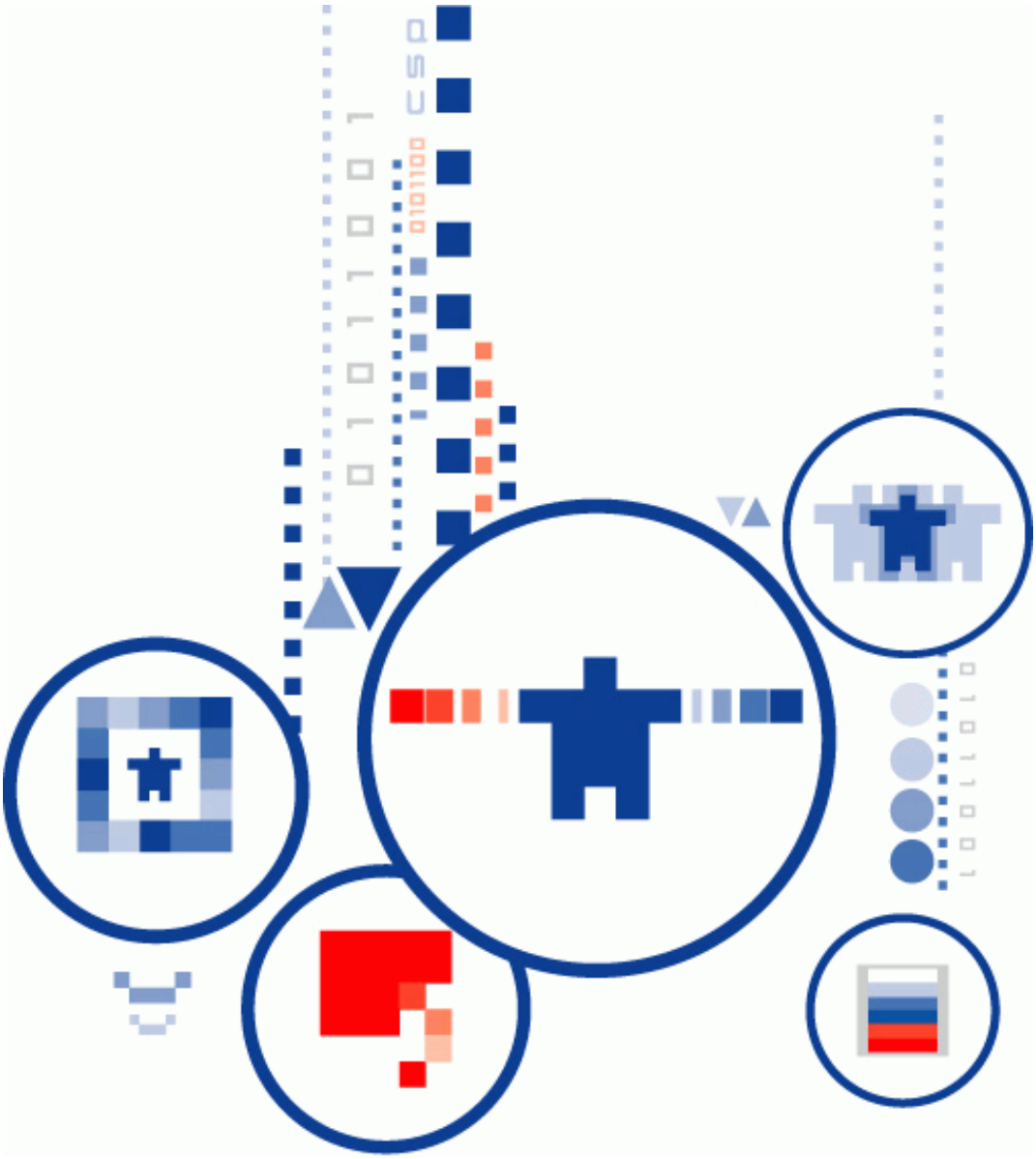

Сервер Электронной Подписи «КриптоПро DSS»

Компонент ПАКМ «КриптоПро HSM»

Технические условия для записи апплета на SIM-карту

СОДЕРЖАНИЕ

О документе

В настоящем документе описаны технические условия для записи на SIM-карту апплета, при помощи которого осуществляется подтверждение операций, обрабатываемых СЭП «КриптоПро DSS».

Обозначения и сокращения

AID	—	Applet IDentifier
ALW	—	Always
BAP	—	Fr. «Bon à Personnaliser» – “good for personalization”
DGI	—	Data Grouping Identifier
EEPROM	—	Electrically Erasable Programmable Read-Only Memory
ICCID	—	Integrated Circuit Card IDentifier
MSL	—	Minimum Security Level
JCVM	—	Java Card Virtual Machine
SIM	—	Subscriber Identification Module
SM	—	Short Message
STK	—	SIM ToolKit
SSD	—	Supplementary Security Domain
TAR	—	Toolkit Application Reference
TLV	—	Tag Length Value
ПИН	—	Персональный идентификационный номер

1. Требования к SIM-карте

К SIM-картам, на которые предполагается запись апплета, предъявляются следующие требования:

- Global Platform 2.1.1 и выше.
- JavaCard 2.2.2 и выше.
- Поддержка интегрального типа int, наличие модуля javacardx.framework.util.intx.
- Алгоритм шифрования DES в режиме CBC.
- Алгоритм дополнения ISO 9797-1 Padding Method 2.
- Алгоритм шифрования AES.
- Поддержка AES-MAC.
- Поддержка HMAC-SHA1.
- Доступ на чтение файла EF ICCID.
- Параметры безопасности: MSL апплета - 010E (необходимо шифрование и CBC-MAC).
- Наличие свободной памяти EEPROM не менее 36 Кб и RAM не менее 1420 байт.
- Поддержка динамического выделения памяти RAM и EEPROM.
- JCVM-буфер размером не менее 1024 байт.
- SM-буфер не менее 1000 байт.
- Свободный TAR апплета, равный 454350.

Размер апплета складывается из (значения в байтах):

- EEPROM = 30134 (пакет) + 1298 (апплет) + 1677 (персонализация) + 2700 (пакет sim-util)
- RAM = 1399 (апплет) + 20 (персонализация)

2. Взаимодействие с терминалом

Для взаимодействия с терминалом (мобильным устройством, в которое вставляется SIM-карта с апплетом), апплет использует возможности, перечисленные в Таблица 1.

Таблица 1 — Взаимодействие с терминалом

Пункт	Описание
Проактивные команды	DISPLAY TEXT, GET INPUT, SEND SHORT MESSAGE, TIMER MANAGEMENT
События, на которые подписан апплет	EVENT_FORMATTED_SMS_PP_ENV, EVENT_FORMATTED_SMS_PP_UPD, EVENT_TIMER_EXPIRATION
STK-меню	Не используется

3. Защита данных при передаче производителю SIM-карт

При обмене информацией между оператором сотовой связи и производителем SIM-карт на разных этапах передаются параметры установки апплета и файлы персонализации, содержащие криптографические ключи. Для защиты данной информации при передаче необходимо применять организационные или технические меры, описанные ниже.

3.1. Защита организационными мерами

Пересылка параметров установки апплета и файлов персонализации без криптографической защиты возможна только при передаче материального носителя (оптический диск, флеш-накопитель и т.п.) с этими данными из рук в руки без использования каналов связи. При этом носитель должен быть передан доверенным лицом оператора сотовой связи доверенному лицу производителя SIM-карт.

3.2. Защита техническими мерами

Пересылка параметров установки апплета и файлов персонализации производится сторонами в подписанном и зашифрованном виде в соответствии с рекомендациями по стандартизации Технического комитета по стандартизации «Криптографическая защита информации» (ТК 26) «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.12–2015, ГОСТ Р 34.13–2015, ГОСТ Р 34.10–2012 и ГОСТ Р 34.11–2012 в сообщениях формата CMS».

При этом используются отдельная ключевая пара отправителя и отдельная ключевая пара получателя, не используемые для других целей, отличных от упомянутых в настоящем документе.

Сертификаты ключей проверки электронной подписи предварительно передаются между сторонами доверенным образом. На стороне производителя SIM-карт используется любое поддерживающее процедуры указанного документа ТК 26 СКЗИ.

4. Установка апплета

Апплет устанавливается в Supplementary Security Domain (SSD). Требования к SSD:

- Поддержка SCP80, KeySet 1, длина ключа – 16 байт.

4.1. Параметры установки апплета

Параметры установки апплета находятся в файле **mobile-id-ecp.conf.** Далее приведены значимые поля установки:

```
[AID]
package=A1130001180006FFF7100D8945435000
applet=A1130001180006FFF7100D8945435008

[INSTALL]
priv=00
appparams=0404810880040F0303060C00

type=SIM
accdomain=00
priority=255
timers=1
msl=010E
```

Application specific parameters (C9) находятся в поле **appparams** и задают следующие значения:

a. **1-й байт** - кол-во последующих байт, описывающих короткий номер платформы для отправки ответных сообщений (L)
b. **2-й байт** – количество цифр в коротком номере
c. **3-й байт** – кодировка значения короткого номера
d. **4..3+L-2 байты** – (L) короткий номер платформы в формате 81h для отправки статусов выполнения команд
e. **2+L байт** - время показа диалогов в командах STATUS по умолчанию (по умолчанию 4)
f. **3+L байт** - максимальное количество попыток ввода ПИН (по умолчанию 15)
g. **4+L байт** - максимальное количество попыток ввода ПИН подряд (по умолчанию 3)
h. **5+L байт** - максимальное количество попыток задания ПИН подряд при активации и смене ПИН (по умолчанию 3)
i. **6+L байт** - минимальный размер ПИН (по умолчанию 6)
j. **7+L байт** - максимальный размер ПИН (по умолчанию 12)
k. **8+L байт**- тип ПИН (0 - только цифры; 1 - цифры и буквы) (по умолчанию 0)

Обязательными являются параметры:

- короткий номер (**4..3+L-2 байты**).

Остальные параметры могут быть не указаны, тогда будут использованы значения по умолчанию.

Пример:

`appparams=0404810880040F0303060C00`

04 — кол-во последующих байт, описывающих короткий номер(4 байта);

04 — кол-во цифр в коротком номере (4 цифры);

81 — кодировка значения короткого номера (всегда 81);

0880 — короткий номер (в данном случае 8008);

04 — время показа диалогов (4 статус команды);

0F — кол-во попыток ввода ПИН (15 попыток);

03 — кол-во попыток ввода ПИН подряд (3 попытки);

03 — кол-во попыток задания ПИН при активации и смене ПИН (3 попытки);

06 — минимальный размер ПИН (6 цифр);

0C — максимальный размер ПИН (12 цифр);

00 — тип ПИН (только цифры).

4.2. Порядок установки апплета

Установка апплета на SIM-карту должна происходить следующим образом.

Апплет должен быть установлен на SIM-карту с персонализированным файлом EF ICCID.

1) Загрузить пакет **com.a1systems.simutil** (A1130001181003). Файл sim-util--<версия>.cap.
2) Загрузить пакет **com.a1systems.javacard.mid.ecp** (A1130001180006FFF7100D8945435000). Файл mobile-id-ecp-<версия>.cap.
3) Установить апплет **com.a1systems.javacard.mid.ecp.Application** (A1130001180006FFF7100D8945435008) из пакета com.a1systems.mid.ecp, указав параметры установки из файла конфигурации mobile-id-ecp.conf.
4) Запустить скрипт персонализации, содержащий:
   a) Одну команду `SELECT by AID 00A40400 10 A1130001180006FFF7100D8945435008`

   b) Одну команду `STORE DATA` с DGI (Data Grouping Identifier), равным `0000 00E20000 50 <DCKA>`,
   где DCKA - соответствующее поле из файла персонализации длиной 0x50.

   c) Команды `STORE DATA` с DGI равным `0001 00E20001 Ln <Строка словаря>`

4.3. Персонализация диалогов апплета

Каждой ситуации (каждому диалогу) в апплете соответствует свой уникальный **DialogID.** Для того, чтобы персонализировать апплет текстами, необходимо загрузить массив, где каждому **DialogID** будет соответствовать текстовая строка.

Для сокращения места, которое занимает текст на SIM-карте, вместо самого текста можно указывать ссылку на другой **DialogID,** который нужно использовать, если его текст подходит для данной ситуации.

Размер памяти, выделяемый для диалогов, зависит от длины текстов, необходимых для персонализации. Значение **EEPROM,** указанное в Разделе 1, соответствует текстам, приведенным в Таблица 3.

4.3.1. Данные команды для DGI = 0001 (строки словаря)

Таблица 2 — Данные команды для DGI = 0001 (строки словаря)

1-й байт	Последующие байты
Идентификатор строки	Текст в формате: ➢ **SMS-default** 7 bit со старшим битом, установленным в 0; ➢ **UCS2** в упакованном формате согласно Приложению B документа 3GPP TS 11.11 V8.14.0 (2007-06); формат 81h. Или ссылка на существующую строку: ➢ **1-й байт** - FF, признак ссылки на существующую строку; ➢ **2-й байт** - идентификатор строки.

4.3.2. Пример готовой команды для строки ID 36:

```
00E200012124811D089EC8B8B1BAB02E20A2C0B5B1C3B5C2C1CF20B7B0BCB5BDB02053494D2E
```

4.3.3. Идентификаторы строк

Таблица 3. Идентификаторы строк

ИД	Описание	Пример
36	Апплет в состоянии LOCK, ему пришла команда активации	Ошибка. Требуется замена SIM.
35	Апплет в состоянии ACTIVE, ему пришла команда активации	Ошибка. Повторная активация невозможна.
33	Апплет в состоянии NULL, ему пришла команда активации	Ошибка. Требуется замена SIM.
37	Диалог активации апплета	Введите код активации. Осталось попыток:
38	Код активации введен неверно	Неверно. Осталось попыток:

ИД	Описание	Пример
39	Исчерпаны N попыток подряд для ввода кода активации	Попытки исчерпаны. Требуется замена SIM.
40	Исчерпаны M попыток	Попытки исчерпаны. Требуется замена SIM.
41	Апплет просит придумать ПИН-код	Придумайте ПИН-код <6-12> <цифр>
42	Апплет просит повторить ввод ПИН-кода	Повторите ввод:
43	Пользователь ввел несовпадающие ПИНы	Несовпадение. Придумайте ПИН-код снова <6-12> <цифр>
44	Пользователь 3 раза не смог задать совпадающие пины	Требуется повторная активация.
45	Успешное завершение активации	Успешно!
68	Апплет в состоянии LOCK, ему пришла команда подписи от DSS	Ошибка. Требуется замена SIM.
66	Апплет в состоянии INIT, ему пришла команда подписи от DSS	Ошибка. Требуется активация.
65	Апплет в состоянии NULL, ему пришла команда подписи от DSS	Ошибка. Требуется замена SIM.
73	Апплету пришла команда подписи от DSS со слишком длинным текстом	Ошибка. Повторите операцию.
69	Апплет запрашивает ввод ПИН-кода	Введите ПИН-код. Осталось попыток:
70	Абонент неверно указал ПИН-код	Неверно. Введите ПИН-код снова. Осталось попыток:
71	Исчерпаны N попыток ввода ПИН-кода	Попытки исчерпаны. Требуется замена SIM.
72	Исчерпаны M попыток ввода ПИН-кода	Попытки исчерпаны. Требуется замена SIM.
77	Абонент ввел верный ПИН код	ПИН-код верный.
74	Абонент ввел верный пин код. Осталось меньше 10 использований ключа	ПИН-код верный. Осталось использований:

ИД	Описание	Пример
75	Подтверждение операции. Пользователь ввел правильный ПИН. Количество использований Ка исчерпано.	ПИН-код верный. Кол-во использований исчерпано.
100	Апплет в состоянии LOCK, ему пришла команда смены ПИН-кода	Ошибка. Требуется замена SIM.
98	Апплет в состоянии INIT, ему пришла команда смены ПИН-кода	Ошибка. Требуется активация.
97	Апплет в состоянии NULL, ему пришла команда смены ПИН-кода	Ошибка. Требуется замена SIM.
101	Апплет просит ввести текущий пин	Введите текущий ПИН-код. Осталось попыток:
102	Пользователь неверно ввел текущий пин код	Неверно. Введите текущий ПИН-код. Осталось попыток:
103	Исчерпаны N попыток ввода текущего ПИН	Попытки исчерпаны. Требуется замена SIM.
104	Исчерпаны M попыток ввода неверного ПИН	Попытки исчерпаны. Требуется замена SIM.
105	Абонент верно указал текущий пин-код. Апплет просит пользователя задать новый пин.	Придумайте ПИН-код <6-12> <цифр>
106	Апплет просит повторит ввод нового пина	Повторите ввод:
107	Абонент указан несовпадающие пины	Несовпадение. Придумайте ПИН-код снова <6-12> <цифр>
108	Абонент 3 раза не смог задать совпадающие ПИНы	ПИН-код не изменен. Повторите снова.
109	Успешно задан новый ПИН	ПИН-код изменен.
129	Смена ключа активации. Апплет получил команду смены ПИН в состоянии NULL.	Ошибка. Требуется замена SIM.
130	Смена ключа активации. Апплет получил команду смены ПИН в состоянии INIT.	Ошибка. Требуется активация.
131	Смена ключа активации. Апплет получил команду смены ключа в состоянии ACTIVE2.	Ошибка. Повторная смена ключа невозможна.

ИД	Описание	Пример
132	Смена ключа активации. Апплет получил команду смены ключа в состоянии LOCK.	Ошибка. Требуется замена SIM.
133	Смена ключа активации. Апплет получил команду смены ключа в состоянии ACTIVE.	Введите текущий ПИН-код:
134	Смена ключа активации. Пользователь неправильно указал текущий ПИН-код.	Неверно. Введите текущий ПИН-код. Осталось попыток:
135	Смена ключа активации. Пользователь неправильно указал текущий ПИН-код. Исчерпан Счетчик 1.	Попытки исчерпаны. Требуется замена SIM.
136	Смена ключа активации. Пользователь неправильно указал текущий ПИН-код. Исчерпан Счетчик 2.	Попытки исчерпаны. Требуется замена SIM.
137	Смена ключа активации. Апплет просит пользователя ввести код активации.	Введите код активации. Блок:
139	Смена ключа активации. Ошибка проверки контрольного числа блока. Апплет просит пользователя ввести код активации снова.	Введите код активации. Блок:
141	Смена ключа активации. Смена ключа активации пройдена успешно.	Успешно.

5. Тестирование апплета

Для тестирования работы криптографического модуля апплета используется контрольный пример, приведенный в данном разделе.

1. Запустите скрипт самопроверки апплета, содержащий
   a. Команду `SELECT by AID`
      `00A40400 10 A1130001180006FFF7100D8945435008`

   b. Команду `SELF TEST`
      `00DD0000 40`
      `9E8446D23DD555F0CD58083EB3080870AC216D1714E3D04A9B97FC2343A82760`
      `C9DCE4E8454E715EF183E31FAE465E3C5DC7D336AC2A377BA4AB1A2BAAAD59756BA`
      `D8603C408EB43067CD4A85A6BDB366845B48164516F11901275A89430FB94`

   c. Команду `GET RESPONSE`
      `00C00000 20`

2. В ответ апплет должен вернуть подпись HMAC ГОСТ Р 34.11–2012 (256 бит):

   `327A42CA109A334627ED149242005FB414F26E86D828FAD0E40545B12133C0EC`

Для проведения дальнейшего тестирования профиля SIM-карт, BAP-карта данного профиля передается оператору связи, который самостоятельно или с привлечением производителя апплета производит полнофункциональное тестирование.

СВЕДЕНИЯ О РАЗРАБОТЧИКЕ

Компания КриптоПро создана в 2000 году и в настоящее время занимает лидирующее положение по распространению средств криптографической защиты информации и электронной цифровой подписи.

Основное направление деятельности компании – разработка средств криптографической защиты информации и развитие Инфраструктуры Открытых Ключей (Public Key Infrastructure) на основе использования международных рекомендаций и российских криптографических алгоритмов.

Компания разработала полный спектр программных и аппаратных продуктов для обеспечения целостности, авторства и конфиденциальности информации с применением ЭП и шифрования для использования в различных средах (Windows, Unix, Java). Новое направление продуктов компании – программно-аппаратные средства криптографической защиты информации и использованием смарт-карт и USB ключей, позволяющих существенно повысить безопасность систем, использующих ЭП.

Компания КриптоПро является разработчиком и поставщиком средств применения ЭП в автоматизированных информационных системах. Кроме этого, компания оказывает консультационные услуги по обеспечению деятельности удостоверяющих центров и применению ЭП в автоматизированных информационных системах предприятий различных форм собственности.

Удостоверяющий центр компании КриптоПро предоставляет организациям (юридическим лицам) услуги по изготовлению и управлению открытыми и закрытыми ключами пользователей информационных систем, включая процедуру подачи и обработки запросов на сертификаты, верификацию запросов на сертификаты, формирования сертификатов, их получения, использования и отзыва. Также Удостоверяющим центром предоставляются иные сервисные функции, связанные с использованием электронных подписей, шифрованием, обеспечением электронного юридически-значимого документооборота.

Контакты:

ООО «КРИПТО-ПРО»

127018, Москва, ул. Сущёвский вал, 18

Телефон: (495) 995 4820

Факс: (495) 995 4820

URL: http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru