ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 24727-1— 2016

Карты идентификационные

ПРОГРАММНЫЕ ИНТЕРФЕЙСЫ КАРТ НА ИНТЕГРАЛЬНЫХ СХЕМАХ

Часть 1

Архитектура

(ISO/IEC 24727-1:2014, IDT)

Издание официальное

Москва
Стандартинформ
2017

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ВНИИНМАШ) и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 25 ноября 2016 г. № 1787-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 24727-1:2014 «Идентификационные карты. Программные интерфейсы карт на интегральных схемах. Часть 1. Архитектура» (ISO/IEC 24727-1:2014 «Identification cards — Integrated circuit card programming interfaces — Part 1:Architecture», IDT).

ИСО/МЭК 24727-1:2014 разработан подкомитетом ПК 17 «Идентификационные карты и устройства идентификации личности» Совместного технического комитета по стандартизации СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

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

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. ИСО и МЭК не несут ответственности за идентификацию подобных патентных прав

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

Содержание

Введение

ИСО/МЭК 24727 представляет собой серию стандартов, устанавливающих требования к программным интерфейсам и протоколам, с помощью которых осуществляется взаимодействие между картами на интегральных схемах (ICC) и резидентными приложениями на разнообразных компьютерных платформах. ICC предоставляют обобщенные сервисы для многосекторного использования, к которым обращаются преимущественно при поддержке доверительных операций идентификации, аутентификации и электронной подписи. Организация и функционирование ICC соответствуют требованиям ИСО/МЭК 7816-4.

Стандарты серии ИСО/МЭК 24727 используют общие принципы эталонной модели взаимосвязи открытых систем, представленные в ИСО/МЭК 7498-1/Рекомендациях МСЭ-Т[1] X.200. Эти принципы предлагают, чтобы связь между взаимодополняющими приложениями на разнообразных компьютерных платформах достигалась при помощи четко определенных процедур, доступ к которым осуществляется через стандартные интерфейсы. Данные процедуры охватывают как аппаратные, так и программные средства, которые позволяют приложениям взаимодействовать между собой даже будучи разделенными сложными каналами связи.

Набор процедур, которые связывают одно приложение с другим, упоминается как стек протоколов. Каждый компонент такого стека включает в себя интерфейс и уровень. Уровень содержит реализацию процедурной функциональности, которая принимает и отвечает на запросы, передаваемые через интерфейс. В стандартах серии ИСО/МЭК 24727 определены интерфейсы, позволяющие независимым реализациям уровня быть взаимозаменяемыми. Это составляет базовое определение функциональной совместимости: независимые реализации являются взаимозаменяемыми.

Чтобы достичь подлинной функциональной совместимости в широком диапазоне доменов приложений, некоторые из которых появились раньше стандартов серии ИСО/МЭК 24727, требуется разнообразие механизмов адресации в пределах соответствующих реализаций. Эти механизмы включают в себя: общую архитектуру, общую семантику, формально определенные интерфейсы, обнаруживаемость, расширяемость, совместимость с предыдущими версиями и испытания на соответствие. Способы реализации этих механизмов рассмотрены в следующих разделах и в остальных частях серии ИСО/МЭК 24727.

[1] Сектор стандартизации электросвязи (ITU-T) Международного союза электросвязи (МСЭ, ITU).

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Карты идентификационные

ПРОГРАММНЫЕ ИНТЕРФЕЙСЫ КАРТ НА ИНТЕГРАЛЬНЫХ СХЕМАХ

Часть 1

Архитектура

Identification cards. Integrated circuit card programming interfaces. Part 1. Architecture

Дата введения — 2018—01—01

1 Область применения

Стандарты серии ИСО/МЭК 24727 устанавливают требования к набору программных интерфейсов и протоколов, с помощью которого осуществляется взаимодействие между картами на интегральных схемах (далее — ICC) и резидентными приложениями на разнообразных компьютерных платформах. ICC предоставляют обобщенные сервисы для многосекторного использования приложений. Организация и функционирование ICC соответствуют требованиям ИСО/МЭК 7816-4. Предполагается, что некоторые домены приложений будут пытаться достичь функциональной совместимости средствами стандартов серии ИСО/МЭК 24727, даже несмотря на то, что приложения существовали еще до появления этих средств. С данной целью установлены различные способы совместимости с предыдущими версиями через механизмы, определенные в стандартах серии ИСО/МЭК 24727.

Настоящий стандарт устанавливает:

- архитектуру системы и принципы функционирования;
- средства достижения функциональной совместимости между разнообразными доменами приложений;
- концептуальные модели данных и сервисов, которые охватывают соответствующие домены приложений, а также
- основы доверительных процессов, возможных при этих моделях.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующий международный стандарт. Для датированных ссылок следует использовать только указанное издание, для недатированных ссылок следует использовать последнее издание указанного документа, включая все поправки.

ISO/IEC 7816-4:2005[1)] Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange (Идентификационные карты. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена)

[1)] Заменен на ИСО/МЭК 7816-4:2013. Однако для однозначного соблюдения требования настоящего стандарта, выраженного в датированной ссылке, рекомендуется использовать только указанное в этой ссылке издание.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями:

3.1 **аутентификация** (authentication): Процесс оценки уровня доверия в ходе проверки идентичности или при идентификации.

3.2 **протокол аутентификации** (authentication protocol): Конкретный процесс аутентификации.

3.3 **карта** (card): Карта на интегральной(ых) схеме(ах).

3.4 **карточное приложение** (card-application): Однозначно адресуемый набор функций, размещенный на ICC, который обеспечивает хранение данных и предоставляет вычислительные сервисы клиентскому приложению.

3.5 **клиентское приложение** (client-application): Программное обеспечение для обработки данных, которому необходим доступ к одному или нескольким карточным приложениям.

3.6

элемент данных (data element): Смысловой элемент информации, прослеживаемый на стыке между картой и устройством сопряжения, для которого определены наименование, описание логического содержания, формат и кодирование.

[ИСО/МЭК 7816-4]

3.7 **набор данных** (data set): Поименованная совокупность структур данных для функциональной совместимости.

3.8 **структура данных для функциональной совместимости** (data structure for interoperability): Файл по ИСО/МЭК 7816-4, идентифицируемый по двухбайтовому идентификатору файла, или информационный объект BER-TLV по стандартам серии ИСО/МЭК 8825, идентифицируемый по строке октетов, кодирующей тег ACH.1[1)].

3.9 **дифференциальное тождество** (differential-identity): Набор информации, который содержит имя, метку и протокол аутентификации.

3.10 **уровень обобщенного доступа к карте** (generic card access layer): Компонент, который предоставляет интерфейс по ИСО/МЭК 24727-2 уровню доступа к сервису.

3.11 **идентификация** (identification): Объединенный аспект набора характеристик и процессов, посредством которого объект может быть распознан или узнан.

3.12 **интерфейс** (interface): Точка, в которой независимые и часто несвязанные системы входят в контакт и воздействуют одна на другую или взаимодействуют друг с другом.

3.13 **функциональная совместимость** (interoperability): Возможность для интерфейса любого карточного приложения, который соответствует стандартам серии ИСО/МЭК 24727, быть используемым любым клиентским приложением, соответствующим стандартам серии ИСО/МЭК 24727.

3.14 **метка** (marker): Элемент информации, входящий в дифференциальное тождество, представляющий собой уникальную характеристику объекта.

3.15 **промежуточное программное обеспечение/промежуточное ПО** (middleware): Программное обеспечение, которое соединяет два отдельных разных приложения.

3.16 **SAL-упрощенный** (SAL-lite): Упрощенный компонент, который предоставляет подмножество API по ИСО/МЭК 24727-3 для обнаружения структур данных клиентским приложением.

3.17 **сервис** (service): Набор функций обработки, доступный в интерфейсе.

3.18 **уровень доступа к сервису** (service access layer): Компонент, который предоставляет API по ИСО/МЭК 24727-3 клиентскому приложению.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

AID — идентификатор приложения (application identifier);

ACD — описание функциональных возможностей приложения (application capability description);

APDU — блок данных прикладного протокола (application protocol data unit);

API — интерфейс программирования приложений (application programming interface);

BER — базовые правила кодирования (basic encoding rules);

CCD — описание функциональных возможностей карты (card capability description);

[1)] Абстрактная синтаксическая нотация версии один.

GCAL — уровень обобщенного доступа к карте (generic card access layer);
GCI — обобщенный интерфейс карты (generic card interface);
ICC — карта на интегральной(ых) схеме(ах) (integrated circuit card);
IFD — устройство сопряжения (interface device);
SAL — уровень доступа к сервису (service access layer);
SAL-упрощенный — упрощенный компонент уровня доступа к сервису (service access layer lightweight component);
TLV — тег-длина-значение (tag-length-value).

5 Функциональная совместимость

Функциональная совместимость касается средств, благодаря которым интерфейсы карточных приложений, соответствующие стандартам серии ИСО/МЭК 24727, могут быть доступны клиентскому приложению, соответствующему стандартам серии ИСО/МЭК 24727. В данных стандартах функциональная совместимость достигается через множество механизмов, в том числе:

- общая архитектура;
- общая семантика;
- формально определенные интерфейсы;
- обнаруживаемость;
- расширяемость;
- совместимость с предыдущими версиями;
- испытания на соответствие.

Все интерфейсы в стандартах серии ИСО/МЭК 24727 определены с использованием формальных языков. Этим обеспечивается строгое выражение грамматики и семантики, благодаря чему интерфейсы могут быть реализованы независимо и переданы через все множество стеков протоколов совместимым образом.

Как показано на рисунке 1, для каждого установленного интерфейса в соответствующих частях серии ИСО/МЭК 24727 должны быть определены поддерживаемые функции.

Стандарты серии ИСО/МЭК 24727 относятся к ICC, которая явно или неявно предоставляет описание функциональных возможностей. Описание функциональных возможностей рассмотрено в 6.6 и более точно определено в ИСО/МЭК 24727-2.

Способы расширения различных интерфейсов и протоколов, к которым обращаются стандарты серии ИСО/МЭК 24727, включая соответствующую технологию ICC, рассмотрены в различных частях данной серии.

6 Архитектура

6.1 Общие положения

Стандарты серии ИСО/МЭК 24727 разделяют функциональные возможности между клиентским приложением, работающим на хост-платформе, и набором сервисов, предоставляемым резидентным карточным приложением ICC, который может использовать клиентское приложение. Доступ к таким сервисам обеспечивается через стек протоколов, который предоставляет сервисный интерфейс, обобщенный интерфейс карты и одно или более резидентных карточных приложений, находящихся на ICC.

6.2 Архитектурные атрибуты

Сервисный интерфейс реализует функции, рассматриваемые в 6.5, которые более точно определены в ИСО/МЭК 24727-3.

Обобщенный интерфейс карты реализует функции, рассматриваемые в 6.8, которые более точно определены в ИСО/МЭК 24727-2.

Связующий интерфейс реализует функции, рассматриваемые в 6.9, которые более точно определены в ИСО/МЭК 24727-3 и ИСО/МЭК 24727-6.

Интерфейс доверительного канала реализует функции, рассматриваемые в 6.10, которые более точно определены в ИСО/МЭК 24727-4.

Карточные приложения управляют наборами данных, включая создание пространства уникальных имен для наборов данных и всю информацию, содержащуюся в них. Каждый набор данных поименован, и список имен наборов данных от карточного приложения доступен клиентскому приложению благодаря непосредственному знанию или в результате обнаружения. Клиентское приложение использует имя набора данных при запросе сервиса, который следует применить к набору данных.

Доступ к наборам данных контролируют с помощью списка управления доступом. Список управления доступом описывает условия защиты, которые должны быть соблюдены, чтобы совершить действие над набором данных. В ИСО/МЭК 24727-3 и ИСО/МЭК 24727-4 приведена дополнительная подробная информация о списках управления доступом, проверке идентичности и действиях.

Карточные приложения организованы на ICC в виде охватывающего карточного альфа-приложения и одного или нескольких содержащихся внутри него карточных приложений. Карточные приложения можно выбирать по AID через сервисный интерфейс.

6.3 Логическая архитектура

На рисунке 1 показаны взаимосвязи между клиентским приложением, уровнями и интерфейсами, определенными в стандартах серии ИСО/МЭК 24727, и резидентным карточным приложением на ICC. Поток запросов от клиентского приложения к карточному приложению показан направляющими стрелками, означающими или запрос, или подтверждение. Каждая стрелка показывает функции, поддерживаемые соответствующим стандартом. Фактический формат и синтаксис запроса или подтверждения описаны в указанной части серии ИСО/МЭК 24727.

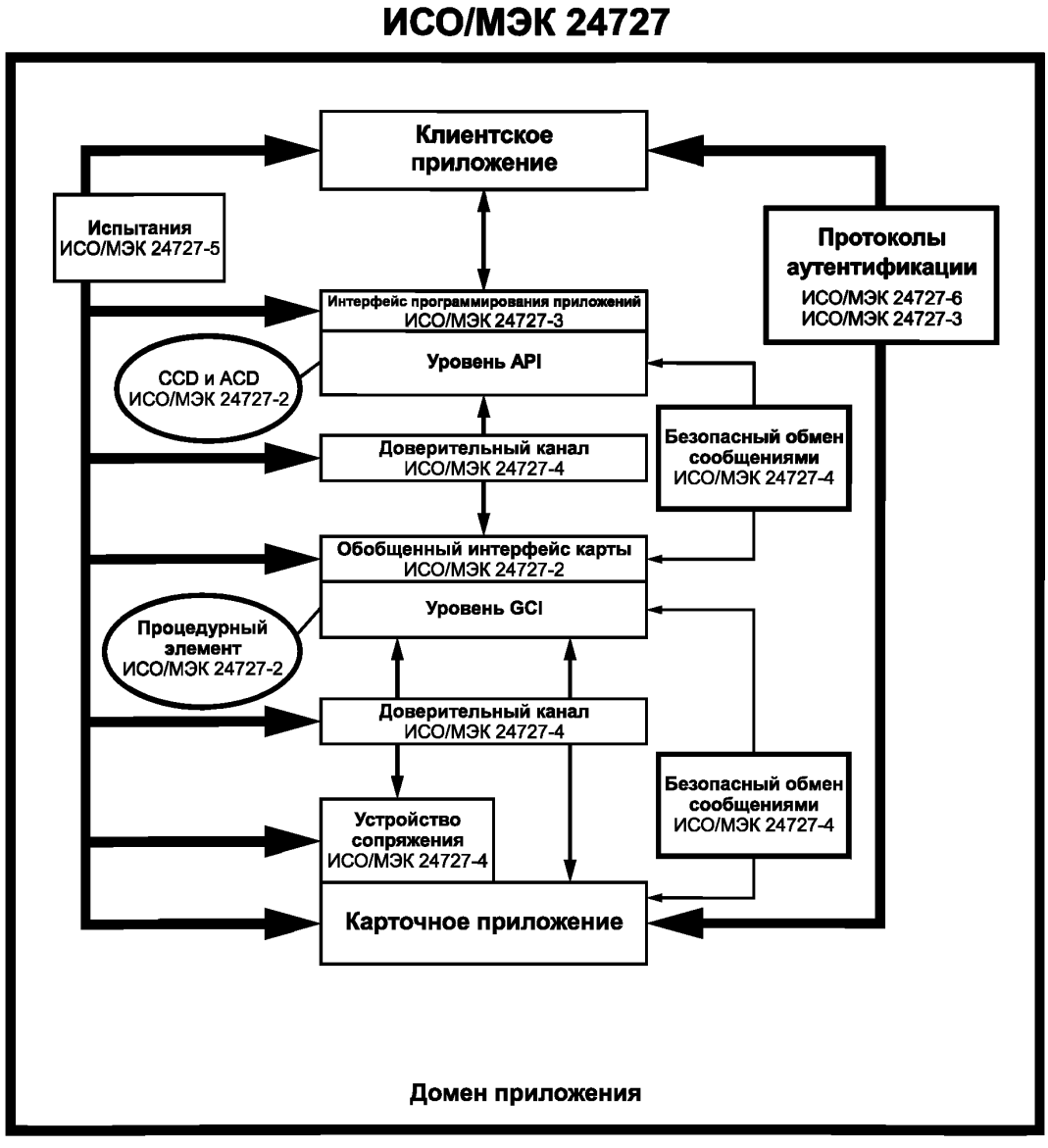


Рисунок 1 — Логическая архитектура по стандартам серии ИСО/МЭК 24727

Функции, предусмотренные в стандартах серии ИСО/МЭК 24727, могут быть реализованы многими способами при соответствии интерфейса, подтвержденном испытаниями по ИСО/МЭК 24727-5.

6.4 Независимость от протоколов

Интерфейсы из стандартов серии ИСО/МЭК 24727 определены с помощью описания на основе нотации АСН.1 с дополняющими XML-описаниями. Интерфейсы определены способом, не зависимым от протоколов, необходимых для установления взаимодействия между клиентским и карточным приложениями.

На рисунке 1 показан стек уровней и интерфейсов, необходимых для обеспечения возможности связи между клиентскими и карточными приложениями.

Механизм прокси-агента представляет собой реализацию интерфейса элемента стека, которая позволяет реализации элемента стека быть разделенной между прокси и агентом, обнаруженным в некой другой точке в пределах стека протоколов. Способный к взаимодействию механизм прокси-агента зависит от спецификации интерфейса, использующей формальные языки, и четко определенного механизма кадрирования. Данные возможности описаны в ИСО/МЭК 24727-4.

В приложении А представлены некоторые полезные в общем конфигурации. Данные конфигурации более детально рассмотрены в ИСО/МЭК 24727-4.

6.5 Интерфейс уровня доступа к сервису для клиентского приложения

ИСО/МЭК 24727-3 содержит подробное описание сервисного интерфейса, доступного клиентскому приложению.

Реализация сервисного интерфейса:

- переводит запрос действия, выраженный в семантике клиентского приложения, в один или несколько обобщенных запросов, выраженных в семантике резидентного карточного приложения ICC;
- переводит одно или несколько обобщенных подтверждений, исходящих от карточного приложения, в подтверждение действия, предназначенное для клиентского приложения.

Сервисный интерфейс включает в себя:

- возможности и средства взаимодействия клиентского приложения с карточным приложением, использующие обобщенный интерфейс карты;
- средства защиты связи клиентского приложения с карточным приложением в соответствии с основами безопасности;
- криптографический сервис;
- сервис дифференциального тождества.

6.6 Описание функциональных возможностей

Сервисный интерфейс и обобщенный интерфейс карты определены таким образом, чтобы облегчать обнаружение функциональных возможностей одного или нескольких резидентных карточных приложений, находящихся на ICC. Информационной структурой, благодаря которой данный механизм обнаружения становится возможным, является описание функциональных возможностей (Capability Description).

В стандартах серии ИСО/МЭК 24727 подробно представлены два уровня описания функциональных возможностей:

- описание функциональных возможностей карты (CCD), используемое, чтобы обнаруживать одно или несколько резидентных карточных приложений ICC. CCD постоянно находится в карточном альфа-приложении. CCD предоставляет информацию по преобразованию APDU;
- описание функциональных возможностей приложения (ACD), которое может быть предоставлено вместе с карточным приложением. ACD, если присутствует, служит для информирования запрашивающей стороны о дополнительных или измененных функциональных возможностях по сравнению с представленными в CCD.

В ИСО/МЭК 24727-2 подробно рассмотрены оба уровня описания функциональных возможностей. Назначение описания функциональных возможностей — сделать возможным обнаружение как через обобщенный интерфейс карты, так и через сервисный интерфейс. Преобразование любой пары команда — ответ между обобщенным интерфейсом карты и сервисным интерфейсом может быть определено с помощью описания функциональных возможностей.

Также в ИСО/МЭК 24727-2 подробно представлена методология описания функциональных возможностей, касающаяся того, как информацию организуют, защищают, извлекают и обновляют, используя резидентные карточные приложения ICC.

Подмножество API, называемое SAL-упрощенный, реализуемое исключительно на локальном хосте, поддерживает возможность обнаружения карточных приложений.

6.7 Модель данных

Сервисный интерфейс, описанный в ИСО/МЭК 24727-3, основан на структуре модели данных, которая определяет элементы данных и их взаимосвязь. Хотя они связаны с приложением, элементы данных и их связи последовательно представлены посредством этой структуры модели данных. Таким образом, относящиеся к приложению модели данных могут быть обнаружены клиентскими приложениями через сервисный интерфейс.

6.8 Обобщенный интерфейс карты

ИСО/МЭК 24727-2 определяет средства доступа к резидентному карточному приложению на ICC. Обобщенный интерфейс карты, описанный в ИСО/МЭК 24727-2, предоставляет фиксированный набор функциональных возможностей.

Реализация обобщенного интерфейса карты:

- переводит обобщенный запрос в один или несколько специфичных запросов;
- переводит одно или несколько специфичных подтверждений в обобщенное подтверждение.

ИСО/МЭК 24727-2 определяет функциональные возможности, применимые для обработки данных, управления безопасностью и администрирования.

6.9 Связующий интерфейс

В ИСО/МЭК 24727-3 приведено подробное описание связующего интерфейса, применимого для компонентов. Механизмы установления связи определены в ИСО/МЭК 24727-4. Реализацию связующего интерфейса используют для создания канала коммуникации между смежными компонентами в коммуникационном стеке.

6.10 Интерфейс доверительного канала

В ИСО/МЭК 24727-4 приведено подробное описание интерфейса доверительного канала, применимого для компонентов стека. Реализацию интерфейса доверительного канала используют для создания канала безопасной коммуникации между смежными компонентами в стеке протоколов.

7 Основы безопасности

В стандартах серии ИСО/МЭК 24727 используют концепцию безопасности и механизмы защиты, определенные в ИСО/МЭК 7816-4:2005.

В стандартах серии ИСО/МЭК 24727 применен безопасный обмен сообщениями, согласующийся с ИСО/МЭК 7816-4 и установленный в ИСО/МЭК 24727-4.

Безопасность при реализации согласно стандартам серии ИСО/МЭК 24727 зависит от способности преобразовывать механизмы архитектуры безопасности, определенные в ИСО/МЭК 24727-3 и ИСО/МЭК 24727-4, в механизмы архитектуры безопасности, поддерживаемые ICC, как установлено в ИСО/МЭК 7816-4.

Обнаружение криптографической информации может быть реализовано в более чем одной форме, например:

- использование описания функциональных возможностей;
- использование ИСО/МЭК 7816-15, как установлено в ИСО/МЭК 24727-2 и ИСО/МЭК 24727-4.

В ИСО/МЭК 24727-3 подробно описаны механизмы обеспечения безопасности с точки зрения клиентского приложения.

Приложение А
(справочное)

Примеры конфигураций реализации

А.1 Общие положения

В настоящем приложении рассмотрены предполагаемые конфигурации стеков. Их более подробные описания приведены в ИСО/МЭК 24727-4. Набор представленных конфигураций стеков охватывает все случаи использования, установленные к настоящему времени. Тем не менее следует отметить, что стандарты серии ИСО/МЭК 24727 не препятствуют специализации этих конфигураций. Несомненно, такая специализация является важным элементом, необходимым для достижения желаемых уровней функциональной совместимости.

Каждая диаграмма представляет собой проекцию физической архитектуры, где одно клиентское приложение находится во взаимодействии с одним карточным приложением, как показано на рисунке А.1. Возможное расширение обменов запросами/подтверждениями через интерфейс карточного приложения не показано на данных рисунках.

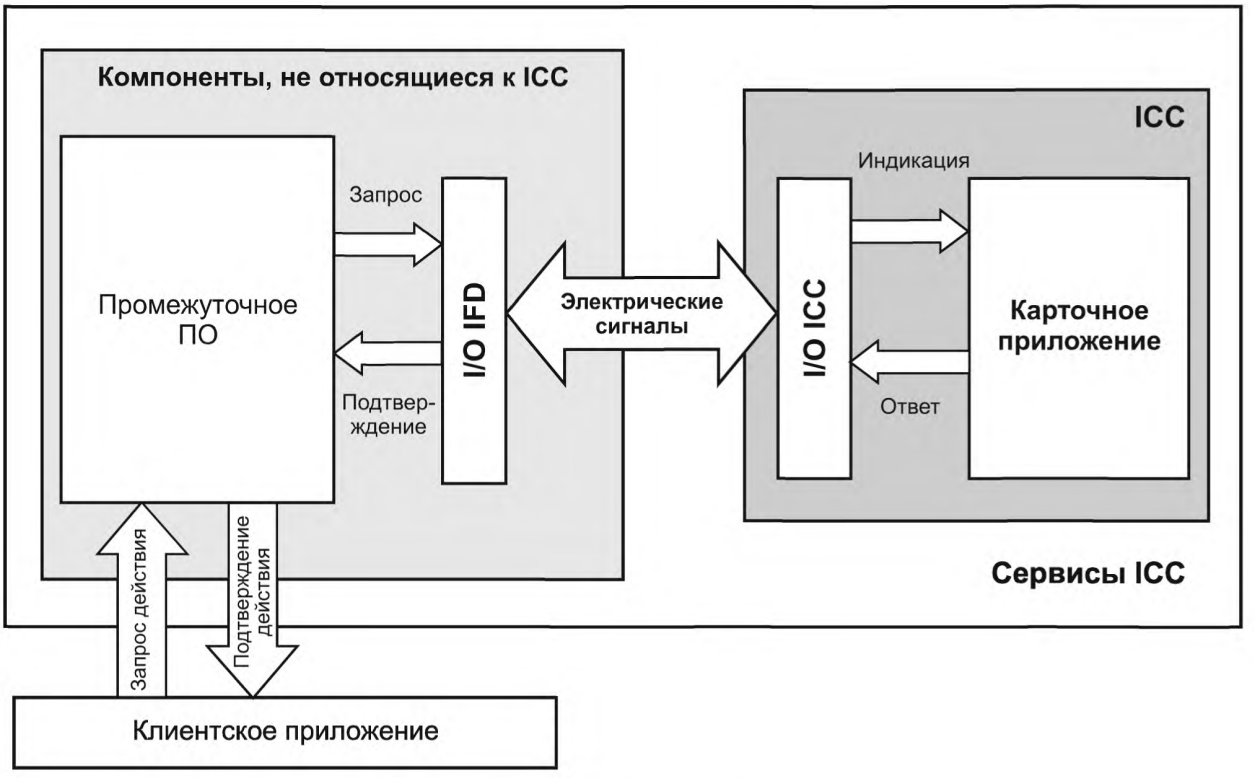


Рисунок А.1 — Физическая архитектура

На рисунке 1 (раздел 6) и на рисунке А.1 показана одна и та же система, но в разных аспектах. На рисунке 1 показано логическое представление архитектуры, а на рисунке А.1 — ее физическое представление. Отображение компонентов между логическим и физическим аспектами зависит от выбранной конфигурации реализации, как показано в общих чертах в следующих подразделах настоящего приложения и детально рассмотрено в ИСО/МЭК 24727-4.

Пояснения к краткому описанию физической архитектуры, представленной на рисунке А.1, приведены ниже.

Сервисы ICC: Реализация, которая предоставляет сервисы клиентскому приложению и включает в работу ICC.

ICC: Элемент сервисов ICC. Является компонентом, идентичным физической ICC.

Компоненты, не относящиеся к ICC: Данный элемент представляет все остальные функциональные возможности, предоставляемые в рамках сервисов ICC. Этот элемент является дополнением к ICC.

Электрические сигналы: Два главных функциональных раздела сервисов ICC осуществляют связь через канал, называемый «Электрические сигналы». Конкретный тип электрических сигналов [например, в соответствии с ИСО/МЭК 7816-3 (протоколы T = 0, T = 1), ИСО/МЭК 7816-12 (USB), ИСО/МЭК 14443 (бесконтактная связь), а также протоколом TLS[1)]] рассмотрен в соответствующих стандартах.

I/O[2)] ICC: Это — компонент ICC. Его назначение заключается в преобразовании сообщений, получаемых по каналу «Электрические сигналы», в запросы, направляемые карточному приложению. Кроме того, данный компонент преобразует подтверждения, получаемые от карточного приложения, в электрические сигналы и посылает их по каналу «Электрические сигналы». Стандарты серии ИСО/МЭК 24727 не определяют I/O ICC.

I/O IFD: Данная функциональность, входящая в состав «компонентов, не относящихся к ICC», отвечает за операции, аналогичные операциям на I/O ICC. Стандарты серии ИСО/МЭК 24727 не определяют I/O IFD.

Карточное приложение: В соответствии с разделом 3.

Промежуточное ПО: В соответствии с разделом 3.

А.2 Конфигурация с отдельными уровнями

Диаграмма конфигурации с отдельными уровнями представлена на рисунке А.2.

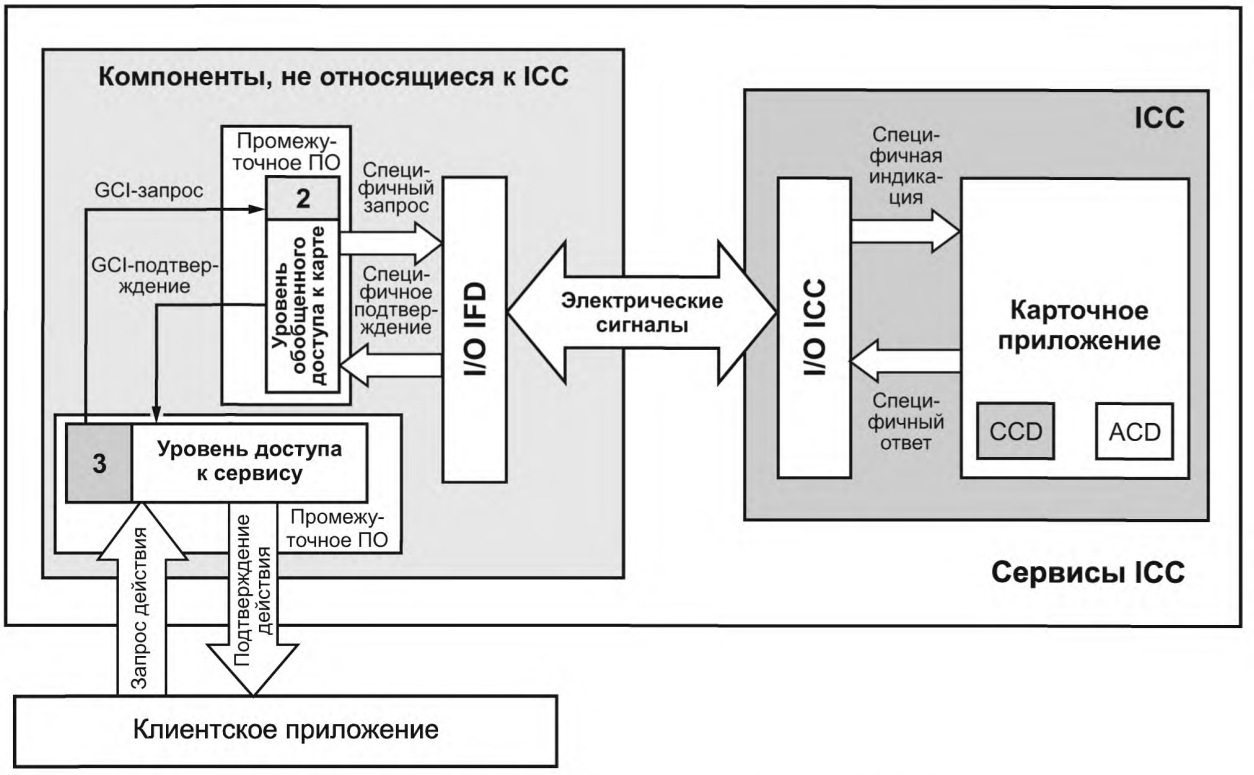


Рисунок А.2 — Отдельная реализация каждого интерфейса и уровня

Данная конфигурация демонстрирует реализацию ИСО/МЭК 24727-2 и ИСО/МЭК 24727-3 в виде отдельных компонентов. Как показано в ИСО/МЭК 24727-4, данный класс реализации может представлять непрозрачный стек ICC или полный сетевой стек.

Данная конфигурация предложена для случая меняющихся требований. Уровень обобщенного доступа к карте, выступающий в качестве прокси ICC, может обеспечивать необходимое преобразование, требуемое для реальной, включенной в работу ICC.

[1)] Безопасность транспортного уровня (transport layer security).

[2)] Ввод/вывод (input/output).

А.3 Объединенная конфигурация

Диаграмма объединенной конфигурации представлена на рисунке А.3.

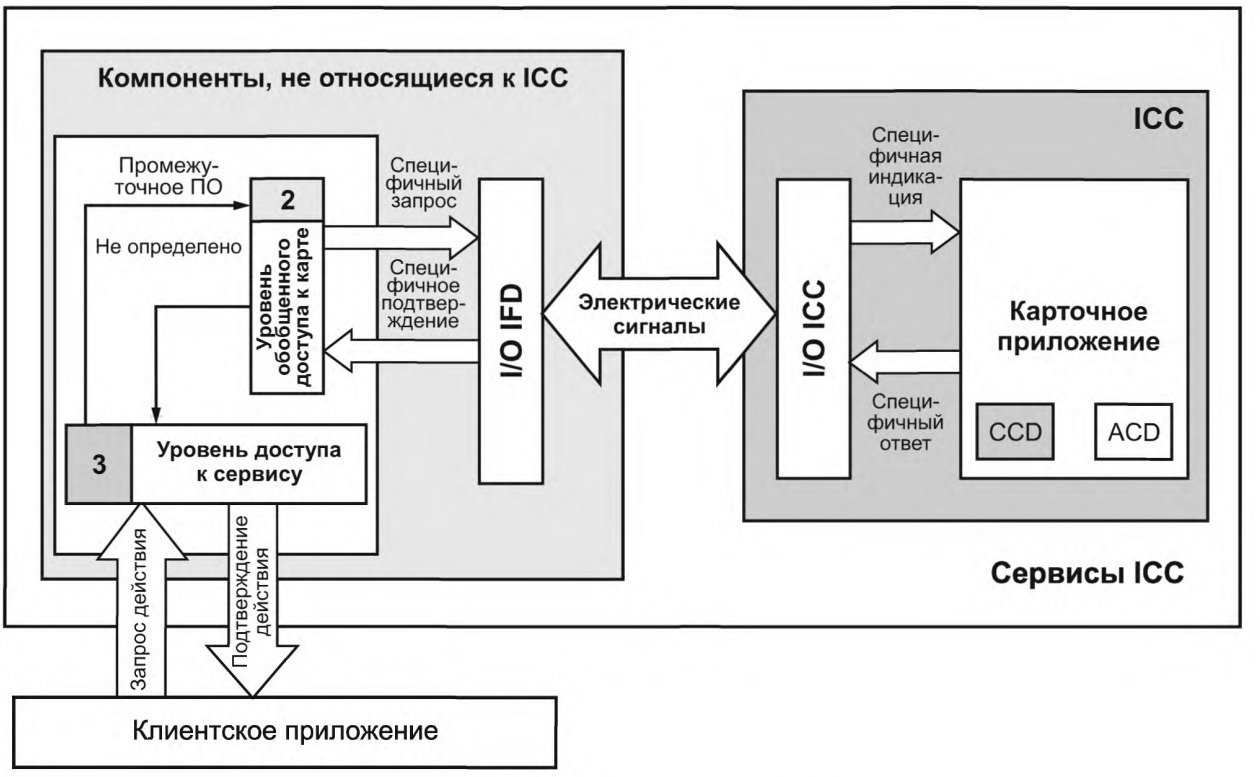


Рисунок А.3 — Объединенная реализация

Данная конфигурация предлагает реализацию сервисного интерфейса, обнаружения и преобразования любого APDU в виде единого компонента программного обеспечения. Взаимодействие между обобщенным интерфейсом карты по ИСО/МЭК 24727-2 и уровнем доступа к сервису по ИСО/МЭК 24727-3 в этом случае не определяют. Как показано в ИСО/МЭК 24727-4, данный класс конфигурации стеков может представлять лояльный стек, удаленный лояльный стек, удаленный стек ICC или резидентный стек ICC.

А.4 Конфигурация с реализацией на ICC уровня обобщенного доступа к карте

Диаграмма конфигурации с реализацией на ICC уровня обобщенного доступа к карте представлена на рисунке А.4.

Данная конфигурация предлагает реализацию на ICC обобщенного интерфейса карты и уровня обобщенного доступа к карте. В ИСО/МЭК 24727-4 это представлено в виде резидентного стека ICC. В данной конфигурации стека доступ к карточному приложению может быть предоставлен с использованием связи на основе APDU через APDU ENVELOPE, указанный в ИСО/МЭК 24727-2[1)], и/или непосредственно через структуру сообщения TLS, если ICC может иметь прямую связь с сетью. Поддержка TLS через прямое сетевое соединение не определена в стандартах серии ИСО/МЭК 7816.

[1)] На APDU ENVELOPE ссылается ИСО/МЭК 24727-4.

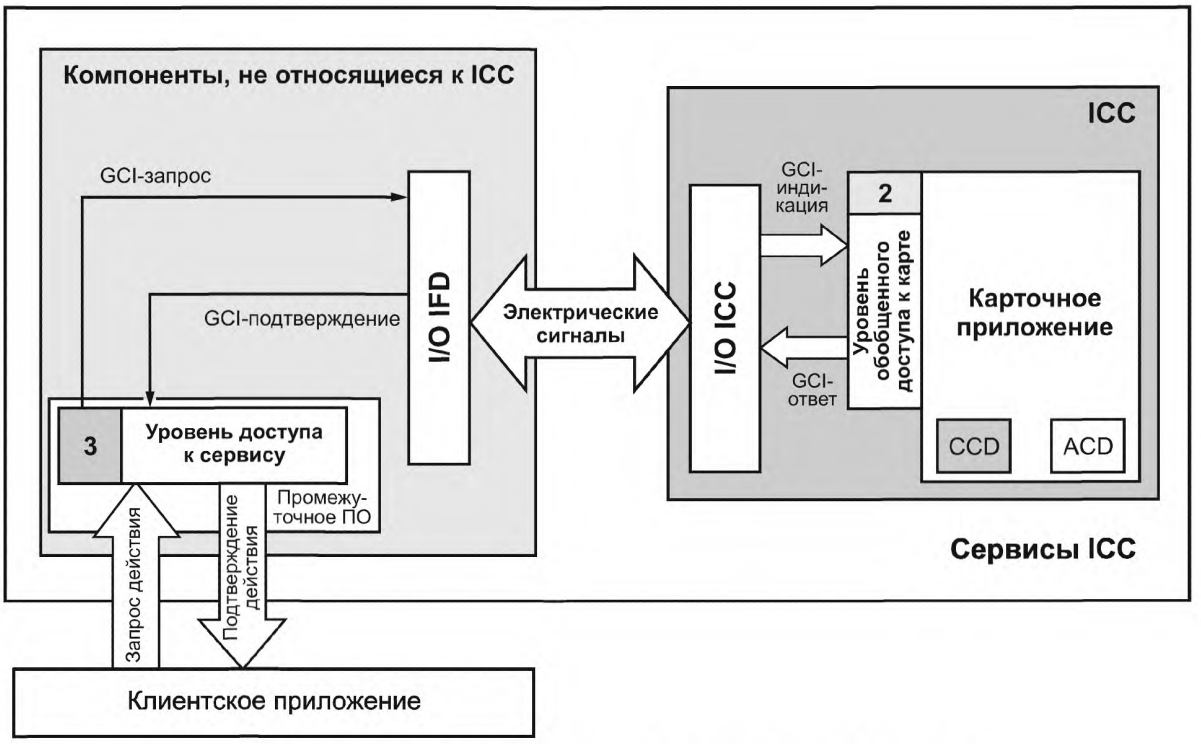


Рисунок А.4 — Уровень обобщенного доступа к карте, реализованный на ICC

А.5 Реализация на ICC уровня доступа к сервису и уровня обобщенного доступа к карте

Диаграмма конфигурации с реализацией на ICC уровня доступа к сервису и уровня обобщенного доступа к карте представлена на рисунке А.5.

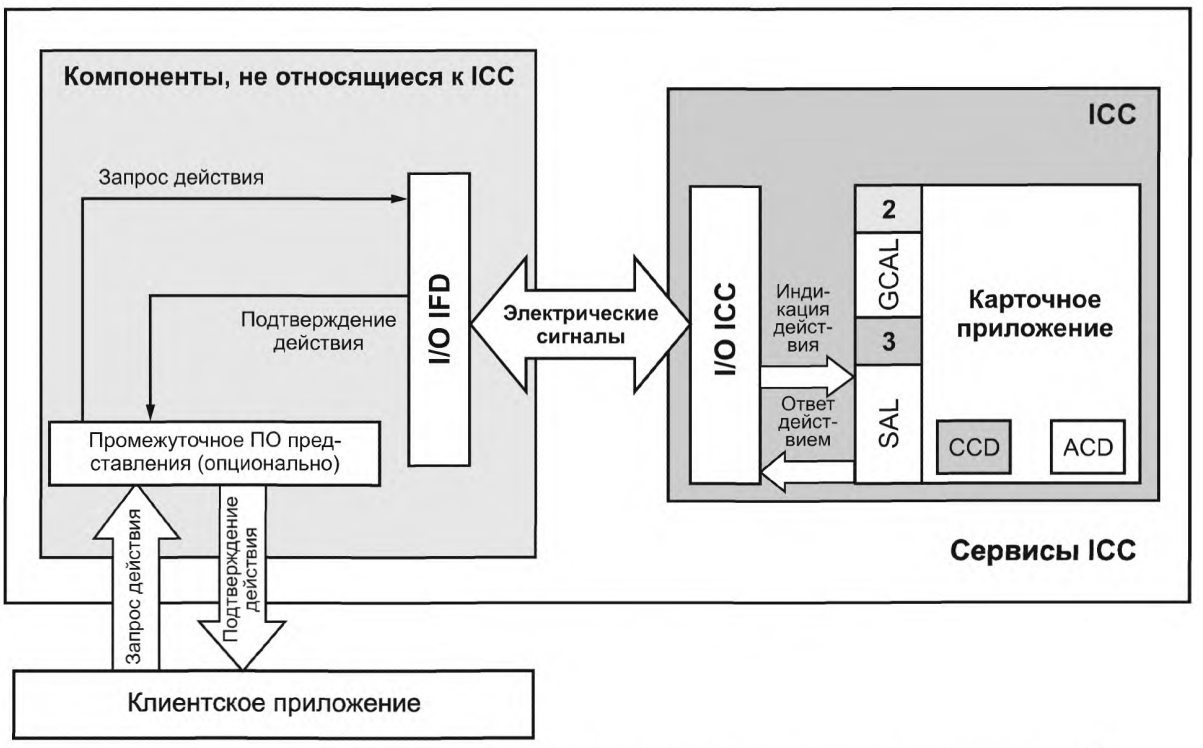


Рисунок А.5 — Уровни доступа к сервису и обобщенного доступа к карте, реализованные на ICC

При данной конфигурации ИСО/МЭК 7816-4 направляет к инкапсуляции действий посредством информационных объектов ACH.1 в форме структур BER-TLV.

А.6 Фиксированное или с загрузкой размещение описания функциональных возможностей на ресурсах компонентов, не относящихся к ICC

Диаграмма конфигурации с фиксированным или с загрузкой размещением описания функциональных возможностей на ресурсах компонентов, не относящихся к ICC, представлена на рисунке А.6.

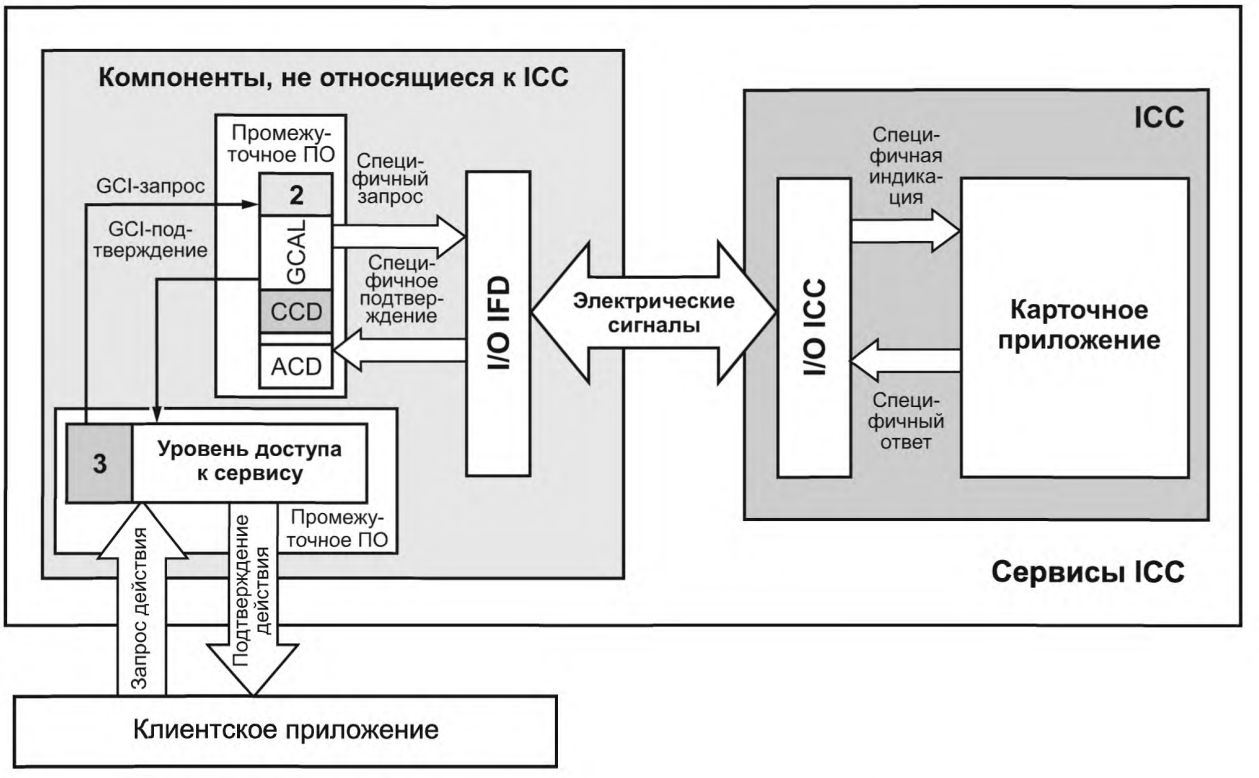


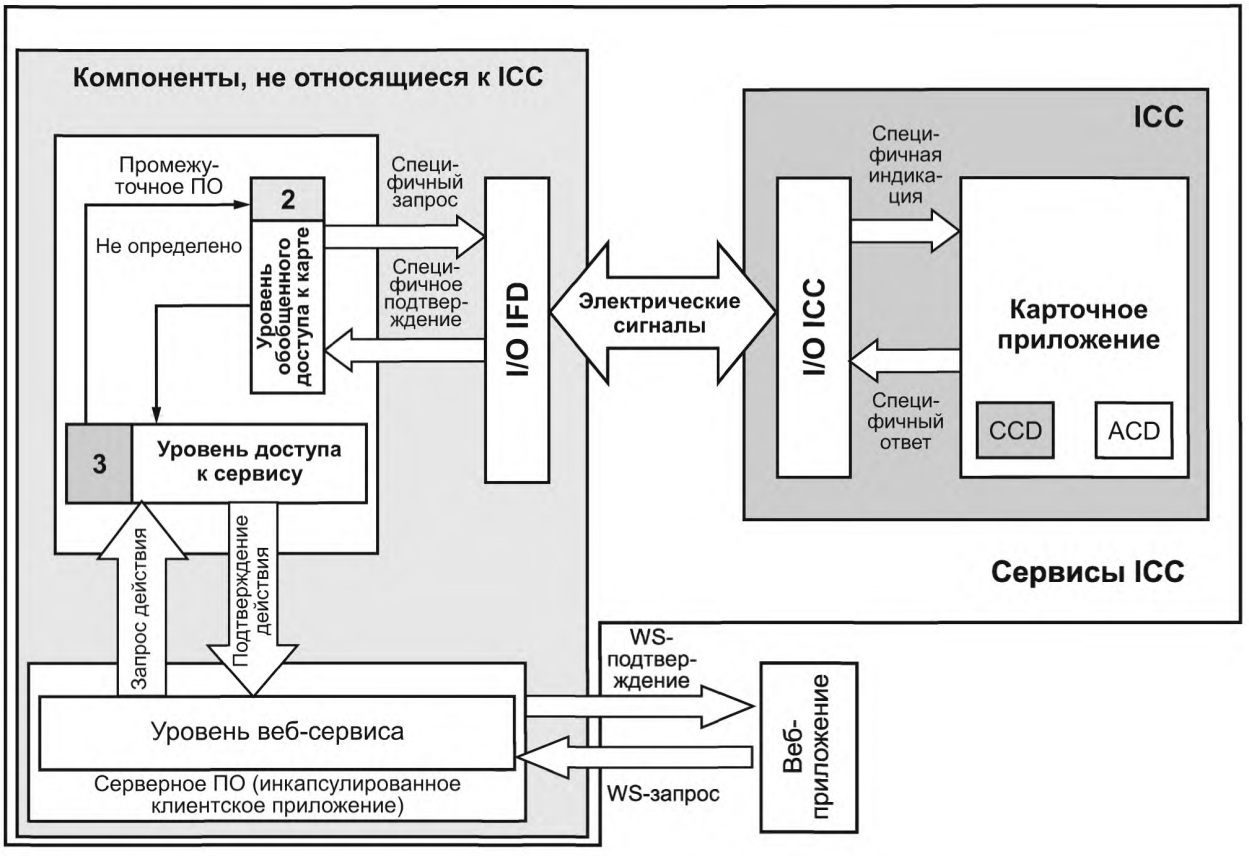
Рисунок А.6 — Загружаемая или фиксированная конфигурация

Загружаемая конфигурация рассчитана на ICC, которая не может поддерживать загрузку описания функциональных возможностей. CCD и ACD предоставляют промежуточное программное обеспечение, используя ресурсы, не связанные с ICC. ИСО/МЭК 24727-2 устанавливает специальный механизм передачи сигналов, посредством которого промежуточное программное обеспечение может обращаться к этим ресурсам.

Фиксированная конфигурация рассчитана на ICC, которая не может поддерживать загрузку описания функциональных возможностей. Более того, промежуточное программное обеспечение поддерживает известный набор реализаций ICC. Описание функциональных возможностей может быть предоставлено явно или следовать из функциональных возможностей промежуточного программного обеспечения (например, загружаемый API).

А.7 Конфигурация с использованием веб-сервиса

Диаграмма конфигурации с использованием веб-сервиса представлена на рисунке А.7.



WS — веб-сервис (web service)

Рисунок А.7 — Конфигурация с использованием веб-сервиса

Данная конфигурация предлагает интерфейс веб-сервиса, который может быть доступен из веб-приложений. Все интерфейсы из стандартов серии ИСО/МЭК 24727 формально определены с использованием прежде всего нотации АСН.1, но во вторую очередь — через XML-описания, что представлено соответственно в ИСО/МЭК 24727-3 и ИСО/МЭК 24727-4.

А.8 Конфигурация со множеством приложений

Диаграмма конфигурации со множеством приложений представлена на рисунке А.8.

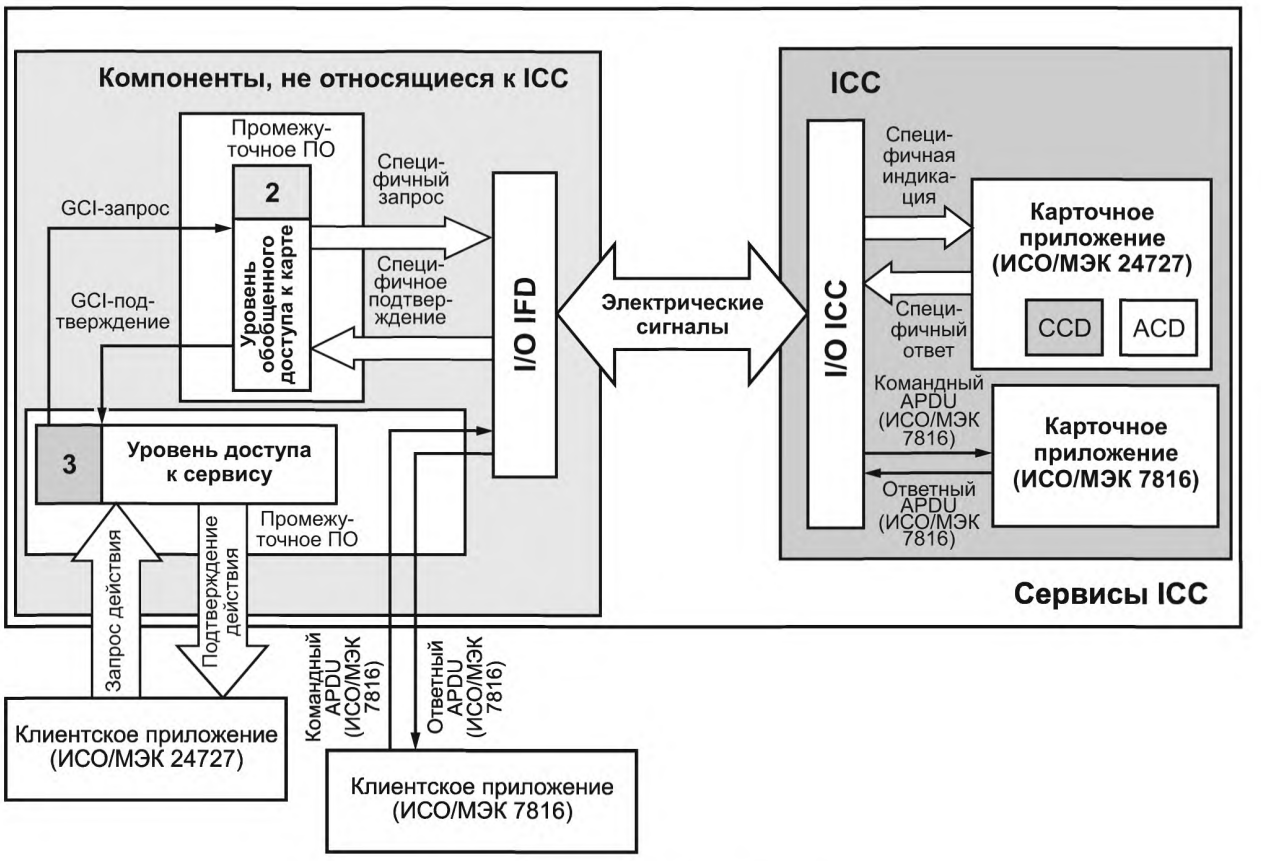


Рисунок А.8 — Конфигурация со множеством приложений

Данная конфигурация демонстрирует сосуществование карточного приложения, соответствующего стандартам серии ИСО/МЭК 24727, на ICC, которая также поддерживает другие карточные приложения — соответствующие стандартам серии ИСО/МЭК 7816. Механизмы размещения и передачи сигналов таких карточных приложений установлены в ИСО/МЭК 24727-3 и ИСО/МЭК 24727-4.

А.9 Распределенная реализация стека

Диаграммы распределенной реализации стека показаны на рисунке А.9.

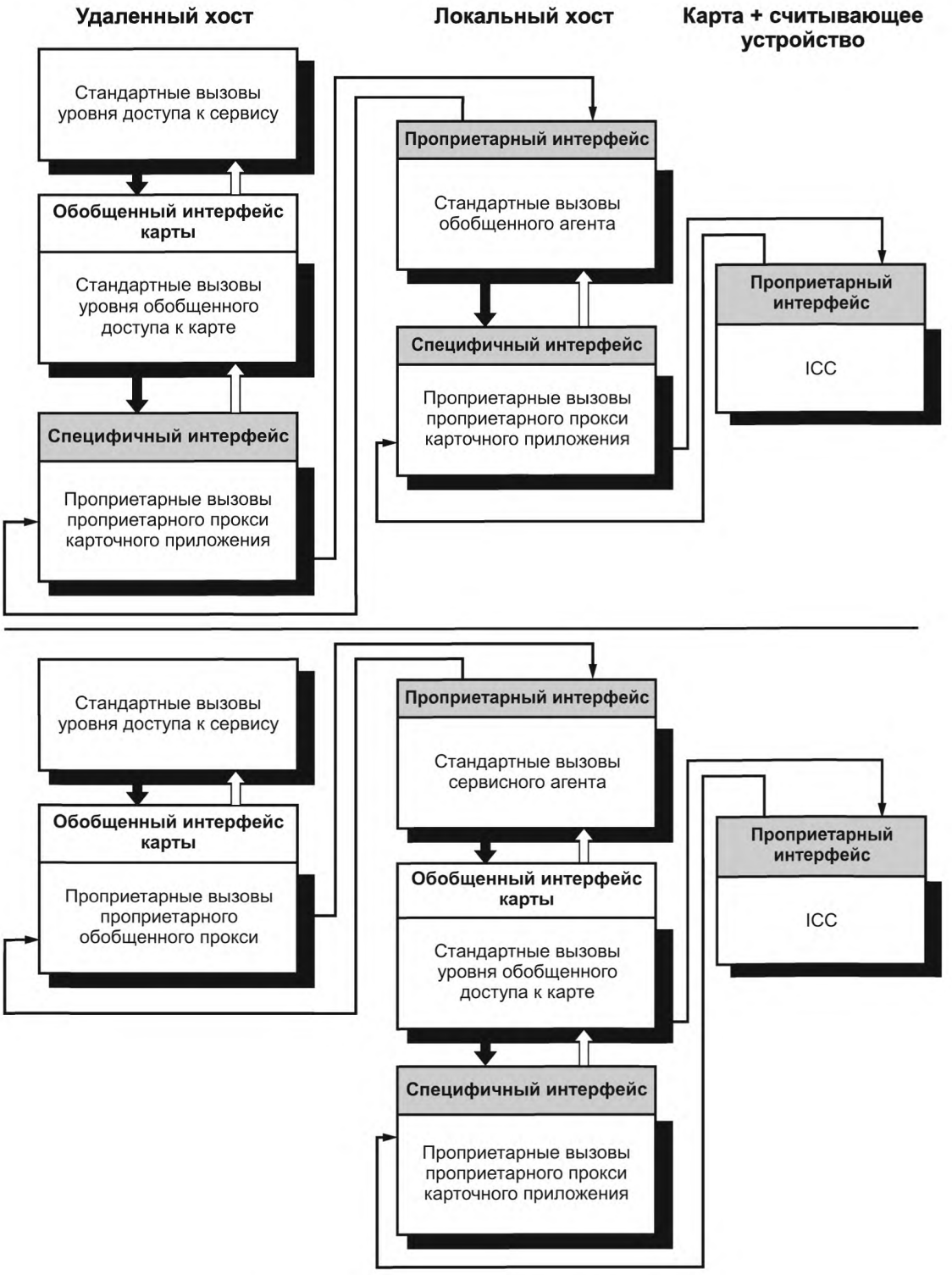


Рисунок А.9 — Распределенная реализация стека

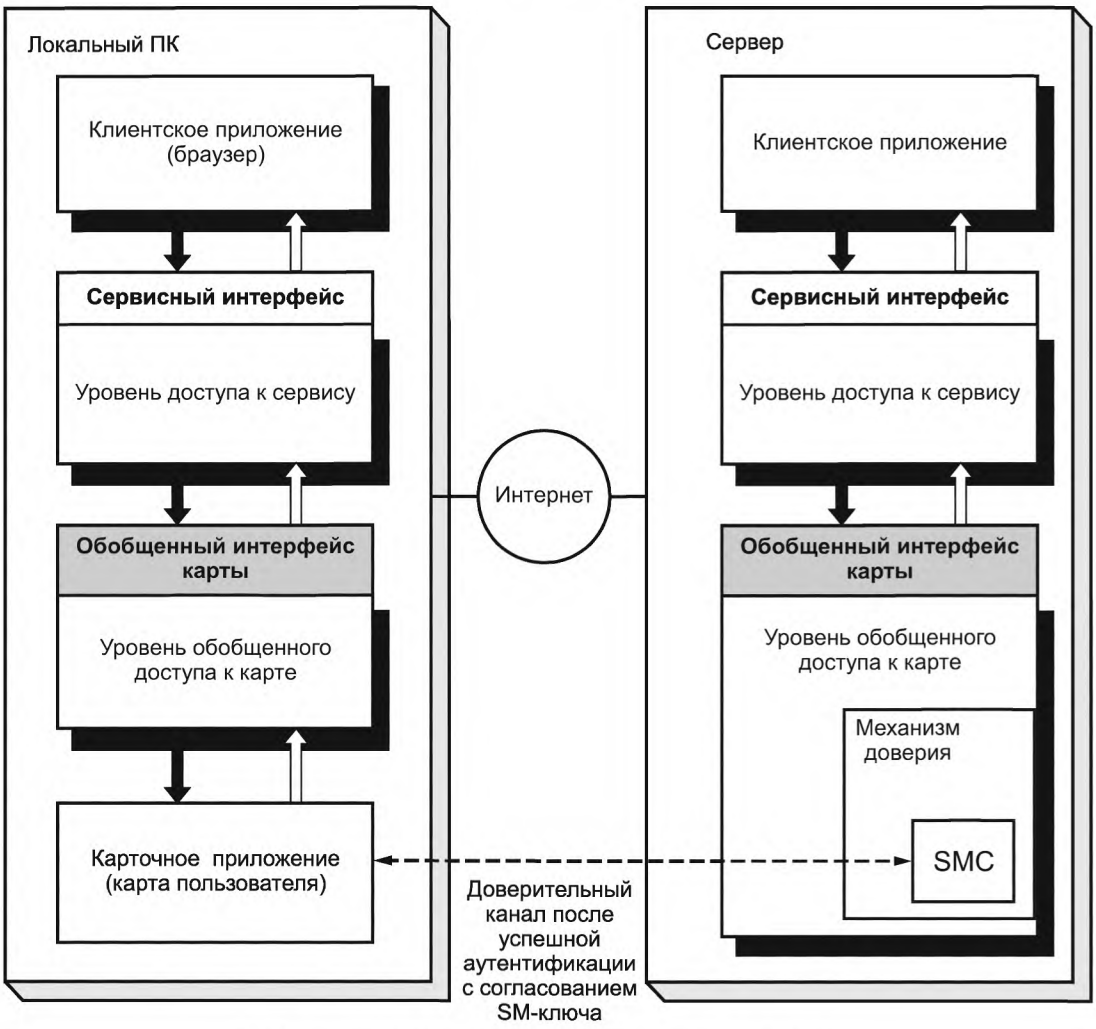
Данные диаграммы используют один и тот же синтаксис (стандартные вызовы, жирный нижний контур прямоугольника) для доступа к специфичному API и обобщенному интерфейсу карты (заштрихованные области). Это гарантирует, что уровни, вставленные в стек или доступные через прокси (например, с помощью эмуляторов карты, инструментария проверки на соответствие), не влияют на стандартные модули при условии, что эти уровни также предлагают обобщенный интерфейс карты и используют стандартные вызовы.

Сервисные вызовы, помеченные как «проприетарные», обеспечивают начальное использование базовых возможностей связи TLS. Они могут последовательно обеспечить использование других протоколов, разрешенных TLS, в том числе исключительно проприетарных протоколов.

Упомянутый механизм прокси-агента описан в ИСО/МЭК 24727-4.

А.10 Распределенная реализация, использующая механизм доверия

Диаграмма распределенной реализации, использующей механизм доверия, показана на рисунке А.10.



SMC — карта с модулем безопасности (security module card);
SM — безопасный обмен сообщениями (secure messaging);
ПК — персональный компьютер

Рисунок А.10 — Распределенная реализация, использующая механизм доверия

Данная конфигурация показывает использование механизмов доверия, описанных в ИСО/МЭК 24727-3 и ИСО/МЭК 24727-4. Серверный уровень обобщенного доступа к карте посылает запрос серверному обобщенному интерфейсу, указывая на необходимость использования механизма доверия.

Механизм доверия с помощью SMC создает защищенный запрос для посылки по доверительному каналу и обрабатывает защищенное подтверждение, поступающее из доверительного канала. Любые ответные данные поступают в виде читаемого текста на серверный уровень обобщенного доступа к карте. Использование SMC подробно рассмотрено в ИСО/МЭК 24727-3 в описаниях API.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 7816-4:2005	IDT	ГОСТ Р ИСО/МЭК 7816-4—2013 «Карты идентификационные. Карты на интегральных схемах. Часть 4. Организация, защита и команды для обмена»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта: IDT — идентичный стандарт.		

Библиография

[1] ETSI TS 102 221, Smart cards; UICC-Terminal interface; Physical and logical characteristics

[2] ETSI TS 102 222, Integrated Circuit Cards (ICC); Administrative commands for telecommunications applications

[3] ETSI TS 102 223, Smart cards; Card Application Toolkit (CAT)

[4] Interoperability Specification for ICCs and Personal Computer Systems, Version 2.0 PC/SC Workgroup, 2004

[5] ISO 3166-1, Codes for the representation of names of countries and their subdivisions — Part 1: Country codes

[6] ISO/IEC 7498-1|ITU-T Rec. X.200, Information technology — Open System Interconnection — Basic Reference Model: The Basic Model

[7] ISO/IEC 7812-1, Identification cards — Identification of issuers — Part 1: Numbering system

[8] ISO/IEC 7816-3, Identification cards — Integrated circuit cards — Part 3: Cards with contacts — Electrical interface and transmission protocols

[9] ISO/IEC 7816-6, Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange

[10] ISO/IEC 7816-8, Identification cards — Integrated circuit cards — Part 8: Commands for security operations

[11] ISO/IEC 7816-9, Identification cards — Integrated circuit cards — Part 9: Commands for card management

[12] ISO/IEC 7816-12, Identification cards — Integrated circuit cards — Part 12: Cards with contacts — USB electrical interface and operating procedures

[13] ISO/IEC 7816-13, Identification cards — Integrated circuit cards — Part 13: Commands for application management in multi-application environment

[14] ISO/IEC 7816-15, Identification cards — Integrated circuit cards — Part 15: Cryptographic information application

[15] ISO/IEC 8825-1, Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

[16] ISO/IEC TR 9577:1999, Information technology — Protocol identification in the network layer

[17] ISO/IEC 9796 (all parts), Information technology — Security techniques — Digital signature schemes giving message recovery

[18] ISO/IEC 9797 (all parts), Information technology — Security techniques — Message Authentication Codes (MACs)

[19] ISO/IEC 9798 (all parts), Information technology — Security techniques — Entity authentication

[20] ISO 9992-2, Financial transaction cards — Messages between the integrated circuit card and the card accepting device — Part 2: Functions, messages (commands and responses), data elements and structures

[21] ISO/IEC 10116, Information technology — Security techniques — Modes of operation for an n-bit block cipher

[22] ISO/IEC 10118 (all parts), Information technology — Security techniques — Hash-functions

[23] ISO/IEC 10536 (all parts), Identification cards — Contactless integrated circuit(s) cards — Close-coupled cards

[24] ISO/IEC 11770 (all parts), Information technology — Security techniques — Key management

[25] ISO/IEC 14443 (all parts), Identification cards — Contactless integrated circuit(s) cards — Proximity cards

[26] ISO/IEC 14888 (all parts), Information technology — Security techniques — Digital signatures with appendix

[27] ISO/IEC 18033 (all parts), Information technology — Security techniques — Encryption algorithms

[28] ISO/IEC 24727-2, Identification cards — Integrated circuit cards programming interfaces — Part 2: Generic card interface

[29] ISO/IEC 24727-3, Identification cards — Integrated circuit card programming interfaces — Part 3: Application interface

[30] ISO/IEC 24727-4, Identification cards — Integrated circuit card programming interfaces — Part 4: Application programming interface (API) administration

[31] ISO/IEC 24727-5, Identification cards — Integrated circuit card programming interfaces — Part 5: Testing procedures

[32] ISO/IEC 24727-6, Identification cards — Integrated circuit card programming interfaces — Part 6: Registration authority procedures for the authentication protocols for interoperability

УДК 336.77:002:006.354 ОКС 35.240.15 Э46 ОКП 40 8470

Ключевые слова: обработка данных, обмен информацией, идентификационные карты, IC-карты, передача данных, программные интерфейсы, архитектура

Редактор *Л.И. Потапова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 01.12.2016. Подписано в печать 29.12.2016. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,52. Тираж 27 экз. Зак. 3337.
Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru