ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59382— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы управления идентичностью

Часть 3

Практические приемы

(ISO/IEC 24760-3:2016, NEQ)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 РАЗРАБОТАН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Акционерным обществом «Аладдин Р.Д.» (АО «Аладдин Р.Д.») и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ)

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 412-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ИСО/МЭК 24760-3:2016 «Информационные технологии. Методы и средства обеспечения безопасности. Структура менеджмента идентификационных данных. Часть 3. Практические приемы» (ISO/IEC 24760-3:2016 «Information technology — Security techniques — A framework for identity management — Part 3: Practice», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

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

Содержание

Введение

Для функционирования автоматизированных (информационных) систем необходимо собирать и формировать информацию о пользователях, связанном с ними программном обеспечении или оборудовании, и принимать решения на основе данной информации. Такие решения, основанные на данных пользователей, могут касаться доступа к приложениям или другим ресурсам.

Реагируя на потребность эффективной и результативной реализации систем, принимающих решения, основанные на идентификационных данных, комплекс стандартов по основам управления идентичностью определяет основные положения выпуска, администрирования и использования данных, помогающих характеризовать цифровой образ субъектов доступа, организаций или компонентов информационной технологии, действующих в интересах физических лиц или организаций.

Для многих организаций надлежащее управление идентичностью является критичным для поддержки безопасности процессов организации. Для физических лиц надлежащее управление идентификационными данными важно для защиты их персональных данных.

Настоящий стандарт определяет практические приемы управления идентичностью. Эти приемы охватывают обеспечение доверия к структуре управления идентичностью, включающей в себя управление доступом к идентификационным данным и другим ресурсам на основе идентификационных данных, политикам доступа, сторонам взаимодействия и способам обмена идентификационными данными, а также управлению целями, которые должны быть реализованы при создании и поддержке системы управления идентификационными данными.

Комплекс стандартов по основам управления идентичностью состоит из следующих частей:

- часть 1. Терминология и концепции;
- часть 2. Эталонная архитектура и требования;
- часть 3. Практические приемы.

Настоящий стандарт является основой для применения других национальных стандартов, связанных с управлением идентификационными данными.

Настоящий стандарт необходимо применять с учетом требований нормативных правовых актов и стандартов Российской Федерации в области защиты информации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Основы управления идентичностью

Часть 3

Практические приемы

Information technology. Security techniques.
A framework for identity management. Part 3. Practice

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт представляет собой руководство по управлению идентичностью и обеспечению уверенности в том, что система управления идентификационными данными соответствует его требованиям.

Настоящий стандарт применим для систем управления идентификационными данными, в которых осуществляется получение, обработка, хранение, передача или использование связанных с сущностями идентификаторов и/или идентификационной информации (в том числе персональных данных) с целью идентификации или аутентификации сущностей и/или с целью принятия решений с применением атрибутов сущностей. Практические приемы управления идентификационными данными могут также рассматриваться в других стандартах.

Положения настоящего стандарта не исключают применение криптографических методов (алгоритмов) при управлении идентичностью, но не устанавливают требования по их реализации.

2 Нормативные ссылки

В настоящем стандарте использованы следующие нормативные ссылки.

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

ГОСТ Р 59381 Информационные технологии. Методы и средства обеспечения безопасности. Основы управления идентичностью. Часть 1. Терминология и концепции

ГОСТ Р 59407 Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных

ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 29100—2013 Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный

Издание официальное

стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 59381, а также следующие термины с соответствующими определениями:

3.1 **профиль идентичности** (identity profile): Идентификационные данные, содержащие атрибуты, определяемые шаблоном идентичности.

3.2 **шаблон идентичности** (identity template): Определение конкретной совокупности атрибутов.

Примечание — Обычно атрибуты в профиле должны поддерживать определенную техническую или деловую цель, как требуется полагающимся сторонам.

3.3 **подделка идентичности** (identity theft): Результат успешного подтверждения ложной идентичности.

4 Уменьшение рисков, связанных с идентичностью, при управлении идентификационными данными

В данном разделе представлены практические приемы снижения рисков, связанных с идентичностью, при эксплуатации системы управления идентификационными данными, которая соответствует требованиям настоящего стандарта.

4.1 Оценка риска

Одна из функций системы управления идентификационными данными заключается в управлении рисками ошибок идентификационных данных, а также в управлении конфиденциальностью, целостностью и доступностью идентификационной информации, которую она хранит, обрабатывает и передает. Необходимо понимать уровень риска, который обуславливается доменом применения. Оператор должен провести оценку риска, чтобы определить уровень риска. Результат может быть использован для определения необходимых критериев управления рисками и процессов системы управления идентификационными данными. Информация, которая требуется системе управления идентификационными данными, включает уровень доверия к требуемой идентификационной информации, а также требования обеспечения конфиденциальности, целостности и доступности данной информации.

ГОСТ Р 59407 определяет такие инструменты управления рисками, как политика, регулирование, проектирование и архитектура. В некоторых случаях, имеющих первостепенное значение для пользователей — субъектов персональных данных, должна предоставляться возможность контроля за использованием персональных данных и обеспечением их защиты.

Примечание — Требования по защите персональных данных определяются в [1], а отдельные рекомендации по их реализации в ГОСТ Р 59407.

Идентификационная информация, управляемая системой управления идентификацией, также может управляться поставщиком идентификационной информации в другом домене посредством использования ссылок. Например, подтверждение идентификационных данных может осуществляться поставщиком услуг, который действует в домене, отличном от того, в котором функционирует система управления идентификационными данными.

При сборе и хранении идентификационной информации системой управления идентификационными данными должны быть реализованы меры управления рисками с целью снижения рисков, идентифицированных в результате оценки риска, осуществляемой в домене применения полагающейся стороной. В соответствии с оцененными уровнями риска полагающейся стороной должны быть определены и специфицированы уровни доверия к идентификационной информации и услугам доступа.

4.2 Уверенность в достоверности идентификационной информации

4.2.1 Общие положения

Уверенность в идентификационной информации, предоставляемой системой управления идентификационными данными, проистекает из процессов, обеспечивающих уверенность в достоверности информации от момента ее сбора до последующего хранения и поддержки системой. Уверенность определяется уровнем доверия, где более высокие уровни доверия соответствуют большей уверенности. Достигаемый уровень доверия зависит от качества идентификационной информации и строгости проверки достоверности идентификационных данных. Уровни доверия определены в ГОСТ Р 58833.

4.2.2 Подтверждение идентичности

Подтверждение идентичности при регистрации сущности в домене должно соответствовать определенному уровню. Достижимый уровень подтверждения идентичности зависит от типа и характеристик информации, а в некоторых случаях и от объема этой информации, например от числа независимых поставщиков идентификационной информации, используемых в качестве источников информации.

Повышение уровня доверия к верификации идентичности можно быть достигнуто:

- с помощью проверки дополнительных мандатов, выпущенных несколькими источниками;
- путем использования доверенной третьей стороны, которой известна информация о сущности, для проверки действительности заявленной идентификационной информации.

Примечание — Способы достижения различных уровней доверия определены ГОСТ Р 58833, при этом требования к подтверждению идентификационных данных рассмотрены в [2].

4.2.3 Мандаты

Система управления идентификационными данными может выпускать различные виды мандатов (токенов, электронных удостоверений доступа), которые отличаются уровнем доверия идентификационной информации, предоставляемой данными мандатами.

Система управления идентификационными данными, выпускающая мандаты высокого уровня доверия с применением криптографических механизмов, должна предоставлять полагающимся сторонам услугу поддержки процесса криптографической проверки достоверности мандатов.

4.2.4 Профиль идентичности

Система управления идентификационными данными может использовать один или несколько профилей идентичности для сбора, структурирования или представления идентификационной информации.

Примечание — Хотя профиль может содержать идентификационную информацию, он не предназначен для идентификации. Профиль обеспечивает предоставление структурированной идентификационной информации о сущности процессам системы.

У сущности может быть много профилей идентичности, в каждом из которых содержатся различные совокупности атрибутов сущности. Например, языковое предпочтение может присутствовать в профиле для интерфейса доступа.

Шаблон идентичности может применяться в качестве национального или отраслевого стандарта. Использование стандартизированного шаблона идентичности для записи идентификационных атрибутов обеспечит применение профиля идентичности в различных доменах.

Профиль идентичности может использоваться в управлении доступом с целью определения требуемых идентификационных атрибутов для роли или привилегии, связанной с доступом к информации. Профиль идентичности может использоваться в качестве предварительно сконфигурированного подмножества идентификационной информации, предназначенного для представления сущности при взаимодействии с услугой.

Атрибут в профиле идентичности может быть связан с уровнем доверия. Использование профиля идентичности с соответствующими уровнями доверия для представления идентификационной информации означает, что каждый элемент информации был проверен, как минимум, на соответствующем уровне доверия. Профиль идентичности, определяющий требования доступа к услугам или ресурсам, может быть связан с определенным дополнительным идентификатором сущности, который может указывать на действия, связанные с определенными привилегиями.

5 Идентификационная информация и идентификаторы

5.1 Общие положения

Организации должны понимать значение обеспечения безопасности информации для своего бизнеса и для обеспечения соответствия нормативным правовым актам, а также должны иметь поддержку руководства, чтобы полнее отвечать запросам потребителей. Что касается вопроса управления идентичностью, организации должны понимать свои обязательства и обеспечивать уверенность в реализации адекватных мер защиты информации для уменьшения рисков и последствий утечки, порчи и потери доступности идентификационной информации при ее сборе, хранении, использовании, передаче и утилизации.

Организации должны определять меры защиты информации и цели их применения для обеспечения уверенности в выполнении требований обеспечения безопасности информации.

5.2 Политика получения доступа к идентификационной информации

Необходимо осуществлять управление идентификационной информацией, относящейся к сущности, для обеспечения уверенности в следующем:

- идентификационная информация остается точной и актуальной с течением времени;
- доступ к идентификационной информации имеют только уполномоченные сущности, и они отвечают за все использование и осуществление изменений идентификационной информации, гарантируя прослеживаемость любой обработки идентификационной информации сущностью независимо от того, является ли она физическим лицом, процессом или системой;
- организация выполняет свои обязательства в отношении предписаний и соглашений;
- обеспечивается защита персональных данных субъектов от риска подделки идентичности и иных видов преступлений, связанных с идентификационными данными.

Примечание — Обычно политика обеспечения безопасности информации подчеркивает необходимость осуществления безопасного управления идентификационной информацией. При ведении дел с третьими сторонами также требуется обеспечение сохранности и защиты идентификационной информации любых сущностей, как обычно документально оформлено в операционных процедурах.

5.3 Идентификаторы

5.3.1 Общие положения

Идентификатор дает возможность однозначным образом отличить одну сущность от другой в домене применения. Сущность может иметь много различных идентификаторов в одном и том же домене. Это облегчает представление сущности в некоторых ситуациях, например, скрывая идентичность сущности при предоставлении идентификационной информации сущности для использования в некоторых процессах или в рамках некоторых систем.

Идентификатор, созданный в одном домене, может намеренно повторно использоваться в другом домене при условии, что используемый идентификатор продолжает обеспечивать уникальность идентичности в рамках другого домена.

5.3.2 Классификация идентификаторов по виду сущности, с которой связан идентификатор

5.3.2.1 Идентификатор, присвоенный сущности, являющейся физическим лицом

Идентификатором физического лица может быть, например, его полное имя, дата рождения, место рождения или различные псевдонимы, такие как номер, присвоенный органами власти в качестве ссылки, например номер паспорта, индивидуальный номер налогоплательщика и т. п. Использование псевдонимов в качестве идентификаторов является частым явлением для идентификаторов физических лиц.

Примечание — Псевдоним может обеспечить конфиденциальность персональных данных при обмене идентификационными данными с полагающейся стороной, так как псевдоним раскрывает меньше персональных данных, чем настоящее имя человека, использованное в качестве идентификатора.

5.3.2.2 Идентификатор, присвоенный сущности, не являющейся физическим лицом

Сущность, не являющаяся физическим лицом, например, устройство или информационный объект, тоже могут быть идентифицирована и зарегистрирована по аналогии с физическим лицом. Идентификаторы устройств дают возможность различать устройства в домене применения.

Примечания

1 Например, IMEI (International Mobile Equipment Identity — международный идентификатор мобильного оборудования) — это идентификатор мобильного телефона в домене мобильной телефонии GSM.

2 Например, ICCID (Integrated Circuit Card Id — уникальный серийный номер SIM-карты GSM) — это уникальный идентификатор устройства в домене мобильной телефонии GSM. SIM-карта также содержит другие идентификаторы, включая идентификатор пользователя, зарегистрировавшего SIM-карту.

Также может требоваться распознание идентификаторов информационных объектов в их доменах. В качестве идентификатора обычно используется один из атрибутов из комбинации их атрибутов.

Примечания

1 Например, наименование процесса, наименование сеанса связи, имя пути, унифицированное имя ресурса, унифицированный идентификатор ресурса (URI) представляют собой примеры идентификаторов информационных объектов.

2 Унифицированный идентификатор ресурса представляет собой пример идентификатора для местоположения, но объект в этом местоположении может меняться в любое время.

5.3.3 Классификация идентификаторов по характеру привязки

5.3.3.1 Прямой идентификатор

Прямой идентификатор (идентификатор, использующий настоящее наименование) представляет собой идентификатор, являющийся долгосрочным в домене своего применения, и который может использоваться в рамках одного или нескольких доменов, а также предоставляет полагающейся стороне возможность получать дополнительную идентификационную информацию сущности, связанной с этим идентификатором. Прямые идентификаторы с использованием настоящего наименования могут включать: адрес электронной почты, номер мобильного телефона, номер паспорта, номер водительского удостоверения, номер карточки социального страхования.

Прямой идентификатор позволяет соотносить идентификационную информацию сущности, известной в различных доменах. Если физическое лицо разрешает устанавливать взаимосвязь своих идентичностей, которая упрощает их использование, непредвиденная взаимосвязь может оказывать негативное влияние на защиту его персональных данных. Из-за природы прямого идентификатора в случае инцидента, связанного с утечкой информации, нарушитель может осуществить такую корреляцию и создать угрозу, например формирования какой-либо связанной с субъектом персональных данных информации, которую субъект персональных данных не планировал раскрывать.

5.3.3.2 Псевдонимный идентификатор

Псевдонимный идентификатор представляет собой идентификатор, являющийся долгосрочным в домене своего применения, который не раскрывает дополнительную идентификационную информацию. Пока никакая другая идентификационная информация не является доступной в данном домене, нельзя осуществить корреляцию идентификационных данных из другого домена с использованием псевдонимного идентификатора. Псевдонимный идентификатор может использоваться для предотвращения нежелательной корреляции идентификационной информации сущностей в разных доменах.

Примечание — Использование псевдонимных идентификаторов не равнозначно псевдонимности идентификационных данных. Других атрибутов, скомбинированных в какой-то момент времени или в различные моменты времени, может быть достаточно для выведения идентификаторов, использующих настоящее имя.

5.3.3.3 Кратковременный идентификатор

Кратковременный идентификатор представляет собой идентификатор, который используется только в течение короткого периода времени и только в единственном домене. Он может меняться для многочисленных случаев использования одной и той же услуги или ресурса.

Примечания

1 В случае правильного применения кратковременный идентификатор затруднит возможность связывания различных идентификаторов, используемых при нескольких попытках доступа одной и той же сущностью.

2 Кратковременный идентификатор часто используется в контексте управления доступом на основе атрибутов, где доступ к ресурсу предоставляется при наличии у сущности определенного атрибута. Например, если доступ к ресурсу предоставляется пользователям, потому что они являются членами определенной группы, то их идентификаторы будут составлены из кратковременного идентификатора и группового идентификатора. Такие идентификаторы сводят к минимуму возможность раскрытия данных или возможность связывания нескольких попыток доступа, но по-прежнему позволяя различить каждую сущность.

5.3.4 Классификация идентификаторов по группированию сущностей

5.3.4.1 Индивидуальный идентификатор

Индивидуальный идентификатор представляет собой идентификатор, связанный только с одной сущностью в домене.

5.3.4.2 Групповой идентификатор

При возникновении необходимости выполнять действия в группе, сущности могут объединяться в групповую сущность. Идентичность группы будет представлять групповую сущность, а идентификатор группы позволит однозначно идентифицировать групповую сущность и регистрировать действия групповой сущности в домене. Идентификаторы групп служат для удовлетворения потребности сущности в выполнении действий в группе или от имени группы, при этом он позволяет скрывать инициатора действий в группе. Соответственно, могут потребоваться дополнительные методы для однозначной идентификации отдельной сущности как члена групповой сущности.

5.3.5 Управление идентификаторами

При обновлении идентификационной информации для известной сущности система управления идентификационными данными может присваивать новый идентификатор изменившейся идентичности, а также может удалить связь старого идентификатора с идентичностью. Измененная идентификационная информация может упреждающим образом сообщаться подсистемам, которые на нее полагаются.

6 Аудит использования идентификационной информации

Управление и обработка идентификационной информации уполномоченными сущностями в определенном домене могут подчиняться различным правовым и нормативным требованиям, что неизбежно влечет за собой определенный уровень мониторинга и прослеживаемости.

Примечание — Эти требования могут быть разносторонними, включая, например, от наличия журналов регистрации и других мер обеспечения защиты персональных данных до поддержки требуемой точности и прослеживаемости отметок времени.

Сущность, предоставляющая услуги, связанные с управлением идентичностью, должна обеспечивать механизмы, гарантирующие возможность проведения аудита.

7 Цели управления и контроля

7.1 Общие положения

Данный раздел определяет цели безопасности и связанные с ними элементы управления, которые подлежат учету при создании или проверке соответствия системы управления идентификационными данными.

Структура управления безопасностью соответствует рекомендациям ГОСТ Р ИСО/МЭК 27002.

7.2 Контекстные компоненты для управления

7.2.1 Создание системы управления идентификационными данными

7.2.1.1 Цель

Создание системы управления с целью инициирования и контроля реализации управления идентификационной информацией сущностей.

7.2.1.2 Определение и документальное оформление домена применения

Требования

Полагающиеся стороны, для которых сущности или группе сущностей дается возможность применять свои идентичности и которые могут использовать идентичности с целью идентификации и для других целей, должны быть задокументированы таким образом, чтобы они были понятны как операторам, так и заинтересованным субъектам.

Рекомендации по реализации

Документация, описывающая границы домена применения и границы системы управления идентификационными данными, должна быть доступна всем заинтересованным сторонам. Эта документация должна определять границы, в которых может быть верифицирована идентичность. Любое потенциальное распространение на другие домены или группы сущностей также должно документально оформляться.

Документация должна определять правовые или иные ограничения, накладываемые на управление идентификационной информацией в домене, и связанные с этим обязательства.

Дополнительная информация

Домен применения идентичности определен по отношению к конкретному набору атрибутов, определяющих группы сущностей.

Автоматизированная (информационная) система организации, имеющая возможность регистрации и предоставления доступа к ресурсам группе сущностей, может являться поддоменом в этой организации.

7.2.1.3 Идентификация поставщиков идентификационной информации, органов идентификационной информации, органов управления идентификационными данными и регулятивных органов

Требования

Для идентификационной информации, управляемой системой управления идентификационными данными, в домене должны быть определены органы идентификационной информации, а также должны быть определены сущности, утверждающие управленческие и нормативные обязанности по защите идентификационной информации.

Рекомендации по реализации

Сущности, связанные с системой управления идентификационными данными в качестве поставщика идентификационной информации, органа идентификационной информации, орган управления идентификационными данными и любые соответствующие регулятивные органы должны быть однозначно определены.

Операции, выполняемые поставщиком идентификационной информации, заключаются в создании, обслуживании и предоставлении доступа к идентификационной информации для сущностей, известных в определенном домене. Следует также определить методы доступа к информации или получения услуг, предоставляемых данными сущностями.

Любые изменения в доступности и методах доступа и получения услуг должны незамедлительно доводиться до сведения заинтересованных сторон.

Дополнительная информация

Сущность может объединять функции поставщика идентификационной информации и орган идентификационной информации.

7.2.1.4 Идентификация полагающихся сторон

Требования

Полагающиеся стороны должны быть известны в домене, содержащем систему управления идентификационными данными.

Рекомендации по реализации

Полагающиеся стороны имеют доверительные отношения с одним или несколькими органами идентификационной информации. Полагающиеся стороны, связанные с органом идентификационной информации, могут быть известны на этапе проектирования. Состав полагающихся сторон может изменяться с течением времени, вступая или прекращая отношения с одним или несколькими органами идентификационной информации в данном домене.

Дополнительная информация

Полагающаяся сторона подвержена риску, вызванному неверной или недействительной идентификационной информацией.

7.2.1.5 Поддержка системы управления идентификационными данными

Требования

Должен быть описан процесс обеспечения уверенности в поддержке значимых операционных сущностей в системе управления идентификационными данными.

Рекомендации по реализации

С течением времени в домене, содержащем систему управления идентификационными данными, могут использовать разные органы идентификационной информации, поставщики идентификационной информации и полагающиеся стороны для поддержки взаимодействия с сущностями. Домены применения также могут создаваться и прекращать свое действие, или могут меняться их условия применения.

Значимые сущности, используемые в системе управления идентификационными данными, например, органы идентификационной информации, поставщики идентификационной информации и полагающиеся стороны, после их замены, архивирования или удаления в их доменах, также могут прекращать существование в системе. Система управления идентификационными данными должна

документально оформлять политики и процессы, обеспечивающие контроль этих значимых сущностей, и обеспечивать уверенность в том, что информация системы управления идентификационными данными не будет потеряна.

7.2.1.6 Гарантии защиты персональных данных

Требования

При наличии физических лиц, осуществляющих взаимодействие в рамках системы управления идентификационными данными, для системы должны быть документально оформлены политики и установлены меры, обеспечивающие (гарантирующие) защиту конфиденциальности персональных данных.

Рекомендации по реализации

Одной из основных целей создания системы управления идентификационными данными является обеспечение уверенности в том, что защита персональных данных физических лиц обеспечивается непрерывно.

Система управления идентификационными данными должна документально оформлять любую обрабатываемую ей чувствительную, с точки зрения защиты персональных данных, информацию о физических лицах, чтобы соответствовать требованиям ГОСТ Р 59381.

Дополнительная информация

Требования к обработке чувствительной, с точки зрения защиты персональных данных, информации представлены в ГОСТ Р 59407 и ГОСТ Р ИСО/МЭК 29100.

7.2.2 Формирование идентификационной информации

7.2.2.1 Цель

Регламентация вопросов определения, документального оформления и передачи идентификационной информации.

7.2.2.2 Представление идентичности

Требования

Ссылка на сущность в системе управления идентификационными данными, которая остается неизменной в течение всего времени, пока сущность остается известной в домене (доменах) системы, называется «ссылочным идентификатором».

В системе управления идентификационными данными должны быть задокументированы требования, гарантирующие уникальную различимость каждой сущности в любом домене применения.

Рекомендации по реализации

Ссылочный идентификатор должен продолжать существовать в системе управления идентификационными данными, по крайней мере, в течение срока существования сущности и может существовать дольше, чем сущность, например, для архивных целей или потребностей государственных органов.

Документация системы управления идентификационными данными должна описывать первичное использование и повторное использование идентификаторов. Ссылочный идентификатор для сущности не должен повторно использоваться, пока любая идентификационная информация, связанная с этой сущностью, включая архивную информацию, зафиксирована в системе.

Генератор ссылочных идентификаторов представляет собой инструментальное средство, которое может способствовать обеспечению уникальных значений ссылочных идентификаторов.

Дополнительная информация

Для упрощения ведения зафиксированной информации для конкретной идентичности, система управления идентификационными данными может использовать генератор ссылочных идентификаторов для присвоения уникального номера записи добавляемым идентичностям.

7.2.2.3 Идентификационная информация

Требования

Совокупность значений атрибутов, требуемых для формирования идентификационной информации, относящейся к сущности, в домене, содержащем систему управления идентификационными данными, должна фиксироваться, проверяться верификаторами и передаваться по запросу полагающимся сторонам.

Рекомендации по реализации

Верификация значений обязательных атрибутов идентичности может приводить к появлению подтвержденной идентичности для сущности.

Процесс аутентификации включает тестирование верификатором одного или нескольких идентификационных атрибутов, предоставленных сущностью, с целью определения — с требуемым уровнем доверия — их достоверности.

7.2.2.4 Определение различных видов сущностей

Требование

Количество различных типов сущностей в домене, содержащем систему управления идентификационными данными, должно быть распознано и описано с помощью различных значений атрибутов, составляющих их идентичность.

Рекомендации по реализации

Элементы внутри или вне автоматизированной системы, такие, как физическое лицо, организация, устройство, подсистема, или группа таких элементов с распознаваемой уникальностью в домене, содержащем систему управления идентификационными данными, представляют собой отличающиеся друг от друга виды сущностей, которые могут описываться разными значениями атрибутов.

Каждый тип сущностей должен быть задокументирован, охватывая семантику и синтаксис идентичности со списком обязательных значений атрибутов для проверки.

7.2.2.5 Аутентификация идентичности

Требования

Процесс проверки идентификационной информации сущности должен быть документально оформлен.

Рекомендации по реализации

Процесс аутентификации включает в себя операции верификатора, который должен установить, что для уровня доверия, необходимого для предоставления услуги сущности, его идентификационная информация является правильной.

Верификатором может быть или действовать от его имени, например орган идентификационной информации конкретного домена.

7.2.3 Управление идентификационной информацией

7.2.3.1 Цель

Обеспечить сохранность и защиту идентификационной информации во всех доменах применения системы управления идентификационными данными, начиная с первоначальной регистрации и заканчивая архивированием или удалением.

7.2.3.2 Гарантии при формировании и управлении идентификационной информацией

Требования

Все обязанности по обеспечению информационной безопасности при формировании и управлении идентификационной информацией должны быть определены и назначены.

Рекомендации по реализации

Распределение обязанностей, связанных с обеспечением информационной безопасности при формировании и управлении идентификационной информацией, должно осуществляться в соответствии с политиками обеспечения безопасности информации. Следует определить ответственность за защиту персональных данных и за выполнение конкретных процессов информационной безопасности при формировании и управлении идентификационной информацией.

Следует определить ответственность за деятельность по управлению рисками информационной безопасности и, в частности, за принятие остаточных рисков при определении уровней доверия, которые необходимо достигнуть при формировании идентификационной информации.

Управление идентичностью должно включать следующее:

- применение приложений(я), реализующих реестр идентичностей;
- установление домена происхождения конкретных значений атрибутов в идентификационной информации;
- поддержку достоверности идентификационной информации в течение жизненного цикла идентичности;
- аутентификацию идентичности;
- уменьшение риска подделки или злоупотребления идентификационной информацией.

Дополнительная информация

Руководитель службы безопасности информации организации, если таковой назначен, должен взять на себя общую ответственность за разработку и реализацию уровней доверия при формировании и управлении идентификационной информацией.

7.2.3.3 Определение и контроль жизненного цикла идентификационных данных

Требования

Формализованный процесс, определяющий и поддерживающий жизненный цикл идентичности в домене применения, а также контролирующий состояние любой идентичности в каждом домене, должен быть документально оформлен.

Рекомендации по реализации

Жизненный цикл идентификационной информации начинается с внесения в реестр и завершается, когда идентификационная информация для сущности удаляется из системы, включая любую архивированную информацию.

Дополнительная информация

Согласно ГОСТ Р 59381 определяются следующие этапы жизненного цикла идентификационных данных:

- неизвестное;
- установленное;
- активное;
- приостановленное;
- архивное;
- удаленное.

7.3 Архитектурные компоненты для управления

7.3.1 Создание системы управления идентификационными данными

7.3.1.1 Цель

Система управления идентификационными данными должна быть задокументирована до ее внедрения.

7.3.1.2 Документальное оформление системы управления идентификационными данными

Требования

Система управления идентификационными данными должна быть документально оформлена до начала ее реализации.

Рекомендации по реализации

Документально оформленный проект архитектуры системы управления идентификационными данными должен определять систему в контексте ее использования на основе причастных сторон и действующих субъектов, а также установленных требований.

Документально оформленный проект должен рассматривать требования в отношении причастных сторон, являющихся и не являющихся действующими субъектами.

Дополнительная информация

Документально оформленный проект должен исчерпывающим образом описывать следующее:

- требования к действующим субъектам;
- требования к причастным сторонам;
- точки зрения;
- модели;
- компоненты;
- процессы поддержки;
- потоки информации и действия.

Дополнительно должен быть также документально оформлен перечень типов действующих субъектов и их взаимодействий с системой.

Документально оформленный проект должен определять сценарий, используемый для создания системы управления идентификационными данными, например, сценарий организации, объединения, сценарий предоставления услуг или сценарий неоднородной системы. Проект должен соответствующим образом определять компоненты и потоки для выбранного сценария.

7.3.1.3 Идентификация органа регистрации идентификационных данных

Требования

Для любой системы управления идентификационными данными должен быть идентифицирован орган регистрации идентификационных данных.

Рекомендации по реализации

Орган регистрации идентификационных данных имеет обязанности и возможности по установлению и обеспечению соблюдения операционных политик, предназначенных для сбора, фиксирования и обновления идентификационной информации.

Обязанности органа регистрации идентификационных данных включают в себя следующее:

- модификацию, создание или отмену операционных политик;

- санкционирование модификации механизмов для установления требуемого уровня доверия к аутентификации сущности для доступа к идентификационной информации и функциям управления системой;

- санкционирование изменений типа информации, зафиксированной в репозитории;

- санкционирование модификации идентификационной информации, зафиксированной в репозитории.

Дополнительная информация

Если орган регистрации идентификационных данных не идентифицирован, эту роль должен играть руководитель службы безопасности информации.

7.3.2 Контроль системы управления идентификационными данными

7.3.2.1 Цель

Обеспечение уверенности в том, что система управления идентификационными данными содержит механизмы обеспечения безопасности и поддержки идентификационной информации.

7.3.2.2 Доступ к системе управления идентификационными данными

Требования

Доступ к системе управления идентификационными данными должен быть ограничен перечнем, включающим лиц, занимающихся ее поддержкой, поставщиков идентификационной информации и полагающиеся стороны, а также лиц, приглашенных для консультирования по собранной о них информации в контексте обеспечения защиты персональных данных.

Рекомендации по реализации

В системе управления идентификационными данными должны быть разработаны необходимые интерфейсы для предоставления доступа нуждающимся в нем сущностям с соответствующими правами, санкционированными органом идентификационной информации или органом регистрации.

7.3.2.3 Требуемые компоненты системы управления идентификационными данными

Требования

Система управления идентификационными данными должна, как минимум, включать следующее:

- репозиторий идентичностей, относящихся к сущностям, распознанным в ее доменах, возможно структурированный с использованием идентификационных шаблонов;

- систему управления, действующую в соответствии с унифицированной политикой, способную собирать идентификационную информацию из различных подтвержденных источников (домены происхождения атрибутов) и удалять эту информацию при прекращении существования условий хранения идентификационной информации;

- интерфейсы управления для предоставления доступа к идентификационной информации;

- компонент хранения, архивирующий информацию о сущностях, которые прекратили свое существование.

Рекомендации по реализации

Системы управления идентификационными данными могут различаться по компонентам в зависимости от модели, разработанной для ее реализации.

Функция управления идентичностью может быть реализована в системе, предназначенной для выполнения организационных функций, таких как управление человеческими ресурсами или управление закупками, поскольку эти системы представляют собой основные (доверенные) источники для системы управления идентификационными данными.

Однако система управления идентификационными данными должна оставаться независимой от любой другой системы в домене, поскольку она отвечает функциональным требованиям, в значительной степени отличающимся от функций управления других систем.

7.3.2.4 Аудит системы управления идентификационными данными

Требования

Система управления идентификационными данными должна регулярно оцениваться или подвергаться аудиту (как правило, ежегодно).

Рекомендации по реализации

Аудит или оценка соответствия должны подтверждать, что система управления идентификационными данными действует согласно документально оформленным политикам и процедурам и соответствует правовым и иным налагаемым внешним образом требованиям, например требованиям защиты персональных данных.

Процедуры оценки соответствия или аудиты должны включать положения, описывающие операции, осуществляемые системой менеджмента идентификационных данных, в частности, в отношении выполнения операционных политик.

Результаты оценки соответствия или аудитов должны подтвердить, что система управления идентификационными данными сообщает о конкретных операциях, например, связанных с уязвимостями, оценивает, соответствуют ли эти операции применимым политикам, например, политикам защиты персональных данных, и предупреждает о любых расхождениях.

Приложение А
(справочное)

Практические приемы управления идентификационной информацией при объединении систем управления идентификационными данными

А.1 Общая информация

Объединение идентичностей представляет собой соглашение между двумя или более доменами, определяющее, как будет осуществляться обмен идентификационной информацией между доменами и управление ею. Соглашение объединения определяет общие протоколы, форматы и процедуры, охватывающие вопросы безопасности (включая защиту персональных данных), управления и аудита, которые будут использоваться во всем объединении.

Объединение идентичностей обычно создается с целью расширения совместимого обмена идентификационной информацией и использования вытекающих из этого преимуществ, таких как расширение потребительской электронной торговли и увеличение продуктивности и результативности предприятия, которые в свою очередь способствуют развитию цифровой экономики.

В объединении идентичностей другие домены объединения официально признают систему управления идентификационными данными конкретного домена. Следовательно, сущности, известные в этом домене, распознаются в других доменах и могут получать в них санкционированный доступ к ресурсам и услугам. Объединение может быть внутренним по отношению к более крупной организации, например организации, состоящей из многих подразделений, неформальной организации или организации, созданной как отдельная сущность, в зависимости от векторов риска и угроз и масштаба мер защиты информации, требуемых при управлении рисками. Если объединение заявляется доверенным, то оно должно быть способным управлять данными рисками.

Источником рисков является информационная асимметрия, присущая структуре объединения. Доверие сторон и их уверенность друг в друге зависят от политик и других процессов управления, устанавливающих структуру доверия, например, известную как круг доверия или цепочка доверия.

Объединение идентичностей устанавливает различные правила, касающиеся формата и шифрования обмена идентификационными данными. Объединение идентичностей должно определять требования безопасности, операционные требования, правила и механизмы:

- для запроса, поставки, хранения, использования и ликвидации идентификационной информации;
- распознавания поставщиков идентификационной информации участвующих доменов;
- предъявления идентификационной информации, запрашиваемой полагающейся стороной в одном из доменов объединения идентичностей;
- защиты персональных данных;
- подтверждения идентичности при внесении в реестр в одном из доменов объединения;
- защиты персональных данных в системе управления идентификационными данными;
- присоединения к объединению идентичностей;
- установления уровней доверия выполняется в соответствии с ГОСТ Р 58833:
  - для подтверждения идентичности при выпуске мандатов;
  - подтверждения подлинности (аутентификации) сущности в рамках объединения идентичностей.

Примечания

1 Установленные требования обеспечивают основу для формирования доверия при обменах идентификационной информацией.

2 Спецификация может относиться к процессу распознавания, например предоставление согласованных свидетельств, процессу сертификации, двустороннему или централизованному предоставлению свидетельств аккредитации независимой третьей стороной.

3 Объединение идентичностей может быть сформировано с установленными общими требованиями или взаимным признанием требований, независимо устанавливаемых каждым доменом или цепочкой доверия.

А.2 Модели доверенных объединений идентичностей

Для объединения идентичностей характерен ряд структур, рассмотренных ниже. В простом объединении идентичностей может быть смешанный состав действующих субъектов, выполняющих различные роли, например:

- операторы структуры доверия (в некоторых контекстах называются операторами объединения идентичностей);
- орган идентификационной информации;
- поставщик идентификационной информации;
- взаимодействующие агенты, предоставляющие идентификационный атрибут или мандат;
- полагающаяся сторона (в некоторых контекстах называется поставщиком услуг);
- субъект (в некоторых контекстах называется запрашивающей стороной).

Объединение идентичностей, как минимум, включает два вида действующих субъектов (рисунок А.1): поставщик идентификационной информации и полагающаяся сторона. Поставщик идентификационной информации осуществляет управление информацией, относящейся к идентификации сущности, а полагающаяся сторона предлагает услуги сущностям, которые удовлетворяют требованиям политик, связанным с данными услугами.

Трехсторонние модели объединения, включающие субъекта, представляют собой типичный базовый уровень в потребительском контексте, ориентированном на пользователя, но могут быть расширены до четырех- или пятисторонних моделей. Многие объединения идентичностей являются более сложными и включают больше действующих субъектов для отражения своих целей, например, «веерные» модели и объединения объединений (в некоторых контекстах называемая межобъединения).

Парное объединение, как изображено на рисунке А.1, является элементарным объединением идентичностей.

Рисунок А.1 — Парная модель объединения идентичностей

Более типичное объединение идентичностей может включать четыре, пять или более сторон, как изображено на рисунке А.2.

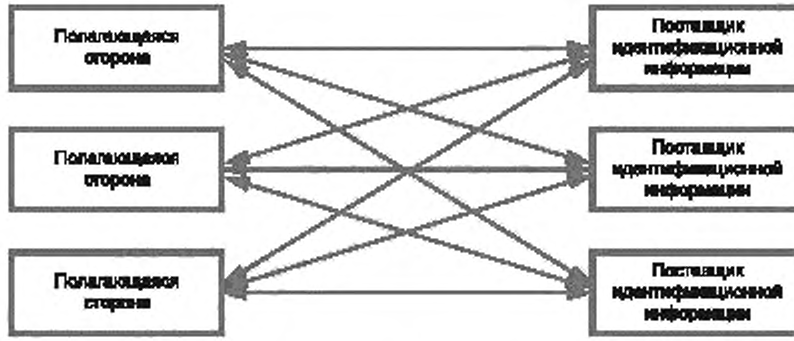

Рисунок А.2 — Сложная модель объединения

В объединении идентичностей с таким и более высоким уровнем сложности появляются дополнительные функциональные компоненты, облегчающие его работу, например, такие как орган идентификационной информации.

Роль оператора объединения заключается в управлении вопросами, возникающими в связи с функционированием объединения. Данную роль может выполнять существующий член объединения или независимая третья сторона.

На рисунке А.2 пользователь (запрашивающая сторона) не участвует в коммуникациях между полагающейся стороной и поставщиком идентификационной информации. Для процессов обмена, ориентированных на пользователя и обеспечение безопасности персональных данных, больше подходит практический прием, при котором пользователь играет роль посредника в обмене сообщениями между полагающейся стороной и поставщиком идентификационной информации, чтобы иметь возможность дать явное согласие на передачу идентификационной информации поставщиком идентификационной информации.

Сами объединения идентичностей могут принимать различные структурные формы в результате управления своей сложностью. Веерные структуры, как изображено на рисунке А.3, предлагают преимущества в виде наличия центрального шлюза, где сконцентрированы технические знания и опыт. Задачей шлюза является управление анонимностью, несвязанностью и ненаблюдаемостью.

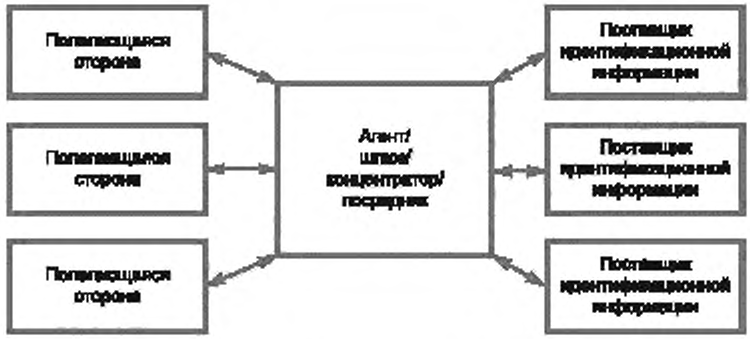

Рисунок А.3 — Шлюзовая модель объединения

Объединение идентичностей использует сеть связи. Эта сеть может быть открытой с одноранговыми коммуникациями всех участвующих поставщиков идентификационной информации или может использовать иерархические взаимосвязи, где идентификационная информация предоставляется через одного или нескольких промежуточных поставщиков идентификационной информации.

Основные действующие субъекты объединения идентичностей — поставщики идентификационной информации и полагающиеся стороны — могут устанавливать официальные доверительные отношения, например круг доверия. Официальные доверительные отношения могут способствовать соглашениям между членами объединения идентичностей, делающим возможным осуществление обмена идентификационной информацией и выполнение междоменных транзакций сущностями, зарегистрированными в различных доменах, образующих объединение.

А.3 Управленческие и организационные вопросы

Объединение идентичностей должно устанавливать правила, регулирующие разработку политики и последующие операционные механизмы структуры доверия для разграничения обязанностей сторон. Управленческие обязанности включают следующее:

- поддержку и/или признание семантики и/или синтаксиса идентификационной информации;
- обнаружение и распознавание поставщиков идентификационной информации и других действующих субъектов участвующих доменов;
- аутентификацию и утверждение требований к идентификационной информации полагающейся стороной в одном из доменов объединения;
- обеспечение безопасности персональных данных, а также конфиденциальности, целостности и доступности операций;
- определение и согласование вопросов, относящихся к тому, какие записи межобъединения могут храниться для целей аудита, в течение какого времени и при каких обстоятельствах к ним можно получить доступ;
- определение и согласование стандартов, механизмов, процессов и технологий передачи идентификационной информации между участниками объединения;
- участие в моделях финансирования и/или возмещения издержек;
- присоединение к объединению и выход из него.

Примечания

1 Эти установленные правила обеспечивают основу для доверия к идентификационной информации.

2 Эти установленные правила могут способствовать обеспечению соответствия и аккредитации членов, например, предоставляя свидетельства проведения аудита независимой третьей стороной, двухсторонней или централизованной сущностью, такой как оператор объединения.

3 Объединения могут формироваться при установлении определенных правил или при взаимном признании этих правил, независимо устанавливаемых каждым доменом, или путем комбинации того и другого.

Объединение структурируются таким образом, чтобы определять для каждого субъекта связанного с ним поставщика идентификационной информации, который проверяет официальную идентификационную информацию субъекта в объединении для целей распознавания, аутентификации и последующего признания. Данный поставщик идентификационной информации будет гарантировать подтверждение идентификационных данных, регистрацию, внесение в реестр, запрос, предоставление, хранение, использование и ликвидацию идентификационной информации в течение согласованного жизненного цикла идентификационных данных и домена применения. При этом необходимо отметить, что в контексте, связанном с физическими лицами, идентификационная информация

может существовать до рождения и оставаться после смерти, по аналогии с концепциями создания и уничтожения, которые применимы к сущностям, не являющимся физическими лицами.

Типичная последовательность операций может быть следующей: попытка субъекта получить доступ к ресурсу у полагающейся стороны, сбор полагающейся стороной информации на необходимом уровне доверия, и перенаправление субъекта к поставщику идентификационной информации для аутентификации, используя мандат. Последующий обмен сообщениями может включать поиск полагающейся стороной дополнительных атрибутов у поставщика идентификационных данных субъекта, которые могли быть переданы полагающейся стороне при условии (в случае физических лиц) согласия субъекта, после чего субъекту предоставляется доступ к запрашиваемому ресурсу.

Объединение идентификационной информации из различных органов в двух отдельных доменах является типичным условием при формировании двумя организациями объединения. В таких вариантах использования должны быть определены процедуры для разрешения противоречий и несоответствий, таким образом, чтобы в домене, полученном в результате объединения:

- ссылочные идентификаторы были уникальными;
- использовались псевдонимы, где это уместно;
- было бы невозможно связать идентификационные данные с не той сущностью.

В объединении должны существовать способы арбитражного разбирательства между поставщиками идентификационных данных, содержащими противоречивую идентификационную информацию.

А.4 Обнаружение

А.4.1 Общая информация о поставщиках идентификационной информации

Метод обнаружения может использоваться для обмена требуемой идентификационной информацией в рамках объединения; он позволяет быстро и динамично определять местонахождение сторон в объединении. Это применимо в крупных объединениях, где отмечаются постоянные изменения состава участников. Объединения и структуры доверия, лежащие в их основе, могут использовать определенные сервисы для улучшения обнаружения и функциональной совместимости.

Необходимо руководство по организации обнаружения. В зависимости от контекстных и межконтекстных правил механизмы обнаружения применяются по-разному.

Эта функция является неотъемлемой частью доверия объединения идентичностей, и ее развитие было мотивировано усложняющимися требованиями структур доверия.

Наиболее распространенными целями обнаружения обычно являются поставщики идентификационной информации. Процесс обнаружения — это возможность, предоставляемая поставщиками идентификационной информации и органами идентификационной информации в объединении, при согласии пользователя/субъекта/запрашивающей стороны или по законодательному/регулятивному требованию. Процесс обнаружения позволяет динамически определять местонахождение органа идентификационной информации для конкретной сущности с целью предоставления определенного требуемого атрибута, когда:

- идентификационная информация не существует;
- уровень доверия информации, полученной полагающейся стороной является недостаточным для необходимого уменьшения риска, связанного с идентификационными данными субъекта, для предоставления доступа к услуге;
- полагающаяся сторона не указывает, какого поставщика идентификационной информации использовать.

Обнаружение в объединении может осуществляться с использованием статических методов, таких как рекомендательные списки или обращение к определенным сервисам. Данные сервисы расширяют существующий диапазон сервисов, связанных с идентичностью, таких как структуры доверия и операторы объединения, задействованных в управлении ими, сущностях участвующих в объединении и их сертификационный статус. Функция указанных сервисов может быть дополнительно расширена путем использования динамических методов обнаружения, таких как публикация и службы метаданных. Динамическое обнаружение способствует эффективному функционированию современных объединений, в которых обычно наблюдается приток и отток участников, присоединяющихся к объединению и выходящих из нее.

Преимущества обнаружения включают освобождение полагающихся сторон от обязательств кэширования или хранения идентификационной информации до тех пор, пока требования или обязательства полагающейся стороны не вызывают необходимость хранения данных. Это существенно снижает ответственность за обработку персональных данных, а также способствует актуальности и точности данных. Механизмы обнаружения также облегчают динамическую регистрацию и снятие с регистрации взаимосвязей в объединении. Динамическое обнаружение может поддерживать модель «принеси свои идентификационные данные» или модели персонального (аппаратного или облачного) хранилища данных в зависимости от конкретного подхода динамического обнаружения.

Деятельность по обнаружению, как и любой другой элемент системы управления идентификационными данными, может ограничиваться применимыми требованиями, например законами, предписаниями или политикой. Поставщики идентификационных данных и полагающиеся стороны должны быть способны поддерживать механизмы обнаружения других поставщиков идентификационных данных в объединении.

А.4.2 Обнаружение поставщика идентификационной информации

Обнаружение поставщика идентификационной информации представляет собой процесс нахождения в объединении поставщика идентификационной информации, который будет предоставлять идентификационную информацию для сущности. Этот процесс может быть следующим:

- пользователь дает ссылку на поставщика идентификационной информации, например, путем выбора из представленного перечня вариантов;
- пользователь дает подсказку, например, почтовый адрес, содержащий ссылку на поставщика идентификационной информации;
- пользователь предоставляет идентификатор, который распространяется среди всех поставщиков идентификационной информации, и один из них, знающий этот идентификатор, отзывается.

Возможен процесс, в котором пользователь выбирает поставщика идентификационной информации из списка поставщиков или из результатов автоматического обнаружения поставщика идентификационной информации при согласии пользователя предоставить такую информацию, как имя пользователя или почтовый адрес.

А.4.3 Обнаружение органа идентификационной информации

Обнаружение органа идентификационной информации представляет собой процесс поиска в объединении органа идентификационной информации, который подходит для аутентификации информации конкретного поставщика идентификационной информации. Процесс обнаружения позволяет использовать возможности, предоставляемые поставщиком идентификационной информации в объединении, для динамического поиска органа идентификационной информации с целью предоставления конкретного обязательного атрибута конкретной сущности. Данный процесс применяется, когда доступная идентификационная информация не указывает, какой орган идентификационной информации использовать.

На рисунке А.4 представлен пример основного диалога процесса обнаружения в контексте организации. Точная последовательность действий в процессе может в некоторой степени различаться в зависимости от целей и контекста объединения и для выполнения требований по обеспечению безопасности персональных данных и поддержке доверия должна включать дополнительные шаги получения согласия пользователя на передачу информации. Он также демонстрирует необходимость поддержки многочисленных поставщиков идентификационной информации.

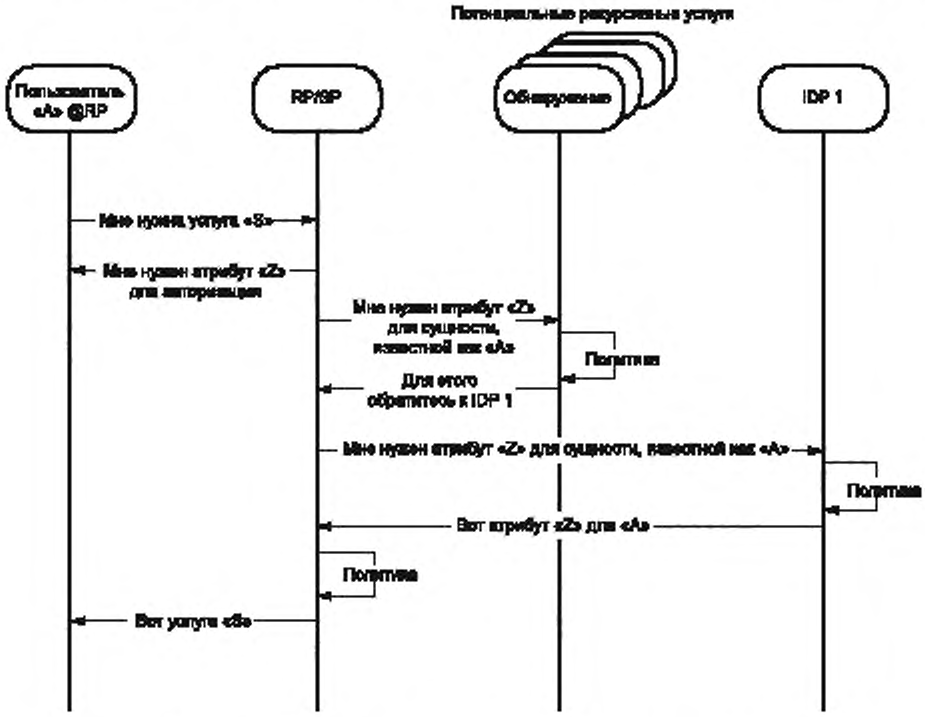

Рисунок А.4 — Пример основного диалога процесса обнаружения в объединении

Примечание — Например, процесс обнаружения органа идентификационной информации аналогичен процессу поиска атрибута, реализованному у поставщика идентификационной информации.

А.5 Вопросы, касающиеся сценариев межобъединений

Состав и структура объединения/объединений (межобъединения) приведены в А.2. Помимо соображений, относящихся к объединению, дополнительные соображения для межобъединения делятся на две категории: доверие и функциональная совместимость. В случаях, когда сущности с идентификационными данными в одном объединении может потребоваться доступ к услугам, предоставляемым другим объединением, должно быть достигнуто соглашение между объединениями, сформированное таким образом, чтобы, по крайней мере, у одного поставщика идентификационной информации в первом объединении были доверительные отношения с соответствующим поставщиком идентификационной информации в другом объединении. Функциональная совместимость между неоднородными объединениями (в каждом могут применяться разное программное обеспечение, разные платформы или разные варианты развертывания) требует строгого соблюдения согласованных зафиксированных политик и процедур, чтобы избежать дублирования идентификационных данных и идентификаторов и, как следствие — результирующих конфликтных ситуаций.

При разработке согласованных процедур для межобъединения необходимо учитывать следующие требования и условия:

- необходимо проанализировать политики и процедуры участвующих объединений чтобы убедиться в их согласованности и отсутствии расхождений;
- необходимо сравнить условия обслуживания и лицензионные соглашения для обеспечения уверенности в их согласовании и отсутствии проблем;
- должны быть реализованы механизмы разграничения доступа к информации для физических лиц, основанные на их идентичности в том или ином объединении должны быть однозначно определены, должны быть доступными и постоянно функционировать внутри объединения;
- следует определить меры для предотвращения подделки идентичности при ее передаче между объединениями;
- необходимо определить правила использования методов, улучшающих обеспечение безопасности персональных данных, например, анонимность или псевдонимность, а также получение согласия при осуществлении обмена идентификационной информацией в объединении;
- следует определить меры защиты информации для выполнения применимых требований, например, нормативных правовых актов, а также предписаний и политик различных объединений;
- должны быть определены способы контроля соответствия применимым требованиям, например законам, регламентам, политикам от различных объединений, особенно в контексте общей юрисдикции;
- необходимо проанализировать законы, регламенты и политики различных объединений из участвующих в объединении (особенно в юридической части) с целью обеспечения уверенности в их согласованности.

А.6 Угрозы и меры защиты информации

А.6.1 Общие положения

При достижении своих целей объединение идентичностей сталкивается с целым рядом угроз и рисков, вытекающих из информационной асимметрии между различными сторонами в отношении описанных выше соображений, характеристик и требований. Диапазон угроз применим в большей или меньшей степени в зависимости от контекста (например, организация или контекст, ориентированный на пользователя). Этапы жизненного цикла идентичности, применяющиеся к пользователям объединения, такие как подтверждение идентификационных данных, внесение в реестр, предоставление, аутентификация и авторизация, наряду с процессами, связанными с функционированием самого объединения, такими как включение участников в объединение, несут с собой неотъемлемые угрозы, которые требуют защиты для уменьшения и управления рисками.

Типовые угрозы аутентификации идентичности и авторизации, а также соответствующие меры противодействия угрозам представлены ниже.

А.6.2 Запрос аутентифицированных идентификационных данных

А.6.2.1 Общая информация

Когда пользователь запрашивает доступ к ресурсу, предоставляемому прикладной системой, прикладная система запрашивает аутентифицированную идентичность, содержащую атрибуты, требуемые ей для принятия решений о санкционировании доступа. Она также может запрашивать дополнительные атрибуты, которые необходимы для прикладного процесса. Для данного случая возможны следующие угрозы и применяются указанные меры защиты.

А.6.2.2 Неавторизированный запрос

Неавторизированный запрос также известен как подделка запроса. Нарушитель, выдающий себя за авторизованного пользователя приложения, подделывает запрос идентификационной информации.

Применяются следующие меры защиты информации: запрос должен быть подписан запрашивающей стороной.

При этом запрос может содержать чувствительную, с точки зрения защиты персональных данных, информацию, и соответственно, раскрытие его создает риск безопасности и угрозы персональным данным. В частности, раскрытие мандата может вызывать риск безопасности для всей системы.

Применяются следующие меры противодействия: аудитория запроса должна ограничиваться путем аутентификации адреса назначения или запрос должен шифроваться или передаваться по защищенному каналу.

А.6.2.3 Фальсификация запроса

При данной угрозе нарушитель модифицирует запрос идентификационной информации.

Применяются следующие меры противодействия: запрос должен быть защищен от нарушения целостности либо путем подписания запроса, либо аутентификации сообщения, либо передачей по защищенному каналу.

А.6.2.4 Подмена запроса

При этой угрозе происходит подмена запроса на другой запрос. Типичным примером такой угрозы является межсайтовая подделка запроса.

Применяются следующие меры противодействия: запрос должен быть криптографическими методами привязан к сеансам связи между приложением пользователя и запрашивающей стороной, а также между приложением пользователя и поставщиком идентификационной информации.

А.6.3 Санкционирование передачи атрибутов

А.6.3.1 Общая информация

Решение о санкционировании передачи атрибута может приниматься субъектом или политикой, устанавливаемой администратором домена. Для данного случая возможны следующие угрозы и применяются указанные меры противодействия.

А.6.3.2 Внедрение политики

Нарушитель может внедрить политику в механизм реализации политики через точку администрирования политики.

Применяются следующие меры противодействия: если сущность формирует политику, то сущность должна быть аутентифицирована и политика должна быть криптографическими методами привязана к сущности или применяемая политика должна быть аутентифицирована (защищена от подделок/подписана) или уязвимости приложений должны быть устранены (закрыты).

А.6.3.3 Перехват интерфейса доступа

Нарушитель перехватывает интерфейс доступа системы и управляет передачей атрибутов. Типичным примером такой атаки является кликджекинг (clickjacking).

А.6.3.4 Маскировка условий

Нарушитель прячет запрашиваемые атрибуты, их назначение и диапазон их распространения путем включения их в долгосрочное соглашение.

Применяются следующие меры противодействия: оператор объединения или другая сущность должны подтвердить соответствие запроса требованиям, установленным объединением.

А.6.4 Получение дополнительных атрибутов

С целью принятия решения о санкционировании и иной обработке ресурс может требовать дополнительных атрибутов. Они могут быть получены у поставщика идентификационной информации или органа идентификационной информации.

Для данного случая возможны вышеупомянутые угрозы и применяются аналогичные меры противодействия. В дополнение к ним могут применяться следующие меры защиты.

А.6.4.1 Контроль местонахождения органа идентификационной информации

Атрибут может быть доступен у нескольких органов идентификационной информации. Значение атрибута может у них различаться, и какое из них является верным, может определяться контекстом.

Применяются следующие меры противодействия: местонахождение органа идентификационной информации должно быть получено через поставщика идентификационной информации в контексте исходного запроса источника атрибутов.

А.6.4.2 Регистрация ресурсов

Требуемые атрибуты могут содержать конфиденциальную информацию. Ресурс, запрашивающий идентификационную информацию, может скомпрометировать эту конфиденциальность. От ресурса может требоваться выполнение определенных условий для получения требуемой информации.

Применяются следующие меры противодействия: регистрация ресурса, запрашивающего дополнительные атрибуты, должна быть выполнена прежде, чем может быть получена информация об источнике атрибутов.

А.7 Объединение органов идентификационной информации

Иногда требуется объединение идентификационной информации, имеющейся в различных достоверных источниках. Это обычно происходит при объединении двух организаций в объединенную организацию. Но перед объединением систем управления идентификационными данными двух различных доменов должны быть определены процедуры для разрешения несоответствий и, в частности, необходимо убедиться в том, что в результирующем домене:

- ссылочные идентификаторы являются уникальными;
- невозможно связать идентификационные данные с не той сущностью.

Для случая невыполнения данных условий должны существовать способы арбитражного разбирательства между поставщиками идентификационных данных, содержащими противоречащую идентификационную информацию.

Приложение Б
(справочное)

Практические приемы управления идентичностью с использованием мандатов на основе атрибутов для улучшения защиты персональных данных

Б.1 Общая информация

Система управления идентификационными данными может быть создана с использованием мандатов на основе атрибутов. Мандаты на основе атрибутов представляют собой ориентированный на пользователя подход в системе управления идентификационными данными, предназначенный для улучшения защиты персональных данных пользователя, но признающий также при этом многосторонние интересы всех сущностей.

Б.2 Действующие субъекты

Б.2.1 Обзор

Система управления идентификационными данными на основе атрибутов распознает следующих основных действующих субъектов:

- субъект, имеющий один или несколько мандатов, которые могут быть использованы для утверждения о том, что определенные атрибуты применимы при их представлении полагающейся стороне;
- полагающаяся сторона, которая принимает подтверждения из мандатов субъекта и доверяет органу, выпустившему мандат (поставщику идентификационной информации);
- поставщик идентификационной информации, который выпускает мандат(-ы) на основе атрибутов для субъекта, гарантируя правильность содержащейся в них информации;
- орган идентификационной информации, который отвечает за обеспечение уровня доверия идентификационной информации, предоставляемой полагающейся стороне.

На рисунке Б.1 представлен обзор действующих субъектов в рассмотренной архитектуре системы управления идентификационными данными.

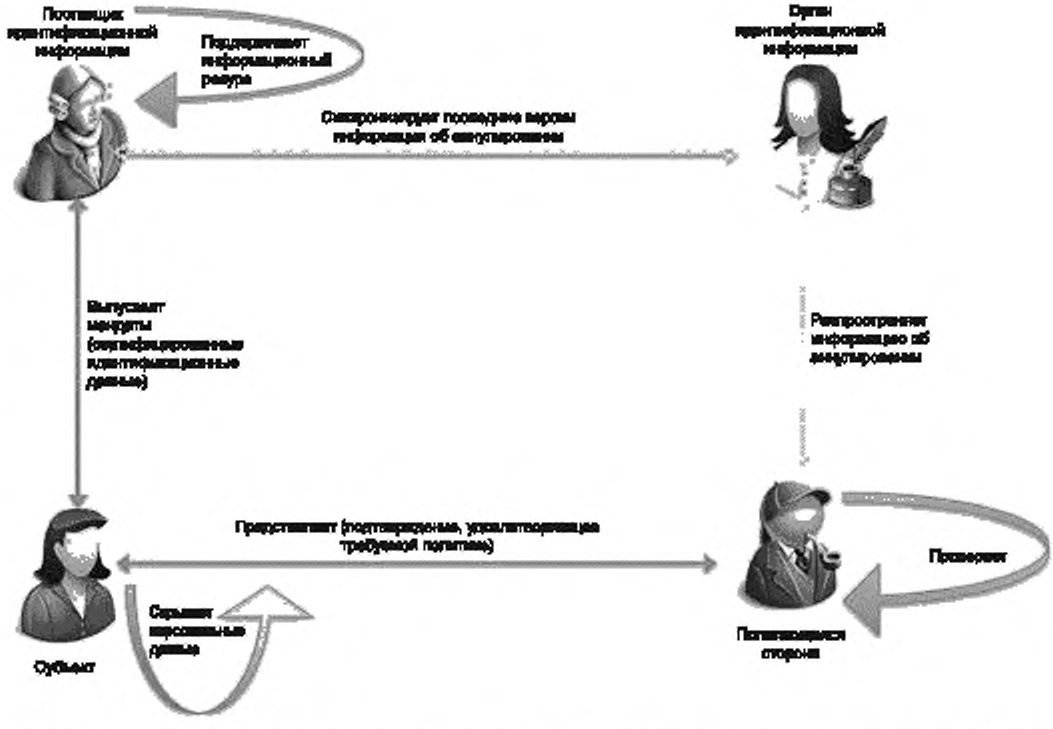

Рисунок Б.1 — Действующие субъекты архитектуры управления идентичностью с использованием мандатов на основе атрибутов и их взаимодействия

Б.2.2 Субъект

Субъект — это центральный действующий субъект в архитектуре, интересы которого включают:

- использование услуг, предлагаемых полагающейся стороной,
- сохранение анонимности при использовании услуг полагающейся стороны;
- наличие возможности оставаться несвязываемым при различных взаимодействиях с полагающейся стороной (избегать копирования);
- исключение связывания полагающейся стороной применения своей идентификационной информации с выпуском атрибутов органом идентификационной информации;
- возможность создавать псевдонимы всякий раз, когда ему хочется создать профиль для определенной полагающейся стороны.

Субъект оперирует устройством, называемым в этом приложении «токеном субъекта», которое содержит мандаты и способно осуществлять обмен с оборудованием, которым оперирует полагающаяся сторона.

Б.2.3 Полагающаяся сторона

Полагающаяся сторона — это поставщик услуг, предоставляющий услуги субъекту. При этом полагающаяся сторона имеет целью предоставление услуг только аутентифицированным субъектам. Полагающаяся сторона публикует политику представления услуг, где определяет условия, которым должны удовлетворять субъекты для аутентификации, чтобы пользоваться ее услугами.

Полагающаяся сторона поддерживает установленные отношения с органом идентификационной информации, чьи подтверждения она принимает.

Интересы полагающейся стороны включают следующее:

- принимаемая идентификационная информация должна быть гарантированно правильной;
- только орган идентификационной информации имеет возможность выпускать/обрабатывать подтвержденную идентификационную информацию о субъектах;
- уверенность, что субъект не может манипулировать подтвержденными значениями атрибутов;
- использование синхронизированной с органом идентификационной информации последней версии реестра идентичностей, чтобы контролировать полученные мандаты и препятствовать принятию любых недействительных (аннулированных) мандатов в качестве действительных.

Б.2.4 Поставщик идентификационной информации

Поставщик идентификационной информации — это компонент системы предоставляющий субъектам подтвержденную идентификационную информацию, которая должна быть представлена по мере необходимости субъектом.

Поставщик идентификационной информации гарантирует правильность и достоверность предоставленной информации.

Этот действующий субъект может:

- выпускать мандаты для одного или нескольких атрибутов субъекта;
- определять, что ранее предоставленная идентификационная информация некой идентичности больше не является действительной.

Мандат, содержащий идентификационную информацию, которая больше не действительна, аннулируется.

Б.2.5 Орган идентификационной информации

Задачи органа идентификационной информации состоят:

- в упреждающем предоставлении полагающимся сторонам информации об аннулированных мандатах, которое заключается в:
  - в синхронизации последней информации об аннулировании (признании недействительности) с поставщиком идентификационной информации;
  - в синхронизации версий реестра идентичностей;
- в распространении последней версии реестра идентичностей среди полагающихся сторон;
- в содействии по запросу полагающейся стороны в подтверждении достоверности мандата;
- в предоставлении информации, которая будет включена в мандат, для обеспечения подтверждения его достоверности.

Б.3 Этапы управления

Б.3.1 Общая информация

Системой управления идентификационными данными на основе атрибутов реализуются следующие этапы управления:

- выпуск мандата, связанного с предоставленными субъекту атрибутами;
- представление мандата, когда субъект требует взаимодействия с системой;
- признание недействительности мандата; когда атрибуты субъекта аннулируются.

Б.3.2 Выпуск мандата

Выпуск мандата представляет собой интерактивный протокол между токеном субъекта и поставщиком идентификационной информации. В результате выпуска мандата субъект становится обладателем одного или нескольких атрибутных мандатов, каждый из которых представляет идентификационную информацию, относящуюся к субъекту.

Атрибутный мандат состоит из следующей информации:

- описание типа атрибута;
- зашифрованного представления значения атрибута;
- параметров для криптографической проверки достоверности идентификационной информации;
- указателя органа идентификационной информации, предоставляющего идентификационную информацию, которая подтверждается мандатом.

Б.3.3 Предъявление мандата

На рисунке Б.2 показаны участвующие в реализации компоненты системы управления идентификационными данными и их взаимодействие. Предъявление — это процесс обмена данными между токеном субъекта и оборудованием полагающейся стороны, выполняемый при запросе доступа к услуге, предлагаемой полагающейся стороной.

Предъявление мандата начинается, когда токен субъекта получает от полагающейся стороны информацию с описанием политики его представления. Политика представления определяет:

- информацию, которая должна предоставляться полагающейся стороне, включая:
  - тип атрибута;
  - уровень раскрытия значения атрибута;
- механизмы аутентификации, которые будут использоваться для проверки достоверности значения атрибута;
- органы идентификационной информации, признанные полагающейся стороной как обеспечивающие безопасность при проверке достоверности.

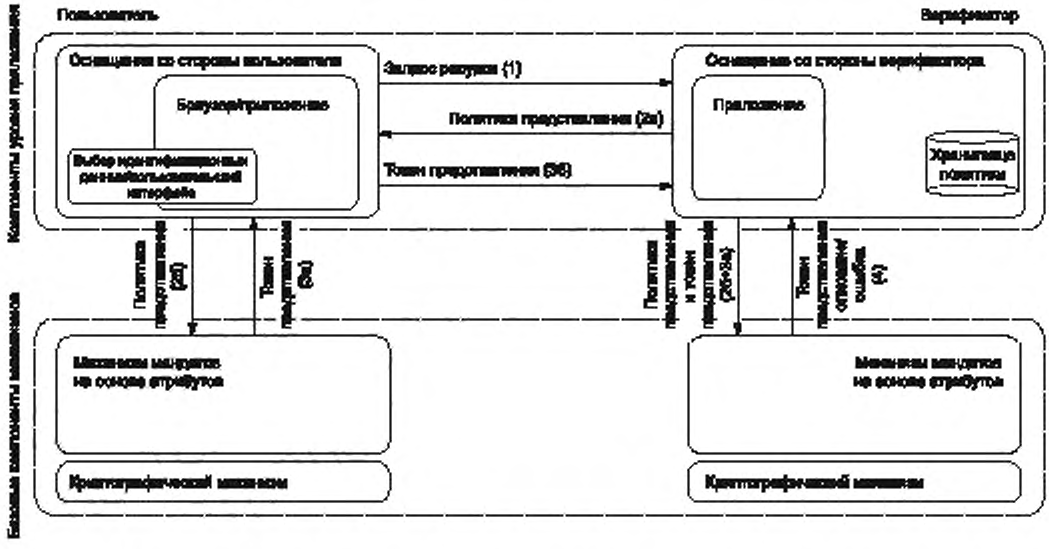

Рисунок Б.2 — Основные компоненты токена субъекта и оборудования полагающейся стороны

Со стороны токена субъекта процесс определяет, какие комбинации мандатов в его памяти будут удовлетворять политике полагающейся стороны, а в каких может потребоваться взаимодействие субъекта (в случае, если возможны различные комбинации, например, если субъект использует различные мандаты от разных поставщиков идентификационной информации). Затем субъект отправляет заполненный запрос полагающейся стороне в виде токена представления.

После получения токена представления полагающаяся сторона проверяет содержащиеся в нем утверждения на действительность (подлинные, полученные от одного из поставщиков идентификационной информации, которым она доверяет), а также то, являются ли они все еще актуальными.

Окончанием предъявления мандата будет результат верификации: «принять» или «отклонить» в зависимости от действительности токена представления.

Б.3.4 Признание недействительности мандата

В обязанности системы, использующей систему управления идентификационными данными, входит определение случаев, когда конкретные мандаты должны быть признаны недействительными (аннулированы). Это обычно происходит, когда определенные взаимосвязи субъекта с выпущенным мандатом (подтвержденной идентификационной информацией) не поддерживаются, например, в случаях нарушения субъектом условий использования, прекращения действия законного контракта между субъектом и поставщиком идентификационной информации и т. д.

В любом случае признание недействительности представляет собой важный процесс в жизненном цикле управления идентичностью с использованием мандатов на основе атрибутов. Когда атрибут становится недействительным, мандат, содержащий этот атрибут, также становится недействительным. При этом в вышеупомянутой архитектуре процесса будет выполнено обновление реестра идентичностей поставщиком идентификационной информации, тем самым прекращая действие ранее выпущенных мандатов. Затем это обновление будет синхронизировано с органом идентификационной информации.

Б.4 Уровни и компоненты архитектуры

Б.4.1 Общая информация

Сущности в системе управления идентификационными данными с мандатами на основе атрибутов могут иметь особые функциональные компоненты, необходимые для их взаимодействия с системой. Архитектура системы управления идентификационными данными с мандатами на основе атрибутов определяет для каждой сущности функциональные компоненты, необходимые для работы с мандатами на основе атрибутов. На рисунке Б.2 представлен обзор функциональных компонентов со стороны субъекта и полагающейся стороны, а более подробное представление компонентов со стороны субъекта показано на рисунке Б.3.

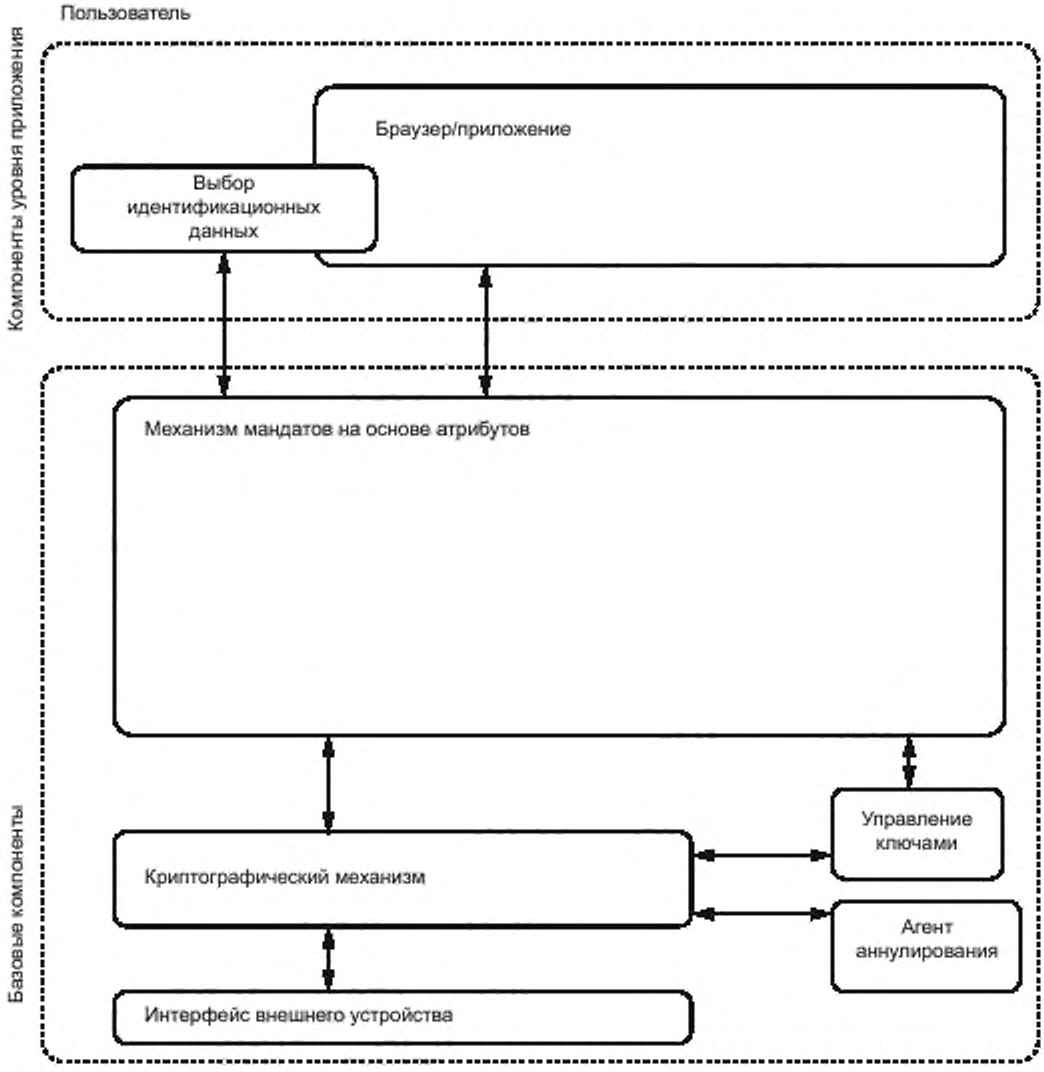

Рисунок Б.3 — Архитектура токена субъекта

Функциональные компоненты каждой стороны могут быть представлены на двух основных уровнях: уровень приложения и базовые компоненты — уровень генерации/верификации подтверждения.

Б.4.2 Уровень приложения

Уровень приложения не является частью архитектуры защиты персональных данных с использованием мандатов на основе атрибутов, но будет действовать поверх нее. Условно этот уровень содержит все компоненты прикладного уровня, которые в случае развертывания со стороны пользователя (субъекта) включают основное приложение и компонент «Выбор идентификационных данных» (см. описание ниже). Уровень приложения со стороны проверяющих и издателей будет также содержать хранилище политики и механизм управления доступом.

Компонент «Выбор идентификационных данных» обеспечивает методы, возможно представленные графическим пользовательским интерфейсом, для поддержки пользователя при выборе предпочтительной комбинации мандата и/или псевдонимов (если существуют разные возможности), удовлетворяющей политике представления. Кроме того, пользовательский интерфейс используется для получения согласия пользователя при раскрытии персональных данных.

Б.4.3 Базовые компоненты — уровень генерации/верификации подтверждения

Б.4.3.1 Общие положения

Уровень подтверждения содержит механизм мандатов на основе атрибутов и специальные компоненты лежащей в его основе технологии, как изображено на рисунке Б.3.

Механизм мандатов на основе атрибутов содержит все технологически независимые методы и функциональные компоненты системы управления идентификационными данными, базирующейся на мандатах на основе атрибутов. Он содержит функции для осуществления анализа полученной политики представления, выбора применимых мандатов для данной политики или запуска характерной для механизма генерации или верификации криптографических свидетельств. Верхний уровень (развертывание) затем взаимодействует с таким же уровнем со стороны другой сущности (полагающейся стороны или поставщика идентификационной информации).

Механизм мандатов на основе атрибутов активируется уровнем приложения и вызывает другие компоненты, как показано на рисунке Б.3:

- криптографический механизм;
- управление ключами;
- агент аннулирования;
- хранилище политики;
- интерфейс внешнего устройства.

Б.4.3.2 Криптографический механизм

Криптографический механизм представляет собой первый компонент, который вызывается механизмом мандатов на основе атрибутов для характерных для механизма криптографических данных. Он обеспечивает общие интерфейсы для генерации требуемой криптографической информации, например создания, представления, верификации или инспектирования токена представления/выпуска. Он обеспечивает реализацию криптографических функций, таких как создание электронной подписи, проверка электронной подписи, выработка общего ключа, доказательство с нулевым разглашением и т. д.

Б.4.3.3 Управление ключами

Компонент «Управление ключами» оперирует криптографическими ключами всех сторон и поддерживает их актуальность (в рамках управления жизненным циклом ключей). При вводе идентификатора для ключа, он возвращает криптографический ключ(и) (или их перечень), являющийся в данное время действительным для данного идентификатора. Данный компонент обеспечивает получение текущей (общедоступной) информации об аннулировании, которая необходима для поддержания актуальности мандатов и проверки того, является ли полученный токен представления все еще действительным.

Б.4.3.4 Агент аннулирования

Компонент «Агент аннулирования» управляет взаимодействием между криптографическим механизмом и органом, выполняющим аннулирования, для генерации или представления токенов/мандатов, которые подлежат аннулированию (признание недействительности). Конкретный шаблон взаимодействия зависит от конкретных механизмов аннулирования, которые могут быть выбраны.

Б.4.3.5 Интерфейс устройства

Компоненты «Интерфейсы устройства» предоставляют необязательные общие интерфейсы, облегчающие интеграцию внешних устройств, таких как смарт-карты, как для «аутсорсинга» вычислений, так и для получения данных, хранящихся на внешнем устройстве. Интеграция внешнего устройства может быть, например, необходима, если требуется привязка ключа к смарт-карте.

Б.4.3.6 Хранилище политики

Со стороны полагающейся стороны хранилище политик хранит политики представления, принятые сущностью, и может также сохранять полученные токены представления с целью архивирования или иных, связанных с обеспечением безопасности целей (см. рисунок Б.3).

Библиография

[1] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»

[2] ISO/IEC TS 29003:2018 Информационные технологии. Методы и средства обеспечения безопасности. Подтверждение идентичности (Information technology — Security techniques — Identity proofing)

УДК 006.354:004.056.5:006.354 ОКС 35.030

Ключевые слова: атрибут, идентификатор, идентификационная информация, идентификационные атрибуты, идентичность, управление идентичностью, система управления идентификационными данными

Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 24.05.2021. Подписано в печать 01.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 3,34.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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