ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 13157-1— 2015

Информационные технологии

ТЕЛЕКОММУНИКАЦИИ И ОБМЕН ИНФОРМАЦИЕЙ МЕЖДУ СИСТЕМАМИ

Безопасность NFC

Часть 1

Службы и протокол безопасности NFC-SEC NFCIP-1

(ISO/IEC 13157-1:2010, IDT)

Издание официальное

Москва
Стандартинформ
2018

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием Государственный научно-исследовательский и конструкторско-технологический институт «ТЕСТ» (ФГУП ГосНИИ «ТЕСТ»), Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 10 сентября 2015 г. № 1329-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 13157-1:2010 «Информационные технологии. Телекоммуникации и обмен информацией между системами. Безопасность NFC. Часть 1. Службы и протокол безопасности NFC-SEC NFCIP-1» (ISO/IEC13157-1:2010 «Information technology — Telecommunications and information exchange between systems — NFC Security— Part 1: NFC-SEC NFCIP-1 security services and protocol», IDT).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Ноябрь 2018 г.

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

ТЕЛЕКОММУНИКАЦИИ И ОБМЕН ИНФОРМАЦИЕЙ МЕЖДУ СИСТЕМАМИ

Безопасность NFC

Часть 1

Службы и протокол безопасности NFC-SEC NFCIP-1

Information technology. Telecommunications and information exchange between systems. NFC Security. Part 1. NFC-SEC NFCIP-1 security services and protocol

Дата введения — 2016—11—01

1 Область применения

Настоящий стандарт определяет службы NFC-SEC Защищенный канал и Совместно используемый секретный ключ для NFCIP-1, а также протокол и виды PDU для данных служб.

Примечания

1 NFC-SEC предназначен исключительно для протокола обмена данными ИСО/МЭК 18092.

2 Настоящий стандарт не затрагивает конкретных механизмов защиты приложения (что обычно необходимо для сценариев использования, связанных со смарт-картами, и стандартизировано в сериях ИСО/МЭК 7816). NFC-SEC может дополнять конкретные механизмы защиты приложений, определенные в ИСО/МЭК 7816.

2 Соответствие

Совместимые реализации используют механизмы защиты в криптографической части NFC-SEC, которая определяет выбранный PID с помощью одной служб или более, определенных в настоящем стандарте.

Совместимые реализации, использующие протокол NFCIP-1, должны также соответствовать требованиям приложения В.

3 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ISO/IEC 7498-1:1994, Information technology — Open Systems Interconnection — Basic Reference Model. Part 1: The Basic Model (Информационные технологии. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель)

ISO 7498-2:1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture (Информационные технологии. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации)

ISO/IEC 10731:1994, Information technology — Open Systems Interconnection — Basic Reference Model — Conventions for the definition of OSI services (Информационные технологии. Взаимосвязь открытых систем. Базовая эталонная модель. Условное обозначение для услуг ВОС)

ISO/IEC 11770-1:1996, Information technology — Security techniques — Key management — Part 1: Framework (Информационные технологии. Методы обеспечения безопасности. Управление ключами защиты. Часть 1. Структура)

Издание официальное

ISO/IEC 13157-2:2010, Information technology — Telecommunications and information exchange between systems — NFC Security — Part 2: NFC-SEC cryptography standard using ECDH and AES (also published by ECMA as Standard ECMA-386 (Информационные технологии. Телекоммуникации и обмен информацией между системами. Безопасность NFC. Часть 2. Криптографический стандарт для NFC-SEC с использованием ECDH и AES

ISO/IEC 18092:2004, Information technology — Telecommunications and information exchange between systems — Near Field Communication — Interface and Protocol (NFCIP-1) (also published by ECMA as Standard ECMA-340) [Информационные технологии. Телекоммуникации и обмен информацией между системами. Интерфейс и протокол связи для ближнего поля-1 (NFCIP-1)]

4 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

4.1 **соединение** (connection): (N)-соединение, определенное в ИСО/МЭК 7498-1.

4.2 **логический объект** (entity): (N)-логический объект, определенный в ИСО/МЭК 7498-1.

4.3 **ключ связи** (link key): Секретный ключ, защищающий коммуникации через защищенный канал.

4.4 **пользователь NFC-SEC** (NFC-SEC User): Объект, использующий службу NFC-SEC.

4.5 **протокол** (protocol): (N)-протокол, определенный в ИСО/МЭК 7498-1.

4.6 **получатель** (Recipient): NFC-SEC-объект, который получает ACT_REQ.

4.7 **защищенный канал** (secure channel): Защищенное NFC-SEC-соединение.

4.8 **отправитель** (Sender): NFC-SEC-объект, который отправляет ACT_REQ.

4.9 **услуга** (service): (N)-услуга, определенная в ИСО/МЭК 7498-1.

4.10 **совместно используемый секретный ключ** (shared secret): Секретный ключ, совместно используемый двумя равноправными пользователями NFC-SEC.

5 Соглашения и обозначения

В настоящем стандарте применены следующие соглашения и обозначения, если не указано иное.

5.1 Представление чисел

Буквы и цифры в круглых скобках представляют собой числа в шестнадцатеричной системе счисления.

Установка битов обозначается НУЛЕМ или ЕДИНИЦЕЙ.

Числа в двоичной системе счисления и битовые комбинации представлены строками, состоящими из цифр 0 и 1, со старшим битом слева. Внутри таких строк может использоваться знак *X* с целью указать, что установка бита не указана внутри строки.

В октетах lsb — бит под номером 1, msb — бит под номером 8.

5.2 Названия

Названия базовых элементов, например конкретных областей, пишутся с прописной начальной буквы.

6 Сокращения

В настоящем стандарте применены следующие сокращения:

ACT_REQ — Activation Request PDU (PDU-запрос на активацию).

ACT_RES — Activation Response PDU (PDU-реакция на активацию).

ENC — Encrypted Packet PDU (PDU-зашифрованный пакет).

ERROR — Error PDU (PDU с ошибкой).

lsb — least significant bit (младший бит).

LSB — Least Significant Byte (младший байт).

msb — most significant bit (старший бит).

MSB — Most Significant Byte (старший байт).

MSG — MesSaGe code (код сообщения).

PCI — Protocol Control Information (протокольная управляющая информация) (см. ИСО/МЭК 7498-1).

PDU — Protocol Data Unit (протокольный блок данных) (см. ИСО/МЭК 7498-1).
PID — Protocol Identifier (идентификатор протокола).
RFU — Reserved for Future Use (зарезервировано для использования в будущем).
SCH — Secure Channel service (служба Защищенный канал).
SDL — Specification and Description Language (язык спецификаций и описаний) (определенный в МСЭ-Т Z.100).
SDU — Service Data Unit (сервисный блок данных) (см. ИСО/МЭК 7498-1).
SEP — Secure Exchange Protocol (протокол безопасного обмена).
SN — Sequence Number (порядковый номер).
SNV — SN variable (переменная SN).
SSE — Shared Secret Service (служба Совместно используемый секретный ключ).
SVC — SerVicE code (код службы).
TMN — Terminate PDU (PDU «Завершить»).
VFY_REQ — Verification Request PDU (PDU-запрос на верификацию).
VFY_RES — Verification Response PDU (PDU-ответ на верификацию).

7 Общие положения

NFC-SEC, как показано на рисунке 1, использует эталонную модель ВОС, определенную в ИСО/МЭК 7498-1.

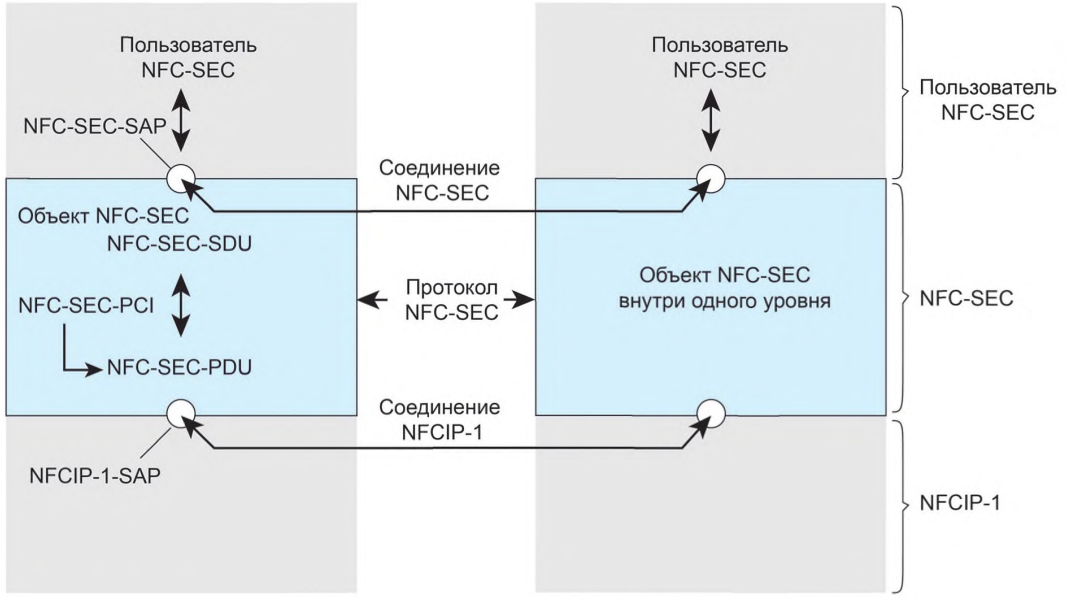


Рисунок 1 — Архитектура NFC-SEC

Пользователи NFC-SEC вызывают и получают доступ к службам NFC-SEC через точки доступа к службам NFC-SEC (NFC-SEC-SAP, NFC-SEC Service Access Point). Объекты NFC-SEC получают NFC-SEC-SDU (запросы) от пользователей NFC-SEC и возвращают им NFC-SEC-SDU (подтверждения).

Настоящий стандарт определяет службу Защищенный канал (SCH) и службу Совместно используемый секретный ключ (SSE).

Для предоставления служб NFC-SEC, объекты NFC-SEC внутри одного уровня обмениваются NFC-SEC-PDU в соответствии с протоколом NFC-SEC посредством NFC-SEC-соединений.

Объекты NFC-SEC внутри одного уровня коммуницируют друг с другом посредством получения доступа к службе передачи данных NFCIP-1 через точки доступа к службам NFCIP-1 (NFCIP-1-SAP, NFCIP-1 Service Access Point), отправляя и получая NFC-SEC-PDU. NFC-SEC-PDU состоит из протокольной управляющей информации NFC-SEC (NFC-SEC-PCI) и одного NFC-SEC-SDU.

8 Службы

Данный раздел определяет две службы SSE и SCH, которые NFC-SEC предоставляет пользователю NFC-SEC. Данные службы позволяют организовать пользователям NFC-SEC криптографически защищенную передачу сообщений между объектами внутри одного уровня посредством протокола, описанного в разделе 9.

Совместно используемые секретные ключи, созданные службами, определенными ниже, должны быть криптографически независимыми от любых совместно используемых секретных ключей, созданных заранее или впоследствии.

8.1 Служба Совместно используемый секретный ключ (SSE)

Служба SSE устанавливает совместно используемый секретный ключ между двумя равноправными пользователями NFC-SEC, который они могут использовать по своему усмотрению.

При вызове SSE должен устанавливаться совместно используемый секретный ключ с помощью механизмов соглашения о ключах и подтверждения ключей, согласно криптографической части NFC-SEC, которая определяет PID.

8.2 Служба Защищенный канал (SCH)

Служба SCH обеспечивает защищенный канал.

При вызове SCH должен устанавливаться ключ связи, путем наследования от совместно используемого секретного ключа, с помощью механизмов соглашения о ключах и подтверждения ключей, и впоследствии должен защищать все коммуникации в любом направлении внутри канала, согласно криптографической части NFC-SEC, которая определяет PID.

9 Механизмы протоколов

Протокол NFC-SEC включает в себя следующие механизмы. На рисунке 2 определена последовательность механизмов протокола.

9.1 Соглашение о ключах

Объекты NFC-SEC внутри одного уровня должны устанавливать совместно используемый секретный ключ, применяя ACT_REQ и ACT_RES, согласно криптографической части NFC-SEC, которая определяет PID.

9.2 Подтверждение ключей

Объекты NFC-SEC внутри одного уровня должны верифицировать согласованный ими совместно используемый секретный ключ, применяя VFY_REQ и VFY_RES, согласно криптографической части NFC-SEC, которая определяет PID.

9.3 Защита PDU

Защита PDU является механизмом только службы SCH.

Объекты NFC-SEC внутри одного уровня должны защищать обмен данными, используя ENC, согласно криптографической части NFC-SEC, которая определяет PID.

Данный механизм должен включать в себя один или более из следующих пунктов, определенных в соответствующем стандарте шифрования NFC-SEC:

- целостность последовательности, соответствующая требованиям 12.3;
- конфиденциальность;
- целостность данных;
- аутентификация источника.

9.4 Завершение

Объекты NFC-SEC внутри одного уровня должны завершить SSE и SCH, используя TMN. После освобождения или деселекции NFCIP-1 или когда NFCIP-1-устройство выключено, экземпляры SSE и SCH должны быть завершены. После перехода в состояние НЕ ЗАНЯТО (IDLE) связанные с данной операцией совместно используемый секретный ключ и ключ связи должны быть уничтожены.

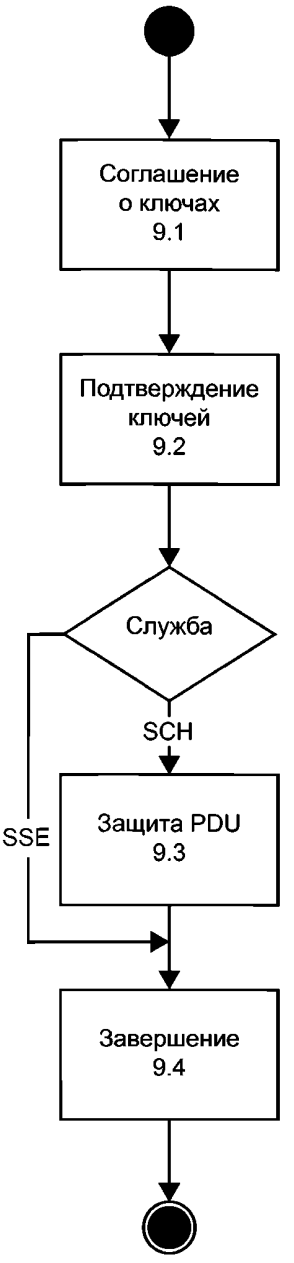


Рисунок 2 — Обобщенная блок-схема служб NFC-SEC

10 Состояния и подсостояния

Модуль протокола NFC-SEC в приложении А указывает переходы состояний для состояний и подсостояний в таблице 1.

Таблица 1 — Состояние

Состояние	Описание
Не занято (Idle)	NFC-SEC находится в готовности запустить новую службу по запросу пользователя NFC-SEC или объекта NFC-SEC внутри одного уровня
Выбор (Select)	NFC-SEC находится в ожидании ACT_RES

Окончание таблицы 1

Состояние	Описание
Установлено (Established)	Служба NFC-SEC запрошена. Данное состояние содержит два подсостояния. В подсостоянии Established_Sender ожидается VFY_RES. В подсостоянии Established_Recipient ожидается VFY_REQ
Подтверждено (Confirmed)	Служба NFC-SEC установлена. Данное состояние содержит два подсостояния. В подсостоянии Confirmed_SSE, совместно используемый секретный ключ готов для получения. В подсостоянии Confirmed_SCH защищенный обмен данными готов

11 NFC-SEC-PDU

NFC-SEC-PDU должны передаваться в PDU «Защищенные данные» NFCIP-1 DEP (Data Exchange Protocol, протокол обмена данными), помещая байт SEP в байт 0 из последовательности байтов транспортных данных DEP. Байты транспортных данных DEP должны содержать ровно один NFC-SEC-PDU.

Структура NFC-SEC-PDU указана на рисунке 3.

SEP	PID	NFC-SEC Payload

Рисунок 3 — Структура NFC-SEC-PDU

Таблица 2 определяет поля NFC-SEC-PDU, как обязательные (*m*, mandatory), запрещенные (*p*, prohibited) или условные (*c*, conditional). Условность (*c*) определяется далее в 11.3.

Таблица 2 — Поля NFC-SEC-PDU

NFC-SEC-PDU	SEP	PID	NFC-SEC Payload
ACT_REQ	*m*	*m*	*c*
ACT_RES	*m*	*p*	*c*
VFY_REQ	*m*	*p*	*c*
VFY_RES	*m*	*p*	*c*
ENC	*m*	*p*	*c*
TMN	*m*	*p*	*p*
ERROR	*m*	*p*	c

11.1 Протокол безопасного обмена (SEP)

Однобайтовое поле протокола безопасного обмена (SEP) определяется следующим образом:

- Значение 00b в SVC указывает на то, что PDU является частью SSE-обмена. Значение 01b в SVC указывает на то, что PDU является частью SCH-обмена.
- Код MSG идентифицирует тип PDU, как определено в таблице 3. Все иные коды являются RFU.
- Биты RFU должны быть установлены в значение НУЛЬ. Получатели должны отклонять PDUc битами RFU, установленными в значение ЕДИНИЦА.

Рисунок 4 определяет присвоение битов.

msb lsb

Bit 8	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1
RFU		SVC		MSG			

Рисунок 4 — Присвоение битов в SEP

Таблица 3 — Типы PDU и их MSG-коды

Код	Название	Описание
0000	ACT_REQ	Запрос на активацию, для запроса новой службы
0001	ACT_RES	Реакция на активацию, для принятия запроса службы
0010	VFY_REQ	Запрос на верификацию, для предоставления на проверку контрольных значений совместно используемого секретного ключа отправителя
0011	VFY_RES	Ответ на верификацию, для предоставления на проверку контрольных значений совместно используемого секретного ключа получателя
0100	ENC	Зашифрованный пакет для защищенного обмена данными
0110	TMN	Запрос на завершение, для завершения службы
1111	ERROR	Ошибка, индикация ошибки
Другой		RFU

11.2 Идентификатор протокола (PID)

Каждая криптографическая часть NFC-SEC настоящего стандарта определяет соответствующий 8-битный PID, который включается только в ACT_REQ.

11.3 Полезная нагрузка NFC-SEC

TMN PDU не должен содержать поля Полезная нагрузка NFC-SEC. Поле Полезная нагрузка NFC-SEC должно состоять из целого числа октетов. Его использование в ERROR PDU определено в соответствующем подразделе ниже. Его использование, структура и кодирование во всех остальных PDU определено в криптографической части NFC-SEC, которая определяет PID.

11.4 Завершить (TMN)

TMNPDU состоит только из поля SEP, как указано в таблице 2.

11.5 Ошибка (ERROR)

ERROR PDU начинается с поля SEP, и если в нем содержится полезная нагрузка, то данная полезная нагрузка должна содержать октетную строку, завершающуюся нулевым символом в поле Полезная нагрузка NFC-SEC.

12 Протокольные правила

Данный раздел определяет правила для протокола NFC-SEC.

12.1 Ошибки протокола и ошибки служб

При получении PDU объектом NFC-SEC в состоянии, когда это не разрешено, он должен ответить с помощью ERROR PDU.

При получении NFC-SEC-объектом PDU, который он не поддерживает или с недопустимым содержимым, определенным в соответствующем стандарте шифрования NFC-SEC, он должен ответить с помощью ERROR PDU.

При получении или отправки NFC-SEC-объектом ERROR PDU, он должен установить состояние протокола в состояние «Не занято».

При получении или отправки NFC-SEC-объектом ERROR PDU, он должен отправить ERROR SDU пользователю NFC-SEC.

При получении SDU объектом NFC-SEC с недопустимым содержимым или в состоянии, когда это не разрешено, он должен ответить с помощью ERROR SDU и не менять состояние.

12.2 Правила взаимодействия

Реализация NFC-SEC может устанавливать верхний предел длины NFC-SEC-SDU. Запросы на пересылку данных, определенные в А.2, с более длинными SDU должны быть отклонены.

Один NFC-SEC-PDU должен содержать ровно один NFC-SEC-SDU.

Объекты NFC-SEC должны отбросить все повторяющиеся NFC-SEC-PDU, как указано в следующем подразделе.

12.3 Целостность последовательности

Стандарты шифрования NFC-SEC, обеспечивающие целостность последовательности, должны определять механизм целостности последовательности, в соответствие с нижеследующим:

- Каждый объект NFC-SEC должен поддерживать свою SNV.
- При создании SCH, получатель должен инициализировать свой SNV с тем же начальным значением, что и SNV отправителя, как указано в криптографической части NFC-SEC, которая определяет PID.
- Криптографическая часть NFC-SEC, которая определяет PID,указывает диапазон значений SNV.
- Сразу после отправки ENC, объект NFC-SEC должен увеличить свою SNV на 1 и затем поместить ее в поле SN.
- Поле SN должно быть защищено механизмом защиты PDU, чтобы внесение любого изменения могло быть обнаружено.
- После получения ENC, объект NFC-SEC должен извлечь поле SN и сравнить его со своим значением SNV. Если SN равняется SNV, то PDU не должно представляться на рассмотрение пользователю NFC-SEC, а должно отбрасываться, при этом состояние и SNV должны оставаться неизменными, как указано в А.4.4.
- Объект NFC-SEC должен увеличить свою SNV на 1.

Состояние «содержимое PDU допустимо?» в А.4.4 должно быть true, если SN равняется SNV, в противном случае — false.

Примечание — В случае наличия ошибок целостности последовательности, NFC-SEC прерывает SCH и уведомляет о данном инциденте обоих равноправных пользователей NFC-SEC. Дальнейшие действия — восстановить SCH с новыми ключами или прервать транзакцию — зависят от пользователей NFC-SEC.

12.4 Криптографическая обработка

Перед отправкой и после получения PDU, отличных от TMN и ERROR, происходит криптографическая обработка, как указано в криптографической части NFC-SEC, которая определяет PID. Если результат криптографической обработки входящих PDU является отрицательным, то решение «содержимое PDU допустимо?» в приложении А будет false.

Приложение А
(обязательное)

Спецификация модуля протокола

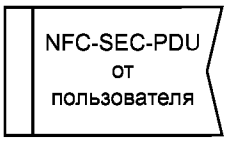
Модуль протокола NFC-SEC в данном приложении определяет последовательность PDU для установления и завершения SSE, а также для установления, использования и завершения SCH.

В дополнение модуль протокола определяет, какие PDU могут быть отправлены или получены в тех или иных состояниях.

А.1 Символы SDL

NFC-SEC-PDU, полученный от объекта NFC-SEC внутри одного уровня, доставленный локальным объектом NFCIP-1.

NFC-SEC-PDU, отправленный объекту NFC-SEC внутри одного уровня, переданный локальному объекту NFCIP-1.



NFC-SEC-SDU, полученный от пользователя NFC-SEC, с запросом на выполнение действия объектом NFC-SEC.

NFC-SEC-SDU, поданный пользователю NFC-SEC, либо в ответ на предыдущий запрос, либо для указания события.

Состояние. В состоянии модуль протокола ожидает какое-либо событие. События, не предусмотренные в схемах, составляют ошибки протокола.

Разветвляющееся условие в процессе обработки событий.

А.2 SDU-запросы

SDU-запросы подаются пользователями NFC-SEC, запрашивающими службу NFC-SEC. Параметры приведены в скобках. Требования к значениям параметров указаны в стандартах шифрования NFC-SEC.

Примечание — Фактический метод реализации примитивов запросов (например, вызовов методов, межпроцессных PDU) выходит за рамки настоящего стандарта.

Вызов службы (Service Invocation)	Запрос на вызов новой службы (тип службы, PID).
Послать данные (Send Data)	Запрос на пересылку данных. Разрешен только для SCH (данные).
Искать данные (Retrieve Data)	Запрос на поиск полученных данных. Разрешен только для SCH.

Искать ключ (Retrieve Secret)	Запрос на поиск установленного совместно используемого секретного ключа. Разрешен только для SSE.
Завершить (Terminate)	Запрос на завершение службы (тип службы).

А.3 SDU-подтверждения

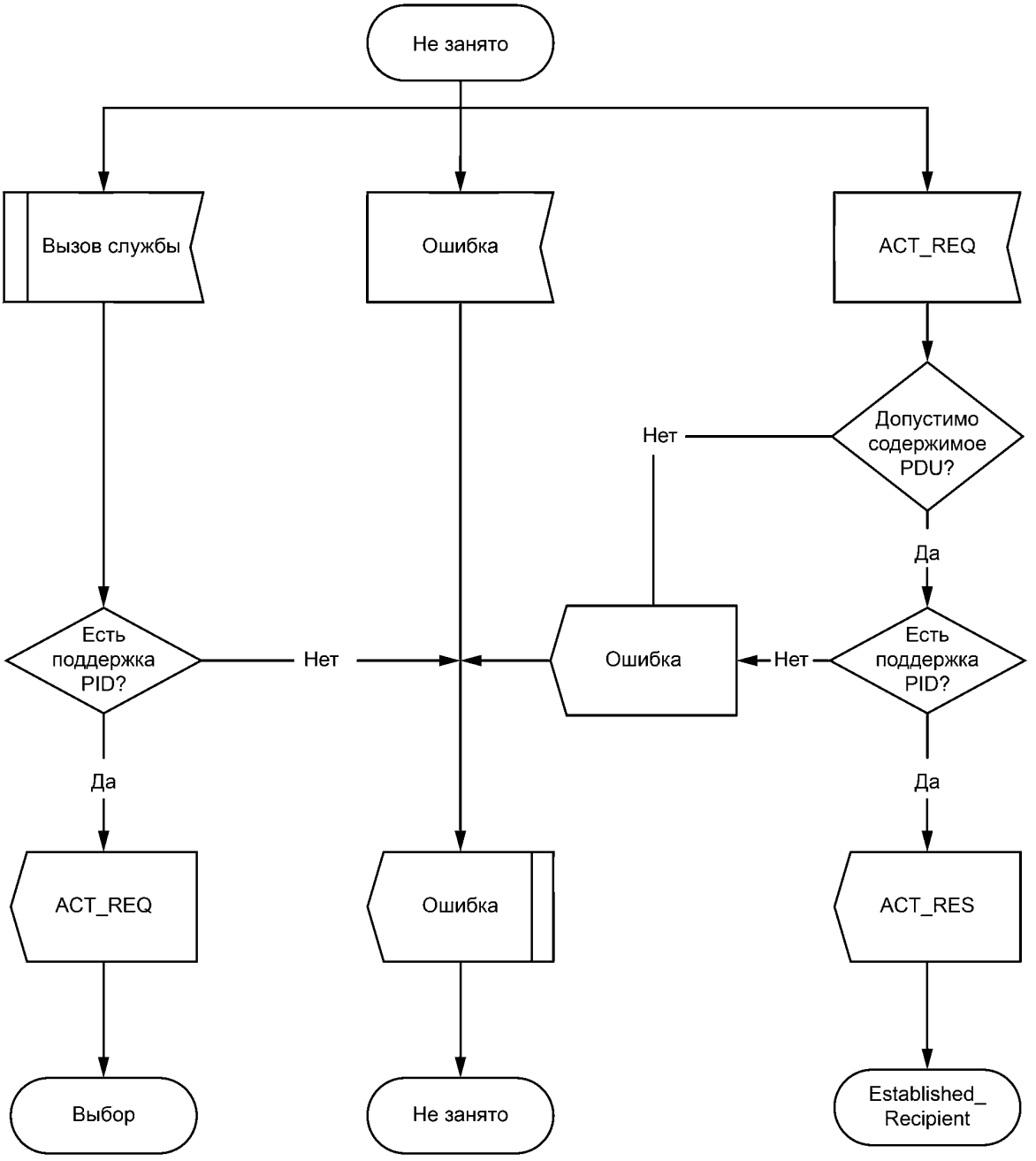
SDU-подтверждения предоставляются объектами NFC-SEC пользователям NFC-SEC. Параметры приведены в скобках. Требования к значениям параметров указаны в стандартах шифрования NFC-SEC.

Примечание — Фактический метод реализации примитивов подтверждения (например, вызовов методов, межпроцессных PDU) выходит за рамки настоящего стандарта.

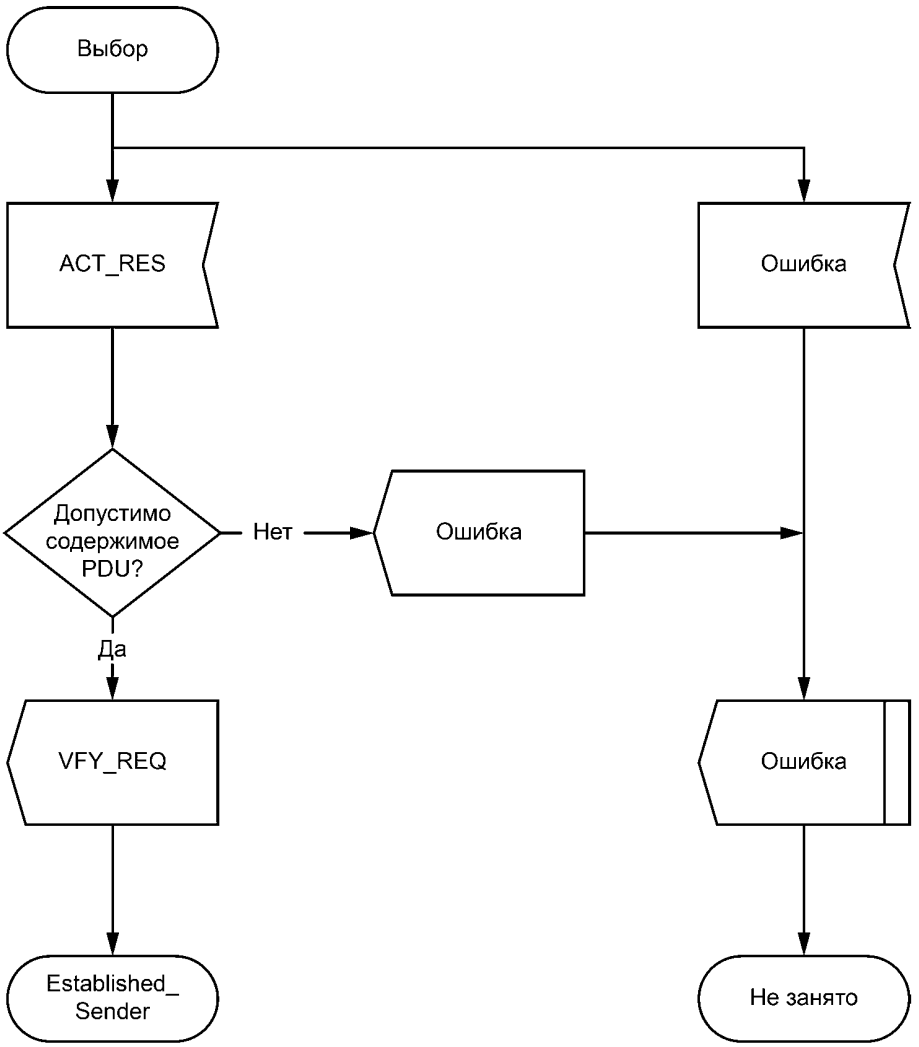
Установлено (Established)	Указывает на успешное установление службы (тип службы).
Данные отправлены (Data Sent)	Указывает результат запроса на пересылку данных (статус). Данный результат может быть положительным или отрицательным, последний — за счет ошибки пересылки или неготовности объекта NFC-SEC к отправке.
Данные имеются (Data Available)	Указывает получение данных.
Возврат данных (Return Data)	Ответ на запрос поиска данных (данные).
Возврат ключа (Return Secret)	Ответ на запрос поиска секретного ключа (совместно используемый секретный ключ).
Завершено (Terminated)	Указывает пользователю на завершение службы (тип службы).
Ошибка (Error)	Указывает на ошибку при обработке запроса или PDU либо на какую-либо другую ошибку. В параметрах может отражаться причина и детали ошибки (детали).

А.4 Диаграммы SDL

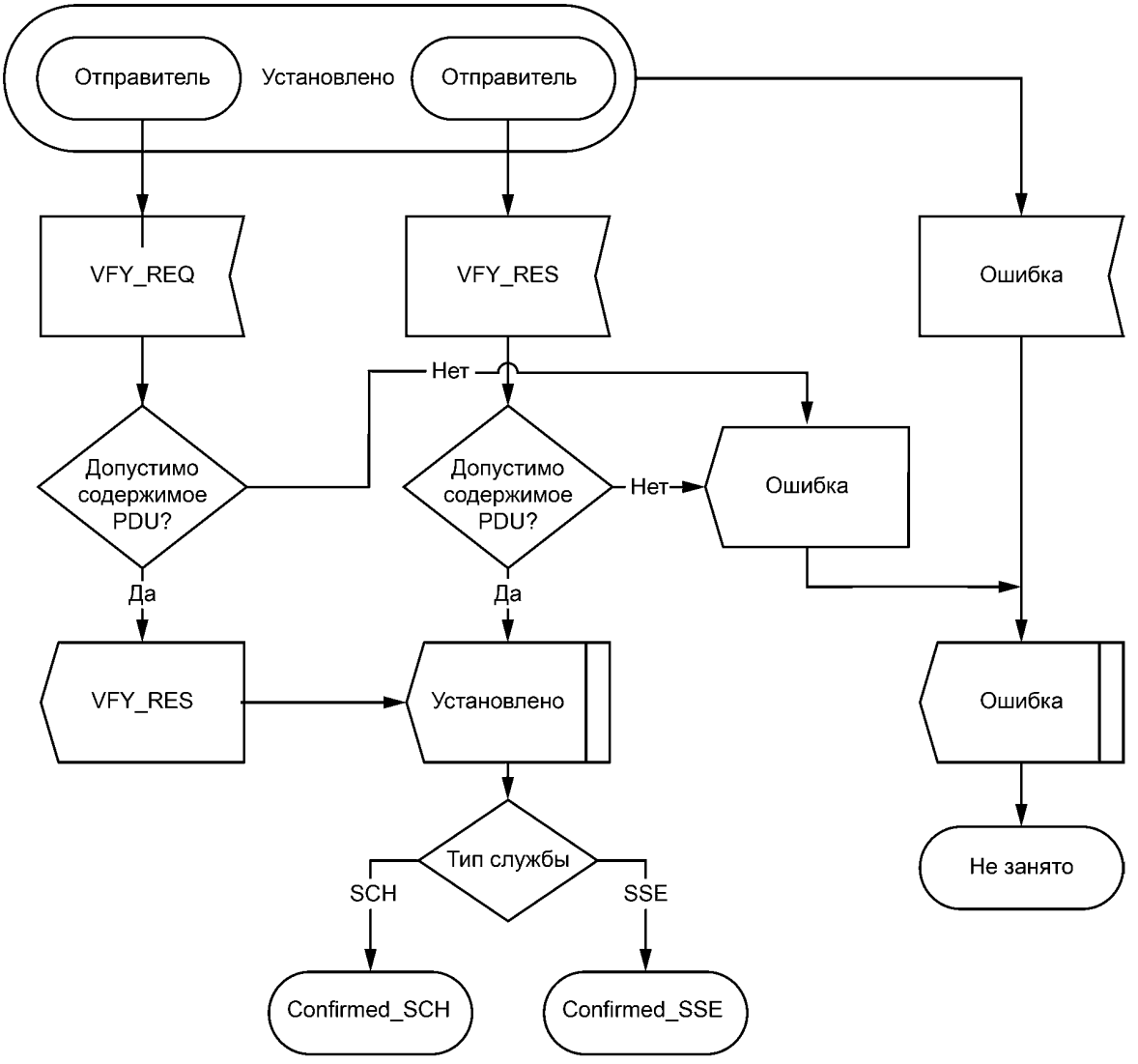
А.4.1 Состояние «Не занято»



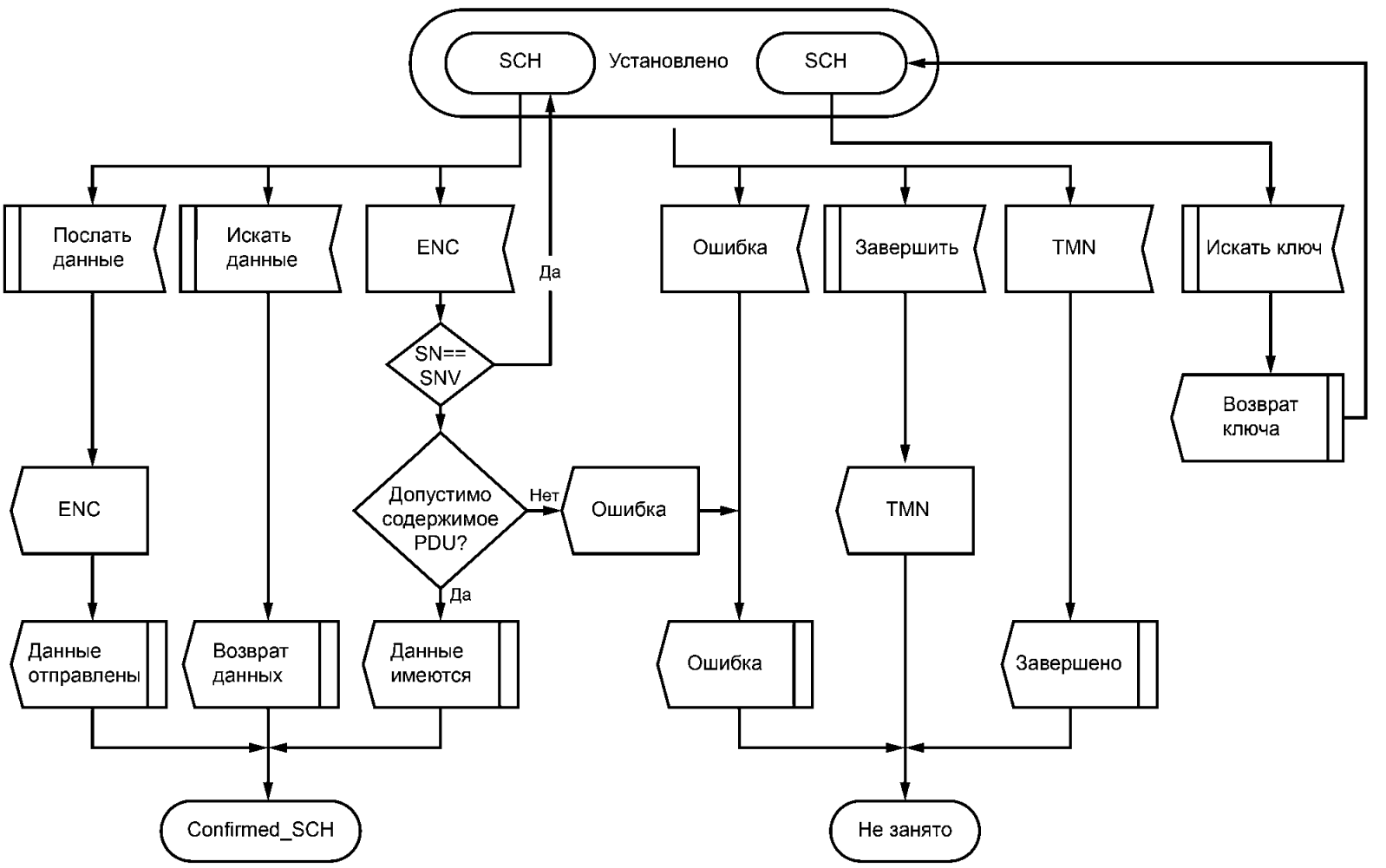
А.4.2 Состояние «Выбор»



А.4.3 Состояние «Установлено»



А.4.4 Состояние «Подтверждено»



Приложение В
(обязательное)

Дополнительные требования при использовании NFC-SEC с ИСО/МЭК 18092 (NFCIP-1)

При использовании настоящего стандарта с реализациями ИСО/МЭК 18092 применяются следующие дополнительные требования.

Данные дополнительные требования, изложенные в В.4, касаются следующих функций:

В.1 Метод заявления NFCIP-1-устройствами поддержки NFC-SEC

Инициатор заявляет о своей поддержке NFC-SEC с помощью поля SECi в ATR_REQ.
Цель заявляет о своей поддержке NFC-SEC с помощью поля SECt в ATR_RES.
Для определения полей SECi и SECt см. В.4.

В.2 Введение защищенного PDU

Дополнительные защищенные PDU используются в протоколе обмена данными, как определено в В.4.

В.3 Расширение правил нумерации PDU для защищенного PDU

Защищенные PDU включены в правила нумерации PDU, как определено в В.4.

В.4 Поправки NFCIP-1

Следующие поправки должны применяться к ИСО/МЭК 18092.

Заменить в 12.5.1.1.1 определение бита 7 PPi следующим:

«
- бит 7: SECi. Инициатор должен устанавливать SECi в значение ЕДИНИЦА, если он поддерживает NFC-SEC; НУЛЬ означает отсутствие поддержки
»

Заменить в 12.5.1.2.1 определение бита 7 PPt следующим:

«
- бит 7: SECt. Цель должна устанавливать SECt в значение ЕДИНИЦА, если она поддерживает NFC-SEC; НУЛЬ означает отсутствие поддержки
»

Заменить в 12.6.1.1.1 определение байта 0: PFB и таблицу 24 следующим:

«
Байт 0: PFB

Байт PFB должен содержать биты для контроля передачи данных и восстановления после ошибки. Байт PFB используется для передачи информации, необходимой для контроля за процессом передачи. Протокол обмена данными определяет следующие базовые типы PDU:

- Информационные PDU для передачи информации на прикладном уровне.
- Защищенные PDU для передачи защищенной информации.
- Подтверждающие PDU для передачи положительных или отрицательных подтверждений. Подтверждающий PDU никогда не содержит поле данных. Подтверждение касается последнего полученного блока.
- Контрольные PDU для обмена контрольной информацией между Инициатором и Целью. Определены два типа контрольных PDU.
- Продления тайм-аута, содержащие поле данных, длиной в 1 байт.
- Привлечение внимания, не содержащее поля данных.

Кодирование PFB, зависящее от его типа, приведено в таблице В.3.

Таблица В.3 — Кодирование битов PFB с 7 по 5

Бит 7	Бит 6	Бит 5	PFB
0	0	0	Информационный PDU
0	0	1	Защищенный PDU
0	1	0	Подтверждающий PDU
1	0	0	Контрольный PDU
Остальные установки являются RFU.			

»

Добавить в 12.6.1.1.1 определение защищенного PDU и добавить рисунок B.3 следующим образом:

«
Определение защищенного PDU:

Бит 7	Бит 6	Бит 5	Бит 4	Бит 3	Бит 2	Бит 1	Бит 0
RFU	RFU	ONE	MI	NAD	DID	PNI	PNI

Рисунок B.3 — Кодирование охраняемых PDU

- бит 7 и бит 6: RFU. Инициатор должен устанавливать их в значение НУЛЬ. Цель должна игнорировать их.
- бит 5: Должен быть установлен в значение ЕДИНИЦА.
- бит 4: Бит, установленный в значение ЕДИНИЦА, показывает, что активировано формирование цепочки многокомпонентной информации.
- бит 3: Бит, установленный в значение ЕДИНИЦА, показывает, что доступен NAD.
- бит 2: Бит, установленный в значение ЕДИНИЦА, показывает, что доступен DID.
- бит 1 и бит 0: Информация о номере пакета PNI.

Информация о номере пакета (PNI) подсчитывает номер пакета, отправленного от Инициатора — Цели, и наоборот, начиная с 0. Данные байты используются для обнаружения ошибок в процессе обработки протоколов.
»

Заменить 12.6.1.2 следующим:

«
12.6.1.2 Обработка информации о номере PDU

12.6.1.2.1 Правила для Инициатора

PNI Инициатора для каждой Цели должна быть установлена в исходное состояние, состоящее из НУЛЕЙ.

При приеме информационного, защищенного или подтверждающего PDU с равным значением PNI, Инициатор должен инкрементировать текущее значение PNI для данной Цели перед необязательной отправкой нового кадра.

12.6.1.2.2 Правила для Цели

PNI Цели должна быть установлена в исходное состояние, состоящее из НУЛЕЙ.

При приеме информационного, защищенного или подтверждающего PDU с равным значением PNI, Цель должна отправить свой ответ с таким же значением PNI и затем инкрементировать значение PNI.
»

Заменить 12.6.1.3.1 следующим:

«
12.6.1.3.1 Общие правила

Первый PDU должен быть отправлен Инициатором.

Когда информационный или защищенный PDU указывает, что принято больше информации, PDU должен быть подтвержден подтверждающим PDU (ACK).

Контрольные PDU используются только в паре. Контрольный запрос должен всегда сопровождаться Контрольным ответом.
»

Заменить 12.6.1.3.3 следующим:

«
12.6.1.3.3 Правила для Цели

Цели разрешено отправлять контрольный PDU (RTO) вместо информационного PDU.

При приеме информационного или защищенного PDU, не содержащего формирования цепочки, это должно быть подтверждено информационным или защищенным PDU.

При приеме подтверждающего PDU (NACK), если значение PNI равно значению PNI предыдущего посланного PDU, предыдущий блок должен быть передан заново.

При приеме ошибочного PDU, Цель не должна отвечать и должна оставаться в том же состоянии.

При приеме контрольного PDU (привлечения внимания), Цель должна ответить отправкой реакции на контрольный PDU (привлечение внимания).
»

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 7498-1:1994	IDT	ГОСТ Р ИСО/МЭК 7498-1—99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель»
ISO 7498-2:1989	IDT	ГОСТ Р ИСО 7498-2—99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации»
ISO/IEC 10731:1994	—	*
ISO/IEC 11770-1:1996	—	*
ISO/IEC 13157-2:2010	—	*
ISO/IEC 18092:2004	—	*

* Соответствующий национальный стандарт отсутствует.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты

УДК 004.71:006.534 ОКС 35.110

Ключевые слова: информационные технологии, телекоммуникации, обмен информацией между системами, безопасность, NFC, службы безопасности NFC-SEC, протокол безопасности NFC-SEC, NFC-SEC, NFCIP-1, коммуникация в ближнем поле

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 26.11.2018. Подписано в печать 06.12.2018. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 1,86.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ» для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru