого уровня.

Защита ЭС ED101 в составе пакета ЭПС с помощью ЗК



Защита ЭС PacketEPD с помощью ЗК



Неподписываемые данные



Подписываемые данные

Рисунок 3 – Иллюстрация, показывающая подписываемые данные при формировании ЗК

2.3 Правила формирования и проверки ЗК

2.3.1 Правила формирования ЗК

Процесс формирования ЗК состоит из следующих этапов:

- a) формирование XML-документа, содержащего защищаемые данные ЭС (пакета ЭС), которые должны быть защищены с помощью ЗК.
- b) выделение из сформированного XML-документа данных, защищаемых ЗК в соответствии с 2.2.5.
- c) применение к XML-документу, содержащему только защищаемые данные, полученному на предыдущем этапе, трансформаций, приведенных в профиле параметров защиты ЭС (пакета ЭС) с помощью ЗК: преобразование XML-документа к нормализованному виду и канонизация. В результате канонизации будет получен массив байт.
- d) формирование (вычисление значения) ЗК: вызов функции СКЗИ по формированию ЗК с передачей ей массива байтов, полученных на предыдущем этапе.
- e) кодирование полученного на предыдущем этапе значения ЗК (в формате библиотеки ЗК, без выделения самого значения ЗК) по алгоритму [base64].
- f) помещение закодированного на предыдущем этапе значения ЗК в элемент dsig:SigValue.
- g) добавление элемента dsig:SigValue в XML-элемент, содержащий защищаемую часть ЭС (пакета ЭС), перед первым дочерним элементом первого уровня по отношению к корню защищаемой части ЭС (пакета ЭС).

2.3.2 Правила проверки ЗК

Процесс проверки ЗК на защищаемой части ЭС (пакета ЭС) состоит из следующих этапов:

- a) получение XML-элемента, содержащего защищаемую ЗК часть ЭС (пакета ЭС).
- b) выделение значения ЗК из элемента dsig:SigValue.
- c) раскодирование значения ЗК, выделенного на предыдущем этапе, по алгоритму [base64].
- d) выделение из XML-элемента, полученного на этапе, описанном в перечислении a), данных, защищаемых ЗК в соответствии с 2.2.5.
- e) применение к XML-документу, полученному на предыдущем этапе, трансформаций, приведенных в профиле параметров защиты ЭС (пакета ЭС) с помощью ЗК: преобразование XML-документа к нормализованному виду и канонизация. В результате канонизации будет получен массив байт.
- f) проверка ЗК: вызов функции СКЗИ по проверке ЗК с передачей ей массивов байтов, полученных на этапах, описанных в перечислениях e) и c).

3. Защита электронных сообщений (пакетов ЭС) с помощью КА

ЭС должны быть защищены с использованием КА. При этом необходимым требованием является передача сообщения получателю в том виде, в котором оно было подписано отправителем.

В данном разделе приводятся правила оформления КА в ЭС, определены подписываемые части XML-документа.

3.1 Область применения

В настоящем разделе приведено описание правил оформления, формирования и проверки КА, применяемого в рамках УФЭБС для обмена электронными сообщениями подразделений Банка России с кредитными организациями и другими клиентами Банка России, расположенными на территории Российской Федерации, при осуществлении безналичных расчетов в валюте Российской Федерации.

Обмен документами в формате XML приводит к возможности несанкционированного доступа к информации. Для предотвращения несанкционированного доступа к информации вводится поддержка шифрования данных на прикладном уровне. Для экономии затрат на передачу и хранение данных вводится поддержка сжатия данных на прикладном уровне.

Процедура разрешения разногласий при обмене электронными сообщениями состоит в доказательстве неизменности отправленного сообщения при доставке до получателя, основанном на применении средств контроля целостности и подтверждения авторства сообщений, представленных отправляющей и получающей сторонами в установленном порядке. В связи с этим необходимым требованием при использовании УФЭБС является передача сообщения получателю в том виде, в котором оно было подписано отправителем. То есть проверяемое ЭС (пакет ЭС) должно в точности (до байта) совпадать с подписанным ЭС (пакетом ЭС). Таким образом, подписанное ЭС (пакет ЭС) должно быть передано в конверте КА в своем двоичном представлении. Для передачи двоичных данных в XML-документе спецификация [XML-schema] рекомендует использовать алгоритм кодирования [base64].

Данные, преобразованные по алгоритму [deflate], можно однозначно восстановить из сжатой последовательности, а выбранный алгоритм шифрования, также, должен однозначно восстанавливать данные при дешифровании. Использование алгоритмов [base64] и [deflate] гарантирует идентичность двоичного представления подписанного и проверяемого ЭС (пакета ЭС).

Ниже (см.рисунок 4,рисунок 5) представлены схемы обработки КА. При построении схем использовались условные обозначения (см.таблицу 7).

Таблица 7 – Условные обозначения, используемые при построении схем обработки КА

Обозначение	Описание	Обозначение	Описание
	Обязательный процесс		Объект
	Оptionальный процесс		Движение между состояниями объекта
	XML-документ, отвечающий требованиям [XML]		Передача объекта процессу

3.2 Требования по защите ЭС (пакета ЭС) с помощью КА

3.2.1 Пространства имен

Для данной версии настоящего документа используются пространства имен:

"urn:cbr-ru:dsig:v1.1" (префикс **dsig**)

"urn:cbr-ru:dsig:env:v1.1" (префикс **sen**)

П р и м е ч а н и е – префикс пространства имен не несет смысловой нагрузки и используется только для привязки имен элементов и атрибутов к названию пространства имен.

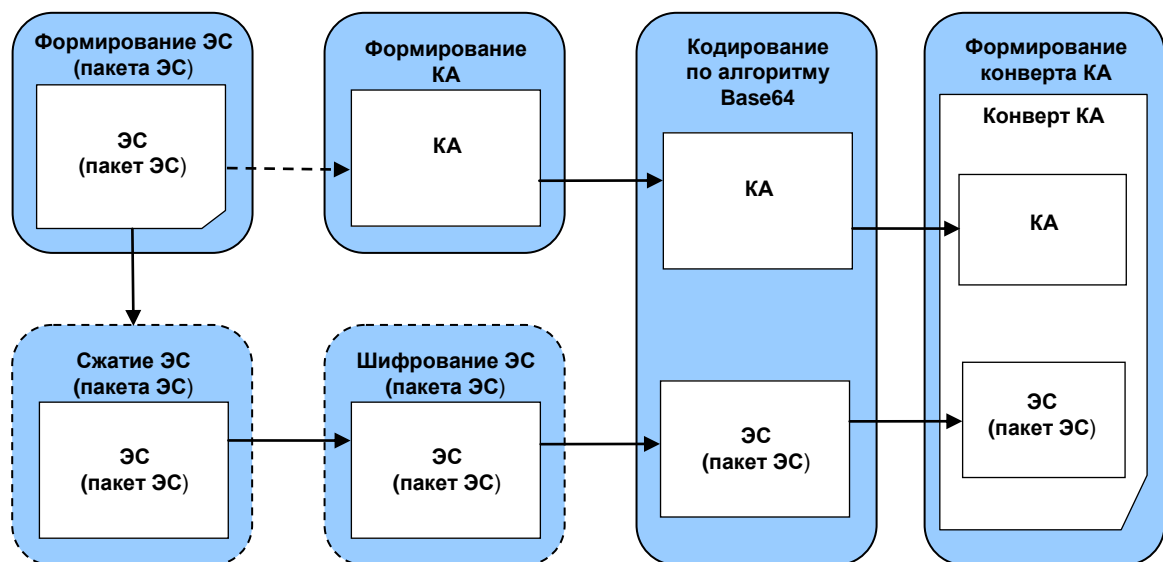


Рисунок 4 – Схема формирования КА

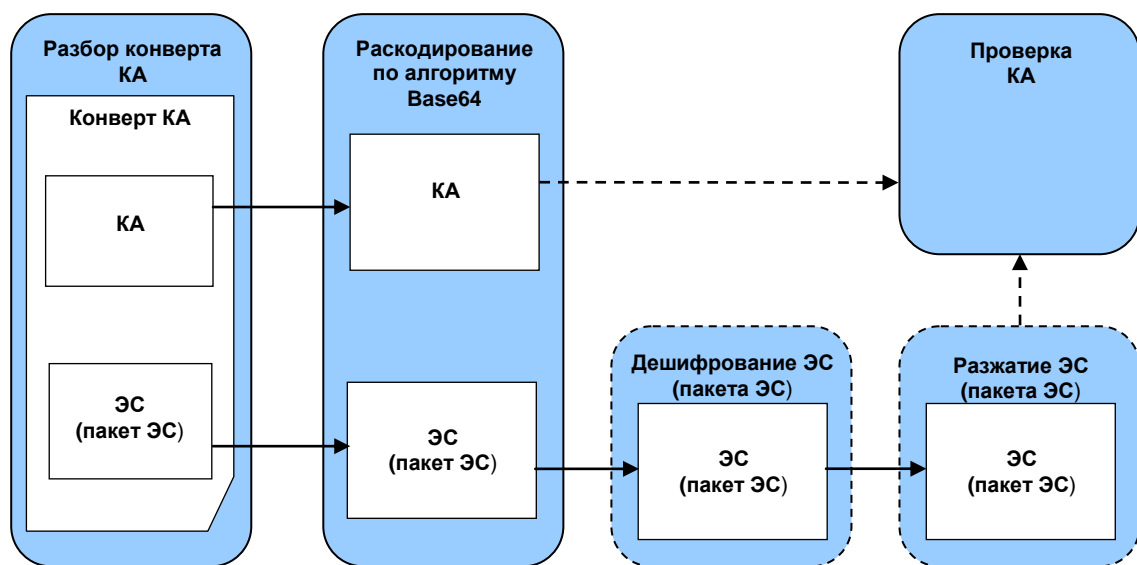


Рисунок 5 – Схема проверки КА

3.2.2 Структура и синтаксис конверта КА

Конверт КА содержит значения КА, а также подписанное ЭС (пакет ЭС). Конверт КА представлен в виде элемента **sen:SigEnvelope**.

Конверт КА состоит из:

- контейнера для значения КА, который представлен в виде элемента **sen:SigContainer**. Контейнер (элемент **sen:SigContainer**) содержит элемент из пространства имен "urn:cbr-ru:dsig:v1.1" со значением КА;
- элемента **sen:Object**, который содержит подписанное ЭС (пакет ЭС), закодированное по алгоритму [base64]. Перед кодированием по алгоритму [base64] ЭС (пакет ЭС) может быть сжато и/или зашифровано.

Описание реквизитов конверта КА (элемента **sen:SigEnvelope**) представлено в таблице ниже (см. т а б л и ц а 8).

Пространство имен
"urn:cbr-ru:dsig:env:v1.1" (префикс **sen**)

Т а б л и ц а 8 – Реквизиты конверта КА

Описание реквизита	Тип реквизита	Кратность
1 Контейнер для КА (sen:SigContainer)		[1]
1.1 Значение КА (any namespace="urn:cbr-ru:dsig:v1.1")	Элемент, содержащий значение КА	[1]
2 Контейнер для подписываемого объекта. (sen:Object)	Элемент, содержащий подписанное ЭС (пакет ЭС), закодированное по алгоритму [base64]	[1]

П р и м е ч а н и е – данная нотация не описывает структуру реквизита со значением КА.

Структурно реквизит со значением КА представлен элементом **dsig:MACValue**, в который помещается значение КА, рассчитываемое по алгоритму, указанному в профиле параметров защиты ЭС (пакета ЭС) с помощью КА (см. т а б л и ц а 10). Значение КА приводится в формате, с которым работает используемое СКЗИ, отдельно значение КА не выделяется. Перед помещением в элемент **dsig:MacValue** значение КА кодируется по алгоритму [base64]. Структура элемента со значением КА представлена в таблице ниже (см. т а б л и ц а 9).

Пространства имен
"urn:cbr-ru:dsig:v1.1" (префикс **dsig**)
"http://www.w3.org/2001/XMLSchema" (префикс **xsd**)

Т а б л и ц а 9 – Реквизиты элемента со значением КА

Описание реквизита	Тип реквизита	Кратность
1 Значение КА (dsig:MACValue)	xsd:base64Binary	[1]

Пример – оформление значения КА:

```
<dsig:MACValue xmlns:dsig="urn:cbr-ru:dsig:v1.1">  
RpxoZ6vnUXn9/nTSC9rkqeWt1NYTc+RxWZ5JbdFW6Vlg+ULhx7uDJFPRIIdqxXJnIugF2xzlpGjCtmh  
4hz9tLAg==</dsig:MACValue>
```

3.2.3 Профиль параметров защиты ЭС (пакета ЭС) с помощью КА

Защита ЭС (пакета ЭС) с помощью КА применяется в соответствии с профилем параметров защиты ЭС (пакета ЭС) с помощью КА (см. т а б л и ц а 10). Профиль защиты ЭС (пакета ЭС) с помощью КА содержит перечень спецификаций и алгоритмов, применяемых для приведения ЭС

(пакета ЭС) к виду, обеспечивающему его защиту системой криптографической защиты информации путем простановки и проверки КА.

Т а б л и ц а 10 – Профиль параметров защиты ЭС (пакета ЭС) с помощью КА

Алгоритм	Идентификатор
Трансформации ЭС (пакета ЭС)	
Преобразование ЭС (пакета ЭС) для приведения к нормализованному виду	не используется
Канонизация XML без комментариев [XML-c14n]	не используется
Кодирование ЭС (пакета ЭС)	
Алгоритм сжатия (необязательный)	http://www.ietf.org/rfc/rfc1951
Алгоритм шифрования (необязательный)	определяется Договором обмена
Алгоритм кодирования Base64	http://www.ietf.org/rfc/rfc2045#base64
Кодирование значения КА	
Алгоритм кодирования Base64	http://www.ietf.org/rfc/rfc2045#base64

Криптографическая защита файлов с ЭС должна обеспечиваться на основе использования СКЗИ, имеющих сертификат или временное разрешение ФСБ, либо временное разрешение Банка России.

3.2.4 Ссылка на подписываемые данные

КА всегда защищает содержимое элемента **sen:Object**. Содержимое элемента **sen:Object** представляет собой XML-документ, содержащий подписываемое ЭС (пакет ЭС), закодированное по алгоритму [base64]. XML-документ, содержащий подписываемое ЭС (пакет ЭС), должен быть сформирован с учетом требований, предъявляемых к оформлению XML-документов (см. главу 7 документа [УФЭБС 2019 1 0 Справочники.doc#XML](#)).

Ниже (см. рисунок 6) представлена иллюстрация, показывающая подписываемые данные при формировании КА.

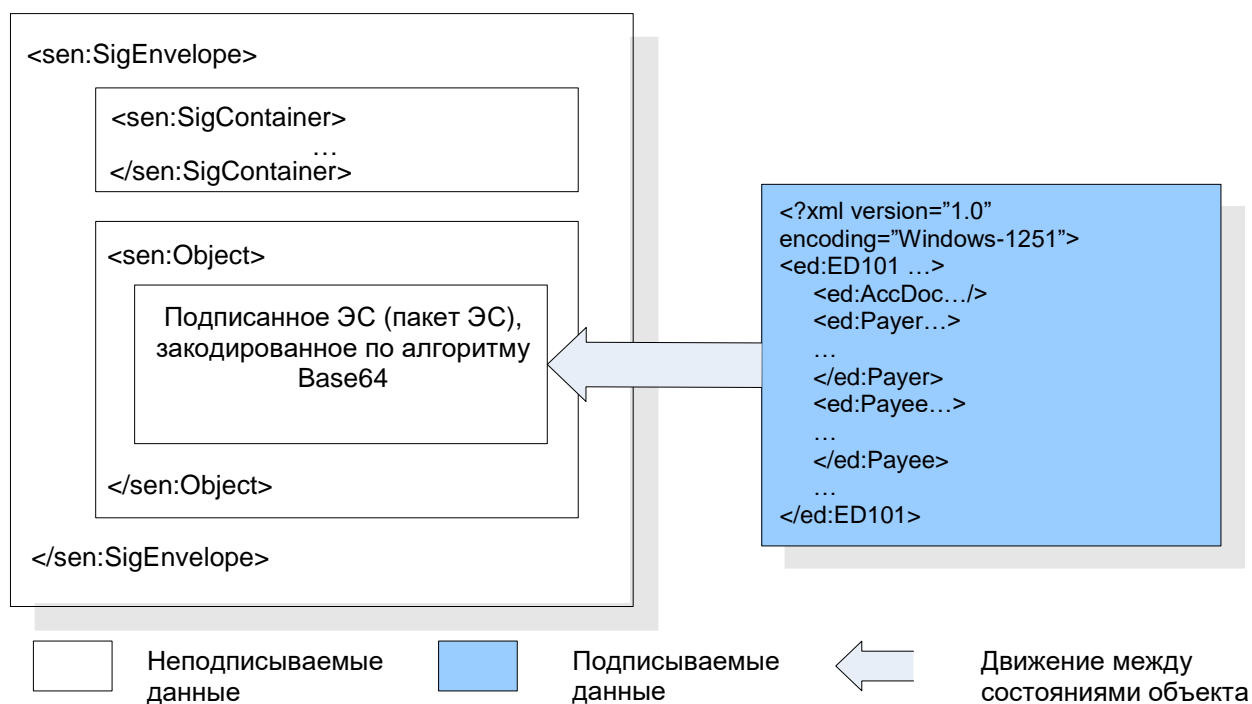


Рисунок 6 – Иллюстрация оформления КА, показывающая подписываемые данные

Подписываемое ЭС (пакет ЭС) может содержать ЗК в качестве реквизитов. В этом случае КА все равно защищает весь XML-документ, содержащий ЭС (пакет ЭС) вместе со всеми

реквизитами (в том числе и со всеми ЗК). Ниже (см. рисунок 7) представлена иллюстрация, показывающая подписываемые данные при формировании КА.

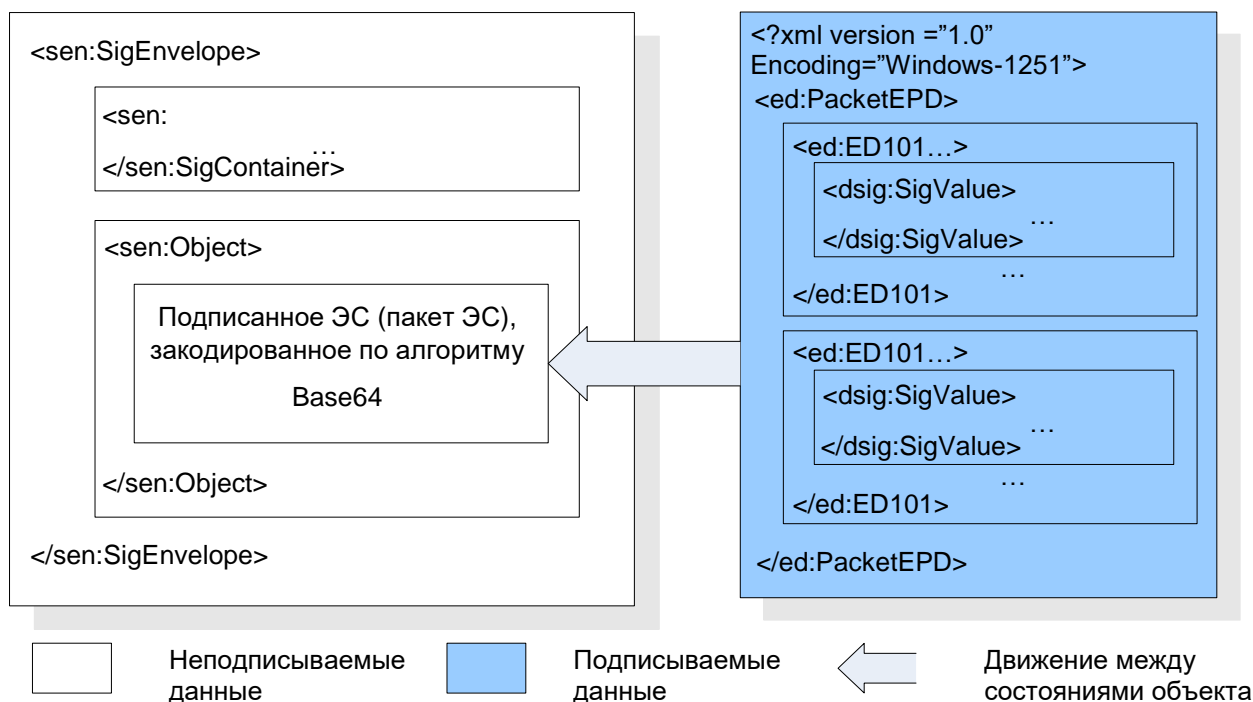


Рисунок 7 – Иллюстрация оформления КА для пакета ЭС с защитой каждого ЭС собственным ЗК

3.3 Правила формирования и проверки КА

Настоящий раздел описывает порядок необходимых преобразований ЭС (пакета ЭС) для формирования и проверки значения КА.

Правила оформления значения КА и определения набора подписываемых данных внутри ЭС (пакета ЭС) приведено в описании форматов ЭС.

3.3.1 Правила формирования КА

Процесс формирования конверта КА состоит из следующих этапов:

а) формирование XML-документа, содержащего ЭС (пакет ЭС), которое должно быть защищено с помощью КА. XML-документ должен быть сформирован с учетом требований, предъявляемых к оформлению XML-документов в соответствии с подразделом 10.1 Альбома форматов;

б) сериализация (согласно [XML]) сформированного на предыдущем этапе XML-документа в массив байтов, для которого будет рассчитываться КА;

в) формирование (вычисление значения) КА: вызов функции СКЗИ по формированию КА с передачей ей массива байтов, полученного на предыдущем этапе;

г) сжатие массива данных, полученного на этапе в), если это предусмотрено Договором обмена;

д) шифрование массива данных, полученного на этапе в), с учетом возможного сжатия на этапе г), если это предусмотрено Договором обмена;

е) кодирование полученного на этапе в) значения КА (в формате библиотеки КА, без выделения самого значения КА по алгоритму [base64]);

ж) помещение закодированного на предыдущем этапе значения КА в элемент `dsig:MACValue`;

з) кодирование массива байтов, полученного на этапе в), с учетом возможного сжатия на этапе г) и/или возможного шифрования на этапе д) по алгоритму [base64];

- i) помещение закодированного на предыдущем этапе массива байтов в элемент `sen:Object`.
- j) оформление конверта КА в соответствии с пунктом 3.2.2.

3.3.2 Правила проверки КА

Процесс проверки КА на XML-документе состоит из следующих этапов:

- a) получение XML-документа, содержащего ЭС (пакет ЭС), защищенное КА;
- b) выделение значения КА из элемента `dsig:MACValue`;
- c) раскодирование значения КА, выделенного на предыдущем этапе, по алгоритму [base64];
- d) выделение ЭС (пакета ЭС), защищенного КА, из элемента `sen:Object`;
- e) раскодирование ЭС (пакета ЭС), выделенного на предыдущем этапе, по алгоритму [base64];
- f) дешифрование массива байтов, полученного на предыдущем этапе, если это предусмотрено Договором обмена;
- g) разжатие массива байтов, полученного на предыдущем этапе, если это предусмотрено Договором обмена;
- h) проверка КА: вызов функции СКЗИ по проверке КА с передачей ей массивов байтов, полученных на этапах c) и e), с учетом возможного дешифрования на этапе f) и/или возможного разжатия на этапе g).

3.4 Шифрование

Шифрование и дешифрование сообщений выполняется средствами СКЗИ, имеющими сертификат или временное разрешение ФСБ, либо временное разрешение Банка России. Обмен и доступ к информации, необходимой для шифрования и дешифрования определяется Договором обмена.

3.5 Сжатие

Сжатие и разжатие данных осуществляется с использованием алгоритма [deflate]. Использование сжатия данных определяется Договором обмена.

Сторона, принимающая сжатое сообщение, должна обеспечивать полную поддержку форматов [deflate] и [zlib].

3.5.1 Структура формата сжатых данных в составе элемента `sen:Object`

Формат сжатых данных представляет собой последовательность двух блоков, первый из которых состоит из четырех байт и содержит длину данных до сжатия, а второй блок в формате [zlib] содержит данные, сжатые по алгоритму [deflate] (см. т а б л и ц а 11).

Т а б л и ц а 11 – Структура формата сжатых данных

Название блока	Описание блока	Длина блока (байт)
Размер данных до сжатия	Четырехбайтовое беззнаковое целое (32 бита) в формате little-endian (первым - младший байт).	4
Сжатый блок данных	Блок данных в формате [zlib], сжатых в соответствии с алгоритмом [deflate].	9-n