ФЕДЕРАЛЬНОЕ АГЕНТСТВО ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ

Интеллектуальные транспортные системы

Электронный сбор платежей — Определение интерфейса для бортовой учетной записи с использованием карты с интегральной схемой

(ISO 25110:2017, MOD)

Издание официальное

Москва
Российский институт стандартизации
2023

Предисловие

1 ПОДГОТОВЛЕН Инфраструктурным центром Московского Политеха с привлечением творческого коллектива специалистов кафедры «Правовое и таможенное регулирование на транспорте» 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 2023 г. №

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО 25110:2017 «Электронный сбор платежей — Определение интерфейса для бортовой учетной записи с использованием карты с интегральной схемой (ICC)» (ISO 25110:2017, «Electronic fee collection — Interface definition for on-board account using integrated circuit card (ICC)» 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.

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)

Содержание

1 Область применения	1
2 Нормативные ссылки	4
3 Термины и определения	4
4 Сокращения	6
5 Модели передачи данных	6
6 Определение интерфейса для доступа к карте с интегральной схемой	11
Приложение А	16
Приложение Б	20
Приложение В	35
Библиография	37

Введение

Электронный сбор платежей (EFC) осуществляется по технологии, связанной с центральной системой учета, использующей бортовой блок (OBU), а также в рамках бортовой системы учета, использующей такие платежные средства, как карта с интегральной схемой (ICC).

Карты ICC широко используются для карт общественного транспорта, таких как средства оплаты метро и автобусов, карты электронных денег для платежей общего назначения, а также для кредитных и банковских карт. Ожидается, что ICC будет использоваться для платежных средств EFC наряду с этими глобальными тенденциями и обеспечит удобство и гибкость.

В настоящее время описания в существующих международных стандартах, связанных с EFC, сосредоточены на центральной системе счетов, которая довольно проста и дает больше возможностей для взаимодействия EFC, чем бортовая учетная запись, которая сложна и требует урегулирования большего количества вопросов.

Принимая во внимание широкое использование транспортных карт и банковских карт, требуется новый международный стандарт, касающийся бортовой системы учета с использованием ICC, как показано на рисунке 1. Кроме того, современный мобильный телефон интегрирован с функциями ICC, так называемый «мобильный электронный кошелек», используется для общественного транспорта или розничных покупок в качестве средства оплаты во многих странах, что подтверждает важность стандартизация данного направления и необходимость для рассмотрения будущих способов оплаты EFC.

Рисунок 1 – Схема работы бортового аккаунта с помощью ICC

На рисунке 2 показан стандарт EFC, в которых OBU используется в качестве средства связи, а ICC несет средства оплаты.

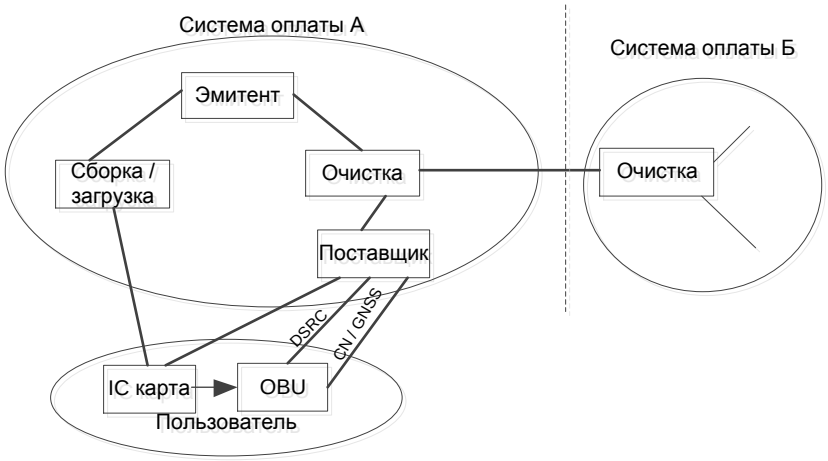


Рисунок 2 – Области применения стандартов EFC

Целью настоящего стандарта является классификация моделей передачи данных на основе эксплуатационных требований и определение конкретного интерфейса доступа ICC для бортовых учетных записей с использованием ICC для каждой модели. Кроме того, настоящего стандарта предоставляет практические примеры транзакций в Приложении Б.

Настоящий стандарт обеспечивает общую техническую платформу для бортовых учетных записей с использованием ICC для решения различных операционных требований и практических

примеров бортовых учетных записей, которые фактически используются или планируются в нескольких странах.

Каждый оператор платных дорог может установить свою собственную спецификацию, выбрав пример модели в настоящем стандарте в соответствии со своими требованиями.

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Интеллектуальные транспортные системы Электронный сбор платежей — Определение интерфейса для бортовой учетной записи с использованием карты с интегральной схемой

Electronic fee collection — Interface definition for on-board account using integrated circuit card

Срок действия __ с 2023– –

до 2026 – –

1 Область применения

В настоящим стандарте определены модели передачи данных между придорожным оборудованием (RSE) и картой с интегральной схемой (ICC), а также описания интерфейсов между RSE и бортовым оборудованием (OBE) для бортовых учетных записей с использованием ICC. Он также предоставляет примеры определений интерфейсов и транзакций, развернутых в нескольких странах.

Настоящий стандарт рассматривает:

— модели передачи данных между RSE и ICC, которые соответствуют категорированным эксплуатационным требованиям и механизму передачи данных для каждой модели;

— определение интерфейса между RSE и OBE на основе каждой модели передачи данных;

— *определение интерфейса для каждой модели;*

— *функциональная конфигурация;*

— определения команд RSE для доступа к ICC;

— формат данных и определения элементов данных команд RSE;

— пример транзакции для каждой модели в Приложении Б.

На рисунке 3 показана конфигурация бортовой учетной записи и

настоящего стандарта. Описания в настоящем стандарте сосредоточены на интерфейсе между RSE и OBU для доступа к ICC.

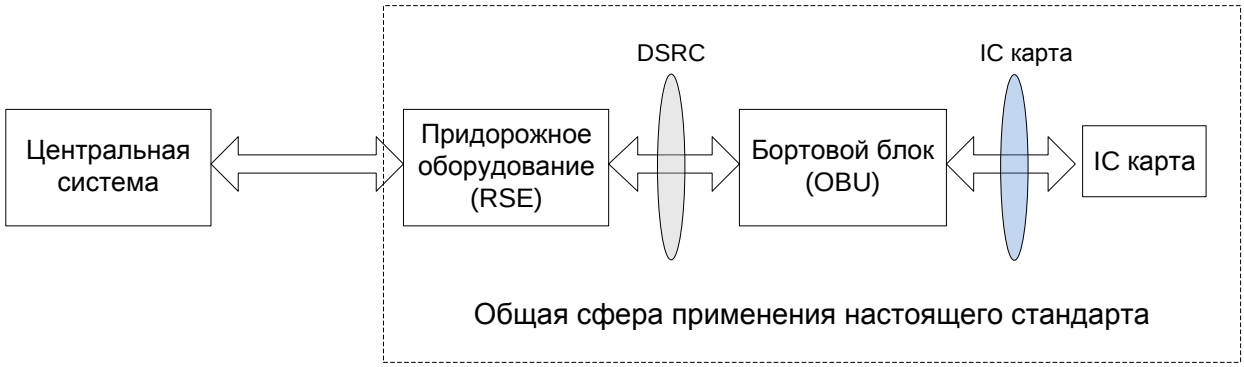


Рисунок 3 – Конфигурация бортовой учетной записи и сфера действия настоящего стандарта

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, выходят за рамки 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.

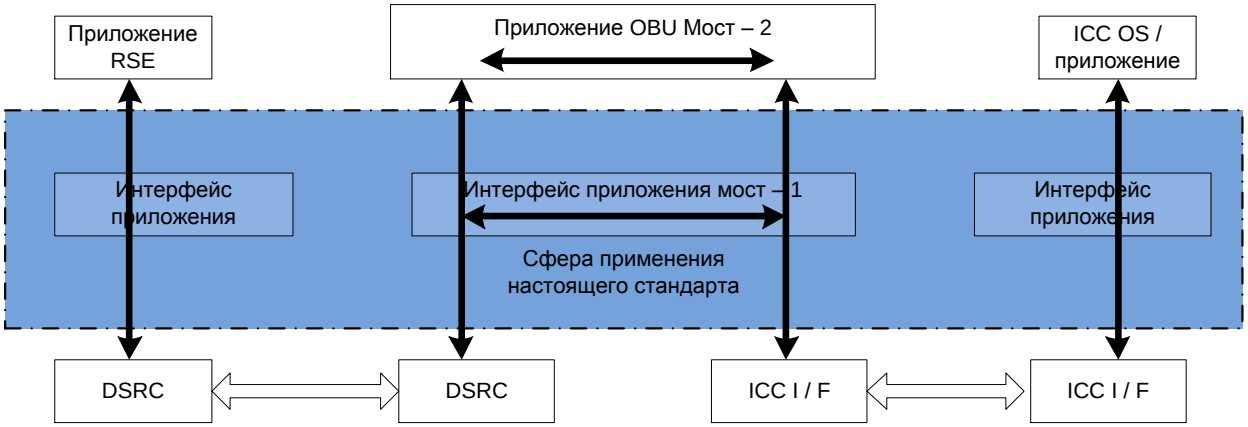


Рисунок 4 – Прикладные интерфейсы RSE, OBU и ISS и область применения настоящего стандарта

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт:

ГОСТ Р 56829 Интеллектуальные транспортные системы. Термины и определения

ГОСТ Р 58833-2020 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 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 (OBE):*** *Все необходимое*

оборудование на борту транспортного средства для выполнения требуемых функций EFC и услуг связи

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

3.5 ***группа данных:*** *Класс тесно связанных атрибутов*

3.6 ***канал:*** *путь передачи информации*

3.7 ***криптография:*** *Принципы, средства и методы преобразования данных, чтобы скрыть их информационное содержание, с целью предотвращения их несанкционированного использования*

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

3.9 **модуль безопасного приложения (SAM):** 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 OBE. Учетные данные для доступа могут содержать пароли, а также информацию на основе криптографии, такую как аутентификаторы.

3.14 **целостность данных:** Данные, которые не были изменены

или уничтожены несанкционированным образом

3.15 **элемент:** <DSRC> каталог, содержащий информацию о приложении в виде атрибутов

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

4 Сокращения

AID – идентификатор приложения;
APDU – единица данных протокола приложения;
ASN.1 – нотация абстрактного синтаксиса;
BST – таблица обслуживания маяка;
DSRC – выделенная связь ближнего действия;
EAL – уровень гарантии оценки;
EFC – электронный сбор платежей;
EID – идентификатор элемента;
ERP – электронное дорожное ценообразование;
EVENT-RT – отчет события;
ICC – карта с интегральной схемой;
IFMS – совместимая система управления тарифами;
OBE – бортовое оборудование.

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 (рисунок 5).

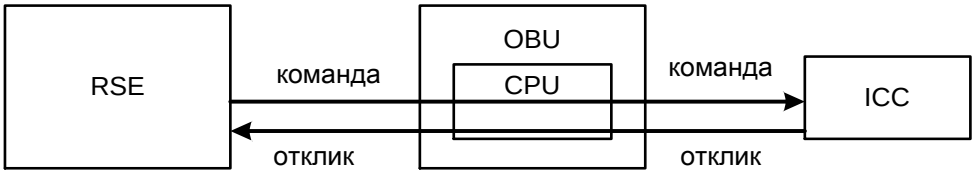


Рисунок 5 – Типовая структура прозрачного типа

5.1.2 Тип кеширования

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

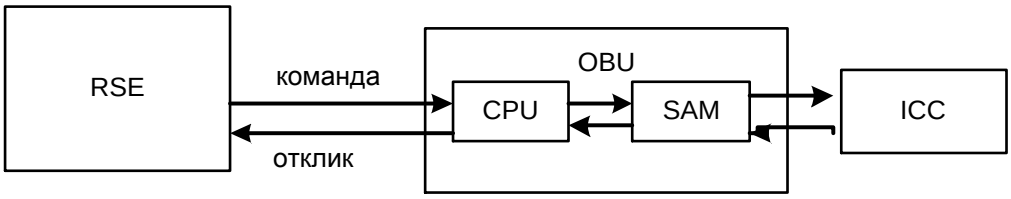


Рисунок 6 – Общая структура типа кэширования

5.1.3 Тип буферизации

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

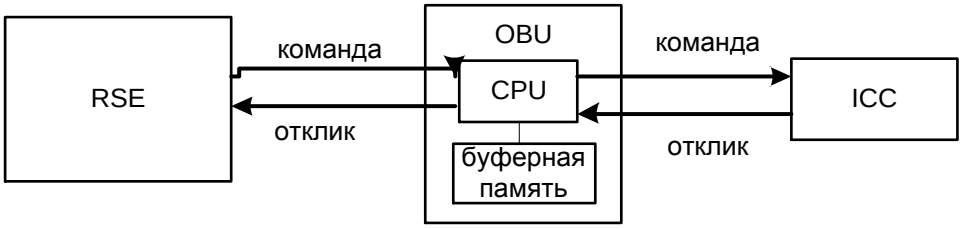


Рисунок 7 – Общая структура типа буферизации

5.2 Символы

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

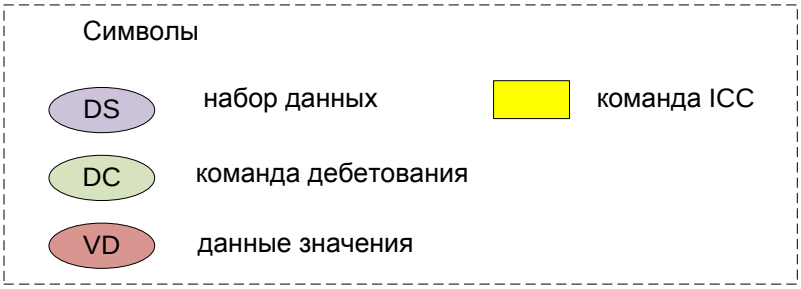


Рисунок 8 – Определение символов

5.3 Прозрачный режим

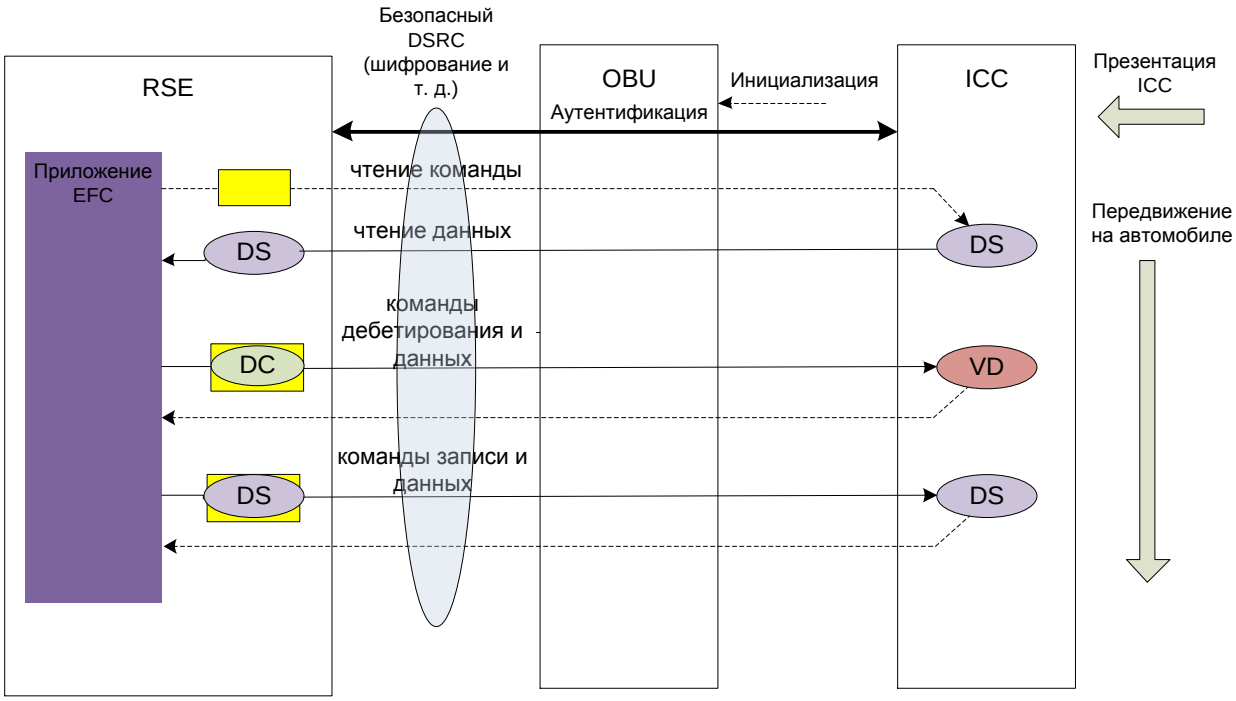
5.3.1 Обзор

В этой модели максимальная скорость транспортного средства зависит от скорости передачи данных между ICC и бортовым блоком, так что транспортное средство должно останавливаться 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.



* Команда «Дебет» используется в случае предоплаты.

Рисунок 9 – Процесс передачи данных

5.4 Тип кеширования

5.4.1 Обзор

В 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 (рисунок 10).

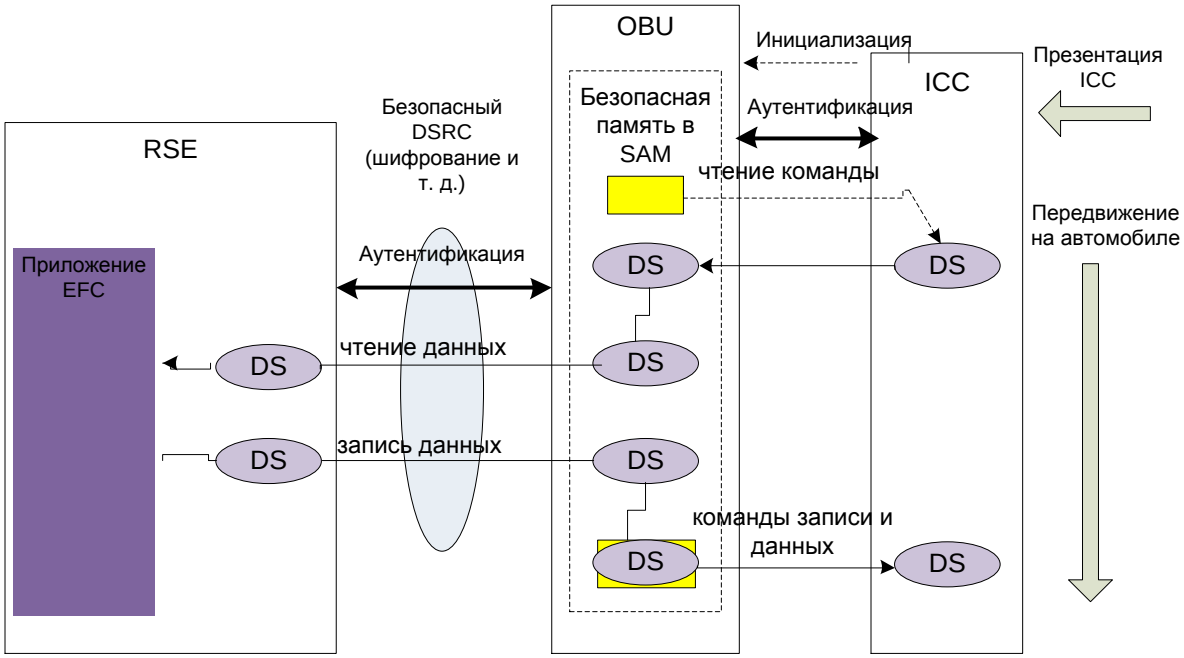


Рисунок 10 – Процесс передачи данных

5.5 Тип буферизации

5.5.1 Обзор

Наборы данных, хранящиеся в ICC, ограничиваются неконфиденциальными 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 в бортовом блоке и использовать даже низкоскоростной ICC (рисунок 11).

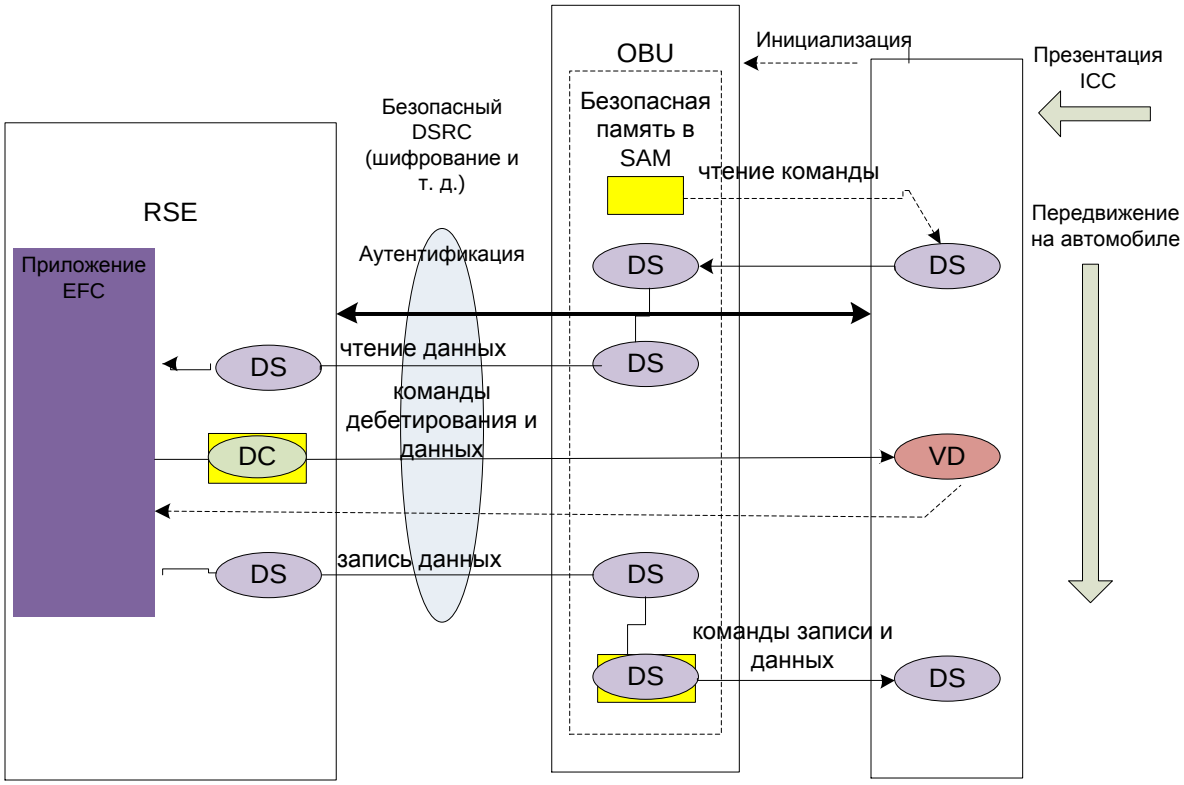


Рисунок 11 – Процесс передачи данных типа буферизации

6 Определение интерфейса для доступа к карте с интегральной схемой

6.1 Прозрачный режим передачи данных

6.1.1 Функциональная конфигурация

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

Определение команд между OBU и ICC должно основываться на ИСО / МЭК 7816-4.

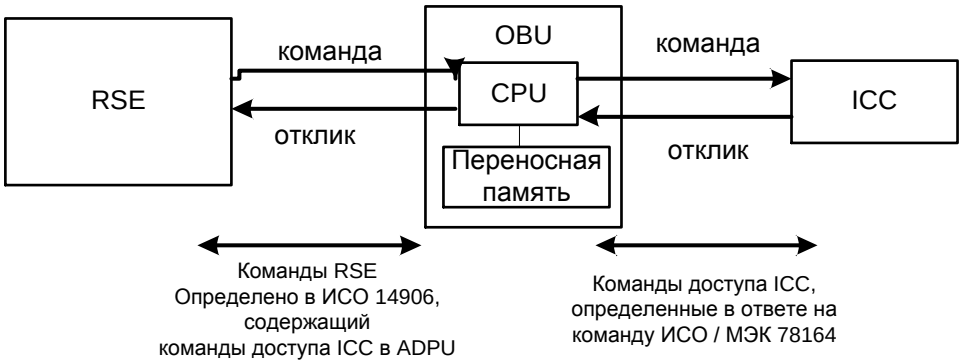


Рисунок 12 – Процесс передачи данных типа буферизации

6.1.2 Команды и ответ между RSE и OBU

Канал передачи, определенный в ИСО 14906, 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.

Таблица 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.

Таблица 2 – Ответ TRANSFER_CHANNEL

Параметр	Тип ASN.1	Значение	Примечания
Параметр ответа	ChannelRq:: = 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 кеширования

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 ADPU для чтения наборов данных, кэшированных в SAM. Определение команды между SAM и ICC должно основываться на ИСО / МЭК 7816-4.

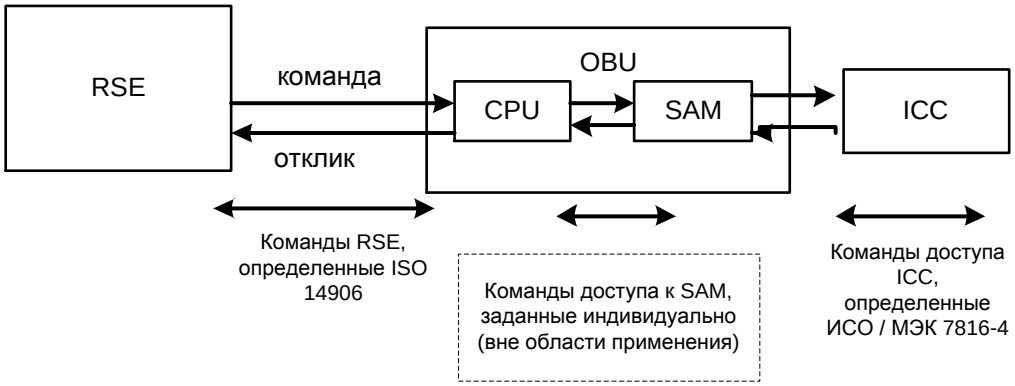


Рисунок 13 – Процесс передачи данных типа буферизации

6.2.2 Команды и ответ между RSE и OBU

Канал передачи, определенный в ИСО 14906, 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	ChannelRq:: = 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.

Определение команд между OBU и ICC должно основываться на ИСО / МЭК 7816-4.

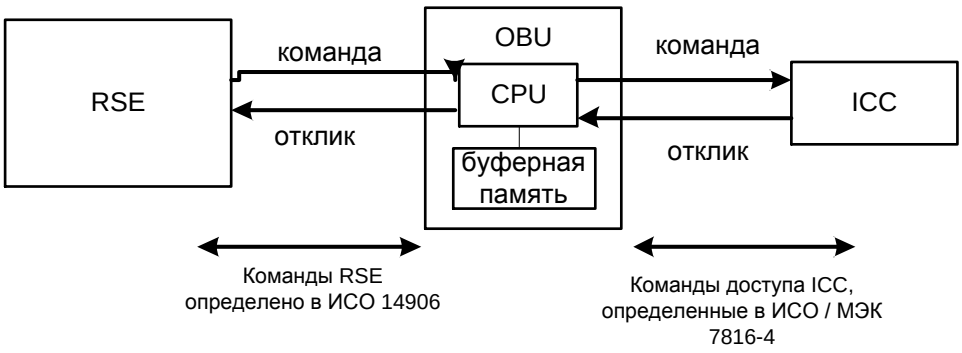


Рисунок 14 – Процесс передачи данных типа буферизации

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 EFC,

определенной в ИСО 14906. 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 дебетования для ICC.

Таблица 6 – Ответ DEBIT

Параметр	Тип ASN.1	Значение	Примечания

Параметр ответа	ChannelRq:: = SEQUENCE {
	channelId ChannelId,
	APDU OCTET STRING
	}
			Присутствует всегда

Код возврата (Ret)	Статус возврата		Дополнительное использование

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

Приложение А
(информационное)
Требования к бортовой учетной записи

А.1 Операционные требования к бортовой учетной записи

Основными факторами эксплуатационных требований к EFC являются скорость транспортного средства и уровень информационной безопасности, как показано на рисунке А.1, которые в значительной степени влияют на конструкцию системы EFC. Уровни информационной безопасности на рисунке А.1, называемые уровнями гарантии оценки (EAL), определены в серии стандартов ИСО 15408.

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 EFC 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 EFC в одной полосе движения. Категория 3 охватывает Категория 2 и EFC / ERP в многополосном свободном потоке, когда автомобиль проезжает на высокой скорости.*

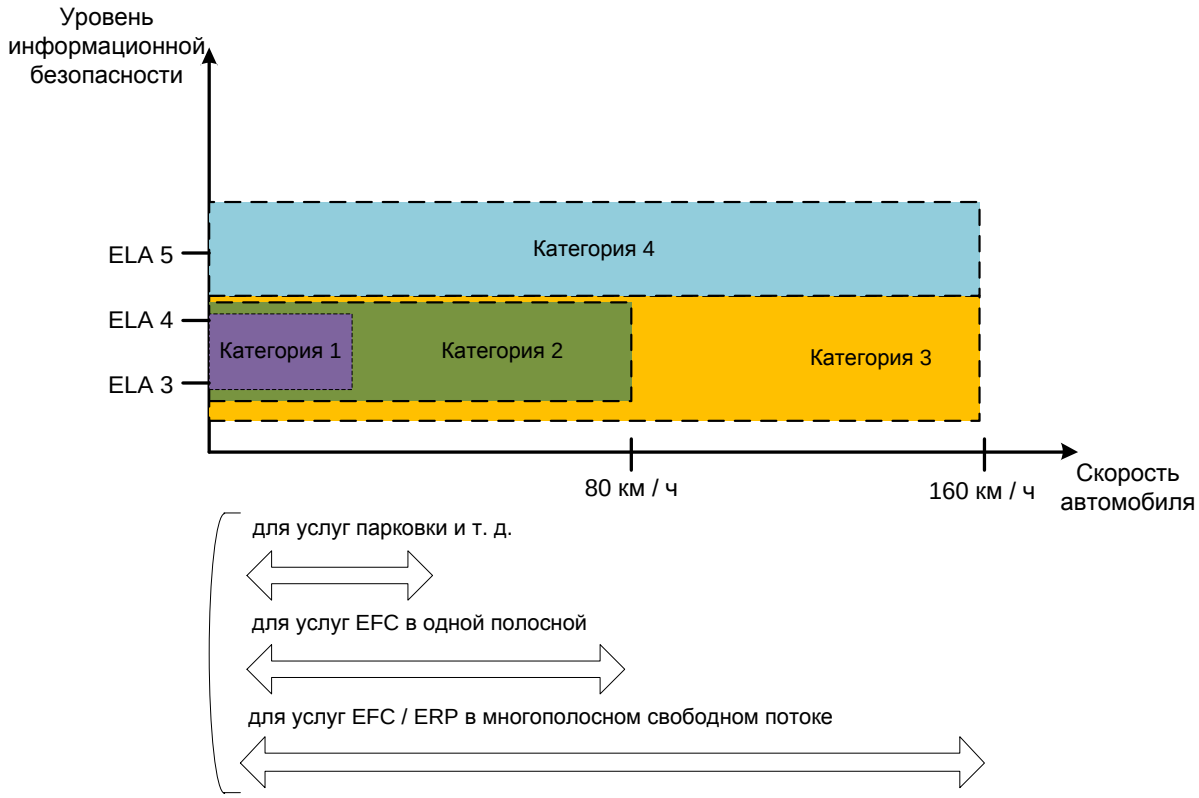


Рисунок А.1 – Эксплуатационные требования

А.2 Типы ICC

ICC, используемый для бортовых учетных записей, классифицируется, как показано на рисунке А.2. Тип контакта ICC на основе серии ИСО / МЭК 7816 в основном используется для финансовых карт, таких как банковские и кредитные карты. Бесконтактный ICC, основанный на серии ИСО / МЭК 14443 или ИСО / МЭК 18092, широко используется в секторе общественного транспорта в качестве средства оплаты и для продажи билетов. Гибридный тип ICC имеет обе функции, определенные серией ИСО / МЭК 7816 и серией ИСО / МЭК 14443 или ИСО / МЭК 18092, а также используется для многофункциональных карт, таких как EFC и карты общественного транспорта.

Есть несколько вариантов, когда ICC используется для EFC. Один из вариантов - использовать его только для оплаты. Другой вариант - использовать его как для оплаты, так и для хранения данных,

связанных с EFC.

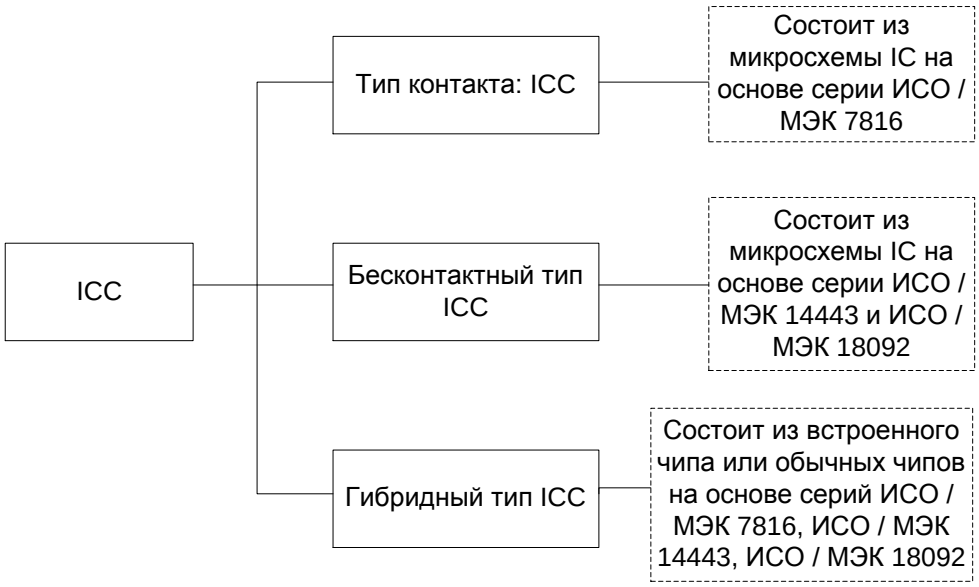


Рисунок А.2 – Типы карт IC

А.3 Требования к взаимодействию для ICC

Для обеспечения безопасности и передачи данных от ICC потенциально требуется, чтобы он имел 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. Расширена функциональная совместимость 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 EFC и архитектурой IFMS общественного транспорта.

В Приложении В показаны отношения оперативной совместимости, когда коды ICC, выпущенные для EFC, 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 кеширования	Тип буферизации
Категория 1	×		
Категория 2	×		
Категория 3	×		×
Категория 4		×	

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

Приложение Б
(информационное)
Пример применения метода доступа ICC

Б.1 Модель с прозрачным шрифтом

Б.1.1 Модель 1 прозрачного типа (для предоплаты)

Б.1.1.1 Общее

В качестве примера модели прозрачного типа 1, доступ к ICC осуществляется с помощью функции канала передачи, определенной в ИСО 14906.

- Команда: TRANSFER_CHANNEL определена ИСО 14906
- AID: Электронный сбор платежей (EFC) как AID = 1 по ИСО 14906
- Идентификатор канала: ICC определен как ChannelID = icc в соответствии с ИСО 14906
- Тип ICC: бесконтактный тип предоплаты ICC

Б.1.1.2 Определение типа данных

А) Определение содержимого APDU в TransferChannel.rq:

```
ICCcommand:: = SEQUENCE{
opCommandBody OCTET STRING – Команда ICC в ИСО/МЭК 7816‑4
}
```

Б) Определение содержимого APDU в TransferChannel.rs:

```
ICCresponse:: = SEQUENCE{
opCommandBody OCTET STRING – Реакция ICC в ИСО/МЭК 7816‑4
}
```

Б.1.1.3 Трансакция

Б.1.1.3.1 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 Б.1.

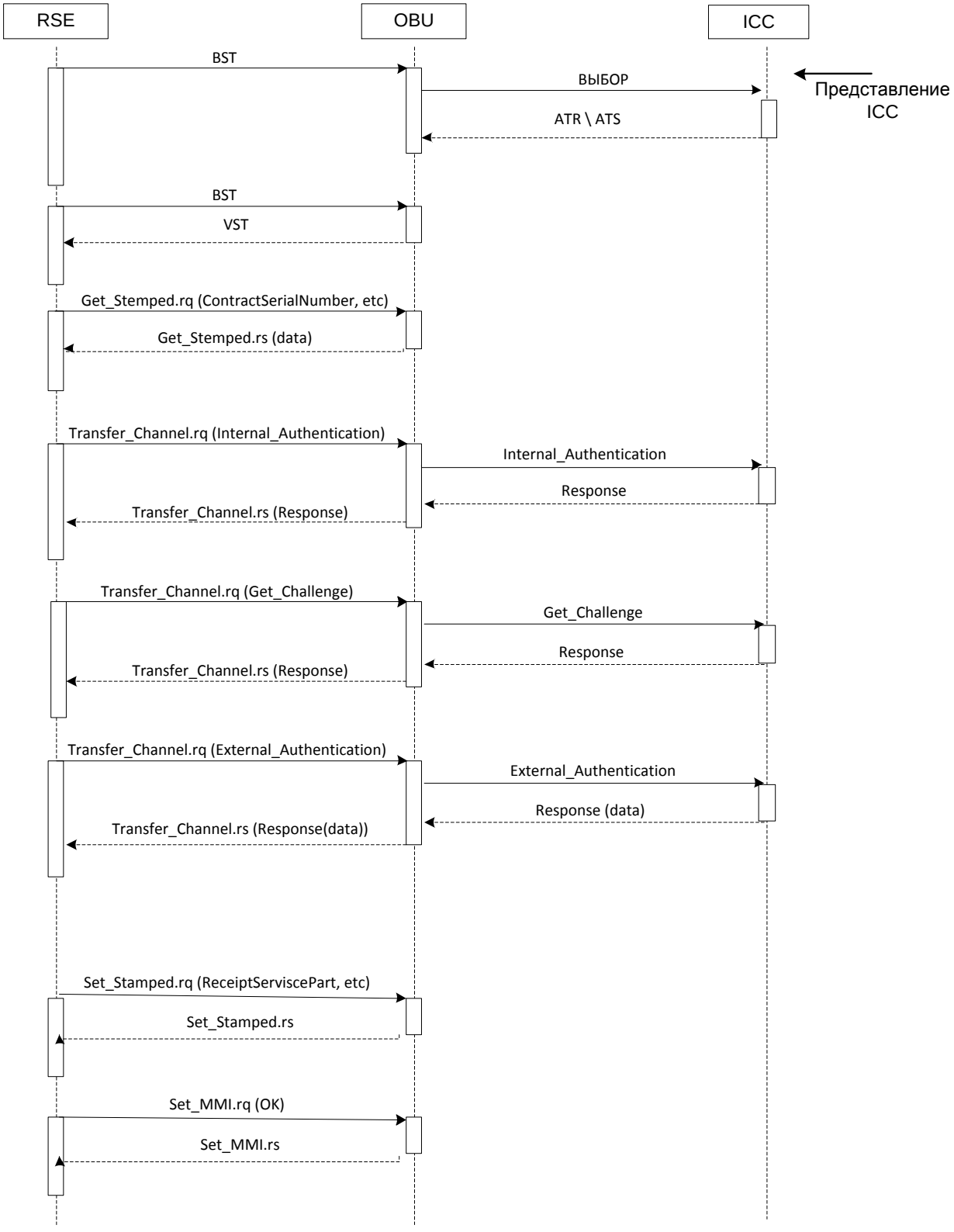


Рисунок Б.1 – Последовательность входной системы

Б) Система выхода

На выходе RSE считывает входную информацию из OBU и сохраняет ее в памяти RSE, и 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 Б.2.

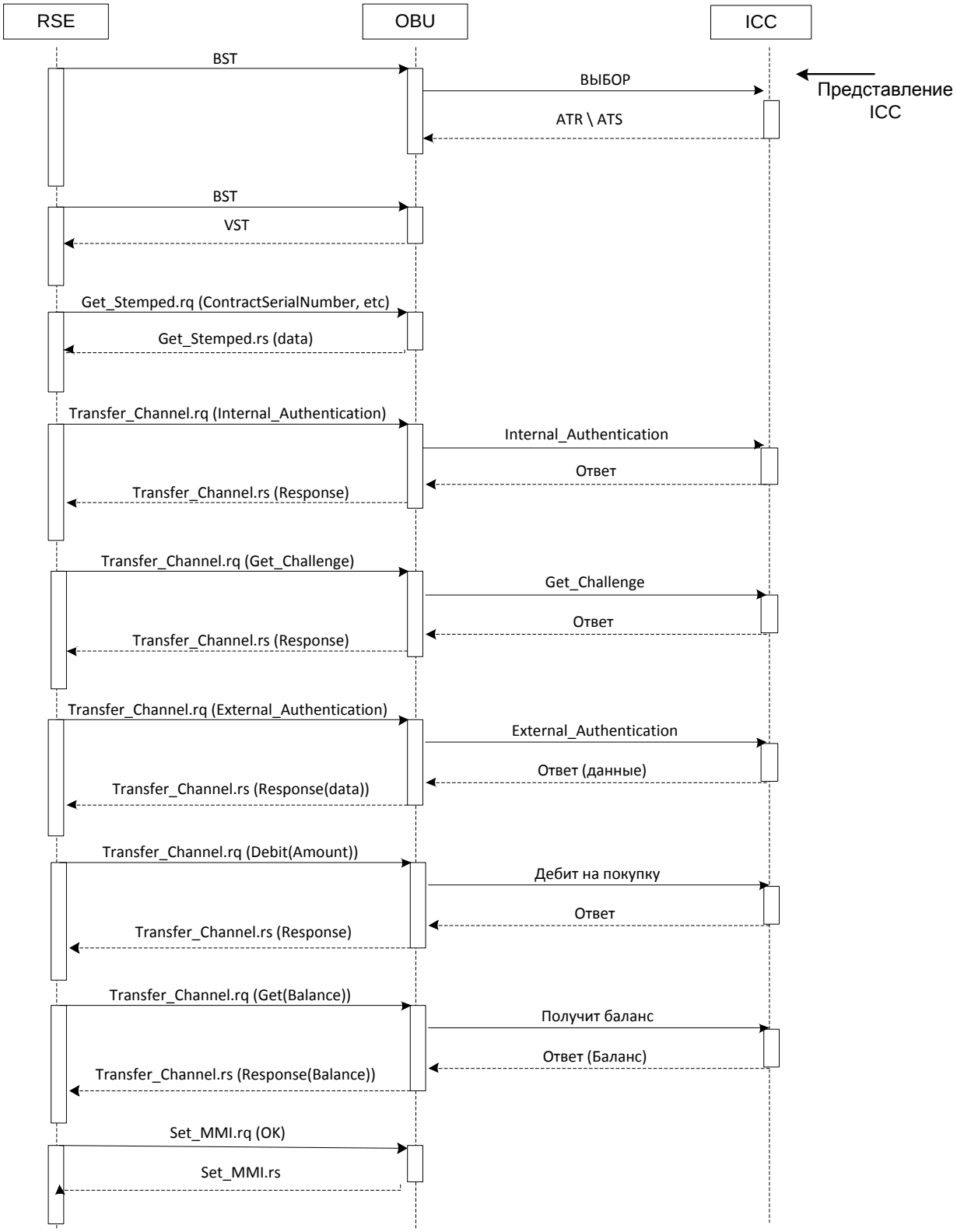


Рисунок Б.2 – Последовательный поток выходящей системы

Б.1.2 Модель 2 прозрачного типа (для постоплаты)

Б.1.2.1 Общее

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, зарегистрированным в ИСО 15628. 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, описанный в ИСО 14906: 2011, 7.1.

Определение команды: определяется базовым интерфейсом приложения DSRC (ИТС форум RC-004 в Японии)

- Команда: TRANSFER_CHANNEL определена ИСО 14906
- AID: Электронный сбор платежей (EFC) как AID = 1 по ИСО 14906
- Идентификатор канала: ICC определен как ChannelID = icc в соответствии с ИСО 14906
- Тип ICC: ICC контактного типа с оплатой в кредит

Б.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 ICC ИСО/МЭК 7816‑4
}
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)
}
```

Б) Определение содержимого APDU в TransferChannel.rs:

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

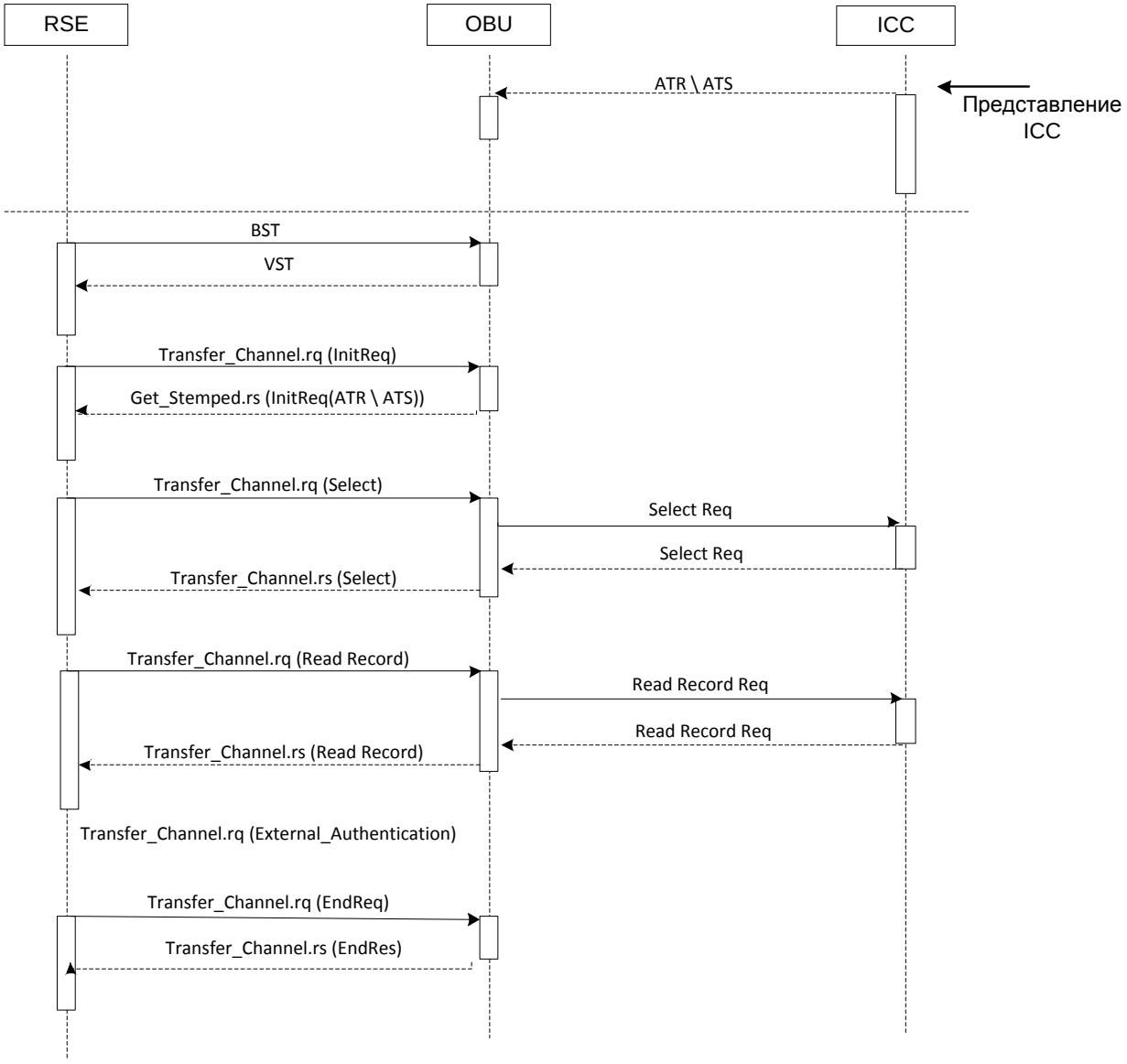
Б.1.2.3 Транзакция

Б.1.2.3.1 Парковочная система

а) Простая система (метод соединения по центру)

В 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 Б.3.

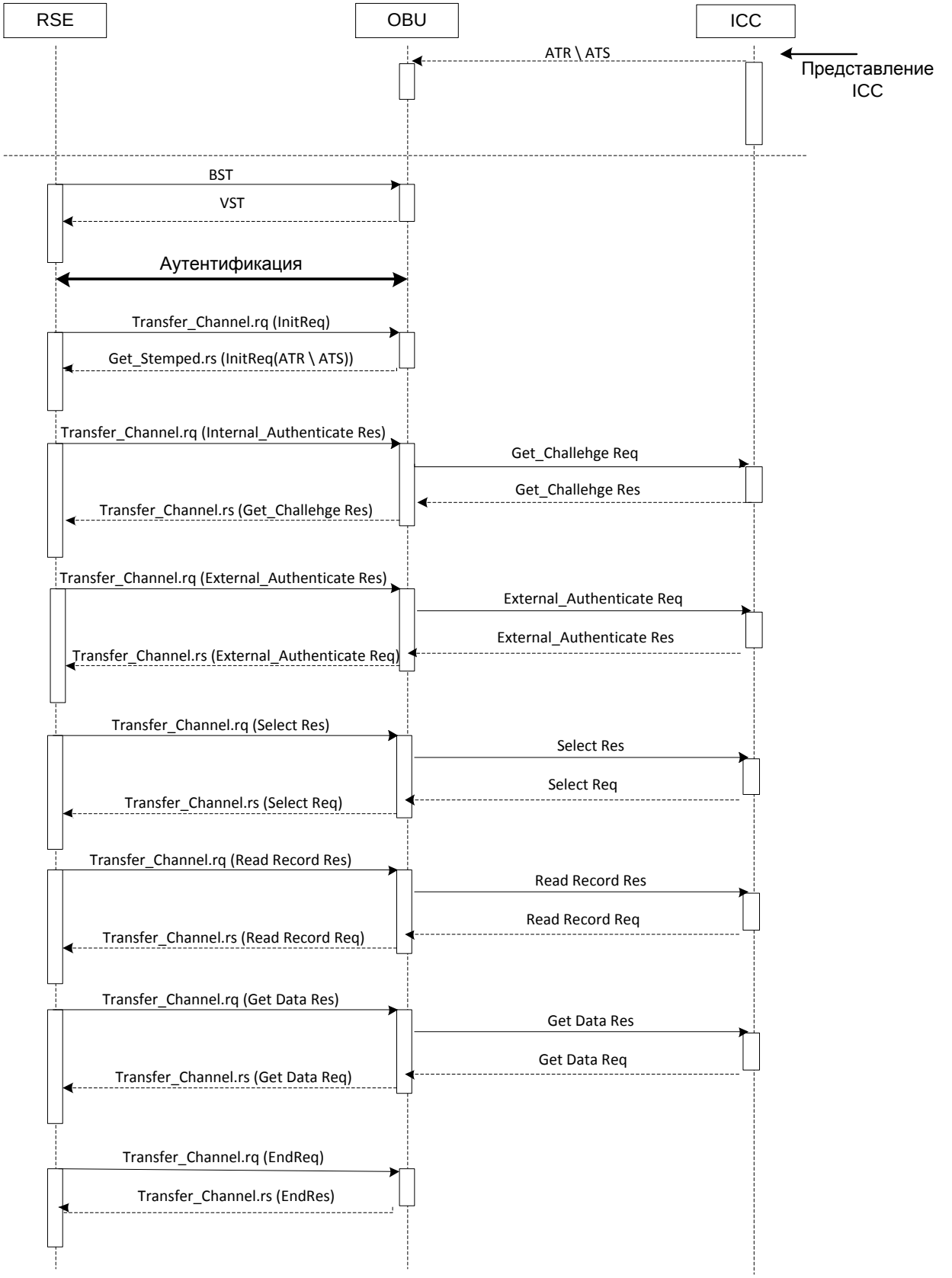


*Номер участника содержится в Read Record Res.

Рисунок Б.3 – Последовательность операций простой системы (метод централизованной цепочки)

б) Комплексная система (прямой метод)

В системе плата за парковку должна проходить по номеру кредитной карты, считываемым непосредственно из кредитной карты ICC, см. Рисунок Б.4.



*Номер кредитной карты содержится в Read Record Res.

Рисунок Б.4 – Последовательность выполнения сложной системы (прямой метод)

Б.2 Модель типа кэширования

Б.2.1 Общее

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 бортовых блоков, получив одобрение от испытательного центра. Следовательно, уровень безопасности данных для ICC и данных, связанных со сбором дорожных сборов, хранящихся в OBU, требует высокого уровня, должны оснащаться SAM, предоставленные сертифицированными производителями.

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

— Команда: TRANSFER_CHANNEL определена ИСО 14906

— AID: электронный сбор платежей (EFC) как AID = 1 или многоцелевой платеж (MPP), определенный как AID = 14 в соответствии с ИСО 14906 (см. примечание)

— Тип ICC: Контактный тип ICC для оплаты кредита

Примечание — Причины, по которым SAM используется в японской ETC:

- реализовать механизм кэширования в бортовом блоке для обеспечения высокой производительности даже при использовании низкоскоростного ICC контактного типа;
- для 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;
- для поддержания конкурентоспособности и быстрого распространения OBU по всей стране.

Примечание — Пояснение к AID = 14:

- Использование AID = 14 описано в ИСО 14906.
- AID, равный 14, определяет контекст многоцелевого платежа. В Японии ИСО 14906 определяет приложение

– интерфейс для DSRC, используемого для многоцелевого платежа (когда AID = 14 используется в Японии, EID и параметр определены через BST).

Б.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_instance Rs [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)),
        attributeIdList AttributeIdList
}
DsetRq:: = vSEQUENCE{
        fill            BIT STRING (SIZE(2)),
        delete          BOOLEAN,
        attributeIdList AttributeIdList,
        dataList        DataList
}
DataList:: = SEQUENCE(0..255) OF Data
Data:: = OCTET STRING(1..255)
AttributeIdList:: = SEQUENCE(0..255)OF attributeID
attributeID:: = INTEGER(0..127,..)
```

Б) Определение содержимого APDU в TransferChannel.rs:

```
RSECommand:: = SEQUENCE{
        eid                                     Dsrc-EID,
        parameter OCTET STRING                  - Параметр не включен в подкоманду
                  (SIZE(0..255)),
        subCommandList   SEQUENCE(0..255)       - Список вспомогательных команд
        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),
 }
```

Б.2.3 Пример транзакции

Б.2.3.1 ETC по фиксированной ставке (открытая система) и оплата в кредит

См. Рисунок Б.5.

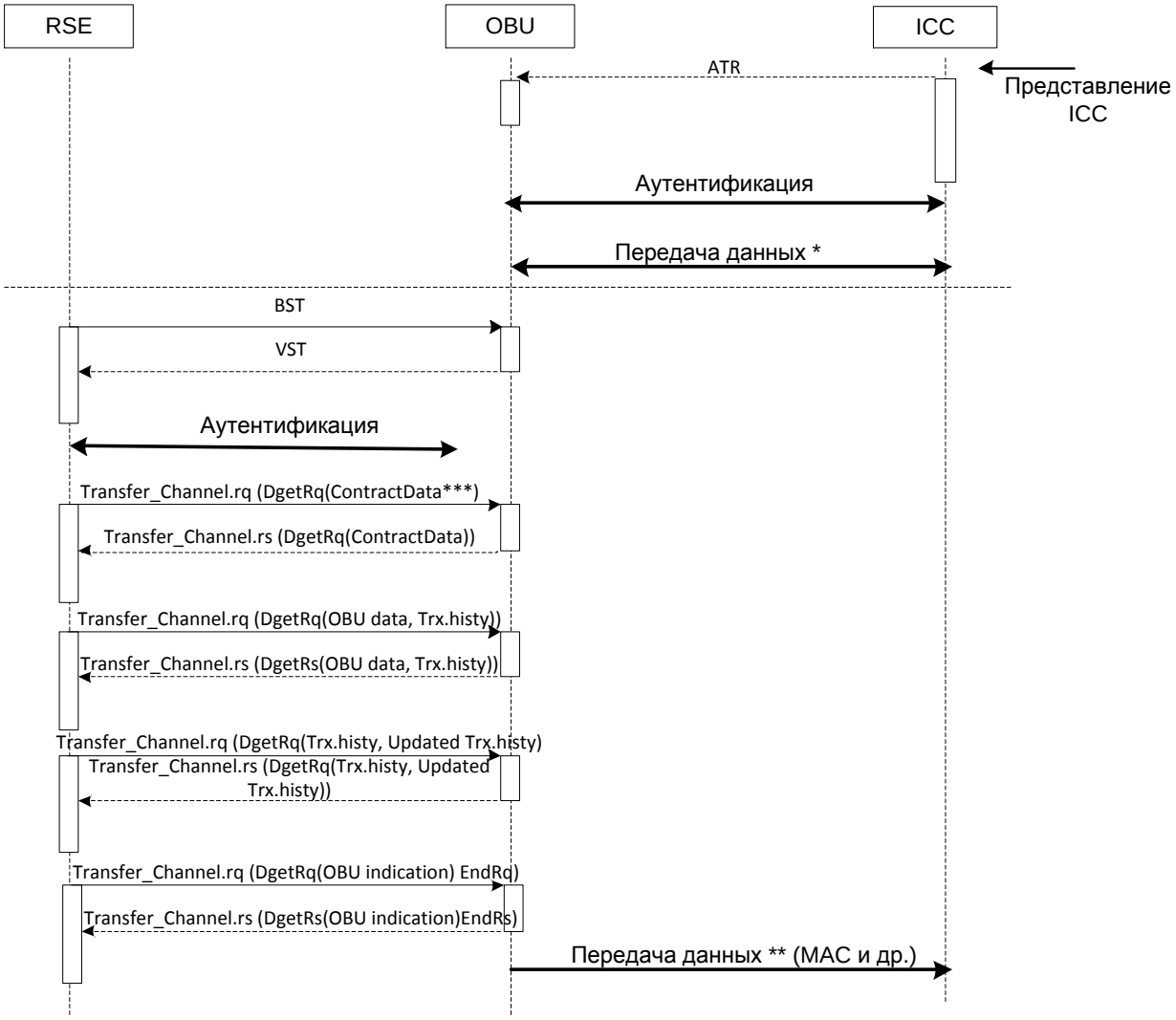
*Следующие наборы данных ICC передаются в OBU после данных контракта представления ICC, данных истории транзакций (история Trx).
** Следующие наборы данных передаются в ICC после завершения данных транзакции DSRC (Trx.), Данных истории транзакции (Trx).
***Номер карты IC включен.

Рисунок Б.5 – Последовательность взимания фиксированной ставки ETC (открытая система) и оплаты кредита

Б.2.3.2 Тарифы на расстояние ETC (закрытая система) и оплата в кредит

См. Рисунок Б.6.

А) Входящая транзакция

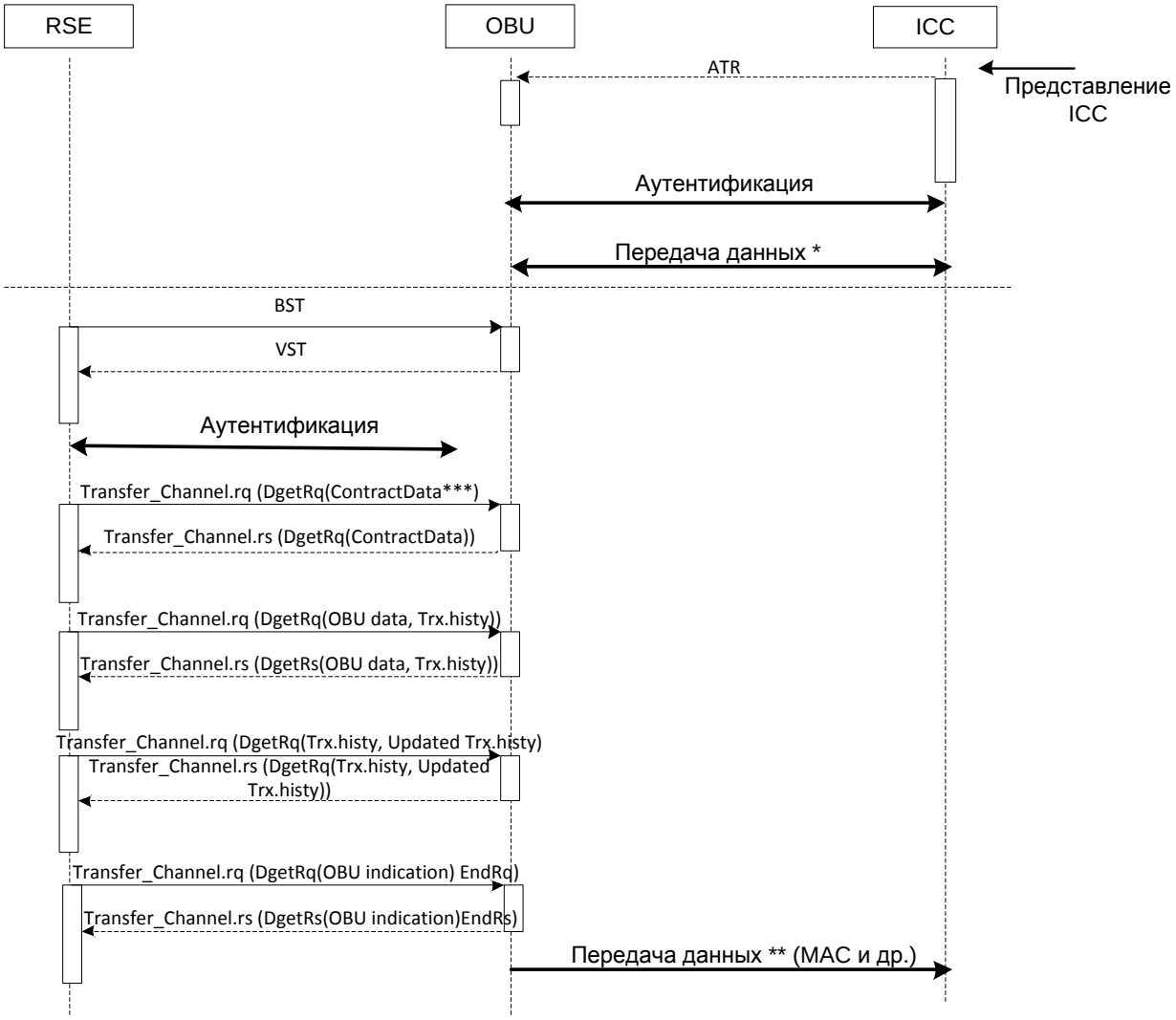


*Следующие наборы данных ICC передаются в OBU после данных контракта представления ICC, данных истории транзакций (история Trx).
** Следующие наборы данных передаются в ICC после завершения данных транзакции DSRC (Trx.), Данных истории транзакции (Trx).
***Номер карты IC включен.

Рисунок Б.6 – Последовательность входящей транзакции

Б) Исходящая транзакция

См. Рисунок Б.7.



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

Рисунок Б.7 – Последовательность исходящий транзакции

Б.3 Модель типа буферизации

Б.3.1 Общее

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, как определено в ИСО 14906.

— AID: Электронный сбор платежей (EFC) как AID = 1 по ИСО 15628

— Тип ICC: Гибридная карта с предоплатой

Б.3.2 Определение команды RSE

Б.3.2.1 Команда дебетования

В данном случае в ActionParameter включает данные для команды ICICI Debit (S2, PSALM 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)), – S2
    RFU OCTET STRING (SIZE(5)), – зарезервировано для использования в будущем
}
```

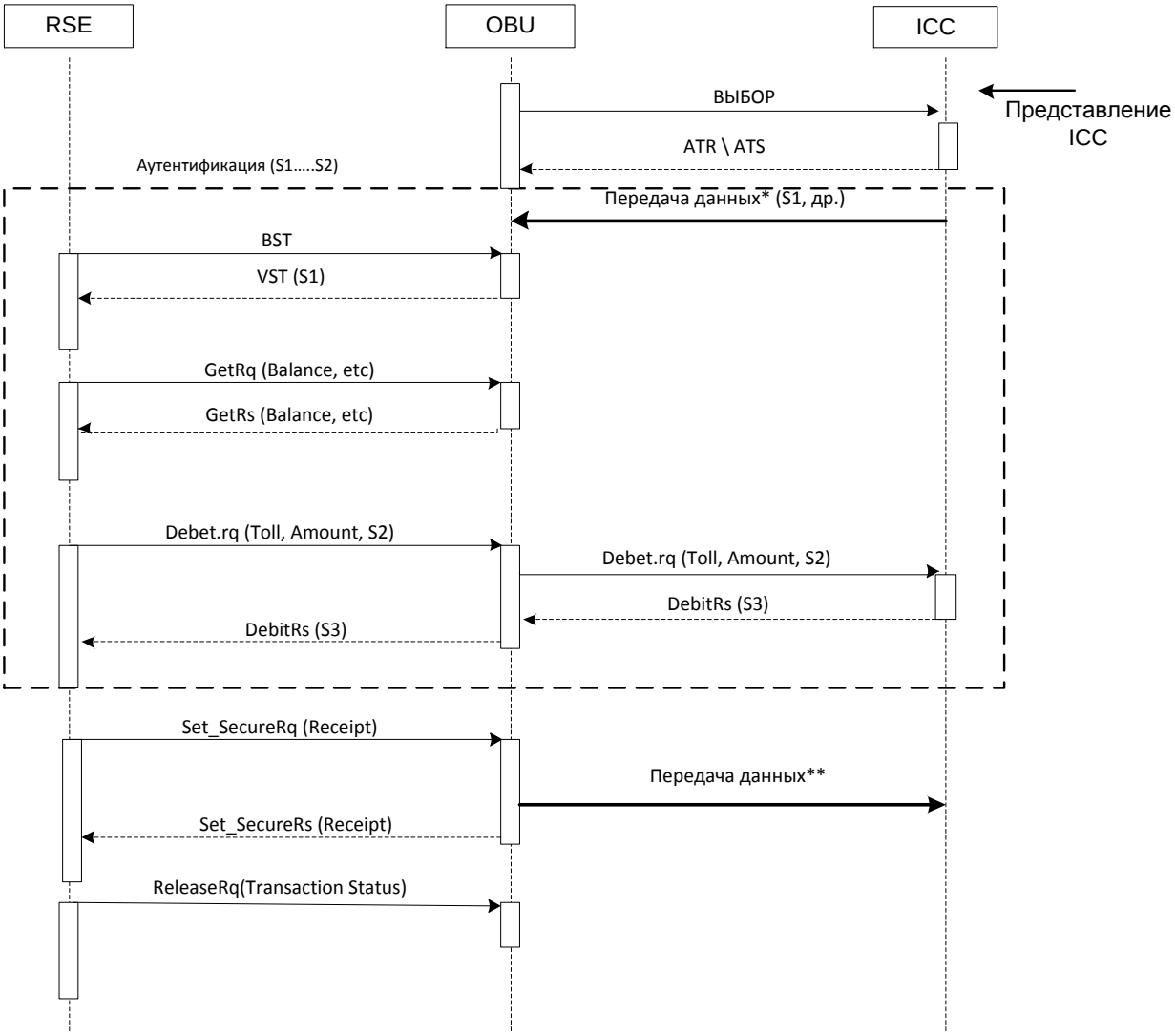
* Применительно для debitAuthenticator

```
debitAuthenticator:: = SEQUENCE{
    parameterLen OCTET STRING (SIZE(1)), – длина S3
    S3 OCTET STRING (SIZE(4)) – подпись S3
}
```

Б.3.3 Транзакция

А) Алгоритм быстрой транзакции ETC и предоплата

См. Рисунок Б.8.



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

** Данные приема успешно записываются в ICC только после того, как MAC, сгенерированный RSE (т. е. SAM), проверен ICC.

Рисунок Б.8 – Алгоритм быстрой транзакции ETC и предоплата

Приложение В
(информационное)
Модели взаимодействия платежного сервиса с другими сервисами

На рисунке В.1 показано отношение эксплуатационной совместимости, при котором коды ICC, выпущенные для EFC, должны использоваться для приложений общественного транспорта и / или розничной торговли.

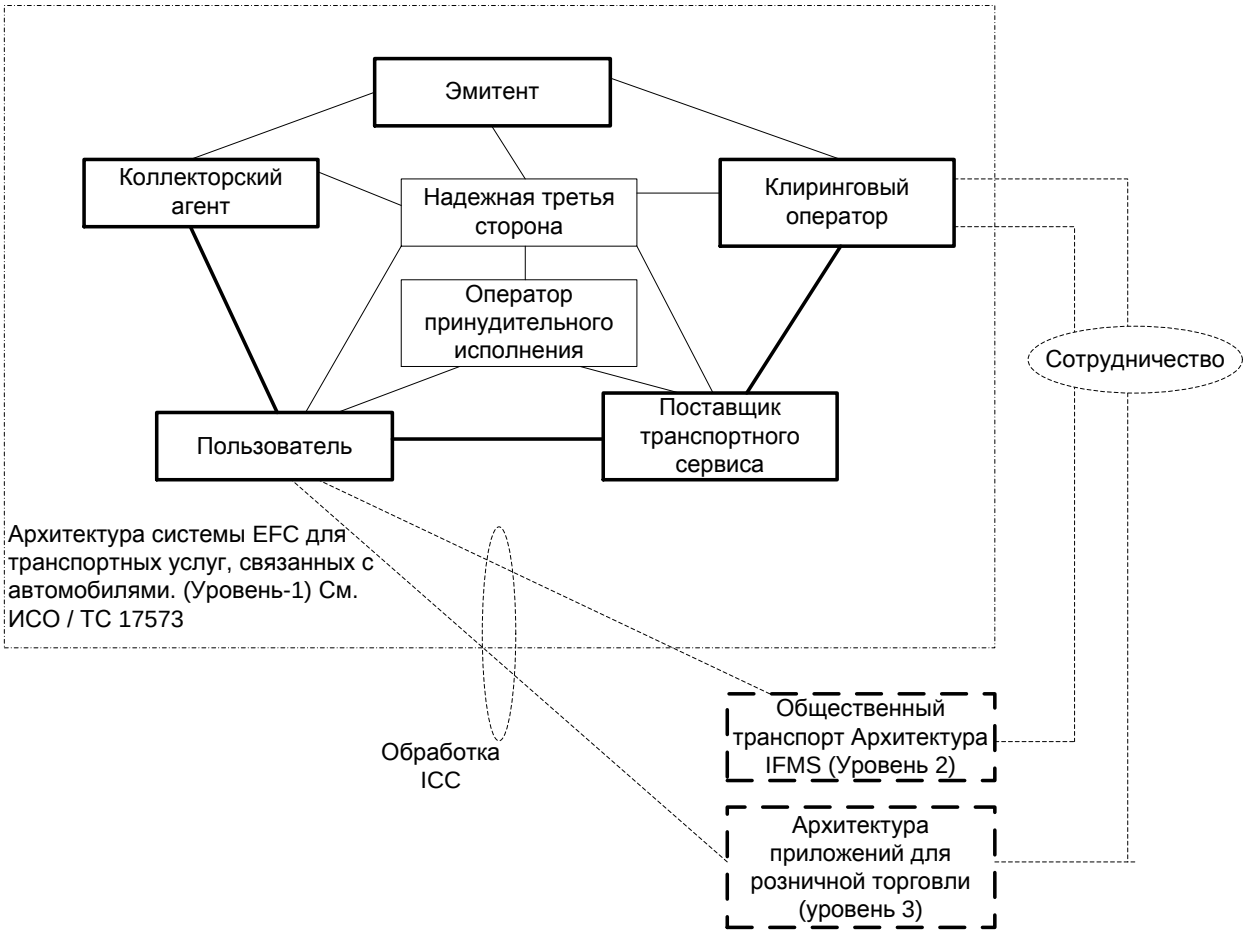


Рисунок В.1 – Модель взаимодействия сервиса EFC с другими сервисами

На рисунке В.2, напротив, показаны другие отношения оперативной совместимости, в которых коды ICC, выдаваемые для

общественного транспорта, рассматриваются как портативные электронные носители, или когда для EFC должны использоваться розничные платежи.

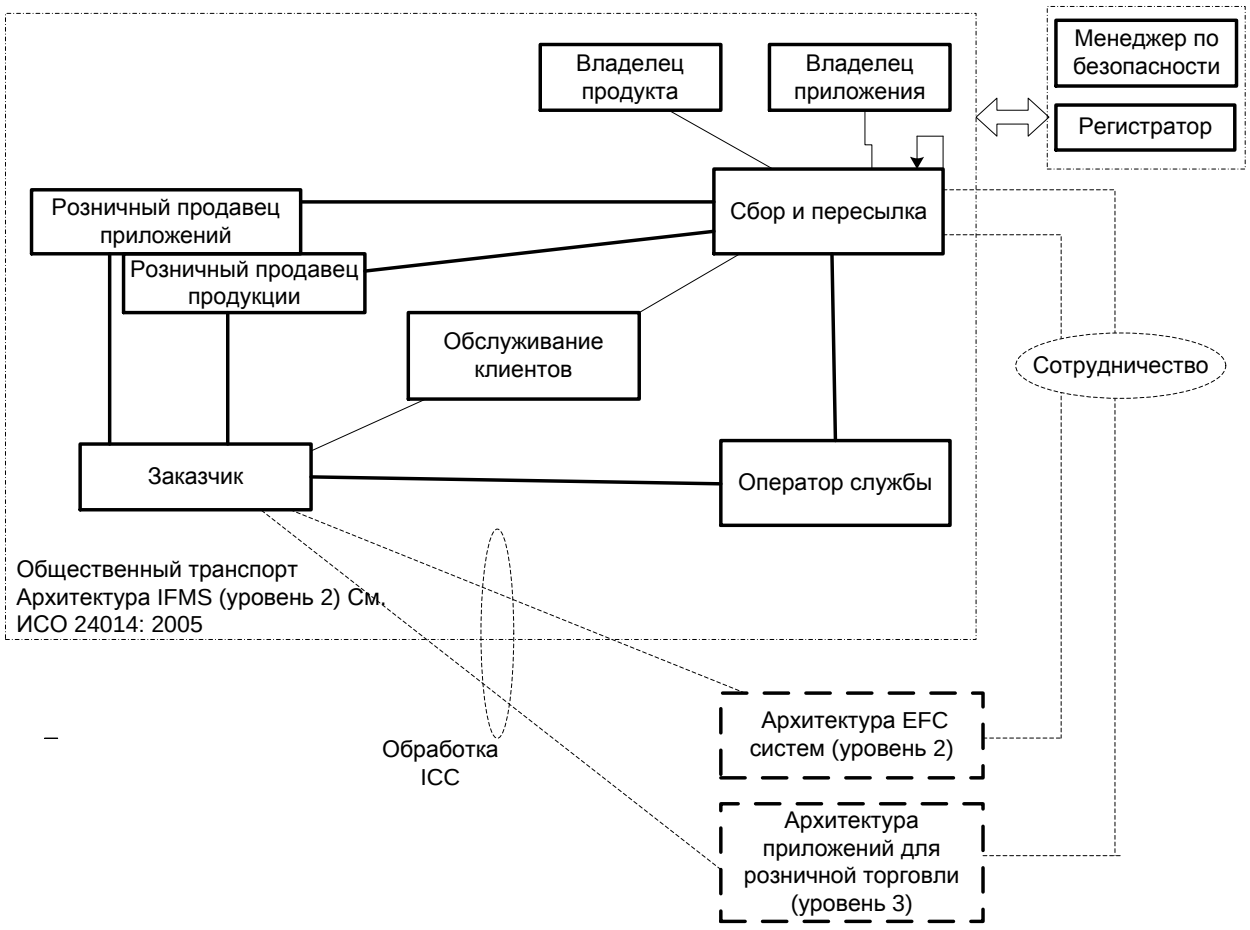


Рисунок В.2 – *Модель взаимодействия сервиса IFMS с другими сервисами*

Библиография

[1] ИСО/МЭК 7498-2:1989	Системы обработки информации - Взаимосвязь открытых систем - Базовая справочная модель - Часть 2: Архитектура безопасности
[2] ИСО/МЭК 7816-1	Удостоверения личности - карты Интегральной схемы (схем) с контактами - Часть 1: Физические характеристики
[3] ИСО/МЭК 7816-2	Идентификационные карточки - карточки интегральной схемы - Часть 2: карты с контакты - размеры и расположение контактов
[4] ИСО/МЭК 7816-3	Удостоверения личности - карты Интегральной схемы - Часть 3: Карты с контактами - интерфейс Electrical и протоколы передачи
[5] ИСО/МЭК 7816-4	Карточки идентификационные. Контактные карточки на интегральных схемах. Часть 4. Организация, защита и команды для обмена
[6] ИСО/МЭК 8824-1	Информационные технологии - Абстрактный синтаксис Нотация 1 (ASN.1): Спецификация базовой нотации - Часть 1:
[7] ИСО/ТС 14907-1	Электронный сбор денежных средств - Процедуры проведения испытаний для пользователя и стационарного оборудования - Часть 1: Описание процедур проведения испытаний

[8] ИСО/ТС 14907-2	Электронный сбор денежных средств - Процедуры проверки для пользователя и стационарного оборудования - Часть 2: испытание Соответствия на бортовой прикладной интерфейс единицы
[9] ИСО/МЭК 14443-3	Удостоверения личности Бесконтактная Часть 3 карт Близости карт интегральной схемы (схем): Инициализация и антистолкновение - Принятый INCITS
[10] ИСО/МЭК 15408-1	Информационные технологии - Методы безопасности - Критерии оценки безопасности ИТ - Часть 1: Введение и общая модель (ISO/IEC 15408-1:2009)
[11] ИСО/МЭК 15408-2	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности
[12] ИСО/МЭК 15408-3	Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки защиты
[13] ИСО/ТС 16785:2020	Электронный сбор платежей (EFC). Определение интерфейса приложения между DSRC-OBE и наружными устройствами на транспортном средстве
[14] ИСО 17573	Автоматический сбор платежей. Архитектура систем для взимания платы за проезд транспортных средств
[15] ИСО/ТС 17574	Электронный сбор денег. Руководящие указания по защитным профилям безопасности

[16] ИСО/ТС 17575-1:2016	Электронный сбор платежей. Определение прикладного интерфейса для автономных систем. Часть 1. Оплата
[17] ИСО/МЭК 18092	Информационные технологии - Телекоммуникации и обмен информацией между системами - Около Полевой Коммуникации - Интерфейсом и Протоколом (NFCIP-1)
[18] ИСО/ТС 19299:2015	Электронный сбор денежных средств - Концепция безопасности
[19] 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

Руководитель разработки:
Богумил В.Н.,
Инженер отдела организации и проведения мероприятий инфраструктурного центра «Автонет» Московского Политеха, к.т.н., доцент