Международный союз электросвязи

МСЭ-Т X.1403

(09/2020)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

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

Безопасные приложения и услуги (2) –
Безопасность технологии распределенного реестра

Руководящие указания по обеспечению безопасности при использовании технологии распределенного реестра для децентрализованного управления определением идентичности

Рекомендация МСЭ-Т X.1403

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.399
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 (1)	
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 (1)	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 (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	**X.1400–X.1429**
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
БЕЗОПАСНОСТЬ СЕТЕЙ 5G	X.1800–X.1819

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

Рекомендация МСЭ-Т X.1403

Руководящие указания по обеспечению безопасности при использовании технологии распределенного реестра для децентрализованного управления определением идентичности

Резюме

Технология распределенного реестра (DLT) и ее конкретные реализации, такие как блокчейн, предоставляют уникальную возможность использования инфраструктуры доверия и платформы, которая может быть полезна для создания доверенной федерации в целях обмена атрибутами и информацией об идентичности. В Рекомендации МСЭ-Т X.1403 рассмотрены относящиеся к электросвязи вопросы конфиденциальности и безопасности при использовании данных DLT для управления определением идентичности.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1403	03.09.2020 г.	17-я	11.1002/1000/14264

Ключевые слова

Технология распределенного реестра, управление определением идентичности.

* Для доступа к Рекомендации наберите в адресном поле вашего веб-навигатора URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации.
Например: http://handle.itu.int/11.1002/1000/11830-en.

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 в целях 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 не получил извещения 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/.

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	2
5	Соглашения	3
6	На пути к децентрализованной цифровой идентичности	3
6.1	Централизованная модель идентичности	3
6.2	Федеративная модель идентичности	4
6.3	Децентрализованная модель идентичности	5
7	Децентрализованная идентичность с использованием DLT	6
7.1	Создание электронного кошелька	7
7.2	Распознавание и аутентификация DID	8
7.3	Преимущества использования DLT для системы децентрализованного управления определением идентичности и доступом (DIdAm)	8
8	Руководящие указания по обеспечению безопасности при использовании DLT для DIdAm	10
8.1	Вопросы безопасности распределенного реестра	11
8.2	Преимущества использования DID для DLT	11
8.3	Угрозы и уязвимости	12
Библиография		16

Рекомендация МСЭ-Т X.1403

Руководящие указания по обеспечению безопасности при использовании технологии распределенного реестра для децентрализованного управления определением идентичности

1 Сфера применения

Технология распределенного реестра (DLT) обеспечивает доверенную инфраструктуру, полезную для построения систем децентрализованного управления определением идентичности при обмене атрибутами и информацией об идентичности.

В настоящей Рекомендации представлен обзор использования DLT для децентрализованного управления определением идентичности. В сферу применения Рекомендации входят:

– краткий обзор использования распределенных реестров для управления определением идентичности и данными идентичности;

– обсуждение преимуществ децентрализованной идентичности для безопасности;

– руководящие указания по необходимым средствам контроля, которые следует использовать в целях смягчения угроз для данных идентичности.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации.

[ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 г.), *Базовые термины и определения в области управления определением идентичности.*

[ITU-T X.1254] Рекомендация МСЭ-Т X.1254 (2012 г.), *Структура гарантии аутентификации объекта*.

[ITU-T X.1277] Recommendation ITU-T X.1277 (2018), *Universal authentication framework.*

[ITU-T X.1278] Recommendation ITU-T X.1278 (2018), *Client to authenticator protocol/Universal 2-factor framework.*

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 заявление (claim) [ITU-T X.1252]: Высказывание о том, что дело обстоит именно таким образом, без возможности представить доказательства.

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

3.1.3 документ DID (DID document) [b-W3C-2]: Набор данных, описывающий субъект DID, включая такие механизмы, как открытые ключи и псевдобиометрические данные, которые субъект DID может использовать для своей аутентификации и подтверждения связи с DID.

3.1.4 объект (entity) [ITU-T X.1252]: Что-либо, что существует отдельно и обособленно и может быть определено в каком-либо контексте.

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

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

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определены следующие термины.

3.2.1 децентрализованный идентификатор (decentralized identifier (DID)): Глобальный уникальный идентификатор, для регистрации которого не требуется централизованный регистрационный орган, поскольку он зарегистрирован с помощью технологии распределенного реестра (DLT) или другой децентрализованной системы.

ПРИМЕЧАНИЕ. – Основано на определении из [b-W3C-2].

3.2.2 субъект DID (DID subject): Объект, к которому относится документ DID, то есть объект, идентифицируемый DID и описываемый документом DID.

ПРИМЕЧАНИЕ. – Основано на определении из [b-W3C-2].

3.2.3 цепочка ключей (key-chain): Относится к задаче обеспечения безопасности хранения личных ключей или данных в доверенном аппаратном блоке устройства.

3.2.4 оконечная точка обслуживания (service endpoint): Адрес распределенного реестра, по которому услуга работает от имени субъекта DID. Примером конкретных услуг являются услуги обнаружения, социальные сети, услуги хранения файлов и услуги хранения верифицируемых заявлений. Оконечные точки обслуживания также могут создаваться с помощью обобщенного протокола обмена данными, такого как расширяемый обмен данными.

ПРИМЕЧАНИЕ. – Основано на определении из [b-W3C-2].

3.2.5 структура доверия (trust framework): Имеющий юридическую силу набор спецификаций, правил и соглашений, регулирующих систему определения идентичности.

3.2.6 кошелек (кошелек идентичности) (wallet (identity wallet)): Приложение, которое в первую очередь позволяет пользователю хранить идентификаторы и регистрационные данные, сохраняя соответствующие личные ключи на своем устройстве.

3.2.7 доказательство с нулевым разглашением (zero knowledge proof): Доказательство с использованием специальной криптографической системы и мастер-секрета, допускающее выборочное раскрытие информации в наборе заявлений. Доказательство с нулевым разглашением доказывает, что некоторые или все данные в наборе заявлений верны без раскрытия какой бы то ни было дополнительной информации, включая идентичность проверяющего.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

DDO	DID document		Документ DID
DID	Decentralized Identifier		Децентрализованный идентификатор
DIdAm	Decentralized Identity and Access Management		Система децентрализованного управления определением идентичности и доступом
DLT	Distributed Ledger Technology		Технология распределенного реестра
IdAM	Identity Access and Management		Управление определением идентичности и доступом
IdSP	Identity Service Provider		Поставщик услуг определения идентичности
IT	Information Technology	ИТ	Информационные технологии
PKI	Public Key Infrastructure		Инфраструктура открытых ключей

PII	Personally Identifiable Information	Информация, позволяющая установить личность
RP	Relying Party	Полагающаяся сторона
SAML	Security Assertion Markup Language	Язык разметки подтверждения безопасности
SP	Service Provider	Поставщик услуг
SSI	Self-Sovereign Identity	Суверенная идентичность
SSO	Single Sign On	Однократная регистрация входа
URL	Uniform Resource Locator	Универсальный указатель ресурса

5 Соглашения

В настоящей Рекомендации применяются следующие глагольные формы для формулировки положений:

a) "должен" – обозначает требование;

b) "следует", "рекомендуется, чтобы" – обозначают рекомендацию;

c) "разрешается" – обозначают разрешение;

d) "может" – обозначает возможность и способность.

6 На пути к децентрализованной цифровой идентичности

Технология распределенного реестра играет решающую роль в развитии и достижении зрелости децентрализованных систем определения идентичности.

Распространение мобильных устройств и интернета вещей усиливает давление на традиционные системы управления определением идентичности и доступом (IdAM), побуждая их продвигаться в направлении создания гибких и интеллектуальных платформ, способных поддерживать системы на основе подвижных и облачных сетей.

Традиционные системы управления определением идентичности опираются на централизованные административные органы, такие как корпоративные службы каталогов, центры сертификации или реестры доменных имен. Каждый из этих организационно централизованных органов выполняет функции самостоятельного доверенного домена. В традиционной системе IdAM централизованный орган может стать компонентом, отказ которого приводит к отказу всей системы (единая точка отказа). Федерация идентичностей [ITU-T X.1252] возникла как временное решение, которое позволило системам IdAM работать в системах с разной организацией, контролирующих свои собственные домены.

С появлением DLT стало возможным разрабатывать решения для децентрализованного управления определением идентичности и доступом (DIdAm). DLT предоставляет средства для доверительного управления без централизованного органа, что позволяет избежать возникновения единой точки отказа. Кроме того, DLT позволяет любому объекту создавать свои собственные идентификаторы в любом количестве распределенных реестров и управлять ими.

Модели цифровой идентичности постоянно развиваются в целях удовлетворения меняющихся деловых потребностей. Существует три основные модели идентичности, которые описаны в разделе 6.

6.1 Централизованная модель идентичности

Это самая старая модель цифровой идентичности, которая в настоящее время применяется чаще всего [ITU-T X.1252]. В централизованной модели идентичности организации выполняют функции поставщиков услуг определения идентичности (IdSP). При использовании этой модели организация устанавливает прямые доверительные отношения с каждым пользователем. Это традиционная обособленная модель, в соответствии с которой организация предоставляет пользователю регистрационные данные, позволяющие ему получать доступ к услугам этой организации.

В этой модели каждая организация действует в качестве IdSP. Организация управляет цифровой идентичностью пользователя и принимает решения, касающиеся установленных доверительных отношений. Доверие между пользователем и IdSP обычно устанавливается посредством применения совместно используемых секретов, таких как имя пользователя и пароль. В некоторых случаях совместно используемые секреты дополняются многофакторной аутентификацией, такой как аппаратные маркеры, биометрические данные или решения на основе FIDO [ITU-T X.1277] и [ITU-T X.1278].

В централизованной модели IdSP может собирать данные о пользователях и хранить их. Эти данные можно монетизировать, передавать или продавать другим сторонам в соответствии с бизнес-моделью IdSP. Пользователям приходится доверять IdSP принятие правильных решений в отношении управления своими данными. Хотя они пользуются услугами организации, в большинстве случаев конечные пользователи не контролируют управление своей идентичностью, личными данными или атрибутами идентичности. Владельцем идентичности пользователя в этой модели является IdSP. Пользователи не имеют возможности передать свои данные другим поставщикам.

При использовании централизованной модели идентичности пользователь должен получать и администрировать отдельные регистрационные данные для каждого из своих деловых отношений с каждым IdSP. Прежде чем разрешить пользователю доступ к своим ресурсам, организация требует от него создания таких регистрационных данных. Такая модель ведет к перегрузке пользователя множеством онлайновых идентичностей. Отсутствие взаимной аутентификации при входе в систему делает эту модель уязвимой для фишинговых атак и атак в целях сбора регистрационных данных. Эта модель побуждает пользователя многократно использовать одни и те же пароли, что ведет к повышению рисков нарушения безопасности и еще большей уязвимости.

При использовании централизованной модели IdSP несет большую нагрузку по управлению жизненным циклом идентичности. В частности требуется, чтобы каждый IdSP выполнял проверку подлинности идентичности [ITU-T X.1254] на этапе регистрации в процессе управления жизненным циклом идентичности. Проверка подлинности идентичности необходима для установления уровня доверия к утверждаемой идентичности. Этот процесс может повторяться в течение всего жизненного цикла данной идентичности. С точки зрения пользователя это проблематично, поскольку при централизованной модели требуется, чтобы пользователь проходил этот этап проверки подлинности идентичности отдельно с каждым поставщиком услуг определения идентичности. Кроме того, угроза взлома данных повышает риск перехвата учетной записи из-за зависимости организаций от централизованных хранилищ данных, которые регулярно подвергаются хакерским атакам.

6.2 Федеративная модель идентичности

Осознав ограничения централизованной модели идентичности, рассмотренные в пункте 6.1, организации разработали федеративную модель идентичности, позволяющую решить эти проблемы. Федеративная модель идентичности направлена на снижение нагрузки на пользователей, которые получают возможность использовать свои идентификационные данные, определенные в одном домене, в других доменах. Язык разметки, предусматривающий защиту данных (SAML) [ITU-T X.1242], обеспечивает дополнительные удобства для пользователей благодаря однократной регистрации входа (SSO).

Федеративные системы управления определением идентичности могут выполнять функции аутентификации и авторизации за пределами границ организаций и систем. Для этого требуется заключение деловых и доверительных соглашений, с тем чтобы идентичность пользователя, определенная у одного поставщика услуг, распознавалась другими поставщиками (членами федерации). Обычно в доверительное соглашение также включается договорное соглашение о владении данными, использовании информации, позволяющей установить личность (PII), и соответствии [ITU-T X.1242].

Федеративная модель выгодна пользователю, поскольку поставщик услуг определения идентичности обычно предоставляет ему возможность однократной регистрации входа. Это уменьшает количество отдельных регистрационных данных, которые пользователю приходится получать и хранить. При использовании этой модели полагающиеся стороны, участвующие в федерации, включая их пользователей, зависят от доступности услуг данного IdSP и его готовности оставаться в федерации.

Как и в случае централизованной модели идентичности, аутентификация в федеративной модели не является взаимной и имеет те же недостатки.

6.3 Децентрализованная модель идентичности

Децентрализованная модель идентичности может быть реализована с использованием DLT или других новых основанных на стандартах технологий, таких как верифицируемые заявления [b-W3C-1] и децентрализованные идентификаторы (DID) ([b-Sovrin], [b-W3C-1] и [b-W3C-2]). Она может опираться на распределенный реестр (DLT) и отношения между пользователем и организацией ([b-Sovrin] и [b-W3C-17]). В этой модели пользователь и организация являются равноправными партнерами.

Децентрализованная идентичность позволяет пользователям принимать на себя контроль и владение своими идентичностями. Степень владения может варьироваться в зависимости от конкретной реализации децентрализованной модели. В частности, в модели суверенной идентичности (SSI) предполагается, что объекты могут управлять своей собственной цифровой идентичностью.

Сегодня большинство решений для определения идентичности имеют ограниченную поддержку контроля над идентичностью, прозрачностью и переносимостью, поскольку эти решения предоставляются поставщиками услуг определения идентичности, предлагающими проприетарные системы. В ближайшем будущем может появиться система управления определением идентичности, полностью соответствующая SSI, но это не исключает необходимости определения ее основополагающих принципов, рассматриваемых в пунктах 6.3.1 и 6.3.2. В разделе 7 дополнительно обсуждается использование DLT для децентрализованного управления определением идентичности.

6.3.1 Децентрализованные идентификаторы

DID [b-W3C-2] – это тип идентификатора для верифицируемых децентрализованных систем определения идентичности. Формат DID позволяет им находиться под контролем субъекта DID, что делает их не зависящими ни от каких централизованных реестров, поставщиков услуг определения идентичности или центров сертификации. DID – это унифицированные указатели ресурсов (URL), которые связывают субъект DID со средствами доверительного взаимодействия с этим субъектом. В число стандартных элементов документа DID (DDO) [b-W3C-2] входят:

1) DID (для самоописания);
2) набор открытых ключей (для верификации);
3) набор протоколов аутентификации (для аутентификации);
4) набор оконечных точек обслуживания (для взаимодействия);
5) отметка времени (для истории ревизий);
6) подпись (для гарантии целостности).

Распознавание DID [b-W3C-2] приводит к созданию DDO, который представляет собой простой документ с описанием способа применения данного конкретного DID. Каждый документ DID содержит как минимум три элемента: криптографический материал, аутентификационные комплексы и оконечные точки обслуживания. Криптографический материал в сочетании с аутентификационными комплексами предоставляет набор механизмов аутентификации субъекта DID (который является пользователем, связанным с DDO). Примерами аутентификационных комплексов могут служить открытые ключи и псевдобиометрические протоколы. Оконечные точки обслуживания обеспечивают надежную связь с субъектом DID.

Чтобы использовать DID [b-W3C-2] с конкретным распределенным реестром, необходимо определить метод DID. Спецификация метода DID может быть основана на [b-RFC 8141]. Метод DID представляет собой набор правил, определяющих, каким образом DID регистрируется, распознается, обновляется и аннулируется в определенном DLT-реестре. Все DID определяются и распознаются в распределенном реестре.

Использование DID на основе DLT [b-W3C-2] уменьшает зависимость идентификаторов от централизованных реестров, а также зависимость управления ключами от централизованных центров сертификации. Поскольку DID находятся в распределенном реестре, каждый объект может выступать в качестве своего собственного доверенного домена, что приводит к созданию децентрализованной инфраструктуры доверия. Это обеспечивает функциональную совместимость между системами централизованных, федеративных и децентрализованных идентификаторов.

DID содержит пару криптографических ключей – открытый и личный [b-W3C-2]. Принадлежность DID подтверждается криптографическими алгоритмами, основанными на личном ключе, которым должен обладать только владелец DID. Следовательно, DID можно публиковать, изменять, запрашивать или удалять. Поскольку в каждой DLT метод DID может быть реализован по-своему, на практике будут иметь место разные реализации операций "создания, чтения, редактирования и удаления" (CRUD) DID.

6.3.2 Верифицируемые регистрационные данные

Верифицируемые регистрационные данные [b-W3C-1] решают задачу обмена регистрационными данными, такими как водительские права, документы, подтверждающие возраст или образование, или медицинские документы, по сети электросвязи таким способом, который поддается проверке и в то же время защищает индивидуальную PII. При таком подходе регистрационные данные состоят из утверждений, называемых верифицируемыми заявлениями. Верифицируемые заявления [b-W3C-1] полезны, когда объект должен доказать, например, что он:

- старше определенного возраста;
- имеет право управлять конкретным транспортным средством;
- нуждается в определенном лекарстве;
- имеет образование и диплом электрика;
- имеет лицензию на осуществление медицинской деятельности;
- имеет разрешение на поездки за границу.

Экосистема верифицируемых регистрационных данных состоит из четырех основных позиций:

1) эмитент, выдающий верифицируемые регистрационные данные, относящиеся к конкретному субъекту;
2) держатель, хранящий регистрационные данные по поручению субъекта. Как правило, держатели также являются субъектами регистрационных данных;
3) верификатор, запрашивающий профиль субъекта. Профиль содержит определенный набор регистрационных данных. Верификатор подтверждает, что представленные в профиле регистрационные данные соответствуют своему назначению;
4) реестр идентификаторов – механизм, используемый для выдачи идентификаторов субъектам.

Заявление [b-W3C-1] – это утверждение, относящееся к субъекту и выраженное в виде отношения субъект–свойство–значение. Заявления можно объединять, представляя информацию о конкретном субъекте в графическом виде.

Передавая данные держателю, эмитент собирает набор заявлений в структуру данных, называемую регистрационными данными, и подписывает эту структуру данных цифровой подписью [b-W3C-1]. Когда верификатор запрашивает данные у держателя, тот обычно собирает набор регистрационных данных в структуру данных, называемую профилем, и подписывает ее цифровой подписью [b-W3C-1].

7 Децентрализованная идентичность с использованием DLT

Децентрализованную идентичность можно представить как идентичность, связанную с DLT. При этом подходе доказательство с нулевым разглашением [b-W3C-1] может связывать идентичности универсальным видимым способом. Децентрализованная идентичность позволяет пользователю подтвердить свою личность доверенной третьей стороне один раз и сохранить подтверждение идентификатора в DLT. DLT действует как надежное хранилище идентичности. DLT предлагает услуги инфраструктуры определения идентичности, в частности для поддержки одноранговой связи, основанные на DLT услуг инфраструктуры открытых ключей (PKI) и протоколов обмена верифицируемыми заявлениями.

Децентрализованная идентичность позволяет пользователям получать доступ к услугам в рамках простого процесса. Например, пользователь взаимодействует с IdSP, который в свою очередь использует DLT для создания DID пользователя, указывающего местоположение доступного пользователю DLT-реестра. Этот шаг прозрачен для конечного пользователя. Он эквивалентен

созданию пары из личного и открытого ключей пользователя. Личный ключ хранится у пользователя в той или иной форме электронного кошелька. Соответствующий открытый ключ хранится в DLT-реестре. Открытый ключ действует как идентификатор электронного кошелька (он же идентификатор пользователя в DLT), хеширован и надежно хранится в реестре. В рамках услуг, предлагаемых DLT, эмитенты DLT могут издавать заявления для конкретного пользователя, подписывать их и выдавать этому пользователю. Такие заявления могут храниться в кошельке пользователя.

В этой модели пользователь может обращаться к услугам, представив поставщику услуг свой идентификатор в форме маркера. Поставщик услуг проверяет идентичность, сравнивая хеш-значения идентификаторов с соответствующими хеш-записями, хранящимися в DLT-реестре. Поставщик услуг предоставляет доступ или отклоняет заявление по результатам верификации.

7.1 Создание электронного кошелька

Работа в стандартах [b-Sovrin] и [b-W3C-1] являет собой пример взаимодействий в поддержку услуги, основанной на идентичности. Пользователь решает взаимодействовать, применяя услуги децентрализованной идентичности надежной системы определения идентичности на основе DLT. В этом случае DLT предоставляет услуги, позволяющие конечному пользователю создать DID и установить связь с реестром. Задача создания DID для пользователя завершается сохранением адреса реестра этого пользователя и созданием пары из открытого и личного ключей для взаимодействия с пользователем. Реестр также может предоставлять услуги, которые можно использовать для создания документа DID и установления необходимых ссылок на документы, указанные пользователем. Реестр предоставляет основные услуги определения идентичности, которые позволяют определять, каким образом следует взаимодействовать с электронным кошельком пользователя, чтобы делать запросы о доступных заявлениях, находящихся под управлением пользователя.

Акт создания DID в реестре приводит к созданию электронного кошелька, посредством которого пользователь будет направлять полагающейся стороне (RP) верифицированные заявления. В электронном кошельке хранятся личные ключи пользователя, открытые ключи и другие профили идентичности пользователя, определяемые методом DID. Применение методов доказательства с нулевым разглашением [b-Sovrin] гарантирует, что заявления можно верифицировать таким способом, чтобы сохранить неприкосновенность PII, и в соответствии с существующим порядком использования традиционных бумажных регистрационных данных и документов. Например, пользователь может доказать в учреждении свой возраст при помощи водительских прав без необходимости привлечения к участию в транзакции органа, выдающего водительские права. Кошелек может представлять собой виртуальный кошелек, одна часть которого находится в мобильном устройстве пользователя, а другая – в облаке. Эта конфигурация позволяет создавать агенты, действующие от имени пользователя и реализующие услуги без необходимости непосредственного участия пользователя.

Процесс состоит из следующих этапов.

1) Регистрация DID. Пользователь загружает электронный кошелек, связанный с поставщиком услуг DLT, и регистрирует его DID в реестре. DLT генерирует пары из личного и открытого ключей, связанные с кошельком идентичности. В рамках процесса регистрации создается адрес и сохраняется в DLT-реестре.

2) Создание идентичности. Для использования DLT в децентрализованных системах определения идентичности предполагается, что существует структура доверия, определяющая перечень доступных участникам услуг определения идентичности. В этом случае пользователь может рассчитывать на наличие эмитента (доверенной стороны), способного подтверждать идентичность пользователей. Пользователи могут начать с самоутверждаемых заявлений. Затем они могут применить первоначальные заявления из своего электронного кошелька для сбора дополнительных заявлений от нескольких поставщиков, чтобы внести их в свой электронный кошелек и тем самым укрепить достоверность своих идентификационных данных в системе. Каждая связь защищена взаимным DID между эмитентом, держателем (пользователем) и верификатором.

3) Верификация. Если держатель (пользователь) желает получить доступ к услуге полагающейся стороны, то полагающаяся сторона (верификатор) запрашивает у пользователя доступ к заявлениям из его кошелька. Затем верификатор обращается к DLT, чтобы проверить подписанные заявления, используя открытые ключи, соответствующие DID, как указано в транзакции. Система считает электронный кошелек источником достоверных данных в отношении личных ключей владельца. Она предполагает, что имела место надлежащая аутентификация, гарантирующая, что объект, выполняющий транзакцию, является законным владельцем электронного кошелька.

4) Валидация заявления. RP использует предоставленные заявления из кошелька для верификации идентичности пользователя и ее атрибутов с применением методов электронной подписи и хеш-валидации на основе PKI, определенных в DLT.

5) Авторизация. По результатам проверок идентичности RP определяет, к каким услугам может быть предоставлен доступ.

7.2 Распознавание и аутентификация DID

Концепция DID [b-W3C-2] может облегчить создание универсального распознавателя [b-DIF] любого DID. Универсальный распознаватель может участвовать на уровне аутентификации совместимых DID. Аутентификация DID позволяет владельцу идентичности установить контроль над DID во время своего взаимодействия с RP. Для этого полагающаяся сторона должна выполнить следующие шаги:

1) полагающаяся сторона преобразует DID владельца идентичности на основе DLT в документ DID;

2) полагающаяся сторона пытается аутентифицировать владельца идентичности, используя объект(ы) аутентификации, найденный(е) в документе DID на основе DLT;

3) в тех случаях, когда подтверждение владельца идентичности распознано как криптографическая подпись, объект аутентификации может включать в себя объект открытого ключа или ссылаться на него.

7.3 Преимущества использования DLT для системы децентрализованного управления определением идентичности и доступом (DIdAm)

Использование DLT в качестве структуры доверия для децентрализованных систем определения идентичности позволяет поставщикам разрабатывать структуры, обеспечивающие им возможность выступать в качестве промежуточного уровня абстракции между пользователем и различными реестрами. Для таких взаимодействий требуются традиционные системы управления определением идентичности и доступом, которые создают надлежащую структуру для поддержки децентрализованных систем. По сути сочетание централизованных и децентрализованных систем можно назвать системой децентрализованного управления определением идентичности (DIdAm) [b-Angelov et al.]. В этом отношении DIdAm [b-Angelov et al.] – это система систем, способных взаимодействовать со многими DLT, поддерживающими децентрализованные модели идентичности, основанные на DID. Это показано на рисунке 1.

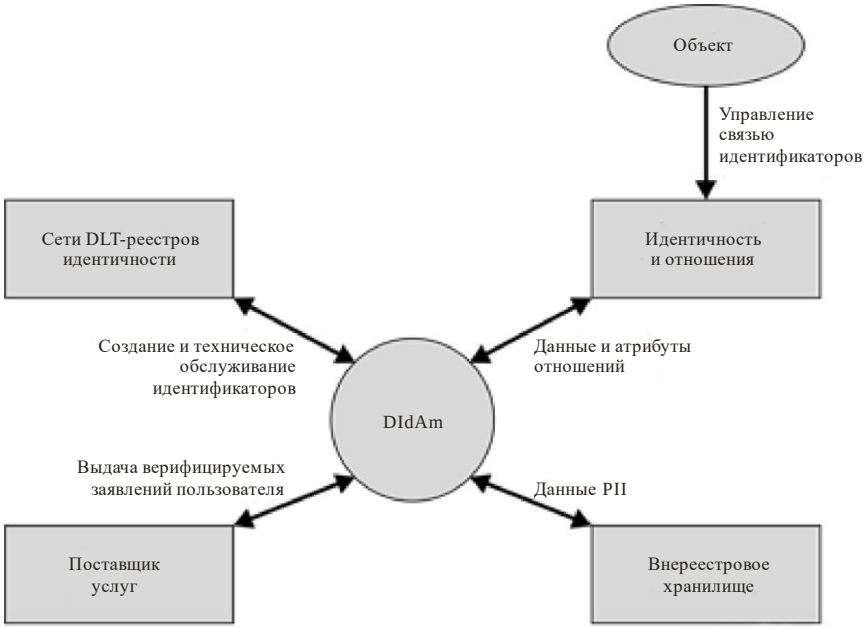

Рисунок 1 – Структура DIdAm

DIdAm состоит из следующих компонентов, использующих DLT.

1) Владелец децентрализованной идентичности – это объект, который управляет своими децентрализованными идентичностями, используя услуги, предлагаемые DIdAm в нескольких реестрах.

2) Поставщики услуг (SP) – эмитенты, предлагающие услуги владельцам идентичностей (начальная загрузка идентичностей). Например, государственные учреждения, такие как управление регистрации транспортных средств, или частные компании, такие как финансовые учреждения.

3) Внереестровое хранилище идентичностей – это база данных, в которой хранятся атрибуты идентичностей, заявления и общая информация пользователей. Пользователь сам решает, где следует хранить эти данные. Обычно это конфиденциальные данные PII, которые следует хранить вне реестра. Рекомендуется, чтобы хранилище обеспечивало возможность чтения и записи по усмотрению пользователя.

4) Системы определения идентичности, основанные на DLT, можно представить как отдельные системы определения идентичности с разными границами доверия и криптографическими ключами. Следовательно, DIdAm должна облегчать взаимодействие между реестрами от имени пользователя.

Услуги DIdAm могут предоставляться внутренними специалистами предприятия либо какой-либо третьей стороной, которая может выступать в роли поставщика таких услуг.

7.3.1 Поддержка децентрализованной идентичности в нескольких DLT-реестрах

Существует ряд требований к интерфейсу [b-Angelov et al.], которые необходимо соблюдать для поддержки децентрализованной идентичности с использованием DID в нескольких DLT-реестрах. Трудности возникают из-за различных требований к структуре доверия, таких как тип DLT-реестра – открытый или частный. Рекомендуется, чтобы DIdAm имела возможность поддерживать пользователей независимо от их предпочтений в отношении типа сети доступа к услугам электросвязи. На рисунке 1 показана DIdAm в виде унифицированного интерфейса, направленного к владельцу идентичности и способного работать с несколькими реестрами.

DIdAm [b-Angelov et al.] играет роль уровня абстракции для конечного пользователя. Она позволяет ему взаимодействовать со многими DLT, используя единый виртуальный интерфейс. DIdAm также выступает в качестве уровня абстракции для предприятия, где она может взаимодействовать с традиционными системами IdM для поддержки внутренних централизованных функций IdM.

Преимуществом такого абстрагирования является возможность для пользователя управлять идентичностями в любом количестве реестров. Это позволяет ему налаживать связи с поставщиками и лучше контролировать свою идентичность.

7.3.2 Поддержка услуг определения идентичности

В традиционных системах IdAm поставщик услуг определения идентичности может подтвердить идентичность пользователя полагающейся стороне. Рекомендуется, чтобы DIdAm [b-Angelov et al.] имела возможность поддерживать эту роль, в частности для обратной совместимости с традиционными системами. Требованиям аттестации могут соответствовать следующие действия.

1) DIdAm следует действовать в качестве доверенного партнера. Ей следует обеспечивать, чтобы владелец идентичности получал точные и действительные подтверждения посредством надлежащих верифицируемых процедур выдачи заявлений для эмитентов.
2) Уменьшение нагрузки на пользователей, связанной с проверкой подлинности идентичности. Как правило, пользователь должен пройти этап проверки подлинности идентичности с каждым эмитентом. Правильно разработанная DIdAm может помочь пользователю преодолеть это ограничение, будучи активным доверенным участником взаимодействия.
3) Валидация данных в режиме реального времени. Проблема традиционных систем – неточные данные. DIdAm может решить ее, предоставляя услуги, которые помогают полагающимся сторонам определить, что атрибуты пользователя не утратили силу.
4) Управление выдачей разрешений. Выдача разрешений – неотъемлемая часть соответствия требованиям. DIdAm может предлагать пользователям и полагающимся сторонам услуги, гарантирующие, что требование в отношении выдачи разрешений соблюдено.

7.3.3 Управление цепочкой ключей

Термин "цепочка ключей" относится к задаче обеспечения безопасности хранения личных ключей, связанных с кошельком, на устройстве пользователя. Существует прямая взаимосвязь между DID, верифицируемыми регистрационными данными и поставщиком услуг. Устройство может быть мобильным устройством или устройством на основе браузера. Поскольку в этой используемой в настоящее время модели безопасности доступ к личным ключам осуществляется для проверки идентичности пользователя, задача защиты пар ключей имеет решающее значение для предотвращения атак в целях кражи персональных данных. При работе с несколькими DID с применением разных DLT пользователи сталкиваются с задачей защиты набора личных ключей, открывающих доступ к их идентичностям во всем пространстве идентичностей.

Цепочка ключей – это структура, в которой надежно хранятся личные ключи, соответствующие DID пользователя. Эта структура принадлежит владельцу идентичности и управляет личными ключами, что означает владение DID. Рекомендуется, чтобы DIdAm могла управлять цепочкой ключей от имени пользователя. В частности рекомендуется, чтобы:

1) при работе в домене DIdAm пользователь мог применять функциональные возможности и хранилище цепочки ключей;
2) управление ключами находилось под контролем пользователя;
3) доступ к цепочке ключей был управляемым и контролируемым;
4) DIdAm могла предоставлять пользователю услуги, позволяющие сохранять и восстанавливать электронный кошелек.

8 Руководящие указания по обеспечению безопасности при использовании DLT для DIdAm

Децентрализованная идентичность решает некоторые ключевые проблемы, присущие централизованным и федеративными моделям определения идентичности. Технология распределенного реестра уязвима в отношении рисков в области кибербезопасности. К рискам в области безопасности относятся риски, возникающие в результате ошибок человека, таких как ошибки при программировании.

Как правило, DID пользователей не следует публиковать в общедоступном реестре, даже если в некоторых случаях может возникнуть необходимость сделать уникальный идентификатор доступным для всех его пользователей. Однако данные, способствующие укреплению доверия пользователей к реестру, такие как открытые ключи IdSP, списки аннулирования и данные, улучшающие совместимость, такие как схемы переменных регистрационных данных, можно сделать открытой информацией по реестрам.

В этом разделе рассматриваются преимущества, проблемы и риски в области безопасности, характерные для децентрализованных моделей идентичности.

8.1 Вопросы безопасности распределенного реестра

Существует два основных типа распределенных реестров: общедоступные и контролируемые. Общедоступные реестры позволяют любому объекту обращаться к реестру, просматривать его, предлагать новые данные или проверять существующие данные при условии соблюдения установленных протоколов реестра. Реестр гарантирует конфиденциальность, целостность, доступность и согласованность данных с помощью протоколов согласования, с тем чтобы установить доверительные отношения между участниками, которые могут не доверять друг другу. Как правило, общедоступные реестры функционируют без какого-либо центрального органа.

Контролируемый реестр – это система, состоящая из доверенных сторон, которым предоставляются права на его использование в соответствии с их ролью в структуре доверия. В этой модели изменять данные реестра могут только избранные участники. В зависимости от доверительных соглашений в некоторых реестрах может быть разрешен открытый доступ для чтения.

В общедоступном реестре доверие гарантируется согласованными протоколами, которые связаны с вычислительными издержками и оказывают непосредственное влияние на пропускную способность и быстродействие системы определения идентичности, работающей с ними. С другой стороны, в контролируемых реестрах гарантии безопасности данных, включая данные идентичности, опираются на доверие их создателей друг к другу. Контролируемые реестры, как правило, быстрее и экономичнее общедоступных.

8.2 Преимущества использования DID для DLT

Децентрализованная идентичность обеспечивает следующие преимущества.

1) Переносимость идентичности. Децентрализованный DID гарантирует физическим лицам контроль над их цифровой идентичностью. Он исключает зависимость от централизованного IdSP. Теоретически люди владеют своими идентификаторами, контролируют их и управляют ими и своими отношениями.
2) Поощряет услуги определения идентичности на основе связей. DID позволяет организациям присваивать цифровые идентификаторы почти любым отношениям. Парные DID с использованием псевдонимов несут в себе PII.
3) Минимизирует риск для безопасности. При использовании DID требуется, чтобы владельцы идентификатора подтверждали свое право собственности, демонстрируя знание личного ключа, связанного с соответствующим открытым ключом. Проверка заявления осуществляется динамически с использованием DLT в режиме реального времени. Проверка может выполняться без использования централизованных серверов, что уменьшает поверхность мишени для атак.
4) Распределение стоимости. Проверка идентичности с применением DLT может выиграть от возможности использования DID для многократной проверки идентичности участников DLT. Это снижает расходы и повышает безопасность.
5) Конструктивная PII. Независимые услуги DID распределяют риск, связанный с использованием центральных хранилищ данных для хранения пользовательской информации, и, следовательно, повышают сложность атаки для злоумышленников.
6) Согласованный и отслеживаемый обмен персональными данными. DID обеспечивает возможность обмена данными между пользователями и поставщиками на основе согласованных правил, что расширяет возможности пользователей по защите своих данных.
7) Динамичная и улучшенная федерация. Использование DID в DLT укрепляет доверие ко

всем организациям, участвующим в экосистеме. Участники могут сосредоточиться на предоставлении услуг, а не на деталях федерации и способах ее настройки.

8) Отказоустойчивость. Децентрализованный характер DLT обеспечивает отказоустойчивость и надежность инфраструктуры.

8.3 Угрозы и уязвимости

Распределенным реестрам присущи традиционные возможности, понижающие риск в области кибербезопасности для информационно-коммуникационной системы. К примерам улучшенных функций обеспечения безопасности относятся:

1) повышенная отказоустойчивость системы – распределенная архитектура DLT предотвращает возникновение единой точки отказа;

2) повышенная надежность – механизмы согласования укрепляют общую целостность распределенных реестров, так как для принятия каких-либо новых данных в реестр требуется консенсус участников;

3) повышенная степень прозрачности – вредоносным программам труднее работать с DLT, так как система имеет множество отдельных уровней безопасности на уровне инфраструктуры реестра.

Децентрализованные системы определения идентичности, созданные с использованием DLT, наследуют риски безопасности, характерные для этих технологий. Кроме того, при использовании DLT для управления определением идентичности возникают дополнительные риски.

8.3.1 Управление данными идентичности

CRUD расшифровывается как Create, Read, Update, Delete (создание, чтение, редактирование, удаление). Это основные операции традиционной базы данных. В DLT, в частности в контролируемом блокчейне, объекты реализации не могут удалять транзакции, записанные в блокчейн. Невозможно даже редактирование существующих транзакций, так как они являются неизменяемыми. Поэтому операции CRUD нельзя считать обычными операциями для работы с пользовательскими данными.

Вместо этого операции на основе технологии блокчейн можно описать как CRAB, Create, Retrieve, Append, Burn (создание, извлечение, дополнение и запись). Операция дополнения, заменяющая редактирование, позволяет разработчикам лишь добавлять в технологию блокчейн новые транзакции, что приводит к изменению текущего состояния (world state – сумма всех прошлых событий/транзакций до настоящего момента). Операция записи в CRAB приводит к тому, что все ключи шифрования аннулируются, так что добавить новые транзакции или внести изменения в состояние реестра актива невозможно.

Поэтому в DLT или при использовании технологии блокчейн важно очень внимательно записывать личные данные, так как их уже нельзя будет удалить или "забыть". Поэтому лучше всего записывать данные вне цепочки, помещая в DLT указатели на эти внешние данные. Однако хранение данных вне реестра также имеет свои недостатки. В частности:

- уменьшается преимущество прозрачности, так как пользователи не знают о том, что у них нет права доступа к данным вне реестра;
- уменьшается преимущество владения данными в сети блокчейн, поскольку когда данные находятся вне реестра, они могут принадлежать любому объекту, который может получить доступ к ним.

8.3.2 Возможность взаимосвязи между ключами DID

Существует вероятность образования взаимосвязи между DID. Это может произойти, если один и тот же DID используется для нескольких отношений. Реестры DLT могут снизить этот риск, если для отношений используются попарно уникальные DID. Это означает, что для каждого отношения используется своя пара DID. В этом сценарии каждый DID действует как псевдоним [b-W3C-2]. Псевдонимный DID передается нескольким сторонам только тогда, когда субъект DID явно разрешает взаимосвязь между этими сторонами.

Следует учитывать, что даже псевдонимные DID могут оказаться взаимосвязанными [b-W3C-2], если могут быть взаимосвязаны данные в соответствующих документах DID. Например, общие имена оконечных точек обслуживания в нескольких документах DID можно использовать для сопоставления информации об одном и том же DID. Поэтому в документах DID псевдонимных DID также должны использоваться попарно уникальные открытые ключи.

8.3.3 Защита ключей DID

Управление личными ключами имеет важное значение. Если главный ключ хранится в незащищенном месте даже на одном устройстве, то вероятно хищение идентичности. Рекомендуется, чтобы использование защищенных хранилищ на устройствах было обязательным требованием.

8.3.4 Способы хранения PII

Не рекомендуется хранить в реестре конфиденциальную информацию. С развитием квантовых вычислений станет возможным взлом любого метода двустороннего шифрования, поэтому основная цель заключается в обеспечении того, чтобы конфиденциальная информация никогда не хранилась в реестре.

Хотя хеш-функции необратимы, они могут быть уязвимыми, поскольку у хакеров имеется неограниченное время для попыток их взлома методом последовательного перебора. По этой причине хеш-значения не следует хранить в реестре.

Вместо хранения в реестре собственно данных, таких как дата рождения, в нем можно хранить в форме "умного" контракта – ответы на вопросы с указанием, например, что человеку больше 21 года. Это можно рассматривать как заявление, соответствующее требованию.

В DLT рекомендуется хранить только хеш-значения личных или конфиденциальных данных. Не следует хранить в реестре данные PII, даже если они зашифрованы. Конфиденциальные данные следует хранить вне реестра и передавать проверенным объектам, которым они необходимы. Такой подход снижает риск того, что взлом DLT приведет к потере конфиденциальных данных. Для обмена данными следует использовать безопасную технологию одноранговых узлов с поддержкой внереестрового доступа. Следует использовать подходящие методы хранения данных вне реестра, включая планы архивирования и восстановления данных. Например, если владелец идентичности утверждает, что он лицензированный поставщик страховых услуг, то это можно проверить с помощью объекта, выступающего в роли доверенного поставщика в системе децентрализованного управления определением идентичности, и сохранить подтверждение в DLT в хешированной форме. Подтверждением может служить хеш-значение заявления с цифровой подписью заявителя. Рекомендуется обеспечить безопасность внереестрового хранилища.

8.3.5 Привязка к поставщику

Реестры могут быть стандартизированы, но компоненты программного обеспечения рассчитаны на конкретное решение и могут быть проприетарными и несовместимыми.

8.3.6 Атаки, нацеленные на идентичность

Распределенный реестр уязвим для атак, нацеленных на идентичность, подобных атакам, нацеленным на традиционную инфраструктуру информационных технологий, таким как спуфинг и атаки Сивиллы. Злоумышленники могут использовать такие атаки для захвата большинства узлов реестра. В случае успеха злоумышленник может взломать процедуру проверки консенсуса и защиту распределенной архитектуры реестра. Этот риск можно уменьшить с помощью решений строгой аутентификации для облачных служб каталогов.

8.3.7 Влияние сетей связи

Распределенная структура DLT может создавать проблемы для работы с множеством участников, у каждого из которых имеются свои собственные решения для защиты инфраструктуры связи. Такая структура создает проблемы для управления определением идентичности, контроля доступа, выбора конфигурации системы безопасности, хранения ключей PKI и управления ими.

Для работы DLT задействуются узлы, использующие разные топологии сетей связи, разный программный код и разные протоколы, которые могут быть уязвимы для угроз безопасности. Воздействие этих угроз варьируется в зависимости от характера DLT-реестра (частный или

общедоступный). Как таковые системы управления определением идентичности и данные идентичности уязвимы для атак на уровне сети связи, нацеленных на DLT. Разработчикам систем управления определением идентичности следует принимать во внимание следующие вопросы на уровне сети связи:

1) влияние, оказываемое нарушениями алгоритма согласования DLT на данные идентичности;
2) способы преодоления конфликтов в DLT или блокчейне;
3) план аварийного восстановления данных идентичности;
4) угрозы для данных идентичности, возникающие в том случае, когда механизмы консенсуса DLT контролирует небольшая группа участников.

8.3.8 Шифрование данных идентичности

Данные идентичности, хранящиеся в реестре, считаются конфиденциальными и личными данными владельца идентичности. Рекомендуется, чтобы пользователь имел возможность получить из реестра справочную информацию по шифрованию данных целиком или постепенно в процессе передачи, в частности при обмене данными между различными поставщиками.

8.3.9 Резервное копирование

Пользователь подвергается риску в отношении защиты своего устройства и содержимого этого устройства, в частности верифицируемых заявлений или секретных ключей и личных данных.

Существует необходимость надлежащего восстановления данных и электронного кошелька пользователя.

Кроме того, пользователям требуются гарантии того, что их данные в реестре защищены и имеют резервные копии. Методы, гарантирующие отсутствие искажения или потери данных, следует сделать доступными в виде услуг для конечных пользователей.

8.3.10 "Умные" контракты

При внедрении децентрализованных систем определения идентичности может потребоваться использование "умных" контрактов. "Умные" контракты создают разработчики с применением языков программирования. Эти программы подвержены ошибкам разработки и программирования, в частности по мере усложнения "умных" контрактов. Ввиду неопределенности в отношении точности "умных" контрактов требуется разработка структуры управления, гарантирующая, что в децентрализованных системах определения идентичности имеются надлежащие процессы и процедуры для устранения любых нарушений, возникающих из-за неточности в "умном" контракте (преднамеренной или случайной).

8.3.11 Управление сертификатами DLT

Системы управления определением идентичности решают задачи управления жизненным циклом идентичности, в число которых входит проверка идентичности. К задачам управления определением идентичности относятся создание, выдача, хранение, аннулирование и замена регистрационных данных, а также выявление мошенничества.

Использование сертификатов в реестрах создает некоторые уникальные проблемы для специалистов по безопасности. В децентрализованных системах определения идентичности потеря или ошибочное размещение личных ключей обходится дороже, чем в традиционных системах доступа. Например, в случае пропажи личных ключей из кошелька пользователя он навсегда теряет доступ к своему реестру DLT. Кража ключей также причинит больший ущерб, поскольку это эквивалентно краже идентичности. Сложность механизмов восстановления также обусловлена характером DLT. Эти проблемы легче решаются в частных реестрах, чем в общедоступных, где требуется консенсус по транзакциям.

Эти вопросы следует включить в проект систем управления DLT, поскольку центральный орган, помогающий бороться с мошенничеством или преодолевать технические трудности, отсутствует. Для этого необходимы доверенная среда управления, гарантирующая охват всех состояний жизненного цикла идентичности с момента создания, и предварительное согласование участниками DLT надлежащих процедур в поддержку услуг восстановления идентичности, таких как управление жизненным циклом ключей, выбор части полезной нагрузки блока, подлежащей шифрованию, аннулирование ключей, защита и восстановление личных ключей, а также действия в случае обнаружения мошенничества.

Библиография

[b-RFC 8141] RFC 8141, *Uniform Resource Names (URNs)*, April 2017.

[b-Angelov et al.] Angel Angelov, Mihail Milkov, Markus Sørensen, *Decentralized Identity Management System for Self-Sovereign Identity*. https://projekter.aau.dk/projekter/files/281068659/Master_Thesis_ICTE4SER4.2.pdf

[b-Baars] Djuri Baars, *Towards Self-Sovereign Identity using Blockchain Technology*. https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf

[b-Blog] Blockchain platforms. https://medium.com/blockchain-blog/17-blockchain-platforms-a-brief-introduction-e07273185a0b

[b-DIF] Decentralized Identity Foundation (DIF). https://identity.foundation/#wgs

[b-Gartner] Gartner, Blockchain, *Evolving Decentralized Identity Design*, Published 1 December 2017 – ID G00324208, By Analysts Homan Farahmand

[b-Sovrin] Sovrin Foundation. https://sovrin.org/

[b-W3C-1] W3C, *Verifiable Credentials Data Model 1.0 Expressing verifiable information on the Web*. https://www.w3.org/TR/2019/CR-vc-data-model-20190725/

[b-W3C-2] W3C, *Decentralized Identifiers (DIDs) v0.13 Data Model and Syntaxes*, August 2019. https://w3c-ccg.github.io/did-spec/

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
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	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; 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, а также соответствующие измерения и испытания
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, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2021 г.