

РУКОВОДЯЩИЙ ДОКУМЕНТ РЕСПУБЛИКИ БЕЛАРУСЬ

**Банковские технологии
ФОРМАТ КАРТОЧКИ ОТКРЫТОГО КЛЮЧА**

**Банкаўскія тэхналогіі
ФАРМАТ КАРТКІ АДКРЫТАГА КЛЮЧА**

УДК [681.3.067:003]:006.354(476)

Ключевые слова: ключ личный подписи, ключ проверки подписи открытый, подпись электронная цифровая, формирования общего ключа протокол

ОКС 35.240.40

Предисловие

1 РАЗРАБОТАН Государственным центром безопасности информации при Президенте Республики Беларусь, ЗАО «Авест»

2 ВНЕСЕН Управлением безопасности и защиты информации Национального банка Республики Беларусь

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Совета директоров Национального банка Республики Беларусь от «__» 2004 г. №

4 ВВЕДЕН ВПЕРВЫЕ

Настоящий руководящий документ не может быть тиражирован и распространен без разрешения Национального банка Республики Беларусь

Издан на русском языке

Содержание

1	Область применения	1
2	Определения.....	1
3	Обозначения и сокращения	2
4	Общие требования к карточке открытого ключа	2
5	Структура карточки открытого ключа	2
6	Заголовок.....	2
7	Информация о владельце открытого ключа, являющемся юридическим лицом.....	3
7.1	Поле для указания наименования организации.....	3
7.2	Поле для указания страны.....	3
7.3	Поле для указания области	3
7.4	Поле для указания населенного пункта.....	3
7.5	Поле для указания подразделения	3
7.6	Поле для указания общих данных.....	3
7.7	Поле для указания адреса электронной почты	3
8	Информация о владельце открытого ключа, являющемся физическим лицом	4
8.1	Поле для указания фамилии, имени и отчества.....	4
8.2	Поле для указания страны.....	4
8.3	Поле для указания области	4
8.4	Поле для указания населенного пункта.....	4
8.5	Поле для указания места работы и должности	4
8.6	Поле для указания подразделения	4
8.7	Поле для указания данных из документа, удостоверяющего личность.....	4
8.8	Поле для указания места жительства.....	4
9	Назначение, область применения и дополнительные атрибуты.....	5
9.1	Поле для указания назначения и области применения ключей	5
9.2	Поле для указания дополнительных атрибутов ключа	5
10	Сроки действия ключей	5
10.1	Поле для указания срока действия открытого ключа	5
10.2	Поле для указания срока использования личного ключа подписи.....	5
11	Информация об открытом ключе.....	5
11.1	Поле для указания наименования алгоритма.....	5
11.2	Поле для указания значения открытого ключа.....	6
11.3	Поле для указания параметров алгоритма	6
12	Подпись и удостоверение карточки открытого ключа	6
12.1	Поле для подписи карточки открытого ключа, если владельцем является физическое лицо.....	6
12.2	Поле для подписи карточки открытого ключа, если владельцем является юридическое лицо	6
12.3	Поле для удостоверения карточки	6
	Приложение А	7
	Приложение Б.....	9

РУКОВОДЯЩИЙ ДОКУМЕНТ РЕСПУБЛИКИ БЕЛАРУСЬ

**Банковские технологии
ФОРМАТ КАРТОЧКИ ОТКРЫТОГО КЛЮЧА****Банкаўскія тэхналогіі
ФАРМАТ КАРТКІ АДКРЫТАГА КЛЮЧА**

Дата введения 2004–07–01

1 Область применения

Настоящий руководящий документ распространяется на карточки открытого ключа, используемые при применении средств криптографической защиты информации, в том числе в технологии электронной цифровой подписи.

Настоящий руководящий документ устанавливает требования к формату карточки открытого ключа.

Настоящий руководящий документ применяется при создании карточек открытого ключа, при разработке и сертификации средств криптографической защиты информации, в том числе средств электронной цифровой подписи.

2 Определения

В настоящем руководящем документе применяются следующие термины с соответствующими определениями:

Алгоритм – алгоритм электронной цифровой подписи или алгоритм протокола формирования общего ключа.

Владелец открытого ключа - физическое или юридическое лицо, являющееся владельцем личного ключа, соответствующего данному открытому ключу.

Идентификатор объекта – значение (отличающееся от других подобных значений), которое связывается с информационным объектом.

Информационный объект – некоторая точно определенная совокупность информации, определение или спецификация, использование которой в конкретном взаимодействии идентифицируется соответствующим именем.

Карточка открытого ключа - документ на бумажном носителе, содержащий значение открытого ключа и подтверждающий его принадлежность какому-либо физическому или юридическому лицу.

Открытый ключ – открытый ключ проверки подписи или открытый ключ для протокола формирования общего ключа.

Протокол формирования общего ключа – криптографический протокол, позволяющий сторонам выработать одинаковый конфиденциальный ключ путем обмена открытыми ключами.

Срок действия открытого ключа - промежуток времени, в течение которого предполагается использовать этот ключ.

3 Обозначения и сокращения

В настоящем руководящем документе применяются следующие обозначения и сокращения:

ЭЦП – электронная цифровая подпись.

4 Общие требования к карточке открытого ключа

4.1 Формат карточки открытого ключа, в том числе обязательность наличия определенных полей, устанавливает собственник информационной системы, в которой применяется карточка открытого ключа, с учетом требований настоящего руководящего документа.

Примечание - Собственник информационной системы, в которой применяется карточка открытого ключа, должен осуществлять контроль за достоверностью данных, указываемых в карточке открытого ключа ее владельцем.

4.2 Содержание полей карточки открытого ключа определяется владельцем открытого ключа, приведенного в карточке.

4.3 Поля карточки открытого ключа должны приводиться в том же порядке, в котором они приведены в тексте настоящего руководящего документа.

4.4 В случае, когда содержание карточки размещается более чем на одном листе бумаги, каждый лист карточки должен быть подписан и удостоверен таким же образом, как это определено в разделе 12.

4.5 Следующие поля карточки открытого ключа являются обязательными:

- поле заголовка;
- поле для указания владельца открытого ключа;
- поле для указания срока действия открытого ключа;
- поле для указания срока использования личного ключа подписи (в случае если формируется карточка открытого ключа проверки подписи);
- поле для указания алгоритма;
- поле для указания значения открытого ключа;
- поле для указания параметров алгоритма.

4.6 Карточка открытого ключа заполняется на государственном языке Республики Беларусь.

5 Структура карточки открытого ключа

Карточка открытого ключа состоит из набора полей, которые в зависимости от их содержания объединяются в разделы. Некоторые поля и разделы являются необязательными. Каждое поле состоит из наименования и содержательной части. Наименование поля должно быть указано в карточке в виде, полностью совпадающем с установленным. Содержание поля указывается в произвольной форме, но оно должно соответствовать установленным требованиям к содержанию поля.

6 Заголовок

Наименование поля: «Карточка открытого ключа».

Содержание поля: информация о карточке открытого ключа. В качестве информации о карточке открытого ключа могут быть указаны сведения о системе, в которой предполагается использовать приведенный в карточке открытый ключ.

7 Информация о владельце открытого ключа, являющемся юридическим лицом

7.1 Поле для указания наименования организации

Наименование поля: «Наименование организации владельца открытого ключа:».

Содержание поля: наименование организации, являющейся владельцем открытого ключа, указанного в карточке открытого ключа. В данном поле может быть приведен юридический адрес указанной организации.

7.2 Поле для указания страны

Наименование поля: «Страна:».

Содержание поля: двухбуквенный международный код страны, в которой зарегистрирована организация, являющаяся владельцем ключей.

7.3 Поле для указания области

Наименование поля: «Область:».

Содержание поля: наименование единицы административно-территориального деления страны, в которой зарегистрирована организация, являющаяся владельцем открытого ключа, указанного в карточке открытого ключа.

7.4 Поле для указания населенного пункта

Наименование поля: «Населенный пункт:».

Содержание поля: наименование населенного пункта, в котором зарегистрирована организация, являющаяся владельцем открытого ключа, указанного в карточке открытого ключа.

7.5 Поле для указания подразделения

Наименование поля: «Подразделение:».

Содержание поля: наименование подразделения, сотрудники которого отвечают за работу с криптографическими ключами, приведенными в данной карточке.

7.6 Поле для указания общих данных

Наименование поля: «Общие данные:».

Содержание поля: данные о сотруднике, ответственном за работу с криптографическими ключами, или, если данные ключи используются автоматизированной службой (сервисом, сервером), то наименование данной службы.

7.7 Поле для указания адреса электронной почты

Наименование поля: «Адрес электронной почты:».

Содержание поля: адрес электронной почты организации, по которому можно связаться с администрацией организации или с сотрудниками, ответственными за использование ключей, при возникновении проблем или для получения дополнительных разъяснений.

8 Информация о владельце открытого ключа, являющемся физическим лицом

8.1 Поле для указания фамилии, имени и отчества

Наименование поля: «Ф.И.О.:».

Содержание поля: фамилия, имя и отчество владельца открытого ключа или другая идентификационная информация о владельце открытого ключа.

8.2 Поле для указания страны

Наименование поля: «Страна:».

Содержание поля: двухбуквенный международный код страны, гражданином которой является владелец открытого ключа.

8.3 Поле для указания области

Наименование поля: «Область:».

Содержание поля: наименование единицы административно-территориального деления страны, в которой находится организация, выдавшая владельцу открытого ключа, указанного в карточке открытого ключа, документ, удостоверяющий личность.

8.4 Поле для указания населенного пункта

Наименование поля: «Населенный пункт:».

Содержание поля: наименование населенного пункта, в котором находится организация, выдавшая владельцу открытого ключа, указанного в карточке открытого ключа, документ, удостоверяющий личность.

8.5 Поле для указания места работы и должности

Наименование поля: «Место работы и должность:».

Содержание поля: наименование организации, в которой работает владелец открытого ключа, и его должности.

8.6 Поле для указания подразделения

Наименование поля: «Подразделение:».

Содержание поля: наименование подразделения организации, в котором работает физическое лицо.

8.7 Поле для указания данных из документа, удостоверяющего личность

Наименование поля: «Данные из документа, удостоверяющего личность:».

Содержание поля: обязательно содержит наименование и номер документа, удостоверяющего личность. Может содержать и другую информацию из документа, удостоверяющего личность владельца открытого ключа.

8.8 Поле для указания места жительства

Наименование поля: «Адрес места жительства:».

Содержание поля: адрес места жительства или прописки владельца открытого ключа на момент формирования карточки.

9 Назначение, область применения и дополнительные атрибуты

В полях раздела может быть указана дополнительная информация, отсутствующая в основном содержании карточки открытого ключа, о назначении и области применения открытого ключа, наличии у владельца ключа прав доступа к той или иной информационной системе, дополнительных атрибутах владельца открытого ключа, необходимых для использования приведенного в карточке открытого ключа в конкретной информационной системе.

9.1 Поле для указания назначения и области применения ключей

Наименование поля: «Назначение ключа:».

Содержание поля: список описаний назначений ключей, области применения и их идентификатора как информационных объектов. Описание каждого назначения должно иметь вид: «Наименование назначения (идентификатор объекта)». Назначение ключей может отсутствовать. В этом случае указывается только идентификатор объекта.

9.2 Поле для указания дополнительных атрибутов ключа

Наименование поля: «Дополнительные атрибуты ключа:».

Содержание: список значений дополнительных атрибутов ключей с указанием идентификатора объекта этих атрибутов и описаниями атрибута. Описания каждого атрибута и его значения должны иметь вид: «Описание атрибута (идентификатор объекта): значение атрибута». Описание атрибута может отсутствовать.

Если дополнительный атрибут может принимать значение «да» (истина) либо «нет» (ложь), и значением атрибута является «да» (истина), то значение атрибута и предшествующий ему символ «:» могут быть опущены.

Поле должно содержать информацию, позволяющую точно установить идентификатор объекта и значение каждого атрибута. В случае необходимости в карточке может быть указано несколько полей дополнительных атрибутов. Каждый атрибут может быть представлен только единожды.

10 Сроки действия ключей

10.1 Поле для указания срока действия открытого ключа

Наименование поля: «Срок действия открытого ключа:».

Содержание: в поле указывается время начала и время окончания действия открытого ключа.

10.2 Поле для указания срока использования личного ключа подписи

Наименование поля: «Срок использования личного ключа подписи:».

Содержание: в поле указывается время начала и время прекращения использования личного ключа подписи.

11 Информация об открытом ключе

11.1 Поле для указания наименования алгоритма

Наименование поля: «Алгоритм:».

Содержание поля: информация, позволяющая точно установить алгоритм, в соответствии с которым получено значение открытого ключа, приведенного в карточке открытого ключа.

11.2 Поле для указания значения открытого ключа

Наименование поля: «Значение открытого ключа:».

Содержание поля: значение открытого ключа. Открытый ключ должен быть представлен в виде, соответствующем требованиям алгоритма и позволяющем однозначно установить его значение.

11.3 Поле для указания параметров алгоритма

Наименование поля: «Параметры алгоритма:».

Содержание поля: значения всех параметров алгоритма и величин, с использованием которых можно точно установить то, что приведенные в этом поле параметры соответствуют требованиям указанного алгоритма. Параметры должны быть представлены в виде, соответствующем требованиям алгоритма и позволяющем однозначно установить их значения. Допускается указание в этом поле вместо значений параметров и величин ссылки на документ, в котором приведены данные, составляющие содержание этого поля.

12 Подпись и удостоверение карточки открытого ключа

12.1 Поле для подписи карточки открытого ключа, если владельцем является физическое лицо

Наименование поля: «Подпись владельца открытого ключа:».

Содержание: собственноручная подпись владельца открытого ключа, его фамилия и инициалы, а также дата подписи карточки.

12.2 Поле для подписи карточки открытого ключа, если владельцем является юридическое лицо

Наименование поля: «Подпись владельца открытого ключа:».

Содержание: собственноручная подпись руководителя организации либо уполномоченного в организации лица, фамилия и инициалы лица, подписавшего карточку, печать организации, а также дата подписи карточки.

12.3 Поле для удостоверения карточки

Наименование поля: «Карточка удостоверена:».

Содержание поля: подписи лиц, удостоверивших карточку открытого ключа. В поле должны быть указаны фамилии и инициалы лиц, удостоверивших карточку, а также даты удостоверения. В поле могут содержаться печати юридических лиц, удостоверивших карточку, а также иная информация о лицах, удостоверивших карточку.

Приложение А
(справочное)

Пример карточки открытого ключа юридического лица

КАРТОЧКА ОТКРЫТОГО КЛЮЧА

*проверки подписи для применения в системе «Клиент-банк» автоматизированной системы
ЗАО «АБВ-банк», всего на двух листах*

Наименование организации владельца открытого ключа: ЗАО «АБВ-банк»

Страна: BY

Область: Гродненская

Населенный пункт: г. Лида

Подразделение: Управление клиентского обслуживания филиала № 17 ЗАО «АБВ-банк»

Общие данные: сервер обработки платежных инструкций АБС «АБВ-банка»

Адрес электронной почты: *srv@abv.by*

Назначение ключа: *подпись документов (1.2.3.1324.56.1.6)*

Дополнительные атрибуты ключа: *идентификатор сервера (1.2.3.1324.56.1.4):
21736485*

Срок действия открытого ключа:

Начало: 12.10.2003 15:45:03

Окончание: 12.10.2013 15:45:02

Алгоритм: *СТБ 1176.2-99*

Значение открытого ключа:

*0509aec8 19a77974 b48408b5 cf651fef 573e1d2e dca1bb1d
f7e39929 ed0e585d 1360043c ebfd6668 899b4cd1 7ddff7ff
502199f8 45d9cdcd 5831687f 02df0bd5 92a99d37 346c3756
8eea1601 4fcaa55d d1f0e2e4 38725311 d1bf17ff 6e7b6c4c
a77a3028 1a4e6131 f8f6e538 f3857970 05da2996 11df43df
39fc5ace a7f54b65.*

*Значение представлено в виде числа, записанного в шестнадцатеричной системе
счисления*

Параметры алгоритма:

Параметр l равен 1022

Параметр r равен 175

Подпись и удостоверение первого листа карточки открытого ключа

Подпись владельца открытого ключа:

23 ноября 2003 г.

Карточка удостоверена:

24 ноября 2003 г.

Начальник отдела автоматизации ЗАО «АБВ-банк»
Стольный А.Н.

Заместитель председателя ЗАО «АБВ-банк»
Смирнов В.В.

Параметр p равен числу (в шестнадцатеричной системе счисления) :

2f0be64f fcddeb67 8f53dec9 82dbe937 ed922564 7f992dd7
c3a59fb9 4c50a434 fc28f140 33b08859 9c01bcfc ecca476d
50d63390 238393f5 90fd9c52 23000699 e7bdbb3a ed3f9298
ee81046a 1139f058 d9b3516d 48fe7f13 13555c5c 8bfdaec4
7e799831 6c3501e7 ab023f11 d2c79b83 6dee6aa5 3e2a6925
a93e0b8d 52b0e9bf.

Параметр q равен числу (в шестнадцатеричной системе счисления):

5cd3 18f6aa2d 57149479 165168b2 07c66f75 a9d4bde5.

Параметр a равен числу (в шестнадцатеричной системе счисления):

16ba9105 946db97b ac6c4976 cb9cb192 bb91b484 835bb4fb
c0677bf5 2ca9669d 8ad12ca5 53c03d37 d25eff5e bf47662f
516277e6 c1ab64be d84bced1 520d6e7d 46d32115 ce48712d
f36bb2aa cfd568be f438cc1f e0841e1f 69c17c00 8522baa9
7153ee12 51ad8e53 5ae62c09 55e0e5c1 94f22bb4 9871d47a
6f17ce7c 21cb9f55.

Параметр N равен числу (в шестнадцатеричной системе счисления):

aaaaaaaa aaaaaaaaa aaaaaaaaa aaaaaaaaa
aaaaaaaa aaaaaaaaa aaaaaaaaa aaaaaaaaa.

Последовательность целых чисел d_0, d_1, \dots, d_i : 512, 257, 129, 65, 33, 17.

Последовательность целых чисел r_0, r_1, \dots, r_s : 175, 88, 45, 23.

Последовательность чисел z_1, \dots, z_{31} , записанных в шестнадцатеричной системе счисления:

529f, 1def, 3d69, 5f8e, 293a, 6659, 21ff, 118c, 283a, 0d78,
1608, 762e, 402b, 5b1b, 372e, 161d, 72a9, 384d, 3fd9, 209d,
55ed, 357a, 45ad, 404c, 6769, 2258, 415c, 13d9, 71af, 6c49,
437d.

Параметр d для генерации параметра a (в шестнадцатеричной системе счисления):

7f0296e 64450de3 9abf9b58 bb82e879 7bdbbdc3 b6bc8850
9b9e2b1b 71b77a42 d5102231 43fac63a c9cc682b d4c35956
b066125b 5cd98e15 8dd14129 360c76dc d9a33601 2de32ac3
1c29fad0 cecef837 ab829b8a 736517e9 651db513 2def0089
b7b28e70 9f1862f0 95753233 16dd8d90 c79332d3 5cf71000
f25231ae 6b9fb31d.

Подпись владельца открытого ключа:

23 ноября 2003 г.

Начальник отдела автоматизации ЗАО «АБВ-банк»
Стольный А.Н.

Карточка удостоверена:

24 ноября 2003 г.

Заместитель председателя ЗАО «АБВ-банк»

Смирнов В.В.

Приложение Б
(справочное)

Пример карточки открытого ключа физического лица

КАРТОЧКА ОТКРЫТОГО КЛЮЧА

*проверки подписи для применения в системе «Клиент-банк» автоматизированной системы
ЗАО «АБВ-банк», всего на двух листах*

Ф.И.О.: *Стольный Артем Никифорович*

Страна: *BY*

Область: *Гродненская*

Населенный пункт: *г. Лида*

Место работы и должность: *ООО «Столарт», директор*

Данные из документа, удостоверяющего личность: *паспорт № КР 283838, выдан
ГОВД г. Лиды 21 декабря 2000 г.*

Адрес места жительства: *г. Лида, ул. Советская, д. 911, кв. 24*

Назначение ключа: *подпись платежных инструкций для банка (1.2.3.1324.56.1.1).*

Дополнительные атрибуты ключа: *идентификатор клиента (1.2.3.1324.56.1.4):
015291342*

Срок действия открытого ключа:

Начало: 12.10.2003 15:45:03

Окончание: 12.10.2013 15:45:02

Алгоритм: *СТБ 1176.2-99*

Значение открытого ключа:

*0509aec8 19a77974 b48408b5 cf651fef 573e1d2e dca1bb1d
f7e39929 ed0e585d 1360043c ebfd668 899b4cd1 7ddff7ff
502199f8 45d9cdcd 5831687f 02df0bd5 92a99d37 346c3756
8eea1601 4fcaa55d d1f0e2e4 38725311 d1bf17ff 6e7b6c4c
a77a3028 1a4e6131 f8f6e538 f3857970 05da2996 11df43df
39fc5ace a7f54b65.*

*Значение представлено в виде числа, записанного в шестнадцатеричной системе
счисления*

Параметры алгоритма ЭЦП:

Параметр l равен 1022.

Параметр r равен 175.

Подпись и удостоверение первого листа карточки открытого ключа

Подпись владельца открытых ключей:

23 ноября 2003 г.

Стольный А.Н.

Карточка удостоверена:

Начальник отдела кадров ООО «Столарт»

24 ноября 2003 г.

Смирнов В.В.

Параметр p равен числу (в шестнадцатеричной системе счисления) :

2f0be64f fcddeb67 8f53dec9 82dbe937 ed922564 7f992dd7
c3a59fb9 4c50a434 fc28f140 33b08859 9c01bcfc ecca476d
50d63390 238393f5 90fd9c52 23000699 e7bdbb3a ed3f9298
ee81046a 1139f058 d9b3516d 48fe7f13 13555c5c 8bfdaec4
7e799831 6c3501e7 ab023f11 d2c79b83 6dee6aa5 3e2a6925
a93e0b8d 52b0e9bf.

Параметр q равен числу (в шестнадцатеричной системе счисления):

5cd3 18f6aa2d 57149479 165168b2 07c66f75 a9d4bde5.

Параметр a равен числу (в шестнадцатеричной системе счисления):

16ba9105 946db97b ac6c4976 cb9cb192 bb91b484 835bb4fb
c0677bf5 2ca9669d 8ad12ca5 53c03d37 d25eff5e bf47662f
516277e6 c1ab64be d84bced1 520d6e7d 46d32115 ce48712d
f36bb2aa cfd568be f438cc1f e0841e1f 69c17c00 8522baa9
7153ee12 51ad8e53 5ae62c09 55e0e5c1 94f22bb4 9871d47a
6f17ce7c 21cb9f55.

Параметр H равен числу (в шестнадцатеричной системе счисления):

aaaaaaaa aaaaaaaaa aaaaaaaaa aaaaaaaaa
aaaaaaaa aaaaaaaaa aaaaaaaaa aaaaaaaaa.

Последовательность целых чисел d_0, d_1, \dots, d_i : 512, 257, 129, 65, 33, 17.

Последовательность целых чисел r_0, r_1, \dots, r_s : 175, 88, 45, 23.

Последовательность чисел z_1, \dots, z_{31} , записанных в шестнадцатеричной системе счисления:

529f, 1def, 3d69, 5f8e, 293a, 6659, 21ff, 118c, 283a, 0d78,
1608, 762e, 402b, 5b1b, 372e, 161d, 72a9, 384d, 3fd9, 209d,
55ed, 357a, 45ad, 404c, 6769, 2258, 415c, 13d9, 71af, 6c49,
437d.

Параметр d для генерации параметра *a* (в шестнадцатеричной системе счисления):

7f0296e 64450de3 9abf9b58 bb82e879 7bdbbdc3 b6bc8850
9b9e2b1b 71b77a42 d5102231 43fac63a c9cc682b d4c35956
b066125b 5cd98e15 8dd14129 360c76dc d9a33601 2de32ac3
1c29fad0 cecef837 ab829b8a 736517e9 651db513 2def0089
b7b28e70 9f1862f0 95753233 16dd8d90 c79332d3 5cf71000
f25231ae 6b9fb31d.

Подпись владельца открытых ключей:

23 ноября 2003 г.

Стольный А.Н.

Карточка удостоверена:

Начальник отдела кадров ООО «Столарт»

24 ноября 2003 г.

Смирнов В.В.