ООО «Компания ДЕМОС»

УДК 654.1

ДКБМ.02-РД.4.1

Инв. № 4

УТВЕРЖДАЮ

генеральный директор

_____ Бородько А.П.

«_____»_____ 2013 г.

ОТЧЕТ О НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЕ

«Исследование технологических сценариев формирования сервисов персональной идентификации граждан для безопасного доступа к государственным и муниципальным услугам на коммуникационной среде оператора мобильной связи»

(Шифр темы: E/M-ID)

_____

Москва 2013

Реферат

Отчет 148 с., 24 рис., 6 табл., 18 источников, 2 прил.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ, ГОСУСЛУГИ, ЗАЩИЩЕННЫЙ ДОСТУП, КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ, КЛЮЧЕВОЙ МАТЕРИАЛ

Объектом исследования являются системы персональной идентификации пользователей государственных и муниципальных сервисов в электронном виде.

Цель работы — исследование технологических сценариев формирования сервисов персональной идентификации граждан для безопасного доступа к государственным и муниципальным услугам на коммуникационной среде оператора мобильной связи.

В работе проводился всесторонний анализ текущего уровня информационной безопасности инфраструктуры доступа к государственным и муниципальным сервисам в электронном виде.

В результате исследования были предложены механизмы обеспечения защищенного доступа к государственным и муниципальным сервисам в электронном виде. Так же были разработаны методические рекомендаций по управлению жизненным циклом ключевого материала инфраструктуры защищенного доступа к государственным и муниципальным сервисам в электронном виде. Разработаны рекомендаций по нормативно-правовому обеспечению процесса взаимодействия сервисов защищенного доступа с инфраструктурой государственных и муниципальных сервисов в электронном виде.

Полученные результаты могут быть использованы при построении сложных распределенных информационных систем в органах государственной

власти, в органах власти субъектов Российской Федерации, местного самоуправления, а также в бюджетных организациях.

Содержание

Нормативные ссылки

В настоящем отчете о НИР использованы ссылки на следующие стандарты.

ГОСТ 15971-90 Системы обработки информации. Термины и определения.

ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

ГОСТ Р 34.10-2001. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.

ГОСТ Р 34.11-94 Информационная технология. Криптографическая защита информации. Функция хэширования.

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения.

ГОСТ Р ИСО 7498-2-99 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

ГОСТ Р 51624-2000 Автоматизированные системы в защищенном исполнении.

ГОСТ Р ИСО/МЭК 7816-1-2010 Карты идентификационные. Карты на интегральных схемах с контактами. Часть 1. Физические характеристики.

ГОСТ Р ИСО/МЭК 7816-2-2010 Карты идентификационные. Карты на интегральных схемах. Часть 2. Карты с контактами. Размеры и расположение контактов.

ГОСТ Р ИСО/МЭК 7816-6-2003 Карты идентификационные. Карты на интегральных схемах с контактами. Часть 6. Элементы данных для межотраслевого обмена.

ГОСТ Р ИСО/МЭК 7816-10-2004 Карты идентификационные. Карты на интегральных схемах с контактами. Часть 10. Электронные сигналы и ответ на восстановление у синхронных карт.

ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

ОСТ 45.127-99. Система обеспечения информационной безопасности Взаимоувязанной сети связи Российской Федерации. Термины и определения.

Определения

В настоящем документе используются следующие термины и определения.

Аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности (ОСТ 45.127-99).

База данных — представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью электронной вычислительной машины (ЭВМ). (п.2 ст.1260 Гражданского кодекса РФ Российской Федерации, часть четвертая, с изменениями от 18 декабря 2006 г. N 230-ФЗ 6 декабря 2011 г.).

Безопасность информации (данных) — состояние защищенности информации (данных), обрабатываемой средствами вычислительной техники или автоматизированной системы, от внутренних или внешних угроз (ОСТ 45.127-99).

Данные — информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека (ГОСТ Р 15971-90, ОСТ 45.127-99).

Дестабилизирующие факторы — явление или событие, следствием наступления которого может быть нарушение конфиденциальности, целостности или доступности информационных ресурсов.

Документ — информационный объект в виде текста, звукозаписи или изображения. В качестве документов могут выступать: нормативные, распорядительные, организационные, договорные, плановые, внутренние документы (служебные записки, заказы-заявки, записи, информационные письма, техническая и проектная документация).

Доступ несанкционированный к информации — доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами (ОСТ 45.127-99).

Доступность — свойство быть доступным и используемым по запросу со стороны уполномоченного логического объекта (ГОСТ Р ИСО 7498-2-99).

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию (ГОСТ Р 50922-2006, ОСТ 45.127-99).

Защита информации от несанкционированного доступа — деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации. (ГОСТ Р 50922-2006).

Защищаемая информация — информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (ГОСТ Р 50922-2006).

Злоумышленник — лицо, осуществляющее осознанные действия по нарушению информационной безопасности объекта защиты.

Идентификация — присвоение субъектам и объектам доступа идентификатора и/или сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация — сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления (Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Информационная безопасность — Свойство информации сохранять конфиденциальность, целостность и доступность. (ГОСТ Р ИСО/МЭК 27001-2006).

Информационные ресурсы — отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах) (Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Информационная система — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи (Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»).

Канал — маршрут передачи информации (ГОСТ Р ИСО 7498-2-99).

Криптографическая защита — защита данных при помощи криптографического преобразования данных (ГОСТ 28147-89).

Мероприятие по защите информации — совокупность действий, направленных на разработку и/или практическое применение способов и средств защиты информации.

Меры обеспечения информационной безопасности — правовые, организационные, программные и аппаратные способы, правила и процедуры использования механизмов обеспечения информационной безопасности.

Механизм обеспечения информационной безопасности — аппаратно-программные и организационные средства системы обеспечения информационной безопасности, реализующие в соответствии с заданной политикой информационной безопасности один или несколько аспектов защиты информационной сферы в соответствии с одним из трех перекрывающих друг друга классов защиты: предотвращение воздействий нарушителя информационной безопасности, обнаружение воздействия

нарушителя информационной безопасности, восстановление (ликвидация) последствия воздействия нарушителя информационной безопасности.

Нарушитель информационной безопасности — физическое или юридическое лицо, общественное объединение, ведомство, процесс, событие, способное произвести несанкционированные или непреднамеренные действия (операции) над информационной сферой объекта защиты, приводящие к нежелательным для пользователя или Компании связи последствиям (ОСТ 45.127-99).

Объект защиты информации — информация, или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации (ГОСТ Р 50922-2006).

Средство защиты информации — техническое, программное средство, вещество и /или материал, предназначенные или используемые для защиты информации (ГОСТ Р 50922-2006).

Угроза безопасности информации — совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее (ГОСТ Р 51624-2000).

Угроза информационной безопасности — см. «угроза безопасности информации».

Целостность информации — способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения) (ОСТ 45.127-99).

Уязвимость — некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации (ГОСТ Р ИСО 7498-2-99).

Обозначения и сокращения

В настоящем документе используются следующие обозначения и сокращения.

AuC — центр аутентификации (Authentication Center)

IMSI — международный идентификатор мобильного абонента (International Mobile Subscriber Identity)

ICCID — карта с интегрированными электронными цепями (Integrated Circuit Card Identifier)

HLR — реестр собственных абонентов (Home Location Register)

MSISDN — цифровой номер встроенных сервисов мобильной станции (Mobile Station Integrated Services Digital Number)

NFC — коммуникация ближнего поля (Near Field Communication)

OTA — по воздуху (Over-the-Air)

OTP — одноразовый пароль (One-Time-Password)

(U)SIM — универсальный идентификационный модуль абонента (Universal) Subscriber Identity Module

VPN — виртуальная частная сеть (Virtual Private Network)

AAA — аутентификация, авторизация, аккаунтинг

БД — база данных

ГЭПС — государственная электронная почтовая связь

ЕПГУ — единый портал государственных услуг

ИВС — информационно-вычислительная сеть

ИБ — информационная безопасность

ИС — информационная система

ИТ — информационные технологии

НСД — несанкционированный доступ

ОС — операционная система

ПГУ — портал государственных услуг

ПО — программное обеспечение

СНИЛС — страховой номер индивидуального лицевого счета застрахованного лица

СОИБ — система обеспечения информационной безопасности

СОРМ — система оперативно-розыскных мероприятий

СУБД — система управления базами данных

ТС — технические средства

ФУО — федеральная уполномоченная организация

Введение

Процедура аутентификации знакома любому пользователю ПК или мобильного телефона. У многих есть магнитные пропуска для прохода в офис, токены для входа в корпоративный VPN (Virtual Private Network). Большинство из нас пользуется этими устройствами не задумываясь, в то время как, в основе них могут лежать совершенно разные технологии. Многообразие услуг, требующих жесткой аутентификации, порождает тезис о необходимости платформы аутентификации «все-в-одном», которая решала бы вопросы доступа к ресурсам, физического доступа, а также предоставляла дополнительные возможности, такие как шифрование и цифровая подпись. Цель данной работы – обобщить опыт в построении схем аутентификации, дать концептуальную схему создания универсального сервиса аутентификации, а также описать дальнейшие перспективы развития этой системы и её эволюции к федеральной инфраструктуре идентификации граждан [1-3].

В соответствии с распоряжением правительства от 20 октября 2010 г. № 1815-р «О государственной программе Российской Федерации «Информационное общество (2011 - 2020 годы)» в указанный период будет проведена масштабная работа по информатизации государственных органов и переводу государственных и муниципальных услуг на схему их предоставления в электронной форме. При этом актуализируется задача идентификации субъектов в электронном взаимодействии при предоставлении государственных и муниципальных услуг в электронной форме, что потребует, в свою очередь наличия удобной и безопасной схемы аутентификации и защищенного доступа подписчика услуги. Примером может служить услуга мобильного (электронного) голосования, которая в данный момент используется в рамках эксперимента - в соответствии с требованиями по проведению голосования в

РФ: необходимо аутентифицировать гражданина перед процедурой голосования.

Таким образом, можно утверждать, что аутентификация является не только ключевым и одним из центральных элементов в безопасности любого вида государственных и муниципальных услуг, но и социально-прагматической потребностью. На сегодняшний день схемы аутентификации востребованы и внедрены для решения широкого круга вопросов – сетевой доступ (VPN, Wi-Fi), доступ к web-ресурсам, подпись контента и DRM (Digital Rights Management), физический доступ, доступ к персональным данным (платежи, медицина) и многое другое.

Очевидно, что востребованность аутентификации в столь широком круге услуг, наводит на мысль об универсальной платформе для защищенного доступа к государственным и муниципальным услугам в электронной форме. Рассмотрим, каким же, по нашему мнению, должен быть современный сервис защищенного доступа к государственным и муниципальным услугам в электронной форме. В первую очередь сервис должен поддерживать возможность взаимодействия с максимально широким спектром услуг и софтверных платформ. Также немаловажной является возможность использовать при аутентификации контейнеры с ключами произвольного типа – токены, смарт-карты, мобильные телефоны и планшетные компьютеры и т.п. Из требований по распространенности платформы для аутентификации вытекает следующая группа требований – по интероперабельности, суть которых сводится к тому, что архитектура сервиса аутентификации не должна ни коим образом зависеть от приложения, с которым он взаимодействует, достигнуть этого можно, например, используя открытые стандарты протоколов аутентификации и работы с ключевым материалом. Также среди ключевых аспектов при разработке предложений по архитектуре сервиса защищенного доступа стоит отметить стоимость такого решения и готовность сопутствующей инфраструктуры – потенциальное внедрение сервиса

защищенного доступа к государственным и муниципальным услугам в электронной форме должно быть максимально доступным и быстрым.

Что касается непосредственно методов аутентификации, для универсальной схемы более всего подходят открытые стандарты, не предъявляющие серьезных требований к аппаратной части пользовательских устройств для аутентификации. Тип ключевого материала, а также набор операций с ним, накладывает ограничения на форм-фактор, в котором будет выполнен контейнер для ключевого материала. Так, например, использовать вычисления по криптографическим алгоритмам можно только со смарт-картой с имплантированным криптографическим процессором. Цена таких смарт-карт достаточно высока, и их будет трудно использовать, например, в мобильных телефонах, в качестве SIM-модулей (Subscriber Identity Module).

Реализация дополнительных возможностей на произвольном устройстве для аутентификации, таких, как шифрование и цифровая подпись, возможна с использованием концепции виртуальной смарт-карты. Коротко суть её такова: поскольку не все устройства обладают достаточными вычислительными возможностями для реализации дополнительной функциональности (например, достаточно «простая» SIM-карта мобильного телефона) помимо встроенных в аутентификатор атрибутов, например сертификата, оператор хранит у себя под надежной защитой своего HSM (Hardware Security Module) дополнительные атрибуты, например ключи для шифрования и цифровой подписи. Аутентифицированный пользователь, получает возможность использовать эти атрибуты на стороне оператора, получая в свой доступ аппаратные возможности HSM для совершения криптографических операций и цифровой подписи. На основе разработанных логической и вероятностной моделей оценки защищённости универсального сервиса аутентификации межет быть разработана методология формирования прикладных политик информационной безопасности любых сервисов потребителя.

Перечисленные условия являются необходимыми, чтобы схема аутентификации стала универсальной и покрывала как можно большее многообразие сервисов. При таком подходе пользователь получает в руки контейнер с ключами, с помощью которого он получает доступ практически к любой услуге. Возникает резонный вопрос об унификации такого подхода на федеральном уровне и создании единого сервиса аутентификации и идентификации федерального масштаба. Без такого сервиса невозможно эффективное, доверенное функционирование систем, разрабатываемых в рамках программы «Электронная Россия» в настоящее время [4, 5].

Использование ресурсов операторов информационно-коммуникационных сетей для аутентификации и идентификации пользователей государственных услуг напрямую обозначено *в Государственной программе «Информационное Общество» на 2011-2020 гг. в разделе 2* («Направления и задачи Программы», Направление 1:»Повышение качества жизни граждан и улучшение условий развития бизнеса»). В этом разделе документа обозначено следующее: *«Появятся новые государственные и муниципальные услуги, реализация которых в настоящее время невозможна, например:* **с *помощью мобильного телефона осуществляется идентификация заявителя,*** *доступ к информационным сервисам предоставления государственных услуг в электронном виде, платежи за государственные услуги…».*

Ресурсы операторов информационно-коммуникационных сетей в настоящий момент уже позволяют в полной мере реализовать сервис защищенного доступа к государственным и муниципальным услугам в электронной форме как федеральную идентификационную службу граждан. Также стоит заметить, что в совокупности операторы информационно-телекоммуникационных сетей обладают пользовательской базой, покрывающей практически все население Российской Федерации, что немаловажно при обеспечении государственными услугами в электронной форме как можно большего числа граждан.

Дальнейшее развитие концепции сервиса идентификации в федеральном масштабе связано главным образом с развитием и совершенствованием сетей связи, и, в первую очередь, переходом операторов на IMS (IP Multimedia Subsystem) – стандартизованный подход к построению инфокоммуникационной сети, позволяющий быстро внедрять новые услуги. С точки зрения сервиса идентификации IMS интересна в первую очередь тем, что имеет выделенные элементы для осуществления управления механизмами аутентификации – AAA-сервер и HSS (Home Subscriber Server). Последний представляет собой универсальную БД, хранящую профиль пользователей. Стандартизованные интерфейсы HSS, в отличие от интерфейсов других БД пользователей, могут обеспечить интеграционное взаимодействие, порождающее глобальную БД пользователей. При этом сам пользователь сможет получить доступ к услуге своего оператора из любой точки мира, за счет IMS-роуминга.

Предложенная в работе схема сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме, позволяет существенным образом повысить доступность и дружественность государственных услуг в электронной форме, а также соблюсти требования законодательства и СОРМ. Основа для такого сервиса защищенного доступа – открытые стандарты. В приложении А приводится дополнительная нормативная база.

1 Экспертиза текущего уровня информационной безопасности инфраструктуры доступа к государственным и муниципальным сервисам в электронном виде

Комлексное обследование уровня ИБ для государственных и муниципальных услуг в электронном виде представляет собой сложную систему организационно-технических мероприятий, требующую разработки методик оценки уровня ИБ и способов аудита. В данной работе экспертиза уровня информационной безопасности инфраструктуры доступа к государственным и муниципальным услугам производится, исходя из следующих принципов:

- заключение по уровню ИБ носит экспертный характер;
- уровень ИБ оценивается с точки зрения используемых при доступе к государственным и муниципальным услугам в электронном виде схем аутентификации и идентификации;
- используемые при доступе к государственным и муниципальным услугам схемы аутентификации и идентификации также оцениваются с точки зрения возможности обеспечения мобильности пользователя и их влияния на ИБ, а также с точки зрения применимости совместно с перспективными средствами получения государственных и муниципальных услуг в электронном виде – мобилльные телефоны, планшетные компьютеры.

Полученные в результате экспертизы материалы являются основой для заклчения об уровне ИБ при доступе к государственным и муниципальным услугам в электронной форме, а также о необходимости использования дополнительных мер по обеспечению информационной безопасности граждан при их доступе к государственным и муниципальным услугам в электронной форме.

1.1 Анализ используемых схем аутентификации/идентификации для доступа к государственным и муниципальным сервисам в электронном виде

В соответствии с Системным проектом инфраструктуры Электронного Правительства Российской Федерации, утвержденным Правительственной комиссией по ИТ 13 июля 2010 года инфраструктура информационных систем электронного правительства выглядит следующим образом. На рисунке 1 приведен состав систем электронного правительства.

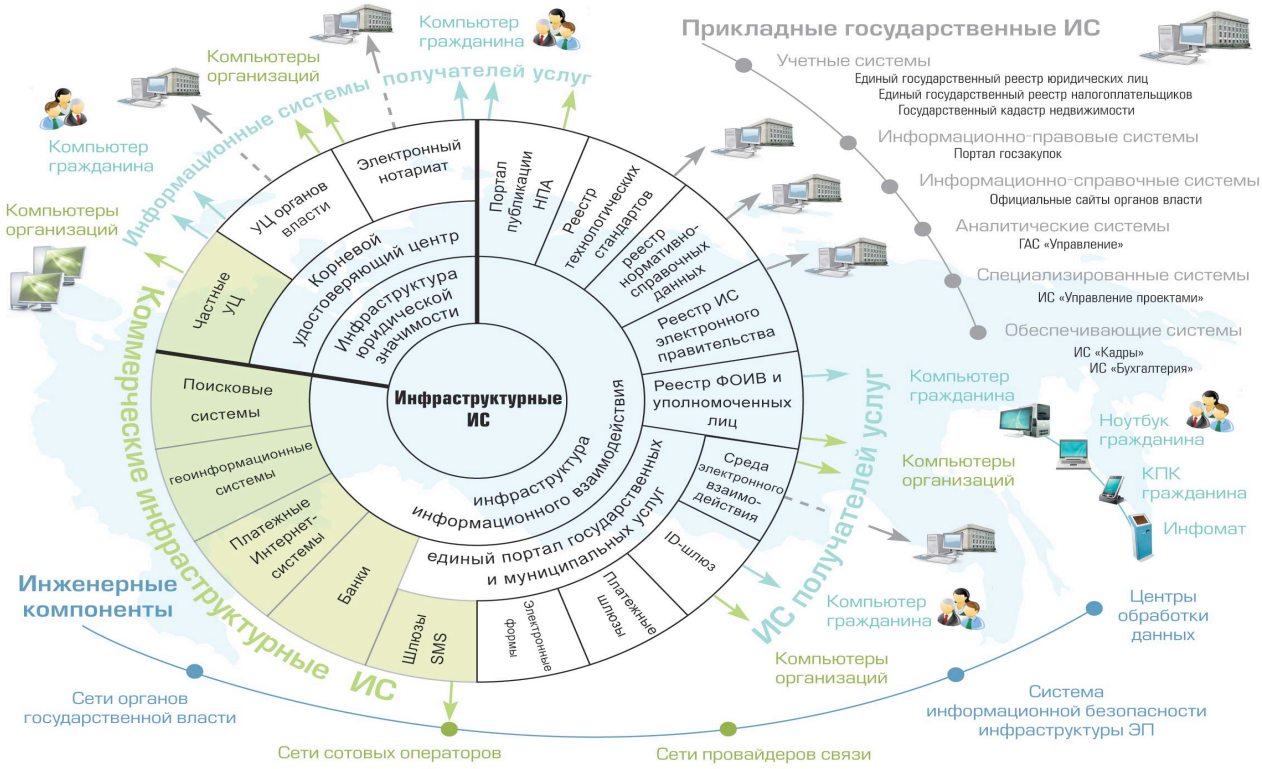

Рисунок 1 — Состав информационных систем электронного правительства

Используемые при реализации инфраструктуры систем электронного правительства способы доступа должны обеспечивать прозрачное взаимодействие с инфраструктурой электронного правительства и бесшовно интегрироваться с ней.

1.1.1 Описание схем аутентификации/идентификации для доступа к государственным и муниципальным сервисам в электронном виде

В соответствии с федеральный законом Российской Федерации от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» предоставление государственных и муниципальных услуг в электронном виде – это предоставление государственных и муниципальных услуг с использованием информационно-телекоммуникационных технологий, в том числе с использованием портала государственных и муниципальных услуг, многофункциональных центров, универсальной электронной карты и других средств, включая осуществление в рамках такого предоставления электронного взаимодействия между государственными органами, органами местного самоуправления, организациями и заявителями. Модернизация общественных коммуникаций – основной тренд развития общественных отношений, в силу того, что общественные коммуникации – одно из базовых проявлений жизнедеятельности общества. В частности, в настоящее время разрабатывается проект электронного правительства с целью перехода к электронному безбумажному документообороту в различных видах общественных коммуникаций.

Базовые варианты идентификации при удаленном доступе граждан и организаций к сервисам электронного правительства перечислены ниже в порядке возрастания надежности [6]:

- нестрогая идентификация на основе синтетического идентификатора пользователя или его аналогов без аутентификации (например, адресом электронной почты);
- идентификация на основе многоразовых логина и пароля, выбранных пользователем;

- идентификация, основанная на информации (знаниях), известных только идентифицируемому лицу (например, данные банковского счета, биографии пользователя, учетных данных мобильного оператора и др.);
- одноразовый пароль с использованием аппаратного токена, смарт-карты, одноразовый пароль, выдаваемый гражданину после установления его личности, одноразовый пароль, передаваемый по независимым каналам связи;
- идентификация на основе инфраструктуры открытых ключей с хранением закрытого ключа подписи на незащищенном носителе;
- идентификация на основе инфраструктуры открытых ключей с хранением закрытого ключа подписи на защищенном от чтения носителе.

На сегодняшний день существуют следующие возможности по аутентификации пользователя в рамках предоставления государственных и муниципальных услуг:

- аутентификация на базе пары логин/пароль, где в качестве логина выступает страховой номер индивидуального лицевого счета (СНИЛС);
- аутентификация на базе инфраструктуры открытых ключей с хранением ключа подписи на защищенном от чтения носителе;
- в восьми пилотных зонах (г. Москве, Астраханской и Волгоградской областях, республиках Башкортостан, Коми, Татарстан, Краснадарском и Хабаровском краях) рассматривается подход к аутентификации с использованием универсальной электронной карты (УЭК).

СНИЛС.

В соответствии с Федеральным законом от 01 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования» каждое застрахованное лицо должно быть зарегистрировано в системе обязательного пенсионного страхования (ОПС). Поэтому Пенсионный фонд Российской Федерации проводит регистрацию всех россиян, включая детей и подростков, в системе ОПС.

При регистрации каждому застрахованному лицу территориальный орган Пенсионного фонда Российской Федерации открывает индивидуальный лицевой счет с постоянным страховым номером и выдает страховое свидетельство обязательного пенсионного страхования (зеленую карточку), которое содержит следующие данные:

- страховой номер индивидуального лицевого счета (СНИЛС);
- фамилия, имя, отчество;
- дата и место рождения;
- пол;
- дата регистрации в системе обязательного пенсионного страхования.

Страховой номер индивидуального лицевого счета является уникальным и принадлежит только одному человеку. СНИЛС используется для идентификации пользователя на портале государственных услуг, где можно получить ключевые государственные услуги: бланки и информацию для получения паспорта, соцпомощи, путевок, информацию о налогах, штрафах в ГИБДД, выписку с индивидуального лицевого счета в ПФР и многое другое.

Чтобы получить доступ к государственным услугам, гражданину следует пройти процесс регистрации на портале, в ходе которого он должен указать множество персональных данных и выбрать пароль. Для авторизации на портале, пользователь должен ввести СНИЛС (в качестве логина), пароль и код активации. Есть два способа получения кода активации:

- доставка ФГУП «Почта России» (среднее время доставки составляет около двух недель);
- получение в Центре продаж и обслуживания клиентов ОАО «Ростелеком» (с собой необходимо иметь паспорт гражданина РФ, страховое свидетельство обязательного пенсионного страхования, идентификационный номер налогоплательщика).

Аутентификация на базе инфраструктуры открытых ключей.

С середины 2011 г. для аутентификации на ЕПГУ стали доступны USB-токены, использующие технологию на базе инфраструктуры открытых ключей. В данный момент используются токены *только одного производителя*, доступные для ОС Linux, Mac OS и Windows.

Схема аутентификации на базе инфраструктуры открытых ключей основывается на сертификатах открытых ключей.

Рисунок 2 иллюстрирует типичный обмен сообщениями при аутентификации на базе *сертификатов*, использующий цифровые подписи. Обмен соответствует стандарту аутентификации субъектов на основе криптографии с *открытыми ключами*.

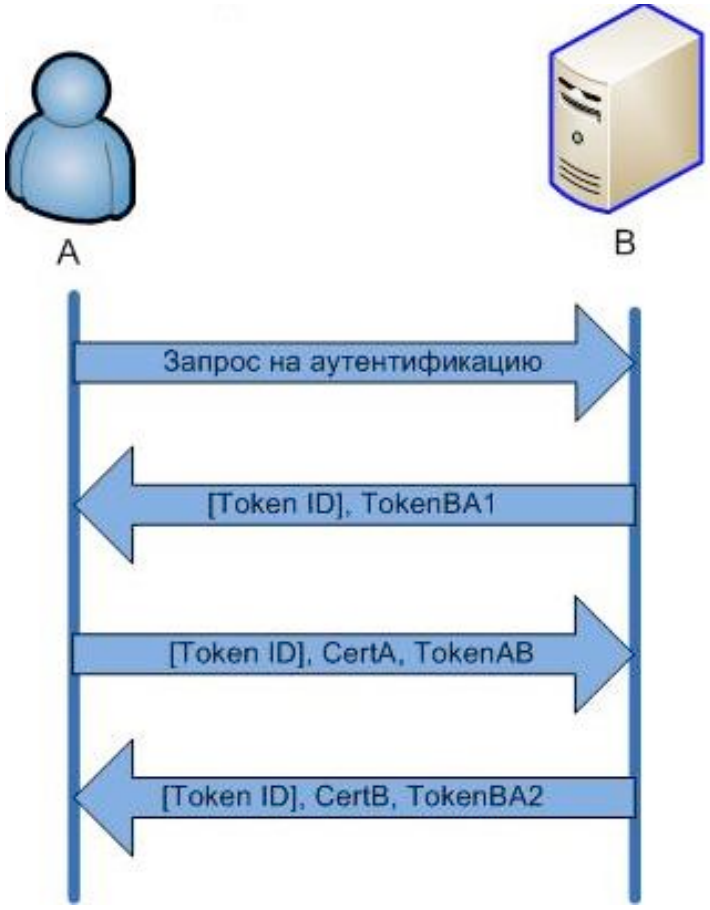

Рисунок 2 — Взаимная аутентификация на базе сертификатов

Если сервер B поддерживает метод аутентификации, запрашиваемый пользователем A, то начинается обмен сообщениями. Сообщение Token ID уведомляет о том, что будет выполняться *взаимная аутентификация*, а также

содержит номер версии протокола и идентификатор протокола. Хотя этот идентификатор не обязателен, он намного упрощает процедуру и поэтому обычно используется. Пользователь А ожидает сообщение Token BA1 от сервера В. Идентификатор протокола в Token ID позволяет пользователю А удостовериться, что сервер В отправляет ожидаемое сообщение. Token BA1 состоит только из случайного числа ran B, это - своего рода запрос, корректным ответом должна быть цифровая подпись числа ran B. Пользователь А подписывает ответ и отправляет свой *сертификат* ключа подписи, для того чтобы сервер В при помощи *открытого ключа* мог выполнить валидацию подписи.

Пользователь А подписывает последовательность из трех элементов: свой запрос ran A, запрос сервера ran B и имя сервера name B. Ran A - это запрос А к серверу В, гарантирующий, что пользователь А подписывает не произвольное сообщение сервера В или другого субъекта, выдающего себя за сервер В. Получив ответ Token AB от пользователя А, сервер В проверяет, совпадает ли значение ran B с соответствующим значением в сообщении Token BA1, а по значению name B устанавливает, действительно ли пользователь А желает пройти аутентификацию сервера В. Если какая-либо из проверок дает отрицательный результат, то и аутентификация завершается неудачно. В противном случае сервер В проверяет подлинность *сертификата* пользователя А и его цифровую подпись, если *сертификат* и подпись валидны, то аутентификация пользователя А сервером В прошла успешно. Ответ сервера В пользователю А завершает *взаимную аутентификацию*.

Ответ сервера Token BA2 состоит из заверенной цифровой подписью последовательности трех элементов: ran A, ran B и name A, где ran A - запрос, сгенерированный А, ran B - исходный запрос сервера В, а name A - имя пользователя А. Получив ответ сервера, пользователь А убеждается, что ran A имеет то же самое значение, что и в сообщении Token AB, а проверяя значение name A - что сервер В намерен аутентифицировать именно его (пользователя

А). Если какая-либо из проверок дает отрицательный результат, то и аутентификация завершается неудачно. В противном случае пользователь А проверяет подлинность *сертификата* сервера В и его цифровой подписи. Если они валидны, то пользователь А аутентифицировал сервер В, и *взаимная аутентификация* выполнена.

УЭК.

В процессе разработки находится универсальная электронная карта (УЭК), которая сможет использоваться в качестве уникального идентификатора. Она выдается гражданам РФ, достигшим 14 лет, на основании заявления, поданного при личном посещении пункта приема заявлений на получение универсальных электронных карт. Она будет идентифицировать гражданина для доступа к тем или иным элементам инфраструктуры электронного правительства как федерального, так и регионального уровня [7].

С помощью карты можно будет получить государственные, региональные и коммерческие услуги в электронном виде с использованием банкоматов, инфокиосков, персональных компьютеров, оснащенных считывателем, мобильных устройств. Универсальная электронная карта также будет приниматься в метро, автобусах, троллейбусах и трамваях. Для этого следует поднести карту к бесконтактному считывателю.

Существует несколько способов доступа к необходимым услугам:

- банкоматы (контактно);
- банковские платежные терминалы (контактно);
- общественный транспорт (бесконтактно);
- сети быстрого обслуживания (бесконтактно);
- государственные, муниципальные и коммерческие системы управления доступом (бесконтактно);
- интернет (при помощи считывающего устройства – ридера).

Внедрение универсальной электронной карты в России отложено до января 2013 г. На рисунке 3 приведен пример УЭК.

Рисунок 3 — Внешний вид универсальной электронной карты

В основе безопасности универсальной электронной карты лежат следующие принципы:

- УЭК не содержит в себе базу данных о гражданине. Персональные данные граждан будут храниться в базах данных государственных министерств и ведомств;
- в соответствии с техническими требованиями к УЭК, универсальная электронная карта соответствует по уровню защищенности смарт-картам, что позволяет обеспечивать информационную безопасности записанной на карту информации, а доступ к карте защищен с помощью ПИН-кода;
- портал УЭК предоставляет гражданам функции по контролю доступа к функциям универсальной электронной карты через личный кабинет на портале УЭК;
- визуальная защита УЭК соответствует уровню, используемому для банковских карт.

В соответствии с информацией размещенной на официальном сайте ОАО «Универсальная Электронная Карта» (www.uecard.ru) являющегося федеральной уполномоченной организацией, осуществляющей функции координатора и оператора проекта по внедрению универсальной электронной карты на основании Распоряжения Правительства Российской Федерации от 12.08.2010 № 1344-р: *обеспечение информационной безопасности, защиты персональных данных и предотвращения попадания карт в свободный оборот будет осуществляться благодаря комплексу мер*.

Необходимый уровень ИБ универсальной электронной карты предполагается обеспечить, помимо физических характеристик ИБ самих карт, за счет:

- унификации процесса персонализации и логистики универсальных электронных карт;
- обеспечения информационной безопасности персональных данных.

При использовании УЭК обеспечение ИБ декларируется за счет использования специализированных программно-аппаратных средств:

- для шифрования передаваемых в процессе информационного обмена с картой данных;
- для обеспечения защиты от несанкционированного считывания информации с карты гражданина бесконтактным способом;
- использование специализированных считывающих устройств – ридеров универсальной электронной карты.

Ридер универсальной электронной карты представляет собой устройство контактного или бесконтактного взаимодействия с картой, снабженое дисплеем, цифровой клавиатурой для набора ПИН-кода, а также сертифицированным аппаратно-программным модулем защиты.

Инфраструктуру универсальной электронной карты образует комплекс взаимосвязанных и взаимодействующих субъектов, представленных на

федеральном уровне – федеральной уполномоченной организацией, на региональном – уполномоченными организациями субъектов РФ.

Федеральный закон №210-ФЗ определяет для ФУО следующие функции:

- организация взаимодействия уполномоченных организаций субъектов Российской Федерации;
- ведение единого реестра универсальных электронных карт, содержащего сведения о выданных на территории Российской Федерации универсальных электронных картах;
- установление перечня и размера тарифов за обслуживание универсальных электронных карт в части, не касающейся функционирования электронных банковских приложений (по согласованию с федеральным органом исполнительной власти, осуществляющим функции по нормативно-правовому регулированию в сфере анализа и прогнозирования социально-экономического развития);
- ведение реестра федеральных, региональных и муниципальных приложений, размещенных на универсальной электронной карте;
- иные функции, определенные Правительством Российской Федерации.

Выпуск универсальных электронных карт производится на базе инфраструктуры банковского сектора. Помимо прочей информации УЭК должна комплектоваться банковским приложением, для обеспечения электронных платежей в рамках предоставления государственных и муниципальных услуг в электронной форме.

Как участники инфраструктуры универсальной электронной карты банки, присоединившиеся к инфраструктуре универсальной электронной карты, подписав соответствующее соглашение с ФУО, выполняют следующие функции:

- обеспечивают предоставление государственных, муниципальных и коммерческих услуг с использованием универсальной электронной карты через свои сети обслуживания клиентов;
- предоставляют гражданам возможность совершения платежных операций по универсальной электронной карте и осуществляют расчеты по этим операциям (в роли Эквайреров);
- осуществляют подготовку данных для персонализации банковского приложения универсальной электронной карты;
- обеспечивают авторизацию платежных операций, совершаемых с использованием универсальной электронной карты и расчеты по этим операциям (в роли Банков-эмитентов).

Персонализация и выпуск универсальных электронных карт будет проводиться на базе инфраструктуры банковского сектора и в соответствии с процедурами персонализации банковских карт.

1.1.2 Анализ применимости существующих схем аутентификции/идентификации (СНИЛС, УЭК) для доступа к государственным и муниципальным сервисам в электронном виде совместно с перспективными способами доступа – мобильные телефоны, планшеты, интернет-киоски, банкоматы

Существующие на сегодняшний день способы доступа к государственным и муниципальным услугам в электронной форме имеют ряд ограничений по форм-фактору и способу их использования. Часть решений, например УЭК, существуют только в форме прототипа.

Указанные причины существенным образом отражаются на возможности использования существующих схем идентификации/аутентификации с новыми перспективными способами доступа к государственным и муниципальным услугам в электронной форме.

Таблица 1 отражает перечень ограничений по использованию той или иной технологии доступа к государственным и муниципальным услугам в электронной форме.

Таблица 1 — Ограничения по использованию существующих средств доступа к государственным услугам в электронной форме

Критерий	**СНИЛС и пароль**	**USB-токен на открытых ключах**	**УЭК**
Форм-фактор	Конверт с паролем	USB-токен	Смарт-карта
Совместимые платформы	Web-портал, клиентская платформа может быть произвольной	Клиентская платформа – Mac OS, Linux, Windows, мобильные платформы не поддерживаются	Используются открытые стандарты, которые позволяют использовать УЭК на любой платформе
Типы услуг, к которым предоставляется доступ	Все услуги	Только портал www.gosuslugi.ru	Все услуги

Продолжение таблицы 1

Уровень информационной безопасности при аутентификации	Низкий, по сравнению с остальными способами аутентификации, высокий риск компрометации пароля	Высокий, при использовании стойкой криптографии	Высокий, при использовании стойкой криптографии
Необходимость наличия специализированного ПО	Нет	Необходимо специализированное клиентское ПО для работы с токеном на пользовательском компьютере	В общем случае не требуется
Требования по аппаратной совместимости	Нет	Необходимо наличие USB-входа типа А	Необходимо наличие в системе ридера для считывания смарт-карт
Возможность использовать дополнительные услуги	Присутствует	Только в рамках ЕПГУ, банковские приложения не поддерживаются	В зависимости от реализации
Совместимость с электронной подписью	Только в режиме реализации подписи на стороне сервера	Возможно за счет аппаратных средств токена	Возможно за счет аппаратных средств карты

Опыт запуска портала госуслуг вызвал большой резонанс в обществе. Это говорит в целом о заинтересованности конечных потребителей (граждан) в получении государственных услуг, взаимодействии с органами госвласти в электронном виде. Но, что самое важное, потребитель хочет получить качественный сервис, гарантирующий безопасность данных, юридическую значимость действий, выполняемых в электронном виде, и, конечно, удобство и сокращение времени на получения госуслуг.

Аутентификацию/идентификацию с помощью СНИЛС для доступа к государственным услугам можно осуществить, используя технические средства, такие как компьютер, мобильный телефон, планшет, интернет-киоск, банкомат. Благодаря ним достигается мобильность пользователей. Но, для того чтобы получить доступ к госуслугам через них, нужны специальные приложения. Например, для мобильного телефона надо создать мобильный портал, так как наличие небольшого дисплея препятствует комфортному пользованию полноразмерного сайта госулуг.

С помощью СНИЛС и соответствуюшего пароля нельзя подключиться к некоторым дополнительным сервисам (например, электронные платежи).

Использование токена с ключами элктронной подписи сопряжено с существенными ограничениями, вызванными форм-фактором этого устройства и совместимыми платформами.

УЭК содержит единое федеральное идентификационное приложение, которое можно универсально использовать в мобильных телефонах, ПК граждан, терминалах и инфоматах, транспортных валидаторах.

В частном случае, для использования УЭК предусмотрено наличие у потребителя специального устройства для чтения такой карты – кард-ридера. Для использования УЭК совместно с мобильными устройствами предусмотрена схема, исключающая ридер.

Из плюсов ридера можно отметить, что при его использовании как с помощью персонального компьютера, так и с помощью мобильных устройств, будет устанавливаться защищенный канал непосредственно между ридером с картой и центром обработки данных уполномоченной организации. Таким образом, будет снят ряд рисков, связанных с возможностью перехвата, подмены или искажения конфиденциальной информации в компьютере, смартфоне или любых других промежуточных точках передачи криптограмм.

1.1.3 Анализ существующих схем аутентификации/идентификации для доступа к государственным и муниципальным сервисам в электронном виде с точки зрения обеспечения мобильности пользователя

Понятие мобильности можно определить следующим образом. Мобильность – это наличие универсального, комбинированного доступа к средствам связи, информации, инструментам и приложениям, которые вы используете в процессе эффективной работы, независимо от того, где вы находитесь и к какому оборудованию вы имеете доступ в определённый момент времени. В данном случае, мобильность достигается минимумом технических средств, требуемых для аутентификации/идентификации доступа к государственным услугам, и возможностью доступа к ним самим, независимо от местоположения пользователя и момента времени.

Наличие государственной системы электронной идентификации и аутентификации, в сочетании с широким распространением интегрированной с Интернетом мобильной связи, создает реальные возможности перехода к бездокументарной идентификации личности как в онлайне, так и в оффлайне. Мобильный телефон сегодня – самое распространенное персональное устройство, пропажа которого обнаруживается в среднем через 20 минут, по сравнению с персональной картой, пропажа которой обнаруживается в среднем через сутки. Эффективность мобильного телефона как персонального идентификатора подтверждается многолетней практикой его использования в платежных системах. Поэтому очень выгодно и удобно использовать именно мобильный телефон в целях аутентификации/идентификации и разрабатывать, соответственно, для него различные программы и приложения [8].

Существующие на сегодняшний день схемы доступа к государственным услугам в электронной форме, а также схемы, проходящие тестирование и прототипирование обладают рядом технических ограничений, которые не во

всех случаях позволяют обеспечить мобильность пользователей государственных услуг, а также их возможный роуминг.

Таблица 1 перечислены существенные ограничения, влияющие в т.ч на мобильность доступа к государственным и муниципальным услугам в электронной форме.

С учетом факторов, обозначенных в таблице 1 можно сделать следующие выводы по поводу обеспечения мобильности, с использованием той или иной схемы доступа к государственным и муниципальным услугам в электронной форме:

- СНИЛС и пароль;
- USB-токен и аутентификация на базе инфраструктуры открытых ключей;
- УЭК.

СНИЛС и пароль – использование для доступа к государственным и муниципальным услугам персонифицированной пары типа логин/пароль позволяет охватить широкий спектр услуг и средств доступа. Данная схема является наиболее широко употребимой и позволяет использовать её совместно с, практически, любыми пользовательскими устройствами доступа (компьютеры, в т.ч планшетные, мобильные телефоны, смартфоны, инфоматы). При использовании данной схемы мобильность главным образом достигается за счет создания единой БД атрибутов доступа, с возможностью использования её в качестве сервиса в произвольной государственной или муниципальной услуге на территории любого субъекта Российской Федерации. Основным недостатком указанного подхода является сравнительно невысокий уровень ИБ самих атрибутов доступа – логина и пароля.

USB-токен и аутентификация на базе инфраструктуры открытых ключей – исходя из технических ограничений, может быть использован только совместно с персональным компьютером или ноутбуком, также поддерживается только ограниченный набор программных платформ. Также

существенным образом ограничена сфера применимости (только сайт www.gosuslugi.ru). Т.о. в текущем виде схема доступа мобильности пользователей не обеспечивает в должном объеме по сравнению с схемой СНИЛС и пароль.

УЭК – исходя из постановления Правительства Российской Федерации от 24 марта 2011 г. N 208 «О технических требованиях к универсальной электронной карте и федеральным электронным приложениям», для использования УЭК необходимо наличие специализированного оборудования для взаимодействия с картой. Однако, для существующих на сегодняшний день карт количество возможных способов использования значительно расширено, что позволяет для ряда услуг, если это позволяет модель угроз, использовать схемы доступа, обеспечивающие инвариантность технических средств доступа, в т.ч. терминальных устройств любого типа.

Таким образом, можно сделать следующий вывод относительно обеспечения мобильности пользователей современными средствами доступа к государственным и муниципальным услугам в электронной форме: из представленных на сегодняшний день средств доступа к государственным и муниципальным услугам в электронной форме возможности по обеспечению мобильности предоставляет только наименее стойкая с точки зрения ИБ, по сравнению с остальными, схема доступа – СНИЛС и пароль.

Мобильность пользователей самым прямым образом связана с возможностью наиболее широкого охвата потенциальной аудитории государственных и муниципальных услуг, а также отражается на непрерывности предоставления этих услуг, возможности роуминга услуг и удобстве пользования.

1.2 Анализ используемых механизмов доступа к государственным и муниципальным сервисам в электронном виде с точки зрения совместимости и возможности использования отечественных криптографических стандартов

Криптография в электронном взаимодействии является наиболее надежным и удобным средством обеспечения информационной безопасности, в т.ч. при организации схем доступа к государственным и муниципальным услугам в электронной форме. По этой причине крайне важным является вопрос о возможности встраивания криптографических методов защиты в схемы доступа к государственным и муниципальным услугам в электронной форме. Использование криптографических средств позволяет существенным образом повысить уровень ИБ при электронном доступе к государственным и муниципальным услугам в электронной форме, а тажке сделать механизмы доступа более пользовательско-ориентированными, за счет упрощения самой процедуры доступа, посредством вовлечения схем электронного взаимодействия.

1.2.1 Реализация методов аутентификации/идентификации в существующих средствах доступа с использованием отечественных криптографических стандартов

Схема с использованием логина/пароля (на основании СНИЛС) в качестве средств аутентификации может быть усилена с использованием криптографических средств, однако это потребует дополнительных технических мероприятий. Сама по себе парольная схема не предполагает использование какого-либо рода криптографии, по этой причине она может лишь являться дополнительным фактором при аутентификации пользователя, например в комбинации с одноразовыми паролями, которые генерируются с помощью OTP-токенов (расширенная многофакторная аутентификация).

Генерация одноразовых паролей в таком токене возможна с использованием хеш-функции ГОСТ Р 34.11-94.

При использовании USB-токенов на основе инфраструктуры открытых ключей сама схема аутентификации построена с применением криптографических средств, при этом использование отечественных криптографических примитивов декларируется всеми производителями USB-токенов, представленными на Российском рынке и предоставляющими возможность доступа к государственным услугам в электронной форме. При этом реализовывается поддержка ГОСТ 28147-89, ГОСТ Р 34.10-2001,ГОСТ Р 34.11-94.

Что касается универсальной электронной карты, то в УЭК предполагается использование следующих механизмов защиты:

- взаимная аутентификация УЭК и терминала на основе сертификатов открытых ключей;
- двухфакторная аутентификация гражданина - владельца карты при попытке получении данных с УЭК (карта + ПИН-код);
- аутентификация при запросе услуги в информационной системе ФУО с использованием криптографических механизмов;
- для того чтобы поставщик услуги мог доверять запросу, производится авторизация запроса на услугу со стороны ФУО (ЭП);
- защита ведомственных блоков данных осуществляется в соответствии с ведомственными требованиями, т.е. ведомства могут установить свои режимы защиты;
- во всей системе, между всеми участниками и всеми компонентами планируется осуществлять шифрование данных при передаче их в каналах связи – между картой и терминалом, между терминалом и оператором канала передачи и до поставщика услуг.

Для обслуживания системы защиты УЭК планируется построить систему управления ключами и сертификатами, включая инфраструктуру открытых ключей (PKI). Она должна удовлетворять следующим требованиям:

- поддержка международных стандартов в части открытых ключей;
- поддержка международных стандартов в части электронных карточек (группа стандартов 7816, Global Platform, DES, RSA);
- поддержка российский стандартов на криптографию (ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001).

Возможны два сценария выпуска УЭК:

- выпуск УЭК с импортной криптографией на импортных микросхемах (без ЭЦП по российским стандартам, но с инфраструктурой RSA);
- выпуск полноценной УЭК с отечественной криптографией на российских микросхемах по мере готовности производства.

Выбор конкретного варианта реализации УЭК зависит от множества факторов, в т.ч. и от выбранной модели угроз. Стоит заметить, что, несмотря на то, что требования по ИБ, которым соответствует большинство банковских решений довольно высокий, модель угроз для государственных и муниципальных услуг в электронной форме значительно жестче.

Таким образом, можно утверждать, что не все существующие схемы доступа к государственным и муниципальным услугам могут быть реализованы, либо усилены с использованием отечественных криптографических стандартов, без изменения или доработки самой схемы доступа. При этом наиболее доступная и обеспечивающая максимальную мобильность схема с использованием СНИЛС и пароля, без дополнительных технических средств и мероприятий не поддерживает отечественную криптографию.

1.2.2 Исследование возможностей использования существующих схем доступа для организации защищенного юридически-значимого взаимодействия с инфраструктурой государственных услуг с использованием отечественных криптографических стандартов

Важной задачей при организации доступа к государственным и муниципальным услугам в электронной форме с помощью средств аутентификации/идентификации является предоставление сопутствующих функций, таких как электронная подпись гражданина.

Средства электронной подписи могут быть либо инкапсулированы в средства аутентификации, либо использоваться в удаленном режиме на стороне сервера электронной подписи в режиме виртуальной смарт-карты.

Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи» устанавливает следующие виды электронной подписи:

- простая электронная подпись, которая посредством использования кодов, паролей или иных средств подтверждает факт формирования электронной подписи определенным лицом;
- усиленная неквалифицированная электронная подпись, которая получена в результате криптографического преобразования информации с использованием ключа электронной подписи, позволяет определить лицо, подписавшее электронный документ, а также позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания и создается с использованием средств электронной подписи;
- усиленная квалифицированная электронная подпись, являющаяся более сложным вариантом усиленной подписи, для которой ключ проверки электронной подписи указан в квалифицированном сертификате, а для создания и проверки электронной подписи используются средства электронной подписи, получившие подтверждение соответствия требованиям, установленным в

соответствии с Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи».

В соответствии с требованиями закона «Об электронной подписи» для создания и проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи должны использоваться средства электронной подписи, которые:

- позволяют установить факт изменения подписанного электронного документа после момента его подписания;
- обеспечивают практическую невозможность вычисления ключа электронной подписи из электронной подписи или из ключа ее проверки.

УЭК и USB-токен на базе инфраструктуры открытых ключей в зависимости от своей реализации могут быть использованы в качестве средств электронной подписи, соответствующих требованиям к средствам электронной подписи, устанавливаемых Федеральным законом от 06.04.2011 N 63-ФЗ «Об электронной подписи».

Однако, УЭК и USB-токен на базе инфраструктуры открытых ключей не являются широко распространенными средствами аутентификации к государственным и муниципальным услугам в электронной форме и не обеспечивают в полной мере мобильность пользователей государственных электронных услуг, в то время как схема аутентификации с использованием СНИЛС и пароля получила гораздо большее распространение и позволяет пользователям государственных и муниципальных услуг оставаться мобильными.

Использование средств электронной подписи совместно с аутентификацией на базе СНИЛС и пароля возможно в формате удаленного использования средств электронной подписи на стороне серверного приложения в формате т.н. *виртуальной смарт-карты*.

В качестве самой виртуальной смарт-карты выступает аппаратный модуль безопасности (HSM – Hardware Security Module), который позволяет

аутентифицированным пользователям использовать средства электронной подписи, входящие в состав аппаратного модуля безопасности в удаленном режиме в формате серверного приложения. С использованием универсального сервиса аутентификации к государственным и муниципальным услугам в электронной форме, пользователь может аутентифицироваться с помощью своих атрибутов доступа и представить документы и файлы для формирования их электронной подписи.

При этом вопрос об управлении ключами электронной подписи, их защищенном хранении и использовании полностью решается на стороне аппаратного модуля безопасности, а пользователь владеет только средствами аутентификации.

1.3 Заключение об уровне защищенности доступа к государственным и муниципальным сервисам в электронном виде и целесообразности использования дополнительных мер по повышению уровня информационной безопасности при взаимодействии с государственными и муниципальными сервисами в электронном виде

Проведенный анализ позволил выявить сильные и слабые стороны существующих схем доступа к госдуарственным и муниципальным услугам в электронной форме.

Результаты анализа представлены в сводной Таблица 2.

Таблица 2 — Сравнительный анализ существующих схем доступа к государственным и муниципальным услугам в электронной форме

Критерий	**СНИЛС и пароль**	**USB-токен на открытых ключах**	**УЭК**
Тип аутентификации	Однофакторная	Однофакторная	Многофакторная

Продолжение таблицы 2

Уровень информационной безопасности атрибутов доступа	Пользователь должен лично заботиться о сохранности своего пароля, уровень ИБ низкий по сравнению с другими схемами доступа.	Атрибуты доступа защищаются аппаратными средствами самого токена. Уровень ИБ – высокий.	Атрибуты доступа защищаются аппаратными средствами карты. Уровень ИБ – высокий.
Возможность импользования многофакторной аутентификации	Возможно с применением дополнительных технических средств	Возможно	Возможно
Обеспечение мобильности	Обеспечивает	Не обеспечивает	Обеспечивает
Возможность использования с отечественными криптографическими стандартами	Возможно с применением дополнительных технических средств	Поддерживаются ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001	Поддерживаются ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001
Возможность использования электронной подписи	Электронная подпись на стороне сервера без использования дополнительных технических средств у пользователя. С использованием дополнительных технических средств – на стороне пользователя.	Поддерживается на стороне самого токена.	Поддерживается на стороне карты, после запуска в производства специализированных карт, поддерживающих работу с криптографическими примитивами.

Наиболее гибкая с точки зрения мобильности и использования дополнительных услуг, таких как электронная подпись, схема – СНИЛС с

паролем – является также и наиболее слабой с точки зрения безопасности атрибутов доступа пользователя. Однако за счет своей гибкости она может быть расширена и усилена с помощью дополнительного фактора аутентификация – с помощью наиболее естесственного в мобильной среде способа, одноразовых паролей (OTP), генерируемых на (U)SIM-карте пользователя, либо доставляемых ему по SMS. При этом пользователю становятся доступными дополнительные функции (электронная подпись и др.) в формате удаленного доступа, в режиме т.н.виртуальной смарт-карты.

(U)SIM-карта оператора связи по уровню защищенности и функциональности по большинству аспектов соответствует уровню УЭК, а по ряду функциональных аспектов превосходит УЭК:

- уровень безопасности (U)SIM-карты как смарт-карты с микропроцессорным чипом полностью аналогичен уровню безопасности УЭК;
- наличие у операторов связи аффилированных партнеров-банков, позволяет записывать на (U)SIM-карту помимо прочих банковские и платежные приложения, что делает возможным использование (U)SIM-карты как технического средства, дополняющего УЭК (использование УЭК в виртуальном режиме);
- современные (U)SIM-карты, поддерживающие технологию NFC (Near Field Communication) для бесконтактного использования приложений на (U)SIM-карте через специальные NFC-считыватели, позволяют использовать мобильный телефон в том числе в бесконтактных транзакциях – аналогично NFC;
- так как мобильный телефон абонента уже является считывателем для (U)SIM-карты, нет необходимости в дополнительном оборудовании, аналогичном ридеру для УЭК, чтобы использовать (U)SIM-карту в мобильной среде в качестве средства доступа к государственным и муницпальным услугам в электронной форме, защищенном контейнере для атрибутов профиля

пользователя, а также для проведения платежных операций с помощью мобильных устройств;

• инфраструктура оператора связи предоставляет гораздо более широкие возможности по персонализации (U)SIM-карт, в том числе с использованием доставки информации «по воздуху» с помощью технологии OTA, что, в свою очередь позволяет: повысить уровень информационной безопасности с помощью ротации ключевого материала, используемого в схемах аутентификации и идентификации, базирующихся на приложениях (U)SIM-карты, без замены самих карт, а также подключать абоненту дополнительные услуги, без замены карты абонента.

Таким образом (U)SIM-карта как персональное средство аутентификации для доступа к государственным и муниципальным услугам в электронной форме позволяет органично дополнить универсальную электронную карту, выпускаемую банковским сообществом, за счет технологических возможностей и ресурсов операторов связи. При этом основным на (U)SIM-карте остается приложение, используемое в схемах аутентификации и идентификации в универсальном сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме, а все функции УЭК абонируются в виртуальном режиме и предоставляются абоненту только после его аутентификации.

Технология виртуальной банковской карты для проведения электронных транзакции и запуска банковских приложений широко отработана по всему миру. В России также запущено использования виртуальных карт, в том числе на стороне операторов мобильной связи.

Использование USB-токенов, опирающихся на проприетарные решения в сфере аутентификации, кардинальным образом сужает возможности мобильности пользователей, обладающих такими атрибутами доступа к государственным и муниципальным услугам в электронной форме, и не позволяет использовать подобное решение в перспективных способах

получения государственных электронных услуг – через мобильные устройства, банкоматы и инфоматы.

Универсальная электронная карта, как состоявшееся и перспективное решение в целом удовлетворяет всем критериям, необходимым для использования её в схемах аутентификации к электронным государственным услугам, совместно с перспективными способами получения этих услуг. При этом схема использования УЭК может быть снабжена, за счет создания универсального сервиса аутентификации к государственным и муниципальным услугам на базе ресурсов оператора связи, удобными интерфейсами к мобильной среде в целом и абонентской базе операторов связи в частности. Указанное обстоятельство позволит увеличить охват средствами доступа к государственным и муниципальным услугам в электронной форме, без значительных затрат со стороны федерального бюджета и банковского сообщества.

2 Разработка технических рекомендаций по созданию сервиса защищенного доступа к государственным и муниципальным сервисам в электронном виде

Предлагаемые технические рекомендации по созданию сервиса защищенного доступа к государственным и муниципальным услугам, предоставляемым в электронном виде, разработаны для решения следующих задач:

- обеспечения безопасности взаимодействия между пользователем государственных и муниципальных услуг в электронном виде и оператором, предоставляющим эти услуги;
- обеспечения мобильности пользователя государственных и муниципальных услуг в электронном виде, за счет:
    - многократного использования пользовательских атрибутов аутентификации совместно с различными способами доступа к государственным и муниципальным услугам в электронной форме;
    - создания единой инфраструктуры доступа ко всем видам государственных и муниципальных услуг в электронной форме;
    - использования гибких интероперабельных схем аутентификации, базирующихся на отечественных криптографических примитивах;
    - повышения уровня информационной безопасности в процедурах аутентификации и регистрации пользователей;
- создания унифицированной схемы доступа к государственным и муниципальным услугам в электронной форме с использованием стандартизованных механизмов.

2.1 Сфера применения сервиса защищенного доступа к государственным и муниципальным услугам в электронном виде на базе ресурсов информационно-коммуникационных сетей

Сервис защищенного доступа к государственным и муниципальным услугам в электронном виде на базе ресурсов информационно-коммуникационных сетей предоставляет функции:

- по аутентификации физических лиц, организаций их контрагентов и уполномоченных представителей;
- аутентификации государственных информационных систем.

Сервис может быть использован для решения следующих прикладных задач:

- аутентификации электронных транзакций, достоверности адресата транзакции, а также совместно с электронной подписью при обеспечении неотказуемости элктронных запросов;
- обеспечение аутентификации в межведомственном взаимодействии;
- аутентификация электронных устройств, не требующих пользовательского взаимодействия;
- обеспечение контртеррористической деятельности, деанонимизация доступа к сети Интернет.

2.2 Описание архитектуры сервиса защищенного доступа к государственным и муниципальным сервисам в электронном виде на базе ресурсов информационно-коммуникационных сетей

Сервис защищенного доступа к государственным и муниципальным услугам в электронной форме относится к классу сервисов управления пользовательскими атрибутами доступа (Identity & Access Management), в состав которого входит несколько основных элементов. На рисунке 4 приведена схема управления пользовательскими атрибутами доступа.

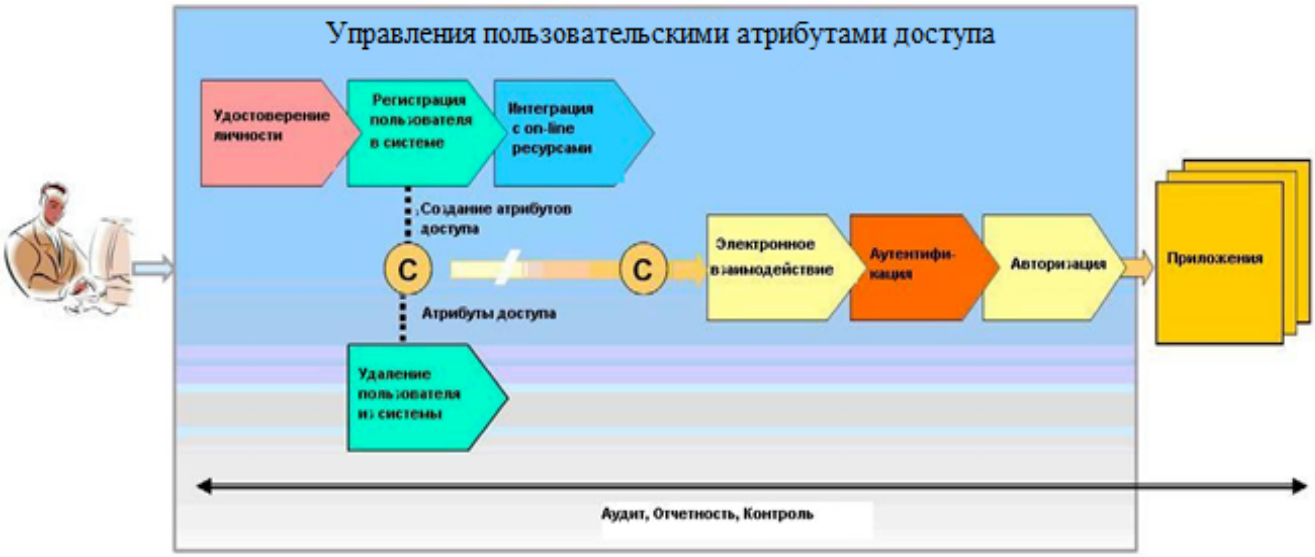

Рисунок 4 — Управление пользовательскими атрибутами доступа

К составным частям процесса управления пользовательскими атрибутами доступа относятся:

- регистрация пользователя;
- интеграция с on-line ресурсами;
- аутентификация;
- выпуск и удаление пользовательских атрибутов доступа;
- защищенное использование пользовательских атрибутов доступа к государственным и муниципальным услугам в электронной форме;
- авторизация;
- аудит, контроль и отчетность.

Регистрация пользователя – необходима для ассоциирования удостоверения личности и персональных данных гражданина с набором атрибутов доступа, используемых в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме.

Интеграция с on-line ресурсами – предоставление информации об атрибутах доступа и ассоциированных с ними персональных данных для использования их в процессе предоставления государственных и

муниципальных услуг в электронной форме, формирование реестров пользователей государственных и муниципальных услуг в электронной форме.

Аутентификация – процесс установления соответствия параметров, характеризующих пользователя, процесс или данные, заданным критериям – является ключевым процессом в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме.

Выпуск и удаление пользовательских атрибутов доступа – после прохождения регистрации для пользователя должны быть созданы необходимые атрибуты для его доступа к государственным и муниципальным услугам в электронном виде. Создание этих атрибутов должно производиться с соблюдением необходимых требований информационной безопасности, а сами атрибуты должны быть проинсталлированы в защищенный контейнер, исключающий возможность их компрометации.

Защищенное использование пользовательских атрибутов доступа к государственным и муниципальным услугам в электронной форме – предполагает организацию электронного взаимодействия с использованием пользовательских атрибутов, исключающее возможность их компрометации и обеспечивающее достаточный уровень информационной безопасности.

Авторизация – предоставление прав на те или иные пользовательские действия в соответствии с информацией в профиле пользователя.

Аудит, контроль и отчетность – для мониторинга работы сервиса защищенного доступа, выполнения требований СОРМ.

2.2.1 Концептуальная схема сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме

Сервис защищенного доступа к государственным и муниципальным услугам в электронной форме представляет собой несколько интегрированных функциональных блоков, состоящих из инфраструктурных элементов специализированного назначения, взаимосвязанных с помощью каналов связи

(как открытых, в случае, где это допустимо, так и защищенных, в случае, если такая защита потребуется).

На следующей диаграмме представлены основные функциональные блоки сервиса защищенного доступа к государственным и муниципальным услугам, реализующие функции регистрации, аутентификации, идентификации и авторизации доступа граждан к государственным и муниципальным услугам в электронной форме. На рисунке 5 предложена концептуальная схема сервиса защищенного доступа к государственным и муниципальным услугам.

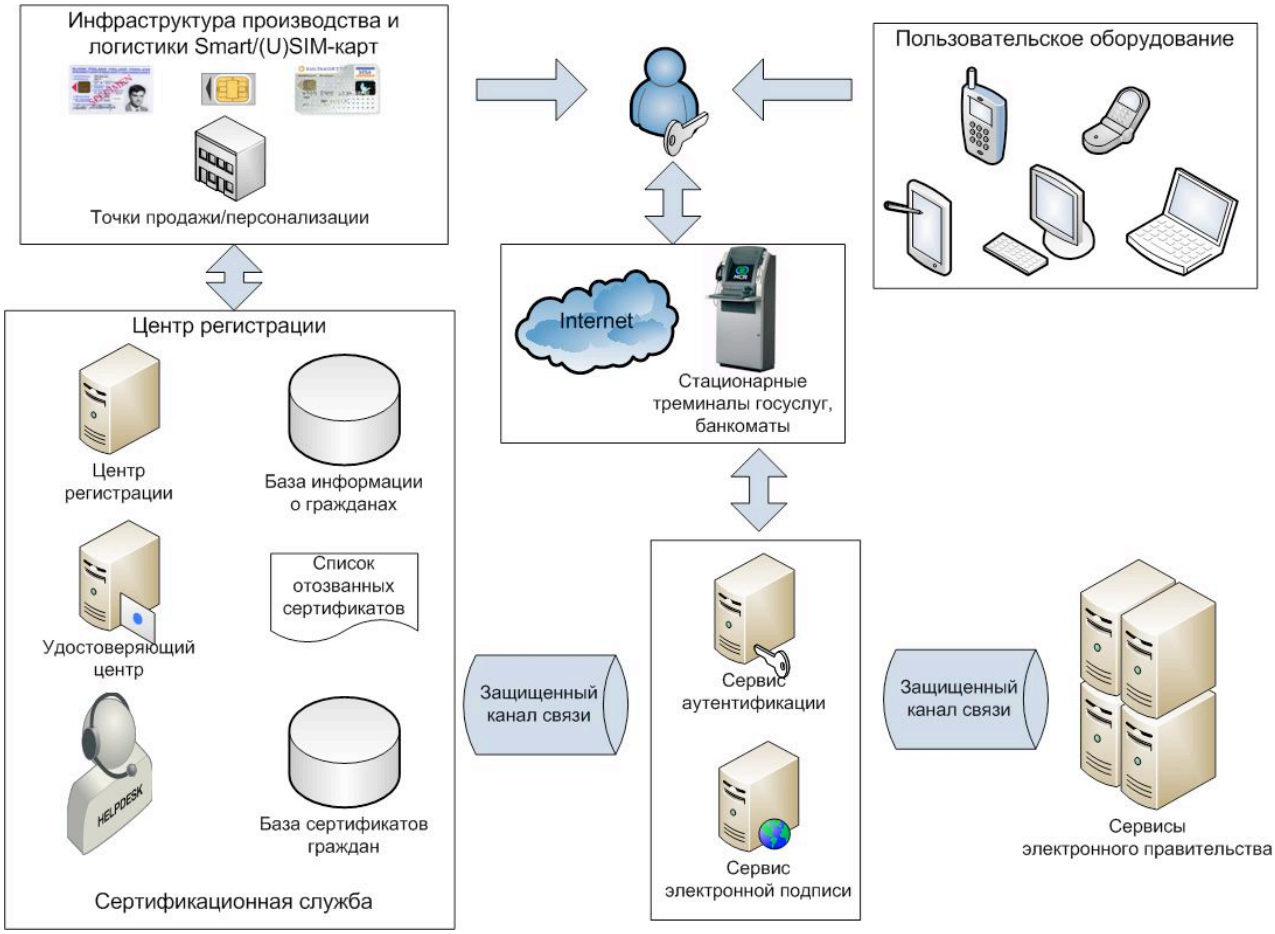

Рисунок 5 — Концептуальная схема сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме на базе ресурсов информационно-коммуникационных сетей

Основными элементами представленной системы являются:

- центр регистрации и сертификационная служба;
- инфраструктура производства и логистики Smart/(U)SIM-карт;
- сервис аутентификации;
- сервис электронной подписи.

Центр регистрации и сертификационная служба – обеспечивают регистрацию граждан в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме, осуществляют формирование информационной базы о пользователях государственных и муниципальных услуг в электронной форме, а также выпуск и защищенное хранение атрибутов профиля пользователя государственных и муниципальных услуг в электронной форме, таких как электронный сертификат гражданина (необходимый, например, для выполнения требований закона № 63- ФЗ от 6 апреля 2011г. «Об электронной подписи»).

Инфраструктура производства и логистики Smart/(U)SIM-карт – в представленной схеме, Smart/(U)SIM-карты могут выступать в качестве защищенных контейнеров для криптографических атрибутов доступа к государственным и муниципальным услугам в электронной форме, входящим в профиль пользователя. Инфраструктура профилирования Smart/(U)SIM-карт, их производства и персонализации (включающая точки продажи Smart/(U)SIM-карт, а также другие точки предоставления абонентских комплектов) осуществляет полный цикл по подготовке и созданию аутентификаторов для сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме.

Сервис аутентификации – непосредственно облачное приложение, реализующее функции AAA для нужд обеспечения защищенного доступа к государственным и муниципальным услугам в электронной форме.

Сервис электронной подписи – облачное приложение, реализующее функции электронной подписи для обеспечения юридически значимого

взаимодействия между пользователем государственных и муниципальных услуг в электронной форме и ведомствами, предоставляющими данные услуги, в соответствии с законом № 63- ФЗ от 6 апреля 2011г. «Об электронной подписи».

В рамках представленной схемы, работа сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме происходит в следующей последовательности.

Во-первых, в рамках работы центра регистрации и сертификационной службы производится подготовка профилей пользователя государственных и муниципальных услуг в электронной форме. Профиль преставляет собой набор атрибутов, таких как: ключи, сертификаты, секреты – необходимых для доступа к государственным и муниципальным услугам в электронной форме, идентификации гражданина, а также обеспечения юридически-значимого взаимодействия между пользователем государственных и муниципальных услуг в электронной форме и ведомствами, предоставляющими данные услуги. При этом часть атрибутов профиля пользователя в дальнейшем не размещается на пользовательском защищенном носителе, доступ к ним пользователь получает удаленно после успешного прохождения аутентификации в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме.

Во-вторых, профили пользователей первоначально производятся в деперсонифицированном виде, в таком же виде они передаются в инфраструктуру производства и логистики Smart/(U)SIM-карт для создания физических, защищенных носителей профиля пользователя государственных и муниципальных услуг в электронной форме.

В-третьих, smart/(U)SIM-карты, содержащие деперсонифицированные профили пользователей, передаются в точки продаж, или центры регистрации граждан для предоставления им государственных и муниципальных услуг в электронной форме.

В-четвертых, при продаже абонентских комплектов, после предъявления гражданином паспорта гражданина Российской Федерации, для предоставления ему услуг связи, производится постпродажная персонализация абонентского комплекта, включающего профиль пользователя государственных и муниципальных услуг в электронной форме, а персональные данные гражданина направляются в центр регистрации для внесения в базу информации о гражданах, таким образом, электронный профиль пользователя государственных и муниципальных услуг в электронной форме становится персонализированным и пользователь может быть идентифицирован на основании имеющихся у него атрибутов.

В-пятых, пользователь с помощью произвольного оборудования для доступа (мобильный телефон, планшетный компьютер, настольный компьютер, ноутбук, коммуникатор) через сеть Интернет, либо посредством специализированных терминалов для доступа к государственным и муниципальным услугам в электронной форме аутентифицируется в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме с помощью своего абонентского комплекта, включающего профиль пользователя государственных и муниципальных услуг в электронной форме. Инициируется защищенная сессия доступа к государственным и муниципальным услугам в электронной форме.

В-шестых, в рамках инициированной защищенной сессии по работе с государственными и муниципальными услугами в электронной форме, пользователю становятся доступны атрибуты его профиля, не размещаемые на пользовательском защищенном носителе, но доступные в рамках защищенной среды сервиса доступа к государственным и муниципальным услугам в электронной форме (например, ключи для выработки цифровой подписи). Информационная безопасность такого рода атрибутов обеспечивается за счет средств сервиса защищенного доступа к государственным и муниципальным

услугам в электронной форме, а не за счет средств безопасности защищенного пользовательского носителя атрибутов, такого как Smart/(U)SIM-карта.

В-седьмых, необходимая для взаимодействия с государственными и муниципальными услугами в эектронной форме информация, включая персональные данные пользователя, предоставляется по запросу из базы информации о гражданах, и не выходит за периметр сервиса защищенного доступа и инфраструктуры государственных и муниципальных услуг в электронной форме, передача информации между которыми производится по защищенным каналам связи.

Таким образом, при реализации данной концептуальной схемы сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме, можно добиться следующих технических и административных эффектов:

- безопасный доступ к государственным и муниципальным услугам в электронной форме с помощью произвольных технических средств – мобильные телефоны, коммуникаторы, планшетные компьютеры, ноутбуки, стационарные компьютеры и специализированные терминалы;
- обеспечение мобильности пользователей, за счет использования единого набора атрибутов доступа, заключенного в профиль пользователя и размещенного на безопасном носителе;
- выполнение требований законодательства по обеспечению взаимодействия, в т.ч. и юридически-значимого, в рамках инфраструктуры электронного правительства, включая требования закона № 63- ФЗ от 6 апреля 2011г. «Об электронной подписи»;
- защита персональных данных граждан, их защищенное использование, без необходимости обеспечивать их защиту на стороне пользователя;
- использование ресурсов операторов информационно-коммуникационных сетей для реализации инфраструктуры сервиса

защищенного доступа к государственным и муниципальным услугам в электронной форме: использование удостоверяющих центров операторов, абонентской базы операторов и инфраструктуры профилирования и производства (U)SIM-карт.

2.2.2 Описание подходов к аутентификации, используемых в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме

В результате анализа нескольких реализаций электронной и мобильной «личности» в нескольких европейских странах, которые соответствуют Директиве Европейского парламента 1999/93 «Об общих условиях использования электронных подписей», опубликованная в Official Journal of the European Communities (OJ) L 13, 19.01.2000, стр. 12, был выбран подход к аутентификации, оптимальный для использования в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме.

В директиве устанавливаются страны-члены ЕС, широко использовавшие электронную «личность» на середину 2001 года.

Среди безопасных технических средств для осуществления аутентификации в электронном взаимодействии наиболее оптимальным и гибким является использование генерируемых одноразовых паролей. Обычно, последнее подразумевает использование специальной смарт-карты. Так как стандартные ПК и ноутбуки не содержат кардридеров, процедура, необходимая перед непосредственным использованием карты, может быть довольно трудоемкой и дорогой. Кроме процедуры формальной регистрации для идентификации пользователя, гражданин должен купить специальный аппаратный компонент (кардридер), что может снизить удобство использования и доступность, так как этого продукта обычно нет в торговых центрах. Кроме того, для кардридера могут быть необходимы дополнительные установки, а так же установка программных компонент для подписных

приложений. Дополнительно к этому, функции некоторых программных компонент, могут быть использованы в фоновом режиме, незаметно для пользователя, соответственно, это вызывает дополнительные препятствия для широкого использования.

На сегодняшний день одноразовые пароли (OTP – One-Time Password), получили широкое распространение, как надежное и удобное средство для аутентификации. Характерным примером может служить решение SecurID от компании RSA Security – двухфакторная аутентификация на основе пользовательских данных (PIN или пароль) и токен-кода [9].

Одноразовый пароль обычно представляет собой сгенерированную последовательность символов, т.н. токен-код, (в целях удобства зачастую просто цифр), которая периодически меняется и имеет достаточно короткое время жизни, т.е. по прошествии некоторого временного отрезка, когда комбинация сменится, предыдущая будет уже непригодна для аутентификации. Алгоритм, по которому токен-код генерируется, синхронизован с сервером таким образом, что для проверки подлинности кода проверяющей стороне не нужна никакая дополнительная информация. Принцип работы такого токена основан на вычислении односторонней функции от времени и секретного значения, и в случае компрометации токен-кода его становится невозможно использовать через несколько минут после генерации. Технически генераторы одноразовых паролей могут быть выполнены в различном виде: брелок с экраном, на котором отображается токен-код , java card applet или midlet, тогда в качестве форм-фактора будут использованы смарт-карта и телефон соответственно.

Поскольку изначально предполагается, что одноразовые пароли главным образом используются для аутентификации пользователей и, по возможности, должны быть всегда «под рукой», то для их реализаций можно выдвинуть ряд требований, при соблюдении которых они становятся удобным и надежным средством аутентификации:

- лёгкость использования;
- безопасность алгоритмов и протоколов;
- гибкость реализации;
- экономичность аппаратной реализации.

Лёгкость использования. OTP-токен должен иметь простой и понятный интерфейс, как для пользователя, который будет читать значение токен-кода и вводить его при аутентификации (либо использовать механизм типа PKCS #11), так и для сервера, который будет производить ресинхронизацию токена, когда это понадобится.

Безопасность алгоритмов и протоколов. Алгоритмы, используемые для генерации токен-кода должны удовлетворять требованиям невозможности получить по токен-коду защищенную информацию, например, инициализирующий вектор, кроме того все криптографические операции должны выполняться внутри защищенной среды, предоставляя наружу только уже готовый к использованию результат. Инициализация токена и его ресинхронизация в свою очередь должны использовать безопасные соединения для передачи инициализирующей информации, зная которую взломщик может имитировать работу токена.

Гибкость реализации. Требование мобильности токена подразумевает возможность его реализации на базе различных форм-факторов (брелки, телефоны, sim-карты).

Экономичность аппаратной реализации. Данный фактор является скорее само-собой разумеющимся, нежели жестоко требуемым.

Сегодня существуют различные технические и организационные подходы к тому, как мобильные устройства могут служить в качестве средства аутентификации. После проведенного анализа мы пришли к двум главным обоснованным альтернативам реализации этой технологии:

1) client-side реализация, при которой криптографические данные хрантятся в модуле идентификации абонента (SIM), расположенном в

мобильном устройстве клиента (модель в настоящее время используется в Эстонии);

2) server-side, когда криптографические данные хранятся на сервере в аппаратном модуле безопасности (HSM) (такая модель используется в Австрии). Ниже краткое описание этих двух альтернатив.

Наиболее очевидное решение – это интеграция модуля аутентификации в (универсальный) модуль идентификации абонента ((U)SIM). Этот подход кажется очевидным, так как (U)SIM-карты уже установлены и интегрированы в телефон, мобильный оператор обеспечивает дистрибутив и закрытые ключи могут быть сгенерированы на карте, так что они никогда не покидают среду безопасности.

(U)SIM – это модуль, который надежно хранит определенную сетевую информацию, используемую для идентификаци и аутентификации абонентов в сети, например:

- как каждая смарт-карта, (U)SIM предусматривает так называемую «ID карту с интегрированными электронными цепями» (ICCID), международный уникальный идентификатор;
- международный идентификатор мобильного абонента (IMSI), уникальный идентификатор, используемый отдельными сетями оператора;
- аутентификационный ключ, используемый для аутентификации SIM в мобильной сети.

Каждый абонент однозначно связан с (U)SIM, который хранит закрытый ключ пользователя, нужный для аутентификации, устойчивой к внешним воздействиям, основанной на подписях.

(U)SIM-карта в телефоне может рассматриваться как смарт-карта, полностью интегрированная с ридером и дисплеем в комбинации с сетевыми функциями.

Аутентификация с использованием одноразовых паролей, генерируемых приложением на (U)SIM-карте пользователя.

На рисунке 6 показана принципиальная схема аутентификации с использованием одноразового пароля, генерируемого на (U)SIM-карте пользователя.

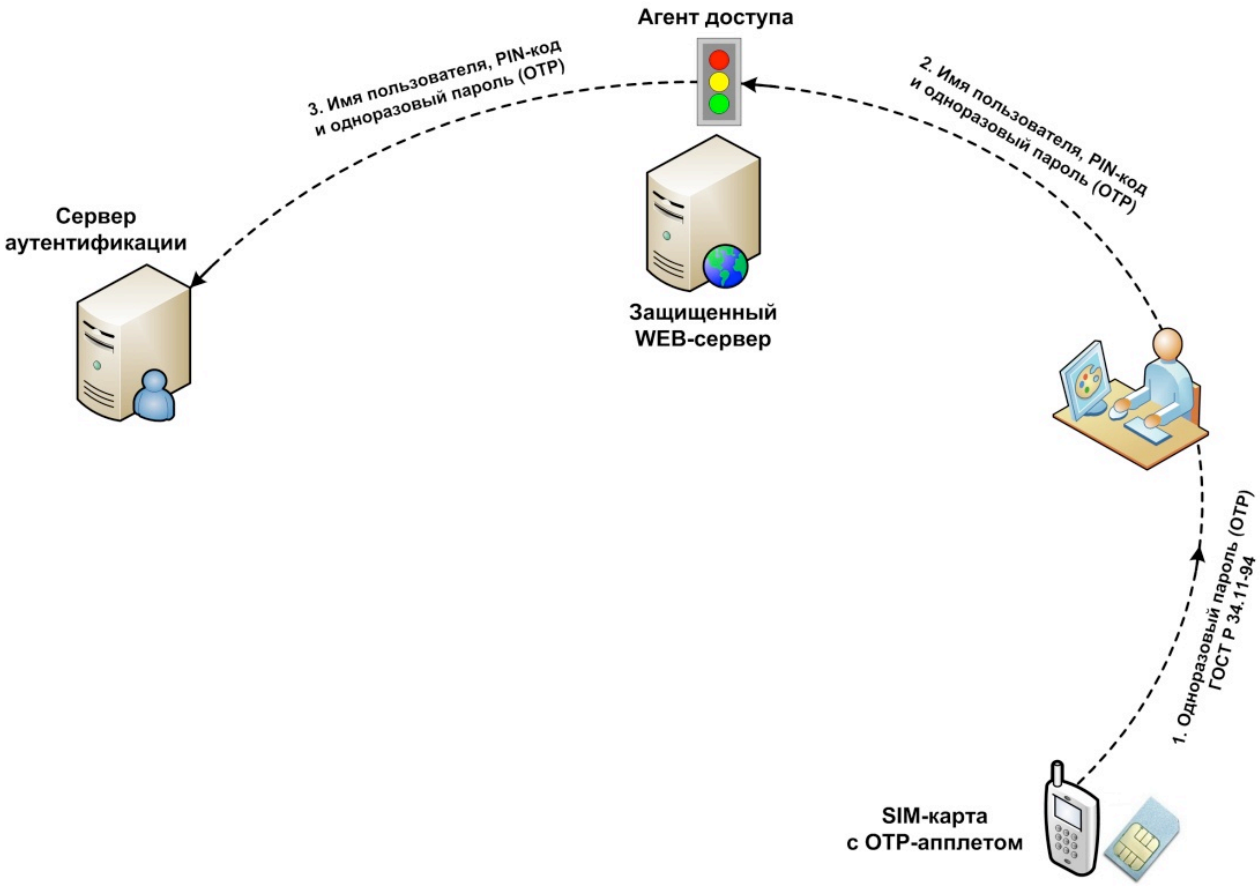

Рисунок 6 — Аутентификация с использованием одноразовых паролей, генерируемых приложением на (U)SIM-карте пользователя

Аутентификация пользователя производится по следующему сценарию:

1) при входе на Web-портал пользователь вводит имя и пароль, после этого система запрашивает одноразовый код доступа;

2) апплет для генерации токен-кода размещается на SIM-карте мобильного телефона;

3) пользователь вызывает его из SIM-меню, генерирует новый токен-код, вводит его в систему и получает доступ к требуемому ресурсу.

В представленной схеме аутентификации токен-код генерируется на основе текущего значения счетчика генераций и не имеет временных ограничений, т.е. допускает отложенное использование.

Аутентификация с использованием одноразовых паролей, доставляемых посредством SMS-сообщений.

Альтернативным способом надежной пользовательской аутентификации является аутентификация с использованием одноразовых паролей, доставляемых посредством SMS-сообщений. На рисунке 7 показана схема аутентификации с использованием одноразовых паролей, доставляемых посредством SMS-сообщений.

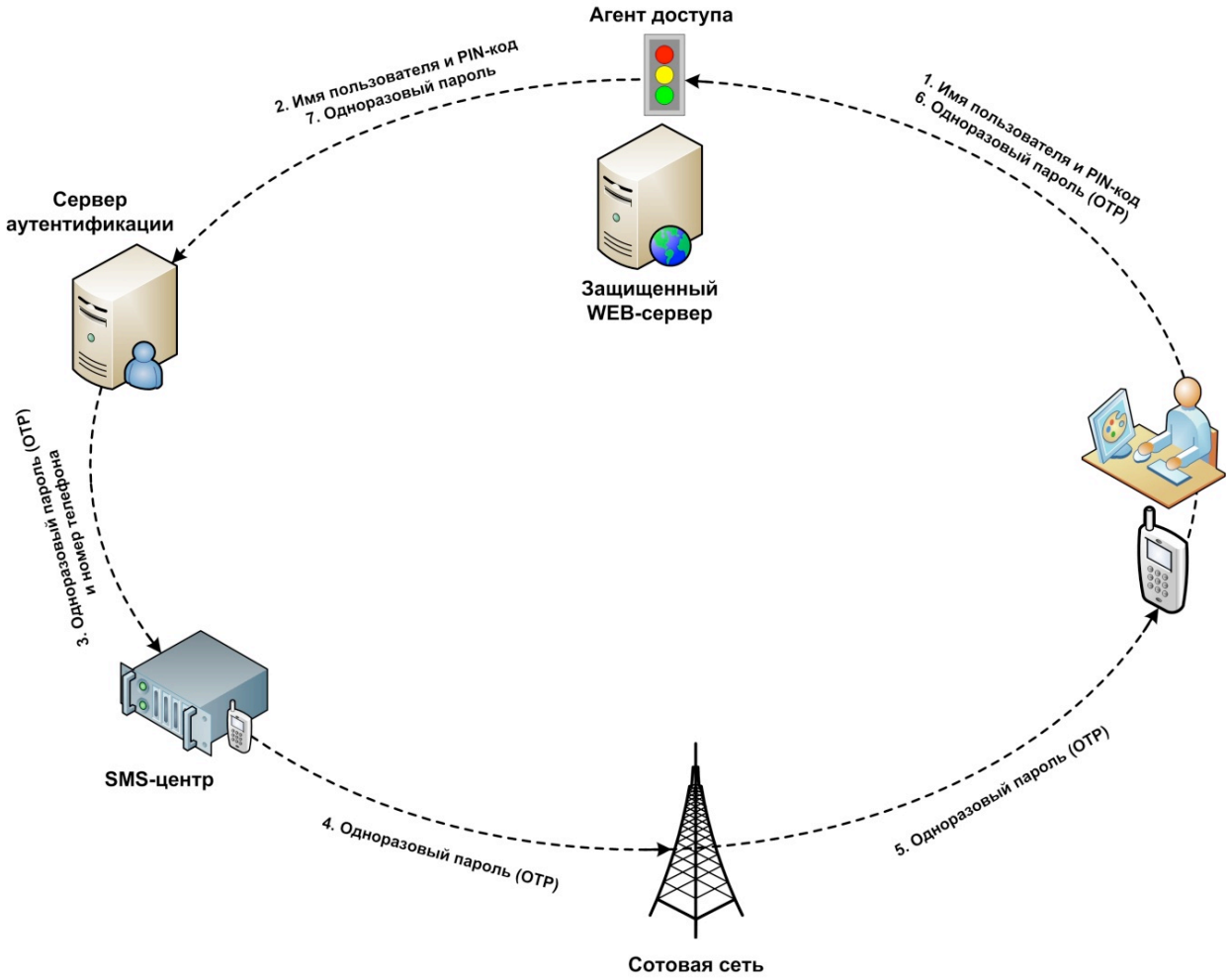

Рисунок 7 — Аутентификация с использованием одноразовых паролей, доставляемых посредством SMS-сообщений

В схеме, представленной на рисунке 7, аутентификация производится следующим образом:

1) при входе на Web-портал пользователь вводит имя и пароль (или PIN-код);

2) на основании имени пользователя сервис аутентификации определяет номер телефона, соответствующий этому имени, и пересылает на него одноразовый код доступа в виде сообщения SMS;

3) пользователь вводит полученный на свой телефон токен-код и получает доступ к требуемому ресурсу.

В указанной схеме токен-код генерируется на основе текущего времени и имеет ограниченную продолжительность действия.

2.2.3 Схема прикладного сервиса аутентификации для сервиса защищенного доступа к государственным и муниципальным услугам в электронном виде

Прикладной сервис аутентификации для сервиса защищенного доступа к государственным услугам в электронной форме выполняет следующие базовые функции по обеспечению защищенного доступа к государственным и муниципальным услугам в электронной форме [9]:

- аутентификация пользователя на основании его атрибутов доступа в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме;
- защищенное хранение атрибутов профиля пользователя внутри аппаратного модуля безопасности (HSM);
- защищенное использование атрибутов профиля пользователя внутри HSM;
- защищенное хранение электронных сертификатов гражданина.

На рисунке 8 представлена схема прикладного сервиса аутентификации.

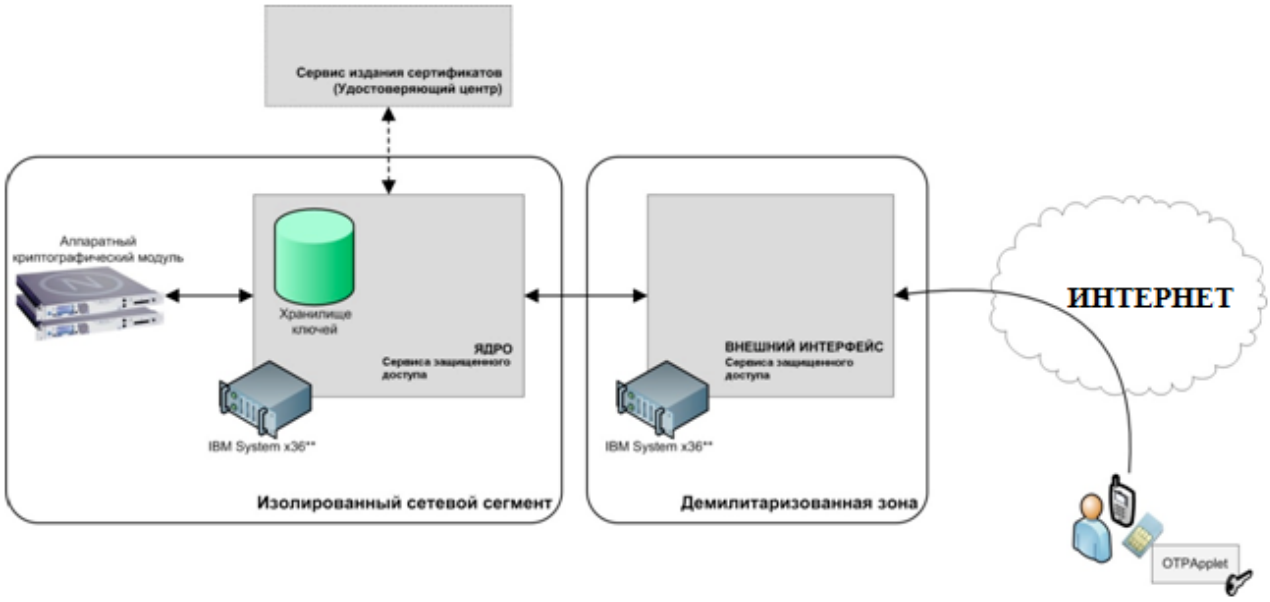

Рисунок 8 — Структурная схема прикладного сервиса аутентификации для нужд сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме

Сервис состоит из следующих зон или периметров:

- внешняя среда, в которой находится пользователь сервиса, включающая сеть Интернет, как основную среду доступа к государственным и муниципальным услугам в электронной форме;
- пользовательский комплект, состоящий из мобильного телефона и специальной (U)SIM-карты, на которую предустановлено приложение в виде Javacard-апплета, реализующее генерацию одноразового пароля с использованием ГОСТ Р 34.11-94;
- демилитаризованная зона, включающая внешний интерфейс сервиса аутентификации, выполняющий функции обработки запросов от пользователей в зависимости от интерфейса, который они используют (web-интерфейс, SOAP, Web-Services и др.), и передачи их для дальнейшей обработки в ядро сервиса аутентификации;
- изолированный сетевой сегмент, в котором расположен основной сервер, реализующий непосредственно аутентификацию пользователя в

процессе его доступа к государственным и муниципальным услугам в электронной форме;

- сервис издания сертификатов, который выполняет выпуск сертификатов гражданина, с привязкой их к персональным данным гражданина.

Сервис аутентификации представляет собой программно-аппаратный комплекс, реализованный на базе серверов приложений совместимых с типом IBM System x36**, а также аппартного модуля защиты информации HSM, он же аппаратный криптографический модуль.

Серверное приложение, реализующее внешний интерфейс сервиса аутентификации отвечает за получение и обработку запросов на аутетинфикацию с помощью и фактически предоставляет интерфейс по встраиванию сервиса аутентификации в интерфейс порталов государственных и муниципальных услуг, в интерфейс соответствующих мобильных порталов и т.п. Среди внешних интерфейсов, взиамодействие по которым возможно с сервисов аутентификации:

- интерфейс просто web-формы;
- SOAP;
- Web-services;
- интерфейс web-формы для мобильного приложения.

Полученный в разном формате запрос на аутентификацию, трансформируется во внутрениий формат сообщений и передается для обработки в ядро сервиса.

Ядро сервиса обрабатывает полученный запрос на аутентификацию, выделяя из него необходимую информацию:

- номер мобильного телефона пользователя государственных и муниципальных услуг в электронной форме;
- его идентификатор внутри системы государственных услуг, например СНИЛС;

- пароль пользователя или PIN-код для доступа к государственным и муниципальным услугам в электронной форме;
- одноразовый пароль, сгенерированный приложением на (U)SIM-карте пользователя.

На основании верификации полученных данных производится принятие решения об аутентификации пользователя и установлении с ним защищенной сессии, посредством внешнего интерфейса сервиса аутентификации.

2.2.4 Описание процедуры регистрации пользователя в сервисе защищенного доступа к государственным и муниципальным услугам в электронном виде

Процедура регистрации и выдачи идентификаторов, независимо от того, кто будет ее проводить, включает несколько основных операций.

Аутентификация регистрируемого объекта – гражданина РФ и или юридического лица. В данном случае аутентификация производится по паспорту или другому удостоверению личности, признаваемому Законодательством, во втором, на основании комплекта предъявленных уставных и регистрационных документов, включающих также доверенность лица, которое представляет организацию во время регистрации.

Оформление договора. Сторонами договора выступают уполномоченный Государством орган (например, Министерство Связи и Массовых коммуникаций), представляющий интересы Государства и гражданин РФ (или представитель юридического лица). Одним из возможных вариантов договора является Договор присоединения, который подписывается новым участником. Со стороны государства подписывается Договор оферты, для присоединения к которому регистрируемый должен оставить собственноручную подпись на бумажном носителе и заполнить соответствующие приложения к договору.

В договоре стороны подтверждают, что принимают правила электронного документооборота (а именно, все действия и процедуры, связанные с

идентификацией, авторизацией, аналогом собственноручной подписи, процедурами входа и отправки сообщений из Личного Кабинета, заверкой документа «электронной печатью», или ЭП и т.п.), свою ответственность в случае передачи идентификатора другому лицу (для граждан) или порядок выдачи внутренних доверенностей сотрудникам на выполнение каких-либо функций по представлению интересов организации (для юридических лиц), порядок замены идентификатора или его восстановления при утрате, дополнительные меры защиты от несанкционированного использования и т.п., в соответствии с требованиями Законодательства, регламентирующего деятельность «Электронного Правительства», а также порядок согласования дополнительных условий, если таковые возникают в дальнейшем с помощью «электронной подписи», которая признана в подписанном Сторонами варианте Договора. Все дальнейшие контакты с государственными структурами граждане смогут вести в зависимости от своего желания и обстоятельств либо с помощью электронных коммуникаций, либо с помощью стандартных («бумажных»).

При регистрации заполняется «Приложение к договору», в котором описывается идентификатор, который выдается гражданину (например, Универсальная Электронная Карта УЭК, номера одного или нескольких мобильных телефонов), которые регистрируемый признает своим идентификатором, СНИЛС и другие необходимые сведения. Приложение является неотъемлемой частью Договора и подписывается Сторонами.

При подписании Договора производится сличение личности с предъявленным документом (аутентификация), копирование предъявленного документа с помощью сканера в электронную форму долговременного хранения, заверка сканированной копии «личной электронной подписью» сотрудника уполномоченной организации и отправка ее в соответствующее региональное электронное хранилище. Гражданин РФ, подписавший Договор получает заверенную «электронную копию удостоверяющего документа на

шаблоне», которая передается ему на адрес его электронной госпочты и/или в любой удобной для него цифровой форме (на цифровом мобильном носителе, флэш-памяти и т.п.).

Все зарегистрированные юридические лица попадают в каталоги Федерального ПГУ (ЕПГУ) или региональных, ведомственных и т.д. порталов всех уровней и становятся доступными для других пользователей через личный кабинет.

Предварительная регистрация, дающая ограниченный доступ и возможности обмена сообщения на уровне, подразумевающем гарантированную возможность административного (но не судебного) разбирательства, осуществляется непосредственно на Государственных и Муниципальных Порталах. Для полноценной юридической значимости на уровне возможных разбирательств в судебных инстанциях необходимо, в соответствии с действующим Законодательством, иметь собственноручную подпись гражданина и его аутентификации в момент подписания (аналог нотариальному заверению).

Процедура регистрации пользователя в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме может быть совмещена с созданием дополнительных атрибутов профиля пользователя, таких как сертификат гражданина и ключи для электронной подписи, которая может быть использована в юридически значимом взаимодействии с ведомствами в рамках электронного правительства.

Процесс регистрации пользователя.

Технический процесс генерации данных для создания подписи полностью выполняется в HSM по ходу первоначального процесса регистрации.

Во-первых, личность подписанта проверяется поставщиком услуг сертификации в соответствии с законными ограничениями. Во время процесса регистрации подписант должен указать номер мобильного телефона, который

он/она хочет использовать в будущем для запуска процесса подписи, и выбрать пароль.

Во-вторых, фактическое владение указанным номером мобильного телефона проверяется непосредственной отправкой на это утройство SMS, которое содержит однодневный одноразовый код (TAN – Token Authentication Number).

В-третьих, подписант должен ввести TAN в веб-форму.

В-четвертых, после проверки TAN сервисом, новые данные для создания подписи генерируются в HSM и здесь же этот сгенерированный закрытый ключ немедленно кодируется опять другим ключом, полученным из номера мобильного телефона и пароля пользователя. Вследствие этого, зашифрованный закрытый ключ можно использовать позже, если только пароль доступен для декодирования. Для гарантии того, что использование закрытого ключа возможно только внутри сертифицированного HSM, кодированный закрытый ключ шифруется опять – на этот раз ключом, известным только HSM. Эти дважды зашифрованные данные для создания подписи могут храниться даже вне сертифицированного HSM в базе данных ключей.

На рисунке 9 представлен протокол регистрации пользователя в сервисе защищенного доступа к государственным и муниципальным услугам, совмещенный с выработкой подписи для этого пользователя.

После выполнения регистрации в сервисе защищенного доступа и выработке атрибутов подписи пользователю становятся доступны государственные и муниципальные услуги в электронной форме, а также его персональная цифровая подпись в режиме виртуальной смарт-карты.

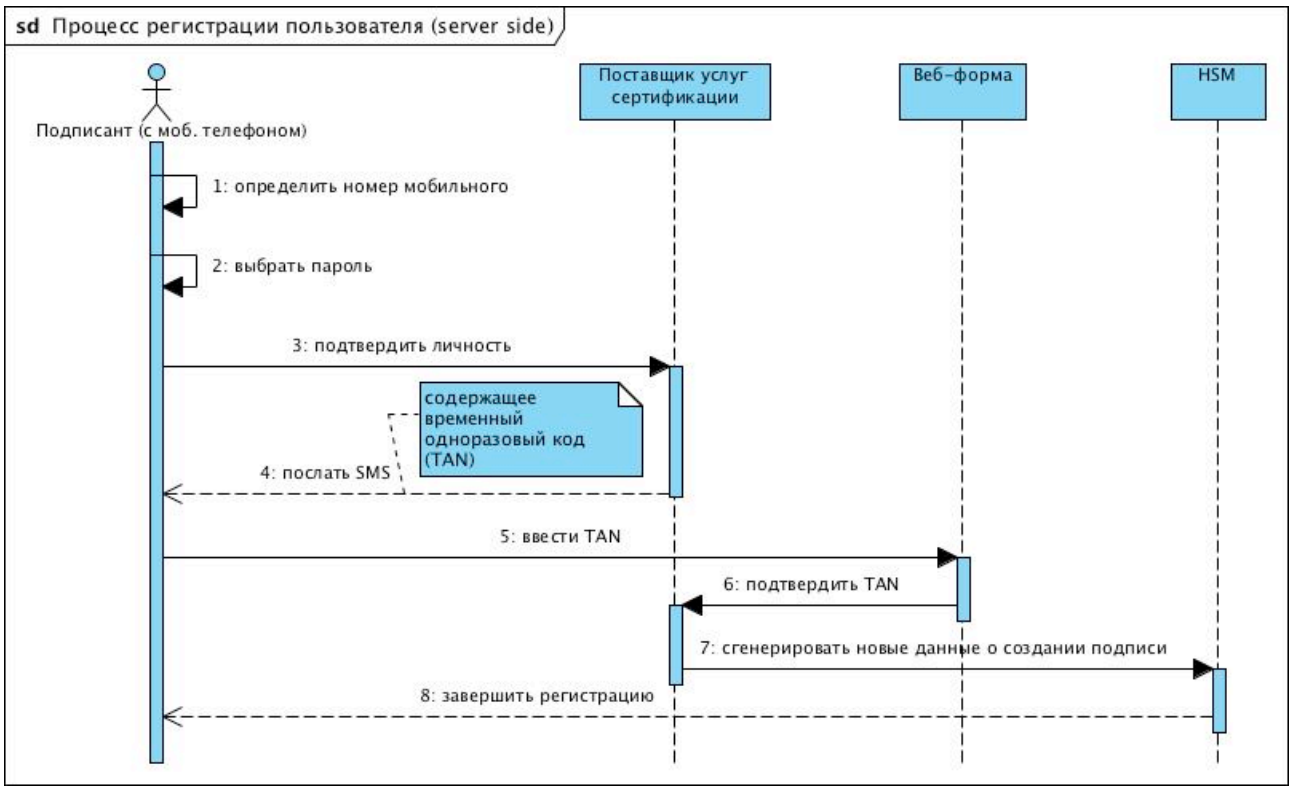

Рисунок 9 — Процесс регистрации пользователя и выработки дополнительных атрибутов

Описание процедуры аутентификации/идентификации пользователя.

На рисунке 10 представлен процесс аутентификации.

Процесс аутентификации.

Типичный процесс аутентификации может проводиться следующим образом:

1) пользователь хочет аутентифицироваться перед провайдером сервиса;

2) провайдер сервиса перенаправляет пользователя в центр аутентификации;

3) пользователь вводит свой номер телефона и пароль. Пароль нужен для предотвращения злоупотребления сервисом;

4) центр аутентификации отправляет на телефон клиента TAN посредством SMS, действительный только в короткий период времени, вместе (необязательно) с хеш-значением сообщения, которое нужно подписать;

5) пользователь проверяет сообщение, которое он собирается подписать онлайн, и сравнивает его хеш-значение со значением, которое он только что получил;

6) если значения совпадают, пользователь вводит TAN вместе с PIN, связанным с его закрытым ключом, в веб-форму;

7) сервер подписывает сообщение, используя HSM и предоставленный PIN-код;

8) результат этой подписи отправляется провайдеру сервиса;

9) провайдер сервиса проводит проверку подписи а также утверждение сертификата;

10) после успешной проверки провайдер сервиса принимает аутентификацию пользователя.

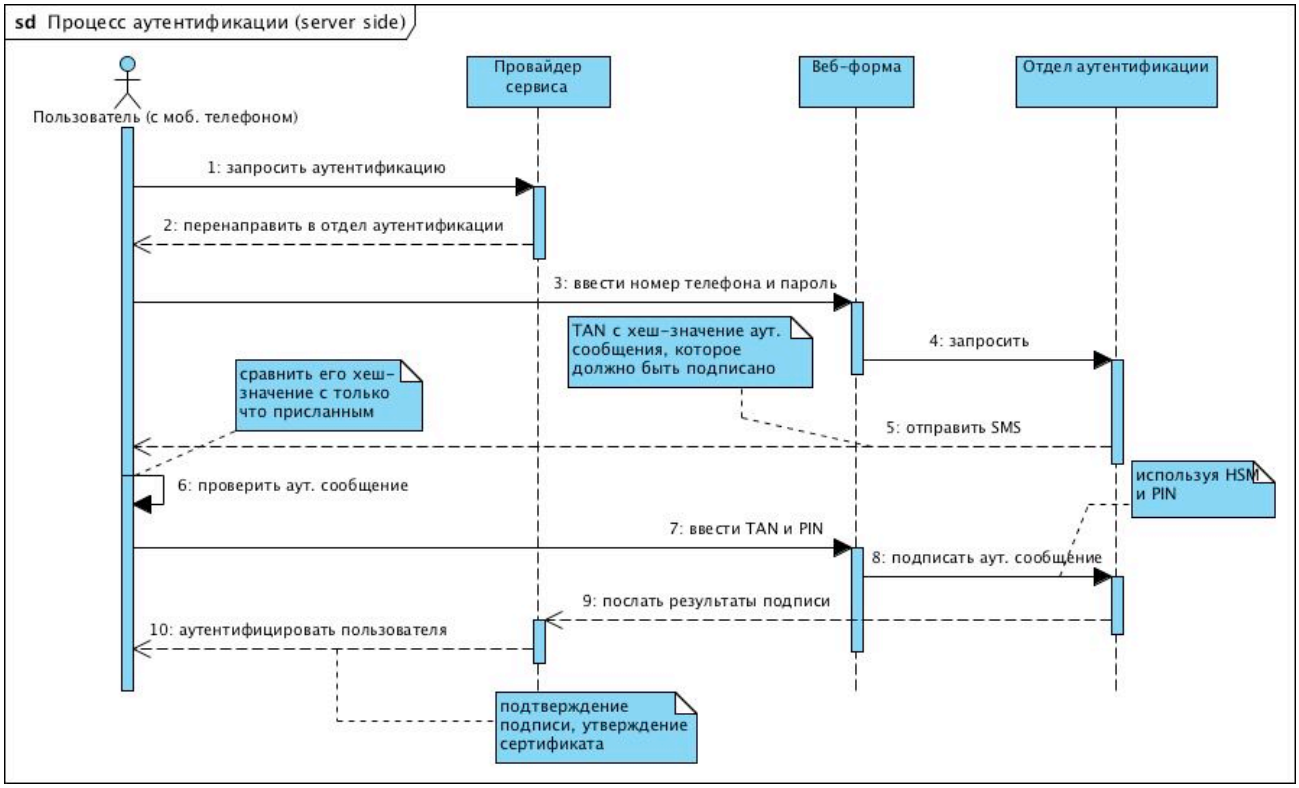

Рисунок 10 — Процесс аутентификации

Процесс подписи.

Последующее использование данных для создания подписи похоже на описанный процесс регистрации.

Если пользователь хочет подписать документ, он/она запускает в приложении запрос подписи (будь это веб-приложение или локально установленное ПО). Этот запрос подписи включает документы/данные, которые нужно подписать, и направляется к поставщику мобильной подписи.

Как только запрос получен HSM, пользователь должен ввести его/ее мобильный номер телефона (который служит в качестве ID пользователя) и его пароль. Ввод происходит естественно через безопасные каналы связи напрямую в веб-приложение мобильной подписи.

После проверки на соответствие указанного номера зарегистрированному пользователю, документ/данные, которые нужно подписать, включая пароль и номер телефона, немедленно передаются в HSM. После, HSM вычисляет хеш-значение (цифровой отпечаток пальца) документа/данных и случайный однодневный одноразовый код (TAN). Оба отрпавляются посредством SMS на указанный номер мобильного телефона. Параллельно, веб-приложение предлагает пользователю еще раз проверить данные, которые надо подписать. В это же время, короткое хеш-значение отображается веб-приложением.

Подписант получает SMS и имеет возможность сравнить хеш-значение, полученное с SMS, с хеш-значением, отображенным веб-приложением. Ввод полученного TAN в веб-интерфейс сервиса мобильной подписи гарантирует, что подписант на самом деле владеет зарегистрированным мобильным телефоном.

Положительный результат проверки приводит к тому, что HSM извлекает соответствующие зашифрованные данные для создания подписи из базы данных ключей и расшифровывает ключом из HSM. На следующем шаге, эти – все еще зашифрованные – данные для создания подписи расшифровываются производной от пароля пользователя. Только теперь закрытый ключ доступен в сертифицированном HSM.

Подпись создается в HSM и подписанный документ/даные передаются во владение подписанту.

На рисунке 11 приведен процесс подписи.

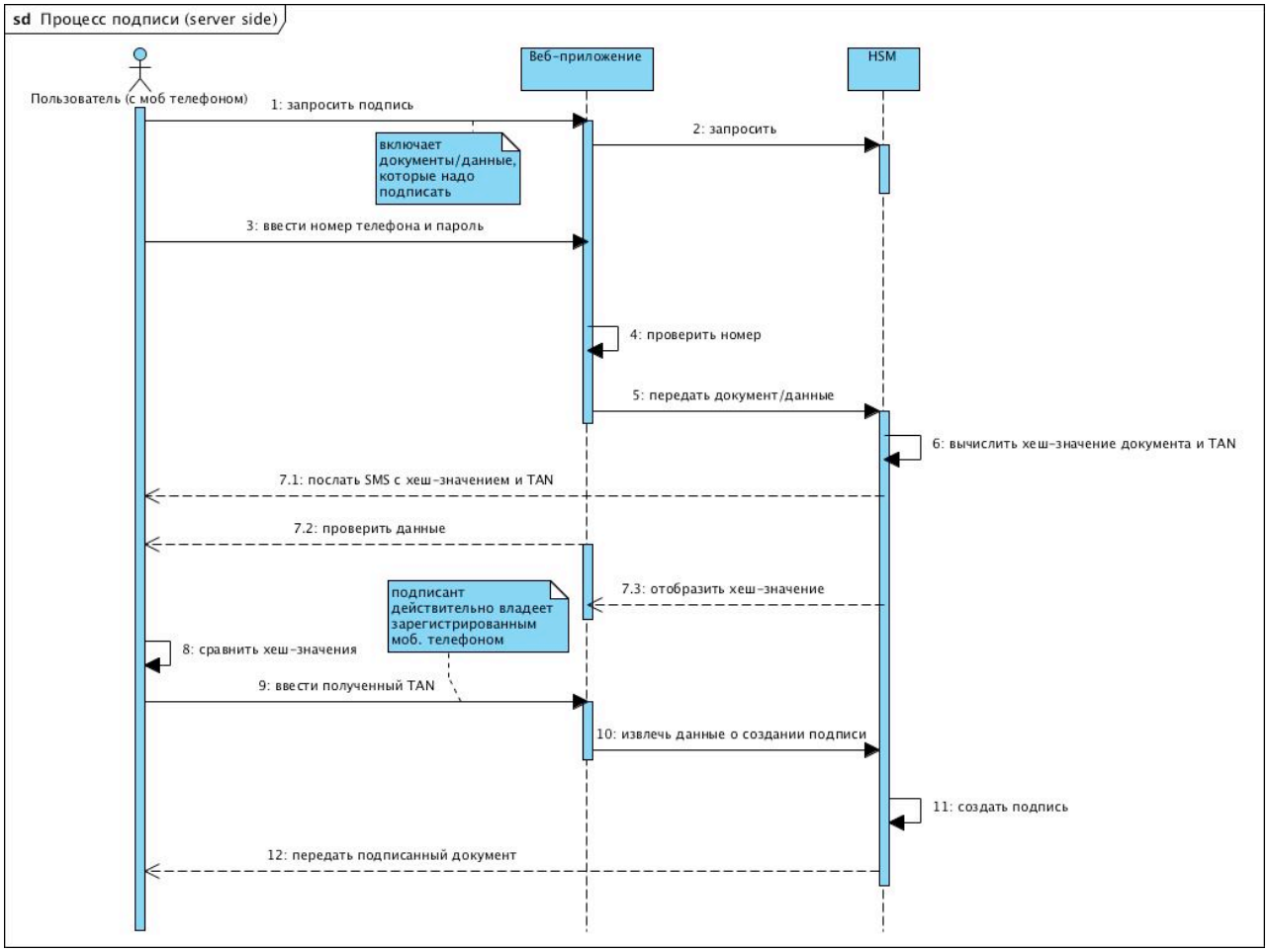

Рисунок 11 — Процедура электронной подписи на стороне сервера

Расшифрование данных для создания подписи и создание самой подписи выполняются исключительно внутри сертифицированного HSM, подобранные механизмы декодирования гарантируют, что технически это возможно только там. С этой точки зрения, безопасность созданной подписи равна безопасности в случае метода, основанного на смарт-карте. Процесс подписи запускается двумя компонентами: обнаружение пароля (фактор «знание») и номера мобильного телефона, и положительный результат проверки владения мобильный телефоном (фактор «владение»). Фактор «знание» проверяется самим HSM в процессе расшифрования данных для создания подписи. Проверка фаткора «владение» осуществляется безопасным приложением, что также включает связь со второстепенными элементами, такими как SMS шлюз или веб фронт-энд.

2.3 Технические требования к процедурам идентификации и аутентификации пользователей

Сервис защищенного доступа к государственным и муниципальным услугам в электронной форме, как сервис федерального масштаба, выдвигает специализированные требования к процедурам аутентификации и идентификации, допустимым к использованию в таком сервисе [10, 11]. Разделяемая идентичность (федерализм) формирует взаимозависимость и спектр обязательств в пространстве взаимодействия с государственными и муниципальными услугами в электронной форме.

Предлагаемые для использования в сервисе защищенного доступа процедуры идентификации и аутентификации должны удовлетворять базовым критериям со стороны пользователей, чтобы обеспечивать необходимый уровень доверия к государственным и муниципальным услугам в электронной форме. Среди потенциальных угроз, с которыми сталкиваются пользователи государственных и муниципальных электронных услуг:

- похищение атрибутов доступа пользователя – пользовательские атрибуты доступа могут быть скомпрометированы мошенником с помощью подставного сайта или какого-либо рода фишинговой атаки;
- снижение уровня конфиденциальности пользователя – многие пользователи не доверяют государственным услугам в электронной форме из-за боязни, что их персональные данные могут быть раскрыты;
- лояльность посредников, предоставляющих госуслуги (в т.ч. сервиса защищенного доступа) – они должны разделять ответственность в случае возникновения инцидентов информационной безопасности.

Для нейтрализации указанных выше проблем процедуры аутентификации должны соответствовать ряду требований, чтобы они могли быть применимы в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме. Перечислим основные:

- использование схем аутентификации, базирующихся на стойких алгоритмах, в т.ч. криптографических – криптография в цифровой среде является наиболее естественным средством обеспечения информационной безопасности;
- интероперабельность механизмов проверки атрибутов доступа – пользовательские атрибуты доступа и процедура аутентификации, их использующая, должны быть применимы независимо от типа прикладной услуги, к которой пользователь пытается аутентифицироваться, либо аппаратной платформы (в т.ч. пользовательского оборудования);
- в соответствии с принципом приоритетности открытых стандартов для использования в инфраструктуре государственных электронных услуг, процедуры аутентификации и идентификации, используемые в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме, должны базироваться на открытых стандартах;
- использование отечественных криптографических стандартов в процедурах идентификации и аутентификации.

Как было указано выше, наиболее естественной и целесообразной с точки зрения создания сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме на базе оператора информационно-коммуникационных сетей. Схема аутентификации – схема, основанная на одноразовых паролях. Схема является доверенной и соответствует высокому уровню информационной безопасности, кроме того генерация одноразовых паролей в соответствии со стандартами, описанными в RFC 4226 и RFC 4758, возможна с использованием отечественного криптографического стандарта ГОСТ Р 34.11-94.

В рамках работ по стандартизации существующих схем работы с одноразовыми паролями, организована рабочая группа, занимающаяся созданием открытых стандартов для механизмов одноразовых паролей – OTPS (One-Time Password Specifications). В результате, усилиями специалистов ряда

лабораторий и компаний из различных стран проведена работа по унификации (стандартизации) схем одноразовых паролей, механизмов и протоколов, результаты которой по итогам нескольких рабочих совещаний приведены на сайте RSA Laboratories [9)].

На текущий момент доступны восемь документов, специфицирующих OTP. Эти документы полностью покрывают основные аспекты использования одноразовых паролей такие, как:

- инициализация OTP-атрибутов в присоединенном токене;
- получение OTP из токена;
- пересылка и проверка OTP.

На рисунке 12 показан полный жизненный цикл одноразового пароля, а также протоколы, используемые на определенных этапах его жизненного цикла.

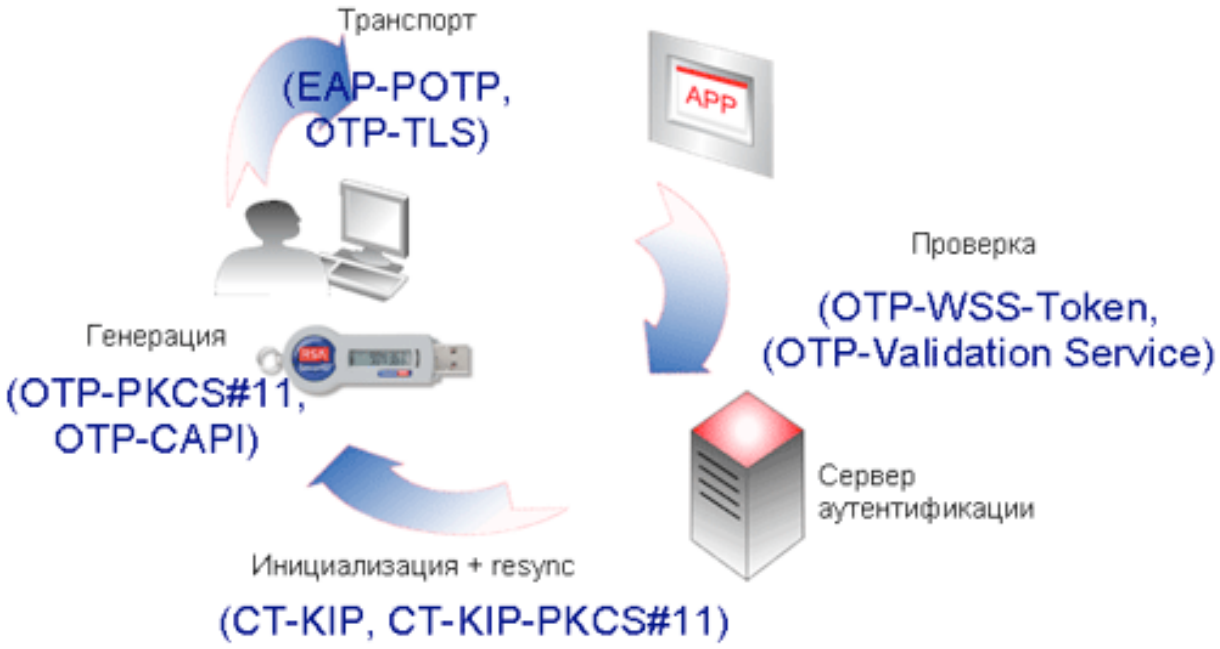

Рисунок 12 — Жизненный цикл одноразового пароля в соответствии с OTPS

Инициализация токена (CT-KIP).

CT-KIP [RFC 4758] – протокол типа клиент-сервер для инициализации и конфигурации криптографического токена с разделяемыми ключами. Он предназначен для использования в коммуникационных и компьютерных системах на основе связанных криптографических токенов. Протокол достаточно удобен и гибок, поскольку не требует ни применения схем с симметричным распределением ключей, ни наличия инфраструктуры открытых ключей.

Версия 1.0 этого протокола опубликована в декабре 2005 г. и описывает четырех-проходовый протокол инициализации типа клиент-сервер, в котором обе стороны вносят вклад в энтропию генерируемых ключей. Коротко его суть состоит в следующем:

- клиент CT-KIP передает серверу информацию о том, какой токен будет инициализирован, поддерживаемую версию протокола, а также для каких алгоритмов шифрования будут сгенерированы ключи. Также передается информация об алгоритмах MAC (Message Authentication Code), поддерживаемых токеном;
- в соответствии с полученной от клиента информацией сервер CT-KIP передает клиенту некоторое случайное значение RS. Вместе с этим случайным значением сервер передает клиенту информацию о том, ключи для какого алгоритма шифрования будут сгенерированы, а также информацию о том, каким шифром будут защищаться данные, передаваемые на следующих проходах протокола (при использовании асимметричной схемы шифрования, передается открытый ключ сервера). Длина RS может зависеть от того, для какого алгоритма шифрования генерируется ключевой материал;
- токен генерирует случайное значение RC и шифрует его, используя выбранный на предыдущем этапе алгоритм шифрования с ключом K, который является либо открытым ключом сервера, либо разделяемым секретом, присланным с его же стороны. Длина RC может зависеть от типа выбранного

ключа. Токен отправляет зашифрованное значение RC серверу. Кроме того, токен вычисляет ключ KTOKEN заданного типа на основе значений RC и RS и ключа K;

- сервер расшифровывает значение RC и вычисляет ключ KTOKEN заданного типа на основе двух значений RC и RS, а также ключа K. После чего сервер ставит в соответствие токену значение KTOKEN и сохраняет его. Впоследствии эта пара может быть использована для проверки или расшифровки данных, полученных от токена;
- после того как сервер запомнит информацию о ключе токена, он посылает подтверждение, которое содержит идентификатор сгенерированного ключа, а иногда также дополнительную информацию о настройках;
- после того как получено подтверждение от сервера, токен ставит в соответствие идентификатор ключа с его значением и сохраняет полученную конфигурационную информацию, если таковая имеется.

Модификация протокола CT-KIP не прекращается, и в марте 2006г. вышла версия 1.1, в которой добавлены одно- и двух-проходовые варианты для упрощения схем распределения ключей, новая схема вычисления MAC, а также XML-схема самого протокола. В целом, аналогов протоколу CT-KIP на текущий момент нет, а в дальнейшем он сможет стать удобным средством для инициализации ключевого материала, не только в приложении к OTP.

Генерация (OTP-PKCS#11 и MS CryptoAPI).

Данные стандарты описывают объекты, процедуры и механизмы (как для PKCS#11, так и для MS CryptoAPI), которые применяются для инициализации и проверки сгенерированных токенов. Основным моментом можно считать то, что эти механизмы предоставляют схему доступа к связанному токену для приложений в режиме совместимости, что существенно облегчает задачу подключения приложения к токену без использования специального API.

На рисунке 13 показано как PKCS#11 интегрируется в приложение, которому требуется аутентификация с использованием OTP-токенов.

В данном случае показан пример связанного аппаратного токена, однако программные реализации токенов имеют аналогичный механизм интеграции. Приложение вызывает процедуру C_Sign, чтобы получить значение одноразового пароля от токена. В примере приложение затем передает полученное значение некоторому Client API, которое в свою очередь уже пересылает его серверу аутентификации по сети. В качестве Client API могут быть использованы стандартные протоколы аутентификации такие, как RADIUS [RFC 2865] или EAP [RFC 3748]. Возможно также использование других протоколов.

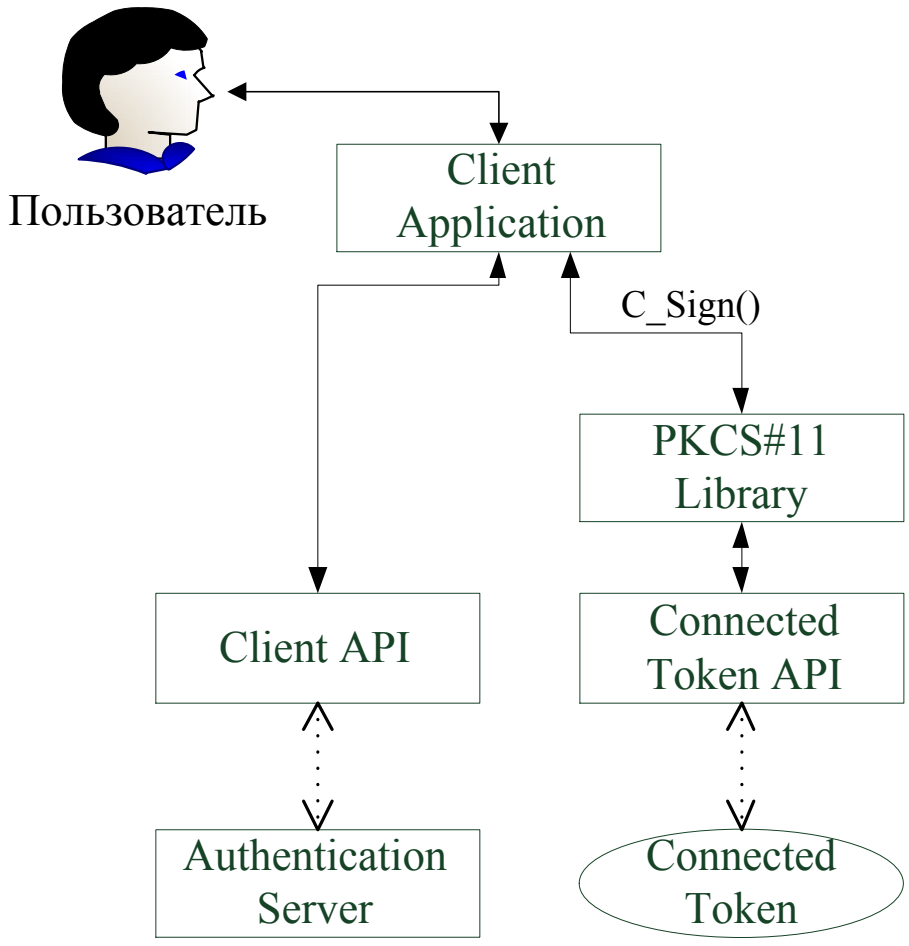

Рисунок 13 — Процедура генерации через PKCS#11

Транспорт (OTP-TLS и EAP-POTP).

EAP – набор протоколов, широко используемых для аутентификации сторон при сетевом доступе, в частности, на основе WiFi, удаленном доступе

PPP и в IPSec. Реализация обычно состоит из станции, точки доступа (NAS – Network Access Server) и сервера аутентификации.

Обычно работа протокола EAP сводится к посылке в NAS атрибутов, которые затем перенаправляются на сервер аутентификации. К особенностям исполнения протокола EAP в применении к одноразовым паролям (т.е. протокола EAP-POTP) можно отнести следующие: EAP-POTP определяет метод, который позволяет программно использовать OTP-токен, осуществляет взаимную аутентификацию сторон и генерирует ключевой материал.

Протокол TLS (Transport Layer Security) широко используется для обеспечения защиты сессий не только при работе в Интернете, но и в других видах сессионного доступа. Данный протокол использует значительное многообразие криптографических методов и шифр-сюит (ciphersuits). В OTP-TLS используется в соединении с т.н. Pre-Shared Key (PSK) шифр-сюитами [RFC 4279]. Главным моментом в протоколе является то, что он определяет вывод PSK из OTP, а также то, что в протоколе определены несколько новых расширений для TLS в зависимости от строгости OTP.

Проверка (OTP-WSS-Token, OTP Validation Service).

Часть спецификации, касающаяся проверки OTP, на сегодняшний день находится в наименее проработанном состоянии и будет, скорее всего, существенно дополняться и расширяться в самое ближайшее время.

OTP-WSS-Token используется для OTP-аутентификации в схемах по обработке запросов к доверенной стороне для WEB-сервисов. В данном протоколе используются XML-кодированные OTP-объекты, которые содержат аутентификационные атрибуты. Пример такого токена приведен на рисунке 14.

Функционально, это аналог OASIS Web Services Security 2 – пользовательский профиль, но привязанный к OTP. Важным моментом в OTP-WSS-Token является то, что могут быть использованы различные типы токенов, в том числе time-based, challenge-based, counter-based, которые могут активироваться либо с сервера, либо с клиента.

```
<otp-wst:OTPToken TokID="AnExampleToken" TokUser="Vitaliy Lyaper">
<TokTimestamp>2005-04-15T20:25:42Z
</TokTimestamp>
<TokNonce>VXUkQQ5c/Iua4LqKeq3ciFzEv/MbZhA==
</TokNonce>
<TokPIN>8761</TokPIN>
<OTP>142857</OTP>
</otp-wst:OTPToken>
```

Рисунок 14 — Пример OTP-WSS-Token

OTP Validation Service – WEB-сервис между взаимодействующими сторонами и сервером проверки OTP для определения аутентичности запросов. Основная функциональность сервиса заключается в отправке OTP-токенов к валидатору и получении ответа типа «да/нет». OTP Validation Service поддерживает большое количество OTP-методов, с помощью которых становится возможным воспроизвести ряд функций, таких как ресинхронизация требуемого OTP-компонента с аутентифицирующим сервисом и управление валидирующим сервисом. Также в сервис включена поддержка защиты сообщений (подпись, шифрование).

2.3.1 Требования по использованию криптографических алгоритмов в процедурах доступа и взаимодействия с инфраструктурой государственных и муниципальных сервисов в электронном виде

Поскольку сервис защищенного доступа к государственным и муниципальным услугам в электронной форме предоставляет доступ гражданам к инфраструктуре государственной значимости, а также создает защищенное поле для юридически значимого взаимодействия, обработки персональных данных граждан и других чувствительных с точки зрения информационной безопасности действий, функционирование сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме должно базироваться на использовании отечественных криптографических алгоритмов в процедурах доступа и взаимодействия.

На основании предложенной архитектуры сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме на базе ресурсов оператора информационно-коммуникационных сетей, формулируются следующие требования по использованию отечественных криптографических алгоритмов в сервисе:

- использование в схеме аутентификации для сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме ГОСТ Р 34.11-94;
- использование в механизмах электронной подписи для осуществления юридически-значимого взаимодействия с государственными органами ГОСТ 34.10-2001;
- для организации дополнительной защиты в случае необходимости передачи чувствительных данных по слабозащищенным каналам связи возможно использование симметричного шифрования по ГОСТ 28147-89.

2.3.2 Технические требования к идентификаторам, используемым в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме

С учетом требований к процедурам аутентификации и идентификации, задействованных в работе сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме, формируется также список функциональных требований к устройствам, используемым в качестве персональных идентификаторов в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме:

- однофакторная аутентификация;
- двухфакторная аутентификация;
- строгая двухфакторная аутентификация;

- многофакторная аутентификация (в комбинации с другими средствами);
- аутентификация с использованием автоматически генерируемых одноразовых паролей;
- наличие большого размера доступной энергонезависимой электрически программируемой памяти (не менее 16Кб) для хранения ключевой информации, паролей, профилей и сертификатов с возможностью доступа к ним только авторизованных пользователей;
- возможность аппаратной реализации западных криптографических алгоритмов (RSA/1024, DES, 3DES, SHA-1) для обеспечения совместимости процедур аутентификации и интеграции в распространенные продукты западных производителей;
- доверенная загрузка ключей шифрования и ЭП;
- поддержка сертифицированных российских криптографических алгоритмов;
- персональный идентификатор должен быть гарантированно уникальным;
- изготовитель должен гарантировать отсутствие выпуска дубликатов устройств;
- ключевая информация (закрытые ключи пользователя), записанные в память или сгенерированные идентификатором, не могут быть из него извлечены;
- трафик между идентификатором и хостом (ридером / компьютером) должен быть надежно защищен;
- длительный срок наработки на отказ для идентификатора;
- идентификатор должен иметь:
    - память, доступ к которой защищен PIN-кодом;
    - средства защиты PIN-кода от подбора методом перебора;

- средства контроля качества вводимого пользователем PIN-кода;

- должна обеспечиваться простота использования и «горячее» подключение идентификатора, в том числе:
  - без использования дополнительных устройств считывания (ридеров);
  - мобильность работы (возможность быстрого перехода на другое рабочее место без копирования и установки пользовательских профилей, сертификатов и пр.);
- возможность использования идентификатора для хранения биометрических данных его владельца;
- наличие инфраструктуры централизованного контроля и управления устройствами, аудита их использования, обработки потерянных / вышедших из употребления идентификаторов, отзыва устройств, восстановления данных при замене идентификаторов;
- возможность крупных поставок идентификаторов в ограниченные сроки;
- наличие неснижаемого запаса у поставщика для оперативной замены по гарантии вышедших из строя идентификаторов;
- наличие необходимых лицензий у поставщика / производителя, разрешений на экспорт/импорт идентификаторов;
- наличие соответствующих сертификатов, подтверждающих отсутствие содержания вредных веществ или их содержание в пределах санитарно-гигиенических норм, безопасность для здоровья человека, пожаробезопасность, отсутствие вредных электромагнитных излучений, влияющих на здоровье человека и на работу находящегося рядом электронного оборудования, на влагозащищенность.

2.4 Рекомендации по использованию ресурсов оператора информационно-коммуникационных услуг (абонентская база, транспортные возможности сети и абонентских устройств) для внедрения государственных и муниципальных сервисов в электронном виде (в том числе сервиса электронного голосования) с целью охвата ими наиболее широких слоев населения Российской Федерации

К ключевым ресурсам оператора информационно-коммуникационных услуг, которые могут быть задействованы в построении инфраструктуры сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме относятся [12, 13]:

- абонентская база оператора связи;
- (U)SIM-карты абонентов;
- удостоверяющий центр оператора связи;
- инфраструктура персонализации (U)SIM-карт;
- сеть распространения абонентских комплектов;
- ресурсы транспортной сети оператора связи.

Перечисленные ресурсы оператора связи позволяют наиболее полным образом охватить население Российской Федерации с целью предоставления государственных и муниципальных услуг в электронном виде, обеспечить создание инфраструктуры для обеспечения юридически-значимого взаимодействия между гражданами и государственными органами с использованием электронной подписи в соответствии с законом №63-ФЗ от 06.04.2011 г. «Об электронной подписи», а также обеспечить защиту персональных атрибутов доступа граждан к государственным и муниципальным услугам в электронной форме.

Основными способами использования ресурсов оператора информационно-коммуникационных услуг в схеме создания сервиса

защищенного доступа к государственным и муниципальным услугам в электронной форме, являются:

- использование абонентской базы оператора информационно-коммуникационных услуг с целью обеспечения всех его абонентов атрибутами доступа к государственным и муниципальным услугам в электронной форме;
- обеспечение информационной безопасности пользовательских атрибутов доступа к государственным и муниципальным услугам в электронной форме с использованием (U)SIM-карт оператора информационно-коммуникационных сетей в качестве защищенного носителя информации;
- выпуск ключей электронной подписи и сертификатов для них с использованием удостоверяющего центра оператора информационно-коммуникационных сетей;
- персонализация абонентских комплектов с целью выполнения требований закона №63-ФЗ от 06.04.2011 г. «Об электронной подписи» при распространений их через инфраструктуру продаж оператора информационно-коммуникационных услуг.

2.4.1 Использование абонентской базы оператора информационно-коммуникационных услуг с целью обеспечения всех его абонентов атрибутами доступа к государственным и муниципальным услугам в электронной форме

Операторы информационно-коммуникационных услуг на сегодняшний день обладают базой абонентских комплектов, превышающей население Российской Федерации. Распространенность и доступность мобильных телефонов позволяет уверенно утверждать, что каждый гражданин Российской Федерации, имеющий право получать те или иные государственные услуги в электронном виде, обладает как минимум одним мобильным телефоном и

абонентским комплектом того или иного оператора связи, состоящего из (U)SIM-карты и договора на оказание услуг связи [14].

На основании закона № 126-ФЗ от 07.07.2003 «О связи» при заключении договора на оказание услуг связи абонент должен предоставить документы, удостоверяющие личность абонента. Таким образом, при получении абонентского комплекта оператора связи происходит его персонализация – устанавливается взаимосвязь между персональными данными абонента и его абонентским комплектом.

Предоставленные в такой форме атрибуты доступа однозначно увязаны с паспортными данными абонента и позволяют тем самым строго идентифицировать абонента при доступе к государственным и муниципальным услугам в электронной форме с использованием этих атрибутов.

Включение в договор абонента оператора сотовой связи пункта о том, что одновременно с услугами связи абонент получает доступ к государственным и муниципальным услугам в электронной форме позволит предоставить атрибуты доступа к государственным и муниципальным услугам всем гражданам заключающим договор об оказании услуг связи, либо производящим замену (U)SIM-карты.

2.4.2 Обеспечение информационной безопасности пользовательских атрибутов доступа к государственным и муниципальным услугам в электронной форме с использованием (U)SIM-карт оператора информационно-коммуникационных сетей в качестве защищенного носителя информации

Пользовательские атрибуты доступа, используемые в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме, нуждаются в обеспечении их информационной безопасности.

Информационная безопасность атрибутов, находящихся во владении пользователя должна обеспечиваться с использованием средств, которые:

- хранят и используют атрибуты доступа в защищенной среде, в том числе не допускающей компрометации атрибутов при физических воздействиях на контейнер;
- имеют достаточную вычислительную мощность для использования отечественных криптографических алгоритмов, задействованных в схемах аутентификации в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме;
- позволяют производить только доверенную загрузку атрибутов на носитель.

(U)SIM-карта оператора связи является защищенным носителем, соответствующим по требованиям защиты информации банковским смарт-картам и на протяжении всего времени существования сетей 2G и 3G мобильной связи служат надежным средством для обеспечения информационной безопасности ключевого материала, используемого для доступа к сети оператора связи, а также другим VAS (Value Added Services).

По уровню защиты (U)SIM-карты соответствуют требованиям:

- ГОСТ Р ИСО/МЭК 7816-6-2003 Карты идентификационные. Карты на интегральных схемах с контактами. Часть 6. Элементы данных для межотраслевого обмена;
- ГОСТ Р ИСО/МЭК 7816-10-2004 Карты идентификационные. Карты на интегральных схемах с контактами. Часть 10. Электронные сигналы и ответ на восстановление у синхронных карт;
- ГОСТ Р ИСО/МЭК 7816-1-2010 Карты идентификационные. Карты на интегральных схемах с контактами. Часть 1. Физические характеристики.

Вычислительная мощность (U)SIM-карт, представленных на Российском рынке, по результатам экспериментальной проверки и нескольких пилотных проектов (МТС , Мегафон) достаточна для реализации схемы аутентификации с

использованием одноразовых паролей, генерируемых с использованием хеш-функции ГОСТ Р 34.11-94 приложением на (U)SIM-карте.

Наконец, инфраструктура профилирования и персонализации (U)SIM-карт, используемая операторами информационно-коммуникационных услуг, описанная в подразделе «2.6 Рекомендации по профилированию и персонализации атрибутов профиля пользователя с использованием ресурсов оператора информационно-коммуникационных сервисов (удостоверяющий центр, абонентская база оператора, абонентские носители информации и идентификаторы)» позволяет загружать атрибуты для сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме доверенным образом.

Все вышесказанное говорит о наличие технической возможности использования (U)SIM-карт оператора связи в качестве защищенного контейнера для персональных атрибутов доступа сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме.

2.4.3 Выпуск ключей электронной подписи и сертификатов для них с использованием удостоверяющего центра оператора информационно-коммуникационных сетей и персонализация абонентских комплектов с целью выполнения требований закона №63-ФЗ от 06.04.2011 г. «Об электронной подписи» при распространений их через инфраструктуру продаж оператора информационно-коммуникационных услуг

Инфраструктура оператора информационно-коммуникационных услуг содержит в своей структуре удостоверяющий центр, который может быть использован для нужд предоставления государственных и муниципальных услуг в электронной форме.

С использованием средств удостоверяющего центра оператора информационно-коммуникационных услуг, для каждой выпускаемой (U)SIM-карты может быть выпущена ключевая пара, допустимая для использования в

режиме с ГОСТ Р 34.10-2001, а также соответствующий сертификат открытого ключа электронной подписи.

В случае проведения процедуры аккредитации соответствующего удостоверяющего центра и включения в процедуру передачи абонентского комплекта процессуальной нормы, связанной с передачей абоненту сертификата открытого ключа подписи, становятся выполнимы нормы закона №63-ФЗ от 06.04.2011 г. «Об электронной подписи» необходимые для выполнения требований закона к квалифицированной электронной подписи.

Инфраструктура профилирования и персонализации (U)SIM-карт, используемая операторами информационно-коммуникационных услуг, описанная в разделе «2.6 Рекомендации по профилированию и персонализации атрибутов профиля пользователя с использованием ресурсов оператора информационно-коммуникационных сервисов (удостоверяющий центр, абонентская база оператора, абонентские носители информации и идентификаторы)« позволяет загрузить информацию о выпущенной ключевой паре для цифровой подписи и сертификате открытого ключа подписи пользователя государственных и муниципальных услуг в электронной форме на (U)SIM-карту абонента, используя технологию доставки данных по воздуху (OTA – over-the-air).

2.5 Описание профиля пользователя государственных и муниципальных сервисов в электронном виде

Профиль пользователя государственных и муниципальных услуг в электронной форме представляет собой совокупность параметров, относящихся к пользователю и взаимоувязанных с его личностью в процессе персонализации атрибутов профиля пользователя и услуг, этому пользователю предоставляемых.

В общем виде профиль пользователя государственных и муниципальных услуг в электронном виде состоит из следующих наборов данных:

- ключевой материал;
- параметры и настройки приложений и услуг электронного правительства;
- приложения, в т.ч. для аутентификации в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме;
- персональный сертификат открытого ключа цифровой подписи гражданина Российской Федерации;
- персональные данные пользователя, в т.ч. биометрическая информация;
- информация о регистрации по месту жительства;
- контактная информация (почтовый адрес для связи, адрес электронной почты, контактный телефон).

Профиль пользователя государственных и муниципальных услуг в электронной форме представляет собой распределенную сущность, которая может размещаться частично в разных информационных системах и на разных носителях, объединяемых единым идентификатором пользователя и набором средств для аутентификации пользователя в этих информационных системах.

К персональным данным, включаемым в профиль пользователя государственных и муниципальных услуг в электронной форме, относятся:

- фамилия, имя, отчество;
- год, месяц, дата и место рождения;
- серия, номер, дата и место выдачи основного документа, удостоверяющего личность;
- адрес;
- семейное, социальное, имущественное положение;
- образование, профессия.

Формат *сертификата открытого ключа* гражданина Российской Федерации соответствует рекомендациям Международного Союза по

телекоммуникациям ITU (X.509) и документе RFC 3280 Certificate & CRL Profile организации инженерной поддержки Интернета Internet Engineering Task Force (IETF).

Сертификат содержит элементы данных, сопровождаемые цифровой подписью издателя сертификата, т.е. оператора информационно-коммуникационных услуг (Рисунок). В сертификате имеется десять основных полей: шесть обязательных и четыре опциональных. Большая часть информации, указываемой в сертификате, не является обязательной, а содержание обязательных полей сертификата может варьироваться. К обязательным полям относятся:

- серийный номер сертификата Certificate Serial Number;
- идентификатор алгоритма подписи Signature Algorithm Identifier;
- имя издателя Issuer Name;
- период действия Validity (Not Before/After);
- открытый ключ субъекта Subject Public Key Information;
- имя субъекта сертификата, т.е. пользователя государственных и муниципальных услуг в электронной форме Subject Name.

Структура сертификата представлена на рисунке 15.

Требования к сертификатам открытого ключа, являющимся квалифицированным устанавливает ФСБ Российской Федерации. В данный момент подготовлен проект приказа «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи», доступный на официальном сайте ФСБ http://www.fsb.ru/files/fsbdoc/project_normakt/sertifkey_26102011.pdf .

Рисунок 15 — Структура сертификата

Параметры и настройки приложений электронного правительства представляют собой блок конфигурации персональных настроек в формате параметр-значение и могут быть использованы при работе с интерфейсом приложений государственных и муниципальных услуг в электронной форме.

Формат распределения параметров внутри профиля, а также необходимость хранения их в защищенном виде, определяется оператором информационно-коммуникационных услуг, формирующим профиль пользователя государственных и муниципальных услуг в электронной форме.

2.6 Рекомендации по профилированию и персонализации атрибутов профиля пользователя с использованием ресурсов оператора информационно-коммуникационных сервисов (удостоверяющий центр, абонентская база оператора, абонентские носители информации и идентификаторы)

«Персонализация сервиса – это возможность пользователя U изменять или порождать услугу A таким образом, что услуга A полностью

соответствует специфичным требованиям пользователя U в рамках своего представления и функционала, после такой персонализации услуга A должна предоставляться пользователю в дальнейшем в установленном им формате, в соответствии с проведенными пользователем U изменениями».

Персонализация как механизм уже давно и успешно используется. Как пример – интернет и компьютеры: каждому пользователю знакомы возможности современных интернет-приложений, начиная от почтового ящика, который можно полностью настроить и кастомизировать, заканчивая приложениями интернет-банкинга, когда пользователь может индивидуально настроить необходимый уровень безопасности, оповещения, установить дополнительное ПО для работы со своим банковским счетом и т.п.

2.6.1 Общие требования к персонализации для атрибутов профиля пользователя государственных и муниципальных услуг в электронной форме

Реализуемые механизмы обеспечения процессов персонализации, должны выполнять ряд требований к организации сервисов, персонализационной информации, а так же поддерживать несколько основополагающих схем работы с персонализационными данными.

В данном документе изложены следующие требования к организации механизмов персонализации для мобильных услуг:

- требования к разнесению данных между несколькими хранилищами (stakeholders);
- требования по организации самой мобильной услуги (далее просто услуги);
- требования по организации персонализационной информации.

Также приведено описание схем персонализации услуг, которые возможно использовать при персонализации государственных и муниципальных услуг в электронной форме.

2.6.1.1 Общие требования к информации о пользователе, с точки зрения её использования в механизмах персонализации

Данные о пользователе, в т.ч. и персонализационные, представляют собой профиль пользователя – User Profile. User Profile должен быть разделен между несколькими хранилищами (stakeholders), для выполнения следующих функций:

- управления пользовательскими настройками (user preference management);
- настройкой сервисов, с которыми работает пользователь, необходимым ему образом (user service customization);
- управление терминальными устройствами;
- обеспечение доступа к данным о пользователе (user information sharing);
- доступ к ключевому материалу пользователя.

2.6.1.2 Требования к процессам персонализации

Общим требованием к разрабатываемым механизмам обеспечения процессов персонализации является независимость от среды, в которой персонализация производится, т.е. профиль пользователя (user profile), должен быть организован таким образом, чтобы поддерживались следующие виды доступа к информации для персонализации (personalization information):

- crossdevice – т.е. вне зависимости от устройства с которым работает пользователь, т.е. персонализационные данные должны находиться либо на сервере, либо внутри usim-модуля пользователя;
- crossnetwork – поддержка роуминга и перехода между сетями, без прерывания предоставления услуги, т.е. должна быть организована передача

необходимых данных между сетями, или организован соответствующий доступ к ним;

- crossservice – разные сервисы должны иметь возможность получать доступ к базовым персонализационным данным (общим для всех).

2.6.1.3 Требования к организации услуг

Услуга, предоставляемая пользователю, должна соответствовать модели физического построения представленной на рисунке 16:

- *ServiceLogic* – программный код, бизнес-логика;
- *ServiceData* – данные необходимые для работы самой услуги(ввод/вывод, данные о внутренних состояних, служебная информация);
- *ServiceContent* – хранимые данные, т.е данные пользователя, с которыми он работает, посредством услуги;
- *ServiceProfile* – настройки самой услуги (размер шрифта, цвет букв и т.п.).

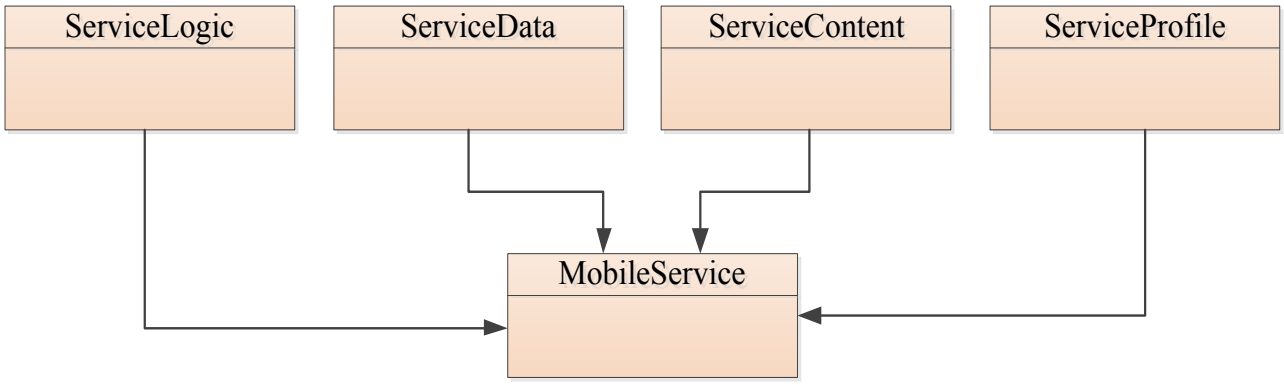

Рисунок 16 — Состав прикладной услуги

При такой организации услуги, легко может быть заменена её любая составляющая, без изменения во всех остальных компонентах, т.е. допустим, при замене схемы персонализации (подробнее об этом в следующем разделе) – изменения затронут только ServiceLogic, а остальные компоненты останутся такими же, как и раньше.

2.6.1.4 Схемы персонализации услуг

Услугу можно смоделировать следующим образом: есть абстрактная идея некоторой услуги (Service Concept), её конкретные имплементации (Service Implementation) и экземпляры услуг (Service Instance), доступные конечному пользователю. На рисунке 17 представлена декомпозиция услуги.

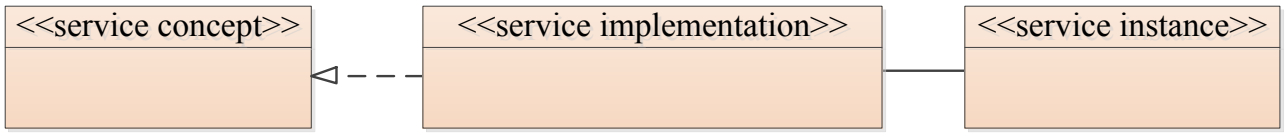

Рисунок 17 — Декомпозиция понятия услуги

В рамках работ по созданию механизмов персонализации необходимо поддерживать следующие схемы соединения персональных данных пользователя и предоставляемой ему услуги:

- каждый экземпляр услуги оперирует с собственными персонализационными данными (связь напрямую с экземпляром услуги, без учета типа имплементации) – указано на рисунке 18;
- несколько экземпляров услуги оперируют одними и теми же персонализационными данными (связь напрямую с экземпляром услуги, без учета типа имплементации) – указано на рисунке 19;
- несколько экземпляров различных услуг оперируют одними и теми же персонализационными данными – указано на рисунке 20.

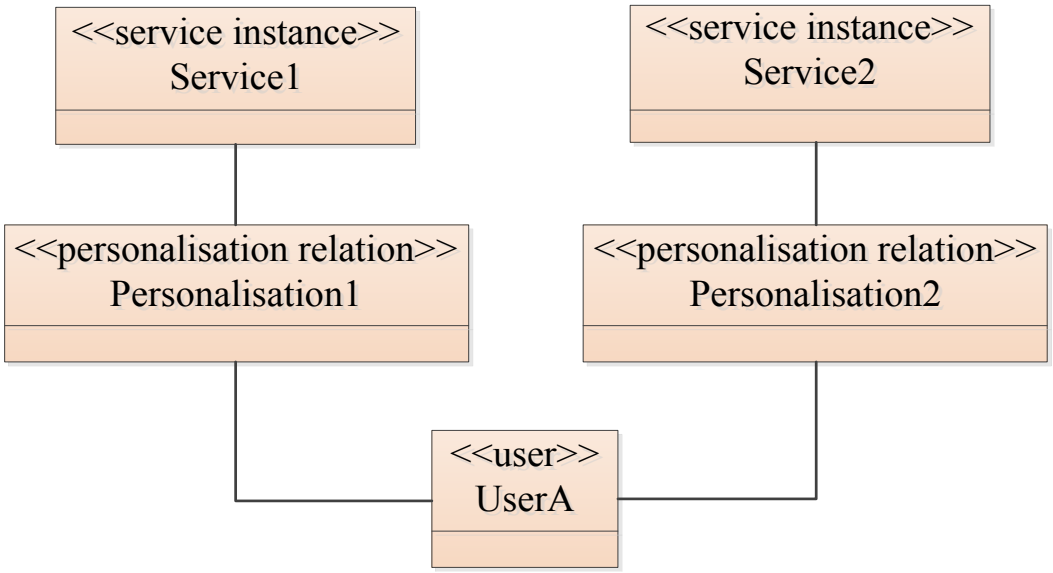

Рисунок 18 — Тип персонализации 1

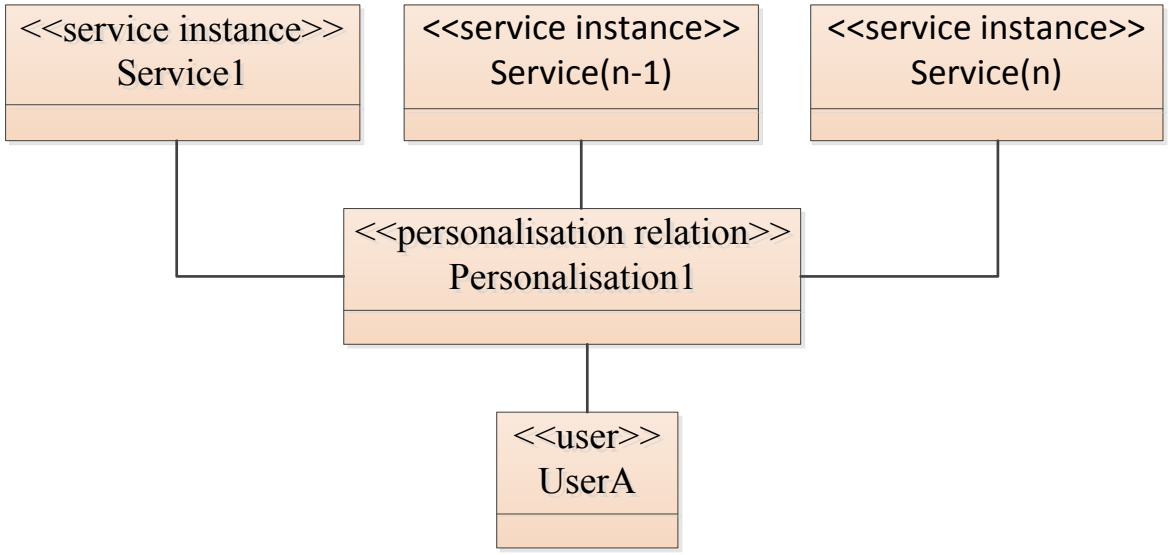

Рисунок 19 — Тип персонализации 2

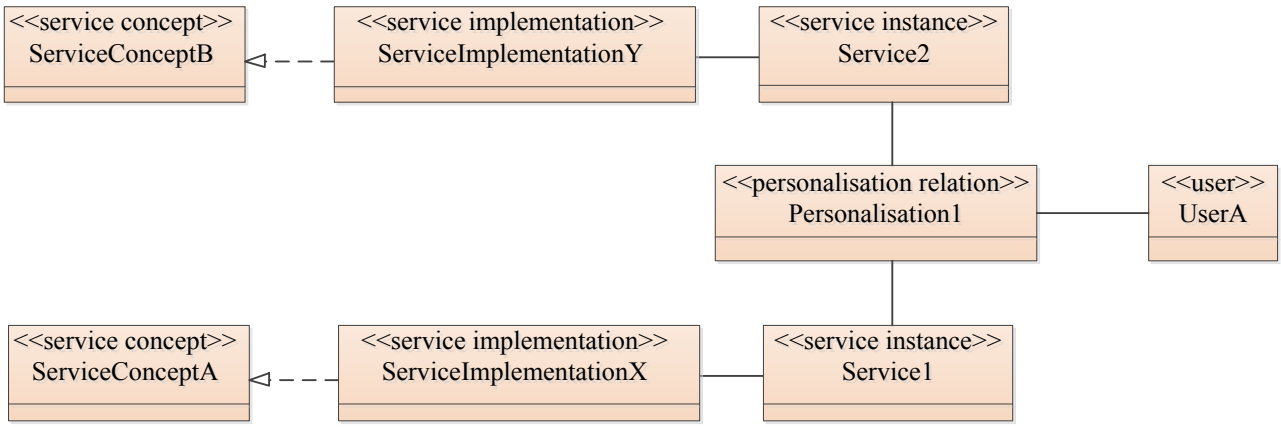

Рисунок 20 — Тип персонализации 3

2.6.1.5 Требования к информации персонализации

Информация персонализации, должна быть организована таким образом, чтобы была возможность реализовывать различные схемы персонализации услуг, при которых некоторые группы услуг могут использовать одни и те же данные. Предлагается следующая модель организации персонализационных данных:

- *Personalisation Information* – компонент, моделирующий всю совокупность персонализационной информации, в идеальном случае должен быть разделяемым между множеством поставщиков услуг и множеством центров предоставления услуг;
- *User Personalisation Information* – персонализационная информация пользователя;
- *Personal Information* – личные данные пользователя (ФИО, адрес, номер телефона, кредитной карты и т.п.), т.е. данные, в большинстве случаев уникальные и не сильно изменяющиеся для каждого пользователя.
- *Personal Generic Preferences* – общие (базовые) настройки для всех услуг, вне зависимости от их типа, имплементации и т.д.;
- *Service Concept Personalisation Information* – настройки, общие для конкретного типа услуг (Service Concept);

- *Service Personalisation Information* – персонализационная информация специфичная для конкретной услуги;
- *Service Personalisation Usage Information* – персонализационная информация, для конкретного типа использования услуги;
- *Personal Service Data* – рабочие данные услуги;
- *Personal Service Content* – пользовательские данные услуги (content);
- *Personal Service Profile* – настройки услуги.

Приведенная схема организации персонализационной информации, позволяет гибко изменять персонализационные данные, характерные для каких либо услуг или групп услуг, при этом не затрагивая остальные, а также позволяет легко интегрировать новые услуги в пользовательское окружение.

На рисунке 21 приведена модель организации персонализационных данных.

Состав персонализационной информации:

- ключи приложений, с помощью которых осуществляется доступ к сервису;
- настройки и предпочтения пользователей;
- пользовательские приложения.

Как видно, состав персонализационной информации довольно разнородный, этой информации довольно много, для каждого сервиса необходимо определять целую структуру данных, зачастую не одну. Для операторов это выливается в несколько важных вопросов.

Где хранить персонализационную информацию?

Каким образом её загружать в хранилище?

Как организовать структуру хранения персонализационной информации?

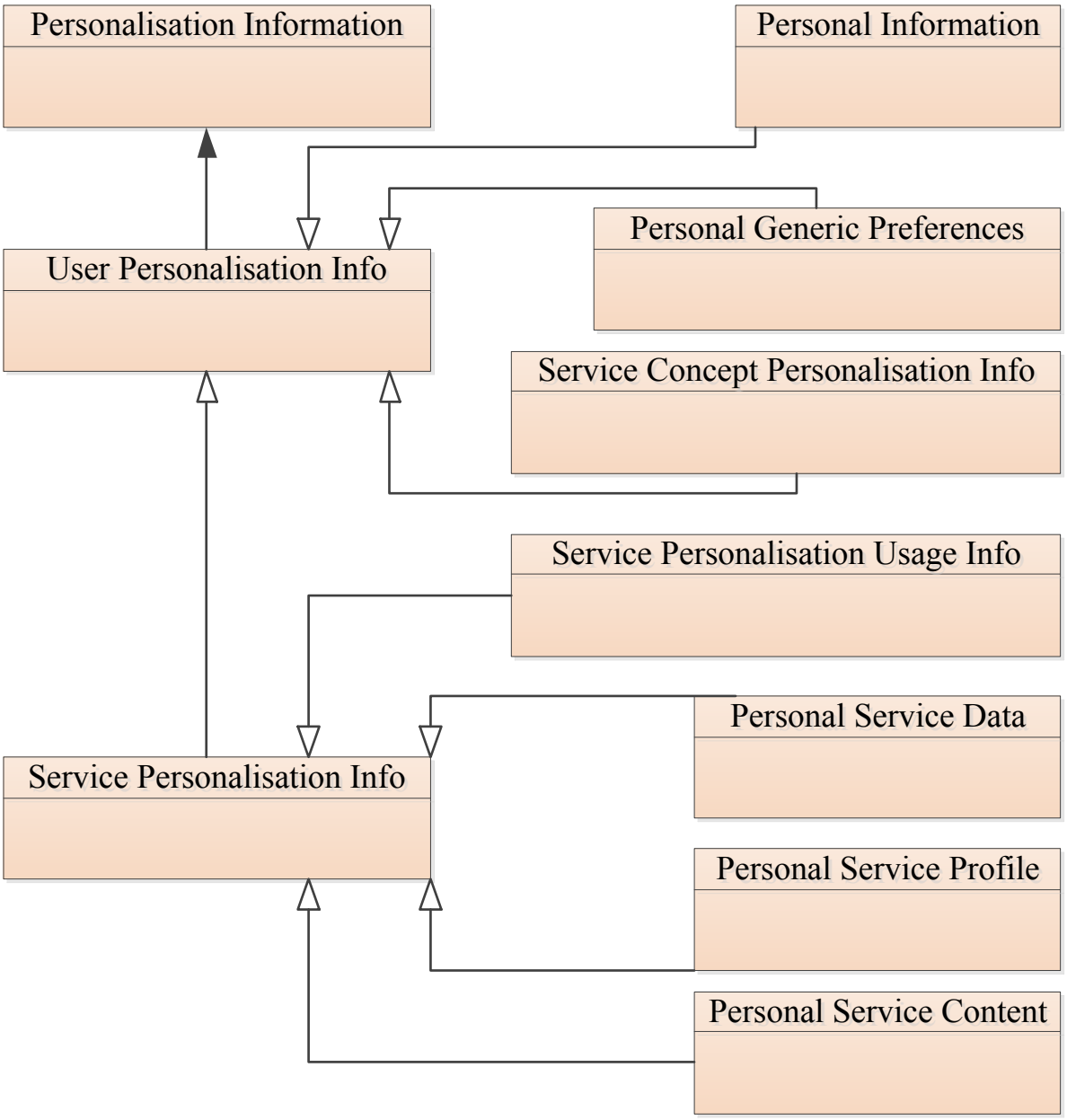

Рисунок 21 — Модель организации персонализационных данных

Первый и последний вопросы довольно сильно взаимосвязаны, в случае мобильных сетей связи есть несколько альтернатив:

- хранение персонализационной информации на (U)SIM-карте;
- хранение персонализационной информации в памяти телефона;
- хранение персонализационной информации у оператора связи с доступом посредством OTA-интерфейса (over-the-air) с использованием соответствующего ключа, хранящегося на (U)SIM-карте.

В сетях 2G для целей хранения персонализационных данных, в состав которых в основном входили ключи для соответствующих сервисов, а также sim-приложения, использовалась SIM-карт (Subscriber Identity Module). В сетях 3G на смену SIM-карте пришла USIM-карта, смарт-карта, характеризующаяся большим объемом памяти, более мощным процессором, а также возможностью применения в сетях UMTS. Для хранения данных на (U)SIM-картах производителями карт формируются соответствующие структуры данных. А вот способов загрузки данных на (U)SIM-карты есть несколько: загрузка при производстве, загрузка данных OTA.

В данной работе рассматривается первый способ, который реализуется в рамках формирования электрического профиля (U)SIM-карты производителем, при этом:

- на карту записываются необходимые ключи для доступа к различным доступным пользователю сервисам (в т.ч. голосовым);
- на карту записываются необходимые данные помимо ключей, например sim-апплеты.

2.6.2 Процедура персонализации для атрибутов профиля пользователя государственных и муницфипальных услуг в электронной форме

Предлагаемая процедура персонализации для нужд сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме, разработана для решения следующих задач:

- защищенное создание, хранение и использование пользовательских атрибутов, в т.ч. атрибутов доступа к инфраструктуре государственных и муниципальных услуг;

- размещение профиля пользователя государственных и муниципальных услуг на (U)SIM-картах оператора информационно-коммуникационных сетей;
- персонификация профиля пользователя государственных и муниципальных услуг, для выполнения требований закона № 63-ФЗ от 06.04.2011г. «Об электронной подписи» для организации в дальнейшем защищенного юридически значимого электронного документооборота между пользователем государственных и муниципальных услуг и ведомствами их предоставляющими.

Процедура переперсонализации атрибутов (U)SIM-карт, изображенная на рисунке 22, используется в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме для достижения следующих целей:

- своевременный выпуск необходимого количества персональных средств аутентификации, достаточного для постепенного охвата электронным доступом к государственным и муниципальным услугам максимально широких слоев населения;
- привязка персональных средств аутентификации к персональным данным их владельца;
- генерация и защищенное хранение ключевого материала, используемого в сервисе аутентификации для государственных и муниципальных услуг в электронной форме;
- выпуск сертификатов открытого ключа гражданина и передача его пользователю в соответствии с требованиями федерального закона от 06.04.2011 N 63-ФЗ «Об электронной подписи»;
- доверенная загрузка персонализационной информации в процессе жизненного цикла (U)SIM-карты пользователя.

Процедура персонализации, представленная на рисунке 22 состоит из следующих основных подпроцессов.

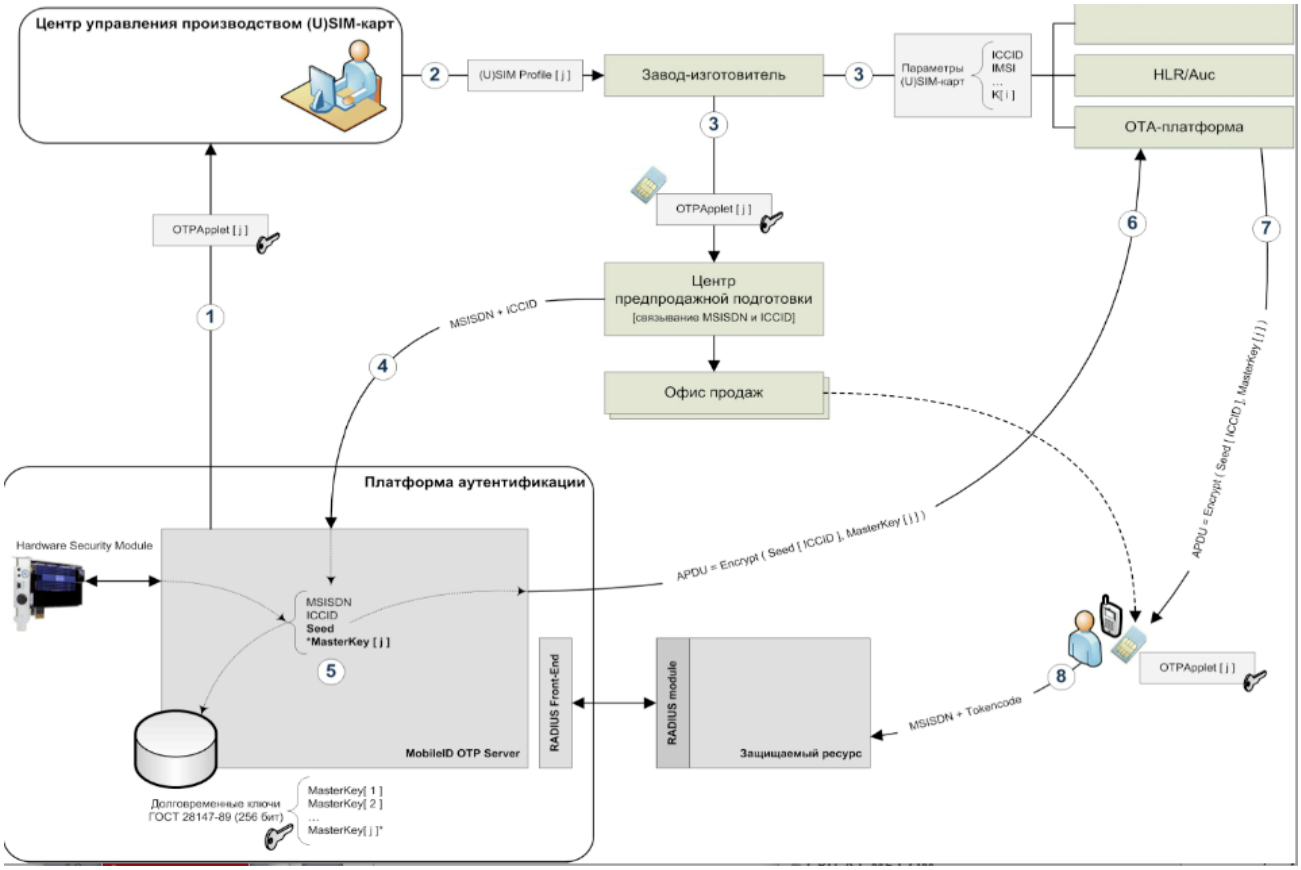

Рисунок 22 — Процедура персонализации в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме

Формирование приложения для (U)SIM-карты. На данном этапе средствами платформы аутентификации, а точнее аппаратного модуля безопасности, используемого в ней, генерируется приложение для (U)SIM-карты и ключевой материал для него (включая мастер-ключ для защищенного обмена данными с приложением). При этом за счет использования аппаратного модуля безопасности (HSM – Hardware Security Module) соблюдаются необходимые требования по защите ключевого материалы, его доверенной генерации приложения для (U)SIM-карты, выполняющего функции по генерации одноразового пароля в схеме аутентификации для доступа к

государственным и муниципальным услугам в электронной форме. Сгенерированные (U)SIM-приложения для генерации одноразовых паролей в схеме аутентификации к государственным и муниципальным услугам в электронной форме передаются либо в зашифрованном виде, либо по защищенному каналу связи в Центр управления производством (U)SIM-карт.

В центре управления производством (U)SIM-карт производится **формирование профиля (U)SIM-карты** для его записи непосредственно на носитель. Профиль (U)SIM-карты представляет собой описание конфигурации конечного продукта, выпускаемого заводом-изготовителем (U)SIM-карт. В профиль входит информация об аппаратной конфигурации выпускаемых (U)SIM-карт, о ключевом материале, записываемом на карты, идентификаторах и приложениях, предустанавливаемых на карты, а также о свободных ячейках памяти на карте и ключах доступа к ним. Эти свободные ячейки памяти могут быть использованы в дальнейшем для записи дополнительных атрибутов на (U)SIM-карту. Приложение для генерации одноразовых паролей в схеме аутентификации для доступа к государственным и муниципальным услугам в электронной форме (OTPApplet) также включается в состав профиля при производтсве специализированных (U)SIM-карт, которые будут использованы в качестве персональных средств аутентификации при доступе к государственным электронным услугам. Сформированный профиль (U)SIM-карты передается на завод-изготовитель.

Данный этап состоит из двух параллельных подпроцессов – непосредственно **выпуска (U)SIM-карт заводом-изготовителем и технических действий со стороны оператора связи по загрузке необходимой информации в оборудование** (HLR – Home Location Register, AuC – Authentication Centre) для активации (U)SIM-карт. Выпущенная заводом-изготовителем (U)SIM-карта уже содержит OTPApplet, однако ещё не содержит ключевого материала, используемого приложением (ключевой материал загружается после получения абоненсткого комплекта пользователем в точке

продаж), после того как карта активирована на оборудовании оператора связи, возможна регистрация карты в сети связи и использование установленных на неё приложений. Выпущенные заводом-изготовителем (U)SIM-карты передаются в центр предпродажной подготовки.

В центре предпродажной подготовки производится **формирование абонентских комплектов** – брендирование (U)SIM-карт, подготовка информационных материалов, прилагающихся к ним. Также в центре предпродажной подготовки производится установление соответствия между номером мобильного телефона пользователя MSISDN (Mobile Station Integrated Services Digital Number) и номером самой карты ICCID (Integrated Circuit Card ID). Таким образом производится связывание каждой копии приложения для генерации одноразовых паролей в схеме аутентификации к государственнным и муниципальным услугам в электронной форме и номера мобильного телефона. Номер мобильного телефона на данный момент ещё не связан с конкретным физическим или юридическим лицом. Информация о связи номера мобильного телефона и номера (U)SIM-карты передается в платформу аутентификации. Сама карта поступает в центр продаж и обслуживания абонентов. В центре продаж при заключении с абонентом договора о предоставлении услуг связи, оператор связи берет в обработку персональные данные абонента, которые могут быть включены в профиль пользователя государственных и муниципальных услуг в электронной форме. В случае, если на карту записан сертификат открытого ключа электронной подписи, пункт о его передаче абоненту может быть включен в договор о предоставлении услуг связи.

Под защитой аппаратного модуля безопасности **производится генерация инициирующего вектора для (U)SIM-приложения OTPApplet**, значение вектора шифруется с помощью мастер-ключа, соответствующего этой копии приложения (MasterKey) и передается на OTA-платформу для загрузки на (U)SIM-карту, используемую пользователем по воздуху. Таким образом

производится активация приложения, используемого для аутентификации при доступе к государственным и муниципальным услугам в электронной форме.

Ключевой материал приложения, генерирующего одноразовые пароли для аутентификации к государственнным электронным услугам в защищенном виде, **передается на ОТА-платформу для активации**.

Загрузка данных с ОТА-платформы на (U)SIM-карту пользователя производится по воздуху. Полученный инициирующий вектор для приложения, генерирующего одноразовые пароли, расшифровывается в защищенной области памяти (U)SIM-карты и сохраняется для использования в схеме аутентификации. Пользовательские атрибуты доступа к государственным и муниципальным услугам с этого момента являются полностью активированными.

Аутентификация с использованием приложения на (U)SIM-карте, генерирующего одноразовые пароли с использованием ГОСТ Р 34.11-94.

Описанная схема персонализации сочетает в себе несколько подходов, которые позволяют обеспечить информационную безопасность ключевого материала (U)SIM-карт и приложений на них, а также выполнить необходимые требования законодательства:

- использование при генерации и хранении ключей и приложений аппаратного модуля безопасности позволяет обеспечивать защиту ключевого материала и приложений на всех стадиях генерации;
- обмен чувствительными данными производится в приведенной процедуре персонализации только шифрованным способом, с использованием блочного шифрования по ГОСТ 28147-89;
- ключевой материал, непосредственно используемый при доступе к государственным и муниципальным услугам в электронном виде, загружается на (U)SIM-карты в зашифрованном виде, тем самым исключается его открытое использование вне доверенных модулей (аппаратный модуль безопасности,

(U)SIM-карта) посредством аффилированной с оператором связи ОТА-платформы;

- предложенная схема персонализации позволяет проводить постперсонализационные мероприятия с использованием ОТА-платформы такие, как загрузка дополнительных атрибутов профиля пользователя на (U)SIM-карту или ротацию ключевого материала, используемого для доступа к государственным и муниципальным услугам в электронном виде.

На сегодняшний день, приведенная схема персонализации атрибутов доступа к государственным и муниципальным услугам в электронном виде может быть развернута на базе любого оператора мобильной связи. В приложении Б приведен сравнительный список персональных средств аутентификации, поставляемых в Россию.

3 Разработка методических рекомендаций по управлению жизненным циклом ключевого материала инфраструктуры защищенного доступа к государственным и муниципальным сервисам в электронном виде

3.1 Описание схемы жизненного цикла ключевого материала, используемого в сервисах защищенного доступа к государственным и муниципальным сервисам в электронном виде

Жизненный цикл любого ключевого материала состоит из определенного набора состояний и возможных переходов между ними. Схема жизненного цикла ключевого материала представлена на рисунке 23.

С точки зрения управления ключевым материалом весь жизненный цикл можно разбить на три основные фазы:

- **предоперационная фаза** – подготовительный этап, включающий в себя генерацию ключевого материала и подготовку его к использованию. В рамках этой фазы ключевой материал создается, распространяется, но еще не доступен для использования в криптографических операциях;
- **операционная фаза** – этап операционного использования ключевого материала;
- **постоперационная фаза** – этап завершения жизни ключевого материала, который длится от момента прекращения операционного использования ключевого материала до его полного физического уничтожения.

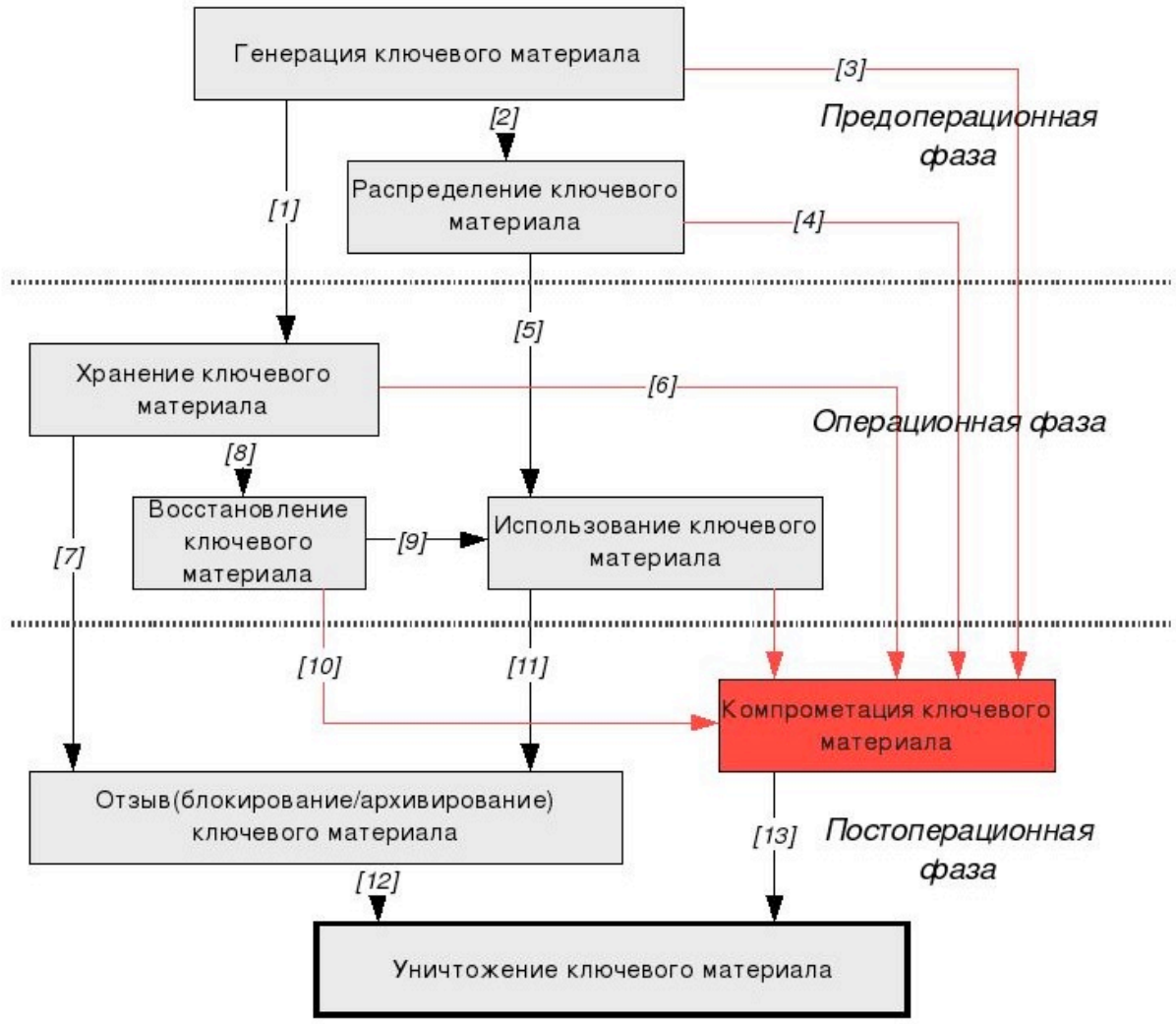

Рисунок 23 — Схема жизненного цикла ключевого материала

Жизненные циклы каждого типа ключевого материала в отдельности.

Ключевой материал сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме.

Ключи для аутентификации и выведения сессионных ключей.

Данный тип ключей предназначен для аутентификации абонента в сети сотовой связи и для выведения сессионных ключей. К таким ключам относятся: ключи, используемые в механизмах аутентификации при доступе к сети связи, а также ключи, используемые при аутентификации в прикладных услугах, предоставляемых оператором связи.

Описание жизненного цикла.

Рассмотрим жизненный цикл этого типа ключевого материала (по рисунку 23):

1) предоперационная фаза:

   • *выработка ключевого материала* осуществляется в рамках персонализационного центра;

   • **переход [2]**: *распределение ключевого материала:* сгенерированный ключевой материал передается в регистры HLR/AuC, а также на заводы в оборудование для производства (U)SIM-карт;

2) операционная фаза:

   • **переход [1]**: *хранение ключевого материала:* резервная копия ключевого материала помещается в БД персонализационного центра;

   • **переход [5]**: *использование ключевого материала:* ключевой материал используется для аутентификации абонента в сети и выведения сессионных ключей;

   • **переход [8] , [9]**: *восстановление ключевого материала:* в случае неудачной доставки ключевого материала, либо при сбое в регистре HLR/AuC ключевой материал может быть восстановлен из БД персонализационного центра и вновь отправлен получателю;

3) постоперационная фаза:

   • **переход [7] , [11]**: *отзыв ключевого материала:* может быть осуществлен по нескольким причинам:

      • продолжительная неактивность абонента;
      • заявление абонента о пропаже (U)SIM-карты;
      • выявление клонов карты в сети;
      • компрометация БД AuC;
      • несовпадение ключей на (U)SIM карте и AuC;

- **переход [12] , [13]**:
  - *уничтожение ключевого материала:* в AuC происходит через некоторое время после отзыва ключевого материала при подтверждении его ненужности, удалить ключевой материал на (U)SIM-карте, в большинстве случаев не представляется возможным;
  - *компрометация ключевого материала;*
- **переход [3] , [6]**: атаки на информационную систему персонализационного центра;
- **переход [4] , [10]**: перехват передаваемых файлов с ключевым материалом, отправка не тому получателю, шифрование не на том транспортном/PGP ключе;
- **переход [14]**: атака на HLR/AuC, атака на (U)SIM-карту, сбой в регистре HLR/AuC или при резервном копировании, нарушение связи ключевого материала с значением IMSI.

Виды компрометации.

На основании описанных выше переходов ключевого материала в скомпрометированное состояние можно составить следующую таблицу 3.

Таблица 3 — Виды компрометации

Этап жизненного цикла	Вид компрометации			
	компрометация конфиденциальности	компрометация целостности	компрометация связи с объектом-владельцем или связанной стороной	компрометация связи с приложением/ областью использования
генерация ключевого материала	x			
хранение ключевого материала	x	x	x	

Продолжение таблицы 3

распределение ключевого материала	x	x	x	x
восстановление ключевого материала	x	x	x	x
использование ключевого материала	x	x	x	

Ключи Security Domains.

Данный тип ключей предназначен для удаленного управления (U)SIM-картой: Remote File Management (RFM), Remote Applet Management (RAM) – удаленному управлению файлами и приложениями на карте. На одной (U)SIM-карте может находиться несколько независимых доменов, ключи для доступа к которым никак не связаны между собой.

Описание жизненного цикла.

Рассмотрим жизненный цикл этого типа ключевого материала (по рисунку 234):

1) предоперационная фаза:
   - *выработка ключевого материала:* осуществляется, как правило, на стороне завода-производителя, но некоторые провайдеры приложений могут сами генерировать такие ключи. Ключи доменов прошиваются непосредственно на (U)SIM-карту и передаются на платформу OTA;
   - **переход [2]**: *распределение ключевого материала:* сгенерированный ключевой материал передается на OTA-платформы, где происходит регистрация (U)SIM-карты;
2) операционная фаза:

- **переход [1]**: *хранение ключевого материала:* резервная копия ключевого материала передается в БД персонализационного центра;
- **переход [5]**: *использование ключевого материала:* ключи доменов используются для удаленного доступа к домену, изменению настроек. Типичными примерами использования могут служить изменение номера sms-центра, добавление новых пунктов меню в STK приложения и т.д.;
- **переход [8] , [9]**: *восстановление ключевого материала:* в случае сбоя на OTA-платформе ключевой материал может быть восстановлен из БД персонализационного центра и вновь отправлен получателю;

3) постоперационная фаза:
   - **переход [7] , [11]**: *отзыв ключевого материала:* не производится;
   - **переход [12] , [13]**:
     - *уничтожение ключевого материала:* происходит при аннулировании (U)SIM-карты одновременно из HLR/AuC, OTA-платформ, платежных систем и др.;
     - *компрометация ключевого материала:*
   - **переход [3]**: компрометация ключевого материала на заводе-производителе крайне маловероятна;
   - **переход [4] , [10]**: перехват передаваемых файлов с ключевым материалом, отправка не тому получателю, шифрование не на том транспортном/PGP ключе;
   - **переход [6]**: атака на информационную систему персонализационного центра;
   - **переход [14]**: атака на (U)SIM-карту маловероятна, атака на OTA-платформу, сбой в ее работе.

На основании описанных выше переходов ключевого материала в скомпрометированное состояние можно составить следующую таблицу 4.

Таблица 4 — Виды компрометации Security Domains

Этап жизненного цикла	Вид компрометации			
	компрометация конфиденциальности	компрометация целостности	компрометация связи с объектом-владельцем или связанной стороной	компрометация связи с приложением/ областью использования
генерация ключевого материала				
хранение ключевого материала	x	x	x	x
распределение ключевого материала	x	x	x	x
восстановление ключевого материала	x	x	x	x
использование ключевого материала	x	x	x	x

Специализированные ключи апплетов\приложений.

Данный тип ключей предназначен для локального доступа к SIM- и (U)SIM-приложениям, находящимся на (U)SIM-карте. К таким ключам относятся: ключи для (U)SIM-приложений, административные ключи, банковские ключи (например, для осуществления электронных платежей).

Описание жизненного цикла.

Рассмотрим жизненный цикл данного типа ключевого материала (по рисунку 23.):

1) предоперационная фаза:

   • *выработка ключевого материала:* осуществляется в рамках персонализационного центра, часть ключей может генерироваться у

сторонних поставщиков или на заводе, в частности ключи банковских приложений;

- **переход [2]**: *распределение ключевого материала:* ключи, сгенерированные сторонними поставщиками, передаются в персонализационный центр и загружаются в его БД, сгенерированный внутри центра ключевой материал передается на заводы-производители в оборудование для производства (U)SIM-карт;

2) операционная фаза:

- **переход [1]**: *хранение ключевого материала:* резервная копия ключевого материала помещается в БД персонализационного центра, за исключением ключей некоторых специализированных приложений (в частности, банковские ключи);
- **переход [5]**: *использование ключевого материала:* ключи данного типа используются для доступа к локальным приложениям, особенности их ипользования зависят от целевого назначения конкретного приложения.
- **переход [8] , [9]**: *восстановление ключевого материала*;

3) постоперационная фаза:

- **переход [7] , [11]**: *отзыв ключевого материала*;
- **переход [12] , [13]**:
  - *уничтожение ключевого материала:* происходит из БД персонализациооного центра, биллинговой системы и других мест хранения при аннулировании (U)SIM-карты, уничтожение ключевого материала непосредственно на (U)SIM-карте не может быть произведено;
  - *компрометация ключевого материала;*
- **переход [3] , [6]**: атака на информационную систему персонализационного центра;

- **переход [4] , [10]**: перехват передаваемых файлов с ключевым материалом, отправка не тому получателю, шифрование не на том транспортном/PGP ключе;
- **переход [14]**: атака на (U)SIM-карту.

Виды компрометации.

На основании описанных выше переходов ключевого материала в скомпрометированное состояние можно составить следующую таблицу 5.

Таблица 5 — Виды компрометации специализированных ключей апплетов\приложений

Этап жизненного цикла	Вид компрометации			
	компрометация конфиденциальности	компрометация целостности	компрометация связи с объектом-владельцем или связанной стороной	компрометация связи с приложением/ областью использования
генерация ключевого материала				
хранение ключевого материала	x	x	x	x
распределение ключевого материала	x	x	x	x
восстановление ключевого материала	x	x	x	x
использование ключевого материала	x	x	x	x

3.2 Рекомендации по обеспечению безопасности жизненного цикла ключевого материала, используемого в сервисах защищенного доступа к государственным и муниципальным сервисам в электронном виде

В данном разделе даются базовые рекомендации по безопасности ключевого материала, используемого в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме, включающие рекомендации по использованию ключей, выбору оптимального периода использования ключевого материала, а также рекомендации по защите ключевого материала в течение его жизненного цикла [15].

Базовые рекомендации.

Каждый ключ должен использоваться только в одной цели (например, шифрование, установление подлинности, обертывание ключа, выработка случайного числа или цифровой подписи). Для этого есть несколько причин.

Во-первых, использование того же самого ключа для двух различных шифровальных процессов может снизить уровень информационной безопасности в одном или обоих процессах.

Во-вторых, ограничение по использованию ключа снижает потенциальный ущерб, который может быть нанесен, если ключ был скомпрометирован.

В-третьих, использование некоторых ключей может влиять друг на друга. Например, если один и тот же ключ используется для обеспечения безопасности транспортировки ключей шифрования данных и выработки цифровой подписи. В этом случае, если время жизни такого ключа в качестве транспортного превышает его время жизни в качестве ключа подписи, могут возникать коллизии в использовании таких ключей.

Принцип однократного использования ключевого материала не противоречит возможности использования одного и того же ключа в случаях, когда один процесс предоставляет несколько прикладных услуг, например,

когда с помощью цифровой подписи обеспечиваются одновременно неотказуемость операции, её целостность и аутентификация субъекта, или в случае когда ключ для симметричного шифрования используется для аутентификации отправителя данных и расшифрования этих данных в одной операции.

Периоды использования ключевого материала.

Период использования ключевого материала – отрезок времени, в течение которого ключ считается действующим и может быть использован в процессах, для которых использование этого ключа определено. В соответствии с этим период использования ключа:

- ограничивает объем информации, связанной с ключевым материалом, тем самым уменьшает потенциальный объем информации, который злоумышленник может использовать для криптоанализа, с целью определения ключа;
- ограничивает объем данных, которые становятся доступны злоумышленнику в случае компрометации ключевого материала;
- ограничивает использование конкретного криптографического алгоритма вплоть до оптимального;
- ограничивает время, которое злоумышленник может потратить на всевозможные типы атак с целью раскрытия ключевого материала;
- ограничивает время, в течение которого информация, защищаемая конкретным ключом, может быть раскрыта;

В некоторых случаях период использования ключевого материала определяется как число транзакций, которые могут быть совершены с использованием данного ключевого материала.

Факторы риска, влияющие на выбор периода использования ключевого материала.

Среди факторов риска, влияющих на выбор периода использования для конкретного ключа, выделяют следующие:

- стойкость криптографических алгоритмов, использующих ключевой материал;
- реализации криптографического алгоритма (программная, аппаратная, класс СКЗИ и т.п.);
- объем данных, который обрабатывается с помощью данного ключа, или количество транзакций;
- тип использования ключевого материала (шифрование данных, цифровая подпись, выработка ключей, защита другого ключевого материала и т.п.);
- тип доступа к ключевому материалу (использование токенов, ручного ввода ключей, аппаратных модулей безопасности);
- процедура обновления ключевого материала;
- количество копий ключа и количество сущностей, их использующее;
- модель угроз для защищаемой с помощью ключа информации.

Ключевой момент – более короткие периоды использования ключевого материала повышают уровень информационной безопасности в целом. С другой стороны, при смене ключей возникают угрозы их компрометации, связанные с транспортировкой и человеческим фактором, поэтому в некоторых случаях целесообразно выбирать более длинные периоды использования ключевого материала, с возможностью обеспечивать более надежную его защиту.

Рекомендации по обеспечению информационной безопасности ключевого материала.

Ключевой материал должен быть доступен прикладным сервисам в течение всего своего жизненного цикла. При этом для обеспечения безопасности ключевого материала рекомендуется использование специализированных технических средств, таких как криптографические токены, смарт-карты, аппаратные модули безопасности.

К ключевому материалу могут быть применены следующие меры по обеспечению информационной безопасности:

- защита целостности;
- защита конфиденциальности;
- корректность использования;
- корректность владения;
- временной интервал обеспечения защиты ключевого материала.

Защита целостности должна обеспечиваться для всех типов ключевого материала. Защита целостности подразумевает проверку источника получения и формата в котором получен ключевой материал. Защита целостности может обеспечиваться за счет использования криптографических механизмов (вычисление контрольных сумм, хеш-сумм, электронных подписей, кодов подтверждения сообщений) или не криптографических механизмов (вычисление CRC), либо за счет использования аппаратных средств защиты ключевого материала.

Защита конфиденциальности. Конфиденциальность ключевого материала достигается за счет использования специализированных технических средств (токены, смарт-карты, аппаратные модули безопасности), либо с применением средств шифрования или обертывания ключей, возможно использование мер административного характера по ограничению доступа к ключевому материалу.

Корректность использования. Под данным термином понимается, что ключевой материал должен использоваться только строго определенными приложениями и для обработки строго определенных типов данных.

Корректность владения. Определяет, там, где это возможно, отношение ключевого материала к владельцу.

Временной интервал обеспечения защиты ключевого материала – интервал времени, на протяжении которого должна обеспечиваться защита ключевого материала.

В таблице 6 приводится сводная информация по рекомендациям по защите ключевого материала в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме.

Таблица 6 — Сводная информация по рекомендациям по защите ключевого материала

Тип ключевого материала	**Для обеспечения какого типа ИБ используется ключевой материал**	**Тип защиты ключевого материала**	**С какими сущностями должен быть связан ключевой материал в течение жизненного цикла**	**Необходимый тип проверки ключевого материала**	**Временной интервал обеспечения защиты ключевого материала**
Закрытый ключ электронной подписи	Аутентификация, целостность, неотказуемость	Целостность, конфиденциальность	Пользователь, приложение, параметры пользовательского окружения, открытый ключ проверки электронной подписи	Проверка владения ключом	С момента генерации до момента окончания периода действия ключа
Симметричные ключи для шифрования и расшифрования	Конфиденциальность	Целостность, конфиденциальность, защищенное хранение	Пользователь, приложение, зашифрованные данные и расшифрованные данные		С момента генерации и до окончания жизненного цикла либо периода использования ключа
Открыты й ключ проверки электронной подписи	Аутентификация, целостность, неотказуемость	Целостность, защищенное хранение	Пользователь, приложение, владелец ключевой пары, параметры пользовательского окружения, закрытый ключ электронной подписи, подписанная информация	Проверка формата	С момента генерации до момента, когда не будет данных, которые подлежат проверке данным ключом

Продолжение таблицы 6

Симметричные мастер-ключи	Вспомогательные функции	Целостность, конфиденциальность, защищенное хранение	Пользователь, приложение, зашифрованные данные и расшифрованные данные		С момента генерации и до окончания жизненного цикла либо периода использования ключа
Параметры пользовательского окружения	Зависит от того, какие ключи связаны с этими параметрами	Защищенное хранение, целостность	Пользователь, приложение, открытые и закрытые ключи	Проверка формата	С момента генерации до момента, когда они более не нужны для генерации ключей и проверки подписей
Инициализирующие векторы	Зависит от алгоритма	Защищенное хранение, целостность	Защищаемая информация		С момента генерации и до момента, когда они более не требуются для обработки данных
Разделяемые секреты	Вспомогательные функции	Конфиденциальность, целостность			С момента генерации и до окончания транзакции.

Механизмы обеспечения безопасности ключевого материала.

Обеспечение безопасности ключевого материала в некоторых случаях заложено непосредственно в протоколах его использования, в некоторых случаях обеспечивается за счет технических средств и организационных мероприятий. В данном параграфе приводится описание механизмов обеспечения безопасности ключевого материала сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме.

Доступность.

Поскольку каналы связи, по которым передается ключевой материал, могут подвергнуться атаке, либо просто перестать быть доступными, задача по обеспечению доступности ключевого материала в первую очередь сводится к

обеспечению избыточности каналов связи и способов доступа к ключевому материалу, а также вводу в действия систем коррекции ошибок при передаче данных и других им подобных не криптографических механизмов.

Целостность.

Контроль целостности позволяет предотвратить и определить изменения ключевого материала. В случае выявления изменения ключевого материала, необходимо принять меры по его восстановлению. Для контроля целостности часто используются криптографические методы. Контроль целостности ключевого материала при его передаче должен производиться с помощью одного или нескольких следующих методов:

- с помощью одного из возможных механизмов, оперирующих контрольной суммой – код подтверждения сообщения, хеш-функция, цифровая подпись;
- с помощью механизмов протокола передачи данных, используемого при транспортировке ключевого материала, включающего средства контроля целостности.

В случае обнаружения изменений в ключевом материале необходимо принять меры реагирования:

- поврежденный ключевой материал не должен быть использован;
- может потребоваться повторная передача ключевого материала;
- информация о произошедшем инциденте должна быть сохранена и проанализирована.

Целостность.

Обеспечение целостности ключевого материала достигается главным образом за счет использования следующих методов:

- шифрование ключевого материала;

- разделение ключевого материала на несколько частей, каждая из которых может быть доступна только по отдельности (одному лицу или процедуре);
- использование специальных технических средств или организационных мер.

Корректность использования ключевого материала.

Корректность использования ключевого материала достигается за счет разграничения доступа к ключевому материалу на уровне пользователя и приложений с использованием административных и технических мероприятий.

4 Разработка рекомендаций по нормативному правовому обеспечению процесса взаимодействия сервисов защищенного доступа с инфраструктурой государственных и муниципальных сервисов

Существует большое количество систем и средств обеспечивающих необходимый уровень защиты от НСД. Имеется хорошая практика разработки, внедрения и использования таких систем как в России, так и за рубежом [16, 17]. Но при рассмотрении проблемы на государственном уровне возникают определенные проблемы, связанные со сложностью распределенных информационных систем. Для решения задачи корректного взаимодействия сервисов защищенного доступа с инфраструктурой государственных и муниципальных сервисов, основываясь на мировом опыте, можно сделать вывод о необходимости выработки единой, стандартизированной системы.

Такой стандарт должен содержать комплексную информацию по конкретной задаче. Он должен описывать как общие вопросы построения и функционирования систем защищенного доступа, так и вопросы реализации конкретных подсистем.

Необходимо описать цели, которые мы хотим достичь, например:

- обеспечить, чтобы подходы к электронной аутентификации личности выдерживали баланс ***основных рисков,*** связанных с необходимостью их использования и удобством ***использования*** в интересах обеих сторон;
- повысить ***общественное доверие*** при электронном общении с государственными учреждениями;
- обеспечить ***согласованность в правительственных процессах*** для электронной аутентификации личности в целях повышения эффективности и максимального удобства в использовании для всех вовлеченных сторон;

- обеспечить государственные учреждения ***механизмами, чтобы определить наиболее подходящий подход*** к электронной аутентификации личности.

Должны быть описаны основные принципы построения и использования сервисов и систем, например:

- обеспечить прозрачность для всех сторон;
- принять стандартный подход к управлению рисками;
- стремиться к согласованности между государственными учреждениями;
- выдерживать баланс доверия, безопасности и простоты использования;
- выбранные решения являются как экономически эффективными, так и удобными.

Также должна быть построена модель угроз для предлагаемых сервисов и даны описания этим угрозам, например:

- отказ в обслуживании (Denial of Service). Данный класс атак направлен на нарушение доступности Web-сервера;
- предсказуемое расположение ресурсов (Predictable Resource Location). Позволяет злоумышленнику получить доступ к скрытым данным или функциональным возможностям. Путем подбора злоумышленник может получить доступ к содержимому, не предназначенному для публичного просмотра;
- недостаточная аутентификация (Insufficient Authentication). Эта уязвимость возникает, когда Web-сервер позволяет атакующему получать доступ к важной информации или функциям сервера без должной аутентификации;

- обратный путь в директориях (Path Traversal). Данная техника атак направлена на получение доступа к файлам, директориям и командам, находящимся вне основной директории Web-сервера;
- утечка информации (Information Leakage). Эти уязвимости возникают в ситуациях, когда сервер публикует важную информацию, например комментарии разработчиков или сообщения об ошибках, которая может быть использована для компрометации системы. Часто разработчики оставляют комментарии в HTML страницах и коде сценариев для облегчения поиска ошибок и поддержки приложения;
- внедрение операторов SQL (SQL Injection). Эти атаки направлены на Web-серверы, создающие SQL запросы к серверам СУБД на основе данных, вводимых пользователем;
- переполнение буфера (Buffer Overflow). Эксплуатация переполнения буфера позволяет злоумышленнику изменить путь исполнения программы путем перезаписи данных в памяти системы;
- подмена содержимого (Content Spoofing). Используя эту технику, злоумышленник заставляет пользователя поверить, что страницы сгенерированны Web-сервером, а не переданы из внешнего источника;
- недостаточная авторизация (Insufficient Authorization). Возникает, когда Web-сервер позволяет атакующему получать доступ к важной информации или функциям, доступ к которым должен быть ограничен;
- отсутствие таймаута сессии (Insufficient Session Expiration). В случае если для идентификатора сессии или учетных данных не предусмотрен таймаут или его значение слишком велико, злоумышленник может воспользоваться старыми данными для авторизации.

С учетом модели угроз должна быть построена модель нарушителя, определены уровни защищенности для разных групп сервисов и описаны механизмы защиты, соответствующие тому или иному уровню защищенности.

4.1 Регламент взаимодействия прикладных сервисов с инфраструктурой защищенного доступа к государственным и муниципальным сервисам в электронном виде

При рассмотрении вопроса взаимодействия прикладных сервисов с инфраструктурой защищенного доступа к государственным и муниципальным сервисам можно упростить схему работ до вопроса взаимодействия веб-сервисов. Данный подход помогает сфокусироваться на решении конкретной задачи, а также воспользоваться уже имеющимися наработками по этому направлению [18].

Аутентификация необходима для ограничения доступа к ресурсам, для выявления участников транзакций и для создания персонализации информации на основе идентификации. В современных системах крайне важны средства для поддержки единого входа: они подтверждают, что аутентификация была выполнена успешно, что позволяет пользователям аутентифицироваться с одной системой и использовать другие сервисы и приложения.

Межсервисная проверка подлинности может выполняться с помощью различных методов: от токенов на основе HTTP, до аутентификации с использованием SSL / TLS-сертификатов. Методы, основанные как HTTP, так и на SSL / TLS, выполняются под слоем сообщение SOAP и прозрачны для работающих веб-служб, в то время как протоколы токенов на основе SOAP требуют взаимодействия между веб-службами. Аутентификация веб-сервисов обычно выполняется с помощью стандарта OASIS WS-Security, который поддерживает маркеры на основе различных стандартов аутентификации: имен пользователей, X.509 PKI сертификатов, тикетов Kerberos или SAML подтверждений. Библиотеки WS-Security доступны для большинства широко используемых платформ разработки веб-сервисов Java и .NET .

Когда провайдер сервиса пытается получить доступ к удаленной веб-службе от имени пользователя, она должна отправить метку аутентификации в

сообщение WS-Security. Эти маркеры передают информацию, что инициатор (например, пользователь или запрашивающая сторона) был аутентифицирован и предоставляют информацию об объекте, например, механизм аутентификации, время и, возможно, атрибуты, которые могут быть применимы. Часто эти знаки принимают форму подтверждений SAML.

Иногда системная служба может быть не в состоянии выполнять действия, которые пользователь или запрашивающая сторона хочет чтобы он выполнял, но он знает удаленный веб-сервис, который может это сделать. Системная служба может ссылаться на другой удаленный сервис для удовлетворения запроса запрашивающей стороны, что известно как связывание сервисов. Системная служба может использовать подтверждение SAML, сообщение WS-Security или оба, чтобы гарантировать, что веб-сервисы доверяют друг другу.

Существуют два различных подхода к связыванию сервисов. Веб-сервис может получить доступ к удаленному веб-сервису или от своего имени или от имени инициатора запроса. В первом случае две веб-службы будут общаться друг с другом как обычно. Во втором случае удаленная веб-служба должна быть обеспечена идентичностью отправителя. Это может быть удовлетворено с использованием WS-Security и SAML. Есть два способа передать личность отправителя на удаленный сервис. Во-первых, если веб-служба получила SAML подтверждение с запросом инициатора, то утверждение SAML может быть передано удаленной веб-службе. Для запрашивающего сервиса может оказаться необходимым подписать либо подтверждение SAML или сообщение SOAP так, чтобы его собственная идентификация также передавалась удаленной службе.

Другой вариант для запрашивающего сервиса — сгенерировать и подписать SAML подтверждение для инициатора запроса и передать SAML подтверждение на удаленный веб-сервис. В такой конфигурации не представляется возможным для удаленного веб-сервиса определить, кто

изначально совершил запрос. Это ограничение может послужить помехой в цепочке доверия, так как цепочка ограничена последним запросом. В отличие от этого, если в SAML подтверждение инициатора используется или подписано, можно проследить запрос назад до инициатора запроса путем пересылки подтверждения SAML на удаленную веб-службу – запрашивающий сервис в состоянии подтвердить, личность инициатора запроса. Если проверка информации об аутентификации требует конфиденциальности, то должны быть использованы SSL / TLS шифрование или функциональность WS-Security.

К использованию подписанных SAML подтвержений аутентификации или авторизации следует подходить с осторожностью. Подписанное подтверждение SAML является меткой, которая может быть использована злоумышленником или вредоносным сервисом. Следует соблюдать осторожность, чтобы гарантировать, что используются временные метки и ограниченные сроки действия. Для решения этой проблемы SAML подтверждения могут быть связаны криптографически с отдельными сообщениями SOAP при помощи подписи родительского тега подтверждения SAML (например, с использованием WS-Security подписать элемент безопасности, а не содержащийся в нем SAML маркер). Хотя подтверждение SAML может быть повторно использовано, оно будет считаться недействительным, если вся подписанная часть сообщения также не будет использоваться повторно, что облегчает для поставщиков задачу обнаружение атак повтора (replay attack).

4.2 Методические рекомендации по интеграции прикладных сервисов с инфраструктурой защищенного доступа к государственным и муниципальным сервисам в электронном виде

Методология.

При проведении процедуры аутентификации могут использоваться различные методы, обеспечивающие определенный уровень доверия.

Достижение необходимого уровня доверия для системы электронной аутентификации – это функция зависимости стойкости процессов регистрации и приема, с одной стороны, и стойкости учетных данных пользователя электронной аутентификации (например, идентификатор пользователя + пароль, биометрический идентификатор) и их управления, с другой. На рисунке 24 показан достижимый уровень доверия.

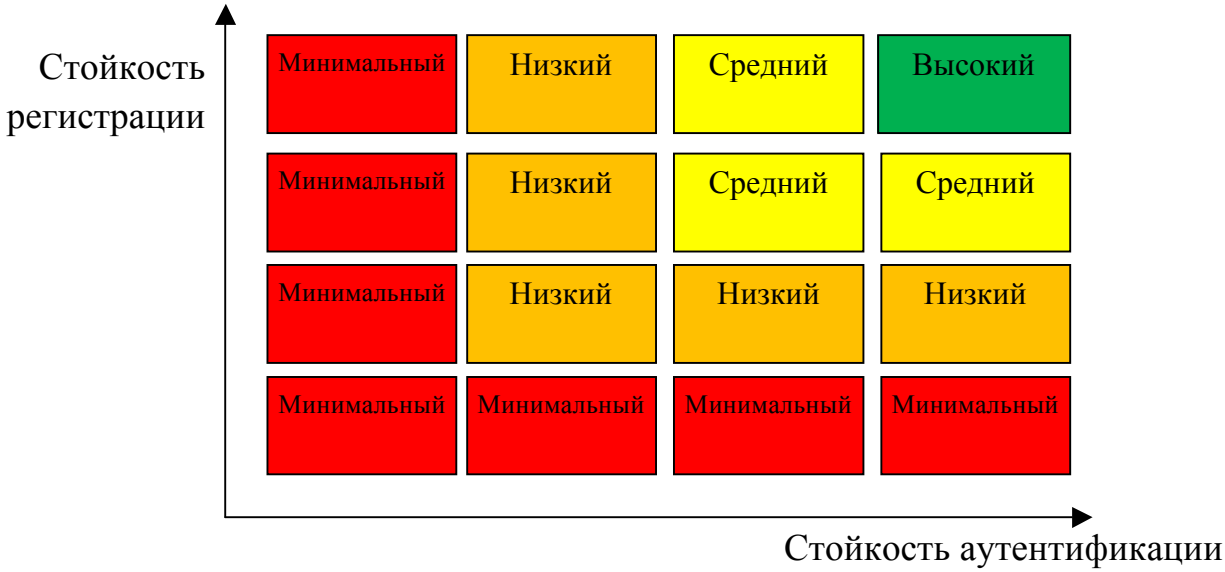

Рисунок 24 — Распределение уровней доверия

Должны быть определены этапы процесса оценки стойкости аутентификации, требуемые проводимой операцией, технологическими компонентами, которые обеспечат желаемую стойкость аутентификации, и бизнес-процессами, необходимыми для достижения этого уровня аутентификации.

Примеры этапов могут быть следующими:

- определить требования электронных услуг, которые должны быть предоставлены, характер базы пользователей, желаемый электронный канал доставки, а также конкретные сервисы, которые должны проходить проверку подлинности;
- определить требования уровня доверия путем проведения всестороннего анализа угроз и рисков, связанных с транзакцией;

- определить наиболее подходящие средства для регистрации клиента услуг, включая сбор и/или проверку личности или другой информации;
- выбрать механизм аутентификации конечных пользователей и процессов, которые должны быть применены для обеспечения конфиденциальности, целостности и надежности на протяжении всего жизненного цикла;
- определить наиболее подходящую модель реализации электронной аутентификации, включая оценку повторного использования существующих систем и процессов;
- оценить экономическую обоснованность и целесообразность реализации модели.

Только технических решений, как правило, не достаточно, чтобы удовлетворить практические требования электронной аутентификации. Электронная аутентификация также включает в себя управление, бизнес-процессы и культурные вопросы. Любое решение электронной аутентификации должно опираться на процедуры, которые четко определяют обязанности отдельных лиц, проводящих онлайн-транзакций.

Роли и обязанности.

В общем стандарте должны быть определены роли и обязанности всех взаимодействующих сторон. Диапазон вопросов, которым должны уделять должное внимание поставщики услуг, будет содержать целый ряд аспектов, в том числе:

- учет потребностей и ожиданий физических и юридических лиц;
- предоставление соответствующего уровня осведомленности конечных пользователей по услугам;
- обеспечение лидерства в области практики электронной аутентификации;
- предоставление эффективных и полезных онлайн-сервисов;

- обеспечение повышающейся надежности и качества услуг.

Что касается учета прав и обязательств юридических и физических лиц, взаимодействующих с онлайн сервисами, то они, как правило, изложены в пользовательском соглашении поставщику услуг и также будут включать:

- предоставление достоверного удостоверения личности;
- поддержание безопасности учетных данных, которые им выдаются;
- использование учетных данных только в целях, для которых они выданы.

5 Заключение о технической возможности создания инфраструктуры защищенного доступа к государственным и муниципальным сервисам в электронном виде на базе сервисов и ресурсов информационно-телекоммуникационных сетей

Задача предоставления гражданам и организациям защищенного доступа к государственным и муниципальным услугам в электронной форме обозначена как одна из наиболее приоритетных в развитии страны, что утверждено в распоряжении правительства Российской Федерации от 20 октября 2010 г. N 1815-р «О ГОСУДАРСТВЕННОЙ ПРОГРАММЕ РОССИЙСКОЙ ФЕДЕРАЦИИ «ИНФОРМАЦИОННОЕ ОБЩЕСТВО (2011 - 2020 ГОДЫ)»«.

В соответствии с целевыми показателями данной программы к 2015 году 100% государственных услуг должны предоставляться в электронной форме.

В этой связи, жизненно важным вопросом для выполнения программы «Информационное общество» является возможность обеспечения граждан и организаций высоконадежными, удобными и недорогими средствами идентификации и аутентификации для доступа к государственным и муниципальным услугам в электронной форме. Вместе с распространением средств аутентификации и идентификации для государственных и муниципальных услуг в электронной форме, возникает задача по созданию сопутствующей инфраструктуры для этих средств, включающей сервисы аутентификации, инфраструктуру профилирования средств аутентификации, сеть логистики для распространения средств аутентификации, а также средства управления.

На сегодняшний день представлено несколько средств, которые можно использовать для аутентификации при доступе к государственным и муниципальным услугам в электронной форме:

- аутентификация на базе логина и пароля, в качестве логина используется СНИЛС;
- аутентификация с использованием USB-токена на базе инфраструктуры открытых ключей;
- аутентификация с использованием УЭК.

Представленные средства аутентификации имеют ряд существенных ограничений по своему использованию и не все из них применимы с наиболее современными средствами доступа к государственным и муниципальным услугам в электронной форме – мобильными телефонами, планшетными компьютерами и ноутбуками.

Наиболее универсальной является схема аутентификации с использованием СНИЛС и пароля – она инварианта к средствам доступа и может быть использована в т.ч. в мобильных устройствах, обеспечивает мобильность самого пользователя за счет отсутствия физического носителя, который необходимо подключать при аутентификации, необходимая инфраструктура по выпуску пользовательских идентификаторов и их адресной доставке уже существует и она является относительно недорогой. Однако существенным недостатком данной схемы аутентификации при доступе к государственным и муниципальным услугам в электронной форме является её сравнительно низкий уровень информационной безопасности, по сравнению с другими схемами доступа (PKI-токен, УЭК). При усилении схемы аутентификации с использованием СНИЛС и пароля за счет дополнительных факторов, например за счет использования токена, генерирующего одноразовые пароли для доступа, указанный недостаток может быть устранен.

Схема с использованием USB-токенов на базе инфраструктуры открытых ключей для доступа к государственным и муниципальным услугам в

электронной форме, содержит в себе наибольшее количество технологических ограничений, существенным образом сужающих сферу её возможного применения. В первую очередь это касается того, что USB-токен на открытых ключах может быть использован только для доступа к ЕПГУ. Также для его использования потребуется установка СПО, которое существует и корректно работает не под все программные платформы для персональных компьютеров, использование же USB-токена на открытых ключах с мобильными устройствами вобще не представляется возможным. Стоимость такого токена составляет порядка 600 рублей. Помимо этого инфраструктура по выпуску, персонализации и распространению таких токенов весьма громоздка и затратна в плане поддержки, её создание необходимо в полной мере финансировать из источников программы «Информационное общество».

Универсальная электронная карта (УЭК) призвана устранить недостатки первых двух средств аутентификации для государственных и муниципальных услуг в электронной форме, однако и она обладает рядом ограничений. Главным образом это касается необходимости наличия считывателя для УЭК – специального устройства для информационного обмена с картой. Использование УЭК оптимально совместно со специализированными терминалами для доступа к государственным и муниципальным услугам в электронной форме, для использования же с персональными средствами доступа, необходимо приобретать считыватель и СПО отдельно. Несомненным достоинством УЭК является то, что вся инфраструктура по выпуску и управлению картами вынесена за пределы инфраструктуры электронного правительства и возложена на операторов УЭК – банковское сообщество.

В качестве наиболее универсального решения, компенсирующего недостатки всех существующих средств аутентификации для государственных и муниципальных услуг в электронной форме, сочетаюшего все их достоинства прдлагается схема, которая:

- расширяет схему аутентификации с использованием СНИЛС и пароля за счет использования дополнительного фактора сильной аутентификации на базе одноразовых паролей;
- для защиты ключевого материала, используемого при аутентификации использует технологию смарт-карт, аналогичную УЭК;
- форм-фактор и техническое исполнение средства аутентификации позволяет использовать его совместно с мобильными устройствами;
- предлагает готовую инфраструктуру по персонализации атрибутов доступа и профилей пользователя;
- позволяет реализовать механизмы квалифицированной электронной подписи с помощью технических средств и инфраструктуры сервиса аутентификации, использующего данное средство аутентификации;
- позволяет охватить наиболее широкие слои населения Российской Федерации без необходимости существенного финансирования со стороны программы «Информационное общество».

В качестве такого средства аутентификации предлагается использовать СНИЛС с паролем, дополнительно с (U)SIM-картой оператора мобильной связи, на которую записано специализированное приложение, генерирующее одноразовые пароли для доступа к государственным и муниципальным услугам в электронной форме. (U)SIM-карта является полноценной смарт-картой, технологически эквивалентной УЭК, а мобильный телефон, который на сегодняшний день есть в пользовании практически у каждого, выполняет в данной схеме роль считывателя смарт-карты. Вынесение приложения, генерирующего одноразовые пароли для доступа к государственным и муниципальным услугам, на (U)SIM-карту не только позволяет обеспечить его информационную безопасность, но и делает возможным его использование совместно с любым мобильным терминалом, представленным на рынке, вне зависимости от модели и производителя.

При этом операторы связи обладают всеми необходимыми ресурсами для создания сервиса защищенного доступа к государственным и муницпальным услугам в электронной форме, вынесенного за периметр инфраструктуры электронного правительства, позволяющего легко масштабировать пользовательский доступ к государственным и муниципальным услугам в электронной форме. Среди указанных ресурсов:

- прототип сервиса аутентификации с использованием приложения на (U)SIM-карте, генерирующего одноразовые пароли с использованием алгоритма ГОСТ Р 34.11-94;
- (U)SIM-карты и инфраструктура для их производства и персонализации, позволяющую доверенным образом загружать на карты при производстве ключи, приложения, сертификаты;
- удостоверящий центр, позволяющий выпускать сертификаты открытого ключа электронной подписи;
- центры регистрации пользователей;
- инфраструктуру продаж и логистики (U)SIM-карт, позволяющую распространять абонентские комплекты и сертификаты открытого ключа электронной подписи, с целью выполнения требований федерального закона Российской Федерации от 6 апреля 2011 г. N 63-ФЗ «Об электронной подписи», для предоставления гражданам квалифицированной электронной подписи в режиме её удаленного использования.

Наличие операторов связи необходимых ресурсов создает все предпосылки к реализации сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме в соответствии с архитектурой и требованиями, изложенными в данной работе. При этом роль государства в рамках создания сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме сводится к инициации работы по указанной тематике, а также вводу в действие нормативной базы, определяющей статус сервиса защищенного доступа к государственным и

муницпальным услугам в электронной форме, роль операторов связи в предоставлении услуг по защищенному доступу к сервисам электронного правительства, а также услуг электронной подписи для граждан при обеспечении юридически-значимого взаимодействия с государственными органами и ведомствами.

На основании проведенных исследований и работ, проводимых самими операторами связи можно сделать заключение о том, что:

- существуют все необходимые предпосылки для создания пилотных зон по предоставлению защищенного доступа к государственным и муниципальным услугам в электронной форме на базе сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме, использующего ресурсы операторов информационно-коммуникационных сетей;
- потенциально возможно обеспечение граждан Российской Федерации средствами квалифицированной электронной подписи, используемой в удаленном режиме на базе сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме;
- необходимо провести научно-исследовательскую работу по разработке предложений по формированию инфраструктуры квалифицированной электронной подписи на базе сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме;
- необходимо разработать предложения по приданию сервису защищенного доступа к государственным и муниципальным услугам юридического статуса, а также разработать соответствующее нормативно-правовое обеспечение.

Заключение

В рамках научно-исследовательской работы «Разработка предложений по созданию системы персональной идентификации граждан в целях безопасного доступа к государственным и муниципальным сервисам в электронном виде» была поставлена цель по разработке технических и методических рекомендаций по созданию универсального сервиса аутентификации и идентификации при предоставлении для граждан государственных и муниципальных услуг в электронном виде на базе технологических возможностей и ресурсов информационно-коммуникационных сетей.

В рамках НИР была проведена экспертиза текущего уровня информационной безопасности инфраструктуры доступа к государственным и муниципальным сервисам в электронном виде, в результате которой:

- было произведено описание и сравнение существующих подходов к аутентификации, используемых для доступа к государственным и муниципальным услуггам в электронном виде: схемы аутентификации на базе СНИЛС и пароля, с использованием USB-токена на базе инфраструктуры открытых открытых ключей, прототипа УЭК;
- произведен анализ существующих схем аутентификации на предмет возможности использования в них отечественных криптографических стандартов.

Проведенная экспертиза показала, что:

- существующие средства аутентификации, используемые для доступа к государственным и муниципальным услугам в электронной форме, не в полной мере обеспечивают мобильность пользователей государственных и муниципальных услуг в электронной форме;
- средства аутентификации, обладающие более высоким уровнем информационной безопасности, несовместимы для использования с

перспективными способами доступа к государственным и муниципальным услугам в электронной форме таким, как мобильные телефоны или планшетные компьютеры;

- универсальная схема аутентификации с использованием СНИЛС и пароля, должна быть усилена дополнительным фактором строгой аутентификации, инвариантным к среде использования;
- при внедрении средств электронной подписи для нужд государственных и муниципальных услуг в электронной форме, необходимо ориентироваться в первую очередь на средства электронной подписи, используемые в удаленном режиме на стороне сервера, для обеспечения максимальной мобильности граждан, а также наиболее широкого охвата населения Российской Федерации средствами электронной подписи.

Для устранения выявленных в результате экспертизы недостатков схем аутентификации, используемых для доступа к государственным и муниципальным услугам в электронной форме, разработана архитектура универсального сервиса аутентификации для государственных и муниципальных услуг в электронной форме на базе ресурсов оператора связи. Основными положениями работы сервиса аутентификации граждан являются:

- использование двухфакторной аутентификации, где в качестве первого фактора выступает комбинация из персонального идентификатора гражданина СНИЛС и пароль, а в качестве второго фактора одноразовый пароль;
- одноразовый пароль генерируется на защищенном носителе – (U)SIM-карте оператора связи – с помощью специализированного приложения;
- мобильный телефон гражданина используется как считыватель для (U)SIM-карты;
- генерация одноразового пароля производится с использованием алгоритма ГОСТ Р 34.11-94;

- инфраструктура персонализации и логистики (U)SIM-карт оператора связи задействована для выполнения требований законодательства и доверенного профилирования средств аутентификации для государственных и муниципальных услуг в электронной форме.

Для универсального сервиса идентификации граждан для безопасного доступа к государственным и муниципальным услугам в электронной форме разработаны:

- технические требования к процедурам идентификации и аутентификации, а также использованию отечественных криптографических алгоритмов в процедурах идентификации и аутентификации;
- разработаны рекомендации по персонализации и профилированию персональных атрибутов доступа к государственным и муниципальным услугам в электронной форме, а также разработана схема персонализации атрибутов доступа;
- разработаны методические рекомендации по обеспечению безопасности ключевого материала, используемого в сервисе защищенного доступа к государственным и муниципальным услугам в электронной форме, а также регламент и методические рекомендации по интеграции прикладных услуг с сервисом аутентификации к государственным и муниципальным услугам в электронной форме.

По результатам работы сформулировано заключение о наличии у операторов связи необходимых ресурсов для реализации сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме в соответствии с архитектурой и требованиями, изложенными в данной работе. При этом роль государства в рамках создания сервиса защищенного доступа к государственным и муниципальным услугам в электронной форме сводится к инициации работы по указанной тематике, а также вводу в действие нормативной базы, определяющей статус сервиса защищенного доступа к государственным и муницпальным услугам в электронной форме, роль

операторов связи в предоставлении услуг по защищенному доступу к сервисам электронного правительства, а также услуг электронной подписи для граждан при обеспечении юридически-значимого взаимодействия с государственными органами и ведомствами.

По результатам НИР в рамках дальнейшего развития тематики аутентификации и обеспечения информационно безопасности в государственных и муниципальных услугах в электронной форме предлагается:

1) исследовать вопросы нормативно-правового регулирования сервиса персональной идентификации граждан в целях безопасного доступа к государственным и муниципальным сервисам в электронном виде и разработать предложения по созданию и совершенствованию соответствующих нормативно-правовых актов;

2) разработать проект нормативно-правового акта, устанавливающего юридический статус сервиса персональной идентификации граждан в целях безопасного доступа к государственным и муниципальным сервисам в электронном виде;

3) разработать предложения по совершенствованию нормативно-правовых актов, регламентирующих использование средств аутентификации и идентификации, используемых для доступа к государственным и муниципальным услугам в электронном виде;

4) разработать стандарт, определяющий технические требования к средствам аутентификации, используемым для дооступа к государственным и муниципальным услугам в электронной форме;

5) разработать механизмы аудита информационной безопаности государственных и муниципальных услуг в электронной форме;

6) инициировать создание опытных зон по развертыванию сервиса персональной идентификации граждан в целях безопасного доступа к государственным и муниципальным сервисам в электронном виде.

Список использованных источников

1) КОНЦЕПЦИЯ ИННОВАЦИОННОГО РАЗВИТИЯ ОТРАСЛИ ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ // ФГУП «Научно-исследовательский институт радио» — Проект

2) ГОСУДАРСТВЕННАЯ ПРОГРАММА РОССИЙСКОЙ ФЕДЕРАЦИИ «ИНФОРМАЦИОННОЕ ОБЩЕСТВО (2011 - 2020 ГОДЫ)» // ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ — РАСПОРЯЖЕНИЕ от 20 октября 2010 г. N 1815-р

3) СИСТЕМНЫЙ ПРОЕКТ ФОРМИРОВАНИЯ В РОССИЙСКОЙ ФЕДЕРАЦИИ ИНФРАСТРУКТУРЫ ЭЛЕКТРОННОГО ПРАВИТЕЛЬСТВА // Министерство связи и массовых коммуникаций Российской Федерации

4) Australian Government e-Authentication Framework – better practice guide to authorisation and access management [Электронный ресурс]: — Режим доступа к ресурсу: http://www.finance.gov.au/publications/agaf-for-business/better-practice/docs/better_practice_guide.pdf

5) NATIONAL STRATEGY FOR TRUSTED IDENTITIES IN CYBERSPACE [Электронный ресурс]: — Режим доступа к ресурсу: http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

6) Digitizing Public Services in Europe: Putting ambition into action [Электронный ресурс]: — Режим доступа к ресурсу: http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/eGovernment_Benchmarking_Method_paper_2010.pdf

7) О ТЕХНИЧЕСКИХ ТРЕБОВАНИЯХ К УНИВЕРСАЛЬНОЙ ЭЛЕКТРОННОЙ КАРТЕ И ФЕДЕРАЛЬНЫМ ЭЛЕКТРОННЫМ ПРИЛОЖЕНИЯМ // ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ — ПОСТАНОВЛЕНИЕ от 24 марта 2011 г. N 208

8) Authentication and Mobile EID for the Public Sector in Moldova [Электронный ресурс]: — Режим доступа к ресурсу: http://egov.md/upload/CN-mobile-eID-eGC-June-2011.pdf

9) One-Time Password Specifications [Электронный ресурс]: RSA Laboratories — Режим доступа к ресурсу: http://www.rsa.com/rsalabs/node.asp?id=2816

10) RFC 4226 «HOTP Algorithm» [Электронный ресурс]: — Режим доступа к ресурсу: http://tools.ietf.org/html/rfc4226

11) RFC 4758 Cryptographic Token Key Initialization Protocol (CT-KIP) Version 1.0 Revision 1 [Электронный ресурс]: — Режим доступа к ресурсу: http://tools.ietf.org/html/rfc4758

12) Trust Framework Provider Adoption Process (TFPAP) For Levels of Assurance 1, 2, and Non-PKI 3 [Электронный ресурс]: — Режим доступа к ресурсу: http://www.idmanagement.gov/documents/TrustFrameworkProviderAdoptionProcess.pdf

13) Amardeo Sarma Virtual Identity Framework for Telecom Infrastructures, Alfredo Matos João Girão Rui L. Aguiar // Wireless Pers Commun (2008) 45:521–543

14) Recommendation ITU-T X.mob-id [Электронный ресурс]: — Режим доступа к ресурсу: http://www.itu.int/md/meetingdoc.asp?lang=en&parent=T09-SG17-C&question=Q10/17

15) Recommendation for KeyManagement – Part 1: General [Электронный ресурс]: — Режим доступа к ресурсу: http://csrc.nist.gov/publications/drafts/800-57/Draft_SP800-57-Part1-Rev3_May2011.pdf

16) Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance [Электронный ресурс]: — Режим доступа к ресурсу:

http://www.idmanagement.gov/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202.pdf

17) National e-Authentication Framework [Электронный ресурс]: — Режим доступа к ресурсу: http://www.finance.gov.au/e-government/security-and-authentication/authentication-framework.html

18) Guide to Secure Web Services [Электронный ресурс]: — Режим доступа к ресурсу: http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

Приложение А

Дополнительные стандарты и рекомендации

Распоряжением Правительства Российской Федерации 10 июня 2011 г. № 1021-р утверждена «Концепция снижения административных барьеров и повышения доступности государственных и муниципальных услуг на 2011-2013 годы».

Федеральный закон от 27 июля 2010 г. N 210-ФЗ «Об организации предоставления государственных и муниципальных услуг» (с изменениями от 6 апреля, 27 июня, 1, 11, 18 июля, 3 декабря 2011 г.).

Постановление Правительства РФ от 8 июня 2011 г. N 451 «Об инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

Распоряжение Правительства Российской Федерации от 15 апреля 2011 N 654-р «О базовых государственных информационных ресурсах».

Постановление Правительства РФ от 16 мая 2011 г. N 373 «О разработке и утверждении административных регламентов исполнения государственных функций и административных регламентов предоставления государственных услуг».

ПРОТОКОЛ от 7 июня 2011 г. № 10 заседания Правительственной комиссии по внедрению информационных технологий в деятельность государственных органов и органов местного самоуправления (ПРИЛОЖЕНИЕ).

Перечень мероприятий программы «Снижение административных барьеров, оптимизация и повышение качества предоставления государственных и муниципальных услуг, в том числе на базе многофункциональных центров предоставления государственных и муниципальных услуг на 2011-2013 годы».

Типовая программа субъекта РФ «Снижение административных барьеров, оптимизация и повышенеи качества предоставления государственных и муниципальных услуг, в том числе на базе многофункциональных центров предоставления государственных и муниципальных услуг на 2011 - 2013 годы».

ТИПОВОЙ ПЛАН мероприятий субъекта Российской Федерации по методическому и правовому обеспечению перехода на межведомственное и межуровневое взаимодействие при предоставлении государственных (муниципальных) услуг.

РЕКОМЕНДАЦИИ по разработке порядка определения размера платы за оказание услуг, необходимых и обязательных для предоставления исполнительными органами государственной власти субъектов Российской Федерации государственных услуг.

ПРОТОКОЛ заседания Правительственной комиссии по проведению административной реформы (Москва) от 23.11.2010 № 109.

Постановление Правительства Российской Федерации от 27 сентября 2011 г. N 797 г. Москва «О взаимодействии между многофункциональными центрами предоставления государственных (муниципальных) услуг и федеральными органами исполнительной власти, органами государственных внебюджетных фондов, органами государственной власти субъектов Российской Федерации, органами местного самоуправления».

Постановление Правительства РФ от 16 мая 2011 г. N 373 «О разработке и утверждении административных регламентов исполнения государственных функций и административных регламентов предоставления государственных услуг» (с изменениями от 19 августа 2011 г.).

Распоряжение Правительства РФ от 25 апреля 2011 г. N 729-р «О перечне услуг, оказываемых государственными и муниципальными учреждениями и другими организациями, в которых размещается государственное задание (заказ) или муниципальное задание (заказ), подлежащих включению в реестры

государственных или муниципальных услуг и предоставляемых в электронной форме».

ПРОЕКТ ПРИКАЗА министерства экономического развития РФ «Об утверждении методических рекомендаций по созданию и обеспечению деятельности многофункциональных центров предоставления государственных и муниципальных услуг».

Постановление Правительства РФ от 11 ноября 2005 г. N 679 «О порядке разработки и утверждения административных регламентов исполнения государственных функций (предоставления государственных услуг)» (с изменениями от 29 ноября 2007 г., 4 мая 2008 г., 2 октября 2009 г., 16 мая 2011 г.).

Постановление Правительства РФ от 24 октября 2011 г. N 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)» (с изменениями от 28 ноября 2011 г.).

Постановление Правительства Российской Федерации от 8 сентября 2010 г. №697 «О системе межведомственного электронного взаимодействия».

ОТВЕТЫ на вопросы, содержащиеся в обращениях органов исполнительной власти субъектов РФ и администраций муниципальных образований в целях разъяснения отдельных положений Федерального закона от 27.07.2010 № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг».

ETSI TS 142 009 V4.0.0 (2001-03). Technical specification. Digital cellular telecommunications system (Phase 2+); Security aspects (3GPP TS 42.009 version 4.0.0 Release 4)

ETSI TS 142 048 V4.0.0 (2001-03). Technical specification. Digital cellular telecommunications system (Phase 2+); Security mechanisms for the SIM application toolkit; Stage 1 (3GPP TS 42.048 version 4.0.0 Release 4)

ETSI TS 143 020 V5.2.0 (2006-06). 2. Technical specification. Digital cellular telecommunications system (Phase 2+); Security-related network functions (3GPP TS 43.020 version 5.2.0 Release 5)

ETSI TS 155 205 V6.1.0 (2003-12). Technical specification. Digital cellular telecommunications system (Phase 2+); Specification of the GSM-MILENAGE algorithms: An example algorithm set for the GSM Authentication and Key Generation Functions A3 and A8 (3GPP TS 55.205 version 6.1.0 Release 6)

ISO/IEC TR 13335-3 (Annex E «Types of Risk Analysis Method»)

Common Methodology for Information Technology Security Evaluation Part 2 Evaluation Methodology (Annex B «General evaluation guidance»)

3GPP2 S.R0082 Enhanced Packet Data Air Interface Security

3GPP2 S.R0083-0 Broadcast-Multicast Service Security Framework

3GPP2 S.R0086-0 IMS Security Framework

3GPP2 S.R0086-A IMS Security Framework

3GPP2 S.S0078-0 Common Security Algorithms

3GPP2 S.S0078-A Common Security Algorithms

3GPP2 S.S0083-A Broadcast-Multicast Service Security Framework

TS 02.09 8.0.1 Security aspects

TS 02.33 8.0.1 Lawful Interception

TS 03.20 8.1.0 Security-related Network Functions

TS 03.20ext 3.0.0 Security-related Network Functions (Ext)

TS 03.33 8.1.0 Lawful Interception; Stage 2

TS 21.133 4.1.0 3G security; Security threats and requirements

TS 22.022 5.0.0 Personalisation of Mobile Equipment (ME); Mobile functionality specification

TS 22.032 5.0.0 Immediate Service Termination (IST); Service description; Stage 1

TS 23.035 5.1.0 Immediate Service Termination (IST); Stage 2

TS 33.105 4.1.0 Cryptographic Algorithm requirements

TS 33.106 6.0.0 Lawful interception requirements

TS 33.120 4.0.0 Security Objectives and Principles

TS 33.141 1.1.1 Presence service; Security

TR 33.817 6.0.0 Feasibility study on (Universal) Subscriber Interface Module (U)SIM security reuse by peripheral devices on local interfaces

TR 33.901 4.0.0 Criteria for cryptographic Algorithm design process

TR 33.941 0.6.0 Presence service; Security

TS 43.020 5.0.0 Security-related network functions

3GPP TS 22.004. General on supplementary services

3GPP TS 22.011. Service accessibility

3GPP TS 22.060. General Packet Radio Service (GPRS); Service description; Stage 1

3GPP TS 23.060. General Packet Radio Service (GPRS); Service description; Stage 2