ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание восьмое, 2021

Часть13. Видимые цифровые печати

Утверждено и опубликовано с санкции Генерального секретаря

Международная организация гражданской авиации

ИКАО

Doc 9303

Машиносчитываемые проездные документы

Издание восьмое, 2021

Часть 13. Видимые цифровые печати

Утверждено и опубликовано с санкции Генерального секретаря

Международная организация гражданской авиации

Опубликовано отдельными изданиями на русском, английском,
арабском, испанском, китайском и французском языках
МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИЕЙ ГРАЖДАНСКОЙ АВИАЦИИ.
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Загрузить и получить дополнительную информацию можно на сайте
www.icao.int/security/mrtd.

Doc 9303. ***Машиносчитываемые проездные документы***
Часть 13. ***Видимые цифровые печати***
ISBN 978-92-9265-273-9

ПОПРАВКИ

Об издании поправок сообщается в дополнениях к *Каталогу продукции и услуг ИКАО;* Каталог и дополнения к нему имеются на веб-сайте ИКАО www.icao.int. Ниже приводится форма для регистрации поправок.

РЕГИСТРАЦИЯ ПОПРАВОК И ИСПРАВЛЕНИЙ

ПОПРАВКИ		
№.	Дата	Кем внесено

ИСПРАВЛЕНИЯ		
№.	Дата	Кем внесено

ОГЛАВЛЕНИЕ

1. СФЕРА ПРИМЕНЕНИЯ

В данной части 13 документа Doc 9303 указаны спецификации цифровой печати для обеспечения подлинности и целостности неэлектронных документов сравнительно недорогим, но весьма надежным способом с использованием асимметричной криптографии. Информация на неэлектронном документе криптографически подписывается, а подпись кодируется в виде двумерного штрих-кода и печатается на самом документе. Такой метод (*видимая цифровая печать)* дает следующие преимущества:

- *Асимметрия.* В связи с использованием асимметричной криптографии стоимость прикрепления цифровой печати значительно выше стоимости выдачи документа, защищенного цифровой печатью. Таким образом, даже при том, что стоимость выдачи документа очень низка, фальсификация или подделка данных персонализации документа является чрезвычайно дорогостоящей.

- *Персонализация.* Каждая цифровая печать верифицирует информацию, напечатанную на физическом документе, и, следовательно, связана с держателем документа. Прямого эквивалента пустого документа не существует, поэтому никакие бланки не могут быть потеряны или украдены.

- *Простота верификации.* Даже неподготовленные люди могут верифицировать документ, защищенный цифровой печатью, с помощью такого недорогого средства, как приложение на смартфоне. Более того, из-за двоичной природы цифровой подписи отличить подлинные документы от поддельных очень просто.

Хотя цифровая печать обеспечивает значительно более высокую защиту документов (обычно бумажных), не имеющих микрочипов, у нее имеются значительные ограничения по сравнению с документами, основанными на чипах. Емкость памяти цифровых печатей обычно составляет максимум несколько Кбайтов и на существующих документах невозможно обновить ни данные, ни криптографические ключи или схемы для цифровой печати. То есть криптографическая гибкость в них не поддерживается. Цифровая печать не обеспечивает никакой защиты от клонирования, не реализует функции защиты конфиденциальности и вследствие износа более подвержена ошибкам считывания, чем документы, основанные на чипах. Кроме того, универсальность криптографических чипов позволяет реализовать такие дополнительные свойства, как схемы подписи, аутентификация терминалов, методы двухфакторной аутентификации на основе общих секретных ключей, то есть PIN-коды или безопасные криптографические протоколы, основанные на симметричных схемах. Поскольку двумерные штрих-коды не могут заменить функциональные или защитные характеристики микрочипов, в проездных документах по мере возможности должны использоваться микрочипы.

2. КОДИРОВАНИЕ ЦИФРОВОЙ ПЕЧАТИ

.

Видимая цифровая печать — это криптографически подписанная структура данных, содержащая элементы документа, закодированная в виде двумерного штрих-кода и напечатанная на документе. В этом разделе приводится описание кодирования и структуры видимой цифровой печати.

2.1 Требования к формату штрих-кода и печатанию

Эта спецификация определяет, как данные кодируются в поток байтов. ДОЛЖНЫ использоваться только двумерные штрих-коды, система обозначения которых указана в стандарте ИСО. Стандартизированные ИСО двумерные штрих-коды включают, например, коды DataMatrix [ISO/IEC 16022], Aztec [ISO/IEC 24778] и QR-коды [ISO/IEC 18004].

Штрих-код СЛЕДУЕТ печатать таким образом, чтобы считывающие устройства (например, имеющиеся в свободной продаже смартфоны или сканеры) могли надежно декодировать штрих-код; в частности, при оценке качества печати СЛЕДУЕТ учитывать стандарт [ISO/IEC 15415]. Результирующие требования к качеству печатания и сканирования зависят от документа; конкретные детали сценария применения МОГУТ быть указаны в профиле. В связи с тем, что качество печатания и сканирования сказывается на частоте ошибок и влияет на надежность верификации цифровой печати, эти требования к качеству ДОЛЖНЫ обеспечивать надежную верификацию штрих-кода, содержащего цифровую печать и все обязательные элементы документа. Еще одно важное требование касается контраста символов штрих-кода, поскольку цифровая печать может быть напечатана на защитной бумаге с цветным фоном (например, зеленым).

При использовании стандартных струйных принтеров печатать РЕКОМЕНДУЕТСЯ с размером модуля (размер одного блока двумерного штрих-кода) по крайней мере 0.3386 мм (длина стороны модуля), что соответствует 4 точкам на длину стороны модуля (т.е. 16 точкам на модуль) на принтере с разрешением 300 dpi или 8 точкам на длину стороны модуля (т.е. 64 точкам на модуль) на принтере с разрешением 600 dpi. Если используются принтеры с высоким разрешением или лазерные принтеры, МОГУТ быть приемлемы меньшие размеры печати. О размещении штрих-кода на документе говорится в соответствующих частях документа Doc 9303.

Закодированный штрих-код состоит из заголовка (см. раздел 2.2), зоны сообщений (см. раздел 2.3) и зоны подписи (см. раздел 2.4). На рис. 1 приводится общая схема структуры.

Рис. 1. Структура цифровой печати

2.2 Заголовок

Заголовок содержит метаданные о документе и кодировании, такие как номер версии, а также даты выдачи документа и создания подписи.

Эта спецификация определяет две версии заголовка, обозначаемые идентификаторами версий "3" и "4" соответственно. Данные версии различаются по определению ссылки на сертификат (см. ниже) и кодированию длины элементов документа (см. раздел 2.3).

Общая длина заголовка составляет 18 байт для версии 3 и переменную для версии 4. Определение заголовка приводится в таблице 1.

Таблица 1. Формат заголовка

Начальная позиция	***Длина (байт)***	***Содержание***
0x00	1	*Магическая константа.* Магическая константа имеет фиксированное значение 0xDC, идентифицирующее штрих-код, соответствующий этой спецификации
0x01	1	*Версия*. Байтовое значение, идентифицирующее версию этой спецификации. Версии, определенные в данной спецификации, идентифицируются байтовым значением 0x02/0x03 соответственно. Число n означает версию n+1, например, значение 0 означает версию 1
0x02	2	*Страна выдачи.* Трехбуквенный код, идентифицирующий государство или организацию выдачи. Трехбуквенный код соответствует документу Doc 9303-3. Если трехбуквенный код содержит менее трех букв, то код ДОЛЖЕН быть дополнен символами-заполнителями (<), например буква D дополняется до D<<. Код кодируется по схеме C40 (см. раздел 2.6) в виде двухбайтовой последовательности
0x04	6 / v	*Идентификатор подписывающего лица и ссылка на сертификат*. Версия 3: девятибуквенный код, идентифицирующий (штрих-код) подписывающее лицо и сертификат. Версия 4: буквенный код переменной длины, идентифицирующий (штрих-код) подписывающее лицо и сертификат ("v" обозначает общую длину этого поля). Код кодируется по схеме C40 (см. раздел 2.6). Для кодирования с переменной длиной см. раздел 2.2.1
0x0A / 0x04+v	3	*Дата выдачи документа.* Дата, когда был выдан документ. Кодируется как указано в разделе 2.3.1
0x0D / 0x07+v	3	*Дата создания подписи*. Дата, когда была создана подпись. Кодируется как указано в разделе 2.3.1
0x10 / 0x0A+v	1	*Ссылка на определение элементов документа*. Код ссылки на документ, который определяет количество и кодирование элементов документа. Это определение является независимым для каждой категории документов, то есть один и тот же код ссылки на определение элементов документа может иметь разные значения для разных категорий типов документов. Значения ДОЛЖНЫ находиться в диапазоне от 01dec до 254dec
0x11 / 0x0B+v	1	*Категория типа документа*. Категория документа, например виза, экстренно выдаваемый проездной документ, свидетельство о рождении.

		Нечетные числа в диапазоне от 01dec до 253dec используются для категорий типов документов, определенных ИКАО
Сумма	18 / 12 + v	

2.2.1 Идентификатор подписывающего лица и ссылка на сертификат

Из-за ограничений по размеру хранить сертификаты, содержащие открытый ключ, соответствующий подписи, в пределах штрих-кода невозможно. Поэтому сертификат ДОЛЖЕН быть приобретен по другому каналу. Чтобы однозначно идентифицировать сертификат и подписывающее лицо, являющееся субъектом сертификата, и связать сертификат со штрих-кодом, в заголовке хранится строка, содержащая идентификатор подписывающего лица и ссылку на сертификат. Эта строка включает:

a) *Идентификатор подписывающего лица*. Сочетание двухбуквенного кода страны (согласно документу Doc 9303-3) подписывающего лица и двух буквенно-цифровых символов для идентификации подписывающего лица в вышеуказанной стране. Идентификатор подписывающего лица ДОЛЖЕН быть уникальным для подписывающего лица в данной стране.

b) *Ссылку на сертификат*:

1) Для заголовка версии 3: шестнадцатеричная строка ровно из пяти символов, которая должна однозначно идентифицировать сертификат данного подписывающего лица.

2) Для заголовка версии 4: шестнадцатеричная строка, содержащая конкатенацию:

i) ровно двух символов, обозначающих количество последующих символов,

ii) символов, которые ДОЛЖНЫ однозначно идентифицировать сертификат данного подписывающего лица.

Обратите внимание, что для конкретного случая использования виз (см. документ Doc 9303-7) подписывающим лицом является *лицо, подписывающее визы*.

Ссылка на сертификат `0 ... 0` зарезервирован для целей тестирования и НЕ ДОЛЖЕН использоваться в производстве.

Идентификатор подписывающего лица и ссылка на сертификат (штрих-код) ДОЛЖНЫ соответствовать отличительному имени субъекта (DN) и серийному номеру сертификата подписывающего лица. Таким образом, после декодирования заголовка сертификат подписывающего лица может быть однозначно идентифицирован.

2.2.2 Ссылка на определение элементов документа и категория типа документа

Сочетание *ссылки на определение элементов документа* и *категории типа документа* определяет конкретный набор правил, таких как эта спецификация. Таким образом, в будущих случаях использования может повторно использоваться один и тот же штрих-код и формат заголовка, но делаться ссылка на различные определения элементов (т. е. ссылка, определяющая список информации, включенной в штрих-код) или категории типов документов. Это позволяет повторно использовать существующие кодовые базы, упрощает реализацию и повышает интероперабельность.

Ссылки на определение элементов документа и категории типов документов для виз и экстренно выдаваемых проездных документов определяются в документах Doc 9303-7 и Doc 9303-8 соответственно.

2.3 Зона сообщений

После заголовка следует зона сообщений. Зона сообщений состоит из закодированных в цифровой форме элементов документа, указанных в этом разделе. Любой порядок элементов документа действителен при условии, что присутствуют все его обязательные элементы.

Каждому элементу документа предшествует:

- тег, идентифицирующий тип элемента (один байт);
- длина элемента (от одного байта до пяти байт).

В зависимости от идентификатора версии (в начальной позиции `0x01` в заголовке, см. таблицу 1) необходимо различать два типа кодирования длины:

- Для версии №3 и ниже длина ДОЛЖНА быть непосредственно закодирована в 1 байт (этот "байт длины" является 2-м байтом непосредственно после "тега" сообщения).
- Для версии №4 и выше длина ДОЛЖНА быть закодирована с использованием схемы DER-TLV в соответствии с [X. 690].

Для визовых документов РЕКОМЕНДУЕТСЯ использовать версию №4 (или выше) и, следовательно, кодирование длины по схеме DER-TLV. Использование версии №3 (или ниже) и, следовательно, прямое кодирование длины допустимо, но не рекомендуется.

Для экстренно выдаваемых проездных документов (ETD) ДОЛЖНЫ использоваться версия №4 (или выше) и, следовательно, кодирование длины по схеме DER-TLV.

2.3.1 Цифровое кодирование элементов документа (двоичное кодирование)

Элементы документа кодируются нижеуказанным способом. В качестве строительных блоков мы рассматриваем следующие основные типы:

a) *Alphanum*: строки прописных[1] буквенно-цифровых символов (например, A-Z, 0-9 и пробел);

b) *Binary*: последовательность байтов;

c) *Int*: положительные целые числа;

d) *Date*: даты.

Эти основные типы преобразуются в последовательность байтов следующим образом:

a) Строки буквенно-цифровых символов кодируются как байты по схеме C40 (см. раздел 2.6).

1. Ограничение на прописные буквы связано с ограниченным объемом данных штрих-кода.

b) Последовательность байтов берется такой, какая она есть.

c) Для положительных целых чисел берется их целочисленное представление без знака.

d) Дата сначала преобразуется в положительное целое число путем объединения месяца, дня и (четыре цифры) года. Это положительное целое число затем объединяется в последовательность из трех байтов, как указано в подпункте c) выше.

Пример: рассмотрим дату 25 марта 1957 года. Объединение месяца, дня и года дает целое число `03251957`, в результате чего получается три байта `0x31 0x9E 0xF5`.

Элемент цифрового документа — это последовательность байтов. Он имеет следующую структуру:

тег | длина | значение.

Тег здесь – это целое число в диапазоне `0-254dec`, выступающее в качестве уникального идентификатора элемента документа. Обратите внимание, что тег `255dec` зарезервирован для обозначения начала подписи. *Длина* состоит из одного-пяти байтов в соответствии с кодированием полей длины по схеме DER-TLV. *Длина* обозначает длину следующего значения. *Значение* – это базовый тип, преобразованный в последовательность байтов.

Пример: рассмотрим элемент документа, кодирующий строку "VISA01" с присвоенным тегом 0x0A. Закодированная последовательность байтов по схеме C40 (см. раздел 2.6) длиной 4 составляет `0xDE515826`. Следовательно, элементом документа является последовательность байтов `0x0A04DE515826`.

Таким образом, конкретный случай использования должен дополнить это определение перечислением того, какие элементы документа должны присутствовать, а какие могут присутствовать факультативно, а также определить их значения тегов и допустимые диапазоны длины.

Дополнительные элементы, т.е. элементы с неизвестными тегами, МОГУТ присутствовать, например, для факультативного использования органом выдачи. Такие дополнительные элементы НЕ ДОЛЖНЫ использовать тег поля дополнительного элемента или тег любого другого факультативного или обязательного элемента. Наличие элементов с неизвестными тегами не влияет на действительность штрих-кода, если подпись признана действительной.

2.4 Зона подписи

Начало зоны подписи обозначается маркером подписи, имеющим значение `0xFF`, закодированное как один байт, за которым следует от одного до пяти байтов, обозначающих длину подписи (количество байтов) с использованием схемы кодирования полей длины DER-TLV.

Ввод алгоритма подписи ДОЛЖЕТ быть (хэш) конкатенацией заголовка и полной зоны сообщений за исключением тега, обозначающего начало зоны подписи или длину подписи. Зона подписи содержит результирующую подпись.

ДОЛЖНЫ использоваться только алгоритмы хэширования и подписи, определенные в документе Doc 9303-12. В связи с результирующим размером подписи РЕКОМЕНДУЕТСЯ использовать алгоритм подписи эллиптической кривой (ECDSA) с длиной ключа не менее 256 бит в сочетании с алгоритмом SHA-256 (на момент создания данного документа).

В результате применения алгоритма подписи ECDSA получается пара положительных целых чисел (`r,s`). Эта подпись ДОЛЖНА храниться в необработанном формате на печати. Битовая длина `r` и `s`

соответствует длине ключа. Так, например, для ECDSA-256 длина `r` и `s` составляет не более 256 бит = 32 байта у каждого числа. Подпись ДОЛЖНА вводиться в память путем вычисления беззнакового целочисленного представления `r` и `s` с потенциальным добавлением ведущих нулей, чтобы `r` и `s` соответствовали их ожидаемой длине (т.е. длине ключа), и присоединением получаемого значения `s` к одному из `r`. Для преобразования между ASN.1 и необработанным форматом (`r,s`) см. добавление B.

2.5 Заполнение

Если заголовок, сообщение и подпись вместе не заполняют имеющееся пространство штрих-кода, то после подписи добавляются заполняющие символы. Все соответствующие символы двумерного штрих-кода определяют методы заполнения в своем соответствующем стандарте, и заполнение ДОЛЖНО следовать этому определению.

2.6 Кодирование строк по схеме C40

Для экономии пространства при кодировании буквенно-цифровых символов и символа-заполнителя < используется схема кодирования C40, как определено в [ISO/IEC 16022]. Ниже указано, как эти определения используются в текущей настройке. Следующие два определения применимы к элементам документа и их цифровому кодированию:

a) Строки состоят только из прописных букв, цифр, <SPACE> (<ПРОБЕЛА>) и символа '<'. Последний используется в качестве символа-заполнителя для машиносчитываемой зоны (МСЗ) проездных документов. Если в строке встречается '<', то перед кодированием все вхождения '< ' заменяются на < SPACE >. Строка НЕ ДОЛЖНА содержать никаких других символов.

b) При заданной длине строки L длина (т.е. количество байтов) соответствующего цифрового кодирования является наименьшим четным числом, которое больше или равно L.

В следующих вычислениях значение байта и соответствующий эквивалент целого числа без знака косвенно преобразуются. Например, мы определяем значение байта формулой, основанной на целочисленной арифметике целых значений.

2.6.1 Кодирование

Кодирование строки символов в последовательность байтов работает следующим образом: сначала строка группируется в кортежи из трех символов и каждый символ заменяется соответствующим значением C40 согласно таблице 2, в результате чего получается тройка (`U1,U2,U3`). Затем для каждой тройки вычисляется значение

```
U = (1600 * U1) + (40 * U2) + U3 + 1.
```

Результат находится в диапазоне от 1 до 64 000, что дает беззнаковое 16-битное целое значение. Это 16-битное значение `I16` упаковывается в два байта

```
Byte 1 = (I16) div 256

Byte 2 = (I16) mod 256.
```

Здесь `div` обозначает целочисленное деление (без остатка), а `mod` обозначает операцию по модулю. Обратите внимание, что эти операции могут быть реализованы с помощью битового сдвига.

Таблица 2. Схема кодирования C40 и соответствие ASCII

Значение C40	*Символ*	*Значение ASCII*	*Значение C40*	*Символ*	*Значение ASCII*
0	Shift 1	n/a	20	G	71
1	Shift 2	n/a	21	H	72
2	Shift 3	n/a	22	I	73
3	<SPACE>	32	23	J	74
4	0	48	24	K	75
5	1	49	25	L	76
6	2	50	26	M	77
7	3	51	27	N	78
8	4	52	28	O	79
9	5	53	29	P	80
10	6	54	30	Q	81
11	7	55	31	R	82
12	8	56	32	S	83
13	9	57	33	T	84
14	A	65	34	U	85
15	B	66	35	V	86
16	C	67	36	W	87
17	D	68	37	X	88
18	E	69	38	Y	89
19	F	70	39	Z	90

2.6.2 Декодирование

Кодирование можно легко инвертировать. С учетом пары байтов пусть `(I1,I2)` обозначают их целочисленные значения без знака. 16-битное значение `I16` пересчитывается как

```
V16 = (I1 * 256) + I2.
```

Тройка (U1,U2,U3) может быть пересчитана следующим образом:

```
U1 = (V16 – 1) div 1600

U2 = (V16 – (U1*1600) – 1) div 40

U3 = V16 – (U1*1600) – (U2*40) – 1.
```

Здесь снова div обозначает целочисленное деление. Символы можно декодировать из тройки (U1, U2, U3), просто найдя соответствующие значения в таблице 2.

2.6.3 Заполнение

Вышеуказанное определение четко сформулировано только в том случае, если длина кодируемой строки кратна трем. Подобно определениям заполнения, приведенным в [ISO/IEC 16022], применяются следующие правила заполнения:

a) Если два значения C40 (=два символа) остаются в конце строки, то эти два значения C40 доводятся до тройки со значением 0 (сдвиг 1). Тройка кодируется, как определено выше.

b) Если остается одно значение C40 (=один символ), то первый байт имеет значение 254dec (0xFE). Второй байт является значением схемы кодирования ASCII символа DataMatrix, соответствующего значению C40. Обратите внимание, что схема кодирования ASCII в DataMatrix для символа ASCII в диапазоне 0–127 – это символ ASCII плюс 1.

3. ИСПОЛЬЗОВАНИЕ ЦИФРОВОЙ ПЕЧАТИ

В этом разделе дается общее описание использования цифровой печати, которая применяется к визовым и экстренно выдаваемым проездным документам. Конкретные требования определяются в соответствующих профилях.

3.1 Содержание и правила кодирования

3.1.1 Заголовок

Кодирование заголовка для цифровых печатей выполняется в соответствии с разделом 2.2. Значение последних 2 байт для ссылки на определение элементов документа и категории типа документа зависит от конкретного профиля документа. Для профилей ИКАО категория типа документа должна быть нечетным числом. Четные числа МОГУТ использоваться для национальных профилей, не указанных ИКАО.

3.1.2 Элементы документа, закодированные в цифровой печати

Элементом документа, который ДОЛЖЕН храниться в печати, является машиночитаемая зона (МСЗ).

Цифровая печать кодирует МСЗ документа. МСЗ может быть любого из типов, указанных в документе Doc 9303. Однако, конкретные профили документов МОГУТ ограничивать виды допустимых типов МСЗ.

Каждый профиль документа МОЖЕТ определять дополнительные ОБЯЗАТЕЛЬНЫЕ и ФАКУЛЬТАТИВНЫЕ поля.

3.1.3 Правила кодирования элементов документа

Кодирование элементов документа зависит от ссылки на определение элементов документа в сочетании с категорией типа документа. Конкретные значения определяются в соответствующих профилях документа.

3.2 Лицо, подписывающее штрих-коды, и создание печати

Чтобы упростить верификацию цифровых печатей в данной спецификации используется существующая инфраструктура открытых ключей (PKI) национального центра удостоверения подписей (CSCA) в целях выдачи и распространения сертификатов, а также списков отозванных сертификатов (CRL). Подробности и профили сертификатов содержатся в документе Doc 9303-12.

3.2.1 Архитектура системы подписи штрих-кодов

Лицо, подписывающее штрих-коды, получает данные из системы персонализации документов для кодирования цифровой печати и использует ключ подписи для ее подписания. На рис. 2 изображена возможная реализация системы персонализации документов лицом, подписывающим штрих-коды, и его клиентом.

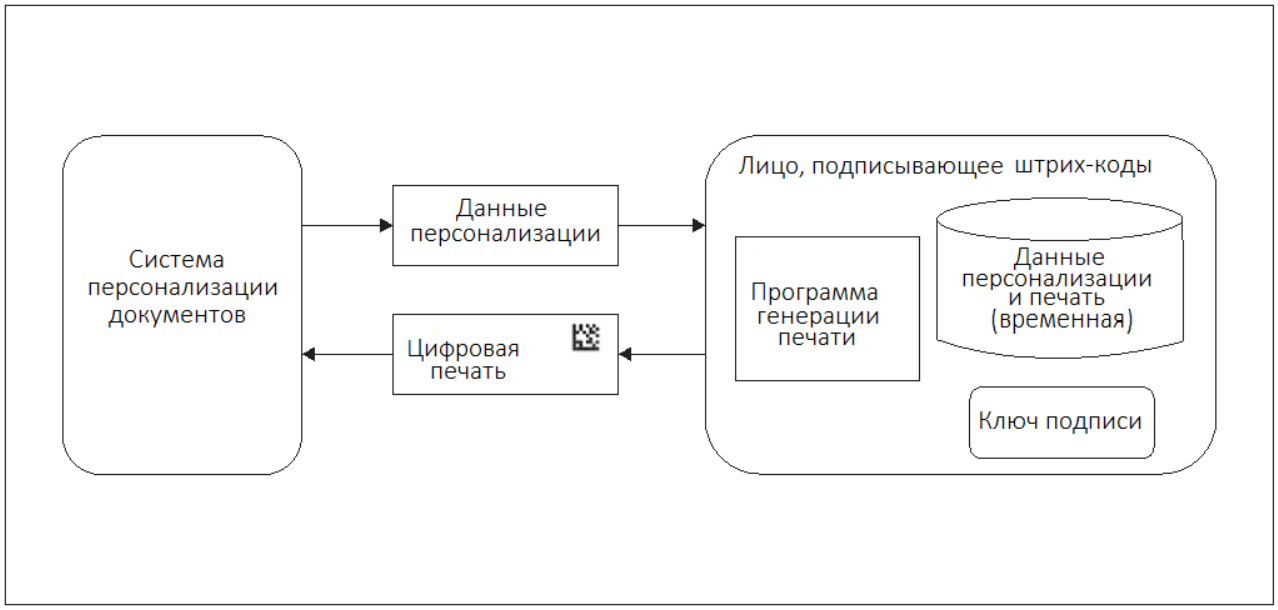

Рис. 2. Персонализация документов: сценарий с централизованным подписанием штрих-кодов

Лицо, подписывающее штрих-коды, полагается на следующее программное обеспечение и данные:

- *Программа генерации печати* производит цифровые печати, соответствующие действующему стандарту. Она получает данные персонализации, отправленные клиентом, подписывает эти данные закрытым ключом подписи и кодирует данные персонализации и подпись в виде штрих-кода. Данные персонализации и цифровая печать являются соответственно входными и выходными данными программы генерации печати. Эти данные должны временно храниться у лица, подписывающего штрих-коды, во время генерации печати.

- *Ключи подписи* (закрытый и открытый ключи) используются для подписания и верификации цифровой печати. Закрытый ключ подписи – это наиболее важные данные лица, подписывающего штрих-коды.

В зависимости от сценария развертывания разграничение между системой персонализации документов и лицом, подписывающим штрих-коды, не всегда является строгим. Например, подписывающее штрих-коды лицо может быть частью системы персонализации в посольстве. Одним из возможных сценариев является расширение системы персонализации путем включения генерации подписей и хранение ключей подписи на смарт-карте в посольстве. Другой подход заключается в создании центрального органа, подписывающего штрих-коды, в родной стране и подключении к нему посольств по защищенному каналу. Наконец, некоторые посольства могут сами не персонализировать документы; в таком случае система персонализации может быть также создана в родной стране и интегрирована с лицом, подписывающим штрих-коды.

Поскольку лицо, подписывающее штрих-коды, производит подпись, оно является исключительно важным компонентом. Подпись позволяет проверить целостность данных штрих-кода, т. е. были ли данные подвергнуты манипуляциям, а также их подлинность, т. е. выданы ли они уполномоченным органом.

Для достижения достаточно высокого уровня безопасности РЕКОМЕНДУЕТСЯ, чтобы подписывающий штрих-коды орган был центральной службой и не размещался в посольствах, если только оперативные, технические или логистические причины не препятствуют централизованному развертыванию. Это делается для того, чтобы сконцентрировать меры безопасности на ограниченном периметре, принимая во внимание наилучшие методы обеспечения восстанавливаемости и бесперебойного функционирования. Подписывающий штрих-коды орган ДОЛЖЕН обеспечивать надежное хранение закрытых ключей подписи.

3.2.2 Безопасность системы подписи штрих-кодов

Система подписи штрих-кодов должна размещаться и эксплуатироваться в соответствии с наилучшими методами обеспечения безопасности в следующих областях: физическая безопасность; серверная и сетевая инфраструктура; процессы разработки и поддержки систем; контроль доступа и безопасность операций. Если подписывающий штрих-коды орган создан как центральная служба, то РЕКОМЕНДУЕТСЯ обеспечить соответствие стандарту [ISO/IEC 27002] по периметру безопасности данного органа, чтобы обеспечить соответствие этим наилучшим методам обеспечения безопасности.

4. СПРАВОЧНЫЕ МАТЕРИАЛЫ (НОРМАТИВНЫЕ)

[ISO/IEC 16022] ИСО/МЭК 16022: "Информационные технологии. Технологии автоматической идентификации и сбора данных. Спецификация символики штрихового кода Data Matrix", 2006

[ISO/IEC 18004] ИСО/МЭК 18004:2006: "Информационные технологии (ИТ). Технологии автоматической идентификации и сбора данных. Спецификация символики штрихового кода QR Code", 2015

[ISO/IEC 24778] ИСО/МЭК 24778:2008: "Информационные технологии. Технологии автоматической идентификации и сбора данных. Спецификация символики штрихового кода Aztec Code", 2008

[ISO/IEC 27002] ИСО/МЭК 27002: "Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по менеджменту информационной безопасности", 2013

[ISO/IEC 15415] ИСО/МЭК 15415:2011: "Информационные технологии. Технологии автоматической идентификации и сбора данных. Спецификация испытаний штрихового кода на соответствие качества печати. Двумерные символы", 2011

[X.690] МСЭ-Т X.690 2008, "СЕТИ ДАННЫХ И ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ. Сетевые и системные аспекты OSI. Абстрактная синтаксическая нотация версии 1 (ASN.1) Информационная технология. Правила кодирования ASN.1"

— — — — — — — —

Добавление A к части 13

ПРИМЕР ИСПОЛЬЗОВАНИЯ (ИНФОРМАЦИОННОЕ)

В этом разделе дается общий обзор использования цифровой печати для защиты неэлектронного документа. Рассматриваемый здесь конкретный случай использования – это защита визового документа (см. рис. A.1). Хотя в других случаях использования технические детали могут отличаться, применяются те же самые общие принципы.

Общий рабочий процесс можно разделить на три этапа. В качестве предварительного условия должны быть сгенерированы сертификаты органа, подписывающего визы (VSC). Затем генерируются цифровые печати, после чего они подтверждаются.

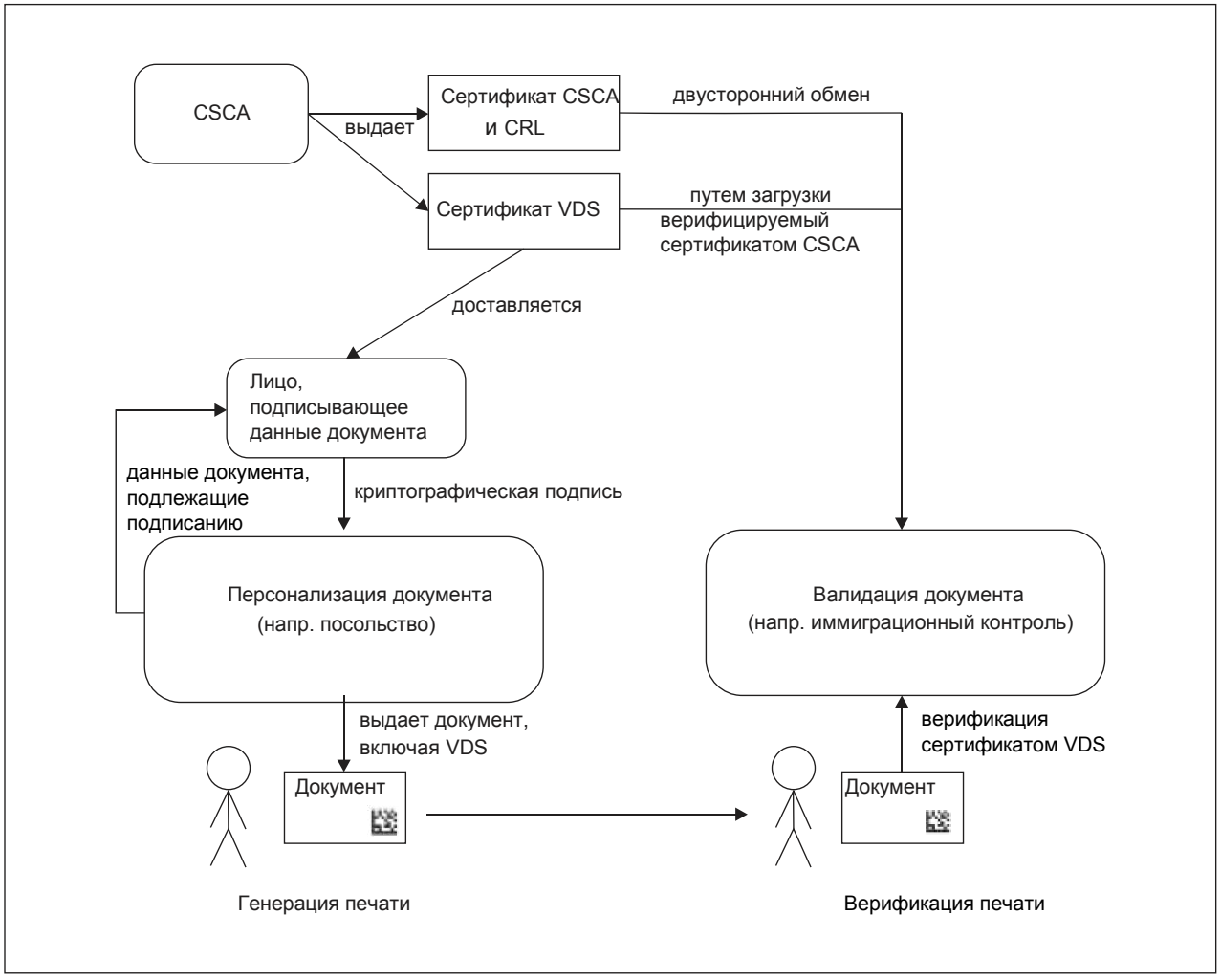

Рис. A.1. Пример использования VDS

A.1 ПРЕДВАРИТЕЛЬНОЕ УСЛОВИЕ: ГЕНЕРАЦИЯ СЕРТИФИКАТА ОРГАНА, ПОДПИСЫВАЮЩЕГО ВИЗЫ

Подписание визы в рамках PKI основано на настройке PKI для электронных паспортов, определенных ИКАО. В основе процесса лежит национальный центр удостоверения подписей (CSCA) каждой страны. CSCA публикует сертификат CSCA, содержащий открытый ключ CSCA. Для обеспечения доверия между странами этот сертификат распространяется надежным образом путем двустороннего обмена или с помощью мастер-списков.

Орган, подписывающий визы – это орган, который фактически подписывает цифровые печати. VSC выдаются центром CSCA и, следовательно, могут верифицироваться с помощью сертификата CSCA.

A.2 ГЕНЕРАЦИЯ ЦИФРОВОЙ ПЕЧАТИ

Цифровая печать генерируется в два этапа:

a) Заявители обращаются за визой в посольство по месту своего проживания. Посольство регистрирует данные заявителя и проверяет, отвечает ли заявитель требованиям для получения визы. Если требования выполнены, посольство направляет цифровое представление записанных данных органу, подписывающему визы (VS). VS может быть либо (1) центральным органом, расположенным в стране, выдающей визы (и посольство подключается к VS по защищенному каналу), либо (2) VS могут быть децентрализованными подразделениями, размещенными в каждом посольстве, которые используют, например, смарт-карты, содержащие криптографические ключи, непосредственно привязанные к системе персонализации. В любом случае VS криптографически подписывает записанные данные.

b) Для подписания орган, подписывающий визы, использует пару ключей, состоящую из закрытого и открытого ключей. Фактическое подписание осуществляется с помощью закрытого ключа, а открытый ключ хранится в сертификате органа, подписывающего визы. Полученная подпись отправляется обратно в систему персонализации виз, если подписывающий визы орган не является локальной частью системы персонализации, печатается на визовой наклейке и прикрепляется к паспорту заявителя.

A.3 ВАЛИДАЦИЯ ЦИФРОВОЙ ПЕЧАТИ

Когда заявители въезжают в страну, выдавшую визы, они предъявляют свои визы в орган по проверке виз (VVA), например, в орган иммиграционного контроля государства выдачи. VVA проверяет подлинность и целостность цифровой печати на визе путем валидации подписи печати и сравнения напечатанной информации на визовой наклейке и в паспорте с цифровой информацией, хранящейся в печати. Подпись печати проверяется путем идентификации соответствующего сертификата VS с помощью идентификатора, хранящегося в заголовке цифровой печати, а затем с помощью открытого ключа сертификата VS. Как указано в предыдущих пунктах, действительность самого сертификата VS может быть проверена с помощью сертификата CSCA.

Примечание

Поскольку все сертификаты находятся в открытом доступе, действительность визы может быть проверена любой третьей стороной, а не только государством выдачи. Таким образом, этот подход может применяться в случае использования союзов стран, когда одна страна выдает визу для другой страны (как делается, например, в Европейском союзе). Другой пример использования – верификация виз авиакомпаниями перед посадкой в самолет.

Примечание

Критерии определения того, можно ли доверять визовому документу, основываясь на цифровой печати и МСЗ визы и паспорта, устанавливаются правилами валидации.

— — — — — — — —

Добавление B к части 13

ПРЕОБРАЗОВАНИЕ ФОРМАТОВ ПОДПИСЕЙ ECDSA (ИНФОРМАЦИОННОЕ)

B.1 КОДИРОВАНИЕ ЦЕЛЫХ ЧИСЕЛ В BER/DER

Целые числа кодируются в соответствии с базовыми правилами кодирования (BER) и отличительными правилами кодирования (DER) в качестве знакового кодирования данных с обратным порядком следования байтов минимальной длины, после чего применяется схема Тег-Длина-Значение (TLV). Они различаются следующими случаями:

a) Предположим, что значение целого числа является положительным, а наиболее значимый бит (MSB) равен нулю в минимальном целочисленном представлении без знака. Тогда беззнаковое целочисленное представление имеет следующий вид в значении BER/DER:

```
|0bbbbbbb| ...
```

b) Предположим, что значение целого числа является положительным, а MSB является единицей в минимальном целочисленном представлении без знака, то есть имеет вид `|1bbbbbbb|...` Тогда байт, содержащий нули, ставится впереди и значение BER/DER равно:

```
|00000000|1bbbbbbb| ...
```

c) Предположим, что значение целого числа является отрицательным. Тогда это значение кодируется как дополнение до двух, например, путем принятия минимального целочисленного представления без знака, инвертирования и добавления единицы. После этого MSB устанавливается на единицу. Например, для -25357 минимальное беззнаковое целочисленное представление равно:

```
|0110 0011|0000 1101|
```

Это инвертируется в

```
|1001 1100|1111 0010|
```

Добавляется единица

```
|1001 1100|1111 0011|,
```

что приводит к значению BER/DER. Обратите внимание, что тот факт, что число является отрицательным, может быть непосредственно выведен из того факта, что MSB (здесь слева) – это один.

Наконец, один дает значение TLV, помещая два байта перед вышеуказанными закодированными значениями BER/DER. Первый байт – это тег с константой `0x02`. Второй байт содержит длину (т. е. количество байтов) следующего закодированного значения BER/DER. Декодирование может быть легко выполнено путем, например, распознавания по MSB, кодируется ли отрицательное или положительное целое число, и применения описанных выше шагов в обратном порядке.

B.2 ПРИМЕР

В таблице B.1 приведены некоторые примеры целых чисел в кодировании BER/DER.

Таблица B.1. Примеры кодирования BER/DER для некоторых целочисленных значений

Значение (дес.)	*Тег (шест.)*	*Длина (шест.)*	*Значение (шест.)*	*Значение (двоичное)*
0	0x02	0x01	0x00	00000000
127	0x02	0x01	0x7F	01111111
128	0x02	0x02	0x00 0x80	00000000 10000000
-129	0x02	0x02	0xFF 0x7F	11111111 01111111

B.3 ПОДПИСИ ECDSA В ASN.1/DER

Описание подписи ECDSA в ASN.1:

```
Signature ::= SEQUENCE {
         r INTEGER, s INTEGER
}
```

Эта последовательность кодируется в соответствии с DER как тройка TLV с тегом `0x30`, длина – как количество байтов следующего значения, а значение – как конкатенация троек TLV кодировки `r`, присоединенных с кодировкой `s`.

Два примера последовательностей (целые числа `r` и `s` подписи ECDSA в действительности, конечно, гораздо больше) приведены в таблице B.2.

Таблица B.2. Кодированные по DER последовательности двух целых чисел

Целые числа		*TLV последовательности*		
R	***S***	*Тег*	*Длина*	*Значение*
127	1	0x30	0x06	0x02 0x01 0x7F 0x02 0x01 0x01
128	127	0x30	0x07	0x02 0x02 0x00 0x80 0x02 0x01 0x7F

Обратите внимание, что для подписи ECDSA числа `r` и `s` всегда являются положительными целыми числами. Поэтому для преобразования необработанной подписи в формат DER необходимо сначала разделить эту подпись пополам, чтобы получить числа `r` и `s` по отдельности, а затем закодировать их в виде закодированной по DER последовательности ASN.1 в соответствии с приведенным выше определением. И наоборот, чтобы декодировать подпись ECDSA в формате DER, нужно сначала декодировать последовательность, извлечь беззнаковое целочисленное представление `r` и `s` и установить как `r`, так и `s` для представления фиксированной длины (= длине размера ключа), удалив или добавив ведущие нулевые байты, если это необходимо (например, в случае ECDSA-256 `r` и `s` должны иметь длину 256 бит = 32 байтам), и прибавив значение, полученное из `s`, к значению, полученному из `r`.

— — — — — — — —

Добавление C к части 13

ПРИМЕРЫ КОДИРОВАНИЯ ПО СХЕМЕ C40 (ИНФОРМАЦИОННОЕ)

C.1 ПРИМЕР 1

Предположим, что строка "XK<CD" должна быть закодирована. По определению перед кодированием все вхождения '<' заменяются на <SPACE> (<ПРОБЕЛ>). В результате получается строка "XK CD", т.е. "XK<SPACE>CD" (вставлен один пробел). Кодирование/декодирование строки "XK<SPACE>CD" по схеме C40 показано в таблице C.1.

Таблица C.1. Пример кодирования/декодирования строки "XK<SPACE>CD"

Операция	***Результат***			
Исходная строка	“XK<SPACE>CD”			
Группировка в тройки	(X, K, <SPACE>)		(C, D,)	
Замена на значения C40 и заполнение	(37, 24, 3)		(16, 17, заполнение)	
Вычисление 16-битного целого значения	60164		26281	
	Байт 1 (div)	**Байт 2 (mod)**	**Байт 1 (div)**	**Байт 2 (mod)**
Получаемая последовательность байтов (десятичная)	235	4	102	169
Получаемая последовательность байтов (шестнадцатеричная)	0xEB	0x04	0x66	0xA9

C.2 ПРИМЕР 2

Предположим, что строка "XKCD" должна быть закодирована. Строка состоит исключительно из прописных букв. Ее кодирование/декодирование по схеме C40 показано в таблице C.2.

Таблица C.2. Пример кодирования/декодирования строки"XKCD"

Операция	***Результат***	
Исходная строка	“XKCD”	
Группировка в тройки	(X, K, C)	(D, ,)
Замена на значения C40 и заполнение	(37, 24, 16)	(разблокировать C40 и кодировать в ASCII)
Вычисление 16-битного целого значения	60177	

Операция	***Результат***			
	Байт 1 (div)	**Байт 2 (mod)**	**Байт 1 (div)**	**Байт 2 (mod)**
Получаемая последовательность байтов (десятичная)	235	11	254	69
Получаемая последовательность байтов (шестнадцатеричная)	0xEB	0x11	0xFE	0x45

— — — — — — — —

Добавление D к части 13

ПРАВИЛА ПОЛИТИКИ ВАЛИДАЦИИ (ИНФОРМАЦИОННОЕ)

Политика валидации – это набор правил валидации, которые позволяют определить действительность печати на документе. Применение этой политики обеспечивает индикацию статуса с одним из следующих значений:

a) ДЕЙСТВИТЕЛЬНАЯ. Подлинность и целостность печати подтверждается. Здесь подлинность означает, что данные в печати были действительно подписаны лицом, подписывающим штрих-коды страны выдачи документа, и соответствующий сертификат лица, подписывающего штрих-коды, действителен. Целостность означает, что данные МСЗ скрепленного печатью документа не были изменены, а цифровая печать не была переставлена с документа, к которому она была первоначально прикреплена.

b) НЕДЕЙСТВИТЕЛЬНАЯ. Печать не признается действительной и требуется дальнейшее расследование. Недействительность может иметь место по следующим трем причинам:

   1) *Мошенничество/подделка*. Это включает в себя несанкционированную персонализацию документа с использованием украденной пустой наклейки, изменение данных персонализации документа с использованием оригинальной наклейки или перестановка наклейки со штрих-кодом с украденного документа (например, паспорта) на другой документ, или другие способы фальсификации.

   2) *Повреждение/разрыв*. Штрих-код не может быть декодирован из-за износа, разрыва или пятен.

   3) *Неизвестные и/или неожиданные ошибки*. Это включает в себя непредсказуемые ошибки. Они возникают, например, из-за неполадок в реализации программного обеспечения, используемого для декодирования, или ошибочного кодирования при персонализации.

К индикации статуса "НЕДЕЙСТВИТЕЛЬНАЯ" привязаны субиндикации статуса. Они указывают на причины недействительности печати. Поскольку вероятность мошенничества зависит от этих причин, индикации и субиндикации статуса рекомендуется связывать с тремя уровнями доверия: "заслуживает доверия", "средняя вероятность мошенничества" и "высокая вероятность мошенничества". Рекомендуемая схема показана в таблице D.1.

Эта общая политика валидации всегда учитывает следующие вопросы:

a) Действительна ли видимая цифровая печать?

b) Действительна ли МСЗ документа?

c) Соответствует ли МСЗ документа видимой цифровой печати?

Ниже приведены правила валидации для каждого типа контроля, перечень критериев валидации, ожидаемые результаты для каждого критерия и результирующие субиндикации статуса.

Валидация видимой цифровой печати

1. Валидация формата

    - если физический формат кодирования не соответствует спецификации или если ошибки, вызванные физическим шумом, невозможно исправить, то фигурирует статус НЕДЕЙСТВИТЕЛЬНАЯ с субиндикацией ОШИБКА_СЧИТЫВАНИЯ;

    - если формат кодирования (т. е. структура печати, состоящая из заголовка, зоны сообщений и зоны подписи, или двоичное/C40 кодирование) не соответствует спецификации, или

    - если значения, ожидаемые в заголовке, неизвестны, или

    - если обязательное поле в зоне сообщений отсутствует, или

    - если формат поля в зоне сообщений не соответствует спецификации версии, определенной в заголовке, то фигурирует статус НЕДЕЙСТВИТЕЛЬНАЯ с субиндикацией НЕПРАВИЛЬНЫЙ_ФОРМАТ, в противном случае валидация продолжается, или

    - если в зоне сообщений присутствует неизвестное поле, то должна быть установлена субиндикация НЕИЗВЕСТНЫЙ_ЭЛЕМЕНТ. Индикация статуса будет ДЕЙСТВИТЕЛЬНАЯ или НЕДЕЙСТВИТЕЛЬНАЯ в зависимости от действительности подписи, верифицируемой на нижеуказанных этапах. Обратите внимание, что если подпись действительна, то само по себе наличие неизвестного элемента не должно нарушать действительность печати.

2. Валидация подписи

    - если сертификат лица, подписывающего штрих-коды, указанный в заголовке печати, отсутствует, то фигурирует статус НЕДЕЙСТВИТЕЛЬНАЯ с субиндикацией НЕИЗВЕСТНЫЙ_СЕРТИФИКАТ;

    - если сертификат лица, подписывающего штрих-коды, указанный в заголовке печати, не был подписан CSCA или если верификация подписи не удалась, то фигурирует статус НЕДЕЙСТВИТЕЛЬНАЯ с субиндикацией НЕНАДЕЖНЫЙ_СЕРТИФИКАТ;

    - если сертификат лица, подписывающего штрих-коды, содержит расширение "Тип документа" и содержимое штрих-кода включает в себя MC3, а тип документа MC3 не содержится в расширении "Тип документа", то фигурирует статус НЕДЕЙСТВИТЕЛЬНАЯ с субиндикацией НЕДЕЙСТВИТЕЛЬНЫЙ_ТИП ДОКУМЕНТА;

    - если срок действия сертификата лица, подписывающего штрих-коды, указанного в заголовке печати, истек, то фигурирует статус НЕДЕЙСТВИТЕЛЬНАЯ с субиндикацией ПРОСРОЧЕННЫЙ _СЕРТИФИКАТ;

    - если сертификат лица, подписывающего штрих-коды, указанный в заголовке печати, отозван то фигурирует статус НЕДЕЙСТВИТЕЛЬНАЯ с субиндикацией ОТОЗВАННЫЙ_СЕРТИФИКАТ;

    - если не удается провести верификацию подписи заголовка и зоны сообщений с использованием сертификата лица, подписывающего штрих-коды, указанного в заголовке печати, то фигурирует статус НЕДЕЙСТВИТЕЛЬНАЯ с субиндикацией НЕДЕЙСТВИТЕЛЬНАЯ_ПОДПИСЬ;

    - в противном случае валидация продолжается.

3. Валидация органа выдачи

    - если CSCA не пользуется доверием системы валидации штрих-кодов на своем доверенном домене, то фигурирует статус НЕДЕЙСТВИТЕЛЬНАЯ с субиндикацией НЕНАДЕЖНЫЙ_ СЕРТИФИКАТ, в противном случае валидация продолжается.

Вышеуказанные правила валидации касаются сравнения данных, хранящихся в печати, с данными, хранящимися в МСЗ документа. Кроме того, может быть проведена ручная проверка тех данных, которые хранятся в печати и напечатаны на документе, но не присутствуют в МСЗ документа.

Таблица D.1. Рекомендуемые уровни доверия в рамках политики, касающейся документов

Индикация статуса	***Субиндикация статуса***	***Уровень доверия***
VALID (ДЕЙСТВИТЕЛЬНАЯ)	-	*Заслуживает доверия*
	UNKNOWN_FEATURE (НЕИЗВЕСТНЫЙ_ЭЛЕМЕНТ)	
INVALID (НЕДЕЙСТВИТЕЛЬНАЯ)	READ_ERROR (ОШИБКА_СЧИТЫВАНИЯ)	*Средняя вероятность мошенничества*
	EXPIRED_CERTIFICATE (ПРОСРОЧЕННЫЙ_СЕРТИФИКАТ)	
	WRONG_FORMAT (НЕПРАВИЛЬНЫЙ_ФОРМАТ)	*Высокая вероятность мошенничества*
	UNKNOWN_CERTIFICATE (НЕИЗВЕСТНЫЙ_СЕРТИФИКАТ)	
	UNTRUSTED_CERTIFICATE (НЕНАДЕЖНЫЙ_СЕРТИФИКАТ)	
	INVALID_DOCUMENTTYPE (НЕДЕЙСТВИТЕЛЬНЫЙ_ТИП ДОКУМЕНТА)	
	REVOKED_CERTIFICATE (ОТОЗВАННЫЙ_СЕРТИФИКАТ)	
	INVALID_SIGNATURE (НЕДЕЙСТВИТЕЛЬНАЯ_ПОДПИСЬ)	

— КОНЕЦ —

ISBN 978-92-9265-273-9