

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1251

(09/2009)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность киберпространства – Управление
определением идентичности

**Структура осуществляемого пользователем
управления в отношении цифровой
идентичности**

Рекомендация МСЭ-Т X.1251

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.379
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т Х.1251

Структура осуществляемого пользователем управления в отношении цифровой идентичности

Резюме

В Рекомендации МСЭ-Т Х.1251 определяется структура для расширения возможностей пользователей по управлению и обмену информацией, связанной с их цифровой идентичностью. В этой Рекомендации также определяются требования пользователя и функциональные требования к обмену информацией, касающейся цифровой идентичности. Эта работа включает обеспечение пользователя возможностью управлять предоставлением информации, позволяющей установить личность.

Источник

Рекомендация МСЭ-Т Х.1251 была утверждена 25 сентября 2009 года 17-й Исследовательской комиссией МСЭ-Т (2009–2012 гг.) в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

Ключевые слова

Цифровой договор, цифровая идентичность, клиент цифровой идентичности, идентичность, взаимный обмен информацией об идентичности, управление определением идентичности, сервер идентичности.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения Исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ получил извещение об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: <http://www.itu.int/ITU-T/ipr/>.

© ITU 2010

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

	Стр.
1 Сфера применения	1
2 Справочные документы	1
3 Определения	1
3.1 Термины, определенные в других документах.....	1
3.2 Термины, определенные в настоящей Рекомендации	2
4 Сокращения и акронимы	3
5 Условные обозначения	3
6 Общие возможности	4
6.1 Возможности пользователя	4
6.2 Функциональные возможности.....	4
6.3 Руководящие указания по обеспечению безопасности	5
7 Расширенные возможности пользователей по управлению взаимным обменом информацией о цифровой идентичности	5
7.1 Введение.....	5
7.2 Угрозы безопасности	6
7.3 Концептуальная модель взаимного обмена информацией о цифровой идентичности	6
7.4 Цифровой договор.....	8
7.5 Три уровня взаимного обмена информацией о цифровой идентичности.....	9
8 Структура взаимного обмена информацией о цифровой идентичности	10
8.1 Принципы разработки.....	10
8.2 Элементы структуры.....	11
Дополнение I – Справочное руководство по реализации структуры управления цифровой идентичностью со стороны, с использованием спецификации WS-Trust и технологии информационной карточки	14
I.1 Введение.....	14
I.2 Справочная информация	14
I.3 Возможности DIIF	15
Библиография	18

Структура осуществляемого пользователем управления в отношении цифровой идентичности

1 Сфера применения

В настоящей Рекомендации определяется структура для расширения возможностей пользователей по управлению и обмену информацией, связанной с их цифровой идентичностью.

В этой Рекомендации также определяются возможности обмена информацией, касающейся цифровой идентичности. Эта работа включает обеспечение пользователя возможностью управлять предоставлением информации, позволяющей установить личность.

ПРИМЕЧАНИЕ. – Использование термина "идентичность" в данной Рекомендации, касающейся управления определением идентичности (IdM), не указывает на его абсолютное значение. В частности, этот термин не обозначает какого-либо положительного результата установления личности.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статуса Рекомендации.

[ITU-T X.1205] Рекомендация МСЭ-Т X.1205 (2008 г.), *Обзор кибербезопасности*.

[ITU-T X.1250] Recommendation ITU-T X.1250 (2009), *Baseline capabilities for enhanced global identity management and interoperability*.

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах:

3.1.1 регистрационные данные (credential) [b-ITU-T X.1252]: Набор данных, представляемых как доказательство утверждаемой идентичности и/или прав.

3.1.2 объект (entity) [b-ITU-T X.1252]: Все, что существует отдельно и обособленно и может быть определено в контексте.

ПРИМЕЧАНИЕ. – Объектом может быть физическое лицо, животное, юридическое лицо, организация, активный или пассивный предмет, устройство, применение программного обеспечения, услуга и т. п., или группа таких лиц. В контексте электросвязи примерами объектов являются точки доступа, абоненты, пользователи, сетевые элементы, сети, применения программного обеспечения, услуги и устройства, интерфейсы и т. п.

3.1.3 федерация (federation) [b-ITU-T X.1252]: Ассоциация пользователей, поставщиков услуг и поставщиков услуг определения идентичности.

3.1.4 идентификатор (identifier) [b-ITU-T X.1252]: Один или несколько атрибутов, используемых для идентификации объекта в том или ином контексте.

¹ Эта Рекомендация может быть неприменима в некоторых странах вследствие их национального законодательства.

3.1.5 идентичность (identity) [b-ITU-T X.1252]: Представление какого-либо объекта в виде одного или нескольких элементов информации, которые позволяют однозначно распознать объекты в каком-либо контексте в той мере, в какой это необходимо. В целях IdM термин "идентичность" толкуется как контекстуальная идентичность (подмножество атрибутов), т. е. разнообразие атрибутов ограничивается рамками с определенными граничными условиями (контекстом), в которых объект существует и взаимодействует.

ПРИМЕЧАНИЕ. – Каждый объект представлен одной целостной идентичностью, которая включает все возможные элементы информации, характеризующие такой объект (атрибуты). Вместе с тем такая целостная идентичность является теоретическим понятием и не может быть описана и практически использована, поскольку число всех возможных атрибутов бесконечно.

3.1.6 управление определением идентичности (identity management) [b-ITU-T Y.2720]: Набор функций и возможностей (например, администрирование, управление и техническое обслуживание, обнаружение, обмен сообщениями, сопоставление и увязка, обеспечение реализации политики, аутентификация и утверждение), используемых для:

- гарантирования информации, подтверждающей идентичность (например, идентификаторов, регистрационных данных, атрибутов);
- гарантирования идентичности объекта (например, пользователей/абонентов, групп, устройств пользователей, организаций, поставщиков доступа к сети и поставщиков услуг, сетевых элементов и объектов, а также виртуальных объектов); и
- обеспечения коммерческих приложений и приложений безопасности.

3.1.7 поставщик услуг определения идентичности (identity service provider) (IdSP) [b-ITU-T X.1252]: Объект, который выполняет верификацию, поддерживает информацию об идентичности других объектов, управляет ею и может ее создавать и назначать.

3.1.8 информация, позволяющая установить личность (personally identifiable information, ПИ) [b-ITU-T Y.2720]: Информация, относящаяся к любому человеку, которая позволяет идентифицировать его личность (включая информацию, позволяющую идентифицировать человека, если она используется в сочетании с другой информацией, даже если эта информация не позволяет четко определить личность).

3.1.9 полагающаяся сторона (relying party) [b-ITU-T Y.2720]: Объект, который полагается на представленную или заявленную идентичность запрашивающего/утверждающего объекта в каком-либо контексте запроса.

3.1.10 пользователь (user) [b-ITU-T X.1252]: Любой объект, использующий ресурс, например систему, оборудование, оконечное оборудование, процесс, приложение или корпоративную сеть.

3.1.11 ориентированная на пользователя (user-centric) [b-ITU-T X.1252]: Система IdM, при которой пользователю предоставляется право контролирования и обеспечения соблюдения различных видов политики конфиденциальности и безопасности, определяющих обмен между объектами информацией об идентичности, в том числе информацией ПИ.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины:

3.2.1 круг доверия (circle of trust): Набор критериев, установленных для объединения организаций в федерацию в целях доверенного доступа к ресурсам друг друга. Следует отметить, что круг доверия представляет собой также конечный результат объединения организаций в федерацию.

3.2.2 цифровой договор (digital contract): Договор, заключаемый в цифровой форме и подписываемый двумя объектами, между которыми достигнуто соглашение.

3.2.3 цифровая идентичность (digital identity): Цифровое представление известной информации о конкретном человеке, группе или организации.

3.2.4 клиент цифровой идентичности (digital identity client): Клиентская программа, которая обеспечивает аутентификацию, управление регистрационными данными и взаимный обмен информацией об идентичности, а также предоставляет пользователю услугу защиты конфиденциальности.

3.2.5 мошенничество с идентичностью (identity fraud): Преступление, при котором самозванец получает ключевые элементы информации, позволяющей установить личность (ПИ), такие как номера социального страхования и номера водительского удостоверения, и использует их для своей личной выгоды.

3.2.6 информация об идентичности (identity information): Информация, служащая для идентификации пользователя, в том числе доверенные (создаваемые сетью) и/или недоверенные (создаваемые пользователем) адреса.

3.2.7 взаимный обмен информацией об идентичности (identity interchange): Процесс распространения информации об идентичности пользователя между поставщиком услуг определения идентичности и полагающейся стороной с помощью клиента цифровой идентичности.

3.2.8 селектор идентичности (identity selector): Относящийся к клиенту цифровой идентичности программный компонент, который находится в распоряжении пользователя и с помощью которого пользователь управляет своей цифровой идентичностью и осуществляет ее передачу.

3.2.9 сервер идентичности (identity server): Сервер, который управляет регистрационными данными пользователя и информацией об идентичности пользователя и предоставляет их клиенту цифровой идентичности.

3.2.10 синхронизация идентичности (identity synchronization): Процесс обновления информации об идентичности пользователя, передаваемой полагающейся стороне, в случае если у поставщика услуг определения идентичности произошло изменение источника информации об идентичности.

3.2.11 прекращение использования идентичности (identity termination): Процесс удаления информации об идентичности пользователя из запоминающего устройства по истечении срока ее действия.

3.2.12 метка идентичности (identity token): Модель данных для цифровой идентичности, которая может содержать информацию о ПИ и регистрационных данных пользователя.

3.2.13 фишинг (phishing): В соответствии с уголовным законодательством мошеннический процесс покушения на получение защищаемой информации, например имен пользователей, паролей и данных о кредитных картах, путем выдачи себя в процессе электронного общения за объект, заслуживающий доверия.

3.2.14 политика конфиденциальности (privacy policy): Заявление о политике, в котором определяются правила защиты доступа к конфиденциальной информации личного характера и ее распространения.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие аббревиатуры:

CoT	Circle of Trust	Круг доверия
DIC	Digital Identity Client	Клиент цифровой идентичности
DIIF	Digital Identity Interchange Framework	Структура взаимного обмена информацией о цифровой идентичности
IdM	Identity Management	Управление определением идентичности
IdS	Identity Server	Сервер идентичности
IdSP	Identity Service Provider	Поставщик услуг определения идентичности
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PKI	Public Key Infrastructure	Инфраструктура открытого ключа
RP	Relying Party	Полагающаяся сторона
SP	Service Provider	Поставщик услуги
XML	eXtensible Markup Language	Расширяемый язык разметки, язык XML

5 Условные обозначения

Нет.

6 Общие возможности

В настоящей Рекомендации определяется следующий набор возможностей. Возможности, которые установлены в изложенных ниже разделах, касающихся требований пользователя и функциональных требований, являются обязательными, если не указано, что они являются необязательными.

6.1 Возможности пользователя

В целях удовлетворения возможностей пользователя должны выполняться следующие условия:

- 1) Поддержка механизмов взаимной аутентификации.
- 2) Предоставление согласованного интерфейса для аутентификации, поддерживающего различные механизмы аутентификации с использованием клиента цифровой идентичности (DIC).
- 3) Предоставление селектора идентичности, который позволяет пользователю делать выбор в отношении того, какие регистрационные данные предполагается использовать для аутентификации. Выбор регистрационных данных, подлежащих использованию для аутентификации, может также ограничиваться рядом требований, накладываемых веб-сайтом. Для удобства пользователя выбор метода аутентификации и связанных с ним регистрационных данных может также делегироваться поставщику услуг определения идентичности (пользователь может выбирать лишь поставщика услуг определения идентичности, а не определенные конкретные регистрационные данные у этого поставщика услуг определения идентичности, подлежащие использованию при аутентификации).
- 4) Предоставление интуитивно понятного и согласованного интерфейса для управления его/ее информацией о регистрационных данных при обеспечении максимальной безопасности.
- 5) Поддержка веб-сайтом механизма автозаполнения при регистрации или подписке, с тем чтобы свести к минимуму взаимодействие пользователя с сайтом, включая возможность для пользователя полностью управлять подключением и отключением такого механизма. Данное требование является необязательным.
- 6) Предоставление информации об идентичности в любое время по желанию пользователя и обеспечение возможности для пользователя полностью управлять взаимным обменом информацией об идентичности с использованием механизма надлежащей защиты конфиденциальности.
- 7) Обеспечение автоматического обновления совместно используемой информации об идентичности при изменении первоначального источника под его/ее полным управлением.
- 8) Предоставление возможности полного осуществляемого пользователем управления применительно к установлению политик безопасности и конфиденциальности и обеспечению их соблюдения, с тем чтобы управление взаимным обменом информацией об идентичности осуществлялось до совместного использования информации об идентичности. Это позволит пользователю непосредственно воздействовать на процессы установления политики и обеспечения ее соблюдения.
- 9) Предоставление пользователям возможности подробно просматривать информацию об идентичности, которую они совместно используют с каждым объектом.
- 10) Поддержка возможности управления сеансом аутентификации, позволяющей избежать необходимости для пользователя систематически осуществлять повторную аутентификацию у поставщика услуг определения идентичности, с тем чтобы получить доступ к веб-сайтам.

6.2 Функциональные возможности

Применительно к структуре взаимного обмена информацией о цифровой идентичности функциональные возможности определяются следующим образом. Они требуются для предоставления минимального набора функций, необходимых структуре взаимного обмена информацией о цифровой идентичности.

- 1) Поддержка комплексного управления регистрационными данными, с помощью которого можно управлять информацией о регистрационных данных пользователя, необходимых для аутентификации.
- 2) Поддержка управления звеном взаимного обмена информацией об идентичности для предоставления пользователю всестороннего представления об объектах, с которыми имеет соединения этот пользователь для осуществления взаимного обмена информацией об идентичности.
- 3) Поддержка многих механизмов аутентификации, которые могут включать аутентификацию на основе пароля, PKI и биометрических данных.
- 4) Поддержка механизмов взаимного обмена информацией об идентичности, которые могут обеспечить двустороннюю связь для совместного использования информации об идентичности пользователя между объектами при помощи клиента DIC.
- 5) Поддержка механизма цифрового договора с целью создания договора о взаимном обмене информацией об идентичности, который должен использоваться для обеспечения соблюдения политики безопасности и конфиденциальности при предоставлении РИ.

- 6) Поддержка синхронизации информации об идентичности с целью последовательного обновления распределенной и совместно используемой информации об идентичности, в случае когда меняется источник распространяемой информации об идентичности. Подлежащая синхронизации информация об идентичности ограничивается РИ, которая изменяется непосредственно пользователем.
- 7) Поддержка преобразования универсальной метки с целью реализации структуры, функционально совместимой с существующими системами управления определением идентичности.
- 8) Обеспечение того, чтобы структура была в максимально возможной степени независима от процесса аутентификации, с тем чтобы избежать появления зависимости между DIC и поддерживаемыми механизмами аутентификации у поставщиков услуг определения идентичности (либо по меньшей мере обеспечение того, чтобы структура могла свободно поддерживать все механизмы аутентификации, в особенности механизмы, характерные для операторов электросвязи).
- 9) Поддержка механизмов, позволяющих поставщику услуг определения идентичности взаимодействовать с пользователем в процессе аутентификации и предоставлять свой собственный интерфейс для аутентификации (графический интерфейс пользователя, GUI).
- 10) Поддержка функции хранения меток идентичности на различных носителях (USB-ключках, SIM-картах, сетевых устройствах хранения и т. д.) при строго определенном уровне хранения, который должен использоваться DIC.

6.3 Руководящие указания по обеспечению безопасности

Ниже приводятся следующие руководящие указания по обеспечению безопасности, которые рекомендуется использовать при создании защищенной структуры DIIF:

- Безопасность общения в DIIF зависит от лежащей в его основе модели доверия, которая, как правило, базируется на инфраструктуре управления ключами (например, PKI или секретный ключ).
- Для обеспечения целостности и конфиденциальности данных (например, с помощью шифрования) при передаче сообщения по сети следует использовать некоторые виды протоколов безопасности на транспортном уровне.
- При подписании цифрового договора сторонами, достигающими соглашения, следует использовать цифровую подпись; при необходимости возможно применение шифрования договора.
- При хранении данных, которые содержат информацию об идентичности и хранятся в DIC, следует использовать цифровую подпись и шифрование.
- В связи с тем что пользователю предоставляется возможность перемещать свою метку идентичности с одного устройства на другое, должна применяться политика, обеспечивающая безопасность данных при их перемещении.

7 Расширенные возможности пользователей по управлению взаимным обменом информацией о цифровой идентичности

7.1 Введение

Федерация идентичности [b-LA-FF] была создана для передачи распределенной информации об идентичности между поставщиком услуг определения идентичности (IdSP) и поставщиком услуг (SP). Если SP хочет гарантировать подлинность информации об аутентификации, полученной от IdSP, то между двумя сторонами должны существовать отношения доверия. Этот домен доверия называется кругом доверия (CoT), который может включать одного или нескольких IdSP и SP. Если в круге доверия у IdSP происходит аутентификация пользователя, то доступ к поставщикам услуг из этого круга доверия разрешается без дополнительной аутентификации. Таким образом, в круге доверия пользователю необходимо пройти аутентификацию лишь однажды.

Однако по мере роста количества CoT возрастает количество процедур аутентификации, которые должен пройти пользователь. В этой ситуации пользователь вынужден проходить аутентификацию при каждом посещении CoT. Это означает, что пользователю необходимо управлять информацией о регистрационных данных, передаваемой от IdSP из CoT. Часто случается, что пользователь забывает пароль или записывает его, тем самым увеличивая риск несанкционированного раскрытия содержания. Федерация в рамках CoT обеспечивает удобный способ обмена информацией об идентичности пользователя. Однако для совместного использования информации об идентичности несколькими CoT предварительно требуется заключить деловое соглашение. Как правило, на завершение необходимо много времени в связи с задействованными юридическими процедурами. Если домен управления определением идентичности ограничивается рамками предприятия, то технология федерации обеспечивает решение, которое можно эффективно и действенно выполнить. Однако в случае если домен, на который рассчитана система управления определением идентичности (IdM), распространяется на интернет, то достижение деловых соглашений между предприятиями, входящими во все федерации, является трудновыполнимой задачей.

Возможно, что в крупномасштабных системах IdM, ориентированных на приложение, услуги и политика, касающиеся идентичности, рассчитаны на то, чтобы удовлетворять требованиям к поставщикам услуг определения идентичности и к поставщикам услуг, и оптимизированы под требования приложений, т. е. под предоставление информации об учетной записи пользователей. При предоставлении пользователю услуги на основе идентичности обмен информацией об идентичности, как правило, осуществляется непосредственно между тем или иным IdSP и SP. В этом случае пользователь имеет ограниченную возможность управления применительно к распространению информации о своей идентичности.

Поскольку информация об идентичности передается в обоих направлениях между объектами предприятия без вмешательства пользователя, вопросы безопасности и защиты конфиденциальности могут быть оставлены без внимания. Проблема появляется из-за того, что два объекта пытаются совместно использовать информацию об идентичности пользователя, которая принадлежит пользователю. Поскольку эти два объекта работают с идентичностью пользователя, они должны иметь предварительное деловое соглашение и соглашение о политике конфиденциальности. Если объекту требуется использовать идентичность пользователя совместно лишь с ее первоначальным владельцем, то каждый объект должен заключить соглашение и установить политику безопасности и конфиденциальности с этим владельцем для использования его/ее информации об идентичности (или с объектом, который управляет определением его/ее идентичности).

Для того чтобы решить эту проблему, в настоящей Рекомендации определяется структура для расширения возможностей пользователя по осуществлению управления при обмене информацией, связанной с цифровой идентичностью пользователя.

7.2 Угрозы безопасности

Весьма вероятно, что большинство возникающих в киберпространстве угроз, за исключением тех, в отношении которых принимаются надлежащие меры, существует в системах IdM. Общие угрозы безопасности в киберпространстве описаны в [ITU-T X.1205].

В системах IdM существуют различные угрозы безопасности, которые делают систему уязвимой или приводят к нарушению безопасности, что подвергает организацию риску. Наиболее распространенным видом угроз безопасности, существующих в условиях IdM, является мошенничество с идентичностью.

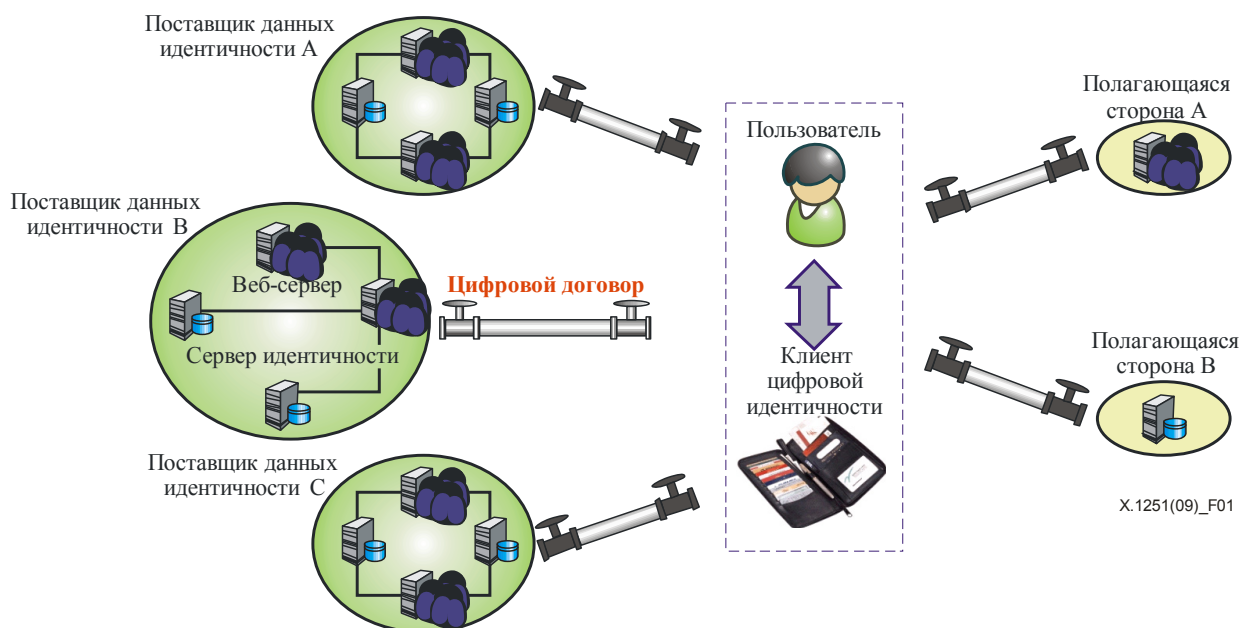
Мошенничество с идентичностью является чрезвычайно острым вопросом, связанным с безопасностью, в частности для организаций, занимающихся хранением и управлением использованием больших объемов информации, позволяющей установить личность. Раскрытие конфиденциальной информации, приводящее к потере личных данных, может не только подорвать доверие клиентов и общее доверие к организации и нанести ощутимый удар по ее репутации, но и вылиться для организаций в серьезные финансовые потери в связи с нарушением защиты данных. В настоящее время мошенничество с идентичностью может иметь форму фишинга.

Фишинг представляет собой попытку третьих лиц получить конфиденциальную информацию от частного пользователя, группы или организации, имитируя или подделывая конкретный, как правило, хорошо известный бренд, обычно для получения финансовой выгоды. Веб-сайт фишинга – это сайт, созданный как имитация законного веб-сайта той организации, бренд которой подделывается. Злоумышленник пытается спровоцировать пользователей на раскрытие личных данных, таких как номера кредитных карт, реквизиты онлайн-банковских данных и другой защищаемой информации, которую он/она может затем использовать для совершения мошеннических действий. В системах IdM фишинг представляет собой серьезную угрозу, поскольку информация об аутентификации жертвы или другая информация, позволяющая установить личность – при захвате злоумышленником, могут быть использованы для кражи идентичности или в другой мошеннической деятельности.

7.3 Концептуальная модель взаимного обмена информацией о цифровой идентичности

В этой концептуальной модели для структуры взаимного обмена информацией о цифровой идентичности (DIF) используется концепция клиента цифровой идентичности (DIC), который может управлять взаимным обменом информацией о цифровой идентичности. Право, которое предоставляется пользователю, с тем чтобы он управлял предоставлением информации об идентичности, может существенно ослабить влияние угроз безопасности, которые описаны в пункте, посвященном этим угрозам (см. пункт 7.2).

На рисунке 1 показана концептуальная модель взаимного обмена информацией о цифровой идентичности.



X.1251(09)_F01

Рисунок 1 – Концептуальная модель взаимного обмена информацией о цифровой идентичности

7.3.1 Сервер идентичности

Сервер идентичности (IdS) является главным сервером, который предоставляет информацию об идентичности пользователя запрашивающему объекту или запрашивает у DIC информацию об идентичности для веб-услуг. IdS может быть поставщиком услуг определения идентичности, если он предоставляет информацию об идентичности; в ином случае он может быть полагающейся стороной (PR), если он использует информацию об идентичности, предоставляемую пользователем. Не исключено, что IdS может одновременно выступать как в роли поставщика услуг определения идентичности, так и в роли полагающейся стороны. В этом случае IdS распространяет информацию о собственной идентичности для некоторых веб-услуг и наряду с этим требует предоставить информацию об идентичности пользователя для ряда других веб-услуг. Веб-сервер может затребовать от IdS информацию об идентичности пользователя для предоставления ему веб-услуг.

7.3.2 Клиент цифровой идентичности

Клиент цифровой идентичности – это программа, которая предоставляет пользователю услуги управления аутентификацией, регистрационными данными и сеансами, взаимного обмена информацией об идентичности и защиты конфиденциальности. Если информации об идентичности должна использоваться совместно с IdSP или с PR, то DIC устанавливает связь с IdS в домене. DIC может заключить с IdS договор, в котором описаны условия предоставления услуги взаимного обмена информацией об идентичности, с тем чтобы расширить возможности, связанные с безопасностью обмена информацией об идентичности. Информация об идентичности каждого пользователя проходит через DIC, поэтому данный рассматриваемый пользователь может управлять совместным использованием своей информации об идентичности. В частности, в зависимости от политики, согласованной между пользователем и объектом, пользователь полностью управляет тем, какие данные об идентичности, в какой момент времени, для какой цели и какому объекту передаются. Раскрытие информации об идентичности пользователя не является необходимым, поскольку клиент имеет о соединении всю информацию, необходимую для запроса и получения информации об идентичности.

7.3.3 Поставщик услуг определения идентичности

Поставщик услуг определения идентичности (IdSP) является объектом, который управляет информацией об идентичности пользователя, предоставляет услуги аутентификации и авторизации и услуги взаимного обмена информацией об идентичности для веб-серверов. IdSP представляет собой концептуальную модель роли, которая может быть присвоена объекту, обеспечивающему управление определением идентичности пользователя и предоставляющего эту информацию клиенту DIC, когда тот ее запрашивает. IdSP управляет информацией об идентичности, которая представляется пользователем или создается им самим.

7.3.4 Полагающаяся сторона

Полагающаяся сторона (PR) является еще одной концептуальной моделью роли, присваиваемой объекту, который запрашивает идентичность пользователя у клиента DIC и предоставляет услуги с использованием полученной информации об идентичности. Полагающаяся сторона не использует поставщика услуг определения идентичности для аутентификации. Пользователь использует клиент DIC, для того чтобы PR могла его аутентифицировать.

7.3.5 Пользователь

Определение пользователя приводится в пункте 3. В концептуальной модели под пользователем, как правило, понимается человек или абонент в контексте системы IdM, ориентированной на пользователя. Пользователь – это конечный пользователь, который владеет клиентом DIC или использует его.

7.4 Цифровой договор

Информация, позволяющая установить личность (РП), передаваемая между поставщиком услуг определения идентичности и полагающейся стороной, должна проходить через клиента цифровой идентичности в среде управления определением идентичности, ориентированной на пользователя. Это дает пользователю возможность управлять использованием своей РП. Цифровой договор заключается только между пользователем и поставщиком IdSP, либо между пользователем и полагающейся стороной. Заключение многосторонних договоров не допускается, поскольку это может усложнить вопросы управления, которые требуется решать пользователю. Цифровой договор является базовым компонентом, который может предоставить пользователю возможность точного управления потоками РП. На рисунке 2 показана структура цифрового договора.



Рисунок 2 – Структура цифрового договора

Виды управления, которые могут быть определены с помощью цифровых договоров, включают в себя некоторые правила, необходимые для урегулирования взаимоотношений в процессе взаимного обмена информацией об идентичности. Цифровой договор, основанный на нормативных правовых актах или других требованиях в отношении политики, может требоваться не для каждого взаимного обмена информацией об идентичности. Он необходим только тогда, когда нужно управлять потоком или кэшированием совместно используемой РП. Данный компонент является таким же гибким и расширяемым, как и договоры в реальном мире (например, соглашения о неразглашении). Кроме того, поскольку цифровые договоры могут быть документами формата XML, то они могут сами управлять своим пересмотром, внесением правок и аннулированием (т. е. договоры в реальном мире). Такой договор включает в себя следующие элементы:

- 1) Общие условия: описание версии, дата соглашения и дата подтверждения, а также любые уведомления для пользователя. Этот элемент является обязательным.
- 2) Цель: предполагаемое использование РП пользователя. Этот элемент является обязательным.
- 3) Ссылки на атрибуты: указание, к каким атрибутам объекта относится договор. Этот элемент является обязательным.

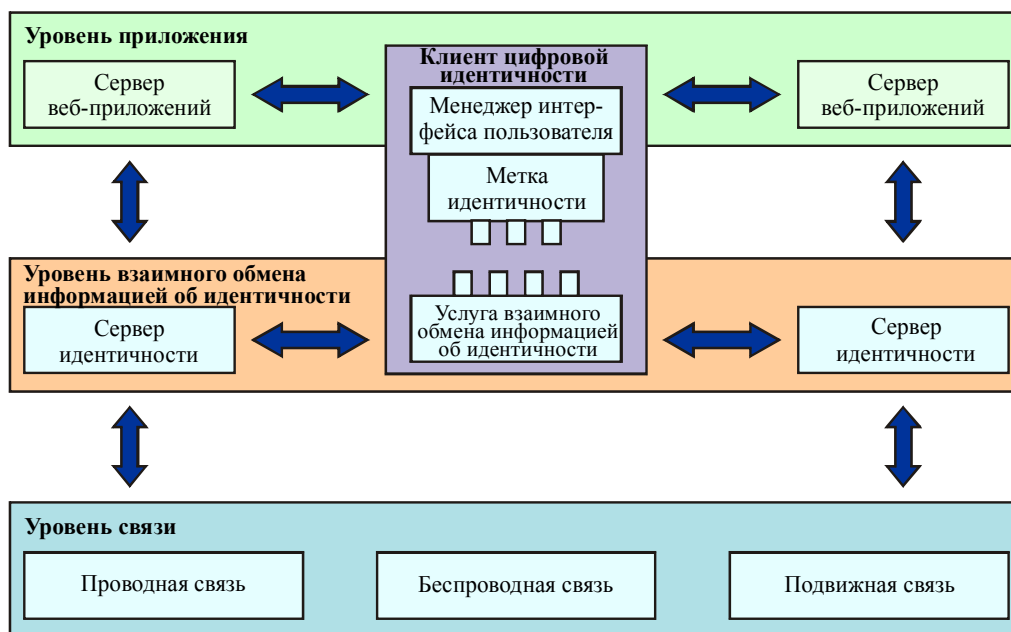
- 4) Политика безопасности: требуется, чтобы в этом элементе содержалась политика аутентификации и информационной безопасности, которые указывают на то, как могут быть аутентифицированы два объекта и каким образом защищается информация. Этот элемент является обязательным.
- 5) Политика конфиденциальности: элемент может содержать заявление о политике конфиденциальности любого вида. Здесь могут быть указаны синхронизация и прекращение действия РП, распространяемой пользователем. Должна обеспечиваться защита конфиденциальности в соответствии с применимым региональным/национальным законодательством в сфере конфиденциальности. Таким образом, этот элемент является необязательным.
- 6) Политика управления доступом: в этом элементе может быть описана любая политика управления доступом или политика авторизации. Этот элемент является необязательным.
- 7) Ссылки на политику: здесь могут быть приведены ссылки на внешне определенную политику. Этот элемент является необязательным.
- 8) Подпись: договор может заключаться двумя объектами, достигшими согласия относительно содержания цифрового договора. В то же время договор может иметь максимум две цифровых подписи, которые соответствуют двум объектам, согласившимся с договором. Однако по причинам, указанным в первом абзаце данного пункта, в договоре может быть не более двух цифровых подписей. Для того чтобы договор был достоверным и целостным, он должен быть подписан двумя объектами. Подписывая договор, пользователь дает свое согласие. Подпись распространяется на указанные на рисунке 2 разделы – от общих положений до ссылок на политику. Этот элемент является обязательным.

7.5 Три уровня взаимного обмена информацией о цифровой идентичности

В этом пункте определяются три уровня: уровни приложения, взаимного обмена информацией об идентичности и связи.

7.5.1 Уровень приложения

Уровень приложения может быть типичным веб-приложением, работающим в интернете или в условиях подвижной связи. Например, пользователь использует веб-браузер для запроса веб-услуги у веб-сервера. Когда объекту в приложении необходимо затребовать услугу идентичности или аутентификации, он обращается к услуге, предоставляемой на уровне взаимного обмена информацией об идентичности. Логично, что DIC находится на обоих уровнях: и на уровне приложения, и на уровне взаимного обмена информацией об идентичности, связывая оба уровня для непрерывного предоставления пользователю услуг, связанных с идентичностью. Каждый раз, когда пользователь пытается зайти на веб-сайт, он/она обращается к селектору идентичности клиента, который является компонентом системы управления пользовательским интерфейсом, для того чтобы выбрать метку, представляющую собой регистрационные данные для аутентификации веб-сайта. Когда веб-приложению необходимо использовать совместно информацию об идентичности пользователя в связи с запросом пользовательской услуги, веб-приложение может просто обратиться к одной из услуг передачи идентичности на уровне передачи идентичности. Расположение описания услуги на уровне взаимного обмена информацией предоставляется для целей администрирования веб-приложения.



X.1251(09)_F03

Рисунок 3 – Уровень взаимного обмена информацией об идентичности

7.5.2 Уровень взаимного обмена информацией об идентичности

Уровень взаимного обмена информацией об идентичности обеспечивает прозрачный уровень звена взаимного обмена информацией об идентичности, для того чтобы обеспечить взаимный обмен информацией об идентичности между объектами и предоставить пользователю полное управление обеспечением ее/его политики безопасности и конфиденциальности.

Посредством введения этого уровня совместное использование информации об идентичности различными объектами может быть разработано и независимо размещено для любого приложения, поскольку приложению нет необходимости знать о подробностях взаимного обмена информацией об идентичности. Кроме того, уровень взаимного обмена информацией об идентичности может выполнять различные функции, связанные с взаимным обменом информации об идентичности для существующих решений IdM, которые не имеют функций взаимного обмена информацией об идентичности. Подробное описание того, как уровень взаимного обмена информацией об идентичности способствует соблюдению политики безопасности и конфиденциальности, приведено в пункте, касающемся цифрового договора (см. пункт 7.4).

7.5.3 Уровень связи

Уровень связи представляет собой независимый уровень, который отвечает за транспортировку данных от одного устройства на другое.

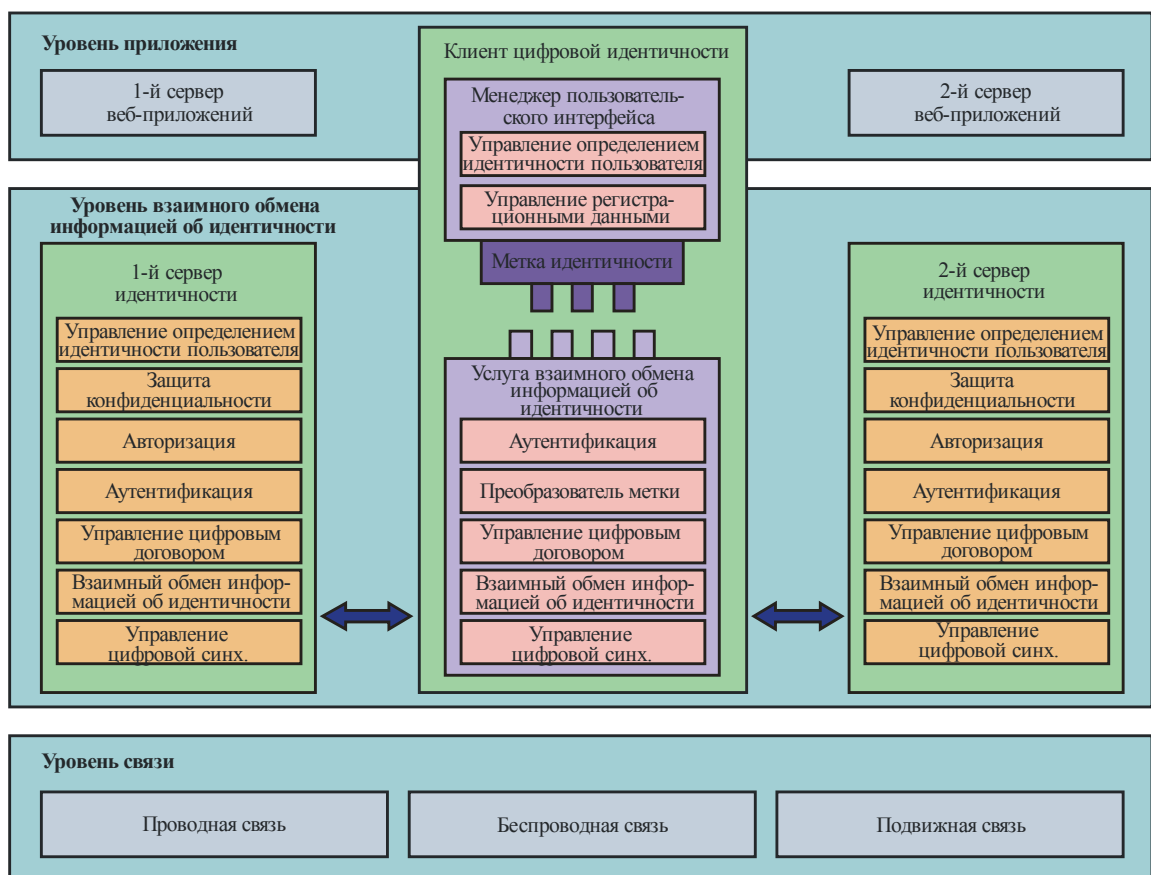
8 Структура взаимного обмена информацией о цифровой идентичности

8.1 Принципы разработки

Структура содержит следующие принципы разработки, обеспечивающие беспрепятственный взаимный обмен информацией об идентичности между объектами в компьютерной среде, в которую входят подвижные и повсеместно распространенные компьютерные системы:

- **Независимость** – Структура не увязывается с каким-либо конкретным приложением или сетевой средой. Иными словами, структура должна быть адаптируема к любой среде, если это необходимо.
- **Возможность подключения** – В условиях подвижной или повсеместной компьютерной среды пользователь может работать с несколькими устройствами, используя их для работы или развлечения. В этом случае то, что требуется для пользователя, – это весьма важная информация об идентичности, которая может установить ее/его идентичность. Эта информация должна быть разработана так, чтобы она подходила для любого устройства, с тем чтобы пользователь мог просто подключить свою информацию об идентичности к этому устройству, чтобы им воспользоваться.

- **Гибкость** – Структура должна быть разработана так, чтобы она была достаточно гибкой для использования в любом устройстве, начиная от оборудованного рабочего места и до малого повсеместно распространенного компьютерного устройства. Структура должна быть достаточно гибкой, чтобы позволять перестраиваться для адаптации к различным компьютерным средам.
- **Масштабируемость** – Структура должна быть пригодной к эксплуатации как в отдельном домене, так и между доменами без необходимости затрачивать ресурсы на связь или вычисления, для того чтобы интегрировать ее в существующую систему.



X.1251(09)_F04

Рисунок 4 – Структура взаимного обмена информацией о цифровой идентичности

8.2 Элементы структуры

DIC является ключевым элементом в этой структуре, и он способствует тому, что звено взаимного обмена информацией об идентичности связывает всех поставщиков услуг определения идентичности пользователя и полагающихся сторон. Пользователь может отзывать и обновлять свою информацию об идентичности каждый раз, когда это необходимо, используя заранее установленное звено взаимного обмена информацией.

DIC состоит из трех частей: менеджера интерфейса пользователя, услуги взаимного обмена информацией об идентичности и признака идентичности.

На рисунке 4 показаны функциональные элементы структуры.

8.2.1 Управление определением идентичности пользователя

Это компонент, который управляет информацией об идентичности пользователя, которая используется совместно с другими объектами. В IdS управление определением идентичности в основном сосредоточено на хранении. С другой стороны, управление определением идентичности в DIC стремится сосредоточить внимание на графическом интерфейсе пользователя, который представляет пользователю информацию об идентичности.

8.2.2 Защита конфиденциальности

Это элемент, который управляет функцией, связанной с конфиденциальностью, защищающей информацию об идентичности пользователя. Он отслеживает информацию об аудите, связанную с использованием и задачами идентичности пользователя. Эта функция также поддерживает ограничения конфиденциальности, описанные в цифровом договоре всякий раз, когда идентичность пользователя используется неумышленно или преднамеренно. Должна обеспечиваться защита конфиденциальности в соответствии с применимым региональным/национальным законодательством в сфере конфиденциальности.

8.2.3 Авторизация

Услуга авторизации предназначена, для того чтобы принимать решения в отношении прав доступа пользователя и обеспечивать исполнение решений об авторизации в зависимости от привилегий пользователя. Авторизация представляет собой дополнительную услугу; она предоставляется только в том случае, когда доступом к ресурсам требуется управлять, основываясь на правах пользователя.

8.2.4 Аутентификация

Это элемент, который обеспечивает выполнение общей концепции аутентификации, поддерживая различные виды механизмов аутентификации. Услуга аутентификации включает в себя взаимную аутентификацию как клиента, так и серверов.

8.2.5 Менеджер цифрового договора

Это элемент, который управляет списком цифровых договоров между пользователем и поставщиком услуг определения идентичности для аутентификации, контроля доступа и защиты конфиденциальности. Менеджер управляет жизненным циклом цифрового договора при помощи цифровой подписи.

8.2.6 Взаимный обмен информацией об идентичности

Это ключевой элемент, который предоставляет услугу взаимного обмена информацией об идентичности. Взаимный обмен информацией об идентичности подразделяется на две услуги: отзыв и обновление. Информация об идентичности хранится у объекта, а DIC может отзываться у объекта его информацию об идентичности и наоборот. Если хранящаяся у объекта информация об идентичности меняется, объект может обновить или доставить эту измененную информацию в DIC и наоборот. Более подробное описание этого элемента не входит в сферу применения настоящей Рекомендации.

8.2.7 Менеджер синхронизации идентичности

Это элемент, который управляет процессом синхронизации идентичности в DIC. При изменении хранящейся у IdSP информации об идентичности IdSP обновляет и меняет эту информацию об идентичности у DIC. В DIC этот элемент выполняет операцию обновления информации об идентичности в функции взаимного обмена информацией об идентичности для каждой полагающейся стороны, которая использует идентичность этого пользователя совместно с DIC. Следует отметить, что получать обновленную информацию об идентичности имеет право только та полагающаяся сторона, которой DIC хотя бы раз доставлял свою информацию об идентичности.

8.2.8 Менеджер интерфейса пользователя

Это элемент, который представляет собой графический интерфейс пользователя для информации об идентичности и полномочиях пользователя. Этот элемент тесно связан с сервером веб-приложений, как правило, когда пользователю необходимо войти в систему, используя аутентификацию, или когда он совместно использует свою информацию об идентичности для некоторых услуг

8.2.9 Управление регистрационными данными

Это элемент, который управляет информацией аутентификации регистрационных данных, формируемой объектом или сайтом. Пользователь может иметь различные регистрационные данные, например пароль, сертификат X.509 и биометрические данные. Общее графическое представление информации о регистрационных данных определяется для неизменных данных пользователя.

8.2.10 Метка идентичности

Метка идентичности представляет собой модель данных для цифровой идентичности. Она может подключаться к клиенту цифровой идентичности и соединять менеджер интерфейса пользователя с услугой взаимного обмена информацией об идентичности, с тем чтобы дать возможность DIC функционировать. Логическое представление метки может быть реализовано при присоединении менеджера интерфейса пользователя. Например, когда пользователь меняет свою рабочую среду, переходя от персонального компьютера на мобильный телефон, ему/ей требуется только перенести метку и подключить ее к мобильному телефону. Аппаратными средствами, которые будут содержать метку, могут быть смарт-карта, USB-метка и т. д.

8.2.11 Услуга взаимного обмена информацией об идентичности

Это часть услуги, которая несет ответственность за взаимный обмен информацией об идентичности и синхронизацию. Для соответствия условиям требуется, чтобы эта часть изменялась в зависимости от того, какая сеть или информационная платформа используется. Например, модуль услуги взаимного обмена информацией об идентичности в персональном компьютере совершенно отличается от модуля, который находится в мобильном телефоне.

8.2.12 Преобразователь метки

Это элемент, который преобразует метку, созданную другой существующей системой IdM, в метку, которая может быть понята и обработана в DIIF. Это элемент шлюза, необходимый для взаимодействия с другими существующими системами IdM с целью обмена различными метками (например, идентичности, безопасности). Этот элемент является необязательным.

Дополнение I

Справочное руководство по реализации структуры управления цифровой идентичностью со стороны, с использованием спецификации WS-Trust и технологии информационной карточки

(Это Дополнение не является неотъемлемой частью настоящей Рекомендации.)

ПРИМЕЧАНИЕ. – Это Дополнение содержит пример преобразования спецификации WS-Trust [b-WS-TRUST] и технологии информационной карточки [B-IS-INTEROP] в возможности настоящей Рекомендации.

I.1 Введение

В данном дополнении описано, как требования, изложенные в настоящей Рекомендации, могут быть выполнены с помощью спецификации WS-Trust и технологии информационной карточки, описанной в [B-CARDSPACE].

I.2 Справочная информация

I.2.1 Клиент цифровой идентичности

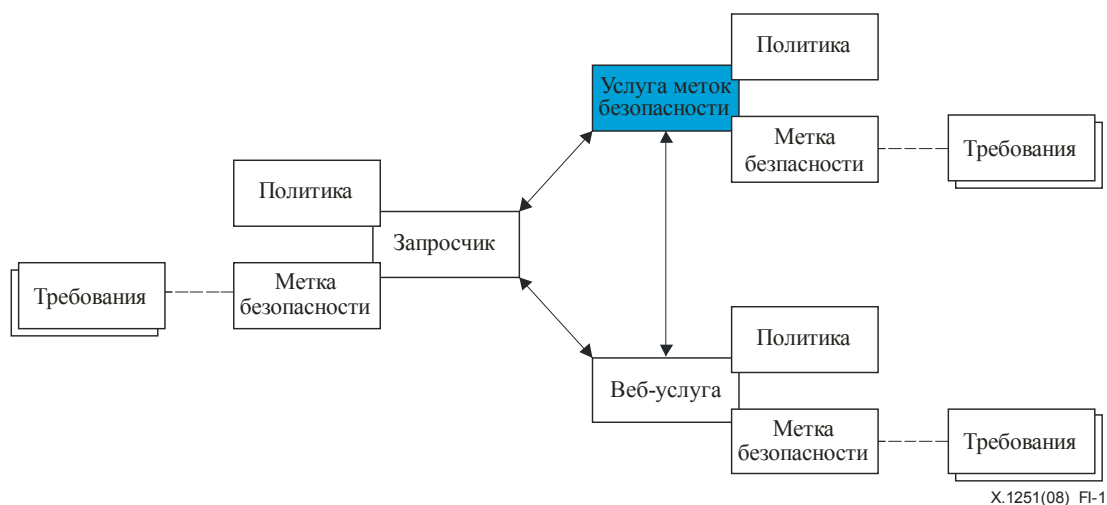
В п. 7.3.2 описывается "концепция клиента цифровой идентичности, который может контролировать передачу информации о цифровой идентичности".

I.2.2 Уровень взаимного обмена информацией об идентичности

В п. 7.5.2 описывается "уровень взаимного обмена информацией об идентичности для обеспечения взаимного обмена информацией об идентичности между объектами и предоставления объекту полного контроля над выполнением правил обеспечения его безопасности и конфиденциальности".

I.2.3 WS-Trust

Спецификация WS-Trust определяет основанные на спецификации WS-Security расширения для реализации структуры запроса и выдачи меток безопасности и для доверенных отношений с брокером. Запросчик, как правило, от имени объекта направляет сообщение метки безопасности запросчика (RequestSecurityToken) (RST) услуге меток безопасности (STS) и получает ответ метки безопасности запросчика (RequestSecurityTokenResponse) (RSTR), как правило, содержащий метку безопасности. Тогда метка безопасности, содержащая набор требований, может быть направлена в веб-услугу в качестве подтверждения идентичности запросчика. При желании услуга меток безопасности может направить RST с просьбой подтвердить или отменить ранее разосланную метку безопасности. Эти взаимосвязи показаны на рисунке I.1.



X.1251(08)_FI-1

Рисунок I.1 – Модель прямого доверия по спецификации WS-Trust

Спецификация WS-Trust может быть использована для реализации разнообразных моделей помимо простой модели прямого доверия. В некоторых случаях косвенная модель будет использоваться там, где для выполнения условий первоначальной метки RST (как на рисунке I.2), IP/STS (поставщик услуг определения идентичности/услуга меток безопасности) передает RST другой STS.

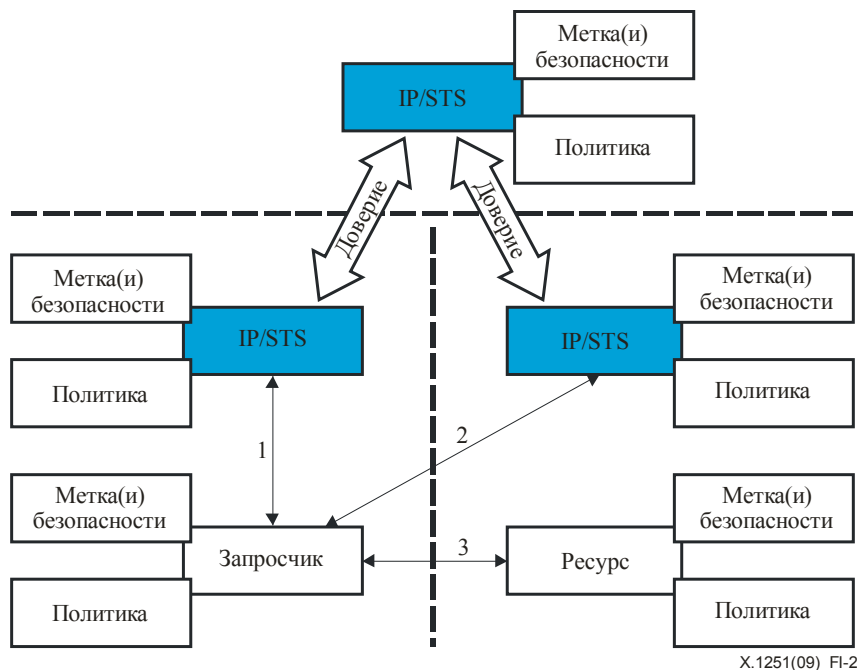


Рисунок I.2 – Модель косвенного доверия по спецификации WS-Trust

I.2.4 Информационная карточка

Технология информационной карточки описана в профиле совместимости селектора идентичности [b-IS-INTEROP]. С технологией информационной карточки селектор идентичности и связанные с ним признаки системы идентичности позволяют объектам управлять своими цифровыми идентичностями, получаемыми от разных поставщиков услуг определения идентичности, а также использовать их в различных контекстах для доступа к онлайн-услугам.

Когда объекты устанавливают связь с IdSP, они получают информационные карточки; эти информационные карточки содержат метаданные, описывающие потенциальные метки безопасности, которые могут быть запрошены через WS-Trust, а также механизмы безопасности, используемые для защиты и аутентификации передачи сообщения. Объект, как правило, размещает свои информационные карточки в хранилище карточек, доступное из его селектора идентичности. Политика безопасности полагающейся стороны определяется с помощью спецификации WS-SecurityPolicy [b-WS-SECURITY] и может быть получена различными путями, в том числе включенными в веб-страницы. Политика безопасности, как правило, устанавливает механизмы, определенные в WS-Security для аутентификации и защиты сообщений. Селектор идентичности оценивает политику полагающейся стороны и набор информационных карточек, размещенных в хранилище карточек пользователя, и позволяет объекту выбирать из множества информационных карточек те, что способны получить метку безопасности в соответствии с политикой. Затем селектор идентичности запрашивает объект информацию аутентификации и при необходимости направляет RST на STS, указанную в выбранной информационной карточке. Затем метка безопасности, полученная в итоговом RSTR, может быть присоединена к сообщению, отправленному полагающейся стороной. В том случае, когда веб-сайт является полагающейся стороной, метка безопасности может быть зарегистрирована как ответ на форму, которая содержала политику [b-IS-GUIDE].

I.3 Возможности DIIIF

Этот пункт повторяет возможности DIIIF и описывает, как спецификация WS-Trust и/или технология информационной карточки могут быть использованы для их удовлетворения.

I.3.1 Общие возможности

I.3.1.1 Возможности пользователя

DIIF должен достичь следующих целей.

- 1) *Предоставление селектора идентичности, который позволяет пользователю делать выбор в отношении того, какие регистрационные данные предполагается использовать для аутентификации.*

Селектор идентичности, описанный в информационной карточке, обеспечивает безопасное, интуитивно понятное и согласованное представление объекта и позволяет объекту выбирать информационные карточки, определяющие различные идентичности, предоставляемые разными IdSP при помощи различных механизмов аутентификации.

- 2) *Предоставление интуитивно понятного и согласованного интерфейса для управления его/ее информацией о регистрационных данных при обеспечении максимальной безопасности.*

Селектор идентичности, описанный в информационной карточке, обеспечивает безопасное, интуитивно понятное и согласованное представление объекта.

- 3) *Поддержка веб-сайтом механизма автозаполнения при регистрации или подписке, с тем чтобы свести к минимуму взаимодействие пользователя с сайтом, включая возможность для пользователя полностью управлять подключением и отключением такого механизма. Данное требование является необязательным.*

Значения этого требования, включенные в признак безопасности, используемый в сочетании с селектором идентичности, описанным в информационной карточке, могут предоставить информацию, которая, как правило, вводится объектом при регистрации.

- 4) *Предоставление информации об идентичности в любое время по желанию пользователя и обеспечение возможности для пользователя полностью управлять взаимным обменом информацией об идентичности с использованием механизма надлежащей защиты конфиденциальности.*

Предположение, связанное с технологией информационных карточек, заключается в том, что IdSP будет предоставлять информацию об идентичности только в ответ на запрос объекта. Политика конфиденциальности полагающейся стороны и IdSP доступна через безопасный интерфейс пользователя селектора идентичности во время выбора информационной карточки.

- 5) *Обеспечение автоматического обновления совместно используемой информации об идентичности при изменении первоначального источника под его/ее полным управлением.*

Значения требования, включенные в метку безопасности, используемую в сочетании с селектором идентичности, описанным в информационной карточке, могут предоставить информацию, которая, как правило, вводится объектом при регистрации. Поскольку те же самые значения требования метки безопасности могут запрашиваться полагающейся стороной при каждой проверке, то изменения, вносимые в эти значения, распространяются без труда.

- 6) *Предоставление возможности полного осуществляемого пользователем управления применительно к установлению политик безопасности и конфиденциальности и обеспечению их соблюдения, с тем чтобы управление взаимным обменом информацией об идентичности осуществлялось до совместного использования информации об идентичности. Это позволит пользователю непосредственно воздействовать на процессы установления политики и обеспечения ее соблюдения.*

Политика безопасности полагающейся стороны и IdSP доступны в безопасном интерфейсе пользователя селектора идентичности, описанного в информационной карточке, во время выбора информационной карточки.

I.3.1.2 Функциональные возможности

- 1) *Поддержка комплексного управления регистрационными данными, с помощью которого можно управлять информацией о регистрационных данных пользователя, необходимых для аутентификации.*

Технология информационной карточки включает в себя селектор идентичности и пользовательский интерфейс управления карточкой.

- 2) *Поддержка управления звеном взаимного обмена информацией об идентичности для предоставления пользователю всестороннего представления об объектах, с которыми имеет соединения этот пользователь для осуществления взаимного обмена информацией об идентичности.*

В том случае, когда метка безопасности, представляющая сеанс связи, возвращается от IdSP, то IdSP может предоставить интерфейс, чтобы дать возможность объекту увидеть набор установленных сеансов связи.

- 3) *Поддержка многих механизмов аутентификации, которые могут включать аутентификацию на основе пароля, PKI и биометрических данных.*

WS-Trust и WS-Security обеспечивают последовательный и удобный протокол, поддерживающий различные механизмы аутентификации. Реализация технологии информационной карточки обеспечивает интуитивные интерфейсы API для начала процесса аутентификации.

- 4) *Поддержка механизмов взаимного обмена информацией об идентичности, которые могут обеспечить двустороннюю связь для совместного использования информации об идентичности пользователя между объектами при помощи клиента DIC.*

Используя технологию информационной карточки, селектор идентичности и хранилище карточек магазина выполняют функциональное назначение, связанное с DIC.

- 5) *Поддержка механизма цифрового договора с целью создания договора о взаимном обмене информацией об идентичности, который должен использоваться для обеспечения соблюдения политики безопасности и конфиденциальности при предоставлении PII.*

Политика безопасности полагающейся стороны и IdSP доступны в безопасном интерфейсе пользователя селектора идентичности, описанного в информационной карточке, во время выбора информационной карточки.

- 6) *Поддержка синхронизации информации об идентичности с целью последовательного обновления распределенной и совместно используемой информации об идентичности, в случае когда меняется источник распространяемой информации об идентичности. Подлежащая синхронизации информация об идентичности ограничивается PII, которая изменяется непосредственно пользователем.*

Значения требования, включенные в метку безопасности, используемую вместе с селектором идентичности, описанным в информационной карточке, могут предоставить информацию, которая, как правило, вводится объектом при регистрации. Так как некоторые значения требований метки безопасности могут быть запрошены полагающейся стороной при каждой проверке, то изменения этих значений распространяются без труда.

- 7) *Поддержка преобразования универсальной метки с целью реализации структуры, функционально совместимой с существующими системами управления определением идентичности.*

WS-Trust обеспечивает механизм передачи метки. Сообщение RST может содержать одну или несколько меток безопасности, а также указание идентичности полагающейся стороны. RSTR может содержать метку безопасности, приемлемую для полагающейся стороны.

I.3.2 Дополнительные возможности

DPIF должен обеспечивать расширяемый механизм для селектора идентичности и связанных с ним протоколов, для того чтобы обеспечить поддержку введения и передачи различных механизмов аутентификации и информации, связанной с подтверждением.

Это включает в себя поддержку программ чтения информационной карточки и устройств ввода биометрических данных, а также связанные с ними форматы данных, описанные в [b-NIST], но не ограничивается этим.

Библиография

- [b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности.*
- [b-ITU-T Y.2091] Рекомендация МСЭ-Т Y.2091 (2008 г.), *Термины и определения для сетей последующих поколений.*
- [b-ITU-T Y.2701] Рекомендация МСЭ-Т Y.2701 (2007 г.), *Требования к безопасности версии 1 СПП.*
- [b-ITU-T Y.2720] Рекомендация МСЭ-Т Y.2720 (2009 г.), *Структура управления определением идентичности в СПП.*
- [b-CARDSPACE] Microsoft (2006). *Introducing Windows CardSpace.*
- [b-ETSI 133 980] ETSI TR 133 980 V8.0.0 (2009), *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Liberty Alliance and 3GPP security interworking.*
- [b-IS-INTEROP] Microsoft (2007). *Identity Selector Interoperability Profile V1.0.*
- [b-IS-GUIDE] Microsoft (2007). *A Guide to Using the Identity Selector Interoperability Profile V1.0 within Web Applications and Browsers.*
- [b-LA-FF] Liberty Alliance, *Liberty ID-FF Protocols and Schema Specification (ver 1.2).*
- [b-NIST] National Institute of Standards and Technology (2006), *FIPS PUB 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors.*
- [b-WS-SECURITY] OASIS (2007), *WS-SecurityPolicy 1.2.*
- [b-WS-TRUST] OASIS (2007), *WS-Trust 1.3.*

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия А	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи