ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 345— 2018

Интеллектуальные транспортные системы

АВТОМАТИЧЕСКАЯ ИДЕНТИФИКАЦИЯ ТРАНСПОРТНОГО СРЕДСТВА И ОБОРУДОВАНИЯ. ЭЛЕКТРОННАЯ РЕГИСТРАЦИЯ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ ТРАНСПОРТНЫХ СРЕДСТВ

Часть 5

Безопасный обмен данными с использованием симметричных технологий

(ISO 24534-5:2011, NEQ)

Издание официальное

Москва
Стандартинформ
2019

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «Научно-исследовательский институт интеллектуальных транспортных систем» (ООО «НИИ ИТС»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 57 «Интеллектуальные транспортные системы»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 31 декабря 2018 г. № 77-пнст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ИСО 24534-5—2011 «Интеллектуальные транспортные системы. Автоматическая идентификация транспортного средства и оборудования. Электронная регистрационная идентификация (ERI) транспортных средств. Часть 5. Безопасный обмен данными с использованием симметричных технологий» (ISO 24534-5:2011 «Intelligent transport systems — Automatic vehicle and equipment identification — Electronic Registration Identification (ERI) for vehicles — Part 5: Secure communications using symmetrical techniques», NEQ)

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 4 мес до истечения срока его действия разработчику настоящего стандарта по адресу: 105005 г. Москва, Армянский пер., д. 9, стр. 1 и в Федеральное агентство по техническому регулированию и метрологии по адресу: 109074 Москва, Китайгородский проезд, д. 7, стр. 1.

В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и также будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Интеллектуальные транспортные системы

АВТОМАТИЧЕСКАЯ ИДЕНТИФИКАЦИЯ ТРАНСПОРТНОГО СРЕДСТВА И ОБОРУДОВАНИЯ. ЭЛЕКТРОННАЯ РЕГИСТРАЦИЯ ИДЕНТИФИКАЦИОННЫХ ДАННЫХ ТРАНСПОРТНЫХ СРЕДСТВ

Часть 5

Безопасный обмен данными с использованием симметричных технологий

Intelligent transport systems. Automatic vehicle and equipment identification.
Electronic registration of Identification data for vehicles. Part 5.
Secure communications using symmetrical techniques

Срок действия — с 2019—06—01
до 2022—06—01

1 Область применения

Настоящий стандарт описывает требования к электронной регистрации идентификационных данных (ERI), основывающейся на идентификаторе транспортного средства (ТС) (например, для распознавания органами государственной власти), предназначенной для использования в следующих случаях:

- при электронной идентификации местных и иностранных ТС органами государственной власти;
- производстве ТС, обслуживании во время эксплуатационного срока и идентификации при его окончании;
- управлении сроком службы (управлении жизненным циклом ТС);
- адаптировании данных ТС (например, при реализации на международном уровне);
- идентификации в целях обеспечения безопасности;
- сокращении количества совершаемых преступлений;
- оказании коммерческих услуг.

В настоящем стандарте учтена политика конфиденциальности и защиты данных и представлен обзор концепции с точек зрения бортового оборудования и оборудования дорожной инфраструктуры, необходимых для работы системы.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ПНСТ 342—2018 Интеллектуальные транспортные системы. Автоматическая идентификация транспортного средства и оборудования. Электронная регистрация идентификационных данных. Часть 2. Эксплуатационные требования.

ПНСТ 343—2018 Интеллектуальные транспортные системы. Автоматическая идентификация транспортного средства и оборудования. Электронная регистрация идентификационных данных. Часть 3. Данные транспортного средства.

ПНСТ 344—2018 Интеллектуальные транспортные системы. Автоматическая идентификация транспортного средства и оборудования. Электронная регистрация идентификационных данных. Часть 4. Безопасный обмен данными с использованием асимметричных технологий

Издание официальное

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **авторизация** (authorization): Предоставление прав и доступа к использованию оборудования.

3.2 **активная угроза** (active threat): Угроза преднамеренного несанкционированного изменения состояния системы

Пример — Модификация сообщений, воспроизведение сообщений, вставка ложных сообщений, маскировка в качестве уполномоченного лица и отказ в обслуживании.

3.3 **аутентификация объекта** (entity authentication): Подтверждение того, что объект является авторизованным.

3.4 **безопасность** (security): Защита информации и данных для того, чтобы неавторизованные лица или системы не могли их читать или модифицировать, а уполномоченным лицам или системам не было отказано в доступе к ним.

3.5 **беспроводной интерфейс** (air interface): Интерфейс без проводника между бортовым оборудованием (OBE) и считывателем/опросным листом, посредством которого соединение бортового оборудования (OBE) со считывателем/запросчиком осуществляется с помощью электромагнитных сигналов.

3.6 **бортовой автор ERI** (onboard ERI writer): Автор ERI является частью ее встроенного оборудования.

Примечание — Встроенный автор ERI может быть, например, устройством с бесконтактным соединением (PCD).

3.7 **взаимная аутентификация** (mutual authentication): Аутентификация объекта, идентифицирующая транспортные средства.

3.8 **внешняя запись ERI** (external ERI reader); **считыватель ERI** (ERI writer): Считыватель ERI, который не является частью ее встроенного оборудования.

Примечания

1 Внешний считыватель ERI не установлен внутри или снаружи транспортного средства.

2 Есть различие между ближним (DSRC) и удаленными внешними авторами. Считывающее устройство для приближения может быть, например, PCD, с учетом [1]. Внешний считыватель ERI может быть частью придорожного оборудования, ручного оборудования или мобильного оборудования. Удаленная внешняя запись ERI может быть частью бэк-офисного оборудования (BOE).

3.9 **время жизни** (lifetime): Период времени, в течение которого существуют предмет оборудования и его функции.

3.10 **встроенное оборудование ERI** (onboard ERI equipment): Оборудование, установленное внутри или снаружи транспортного средства и используемое для целей ERI.

Примечание — Встроенное оборудование ERI содержит ERT и, возможно, дополнительные устройства связи.

3.11 **встроенный считыватель ERI** (onboard ERI reader): Считыватель ERI является частью ее встроенного оборудования.

Примечание — Встроенный считыватель ERI может быть, например, устройством с бесконтактным соединением (PCD).

3.12 **вызов** (challenge): Элемент данных, выбранный случайным образом и отправленный верификатором заявителю, который используется заявителем в сочетании с секретной информацией, хранящейся заявителем, для генерации ответа, который отправляется верификатору.

Примечание — В настоящем стандарте термин «вызов» используется также в том случае, если ERT не имеет возможности шифрования, и вызов просто копируется без сохранения секретной информации.

3.13

данные ERI (ERI data): Данные идентификации транспортного средства, которые могут быть получены из ERT, состоящей из идентификатора транспортного средства и возможных дополнительных данных транспортного средства.

[ПНСТ 343—2018, пункт 3.4]

3.14 **доверитель** (principal): Объект, чья личность может быть аутентифицирована.

3.15 **домен безопасности** (security domain): Набор элементов, политика безопасности, орган безопасности и набор относящихся к безопасности действий, в которых элементы подчиняются политике безопасности для указанных действий, а политика безопасности администрируется центром безопасности для домена безопасности.

3.16

дополнительные данные транспортного средства (additional vehicle data): Данные электронной регистрации идентификационных данных (ERI) в дополнение к идентификатору транспортного средства.

[ПНСТ 343—2018, пункт 3.1]

3.17 **заявитель** (claimant): Объект, который является или представляет собой принципал для целей аутентификации, включая функции, необходимые для участия в обмене аутентификацией от имени принципала.

3.18 **идентификация** (identification): Действие или акт установления личности.

Примечание — См. также идентификацию транспортного средства.

3.19 **идентификация транспортного средства** (vehicle identification): Действие или акт идентификации транспортного средства.

3.20 **ключ** (key): Последовательность символов, которая управляет работой криптографического преобразования (например, шифрование, дешифрование, вычисление функции криптографической проверки, генерация подписи или проверка подписи).

Примечание — Адаптировано с учетом [2], определение 4.8.

3.21 **ключ системного оператора** (system operator key): Ключ доступа к системному оператору.

3.22 **контроллер** (verifier): Объект, который является или представляет объект, требующий аутентифицированного удостоверения личности.

Примечание — Верификатор включает в себя функции, необходимые для участия в обмене аутентификацией.

3.23 **контроль доступа** (access control): Предотвращение несанкционированного использования ресурса, в том числе несанкционированным образом.

3.24 **конфиденциальность** (confidentiality): Информация не предоставляется или не раскрывается неавторизованным лицам, организациям или процессам.

3.25 **конфиденциальность** (privacy): Право отдельных лиц контролировать или влиять на сбор и хранение информации, связанной с ними, а также на адресную передачу данной информации.

Примечание — Так как этот термин является правом отдельных лиц, его определение может носить субъективный характер, что необходимо учитывать при определенных обстоятельствах.

3.26 **маскарад** (masquarade): Процесс, предваряющий сущность как другую сущность.

3.27 **обнаружение манипуляции** (manipulation detection): Механизм, который используется для определения того, был ли модифицирован блок данных (случайно или преднамеренно).

3.28 **оператор системы ERI** (ERI system operator): Устройство записи ERI, используемое для прямого или косвенного ввода данных ERI в ERT путем вызова транзакций ERI.

Примечание — Если копир ERI обменивается блоками данных протокола ERI непосредственно по каналу передачи данных с ERT, его также называют ERR. Если он обменивается данными через один или несколько узлов, только последний узел в этой последовательности называется ERR. Как следствие внешний писатель ERI может в зависимости от конфигурации на борту действовать не для всех транспортных средств в качестве ERR.

3.29 **орган безопасности** (security authority): Субъект, отвечающий за определение, реализацию или применение политики безопасности.

3.30 **организация регистрации** (registration authority): Организация, ответственная за запись данных ERI и данных безопасности в ERT в соответствии с местным законодательством.

Примечание — Предполагается, что регистрирующий орган в отношении данных ERI может быть одним и тем же органом, ответственным за ведение официального реестра, в котором перечислены транспортное средство, его владелец или арендатор.

3.31 **от конца до конца** (end-to-end encipherment): Шифрование данных внутри или в исходной конечной системе с соответствующим дешифрованием, происходящим только внутри или в конечной системе.

3.32 **открытый текст** (cleartext): Данные, семантическое содержание которых понятно и доступно.

3.33 **отличительный идентификатор** (distinguishing identifier): Информация, которая однозначно отличает сущность объекта.

3.34 **пассивная угроза** (passive threat): Угроза несанкционированного раскрытия информации без изменения состояния системы.

3.35 **порядковый номер** (sequence number): Параметр времени, значение которого соответствует заданной последовательности, которая не повторяется в течение определенного периода времени.

3.36 **расшифровка дешифрования** (decipherment decryption): Разворот соответствующей обратимой шифровки.

3.37 **секретный ключ** (secret key): Ключ, который используется с симметричным криптографическим алгоритмом.

Примечания

1 Владение секретным ключом ограничено (как правило, не более двух объектов).

2 Для ERI в зависимости от политики управления ключами может быть только одна сущность или несколько объектов.

3.38 **системный оператор** (system operator): Организация системного оператора, ответственная за работу системы.

Примечание — В настоящем стандарте системный оператор также выступает в качестве регистрирующего органа и органа безопасности в своей юрисдикции.

3.39 **служба безопасности** (security service): Услуги, предоставляемые на уровне связи открытых систем, что обеспечивает адекватную безопасность систем или передачу данных.

3.40 **случайное число** (random number): Параметр времени, значение которого непредсказуемо.

3.41 **список контроля доступа** (access control list): Список сущностей со своими правами доступа, которым разрешен доступ к ресурсу.

3.42 **угроза** (threat): Потенциальное нарушение безопасности.

3.43 **устройство чтения ERI** (ERI reader): Устройство, используемое для прямого или косвенного считывания данных ERI из ERT путем вызова транзакций ERI.

Примечание — Если считыватель ERI обменивается блоками данных протокола ERI напрямую по каналу передачи данных с ERT, его также называют ERR. Если считыватель ERI обменивается данными через один или несколько узлов, только последний узел в этой последовательности называется ERR. Как следствие внешний считыватель ERI может в зависимости от конфигурации на борту действовать не для всех транспортных средств в качестве ERR.

3.44 **целостность данных** (data intergity): Данные не изменены или уничтожены несанкционированным образом.

3.45 **шифрование** (encipherment encryption): Криптографическое преобразование данных для создания зашифрованного текста.

Примечание — Шифрование может быть необратимым, и в этом случае соответствующий процесс дешифрования не может быть осуществлен.

3.46 **шифрованный текст** (chipertext): Данные, полученные с помощью шифрования, семантическое содержание которых недоступно.

3.47 **электронная регистрационная метка;** ERT (electronic registration tag): Встроенное устройство ERI, которое содержит данные, включая соответствующие внедренные положения безопасности и один или несколько интерфейсов для доступа к этим данным.

Примечания

1 В случае высокой безопасности электронная регистрационная метка (ERT) является типом защищенного прикладного модуля (SAM).

2 ERT может быть отдельным устройством или может быть встроено в бортовое устройство, которое также предоставляет другие возможности (например, DSRC-связь).

3.48 **электронная регистрация идентификационных данных;** ERI (electronic registration identification): Действие или акт идентификации транспортного средства посредством электронных средств.

3.49 **электронный регистратор чтения данных;** ERR (electronic registration reader): Устройство, используемое для чтения или чтения/записи данных из/в электронную регистрационную метку (ERT).

Примечания

1 ERR связывается напрямую, то есть через линию данных OSI, с ERT.

2 ERR также может быть считывателем и/или записывающим устройством ERI либо выступать в качестве ретранслятора в обмене между протоколами ERI, ERT и считывающим устройством ERI.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

AEI — автоматическая идентификация оборудования (Automatic Equipment Identification);

AES — расширенный стандарт шифрования (Advanced Encryption Standard);

ASN.1 — абстрактная синтаксическая ротация (Abstract Syntax Notation One);

AVI — автоматическая идентификация транспортного средства (Automatic Vehicle Identification);

BOE — бэк-офисное оборудование (Back Office Equipment);

DES — стандарт шифрования данных (Data Encryption Standard);

EN — европейский стандарт [Europäische Norm (German), European Standard (English)];

ERI — электронная регистрация идентификационных данных (Electronic Registration Identification);

ERR — электронный регистратор чтения: устройство, используемое для чтения или чтения/записи данных из/в ERT (Electronic Registration Reader);

ERT — электронная регистрационная метка (Electronic Registration Tag);

EU — Европейский Союз (European Union);

IEC — Международная электротехническая комиссия (International Electrotechnical Commission);

ISO — Международная организация по сертификации (International Organization for Standardization);

OBE — бортовое оборудование (Onboard Equipment);

OSI — объединенные открытые системы (Open Systems Interconnection);

PICS — заявления о соответствии реализации протокола(ов) [Protocol Implementation Conformance Statement(s)];

PIN — персональный идентификационный номер (Personal Identification Number);

SAM — защищенный прикладной модуль (Secure Application Module);

Triple-DES — стандарт шифрования с тремя данными (Triple-Data Encryption Standard);

VIN — идентификационный номер транспортного средства (Vehicle Identification Number).

5 Концепция системных коммуникаций

5.1 Общие положения

В настоящем разделе представлено объяснение того, каким образом данные ERI и данные безопасности могут быть считаны или записаны в ERT, а также идентифицированы ТС. Кроме того, описаны варианты, которые могут или не могут быть использованы при фактической реализации. Нормативные требования к интерфейсам приведены в разделе 6 и приложении А. В приложении Б представлена форма для определения ограничений фактической реализации протокола связи.

В настоящем разделе рассмотрены только интерфейсы с использованием методов симметричного шифрования. Симметричные методы шифрования основаны на секретных ключах, которые совместно применяются одним пользователем или сообществом нескольких пользователей. Такое сообщество по сути является закрытой группой пользователей, которой доверены секретные ключи, не раскрывающаяся посторонним лицам.

Предполагается, что пользователи закрытой группы работают в пределах юрисдикции одного оператора системы ERI, ответственного за управление ключами и выступающего в качестве регистрирующего органа в своей юрисдикции.

Общий интерфейс, основанный на асимметричных методах, с различными уровнями безопасности (security) и поддержкой сотрудничества между несколькими (регистрирующими) органами (то есть несколькими доменами безопасности) определен в ПНСТ 344—2018.

5.2 Описание параметров

5.2.1 Идентификация регистрационных параметров транспортного средства

ERI — это действие или акт идентификации ТС с помощью электронных средств для целей, указанных в настоящем стандарте.

Идентификатор, используемый для идентификации ТС, называется идентификатором ТС.

Примечание — Предпочтительным вариантом идентификатора ТС является VIN, который назначается ТС его изготовителем (см. [3]), но также поддерживаются альтернативные варианты (см. ПНСТ 343—2018 для получения подробной информации об идентификаторе ТС и дополнительных данных о ТС).

В настоящем стандарте комбинация практически уникального ТС и уникального номера ERT использована в качестве однозначного отличительного идентификатора.

5.2.2 Концепция системы и поддерживаемые интерфейсы

На рисунке 1 представлены интерфейсы, указанные в данном пункте.

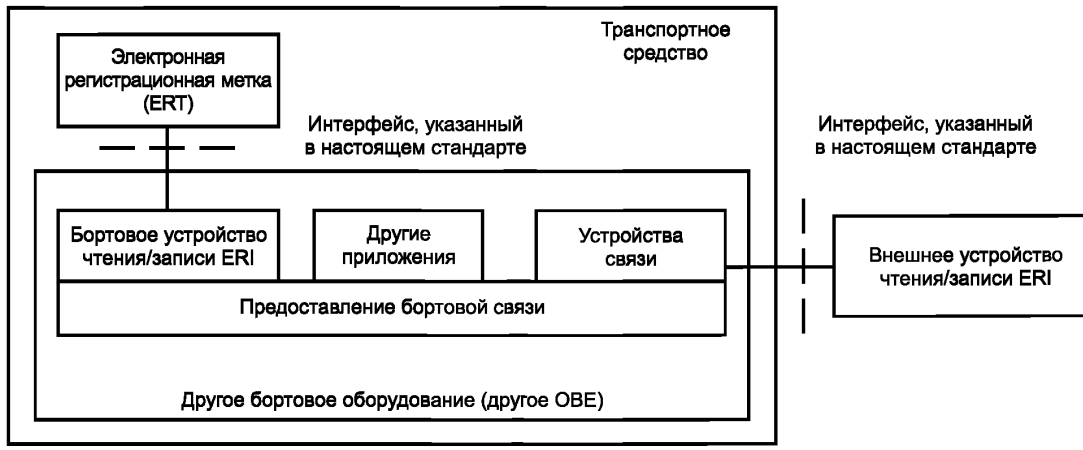

Рисунок 1 — Концепция системы и поддерживаемые интерфейсы

Встроенный компонент, обеспечивающий безопасную среду для данных ERI и данных безопасности, называется электронной регистрационной меткой ERT.

Примечание — Исполнитель может интегрировать другие положения в ERT, если это не ставит под угрозу ее безопасность.

ERT работает в одном из двух режимов:

- неактивированный режим, когда ERT не содержит ключей системного оператора. При работе в ненагруженном режиме фаза аутентификации (см. ниже) не поддерживается, и единственной разрешенной операцией является ввод ERT;
- режим ввода в эксплуатацию, когда системный оператор записал свои ключи в ERT. При работе в режиме ввода в эксплуатацию поддерживается фаза аутентификации (см. ниже).

Системный оператор также может выводить из эксплуатации ERT, т. е. удалить все ключи. Затем ERT возвращается в неактивированный режим, и единственная разрешенная операция — это повторный ввод ERT.

ERT адаптируется к конкретному ТС на одном или нескольких этапах:

- во-первых, ERT настраивается с идентификатором ТС и в необязательном порядке с дополнительными данными ERI. Этот шаг может быть выполнен только один раз в течение жизни ERT;
- во-вторых, системный оператор может регистрировать изменения дополнительных данных ERI (т. е. данные ERI, за исключением идентификатора ТС).

Данные ERI могут быть записаны/обновлены только в режиме ввода в эксплуатацию и только системным оператором.

Предполагается, что все ERT и все встроенные и внешние считыватели и писатели будут частью одного и того же домена безопасности, т. е. в пределах юрисдикции одного системного оператора ERI, ответственного за политику безопасности и ее реализацию, причем системный оператор также действует как регистрирующий орган в своей юрисдикции.

Примечание — Для удовлетворения потребностей различных системных операторов в ERT могут быть включены различные варианты дополнительных данных ERI (подробнее см. ПНСТ 343–2018).

Положения о бортовой связи должны быть способны передавать данные из/в ERT без их изменения.

Примечание — Положения о бортовой связи могут быть, например, частью бортовой платформы для транспортных применений.

Устройство связи может взаимодействовать с устройством считывания/записи ERI на коротких расстояниях или с пультом дистанционного управления бэк-офисным оборудованием (BOE).

Встроенное коммуникационное устройство, внешнее по отношению к ERT, которое взаимодействует с внешним считывающим устройством/считывателем ERI, действует как ретранслятор между этим внешним считывающим устройством/считывателем ERI и встроенным устройством чтения/записи ERI. Устройство связи также может быть использовано для других приложений.

5.2.3 Используемые роли

В контексте настоящего стандарта выделяются следующие роли для физических или юридических лиц:

а) для системного оператора, ответственного за работу системы ERI, также являющегося органом безопасности для домена безопасности ERI и отвечающего за создание секретных ключей, которые будут использованы при проведении аутентификации. Системный оператор также действует как регистрирующий орган, т. е. в качестве органа для записи данных, связанных с ТС, в ERT.

Примечания

1 Ожидается, что регистрирующий орган в отношении данных ERI будет также органом, ведущим регистр, в котором указано ТС.

2 Предположительно каждое ТС указано в регистре, который содержит идентификатор ТС и дополнительные данные, относящиеся к ТС. Неявно предполагается, что этот регистр также идентифицирует тот регистр, который отвечает за ТС (например, его владелец, оператор, хранитель, арендатор и/или водитель);

б) органов власти, которые имеют право (например, в силу действующего законодательства) и уполномочены системным оператором читать данные ERI и зашифрованные записи списка контроля доступа ТС.

Примечание — Роли и требования, связанные со спецификацией, проектированием и производством (включая тестирование) ERT, выходят за рамки настоящего стандарта.

5.2.4 Коммуникационный контекст для чтения

На рисунке 2 представлен контекст связи для чтения данных ERT.

Бортовой или внешний считыватель ERI использован для чтения данных ERT. Встроенное устройство чтения ERI взаимодействует непосредственно с ERT. Внешнее устройство чтения ERI напрямую или косвенно связывается с ERT: непосредственно в случае ручного считывателя или интегрированного устройства ERI либо опосредованно через бортовой модуль связи и встроенный считыватель ERI. Бортовой модуль связи также может быть использован для других приложений.

Сенсорная система (которая выходит за рамки настоящего стандарта) может быть использована для запуска внешнего считывателя ERI, фиксирующего на присутствие ТС.

Различные стороны, которые могут считывать данные ERI из ERT, описаны в 5.3.3; права доступа различных объектов — в 5.3.5.

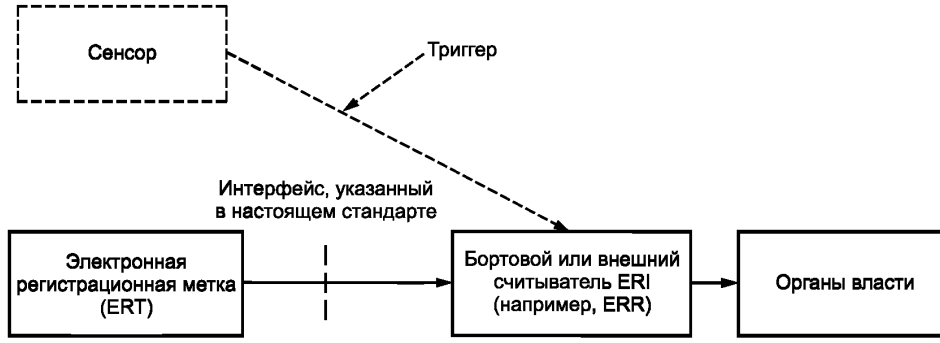

Рисунок 2 — Коммуникационный контекст для чтения из ERT

Оборудование, используемое организацией в офисе (т. е. не на обочине дороги), называется бэк-офисным оборудованием (BOE).

Распределение функций между BOE и внешним считывателем ERI выходит за рамки настоящего стандарта.

5.2.5 Коммуникационный контекст для написания

На рисунке 3 представлен контекст связи для записи данных в ERT.

Бортовая или внешняя запись ERI использована для записи данных в ERT. Встроенный ERI-коммуникатор напрямую взаимодействует с ERT. Внешний ERI-коммуникатор напрямую или косвенно связывается с ERT: непосредственно в случае ручного считывателя или интегрированного устройства ERI или косвенно через встроенный модуль связи и встроенный автор ERI. Бортовой модуль связи также может быть использован для других приложений.

Различные стороны, которые могут записывать данные ERI (безопасность) в ERT, описаны в 5.3.3; права доступа различных объектов — в 5.3.5.

Распределение функций между BOE и внешним устройством ERI выходит за рамки настоящего стандарта. Системный оператор может, например, поручить писателю действовать от его имени или использовать его, к примеру, только как ретранслятор для удаленного письма из своего офиса.

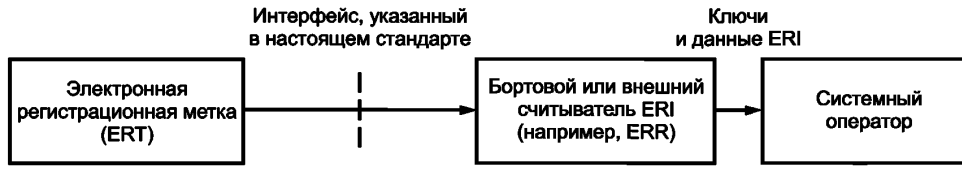

Рисунок 3 — Коммуникационный контекст для записи данных в ERT

5.2.6 Поддерживаемые уровни обслуживания

В настоящем стандарте описана поддержка безопасного взаимодействия с ERT в пределах одной юрисдикции на основе симметричных методов шифрования.

В настоящем стандарте определен более общий интерфейс, основанный на асимметричных методах с различными уровнями безопасности (security) и поддерживающий сотрудничество между несколькими (регистрирующими) органами (например, доменами безопасности).

5.3 Службы безопасности

5.3.1 Предположения

Концепция безопасности обмена данными между ERT и считывателем или автором ERI основана на следующих предположениях:

а) использование ERT может быть обязательным, и, следовательно, ERT должна быть устойчивой к угрозам мошенничества. Используя терминологию (см. [4]), ERT должна быть устойчивой к активным угрозам (например, изменение сообщений, их воспроизведение, вставка ложных сообщений и маскировка);

б) чтение ERT должно быть пригодным в качестве юридического доказательства;

в) у ERI должна быть возможность обеспечить высокий уровень защиты частной жизни (т. е. не может быть легкое отслеживание местонахождения ТС и, следовательно, его водителя); следовательно, ERT также должна быть устойчивой к пассивным угрозам;

г) у ERI должна быть возможность предусмотреть меры защиты, для того чтобы предотвратить использование ERI для запуска атаки на ТС;

д) эффективность механизмов безопасности должна быть достижимой в течение времени, доступного для взаимодействия до тех пор, пока ТС движется.

Пример — Чтение ТС со скоростью 180 км/ч в пределах диапазона считывания 10 м должно быть достигнуто в течение 200 мс.

5.3.2 Аутентификация объекта при чтении данных ERI

Доверие к подлинности чтения ERI зависит от следующих аспектов аутентификации, которые должны быть полностью выполнены, для того чтобы полностью доверять чтению:

а) ERT настраивают с правильным идентификатором ТС и прикрепляют к правильному ТС;

б) ERT не может быть удалена из ТС, не делая ее неработоспособной;

в) данные ERI считываются из подлинного ERT, т. е. из законного устройства (это нереплицированное сообщение от поддельного устройства);

г) данные ERI правильно считываются из ERT (целостность данных, обнаружение манипуляций). Это достигается стандартными механизмами, используемыми при передаче данных и в качестве побочного эффекта путем шифрования данных ERI (значение дешифрования поврежденного зашифрованного текста ничтожно);

д) когда данные ERI правильно прочитаны из подлинного ERT по конкретному запросу, впоследствии будет сложно оспаривать, что эти данные не прочитаны из этого компонента по этому запросу, что достигается путем шифрования данных ERI вместе с кодом вызова, предоставляемым считывателем ERI.

Примечания

1 Требования настоящего стандарта относятся к положениям, приведенным в перечислениях в)—д). Условия, приведенные в перечислениях а) и в), указаны в ПНСТ 342—2018.

2 Использование технической терминологии (см. [5]), приведенное в перечислениях в) и г), поддерживается с использованием двухстороннего механизма взаимной аутентификации с однонаправленными ключами. Единственность/своевременность контролируется созданием и проверкой случайных чисел и порядковых номеров.

5.3.3 Конфиденциальность при чтении данных ERI

Настоящий стандарт поддерживает конфиденциальность, предоставляя данные ERI в зашифрованном тексте. Зашифрованные данные ERI затем могут находиться в свободном доступе, но расшифровать и интерпретировать их могут только уполномоченные лица/оборудование (сквозная шифровка).

Для того чтобы защитить зашифрованные данные ERI, можно использовать в качестве псевдонима последовательность или случайное число, которые можно добавить к данным ERI до шифрования.

Конфиденциальность требуется только для чтения данных ERI из ERT, а не для записи данных в ERT.

5.3.4 Ключи для аутентификации и конфиденциальности

Тот же секретный ключ используется как для аутентификации, так и для конфиденциальности.

Транспортное средство может быть зарегистрировано в течение многих лет, и на протяжении этого времени другие ТС регистрируются и снимаются с учета. Как следствие, системный оператор должен либо иметь всегда одни и те же ключи, либо использовать разные ключи для различных ТС; для того чтобы поддерживать этот последний параметр, ключ можно идентифицировать с помощью идентификатора ключа. Как ERT, так и ERI-считыватель/писатель могут использовать несколько ключей.

Для того чтобы осуществлялось взаимодействие ERT с одним или несколькими ключами и считывателями/писателями ERI с одним или несколькими ключами, используется следующая процедура:

а) если считывататель/писатель ERI хочет выбрать ключ ERT, он отправляет списку ERT форму номера ключей, которую ERT может выбрать для своих ответов;

б) если ERT имеет один из запрошенных ключей, она использует один из них. Если ERT не содержит запрошенный ключ, но имеет один или несколько других ключей, она может выбрать любой ключ, который имеет для своих ответов. Если в ERT отсутствует ключ, она просто не использует ни одной клавиши;

в) если ERT хочет выбрать ключ считывания/записи ERI, она отправляет считывателю/писателю список номеров клавиш, используя которые можно выбрать ответы;

г) если считыватель/писатель ERI имеет один из запрошенных ключей, он использует один из них; если не имеет, — считыватель/писатель использует для своих ответов тот же ключ, который используется ERT в ее запросе.

5.3.5 Контроль доступа к данным ERI

Контроль доступа невозможен, если по крайней мере один ключ не загружен в ERT.

Если один или несколько ключей загружены в ERT, управление доступом основано на взаимной процедуре аутентификации с использованием однонаправленных секретных ключей.

Есть две группы ключей: одна для системных операторов и одна для органов власти.

Ключ системного оператора обеспечивает полный доступ для чтения и записи как к данным ERI, так и к данным безопасности.

Ключ полномочий предоставляет доступ только для чтения:

а) к данным ERI: идентификатор ТС и дополнительные данные ТС;

б) историческим данным, при их наличии;

в) записям списка контроля доступа (см. ниже) в зашифрованном тексте, которые могут быть дешифрованы системным оператором.

5.4 Описание архитектуры связи

5.4.1 Общая концепция коммуникации для идентификации транспортных средств

На рисунке 4 представлена концепция связи для идентификации ТС.

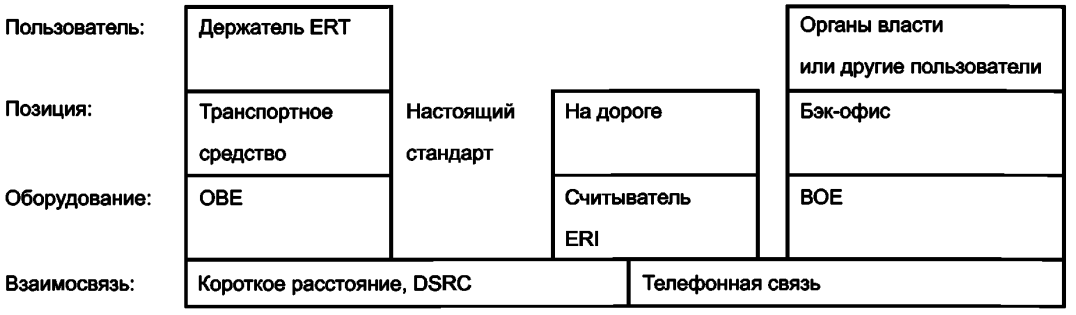

Рисунок 4 — Общая концепция местной связи для идентификации

В настоящем стандарте изложена информация относительно воздушного интерфейса между бортовым оборудованием ERI в ТС и кратковременным внешним считывателем ERI.

Примечание — Транспортное средство, внешний интерфейс, считыватель ERI соответствуют эталонной точке DELTA; внешний интерфейс считывателя ERI бэк-офиса — эталонной точке ALPHA (см. [6]).

Интерфейс между внешним считывающим устройством ERI и оборудованием BOE выходит за рамки настоящего стандарта. Это может быть использовано, например, для ввода в эксплуатацию считывателя ERI, обмена белыми или черными списками и/или загрузки результатов чтения, будучи, например, локальным интерфейсом в бэк-офисе или в широкополосном сетевом интерфейсе.

5.4.2 Общая концепция связи для удаленного доступа

В настоящем стандарте также уделено внимание поддержке удаленного доступа к ERT. Системный оператор может, например, использовать удаленный доступ в случае его реализации для проверки или обновления дополнительных данных ERI или данных безопасности.

На рисунке 5 представлена концепция связи для удаленного доступа к ERT ТС.

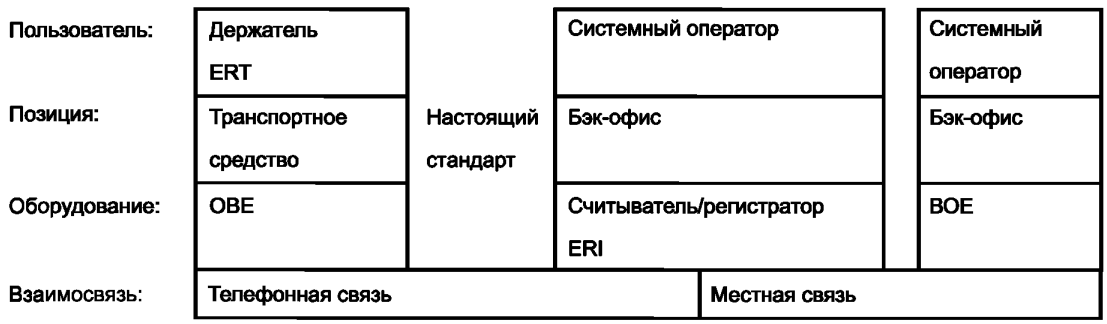

Рисунок 5 — Общая концепция коммуникации для удаленного доступа

В настоящем стандарте описан сетевой интерфейс между бортовым оборудованием ERI в ТС и дистанционным внешним устройством чтения/записи ERI.

Примечание — Независимо от того, реализованы ли возможности удаленного доступа, их описание выходят за рамки настоящего стандарта.

5.4.2.1 Бортовая связь

На рисунке 6 представлен абстрактный обзор возможной архитектуры бортовой связи.

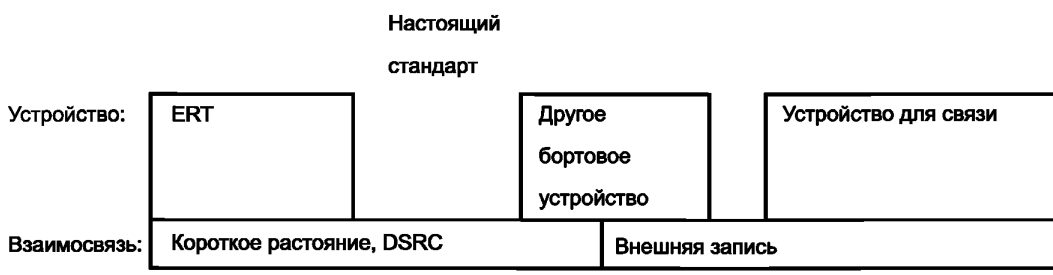

Рисунок 6 — Архитектура бортовой связи

Примечание — ERT и устройство связи могут быть отдельными компонентами. Это может или не может иметь место для конкретной реализации.

5.5 Интерфейсы

5.5.1 Ближний радиоинтерфейс

При взаимодействии бортового оборудования ERI и внешнего считывателя/записывающего устройства ERI на коротких расстояниях использован стек протоколов, как показано на рисунке 7.

AVI (приведено в [4], плюс дополнительные услуги)
Уровень ERI (добавление служб безопасности ERI и управления ими)
Прикладной уровень или аналогичный уровень
Нижний слой

Рисунок 7 — Беспроводной стек протокол

Взаимосвязь между этими слоями и опорными точками BETA-ZETA (см. приложение A [6]) изображено на рисунке 8 (контрольная точка ALPHA расположена между считывающим устройством ERI и оборудованием BOE).

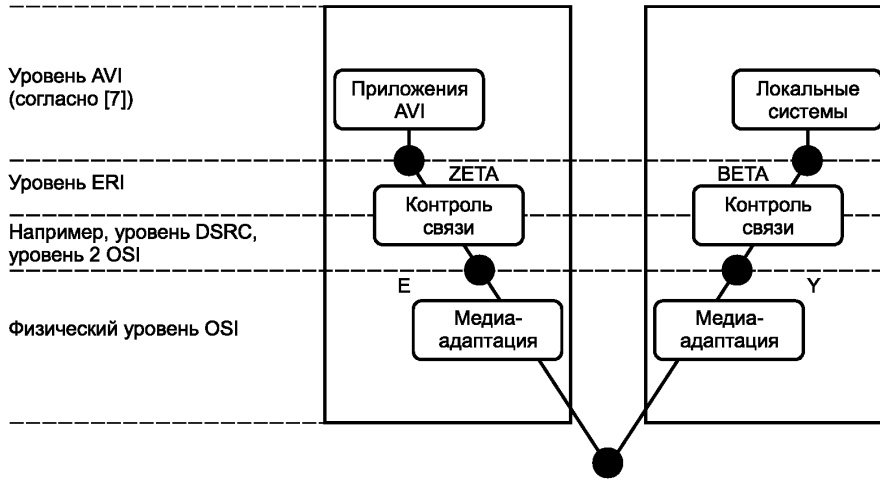

Рисунок 8 — Расположение уровня ERI в эталонной архитектуре (см. [6])

5.5.2 Встроенный интерфейс с ERT

При взаимосвязи между ERT и бортовым считывателем/записывающим устройством ERI использован стек протоколов, как показано на рисунке 9.

AVI (плюс дополнительные услуги)
Уровень ERI (добавление служб безопасности ERI и управления ими)
Уровень передачи (см. [8])
Нижние слои (см. [8], [9])

Рисунок 9

6 Требования к интерфейсу

6.1 Описание интерфейса

В настоящем разделе определен интерфейс для доступа к данным ERI в ERT и представлены следующие подразделы:

- 6.2, в котором приведено абстрактное определение;
- 6.3, в котором определен бортовой интерфейс с ERT;
- 6.4, в котором определен ближний воздушный интерфейс между бортовым оборудованием ERI и внешним устройством чтения/записи ERI;
- 6.5, в котором определен интерфейс для удаленного доступа.

Бортовой интерфейс определяется как реализация абстрактных определений, приведенных в 6.2.

Внешние интерфейсы, как определено в 6.4 и 6.5, используются либо для непосредственного общения с ERT, если положения бортовой связи интегрированы в ERT, либо косвенно для передачи блоков данных протокола ERI на бортовой считыватель/запись ERI (см. рисунок 1).

6.2 Абстрактные определения транзакций

6.2.1 Обзор транзакций

В таблице 1 перечислены обязательные и необязательные транзакции.

Таблица 1 — Обязательные и необязательные транзакции

Подраздел	Транзакция	Req	Описание
6.2.4	mutualAuthenticate1	R	Требования для взаимной аутентификации
6.2.5	mutualAuthenticate2	R	Требования для взаимной аутентификации
6.2.6	getSecretKeyEriData	R	Для ERI со стороны органов власти или системного оператора
6.2.7	setSecretKeyEriData	R	Для настройки ERT и дополнительного обновления данных ERI системным оператором
6.2.8	commissionSecretKeyErt	A, C	Для загрузки системным оператором своих данных симметричного ключа ERT
6.2.9	decommissionSecretKeyErt	O	Для удаления ключей системного оператора
6.2.10	updateAccessControlList	A, C	Для добавления или удаления полномочия в/из списка управления доступом ERT
6.2.11	getCiphertextAccessControl ListEntry	O	Для получения записи списка управления доступом в тексте шифрования органом власти или системным оператором
6.2.12	endOfSession	R	Для указания конца сеанса ERI.
Примечание — Столбец, озаглавленный «Req», указывает на следующее: требуется ли всегда транзакция (R), требуемая для конфиденциальности (C), необходимая для аутентификации (A) или необязательная (O).			

6.2.2 Фазы сеанса

Взаимодействие с ERT ориентировано на сеанс. Полный сеанс состоит из последовательности следующих фаз:

а) фазы взаимной аутентификации, которая обеспечивает взаимную аутентификацию считывателя/записи ERI и ERT, если ERT находится в режиме ввода в эксплуатацию. На этом этапе последовательно выполняются транзакции взаимного подтверждения и взаимной аутентификации. Если ERT находится в неактивном режиме, фаза взаимной аутентификации пропускается;

б) фазы обмена данными, которая запускается непосредственно для ERI в неактивном режиме и для ERT, является режимом ввода в эксплуатацию после успешной взаимной аутентификации. На этапе обмена данными данные ERI или данные безопасности обмениваются между считывателем/записывающим устройством ERI и ERT. На этом этапе транзакции обмена данными данные могут быть вызваны в любом порядке;

в) этап освобождения сеанса, который завершает сеанс.

В случае ошибки и если не указано иное, сеанс прекращается без дальнейшего уведомления.

6.2.3 Операции ERI и блоки данных протокола

6.2.3.1 Концепция транзакции

Запись и чтение данных в/из ERT достигаются посредством транзакций, которые определяются как экземпляры класса информационных объектов TRANSACTION.

Класс информационных объектов TRANSACTION определен следующим образом:

```
TRANSACTION ::= CLASS {
&ArgumentType                   ,
&ResultType                     ,
&transactionCode                INTEGER UNIQUE
}
WITH SYNTAX {
ARGUMENT                        &ArgumentType
RESULT                          &ResultType
                                &transactionCode
CODE  }
```

Сделка должна быть вызвана считывателем ERI, создателем ERI и выполнена ERT.

Никакая транзакция не должна вызываться встроенным устройством чтения/записи ERT, в то время как ERT все еще выполняет другую транзакцию.

Поле &ArgumentType должно указывать тип данных аргумента транзакции. Если его исключить, транзакция не принимает значения аргумента.

Поле &ResultType должно указывать тип данных возвращаемого значения с результатом транзакции.

Поле &transactionCode указывает целочисленное значение, которое используется для идентификации транзакции, например, когда он должен быть вызван.

6.2.3.2 Единицы данных протокола ERI

Блоки данных протокола ERI (PDU) определены следующим образом:

```
SecretKeyEriPdu ::= CHOICE {
requestPdu                      SecretKeyEriReqPdu,
reponsePdu                      SecretKeyEriRspPdu
}

SecretKeyEriReqPdu ::= SEQUENCE {
transactCode            TRANSACTION.&transactionCode ({SecretKeyEriTransactions}),
argument                    TRANSACTION.&ArgumentType
                            ({SecretKeyEriTransactions} {@.transactCode}) OPTIONAL
}

SecretKeyEriRspPdu ::= SEQUENCE {
transactCode            TRANSACTION.&transactionCode ({SecretKeyEriTransactions}),
result                      TRANSACTION.&ResultType
 ({SecretKeyEriTransactions} {@.transactCode})
}

SecretKeyEriTransactions TRANSACTION ::= { mutualAuthentication1
| mutualAuthentication2 |   getSecretKeyEriData | setSecretKeyEriData |
commisionSecretKeyErt | decommisionSecretKeyErt |
updateAccessControlList | getCipertextAccessControlListEntry | endOfSession
}
```

Секция протокола секретных ключей ERI имеет тип SecretKeyEriPdu и либо SecretKeyEriReqPdu, либо SecretKeyEriRspPdu.

Секция протокола данных SecretKeyEriReqPdu используется для вызова транзакции, выполняемой ERT.

Блок данных протокола SecretKeyEriRspPdu используется для результата транзакции, выполняемой ERT.

SecretKeyEriTransactions задает набор транзакций ERI.

Компонент transactCode должен содержать значение кода транзакции для транзакции в установленном EriTransactions.

Компонент аргумента, при его наличии, должен быть того же типа, который указан для аргумента транзакции, идентифицируемой значением transactCode.

Компонент аргумента должен присутствовать, если аргумент для транзакции определен, и отсутствовать, если аргумент не определен.

Компонент результата должен быть того же типа, что и для результата транзакции, идентифицированного значением transactCode.

6.2.4 Взаимная аутентификация 1

6.2.4.1 Определение услуги

Транзакция mutualAuthentication1 является первой транзакцией, которая будет использована на этапе взаимной аутентификации.

Транзакция взаимной аутентификации 1 вызывается считывателем/записью ERI и выполняется ERT, работающей в режиме ввода в эксплуатацию.

Если ERT работает в неактивированном режиме, т. е. еще не содержит ключа, транзакция игнорируется и ответ не создается.

6.2.4.2 Спецификация протокола

Операция взаимной аутентификации определена следующим образом:

```
        mutualAuthentication1 TRANSACTION ::= {
        ARGUMENT OCTET STRING RESULT OCTET
STRING
        CODE   1
        }
```

OCTET STRING используется как для аргумента, так и для результата транзакции.

6.2.5 Взаимная аутентификация 2

6.2.5.1 Определение услуги

Транзакция mutualAuthentication2 является второй и последней транзакцией, которая будет использована на этапе взаимной аутентификации.

Совместная транзакция взаимной аутентификации 2 вызывается считывателем/писателем ERI после получения удовлетворительного ответа на ее транзакцию взаимной аутентификации.

Ответ на транзакцию mutualAuthentication1 является только удовлетворительным, если он содержит вызов ERT, зашифрованный с помощью правильного секретного ключа.

Транзакция используется вызывающим считывателем ERI/записывающим устройством, для того чтобы сигнализировать ERT о том, что он принял аутентификацию ERT, и ответить на запрос аутентификации от ERT.

Транзакция mutualAuthentication2 выполняется ERT, и ответ отправляется только в том случае, если запрос от считывателя/записи ERI был удовлетворительным. Если ответ неудовлетворительный, ERT не отправляет ответ.

Запрос от считывателя/записи ERI является только удовлетворительным, если он содержит вызов читателя/писателя, зашифрованный с помощью правильного секретного ключа.

6.2.5.2 Спецификация протокола

Операция взаимной аутентификации определена следующим образом:

```
        mutualAuthentication2 TRANSACTION ::= {
        ARGUMENT OCTET STRING RESULT OCTET
STRING
        CODE   2
        }
```

OCTET STRING используется как для аргумента, так и для результата транзакции.

6.2.6 Получение данных секретного ключа ERI

6.2.6.1 Определение услуги

Для получения данных ERI из ERT следует использовать транзакцию данных секретного ключа ERI.

Получение транзакции данных секретного ключа ERI должно быть вызвано только на этапе обмена данными и выполнено только ERT в тот момент, когда она настроена и находится в режиме ввода в эксплуатацию.

Если транзакция не вызывается на этапе обмена данными или ERT не настроена либо не активирована, вызов должен быть проигнорирован, транзакция не должна выполняться, и результат не будет получен (см. таблицу 2).

Таблица 2 — Получение параметров транзакции данных секретного ключа ERI

Параметр	Запрос	Ответ	Примечание
Аргумент	O	—	В открытом или зашифрованном виде
Данные ERI	—	M	В открытом зашифрованном тексте
Примечание — M — параметр является обязательным; O — параметр не является обязательным.			

6.2.6.2 Первоначальный запрос

Запрос содержит операцию, которая должна быть записана в ERT в открытом или в зашифрованном тексте.

6.2.6.3 Ответный примитив

Ответ содержит данные ERI, хранящиеся в открытом тексте ERT или в зашифрованном тексте.

6.2.6.4 Спецификация протокола

Получение транзакции данных секретного ключа ERI определяется следующим образом:

```
getSecretKeyEriData TRANSACTION ::= {
ARGUMENT OCTET STRING RESULT OCTET STRING
CODE   3
}
```

OCTET STRING используется как для аргумента, так и для зашифрованного результата транзакции.

6.2.7 Установление данных ERI секретного ключа

6.2.7.1 Определение услуги

Сетчатый секретный ключ данных ERI должен быть использован для записи данных ERI в ERT.

Сетчатая транзакция данных секретного ключа ERI должна быть вызвана только на фазе обмена данными и выполнена только ERT в тот момент, когда она находится в режиме ввода в эксплуатацию.

Если транзакция не вызывается на этапе обмена данными или ERT находится в режиме без оплаты, вызов игнорируется, транзакция не должна выполняться, и результат не будет получен (см. таблицу 3).

Таблица 3 — Установка параметров транзакции данных секретного ключа ERI

Параметр	Запрос	Ответ	Примечание
Данные ERI	M	—	В открытом или зашифрованном виде
Результат	—	M	—
Примечание — M — параметр является обязательным.			

6.2.7.2 Первоначальный запрос

Запрос содержит данные ERI, которые должны быть записаны в ERT в открытом или в зашифрованном тексте. Новые данные ERI полностью заменят старые данные ERI.

6.2.7.3 Ответный примитив

Ответ используется для указания результата выполненной транзакции.

6.2.7.4 Спецификация протокола

Сетчатая транзакция данных секретного ключа ERI определена следующим образом:

```
setSecretKeyEriData TRANSACTION ::= {
ARGUMENT OCTET STRING RESULT OCTET STRING
        CODE                4
        }
```

OCTET STRING используется как для аргумента, так и для результата транзакции.

6.2.8 Ввод в эксплуатацию секретного ключа ERT

6.2.8.1 Определение услуги

Сделка ввода в эксплуатацию должна быть использована для ввода в эксплуатацию ERT или обновления параметров безопасности ERT.

Данные безопасности, введенные или обновленные с помощью этой транзакции, состоят из ключей доступа для системного оператора и идентификаторов ключей, связанных с этими ключами.

Сделка по вводу в эксплуатацию должна быть использована только на этапе обмена данными.

Если транзакция не вызывается на этапе обмена данными, вызов игнорируется, транзакция не должна выполняться, и результат не будет получен (см. таблицу 4).

После успешной транзакции с помощью ERT, ERT находится в режиме ввода в эксплуатацию (см. таблицу 4).

Таблица 4 — Ввод в эксплуатацию секретных ключей параметров транзакции ERT

Параметр	Запрос	Ответ	Примечание
Поручительные данные	M	—	В открытом или зашифрованном виде
Результат	—	M	—
Примечание — M — параметр является обязательным.			

6.2.8.2 Первоначальный запрос

Запрос содержит данные безопасности, которые должны быть записаны в ERT в зашифрованном тексте.

Новые данные безопасности полностью заменят старые данные ERI.

6.2.8.3 Первоначальный ответ

Ответ используется для указания результата транзакции ввода в эксплуатацию.

6.2.8.4 Спецификация протокола

Сделка секретного ключа ввода в эксплуатацию определяется следующим образом:

```
commissionSecretKeyErt TRANSACTION ::= {
ARGUMENT OCTET STRING RESULT OCTET STRING
        CODE                5
        }
```

OCTET STRING используется как для аргумента, так и для результата транзакции.

6.2.9 Секретный ключ снятия с эксплуатации ERT

6.2.9.1 Определение услуги

Операция снятия с эксплуатации должна быть использована для вывода из эксплуатации ERT, т. е. для удаления параметров безопасности ERT и списка контроля доступа.

Операция снятия с эксплуатации должна быть использована только на этапе обмена данными.

Если транзакция не вызывается на фазе обмена данными, вызов игнорируется, транзакция не должна выполняться, и результат не будет получен.

После успешной транзакции с помощью ERT, ERT находится в неактивном режиме (см. таблицу 5).

Таблица 5 — Параметры транзакции секретного ключа деблокирования ERP

Параметр	Запрос	Ответ	Примечание
Аргумент			
Результат			
Примечание — Пусто — параметр не используется.			

6.2.9.2 Первоначальный запрос

Запрос не содержит данных.

6.2.9.3 Ответный примитив

Ответ не содержит данных.

6.2.9.4 Спецификация протокола

Сделка секретного ключа ERT по снятию с эксплуатации определяется следующим образом:

```
decommissionSecretKeyErt TRANSACTION ::= {
        ARGUMENT      NULL
        RESULT        NULL
        CODE          6
        }
```

Значение NULL используется как для аргумента, так и для результата транзакции.

6.2.10 Обновление списка управления доступом

6.2.10.1 Определение услуги

Транзакция updateAccessControlList должна быть использована для добавления или удаления записей из списка управления доступом ERT.

Список управления доступом содержит ключи и связанные с ними идентификаторы ключей для полномочий.

Транзакция должна быть вызвана только на этапе обмена данными и выполнена только ERT в тот момент, когда она находится в режиме ввода в эксплуатацию.

Если транзакция не вызывается на этапе обмена данными или ERT находится в режиме без оплаты, вызов игнорируется, транзакция не должна выполняться, и результат не будет получен (см. таблицу 6).

Таблица 6 — Обновление параметров транзакций списка контроля доступа

Параметр	Запрос	Ответ	Примечание
Аргумент	M	—	В зашифрованном виде
Результат	—	M	—
Примечание — M — параметр является обязательным.			

6.2.10.2 Первоначальный запрос

В случае добавления ключа запрос содержит ключ доступа для органа и связанный с ним ключевой идентификатор.

В случае добавления ключа и списка управления доступом запрос уже содержит ключ с тем же ключевым идентификатором, поэтому старый ключ заменяется новым.

Если ключ должен быть удален, запрос содержит идентификатор ключа, связанный с этим ключом.

6.2.10.3 Ответный примитив

Ответ используется для указания результата транзакции списка управления доступом к обновлению.

6.2.10.4 Спецификация протокола

Операция updateAccessControlList определена следующим образом:

```
        updateAccessControlList TRANSACTION ::= {
        ARGUMENT OCTET STRING RESULT OCTET
STRING
                CODE   7
                }
```

OCTET STRING используется как для аргумента, так и для результата транзакции.

6.2.11 Получение списка записей контроля зашифрованного текста

6.2.11.1 Определение услуги

Операция getCiphertextAccessControlListEntry должна быть использована для извлечения записи списка управления доступом в зашифрованном тексте из ERT.

Транзакция должна быть вызвана только на этапе обмена данными и выполнена только ERT в тот момент, когда он находится в режиме ввода в эксплуатацию.

Если транзакция не вызывается на этапе обмена данными или ERT находится в режиме без уплаты, вызов игнорируется, транзакция не должна выполняться, и результат не будет получен (см. таблицу 7).

Таблица 7 — Получение параметров транзакции списка контроля зашифрованного текста

Параметр	Запрос	Ответ	Примечание
Аргумент	M	—	В зашифрованном виде
Результат	—	M	—
Примечание — M — параметр является обязательным.			

6.2.11.2 Первоначальный запрос

Запрос содержит номер записи списка управления доступом, из которого должен быть возвращен ключ и связанный с ним идентификатор ключа.

6.2.11.3 Ответный примитив

Ответ должен содержать ключ и связанный с ним ключевой идентификатор, формирующий запись в списке управления доступом, как указано в запросе.

6.2.11.4 Спецификация протокола

Операция getCiphertextAccessControlListEntry определена следующим образом:

```
        getCiphertextAccessControlListEntry TRANSACTION
::= {
        ARGUMENT OCTET STRING RESULT OCTET
STRING
                CODE   8
                }
```

OCTET STRING используется как для аргумента, так и для результата транзакции.

6.2.12 Окончание сессии

6.2.12.1 Определение услуги

Конец сеансовой транзакции должен быть использован для сигнализации окончания сеанса.

Конец сеансовой транзакции должен быть вызван только на этапе обмена данными, и после вызова сеанс переходит к фазе освобождения сеанса (см. таблицу 8).

Таблица 8 — Параметры транзакции конца сеанса

Параметр	Запрос	Ответ	Примечание
Аргумент	O	—	В открытом или зашифрованном виде
Примечание — O — параметр является необязательным.			

6.2.12.2 Первоначальный запрос

Запрос содержит операцию, которая должна быть записана в ERT в открытом или в зашифрованном тексте и используется для сигнализации окончания сеанса между ERT и считывателем/записью ERI.

6.2.12.3 Ответный примитив

Ответ не несет никакой ценности. Он используется только для подтверждения окончания сеанса.

6.2.12.4 Спецификация протокола

Конец транзакции сеанса определен следующим образом:

```
endOfSession TRANSACTION ::= {
    ARGUMENT                    OCTET STRING
    RESULT                      NULL
    CODE    }                   9
```

В транзакции использованы аргумент OCTET STRING для аргумента и значение NULL для его результата.

6.3 Бортовой интерфейс к ERT

6.3.1 Общие требования к интерфейсу к ERT

Идентификатор ERI и идентификатор чипа могут быть доступны только в соответствии с условиями настоящего стандарта.

Блоки данных протокола прикладного уровня, подлежащие обмену с ERT, должны быть блоком данных протокола ERI типа SecretKeyEriPdu, т. е. типа SecretKeyEriReqPdu или типа SecretKeyEriRspPdu.

Блок данных протокола ERI должен быть закодирован в соответствии с каноническим вариантом стандартного варианта кодирования (PER) (CANONICAL-PER) ALIGNED.

Примечания

1 При необходимости блок данных протокола ERI может быть сегментирован и повторно собран (см. [3]).

2 Не допускаются столкновения между бортовым считывателем или записывающим устройством и считывающим устройством (ручным). При необходимости другое бортовое оборудование ERI должно быть отключено в тот момент, когда используется ручное считывающее устройство ERI или устройство записи.

6.3.2 Интерфейс

Если интерфейс с ERT, интерфейс между ERT и бортовым считывателем/считывателем ERI должен соответствовать определенным требованиям (см. [8]):

- ERT действует как PICC (бесконтактная интегральная плата) типа A или B;
- встроенный считыватель/считыватель ERI действует как PCD (устройство с бесконтактным соединением), поддерживающее оба типа A и B.

Блок данных протокола ERI должен быть напрямую передан с использованием поля INF одного из нескольких I-блоков (см. [1]).

Блок данных протокола ERI не должен быть упакован в модули данных протокола прикладных протоколов (см. [8]).

Сегментация и повторная сборка блока данных протокола ERI должны быть выполнены, если требуется, с цепью (см. [8]).

6.4 Интерфейс ближнего радиоизлучения

6.4.1 Общие требования к воздушному интерфейсу ближнего радиуса действия

Ближний радиоинтерфейс должен быть способен обмениваться блоками протокола данных ERI типа SecretKeyEriPdu и кодироваться в соответствии с каноническим вариантом PER (CANONICAL-PER) ALIGNED.

Протоколы нижнего уровня (сеанс и ниже, если применимо) должны соответствовать применимым международным стандартам.

Примечание — При необходимости блок данных протокола ERI может быть сегментирован и повторно собран (см. [10]).

6.4.2 Использование протокола уровня приложения DRSC

6.4.2.1 Общие положения

Если для транзакций ERI используется протокол уровня приложения DSRC, то применяется, как указано в этом пункте.

Примечание — Это делает интерфейс ERI DSRC совместимым с другими интерфейсами приложений DSRC (см. [11]).

6.4.2.2 Использование службы инициализации DSRC

Когда DSRC-связь применяется для транзакций ERI, служба инициализации должна быть использована следующим образом:

а) либо компонент mandApplications, либо компонент nonmandApplications T-PDU запроса инициализации (таблица обслуживания маяков, BST) должен содержать компонент приложения ERI;

б) компонент приложений T-PDU с инициализацией-ответом (таблица обслуживания TC, VST) должен содержать компонент приложения ERI;

в) значение компонента приложения ERI в запросе инициализации или инициализации-ответа должно быть следующим:

1) вспомогательный компонент должен иметь значение «идентификация автоматизированного TC»,

2) компонент eid может быть опущен и, при его наличии, должен быть проигнорирован приложением ERI,

3) компонент параметра может быть опущен или содержать необходимые данные (например, данные аутентификации).

Примечания

1 Обозначение приложения как обязательное или необязательное и его положение в списке приложений выходят за рамки настоящего стандарта. Оно влияет только на приоритет приложения ERI по отношению к другим приложениям, указанным в BST (см. 7.3.2).

2 Однако компонент eid и компонент параметров могут быть использованы для других приложений без ERI, AVI.

6.4.2.3 Использование запроса на действие DSRC

Запрос транзакции ERI отправляется из считывателя/записи ERI во встроенный блок DSRC в качестве запроса действия следующим образом:

а) значение компонента режима должно быть TRUE (т. к. все транзакции ERI подтверждены);

б) значение компонента eid должно быть 0;

в) значение компонента actionType должно быть секретным KeyEriTransaction << для регистрации с NEN >>;

г) компонент accessCredentials не должен присутствовать;

д) значение компонента accessParameter передается как принятое в ERT значение secretKeyEriReqPdu;

е) компонент iid не должен присутствовать.

Примечание — Запрос-запрос должен иметь тип Action-Request, который определен следующим образом:

```
Action-Request ::= SEQUENCE {
        mode                    BOOLEAN,
        eid                     Dsrc-EID,
        action                  Type ActionType,
        accessCredentials       OCTET STRING (SIZE (0..127,...)) OPTIONAL,
        actionParameter         Container OPTIONAL,
        iid                     Dsrc-EID OPTIONAL
        }
(end of note)
```

6.4.2.4 Использование ответного действия DSRC

Ответ транзакции ERI, полученный от ERT, отправляется встроенным блоком DSRC во внешний считыватель ERI в качестве ответа следующим образом:

а) значение компонента eid должно быть 0;

б) компонент iid не должен присутствовать;

в) значение компонента responseParameter должно быть значением secretKeyEriRspPdu, полученным от ERT;

г) компонент ret может быть опущен и, при его наличии, должен быть проигнорирован, когда также присутствует secretKeyEriRspPdu.

Примечание — Реакция на действие должна быть по типу Action-Response, которая определена в следующим образом:

```
Action-Response ::= SEQUENCE {
        Fill                    BIT STRING (SIZE(1)),
        eid                     Dsrc-EID,
        iid                     Dsrc-EID OPTIONAL,
        responseParameter       Container OPTIONAL,
        ret                     ReturnStatus OPTIONAL
        }
(end of note)
```

Если устройство DSRC не способно передавать секретный ключ KeyEriReqPdu в ERT, в придорожный блок возвращается содержащий компонент ret типа ReturnStatus.

Примечание — Механизмы, которые будут использованы для передачи SecretKeyEriReqPdu от устройства DSRC к устройству ERI, выходят за рамки настоящего стандарта. Предполагается, что появится общая бортовая платформа или сеть, которые могут быть использованы для этой цели. Тем временем изготовителю устройства DSRC, возможно, придется справляться с различными средствами для подключения своего устройства DSRC к бортовому считывателю/записывающему устройству ERI.

6.4.3 Нижние слои

Уровень применения DSRC должен использовать нижние слои.

6.5 Интерфейс удаленного доступа

Интерфейс удаленного доступа должен быть способен обмениваться блоками протокола данных ERI типа SecretKeyEriPdu и кодироваться в соответствии с правилами PER.

Бортовое устройство, предоставляющее удаленный доступ к ERT, должно обеспечивать передачу блоков данных протокола ERI, полученных от одноранговой сети (сотовой сети), в ERT и обратно.

Протоколы нижнего уровня (сотовая сеть) (сеанс и ниже, если применимо) должны соответствовать применимым международным стандартам.

Примечание — При необходимости блок данных протокола ERI может быть сегментирован и повторно собран (см. [7]).

Приложение А
(обязательное)

ASN.1. Определения модулей

А.1 Обзор

Это приложение содержит следующие модули ASN.1:
а) модуль транзакций секретного ключа;
б) уменьшенный модуль для того, чтобы показать, каким образом его можно использовать.

А.2 Модули ASN.1

Примечание — Этот раздел можно в целом преобразовать в простой текст и затем скомпилировать, поэтому он не содержит заголовков и заголовков дополнительных предложений.

```
– SECRET KEY TRANSACTIONS MODULE –
EriSecretKeyTransactionsModule
{iso(1) standard(0) iso24535 (24534) secretKeyTransactions (5) version (0)}
DEFINITIONS AUTOMATIC TAGS ::= BEGIN

-- Electronic Registration Identification (ERI)
-- Secret Key Transactions

-- EXPORTS everything;

SecretKeyEriPdu ::= CHOICE {
        requestPdu              SecretKeyEriReqPdu,
        reponsePdu              SecretKeyEriRspPdu
        }

SecretKeyEriReqPdu ::= SEQUENCE {
        transactCode            TRANSACTION.&transactionCode ({SecretKeyEriTransactions}),
        argument                TRANSACTION.&ArgumentType
                                ({SecretKeyEriTransactions} {@.transactCode}) OPTIONAL
        }

SecretKeyEriRspPdu ::= SEQUENCE {
        transactCode            TRANSACTION.&transactionCode ({SecretKeyEriTransactions}),
        result                  TRANSACTION.&ResultType
        }                       ({SecretKeyEriTransactions} {@.transactCode})

-- TRANSACTIONS

TRANSACTION ::= CLASS {
        &ArgumentType           ,
        &ResultType             ,
        &transactionCode        INTEGER UNIQUE
        }
WITH SYNTAX {
        ARGUMENT                &ArgumentType
        RESULT                  &ResultType
        CODE                    &transactionCode
        }
```

```
SecretKeyEriTransactions TRANSACTION ::= { mutualAuthentication1 | mutualAuthentication2 |
        getSecretKeyEriData | setSecretKeyEriData |      commisionSecretKeyErt | decommissionSecretKeyErt |
        updateAccessControlList | getCipertextAccessControlListEntry | endOfSession
        }
-- Mutual authentication phase transactions
mutualAuthentication1 TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        1
        }
mutualAuthentication2 TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        2
        }
-- Data exchange phase transactions
getSecretKeyEriData TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        3
        }
setSecretKeyEriData TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        4
        }
commissionSecretKeyErt TRANSACTION ::= {
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        5
        }
decommissionSecretKeyErt TRANSACTION ::= {
        ARGUMENT                    NULL
        RESULT                      NULL
        CODE                        6
        }
updateAccessControlList TRANSACTION::={
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        7
        }
```

```
getCipertextAccessControlListEntry TRANSACTION::={
        ARGUMENT                    OCTET STRING
        RESULT                      OCTET STRING
        CODE                        8
        }

-- Session release phase transactions

endOfSession TRANSACTION ::= {
        ARGUMENT    OCTET STRING
        RESULT      NULL
        CODE 9
        }

END
-- Reduced ISO 15628 MODULE —
DSRCData { iso(1) standard(0) iso15628(15628) dsrcData (1) reducedVersion (24534) }
DEFINITIONS AUTOMATIC TAGS ::=BEGIN

-- Derived from ISO/DIS 15628 version 2003-05-19
```

Исправлен синтаксис модуля и инструкции включения, для того чтобы избежать ошибок компилятора ASN.1. Все, что признается избыточным ПНСТ 344—2018, опущено.

```
IMPORTS
        SecretKeyEriReqPdu, SecretKeyEriRspPdu
        FROM EriSecretKeyTransactionsModule;

Container::=CHOICE{
-- The values 1..16 ommitted
        secrtetKeyEriReqPdu         [19] EriSecretKeyTransactionsModule.SecretKeyEriReqPdu,
                                    -- only to be used in an Action-Request
        secrtetKeyEriRspPdu         [20] EriSecretKeyTransactionsModule.SecretKeyEriRspPdu,
                                    -- only to be used in an Action-Response
        ... -- extension marker
        }

    END
```

Приложение Б
(справочное)

Эксплуатационные сценарии

Б.1 Обзор

В этом приложении представлены три примера сеансов между ERT и считывателем или писателем ERI:

а) сеанс идентификации, в котором данные ERI считываются из ERT;

б) сеанс чтения и записи данных ERI, в котором данные ERI считываются из ERT, а затем новые данные ERI записываются в ERT;

в) сессия по записи и повторной ввод в эксплуатацию, в которой данные ERI и данные безопасности записываются в ERT.

Б.2 Идентификация транспортного средства

Пример сценария связи для идентификации ТС показан на рисунке Б.1.

Этот сценарий включает следующие шаги:

а) этап взаимной аутентификации с транзакциями взаимной аутентификации 1 и 2;

б) этап обмена данными, в котором ТС идентифицировано с транзакцией данных ERI с секретным ключом;

в) этап освобождения сеанса с завершением сеансовой транзакции.

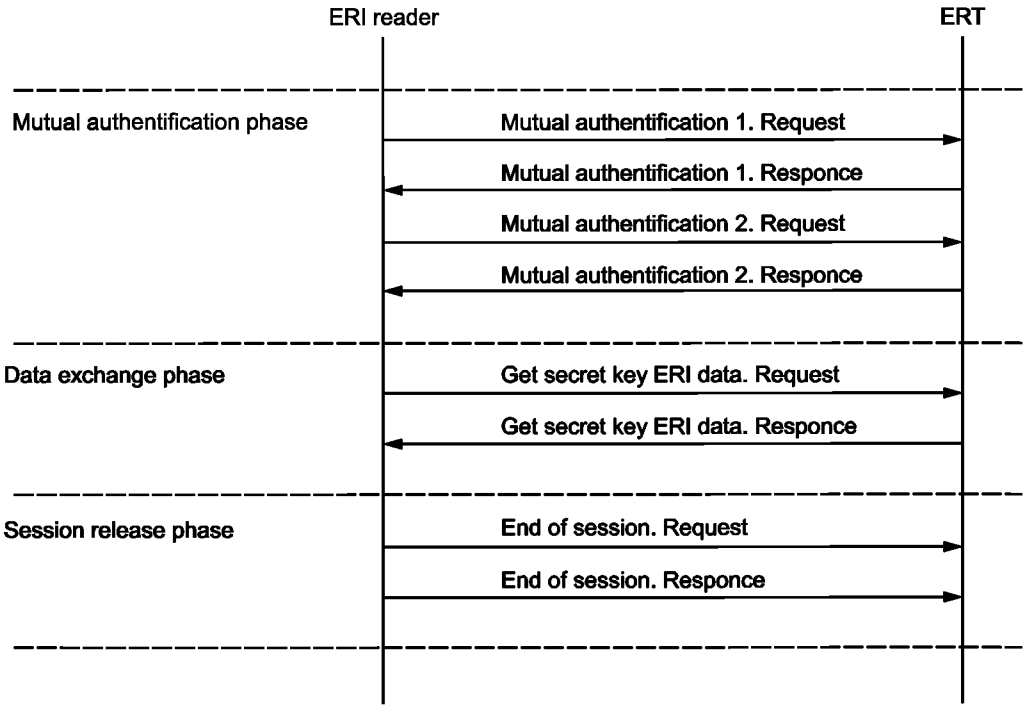

Рисунок Б.1 — Идентификация транспортного средства

Б.3 Сессия чтения и записи данных ERI

Пример сценария связи для чтения и записи данных ERI представлен на рисунке Б.2.

Этот сценарий включает следующие этапы:

а) взаимную аутентификацию с транзакциями взаимной аутентификации 1 и взаимной аутентификации 2;

б) фазу обмена данных, в которой

- данные ERI считываются в зашифрованном тексте с транзакцией данных секретного ключа ERI и
- новые ERI-данные, которые записываются в ERT с заданной транзакцией данных секретного ключа ERI в зашифрованном или в открытом тексте;

в) освобождение сеанса с завершением сеансовой транзакции.

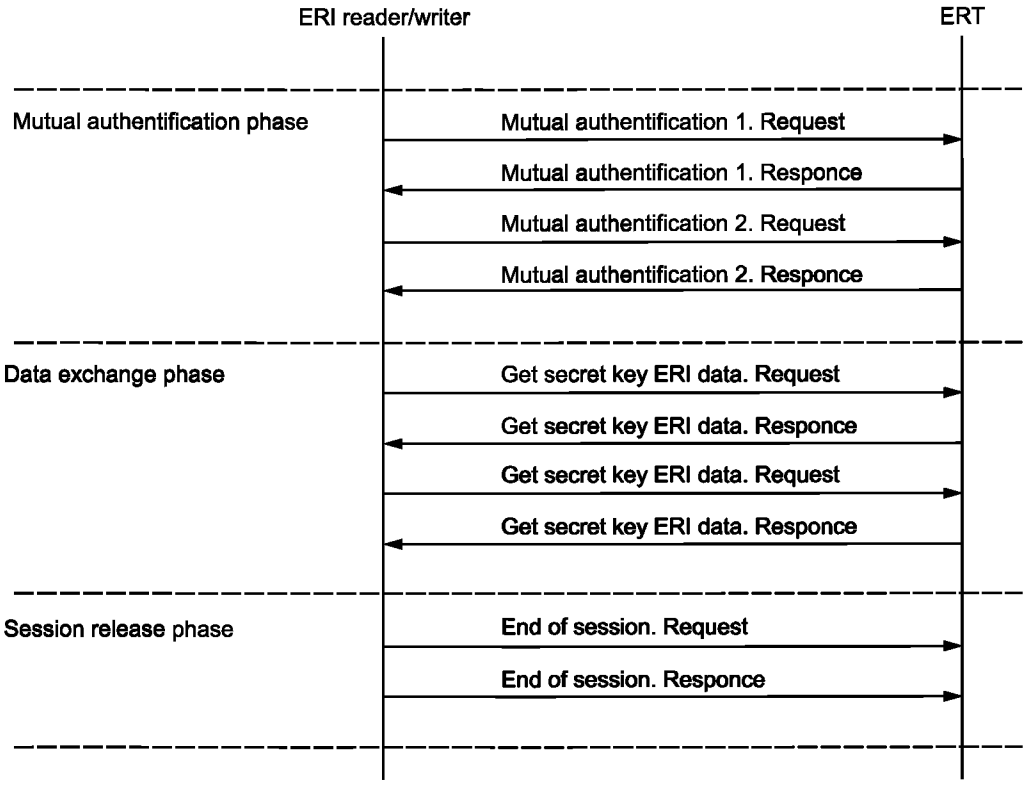

Рисунок Б.2 — Сеанс чтения и записи данных ERI

Б.4 Списание и ввод в эксплуатацию

Пример сценария связи для записи данных ERI и ввода в эксплуатацию ERT показан на рисунке Б.3.

Этот сценарий включает следующие этапы:

а) взаимную аутентификацию с транзакциями взаимной аутентификации 1 и взаимной аутентификации 2;

б) фазу обмена данными, в которой:

1) новые данные ERI записываются в ERT с установленной транзакцией данных секретного ключа ERI либо в зашифрованном тексте, либо в виде открытого текста,

2) ERT вводится в эксплуатацию с его транзакцией;

в) этап освобождения сеанса с завершением сеансовой транзакции.

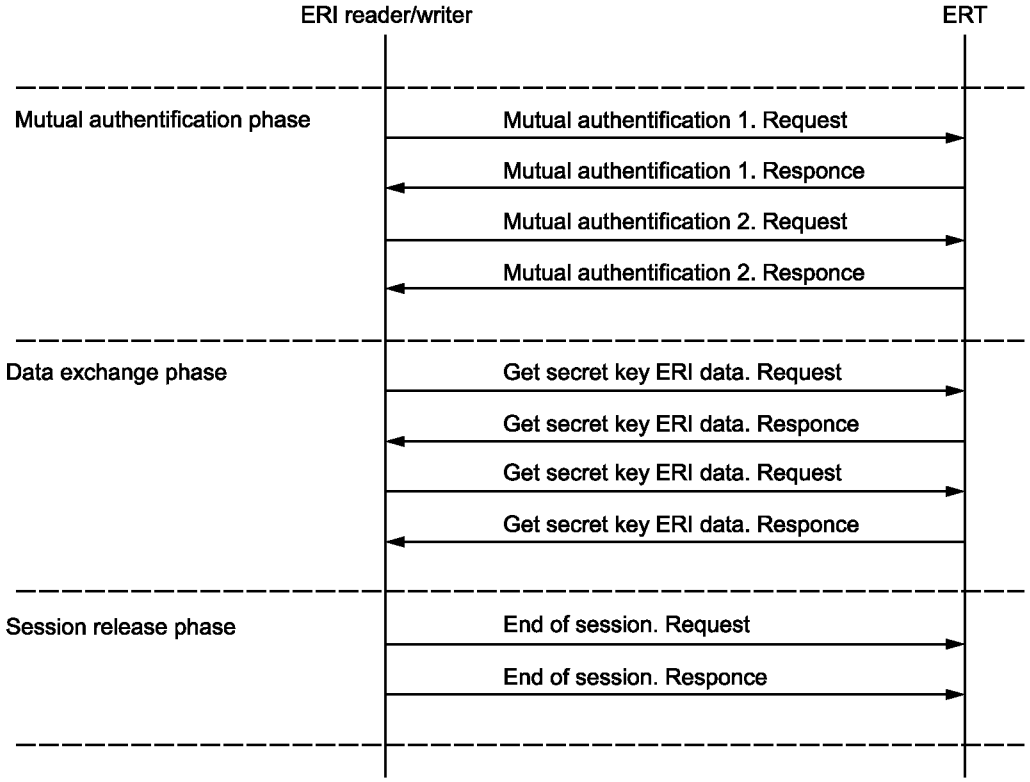

Рисунок Б.3 — Списание и ввод в эксплуатацию

Приложение В
(обязательное)

Проформы PICS

В.1 Обзор

В этом приложении содержатся проформы формирования выполнения протокола (PICS), которые будут использованы для ERT и считывателей/писателей ERI.

В.2 Поддержка транзакций

Этот раздел относится как к ERT, так и к читателям/писателям ERI.

В.2.1 GetSecretKeyEriData

Дополнительная поддержка данных ERI	Да/нет
Время ответа ERT для идентификатора ТС, мс	—
Время ответа ERT для записи данных ERI максимальной длины, мс	—

В.2.2 SetSecretKeyEriData

Поддержанный	Да/нет
Дополнительная поддержка ERI	Да/нет

В.2.3 CommissionSecretKeyErt

Поддержанный	Да/нет

В.2.4 DecommissionSecretKeyErt

Поддержанный	Да/нет

В.2.5 UpdateAccessControlList

Поддержанный	Да/нет

В.2.6 GetCiphertextAccessControlListEntry

Поддержанный	Да/нет

В.3 Вместимость склада ERT

Этот раздел применим только для ERT.

В.3.1 Емкость хранилища данных ERI

Описание	Максимальное значение или диапазон
Максимальная запись данных ERI	—

В.3.2 Емкость хранилища данных

Описание	Максимальное значение или диапазон
Оператор с секретным ключом максимальной длины, бит	
Идентификатор ключа максимальной длины	
Максимальное количество ключей, которые могут быть сохранены с их идентификатором ключа	

B.3.3 Хранение ключа управления

Описание	Максимальное значение или диапазон
Секретные ключи максимальной длины, бит	
Идентификатор ключа максимального значения	
Максимальное количество ключей, которые могут быть сохранены с их идентификатором ключа	

B.3.4 Общие значения

Описание	Максимальное значение или диапазон
Целые числа (минимальное и максимальное значение)	
Строки (максимальный размер)	

Библиография

[1]	ИСО/МЭК 14443 (все части)	Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты близкого действия.
[2]	ИСО 14815	Телематика дорожного транспорта и транспортного движения. Идентификация автоматических транспортных средств и оборудования. Спецификации системы
[3]	ИСО/МЭК 7498-1	Информационная технология (ИТ). Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель
[4]	ISO 3779	Транспорт дорожный. Идентификационный номер автомобилей (VIN). Содержание и структура
[5]	ИСО 7498-2-99	Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации
[6]	ИСО/МЭК 7816-3	Карты идентификационные. Карты на интегральных схемах. Часть 3. Карты с контактами. Электрический интерфейс и протоколы передачи
[7]	ИСО 14814:2006	Телематика дорожного транспорта и транспортного движения. Идентификация автоматических транспортных средств и оборудования. Эталонная архитектура и терминология
[8]	ИСО/МЭК 8824 (все части)	Информационная технология. Взаимосвязь открытых систем. Спецификация абстрактно-синтаксической нотации версии один (АСН.1)
[9]	ИСО/МЭК 10181-2	Информационные технологии. Взаимодействие открытых систем. Основы безопасности для открытых систем. Основа аутентификации
[10]	ИСО/МЭК 10181-1	Информационные технологии. Взаимодействие открытых систем. Основы безопасности для открытых систем. Обзор
[11]	ИСО/МЭК 10646	Информационные технологии. Универсальный набор кодированных символов (UCS)

УДК 656.13:006.354 ОКС 35.240.60

Ключевые слова: интеллектуальные транспортные системы, электронный сбор платы за проезд, архитектура систем сбора платы за проезд, бортовое оборудование

БЗ 2—2019/32

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 06.02.2019. Подписано в печать 12.02.2019. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,78.

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