



ПРЕДВАРИТЕЛЬНЫЙ
НАЦИОНАЛЬНЫЙ
СТАНДАРТ
РОССИЙСКОЙ
ФЕДЕРАЦИИ

ПНСТ
879—
2023
(ISO 25110:2017)

Интеллектуальные транспортные системы

**ЭЛЕКТРОННЫЙ СБОР ПЛАТЕЖЕЙ.
ОПРЕДЕЛЕНИЕ ИНТЕРФЕЙСА
ДЛЯ БОРТОВОЙ УЧЕТНОЙ ЗАПИСИ
С ИСПОЛЬЗОВАНИЕМ КАРТЫ
С ИНТЕГРАЛЬНОЙ СХЕМОЙ**

[ISO 25110:2017, Electronic fee collection — Interface definition for on-board account using integrated circuit card (ICC), MOD]

Издание официальное

Москва
Российский институт стандартизации
2023

Предисловие

1 ПОДГОТОВЛЕН Инфраструктурным центром Федерального государственного автономного образовательного учреждения высшего образования «Московский политехнический университет» (Московский политех) с привлечением творческого коллектива специалистов кафедры «Правовое и таможенное регулирование на транспорте» Федерального государственного бюджетного образовательного учреждения высшего образования «Московский автомобильно-дорожный государственный технический университет (МАДИ)» на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

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 29 ноября 2023 г. № 76-пнст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО 25110:2017 «Электронный сбор платежей. Определение интерфейса для бортовых счетов с использованием карточек на интегральных схемах» (ISO 25110:2017 «Electronic fee collection — Interface definition for on-board account using integrated circuit card (ICC)» MOD) путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом.

Внесение указанных технических отклонений направлено на учет специфичных отраслевых требований и особенностей аспекта стандартизации, характерных для Российской Федерации, а также правовых требований, установленных в Российской Федерации.

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5)

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 направлять не позднее чем за 4 мес до истечения срока его действия разработчику настоящего стандарта по адресу: 127083 Москва, ул. Мишина, д. 35 и/или в Федеральное агентство по техническому регулированию и метрологии по адресу: 123112 Москва, Пресненская набережная, д. 10, стр. 2.

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.rst.gov.ru)

© ISO, 2017

© Оформление. ФГБУ «Институт стандартизации», 2023

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

II

Содержание

1 Область применения	1
2 Нормативные ссылки.	2
3 Термины и определения	2
4 Сокращения	3
5 Модели передачи данных	4
6 Определение интерфейса для доступа к карте с интегральной схемой.	7
Приложение А (справочное) Требования к бортовой учетной записи	11
Приложение В (справочное) Пример применения метода доступа к карте с интегральной схемой	13
Приложение С (справочное) Модели взаимодействия платежного сервиса с другими сервисами. . . .	25
Библиография	27

Введение

Электронный сбор платы осуществляется по технологии, связанной с центральной системой учета, использующей бортовой блок, а также в рамках бортовой системы учета, использующей такие платежные средства, как карта с интегральной схемой.

Карты с интегральной схемой широко используются для карт общественного транспорта, таких как средства оплаты метро и наземного транспорта общего пользования, карты электронных денег для платежей общего назначения, а также для кредитных и банковских карт. Ожидается, что карты с интегральной схемой будут использоваться для платежных средств в системах электронного сбора платежей наряду с указанными глобальными тенденциями, что обеспечит в дальнейшем удобство и гибкость.

В настоящее время описания в существующих международных стандартах, связанных с системами электронного сбора платы, сосредоточены на центральной системе счетов, которая довольно проста и дает больше возможностей для взаимодействия элементов системы электронного сбора платы, чем бортовая учетная запись, которая является сложной и требует урегулирования большого количества вопросов.

Необходимость нового международного стандарта, касающегося бортовой системы учета с использованием карты с интегральной схемой, как показано на рисунке 1, обусловлена широким использованием транспортных и банковских карт. Кроме того, современный мобильный телефон, интегрированный с функциями карты с интегральной схемой (так называемый «мобильный электронный кошелек»), используется для общественного транспорта или розничных покупок в качестве средства оплаты во многих странах, что подтверждает важность стандартизации данного направления и необходимость рассмотрения будущих способов оплаты в системах электронного сбора платы.

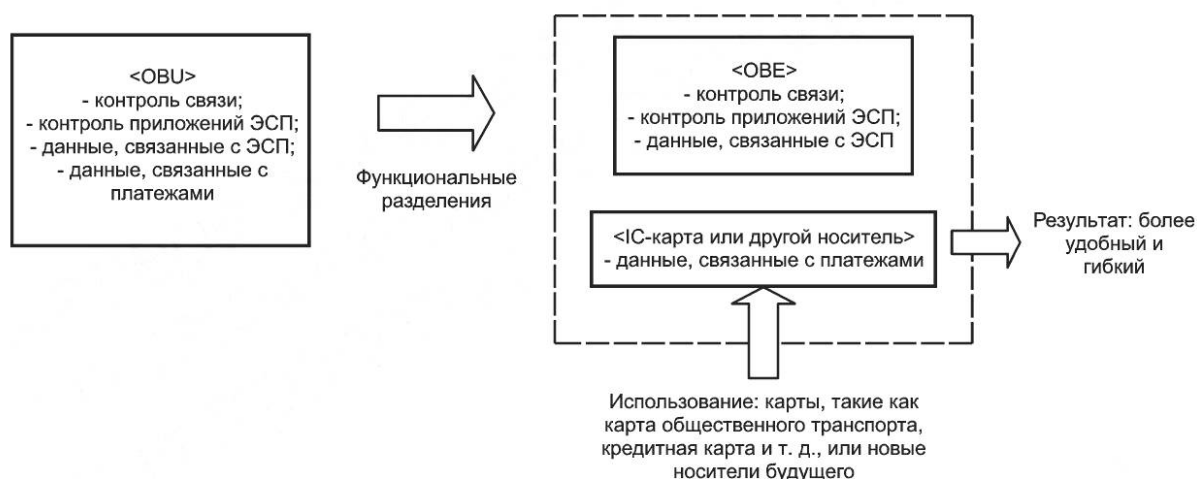


Рисунок 1 — Схема работы бортового аккаунта с помощью карты с интегральной схемой

На рисунке 2 показан стандарт системы электронного сбора платы, в которых бортовой блок используется в качестве средства связи, а карта с интегральной схемой несет средства оплаты.

Используемый здесь и далее термин «очистка» означает технологическую подготовку блока памяти бортового блока к осуществлению следующей транзакции (см. [1]).

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Интеллектуальные транспортные системы

ЭЛЕКТРОННЫЙ СБОР ПЛАТЕЖЕЙ. ОПРЕДЕЛЕНИЕ ИНТЕРФЕЙСА ДЛЯ БОРТОВОЙ УЧЕТНОЙ ЗАПИСИ С ИСПОЛЬЗОВАНИЕМ КАРТЫ С ИНТЕГРАЛЬНОЙ СХЕМОЙ

Intelligent transport systems.
Electronic fee collection. Interface definition for on-board account using integrated circuit card

Срок действия с 2024—06—01
С правом досрочного применения до 2027—06—01

1 Область применения

В настоящем стандарте определены модели передачи данных между придорожным оборудованием и картой с интегральной схемой, а также описания интерфейсов между придорожным оборудованием и бортовым оборудованием для бортовых учетных записей с использованием карты с интегральной схемой. Настоящий стандарт также содержит примеры определений интерфейсов и транзакций, применимых в нескольких странах.

Настоящий стандарт рассматривает:

- модели передачи данных между придорожным оборудованием и картой с интегральной схемой, которые соответствуют категоризованным эксплуатационным требованиям и механизму передачи данных для каждой модели;
- определение интерфейса между придорожным оборудованием и бортовым оборудованием на основе каждой модели передачи данных;
- определение интерфейса для каждой модели;
- функциональную конфигурацию;
- определения команд придорожного оборудования для доступа к карте с интегральной схемой;
- формат данных и определения элементов данных команд придорожного оборудования;
- пример транзакции для каждой модели в приложении В.

На рисунке 3 показана конфигурация бортовой учетной записи и область применения настоящего стандарта. Описания в настоящем стандарте сосредоточены на интерфейсе между придорожным оборудованием и бортовым блоком для доступа к карте с интегральной схемой (ICC).

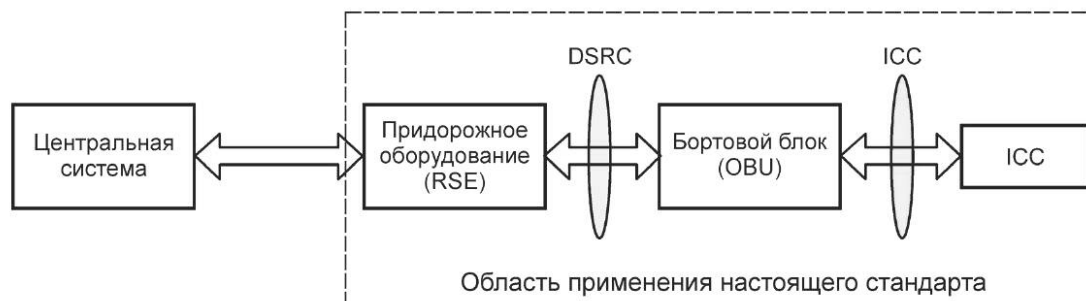


Рисунок 3 — Конфигурация бортовой учетной записи и область применения настоящего стандарта

На рисунке 4 показана структура уровней RSE, OBU и ICC, где средний уровень интерфейсов приложений обозначен как практическая область применения настоящего стандарта.

Примечание — Существующие стандарты для физического и других уровней протокола как между RSE и OBE, так и между OBE и ICC выходят за рамки настоящего стандарта. Например, элементы, связанные с DSRC (L-1, L-2 и L-7) и элементы, связанные с ICC, не входят в область применения настоящего стандарта.

В OBU содержатся два типа виртуальных мостов. Первый тип — это мост-1, на котором команда RSE, отправленная из RSE, декомпозируется, а команда доступа ICC, содержащаяся в блоке данных протокола приложения (APDU) команды RSE, передается в интерфейс ICC для доступа к ICC. Второй тип — это мост-2, в котором команда RSE, отправляемая из RSU, преобразуется в команду доступа ICC и передается в интерфейс ICC для доступа к ICC.

Мост-1 соответствует прозрачному типу и типу буферизации, определенным в настоящем стандарте, тогда как мост-2 соответствует типу кэширования.

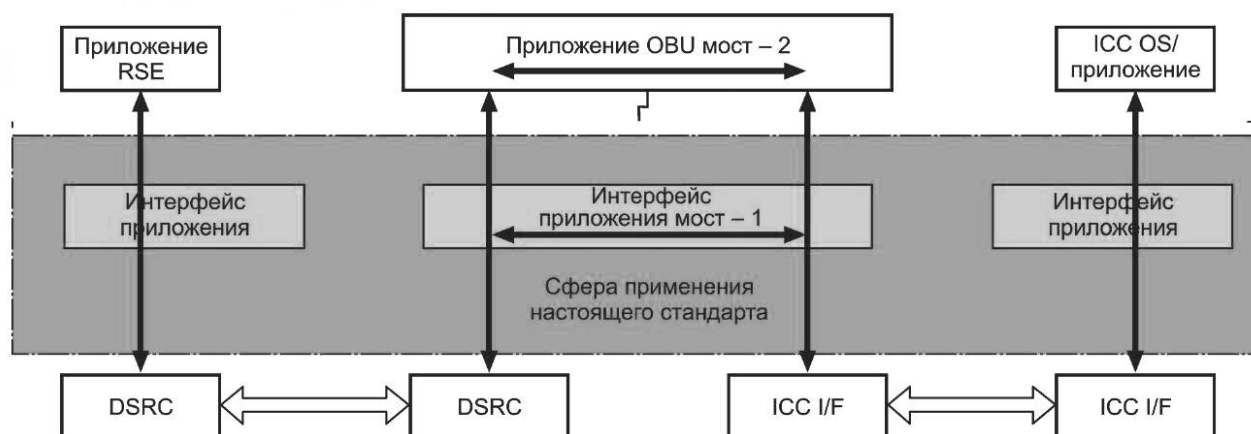


Рисунок 4 — Прикладные интерфейсы RSE, OBU и ISS и область применения настоящего стандарта

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 56829 Интеллектуальные транспортные системы. Термины и определения

ГОСТ Р 58833 Защита информации. Идентификация и аутентификация. Общие положения

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 термины по ГОСТ Р 56829, ГОСТ Р 58833, а также следующие термины с соответствующими определениями:

3.1 атрибут: Адресный пакет данных, состоящий из одного элемента данных или структурированных последовательностей элементов данных.

3.2 аутентификатор: Зашифрованные данные, которые используются для аутентификации.

3.3 бортовое оборудование: Все необходимое оборудование на борту транспортного средства для выполнения требуемых функций ЭСП и услуг связи.

3.4 бортовой блок: Единый электронный блок на борту транспортного средства для выполнения определенных функций ЭСП и связи с внешними системами.

3.5 группа данных: Класс тесно связанных атрибутов.

3.6 канал: Маршрут передачи информации.

3.7 криптография: Принципы, средства и методы преобразования данных для защиты их информационного содержания с целью предотвращения их несанкционированного использования.

3.8 модель транзакции: Функциональная модель, описывающая общую структуру транзакций электронного платежа.

3.9 модуль безопасного приложения: Физический модуль, который безопасно выполняет криптографические функции и хранит ключи.

3.10 поставщик транспортных услуг: Организация, предоставляющая транспортные услуги, такие как обеспечение дорог.

3.11 придорожное оборудование: Оборудование, расположенное вдоль дороги, стационарное или мобильное.

3.12 транзакция: Весь обмен информацией между двумя физически разделенными средствами связи.

3.13 учетные данные доступа: Доверенная аттестация или защищенный модуль, который устанавливает заявленную идентичность объекта или приложения.

Примечание — Учетные данные доступа несут информацию, необходимую для выполнения условий доступа, чтобы выполнить операцию над адресуемым элементом в ОВЕ. Учетные данные для доступа могут содержать пароли, а также информацию на основе криптографии, такую как аутентификаторы.

3.14 целостность данных: Способность данных не подвергаться изменению или аннулированию в результате несанкционированного доступа.

3.15 элемент: Каталог в структуре технологического обеспечения выделенной связи ближнего действия, содержащий информацию о приложении в виде атрибутов.

3.16 эмитент: Субъект, ответственный за выдачу платежных средств пользователю.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ЭСП	— электронный сбор платы;
AID	— идентификатор приложения (application identifier);
APDU	— единица данных протокола приложения (application protocol data unit);
ASN.1	— нотация абстрактного синтаксиса (abstract syntax notation one);
BST	— таблица обслуживания маяка (beacon service table);
CPU	— микроконтроллер (central processing unit);
DC	— команда дебетования (debit command);
DS	— набор данных (data set);
DSRC	— выделенная связь ближнего действия (dedicated short-range communication);
EAL	— уровень гарантии оценки (evaluation assurance level);
EID	— идентификатор элемента (element identifier);
ERP	— электронное дорожное ценообразование (electronic road pricing);
ETC	— система оплаты платных дорог (electronic toll collection);
ICC	— карта с интегральной схемой (integrated circuit card);
IFMS	— совместимая система управления тарифами (interoperable fare management system);
MAC	— средний контроль доступа (medium access control);
OBE	— бортовое оборудование (on-board equipment);
OBU	— бортовой блок (on-board unit);

RSE — придорожное оборудование (road-side equipment);
 SAM — модуль безопасного приложения (secure application module);
 VD — данные значения (value data).

5 Модели передачи данных

5.1 Обзор

Существует три типа моделей передачи данных для бортовых учетных записей, использующих ICC для выполнения операционных требований, описанных в приложении А.

5.1.1 Прозрачный тип

Данные команды ICC передаются напрямую от RSE к ICC через OBU. OBU временно сохраняет данные команды ICC и данные ответа в буферной памяти (см. рисунок 5).

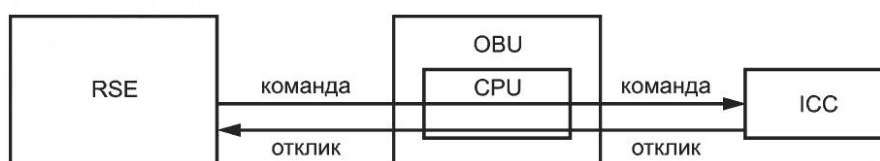


Рисунок 5 — Типовая структура прозрачного типа

5.1.2 Тип кэширования

Данные, относящиеся к ЭСП, считываются из ICC во время презентации и сохраняются в SAM блока OBU. При обмене данными DSRC данные в SAM, относящиеся к ЭСП, передаются в RSE (см. рисунок 6).

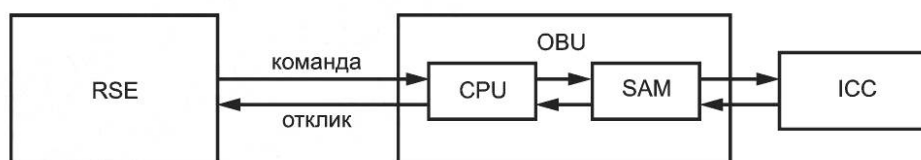


Рисунок 6 — Общая структура типа кэширования

5.1.3 Тип буферизации

Данные, относящиеся к ЭСП, которые ограничены неконфиденциальными данными, считываются из ICC при представлении и сохраняются в буферной памяти в OBU [8]. При обмене данными DSRC данные в буферной памяти, относящиеся к ЭСП, передаются в RSE (см. рисунок 7).

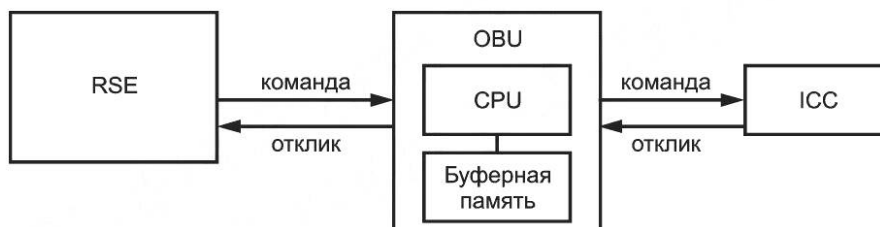


Рисунок 7 — Общая структура типа буферизации

5.2 Символы

В механизме передачи данных каждой модели применяются символы, приведенные на рисунке 8.

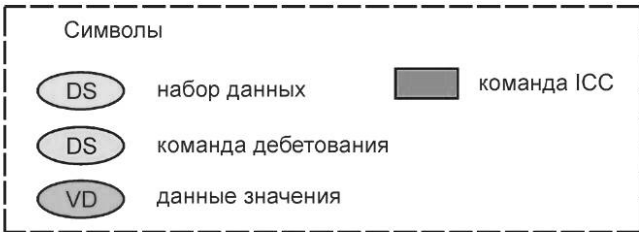


Рисунок 8 — Определение символов

5.3 Прозрачный тип

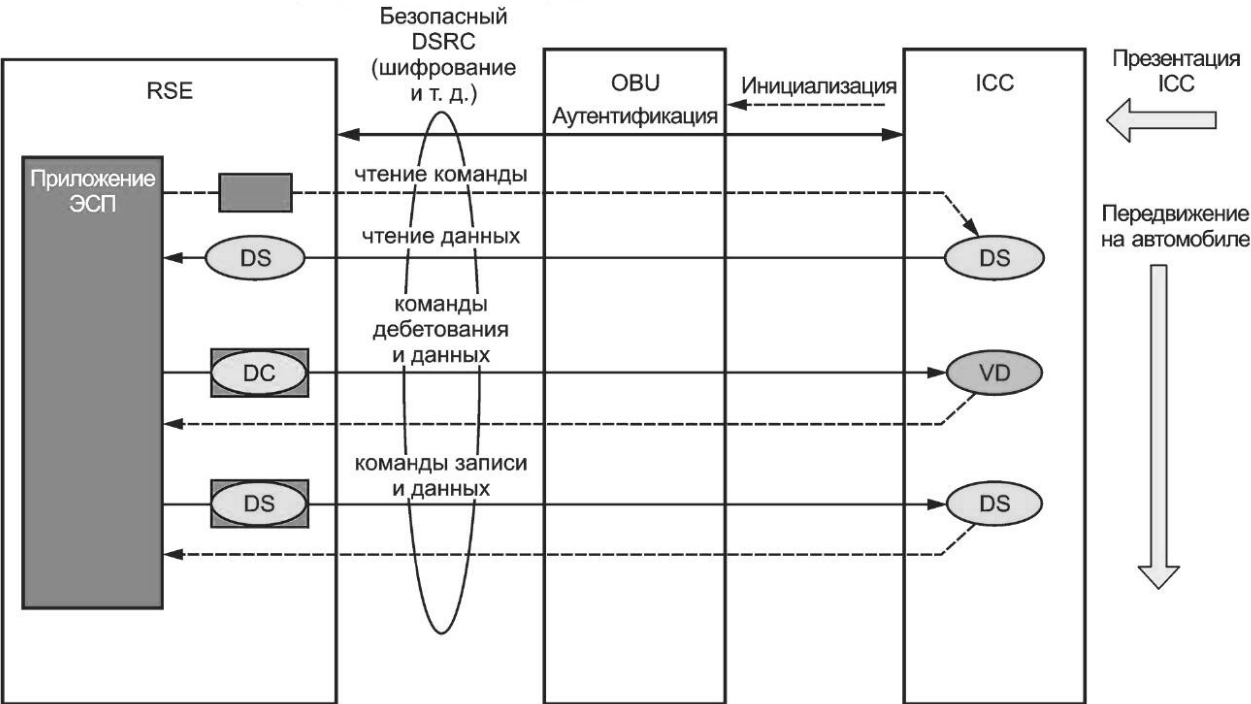
5.3.1 Обзор

В этой модели максимальная скорость транспортного средства зависит от скорости передачи данных между ICC и OBU, так что транспортное средство должно остановиться или медленно проехать под антенной RSE в случае использования обычного контактного ICC. Особенность прозрачного типа состоит в том, чтобы упростить OBU за счет устранения защищенной памяти внутри OBU, а производительность будет улучшена в соответствии с разрабатываемым ICC с высокой скоростью передачи данных.

5.3.2 Процесс передачи данных

В этой модели обмен данными между RSE и ICC обрабатывается непосредственно после установления связи DSRC и завершения аутентификации между RSE и OBU. Взаимная аутентификация между ICC и RSE обрабатывается непосредственно перед обменом данными приложения и доступом к данным значений.

В последовательности чтения команда READ отправляется от RSE к ICC через OBU для считывания набора данных, хранящихся в ICC. В ответе READ набор данных, хранящийся в ICC, передается от ICC к RSE через OBU. В последовательности записи выполняется та же процедура. В случае предоплаты команда дебетования отправляется с RSE и выполняется та же процедура, как показано на рисунке 9.



Примечание – Команда дебетования используется в случае предоплаты.

Рисунок 9 — Процесс передачи данных прозрачного типа

5.4 Тип кэширования

5.4.1 Обзор

В этой модели OBU считывает наборы данных из ICC и сохраняет их в защищенной памяти внутри OBU после вставки и завершения аутентификации. Особенностью этого типа является то, что высокая скорость обмена данными между RSE и OBU выполняется даже при использовании ICC с низкой скоростью передачи данных. Благодаря этому типу кэширования максимальная скорость автомобиля повышается до производительности связи DSRC, не связанной со скоростью передачи данных ICC.

5.4.2 Процесс передачи данных

В этой модели считанные данные из ICC хранятся в защищенной памяти, такой как SAM, внутри OBU для обеспечения информационной безопасности.

Особенность этого типа заключается в том, чтобы справляться с высокой скоростью транспортного средства за счет обработки высокой скорости обмена данными между RSE и OBU, не имеющей отношения к типу ICC (см. рисунок 10).

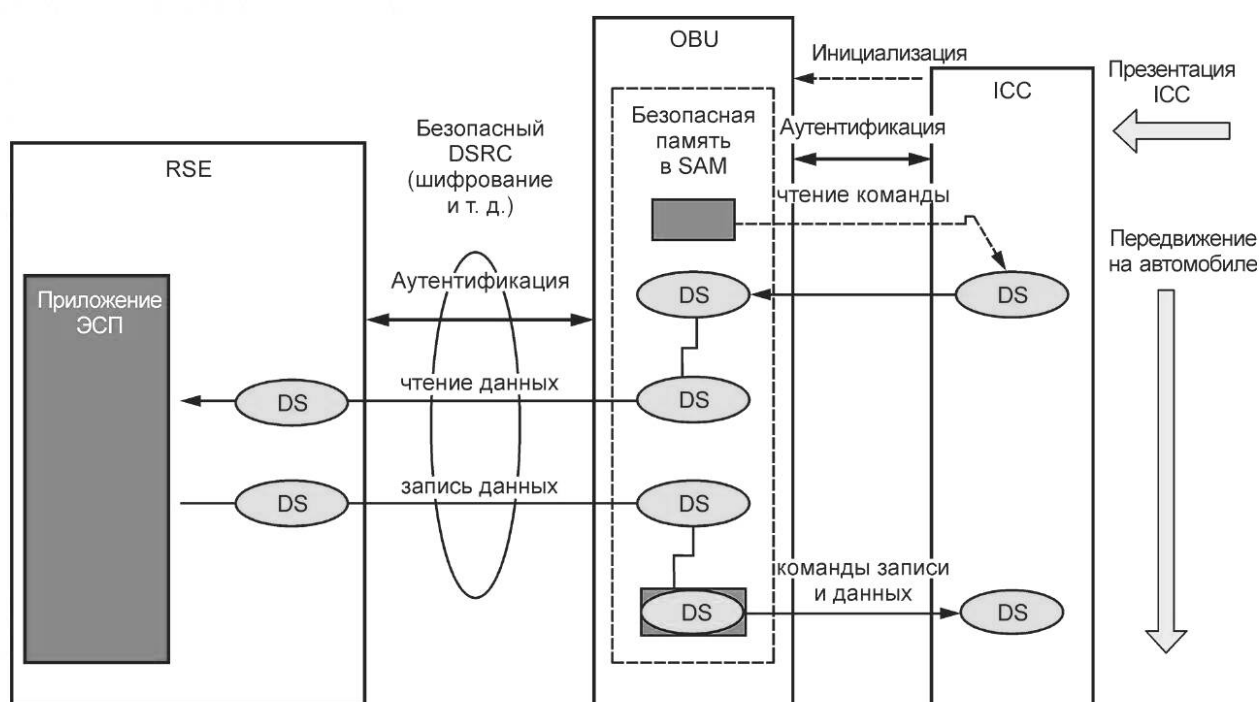


Рисунок 10 — Процесс передачи данных типа кэширования

5.5 Тип буферизации

5.5.1 Обзор

Наборы данных, хранящиеся в ICC, ограничиваются не конфиденциальными данными, чтобы не подвергаться фальсификации или раскрытию. В этом типе буферизации метод передачи данных такой же, как и тип кэширования и наборы данных ICC считываются и сохраняются в буферной памяти внутри OBU, когда ICC вставляется в OBU. Наборы данных, хранящиеся в буферной памяти, передаются в RSE во время последовательности чтения DSRC. В случае записи наборы данных RSE передаются в OBU и сохраняются в буферной памяти OBU, а затем передаются в ICC.

5.5.2 Процесс передачи данных

Особенность этого типа — возможность исключить SAM из OBU и использовать даже низкоскоростной ICC (см. рисунок 11).

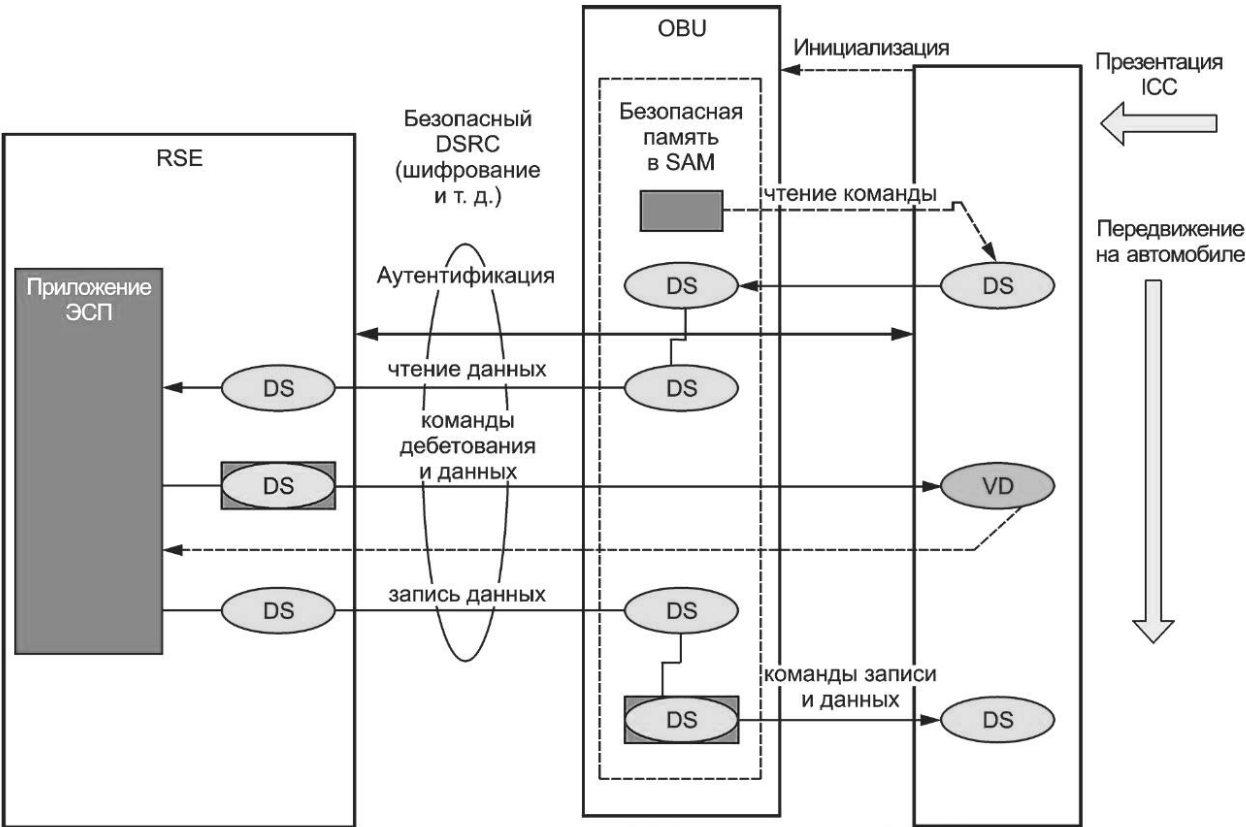


Рисунок 11 — Процесс передачи данных типа буферизации

6 Определение интерфейса для доступа к карте с интегральной схемой

6.1 Прозрачный тип передачи данных

6.1.1 Функциональная конфигурация

Функциональная конфигурация прозрачного типа показана на рисунке 12. RSE отправляет команду RSE, содержащую команды доступа ICC, в APDU, чтобы напрямую выполнить операцию чтения/записи ICC.

Требования к определению команд между OBU и ICC приведены в [1].

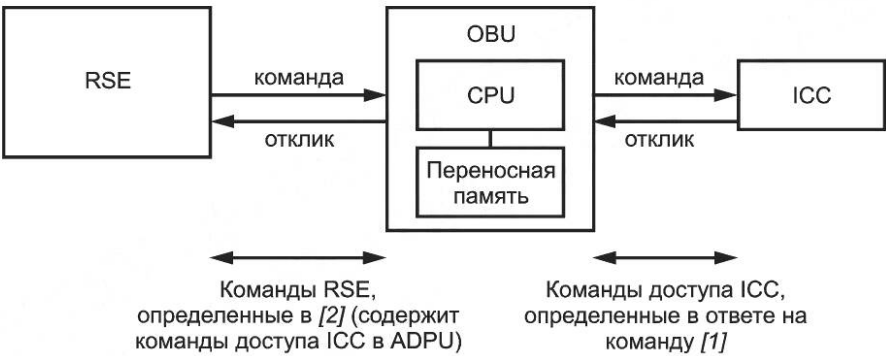


Рисунок 12 — Функциональная конфигурация прозрачного типа передачи данных

6.1.2 Команды и ответ между RSE и OBU

Канал передачи, представленный в [2], используется в качестве базовой команды RSE для доступа к ICC из RSE напрямую с указанием идентификатора канала в параметре действия как идентификатор канала = ICC (см. таблицы 1 и 2).

Т а б л и ц а 1 — Запрос TRANSFER_CHANNEL

Параметр	Тип ASN.1	Значение	Примечания
Идентификатор элемента EID	Dsrc-Eid	0	
Тип действия	INTEGER(0..127,...)	8	Канал передачи
Учетные данные для доступа	OCTET STRING		
Параметр действия	ChannelRq:: = SEQUENCE { channelId ChannelId, APDU OCTET STRING }		Присутствует всегда Channel ID = ICC
Режим	BOOLEAN	TRUE	

Параметр APDU (единица данных протокола приложения) должен содержать команду ICC.

Т а б л и ц а 2 — Ответ TRANSFER_CHANNEL

Параметр	Тип ASN.1	Значение	Примечания
Параметр ответа	ChannelRs:: = SEQUENCE { channelId ChannelId, APDU OCTET STRING }		Присутствует всегда
Код возврата (Ret)	Статус возврата		Дополнительное использование

Параметр APDU в ответе должен содержать ответ ICC.

6.2 Тип кэширования

6.2.1 Функциональная конфигурация

Функциональная конфигурация типа кэширования показана на рисунке 13. Наборы данных, хранящиеся в ICC, считываются и кэшируются в SAM OBU, когда ICC вставляется в OBU. Во время связи DSRC RSE отправляет команду RSE, включая команду доступа SAM, в APDU для чтения наборов данных, кэшированных в SAM.

Требования к определению команды между SAM и ICC приведены в [1].

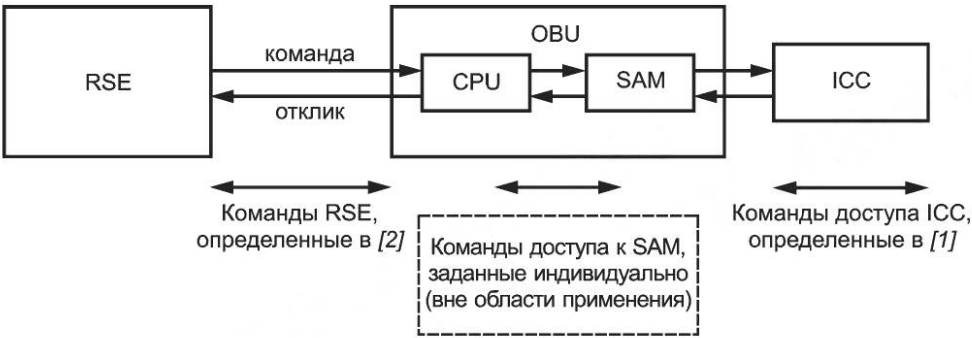


Рисунок 13 — Функциональная конфигурация типа кэширования

6.2.2 Команды и ответ между RSE и OBU

Канал передачи, представленный в [2], используется как основная команда RSE для доступа к SAM OBU из RSE напрямую с указанием идентификатора канала в параметре действия как идентификатор канала = SAM1 (1) или SAM2 (2) см. таблицы 3 и 4.

Таблица 3 — Запрос TRANSFER_CHANNEL

Параметр	Тип ASN.1	Значение	Примечания
Идентификатор элемента EID	Dsrc-Eid	0	
Тип действия	INTEGER(0..127,..)	8	Канал передачи
Учетные данные для доступа	OCTET STRING		
Параметр действия	ChannelRq:: = SEQUENCE { channelId ChannelId, APDU OCTET STRING }		Присутствует всегда Channel ID = SAM1 (1) или SAM2(2)
Режим	BOOLEAN	TRUE	

Параметр APDU в параметре действия должен содержать команду ICC или ее элементы данных.

Таблица 4 — Ответ TRANSFER_CHANNEL

Параметр	Тип ASN.1	Значение	Примечания
Параметр ответа	ChannelRs:: = SEQUENCE { channelId ChannelId, APDU OCTET STRING }		Присутствует всегда
Код возврата (Ret)	Статус возврата		Дополнительное использование

Параметр APDU в ответе должен содержать ответ ICC или его элементы данных.

6.3 Тип буферизации

6.3.1 Функциональная конфигурация

Функциональная конфигурация типа буферизации показана на рисунке 14. Наборы данных, хранящиеся в ICC, считываются и сохраняются в буферной памяти OBU, когда ICC вставляется в OBU. Во

время связи DSRC RSE отправляет команду RSE для чтения наборов данных, хранящихся в буферной памяти.

Требования к определению команд между OBU и ICC приведены в [1].

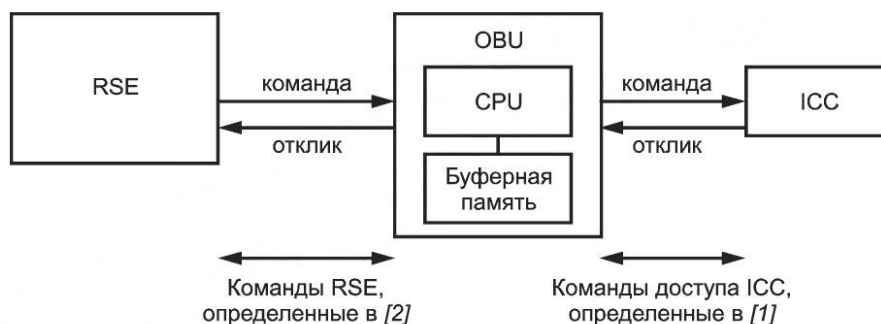


Рисунок 14 — Функциональная конфигурация типа буферизации

6.3.2 Команды и ответ между RSE и OBU

Поскольку в этом типе буферизации необходимые наборы данных, хранящиеся в ICC, передаются в буферную память OBU, GET или SET используется в качестве команды RSE. Кроме того, для процесса предоплаты используется дебет или кредит функции ЭСП, определенной в [2] (см. таблицы 5 и 6).

Таблица 5 — Запрос DEBIT

Параметр	Тип ASN.1	Значение	Примечания
Идентификатор элемента EID	Dsrc-Eid		Неравно 0
Тип действия	INTEGER(0..127,..)	13	
Учетные данные для доступа	OCTET STRING		Дополнительное использование
Параметр действия	DebitRq:: = SEQUENCE { debitPaymentFee PaymentFee, nonce OCTET STRING keyRef INTEGER(0..255) }		Присутствует всегда
Режим	BOOLEAN	TRUE	

Каждый параметр в параметре действия должен содержать элементы данных команды дебета для ICC.

Таблица 6 — Ответ DEBIT

Параметр	Тип ASN.1	Значение	Примечания
Параметр ответа	DebitRs:: = SEQUENCE { debitResult ResultFin, debitAuthenti- OCTET STRING cator }		Присутствует всегда
Код возврата (Ret)	Статус возврата		Дополнительное использование

Каждый параметр в параметре ответа должен содержать элементы данных дебетевого ответа для ICC.

Приложение А (справочное)

Требования к бортовой учетной записи

А.1 Операционные требования к бортовой учетной записи

Основными факторами эксплуатационных требований к ЭСП являются скорость транспортного средства и уровень информационной безопасности, как показано на рисунке А.1, которые в значительной степени влияют на конструкцию системы ЭСП. Уровни информационной безопасности на рисунке А.1, называемые EAL, представлены в [3]—[5].

Категория 4 выполняется специально разработанным механизмом безопасности, таким как SAM, встроенным в OBU в дополнение к механизму безопасности ICC, в то время как механизмы безопасности категорий 1, 2 и 3 выполняются ICC.

Категория 4 охватывает все услуги ЭСП с высоким уровнем безопасности. Категория 1 включает оплату парковки и оплату проезда, когда транспортное средство останавливается или проезжает на малой скорости под придорожной антенной. Категория 2 охватывает услуги категории 1 и ЭСП в одной полосе движения. Категория 3 охватывает категорию 2 и ЭСП/ERP в многополосном свободном потоке, когда автомобиль проезжает под придорожной антенной на высокой скорости.

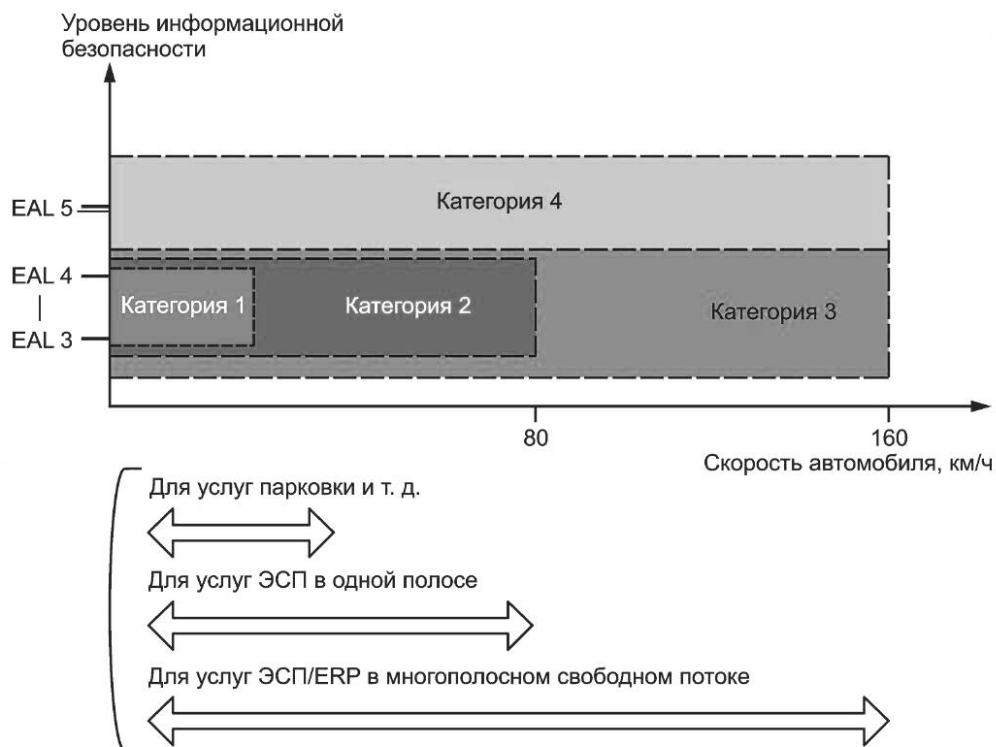


Рисунок А.1 — Эксплуатационные требования

А.2 Типы ICC

ICC, используемый для бортовых учетных записей, классифицируется, как показано на рисунке А.2. Тип контакта ICC (см. [1], [6]—[8]) в основном используется для финансовых карт, таких как банковские и кредитные карты. Бесконтактный ICC (см. [9]—[12] или [13]) широко используется в секторе общественного транспорта в качестве средства оплаты и для продажи билетов. Гибридный тип ICC имеет обе функции, представленные в [1], [6]—[8] и [9]—[12] или [13], а также используется для многофункциональных карт, таких как ЭСП и карты общественного транспорта.

Есть несколько вариантов, когда ICC используется для ЭСП. Один из вариантов — использовать его только для оплаты. Другой вариант — использовать его как для оплаты, так и для хранения данных, связанных с ЭСП.

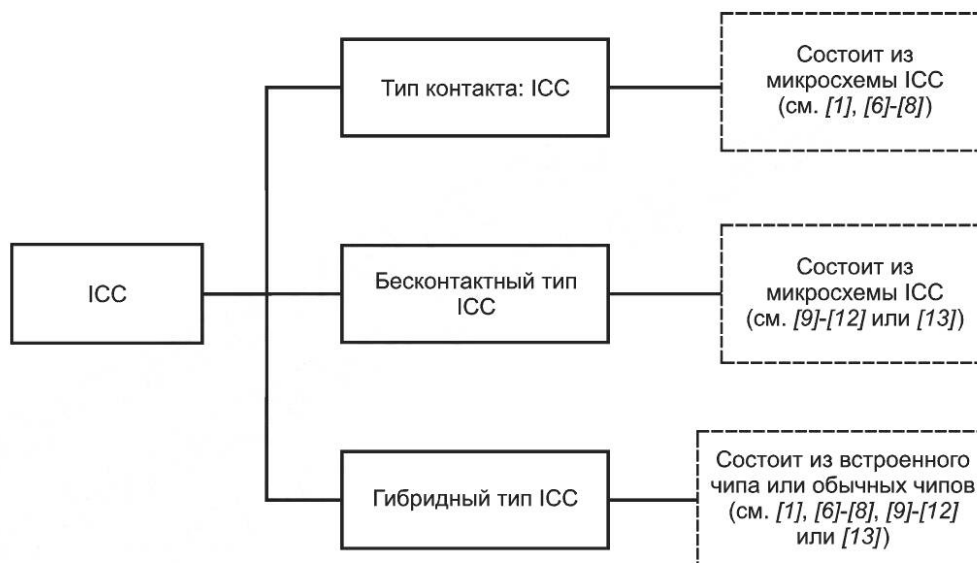


Рисунок А.2 — Типы карт ICC

А.3 Требования к взаимодействию для ICC

Для обеспечения безопасности и передачи данных от ICC потенциально требуется, чтобы она имела возможность взаимодействия с другими сервисами в качестве обычного платежного средства. Предполагается, что уровень функциональной совместимости, необходимый для ICC, можно разделить на следующие три уровня:

- уровень 1 — взаимодействие с группой операторов платных дорог, работающих по контракту;
- уровень 2 — функциональная совместимость, расширенная для приложений общественного транспорта;
- уровень 3 — дальнейшее расширение функциональной совместимости для розничных приложений.

Особенно в отношении уровня 2 следует рассмотреть схему взаимодействия, основанную на сотрудничестве с архитектурой ЭСП и архитектурой IFMS общественного транспорта.

В приложении С показаны отношения оперативной совместимости, когда коды ICC, выпущенные для ЭСП, должны использоваться для приложений общественного транспорта и/или розничной торговли.

А.4 Производительность каждой модели передачи

В таблице А.1 показана связь с доменами категорий, определенными на основе эксплуатационных требований и моделей передачи данных.

Таблица А.1 — Связь с доменами категорий и моделями передачи данных

Категория	Модель передачи данных		
	Прозрачный тип	Тип кэширования	Тип буферизации
Категория 1	×		
Категория 2	×		
Категория 3	×		×
Категория 4		×	

Примечание — В случае прозрачного типа каждая категория зависит от скорости передачи типа ICC.

Приложение В
(справочное)**Пример применения метода доступа к карте с интегральной схемой****В.1 Модель с прозрачным шрифтом****В.1.1 Модель 1 прозрачного типа (для предоплаты)****В.1.1.1 Обзор**

В качестве примера модели прозрачного типа 1 доступ к ICC осуществляется с помощью функции канала передачи (см. [2]):

- команда: TRANSFER_CHANNEL (см. [2]);
- AID: Электронный сбор платы (ЭСП) как AID = 1 (см. [2]);
- идентификатор канала: ICC определен как ChannelID = icc (см. [2]);
- тип ICC: бесконтактный тип предоплаты ICC.

В.1.1.2 Определение типа данных

а) Определение содержимого APDU в TransferChannel.rq:

```
ICCcommand:: = SEQUENCE{  
  opCommandBody OCTET STRING — команда ICC (см. [1])  
}
```

б) Определение содержимого APDU в TransferChannel.rs:

```
ICCresponse:: = SEQUENCE{  
  opCommandBody OCTET STRING — реакция ICC (см. [1])  
}
```

В.1.1.3 Транзакция. Тарификация на основе расстояния ETC (закрытая система)

а) Система входа.

На входе выполняется взаимная аутентификация между RSE и ICC, и входящая информация записывается в ReceiptServicePart памяти OBU (см. рисунок В.1).

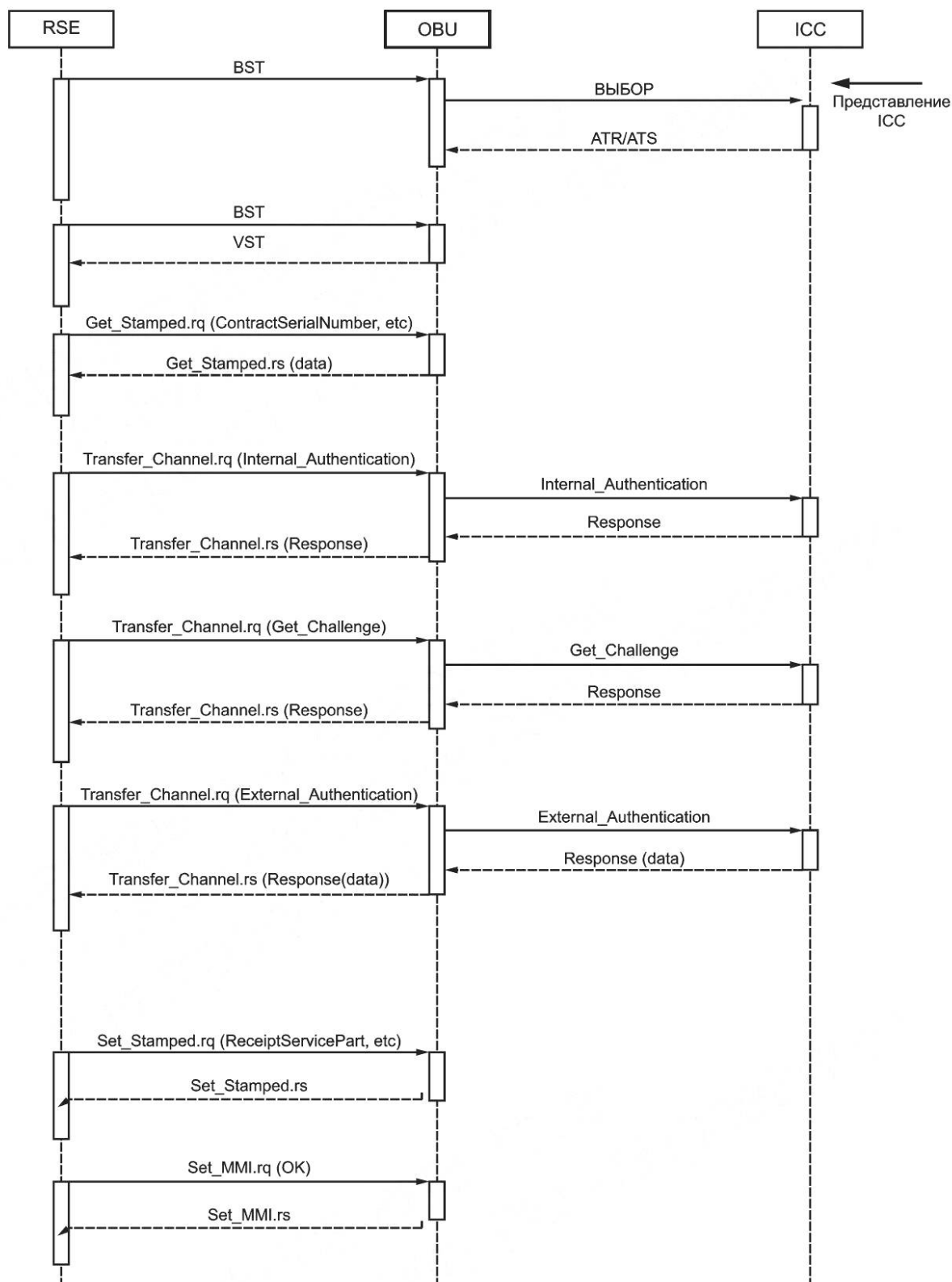


Рисунок В.1 — Последовательность входной системы

b) Система выхода.

На выходе RSE считывает входную информацию из OBU и сохраняет ее в памяти RSE, при этом выполняется взаимная аутентификация между RSE и ICC. RSE рассчитывает плату в соответствии с входной информацией и отправляет команду в ICC напрямую через OBU, используя функцию канала передачи (см. рисунок В.2).

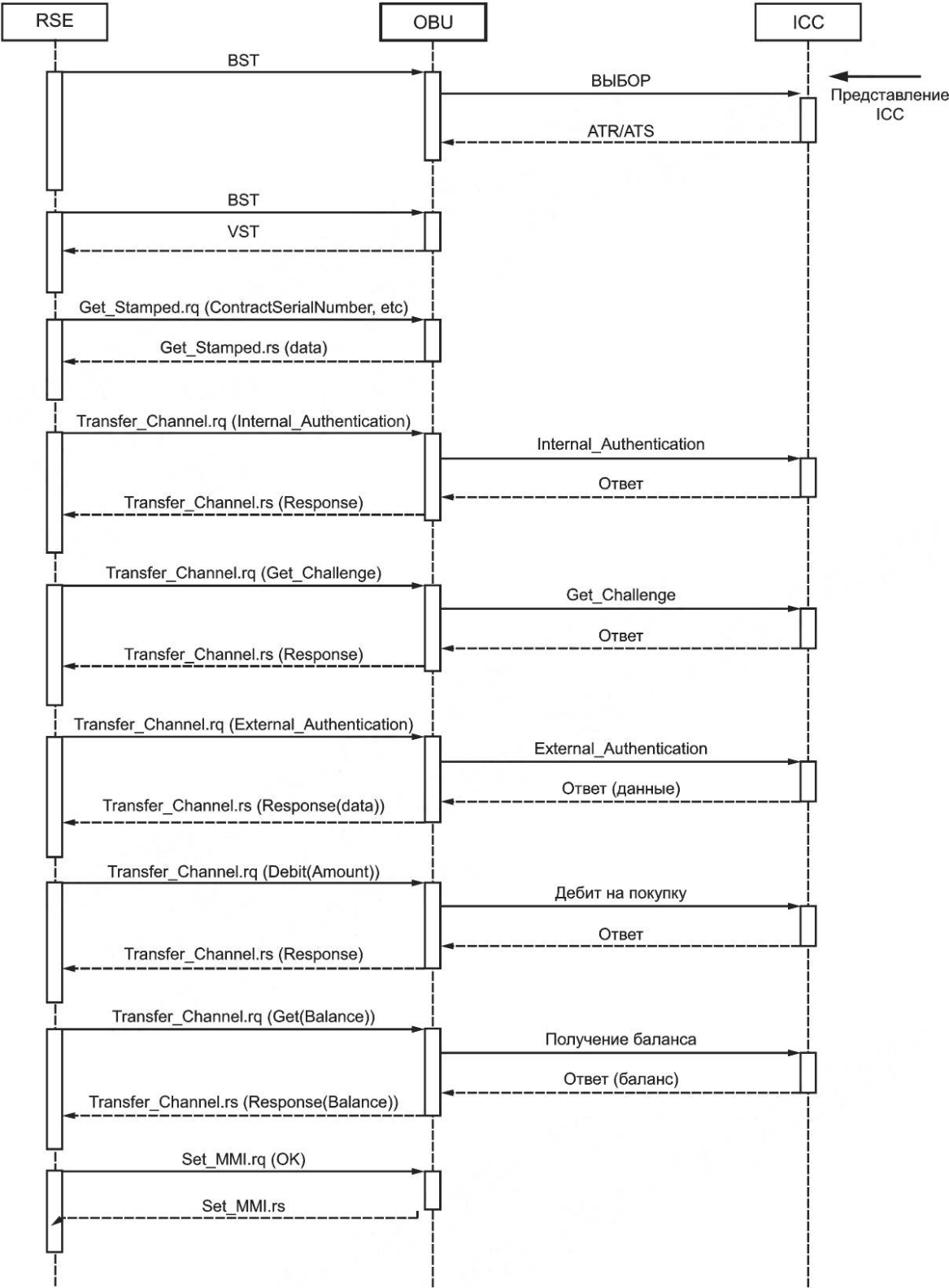


Рисунок В.2 — Последовательный поток выходящей системы

В.1.2 Модель 2 прозрачного типа (для постоплаты)

В.1.2.1 Обзор

В качестве примера модели прозрачного типа представлен метод доступа ICC, определенный в «базовом интерфейсе приложения DSRC».

«Базовый интерфейс приложения DSRC» создан для предоставления множества информационных услуг, таких как информация о движении и дорогах, информация о водителе/пассажирах, информация о парковках и т. д., с идентификатором приложения AID = 18 (см. [14]). В дополнение к основным информационным услугам доступ ICC определен для приложения оплаты парковки.

В этом подпункте сообщение отправки, определенное в «базовом интерфейсе приложения DSRC», представлено как эквивалентный метод канала передачи (см. [2], пункт 7.1).

- Определение команды: определена базовым интерфейсом приложения DSRC.
- команда: TRANSFER_CHANNEL (см. [2]);
- AID: ЭСП как AID = 1 (см. [2]);
- идентификатор канала: ICC определен как ChannelID = icc (см. [2]);
- тип ICC: ICC контактного типа с оплатой в кредит.

B.1.2.2 Определение типа данных

a) Определение содержимого APDU в TransferChannel.rq:

```
CCAccessCommand:: = SEQUENCE{
  versionIndex Version,
  accessCommand AccessCommand
}
Version:: = SEQUENCE{
  version INTEGER(0..15),
  fill BIT STRING(SIZE(4)) –0 fill
}
AccessCommand:: = CHOICE{
  dummy                                [0] NULL,
  operationCommand                    [1] OperationCommand,
  accreditationInfoCommand            [2] AccreditationInfoCommand,
  dummy                                [3–254] NULL,
  obuDenialResponse                   [255] ObuDenialResponse
}
operationCommand:: = SEQUENCE{
  opCommandType OpCommandType,
  opSecurityProfileOpSecurityProfile,
  opCommandBody OCTET STRING — Команда/реакция (см. [1])
}
OpCommandType:: = ENUMERATED{
  iCCCommand (0), — Отправить команду ICC
  reservedForFutureUse (1),
  endRequest (2),
  initRequest (3),
  reservedForFutureUse (4—127),
  iCCResponse (128), — Отправить реакцию ICC
  reservedForFutureUse (129),
  endResponse (130),
  initResponse (131),
  reservedForFutureUse (132—255)
}
```

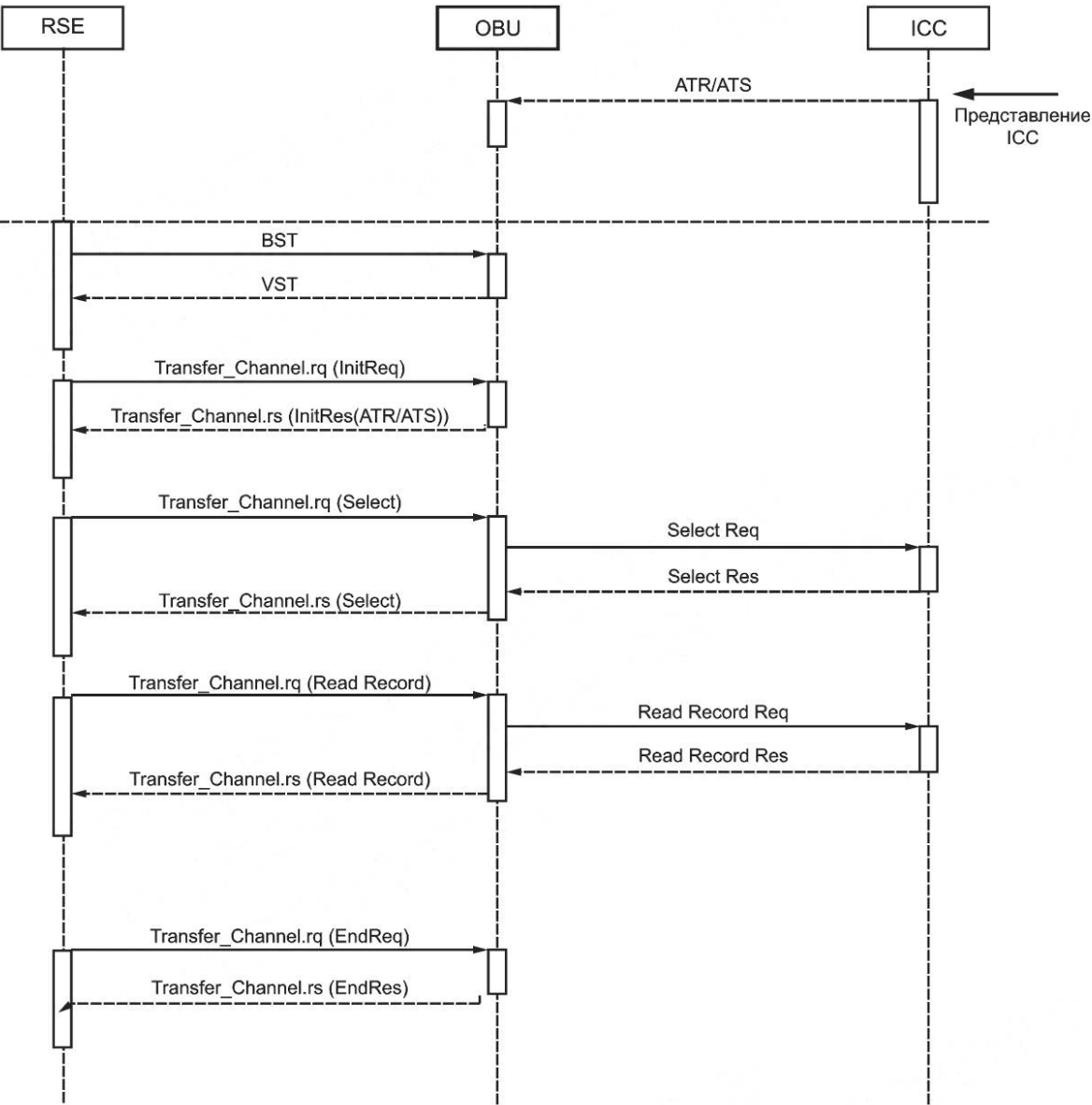
b) Определение содержимого APDU в TransferChannel.rs:

```
ICCAccessResponse:: = SEQUENCE{
  versionIndex Version,
  accessCommand AccessCommand
}
```

В.1.2.3 Транзакция. Парковочная система

а) Простая система (метод соединения по центру).

В этой системе плата за парковку должна проходить по номеру кредитной карты, зарегистрированной в центральной системе, в которой номер кредитной карты и номер участника связаны. Чтобы заключить договор о членстве и оплате, номер кредитной карты должен быть зарегистрирован в системе центра заранее (см. рисунок В.3).

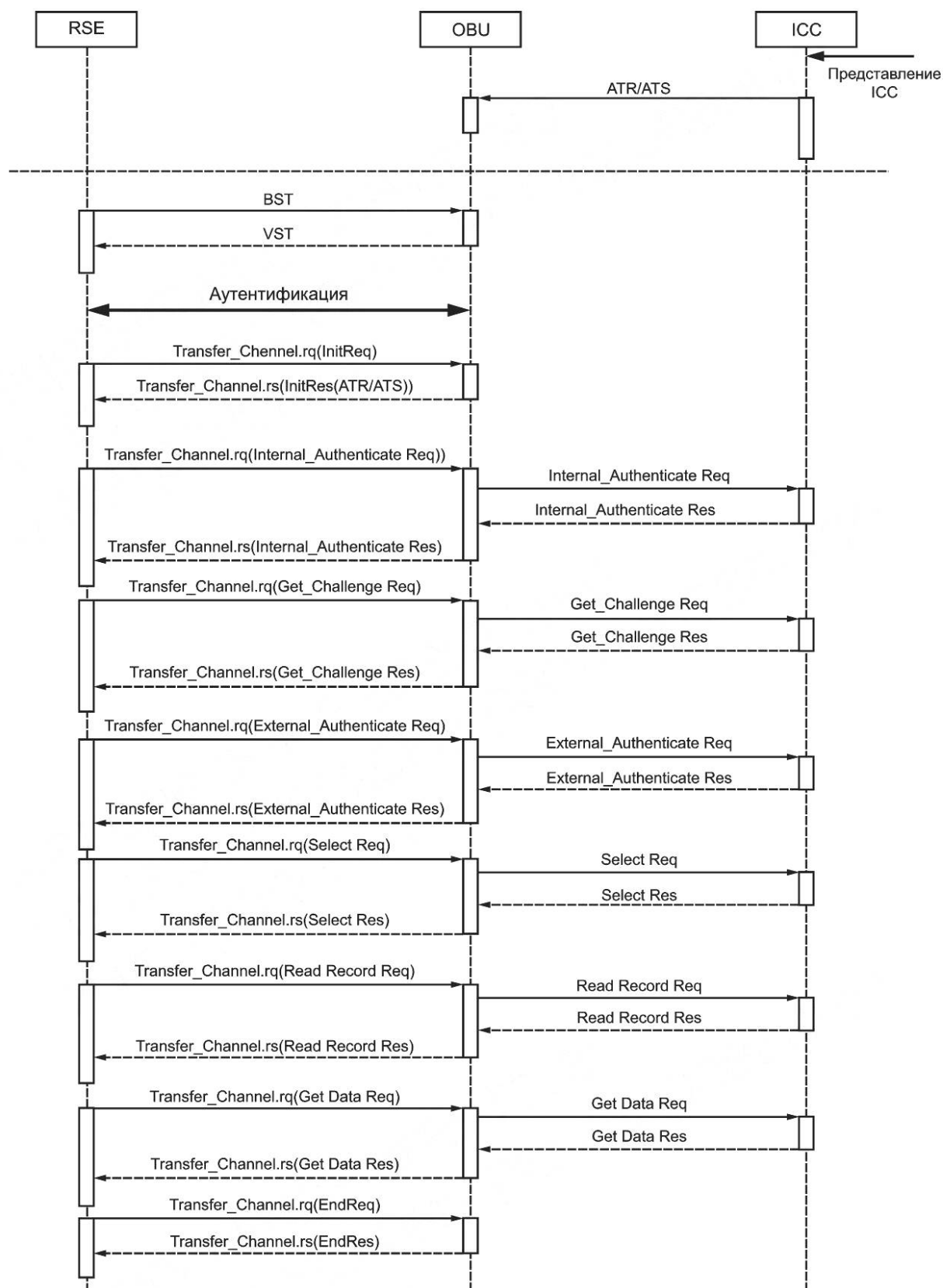


Примечание – Номер участника содержится в Read Record Res.

Рисунок В.3 — Последовательность операций простой системы (метод централизованной цепочки)

б) Комплексная система (прямой метод).

В этой системе плата за парковку должна проходить по номеру кредитной карты, считываемому непосредственно из кредитной карты ICC (см. рисунок В.4).



Примечание – Номер кредитной карты содержится в Read Record Res.

Рисунок В.4 — Последовательность выполнения сложной системы (прямой метод)

В.2 Модель типа кэширования

В.2.1 Обзор

В качестве примера модели типа кэширования описывается метод доступа ICC, используемый для японских ETC. В японской ETC распространение бортовых блоков основано на розничных продажах в автомагазинах, и любой производитель может участвовать на рынке бортового оборудования, получив одобрение от испытательного центра. Следовательно, для ICC и данных, связанных со сбором дорожных сборов, хранящихся в OBU, требуется высокий уровень обеспечения безопасности данных. Для этого бортовые блоки должны, на уровне изготовителя, оснащаться SAM, предоставленными сертифицированными производителями.

- Определение команды: определена стандартом интерфейса DSRC (ETC-B02230P) с использованием для ETC Японии.

- команда: TRANSFER_CHANNEL (см. [2]);
- AID: ЭСП как AID = 1 или многоцелевой платеж (MPP), определенный как AID = 14 (см. [2]);
- Тип ICC: контактный тип ICC для оплаты кредита.

Примечания

1 Причины, по которым SAM используется в японской ETC:

- для реализации механизма кэширования в бортовом блоке для обеспечения высокой производительности даже при использовании низкоскоростного ICC контактного типа;

- обеспечения совместимости в отношении приложения ETC и механизма безопасности между RSE и OBU. SAM содержит не только механизм безопасности, но и приложение ETC для выполнения процессов кэширования и обработки данных с помощью ICC;

- поддержания конкурентоспособности и быстрого распространения OBU по всей стране.

2 Пояснение к AID = 14:

- использование AID = 14 представлено в [2];
- AID, равный 14, определяет контекст многоцелевого платежа. Определение приложения для DSRS, используемого для многоцелевого платежа в Японии, представлено в [2].

В.2.2 Определение типа данных

а) Определение содержимого APDU в TransferChannel.rq:

```
RSECommand:: = SEQUENCE{
    eid                                Dsrc-EID,
    parameter OCTET STRING             - Параметр не включен в подкоманду
        (SIZE(0..255)),
    subCommandList                     - Список вспомогательных команд
        SEQUENCE(0..255)              OF
        SubCommand
}
SubCommand:: = CHOICE{
    dgetRq                            [0] DgetRq,
    dgetRs                            [1] DgetRs,
    dget_instanceRq                   [2] Dget_instanceRq,
    dget_instanceRs                   [3] Dget_instanceRs,
    dsetRq                            [4] DsetRq,
    dsetRs                            [5] DsetRs,
    dendRq                            [6] DendRq,
    dendRs                            [7] DendRs,
    dummy                             [8—31] NULL — Будущее использование
}
DgetRq:: = SEQUENCE{
    fill                              BIT STRING (SIZE(3)),
    attributeldList                   AttributeldList
}
}
```

```

DsetRq:: = vSEQUENCE{
    fill                BIT STRING (SIZE(2)),
    delete              BOOLEAN,
    attributeldList     AttributeldList,
    dataList            DataList
}
DataList:: = SEQUENCE(0..255) OF Data
Data:: = OCTET STRING(1..255)
AttributeldList:: = SEQUENCE(0..255) OF attributeld
attributeld:: = INTEGER(0..127,...)
    
```

b) Определение содержимого APDU в TransferChannel.rs:

```

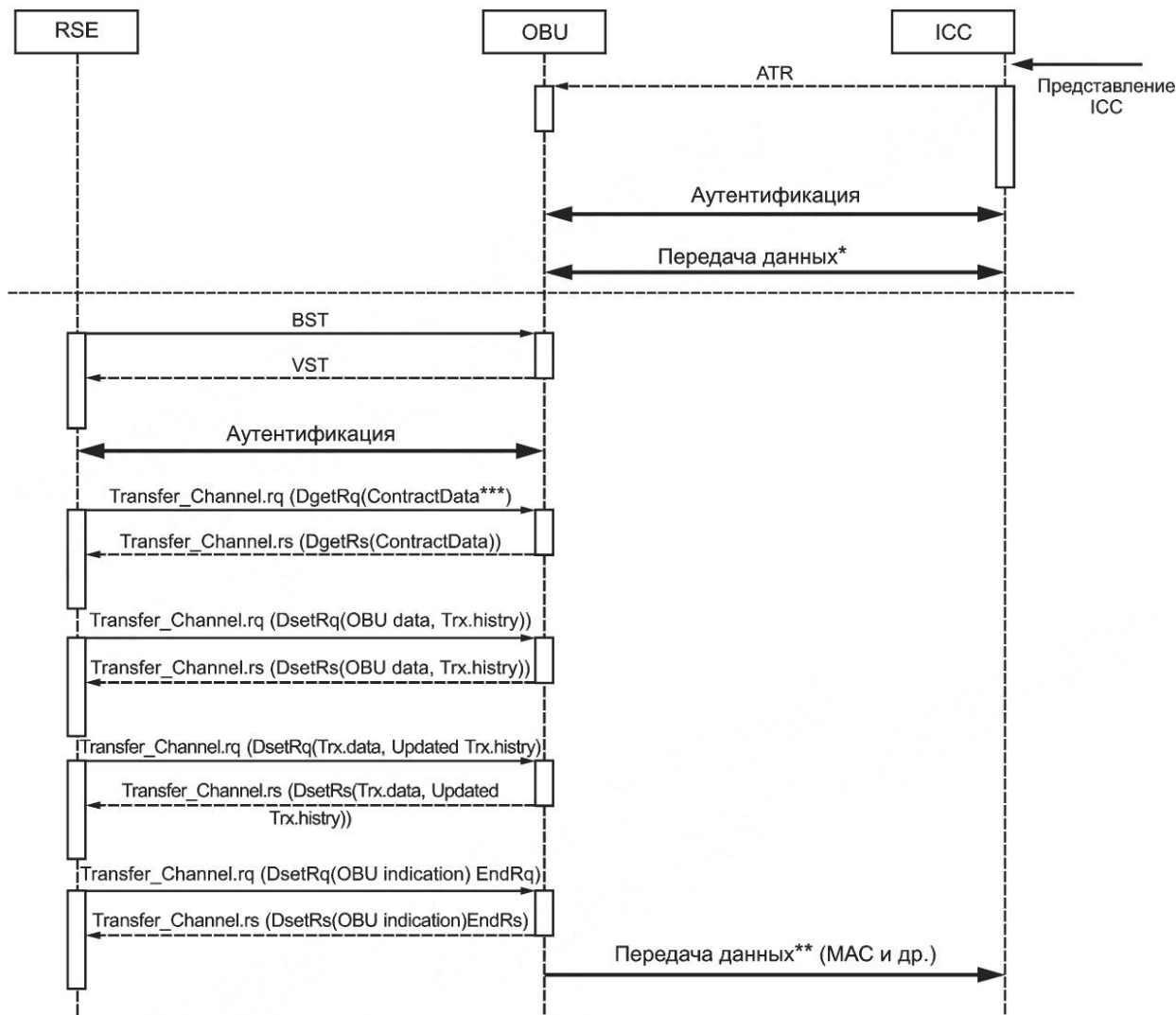
RSECommand:: = SEQUENCE{
    eid                Dsrc-EID,
    parameter OCTET STRING (SIZE(0..255)),
    subCommandList SEQUENCE(0..255) OF SubCommand
}
DgetRs:: = SEQUENCE{
    fill                BIT STRING (SIZE(3)),
    ret                INTEGER(0..255),
    dataList            DataList
}
DsetRs:: = SEQUENCE{
    fill                BIT STRING (SIZE(3)),
    ret                INTEGER(0..255),
}
    
```

- Параметр не включен в подкоманду

- Список вспомогательных команд

В.2.3 Пример транзакции

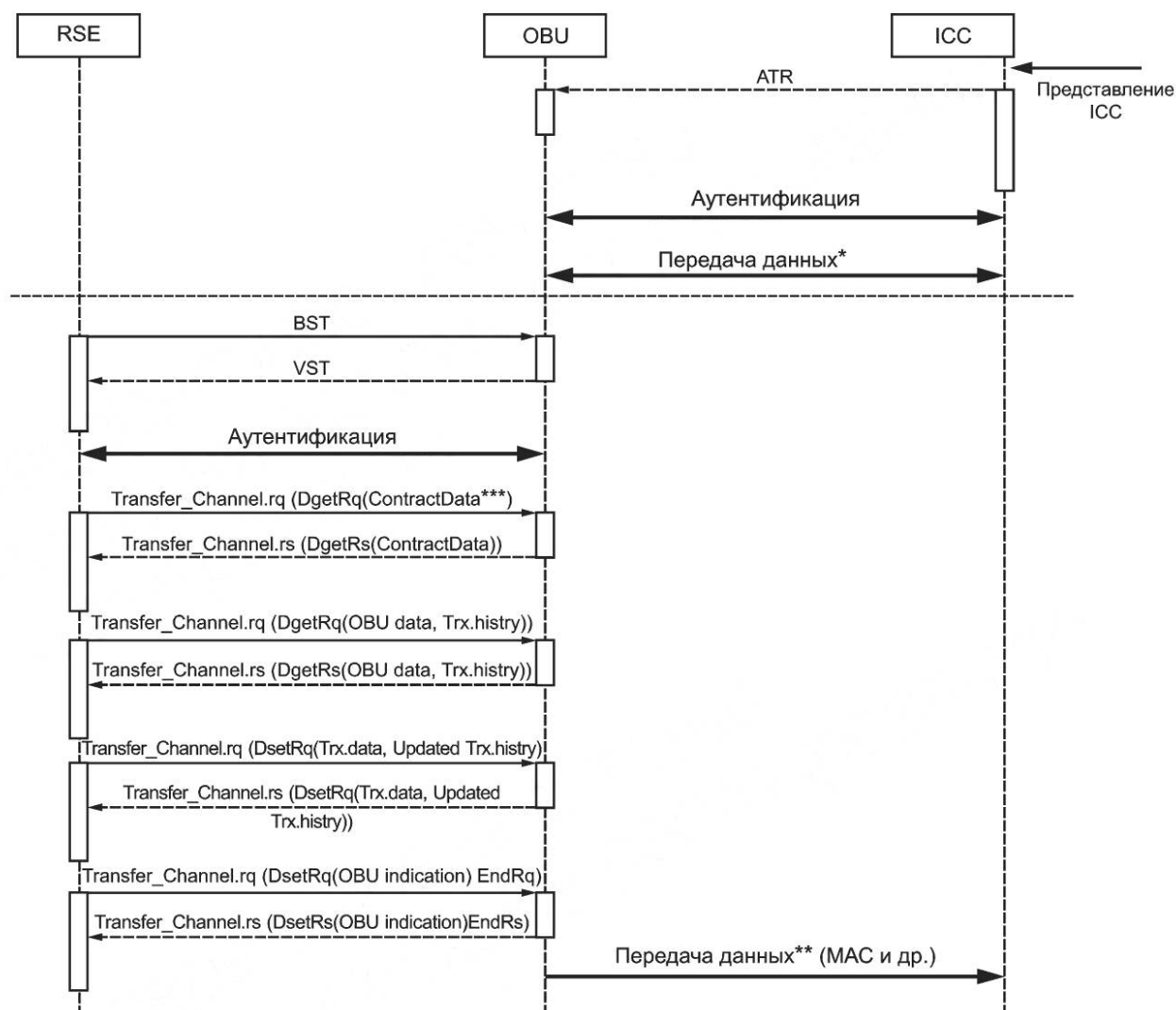
В.2.3.1 ЕТС по фиксированной ставке (открытая система) и оплата в кредит
См. рисунок В.5.



*Указанные наборы данных ICC передаются в OBU после данных контракта представления ICC, данных истории транзакций (история Trx).
** Указанные наборы данных передаются в ICC после завершения данных транзакции DSRC (Trx.), данных истории транзакции (Trx).
***Номер карты IC включен.

Рисунок В.5 — Последовательность взимания фиксированной ставки ETC (открытая система) и оплаты кредита

В.2.3.2 Тарифы на расстояние ETC (закрытая система) и оплата в кредит
а) Входящая транзакция.
См. рисунок В.6.



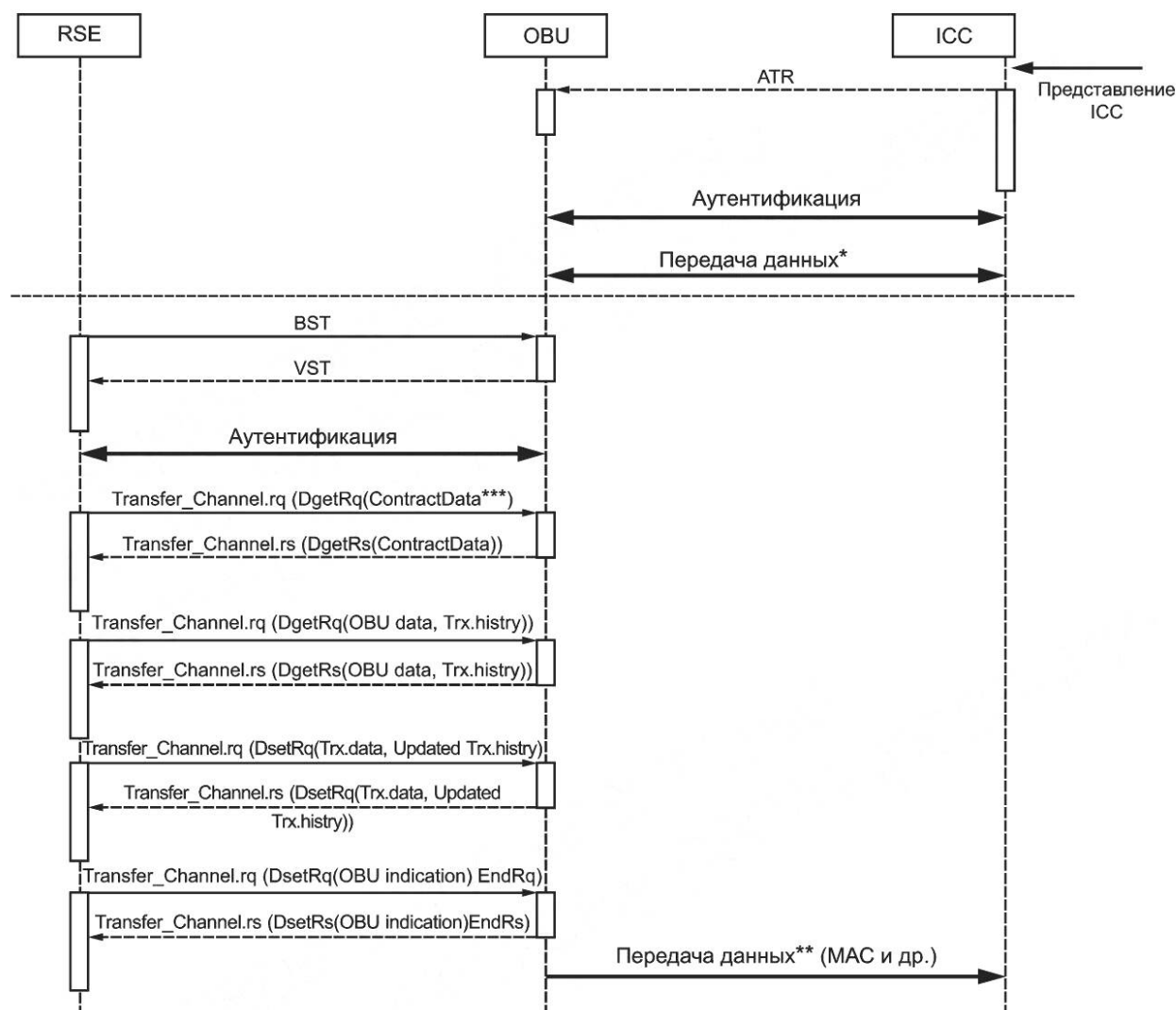
*Указанные наборы данных ICC передаются в OBU после данных контракта представления ICC, данных истории транзакций (история Trx).

** Указанные наборы данных передаются в ICC после завершения данных транзакции DSRC (Trx.), данных истории транзакции (Trx).

***Номер карты IC включен.

Рисунок В.6 — Последовательность входящей транзакции

b) Исходящая транзакция.
См. рисунок В.7.



*Указанные наборы данных ICC передаются в OBU после данных контракта представления ICC, данных истории транзакций (история Trx).

** Указанные наборы данных передаются в ICC после завершения данных транзакции DSRC (Trx.), данных истории транзакции (Trx).

***Номер карты IC включен.

Рисунок В.7 — Последовательность исходящий транзакции

В.3 Модель типа буферизации

В.3.1 Обзор

В качестве примера модели типа буферизации представлен метод доступа ICC, используемый в корейской ETC. В корейских ETC гибридный тип ICC используется не только для ETC, но и в случае, когда водитель может проехать по платной полосе, прикоснувшись своим ICC к придорожному считывателю:

- определение команды: определено корейскими стандартами ETC;
- команда: инициализация, действие (дебет, безопасная установка), получение и выпуск *представлены в [2]*;
- AID: ЭСП как AID = 1 (см. [14]);
- тип ICC: гибридная карта с предоплатой.

В.3.2 Определение команды RSE. Команда дебетования

В данном случае в ActionParameter включены данные для команды ICICI Debit (S2, PSAM ID и т. д.).

Применительно для одноразового номера:

nonce:: = SEQUENCE{

length OCTET STRING (SIZE(1)), — длина одноразового номера

PPSAM OCTET STRING (SIZE(3)), — PSAM ID-провайдера

PSAM OCTET STRING (SIZE(8)), — PSAM ID

NTPSAM OCTET STRING (SIZE(4)), — PSAM номера транзакции

S2 OCTET STRING (SIZE(4)), — подпись S2

RFU OCTET STRING (SIZE(5)), — зарезервировано для использования в будущем

}

Применительно для debitAuthenticator:

debitAuthenticator:: = SEQUENCE{

parameterLen OCTET STRING (SIZE(1)), — длина S3

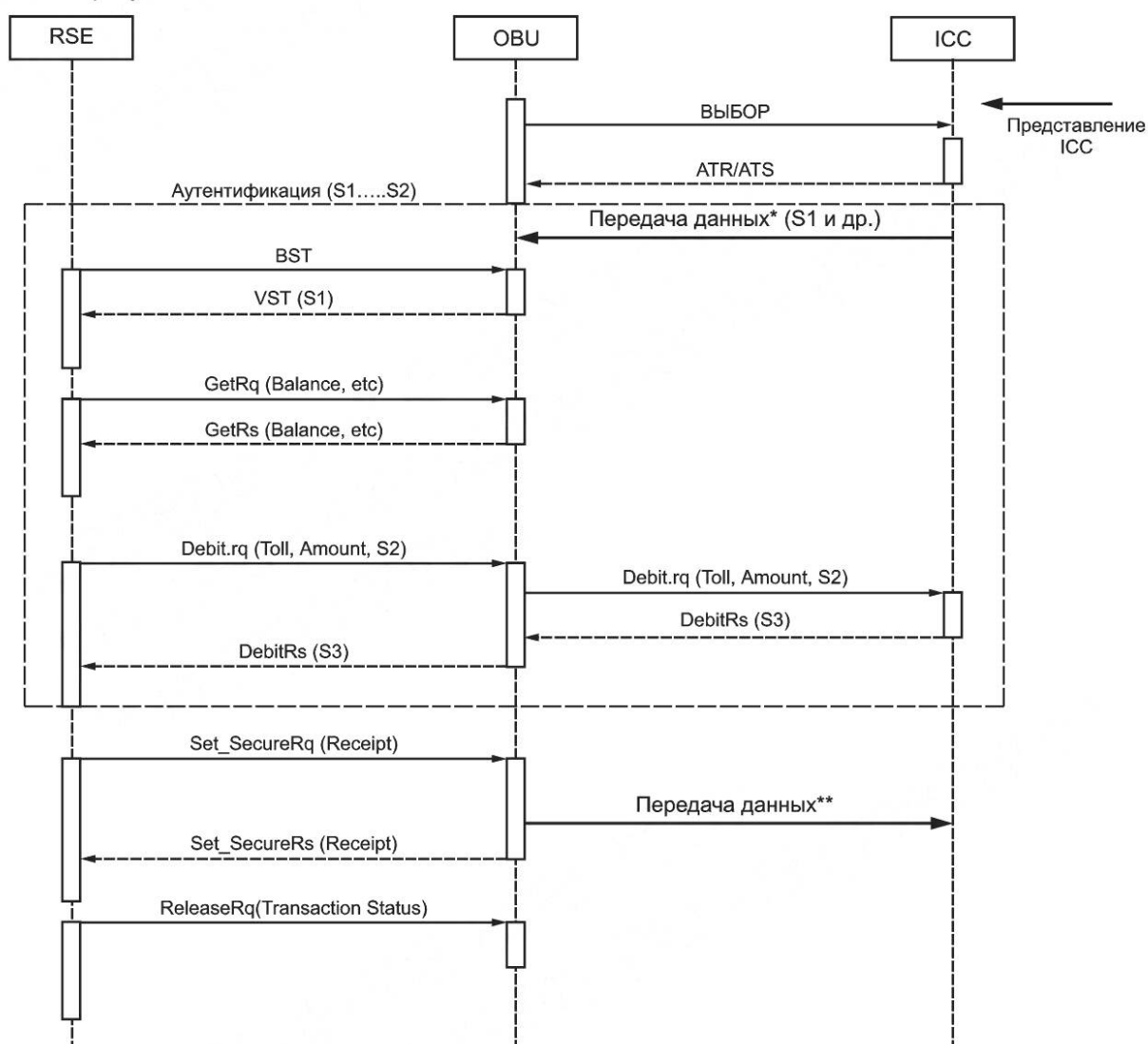
S3 OCTET STRING (SIZE(4)) — подпись S3

}

В.3.3 Транзакция

а) Алгоритм быстрой транзакции ETC и предоплата.

См. рисунок В.8.



* Указанные наборы данных ICC передаются в OBU после данных баланса представления ICC, информации о карте. Затем генерируются и передаются в OBU начальные данные аутентификации ICC (S1).

** Данные приема успешно записываются в ICC только после проверки MAC, сгенерированного SAM

Рисунок В.8 — Алгоритм быстрой транзакции ETC и предоплаты

Приложение С
(справочное)

Модели взаимодействия платежного сервиса с другими сервисами

На рисунке С.1 показано отношение эксплуатационной совместимости, при котором коды ICC, выпущенные для ЭСП, необходимо использовать для приложений общественного транспорта и/или розничной торговли.

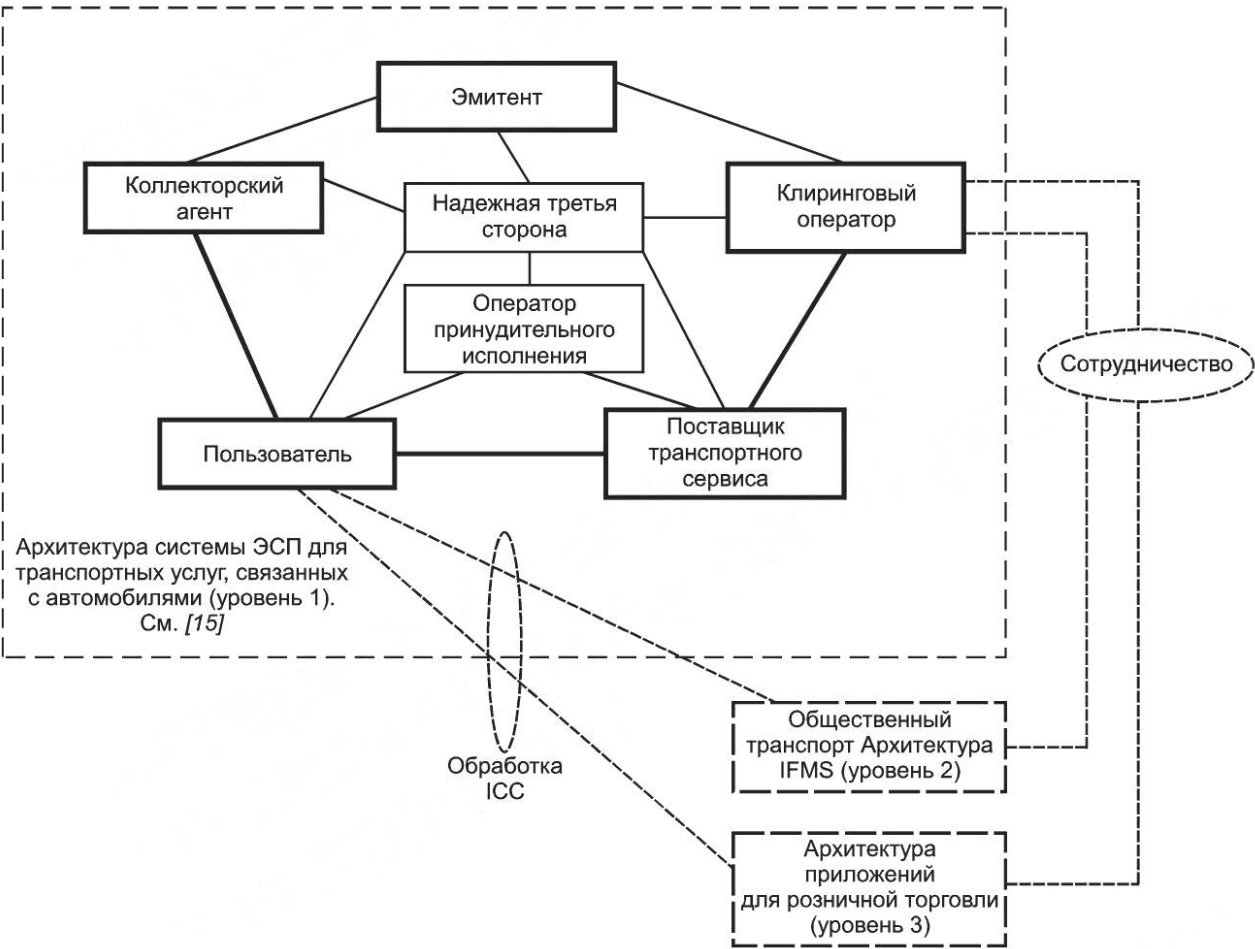


Рисунок С.1 — Модель взаимодействия сервиса ЭСП с другими сервисами

На рисунке С.2, напротив, показаны другие отношения оперативной совместимости, в которых коды ICC, выдаваемые для общественного транспорта, рассматриваются как портативные электронные носители либо при использовании ЭСП в розничной торговле в качестве платежного средства.

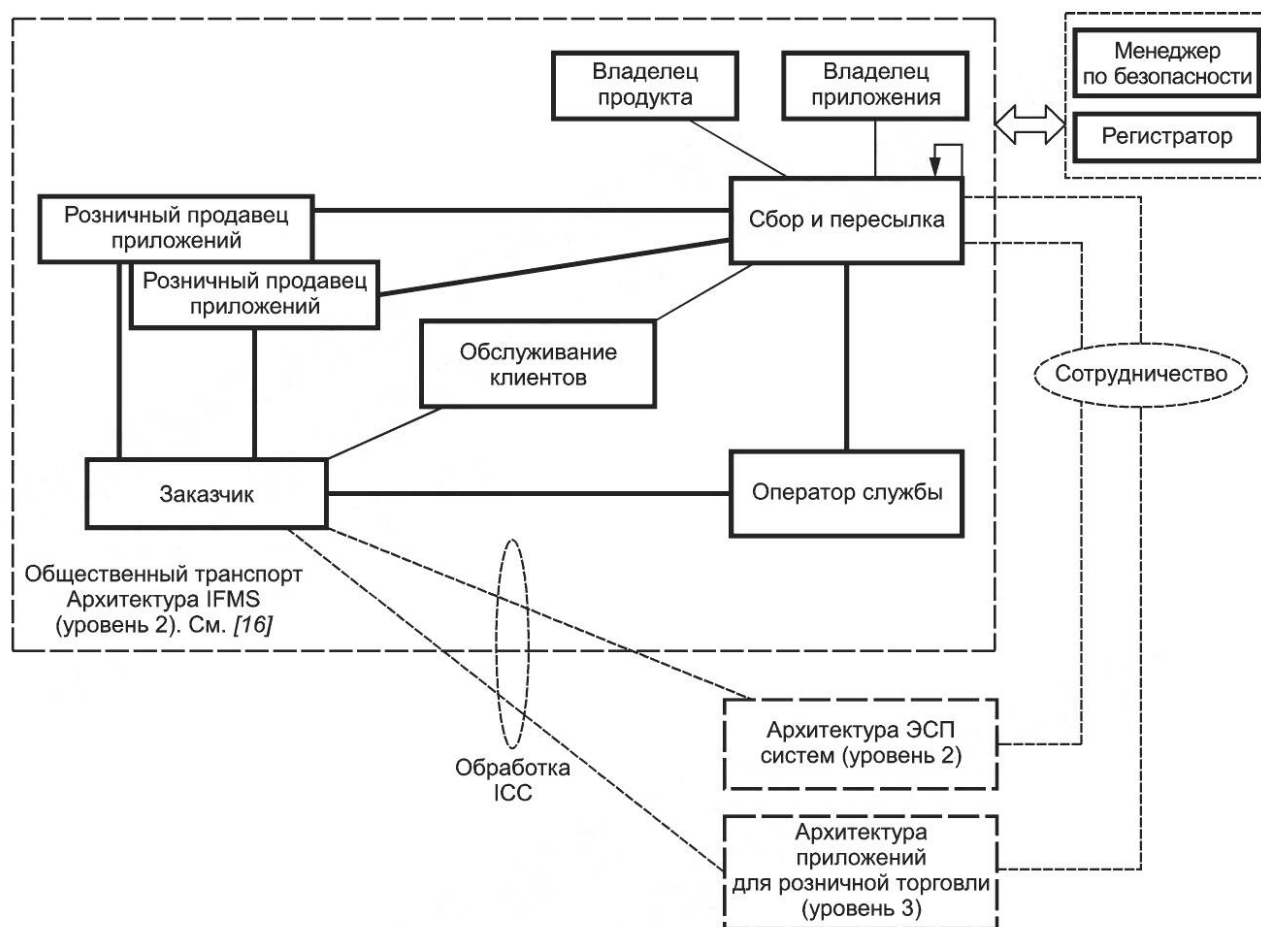


Рисунок С.2 — Модель взаимодействия сервиса IFMS с другими сервисами

Библиография

- [1] ИСО/МЭК 7816-4 Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 4. Организация, защита и команды для обмена
- [2] ИСО 14906 Электронный сбор платежей. Определение прикладного интерфейса для выделенной связи ближнего действия
- [3] ИСО/МЭК 15408-1 Информационные технологии. Методы безопасности. Критерии оценки безопасности ИТ. Часть 1. Введение и общая модель (ISO/IEC 15408-1:2009)
- [4] ИСО/МЭК 15408-2 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности
- [5] ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки защиты
- [6] ИСО/МЭК 7816-1 Удостоверения личности. Карты интегральной схемы (схем) с контактами. Часть 1. Физические характеристики
- [7] ИСО/МЭК 7816-2 Идентификационные карточки. Карточки интегральной схемы. Часть 2. Карты с контактами. Размеры и расположение контактов
- [8] ИСО/МЭК 7816-3 Удостоверения личности. Карты интегральной схемы. Часть 3. Карты с контактами. Интерфейс Electrical и протоколы передачи
- [9] ИСО/МЭК 14443-1 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты ближнего действия. Часть 1. Физические характеристики
- [10] ИСО/МЭК 14443-2 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты ближнего действия. Часть 2. Радиочастотный энергетический и сигнальный интерфейс
- [11] ИСО/МЭК 14443-3 Удостоверения личности. Карты на интегральных схемах бесконтактные. Карты ближнего действия. Часть 3. Инициализация и антистолкновение
- [12] ИСО/МЭК 14443-4 Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты ближнего действия. Часть 4. Протокол передачи
- [13] ИСО/МЭК 18092 Информационные технологии. Телекоммуникации и обмен информацией между системами. Коммуникации в ближнем поле. Интерфейс и протокол
- [14] ИСО 15628 Дорожный транспорт и телематика на транспорте. Специализированная связь на коротких расстояниях (DSRC). Прикладной уровень DSRC
- [15] ИСО 17573 Автоматический сбор платежей. Архитектура систем для взимания платы за проезд транспортных средств
- [16] ИСО 24014-1 Транспорт общественный. Система менеджмента тарифов, взаимодействующая с другими системами. Часть 1. Архитектура

УДК 004.73:006.354

ОКС 35.240

Ключевые слова: интеллектуальные транспортные системы, бортовое оборудование, автомобильный транспорт, интерфейс

Редактор *М.В. Митрофанова*
Технический редактор *В.Н. Прусакова*
Корректор *И.А. Королева*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 01.12.2023. Подписано в печать 15.12.2023. Формат 60×84 $\frac{1}{8}$. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,35.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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

