ITUПубликации
Рекомендации

Международный союз электросвязи
Сектор стандартизации

Рекомендация

МСЭ-Т X.1410 (03/2023)

СЕРИЯ X: Сети передачи данных, взаимосвязь открытых систем и безопасность

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

Архитектура безопасности управления обменом данными на основе технологии распределенного реестра

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	X.1000-X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	X.1100-X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	X.1200-X.1299
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	X.1300-X.1499
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.1350-X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370-X.1399
Безопасность технологии распределенного реестра (DLT)	**X.1400-X.1429**
Безопасность приложений (2)	X.1450-X.1459
Безопасность веб-среды (2)	X.1470-X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	X.1500-X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	X.1600-X.1699
КВАНТОВАЯ СВЯЗЬ	X.1700-X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	X.1750-X.1799
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800-X.1819

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

Рекомендация МСЭ-Т X.1410

Архитектура безопасности управления обменом данными на основе технологии распределенного реестра

Резюме

В Рекомендации МСЭ-Т X.1410 определена архитектура безопасности управления обменом данными на основе технологий распределенного реестра (DLT). На базе этой архитектуры в настоящей Рекомендации также определены интерфейсы между функциональными объектами и процедуры управления обменом данными на основе DLT. Технология распределенного реестра преобразует отрасли, позволяя создавать инновационные решения, и изменяет методы работы органов государственной власти, учреждений и предприятий. Благодаря своим свойствам децентрализации и защиты от несанкционированного доступа эта технология обеспечивает решение для безопасного тиражирования данных, обмена данными и синхронизации данных в распределенной компьютерной сети. Существующие подходы к обмену коммерческими данными и информацией, позволяющей установить личность (PII), между компаниями и цифровыми платформами привели к появлению уязвимостей конфиденциальности вследствие взлома или неудовлетворительного управления данными. Внедрение в процесс управления обменом данными технологий DLT или блокчейна позволяет физическим лицам и компаниям осуществлять прямой контроль над своей собственной конфиденциальной информацией. При использовании решений на основе DLT в сети хранятся только данные, не относящиеся к категории PII, например хеш-значения данных. Данные PII, относящиеся к владельцу данных, хранятся вне сети. Решение на основе DLT упрощает процессы отслеживания, проверки и изменения состояния данных.

Хронологическая справка *

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор
1.0	МСЭ-Т X.1410	03.03.2023 г.	17-я	11.1002/1000/15109

Ключевые слова

DLT, архитектура безопасности, обмен данными.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL https://handle.itu.int/ после которого укажите уникальный идентификатор Рекомендации.

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

Рекомендация МСЭ-Т X.1410

Архитектура безопасности управления обменом данными на основе технологии распределенного реестра

1 Сфера применения

В настоящей Рекомендации определена архитектура безопасности обмена данными на основе DLT. В настоящую Рекомендацию входят:

– проект архитектуры безопасности обмена данными на основе технологии распределенного реестра (DLT);

– спецификация логических функций архитектуры безопасности обмена данными;

– спецификация интерфейсов между логическими функциями архитектуры безопасности;

– спецификация процедур обмена данными на основе DLT.

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 статус Рекомендации.

[ITU-T X.1408] Recommendation ITU-T X.1408 (2021), *Security threats and requirements for data access and sharing based on the distributed ledger technology*.

3 Определения

3.1 Термины, определенные в других документах

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

3.1.1 адрес (address) [b-ITU-T FG DLT D1.1]: Идентификатор объекта(ов), выполняющего транзакции или другие действия в блокчейне или сети распределенного реестра.

3.1.2 блокчейн (blockchain) [b-ITU-T X.1400]: Разновидность распределенного реестра, состоящего из данных, записанных в цифровом формате и организованных в виде последовательно нарастающей цепочки блоков, причем все блоки криптографически связаны и защищены от несанкционированного повреждения и изменения.

3.1.3 орган по сертификации (certification authority, CA) [b-ITU-T X.509]: Орган, которому один или несколько пользователей доверили разработку и скрепление цифровой подписью сертификатов открытых ключей. Орган по сертификации может выполнять факультативную функцию по созданию ключей для пользователей.

3.1.4 поставщик данных (data provider) [b-ISO/IEC/IEEE 15939]: Физическое лицо или организация, предоставляющие данные.

3.1.5 идентичность (identity) [b-ISO/IEC 29100]: Набор свойств, который может использоваться для идентификации субъекта информации, позволяющей установить личность.

3.1.6 вне блокчейна (off-chain) [b-ISO 22739]: Относится к блокчейн-системе, но находится, выполняется или запускается за ее пределами.

3.1.7 в блокчейне (on-chain) [b-ISO 22739]: Находится, выполняется или запускается внутри блокчейн-системы.

3.1.8 информация, позволяющая установить личность (personally identifiable information (PII)) [b-ISO/IEC 29100]: Любая информация, которая: a) может быть использована для идентификации субъекта PII, к которому относится такая информация; или b) прямо или косвенно связана с субъектом PII.

ПРИМЕЧАНИЕ. – Для определения возможности идентификации субъекта PII следует учесть все способы идентификации этого физического лица, которые, исходя из разумных предположений, может использовать заинтересованное лицо, хранящее данные, или любая другая сторона.

3.1.9 инфраструктура открытых ключей (public-key infrastructure, PKI) [b-ITU-T X.509]: Инфраструктура, способная поддерживать управление открытыми ключами для обеспечения услуг аутентификации, шифрования, целостности или фиксации авторства.

3.1.10 смарт-контракт ("умный" контракт) (smart contract) [b-ITU-T X.1400]: Программа, созданная на основе системы распределенного реестра, которая кодирует правила для конкретных типов транзакций системы распределенного реестра таким образом, чтобы эти транзакции можно было проверить и осуществить после выполнения определенных условий.

3.1.11 система симметричного шифрования (symmetric encryption system) [b-ISO/IEC 18033-1]: Метод шифрования, используемый для защиты конфиденциальности данных и состоящий из трех компонентов: алгоритма шифрования, алгоритма дешифрования и метода генерирования ключей, причем алгоритмы шифрования и дешифрования используют один и тот же ключ.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определен следующий термин.

3.2.1 потребитель данных (data consumer): Пользователь, который считывает данные и работает с ними в рамках выявленных лексических или программных границ.

ПРИМЕЧАНИЕ. – Взято из [b-ISO/IEC 20944-1].

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы:

API	Application Programming Interface	Интерфейс прикладного программирования
CA	Certification Authority	Орган по сертификации
DLT	Distributed Ledger Technology	Технология распределенного реестра
PII	Personally Identifiable Information	Информация, позволяющая установить личность
PKI	Public Key Infrastructure	Инфраструктура открытых ключей

5 Соглашения по терминологии

В настоящей Рекомендации:

ключевое слово "**рекомендуется**" означает требование, которое рекомендуется, но не является абсолютно необходимым; таким образом, для заявления о соответствии настоящей Рекомендации это требование не является обязательным;

ключевые слова "**может**" и "**факультативно**" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Эти термины не означают, что вариант реализации поставщика должен обеспечивать выполнение соответствующей функции, активируемой по желанию оператора сети/поставщика услуг. Это означает лишь, что поставщик может факультативно предоставить данную функцию и по-прежнему заявлять о соответствии спецификации.

Для обозначения функций в настоящей Рекомендации используется *курсив.*

6 Архитектура обмена данными на основе DLT

Благодаря своим свойствам децентрализации и защиты от несанкционированного доступа эта технология обеспечивает решение для безопасного тиражирования данных, обмена данными и синхронизации данных в распределенной компьютерной сети. Существующие подходы к обмену коммерческими данными и информацией, позволяющей установить личность (PII), между компаниями и цифровыми платформами привели к появлению уязвимостей конфиденциальности вследствие взлома или неудовлетворительного управления данными. Внедрение в процесс управления обменом данными технологий DLT или блокчейна позволяет физическим лицам и компаниям осуществлять прямой контроль над своей собственной конфиденциальной информацией. При использовании решений на основе DLT в сети хранятся только данные, не относящиеся к PII, например хеш-значения данных. Данные PII, относящиеся к владельцу данных, хранятся вне сети. Решение на основе DLT упрощает процессы отслеживания, проверки и изменения состояния данных. В данном контексте в настоящей Рекомендации определена архитектура безопасности управления обменом данными на основе DLT. Для управления обменом данными используется симметричная система шифрования, когда в алгоритмах шифрования и дешифрования используются один и тот же ключ. Угрозы безопасности описаны в [ITU-T X.1408].

Настоящая Рекомендация разработана на основе [ITU-T X.1408]. Притом что [ITU-T X.1408] разработана с концептуальной точки зрения, настоящая Рекомендация разработана с точки зрения реализации. В таблице 1 сопоставляется терминология, используемая в настоящей Рекомендации и в [ITU-T X.1408].

Таблица 1 – Сопоставление терминологии настоящей Рекомендации и [ITU-T X.1408]

Настоящая Рекомендация	[ITU-T X.1408]
Поставщик данных	Участник процесса обмена данными (владелец данных)
Потребитель данных	Клиент – потребитель данных (обработчик данных)
Сервер хранения ключей	Сервер управления ключами
Сервер хранения данных	Сервер хранения данных (поставщик услуг хранения данных)
Управление обменом данными на основе DLT	Брокер данных

6.1 Обзор функциональной архитектуры

На рисунке 1 показана функциональная архитектура системы управления обменом данными на основе DLT с точки зрения реализации. Она соответствует архитектуре доступа к данным и обмена данными на основе DLT, показанной на рисунке B.1 [ITU-T X.1408]. Последняя разработана с концептуальной точки зрения и представляет собой архитектуру высокого уровня. Функциональная архитектура, показанная на рисунке 1, состоит из пяти функциональных компонентов, обозначенных блоками синего цвета, и трех функциональных компонентов, обозначенных блоками серого цвета.

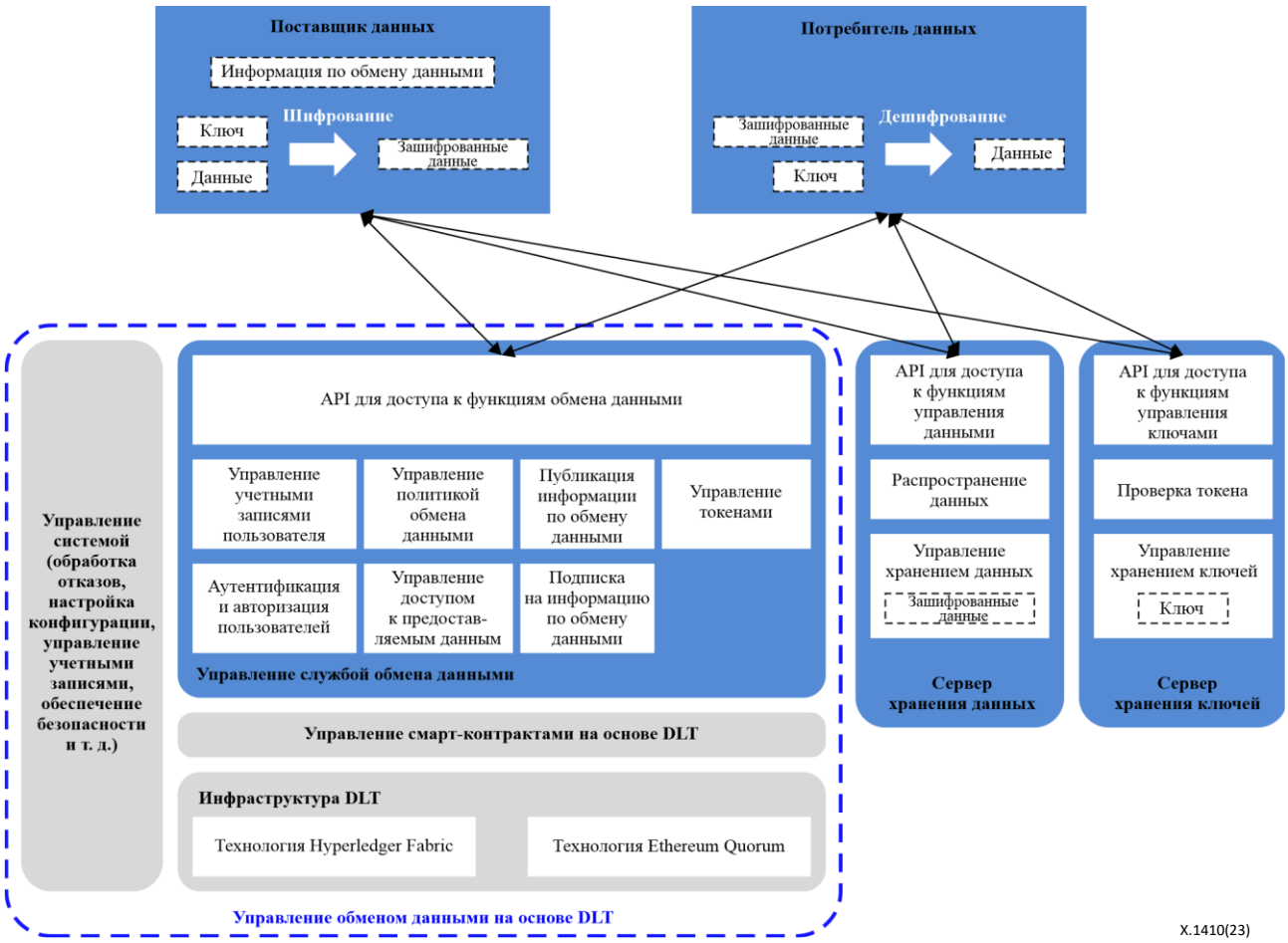

Рисунок 1 – Функциональная архитектура системы управления обменом данными на основе DLT

Эти компоненты можно описать следующим образом:

– пятью синими блоками обозначены функциональные компоненты *поставщика данных, потребителя данных, управления службой обмена данными, сервера хранения ключей и сервера хранения данных,* которые определены и подробно описаны в пункте 6.2;

– тремя серыми блоками обозначены функциональные компоненты *инфраструктуры DLT, управления смарт-контрактами на основе DLT и управления системой (например, отказами, конфигурацией, характеристиками, учетными записями, обеспечением безопасности),* в которых используются существующие платформы DLT с открытым исходным кодом (например, Hyperledger Fabric) и которые не рассматриваются в настоящей Рекомендации.

Процедуры управления обменом данными на основе DLT описаны в Приложении A.

6.2 Функциональные компоненты

6.2.1 Поставщик и потребитель данных

В настоящей Рекомендации вводятся два типа пользователей: поставщик данных (т. е. пользователи, которые предоставляют свои данные) и потребитель данных (т. е. пользователи, которые потребляют данные, предоставленные другими пользователями). У пользователей обоих типов имеются следующие одинаковые функциональные возможности:

1) получать цифровые сертификаты (включая открытые ключи) и соответствующие секретные ключи из органа по сертификации (CA);

2) безопасно хранить полученные цифровые сертификаты и соответствующие секретные ключи;

3) поддерживать установление соединения с сервером управления обменом данными на основе DLT;

4) получать и хранить цифровые сертификаты, параметры настройки сети и конфигурации сетевых узлов DLT;

5) получать уведомления из системы управления обменом данными на основе DLT;

6) использовать симметричную систему шифрования.

У поставщика и потребителя данных имеются собственные конкретные функциональные возможности.

– *Поставщик данных* обладает следующими функциональными возможностями:

1) собирать необработанные данные и десенсибилизировать их (например, делать данные анонимными, удаляя конфиденциальную информацию, такую как имя, номер мобильного телефона, данные кредитной карты), не ухудшая качество передаваемых данных;

2) генерировать ключ симметричной системы шифрования;

3) шифровать данные с помощью ключа, используя симметричную систему шифрования;

4) безопасно хранить шифротекст и соответствующий ключ шифрования на локальном или удаленном сервере;

5) обеспечить взаимную аутентификацию в системе управления обменом данными на основе DLT;

6) передавать в систему управления обменом данными на основе DLT информацию по обмену данными, в том числе идентификатор поставщика данных, открытый ключ поставщика данных, идентификатор шифротекста и адрес его хранения, идентификатор ключа шифрования и адрес его хранения, перечень отраслей, организациям которых разрешен доступ к данным, перечень пользователей, которым разрешен доступ к данным, и другие атрибуты данных (такие, как категория, характеристика, условия использования и цена данных);

7) объединять информацию по обмену данными с другой информацией для формирования политики обмена данными и подписывать такую политику обмена данными своим секретным ключом; 8) передавать политику обмена данными с соответствующей цифровой подписью в систему управления обменом данными на основе DLT; 9) получать от системы управления обменом данными на основе DLT уведомления о создании смарт-контракта обмена данными; 10) управлять политикой обмена данными, например правилами поиска и обновления.

– *Потребитель данных* обладает следующими функциональными возможностями:

1) подписываться на публикуемые сообщения обмена данными;

2) производить взаимную аутентификацию в системе управления обменом данными на основе DLT;

3) получать информацию по обмену данными;

4) передавать в систему управления обменом данными на основе DLT информацию о потребителе данных (например, идентификатор потребителя данных, открытый ключ потребителя данных) и информацию по обмену данными (например, идентификатор поставщика данных, открытый ключ поставщика данных, идентификатор шифротекста и идентификатор ключа шифрования) вместе с цифровой подписью (выполняемой с применением секретного ключа потребителя данных);

5) получать от системы управления обменом данными на основе DLT уведомления с информацией по обмену данными, адресом хранения ключа, адресом хранения шифротекста и токеном доступа;

6) передавать на сервер хранения ключей токен доступа для получения ключа шифрования данных в соответствии с адресом хранения ключа;

7) получать шифротекст по адресу хранения данных;

8) расшифровывать шифротекст полученным ключом симметричного шифрования для получения данных в виде открытого текста;

9) управлять записями об обращении к предоставленным данным.

6.2.2 Управление службой обмена данными

Ниже описаны функциональные возможности каждого компонента системы управления службой обмена данными.

– Компонент ***управления учетными записями пользователей*** выполняет функции управления учетными записями пользователей, такими как создание, обновление, запрос или удаление.

– Компонент ***аутентификации и авторизации пользователей*** обеспечивает следующие функциональные возможности:

1) осуществлять взаимную аутентификацию пользователей (т. е. поставщика данных и потребителя данных);

2) разрешать пользователям обмен данными и доступ к предоставленным данным.

– Компонент ***управления политикой обмена данными*** обеспечивает следующие функциональные возможности:

1) получать от поставщика данных информацию по обмену данными и политике обмена данными вместе с соответствующей цифровой подписью; 2) создавать транзакции DLT в соответствии с информацией, полученной от поставщика данных; 3) передавать транзакции DLT в нижележащие компоненты (т. е. в *инфраструктуру DLT* и в компонент *управления смарт-контрактами*) для создания смарт-контрактов обмена данными, которые будут распространяться среди сетевых узлов DLT; 4) уведомлять *поставщика* данных и компонент *публикации информации по обмену данными* о создании смарт-контракта обмена данными; 5) разрешать поставщикам данных управлять предоставляемыми ими данными.

– Компонент ***управления доступом к предоставляемым данным*** обеспечивает следующие функциональные возможности:

1) принимать от потребителя данных запросы на получение доступа к данным (включая информацию о потребителе данных, информацию о запрашиваемых данных и соответствующую цифровую подпись) и проверять, разрешен ли потребителю данных доступ к данным, в соответствии с политикой обмена данными (например, доступ к предоставляемым данным могут получать только потребители данных из определенной отрасли или страны); 2) создавать транзакции DLT в соответствии с информацией, полученной от потребителя данных; 3) передавать транзакции DLT в нижележащие компоненты (например, в *инфраструктуру DLT*) для создания записей о доступе к данным, которые распространяются среди сетевых узлов DLT; 4) уведомлять компонент *управления токенами* о создании транзакции доступа к данным и необходимости создания токена доступа; 5) получать токен доступа от компонента *управления токенами*; 6) передавать потребителю данных информацию для доступа к предоставляемым данным (например, токен доступа, адрес хранения ключа, адрес хранения данных); 7) разрешать потребителю данных управлять относящимися к нему записями об обращении к предоставленным данным.

– Компонент ***публикации информации по обмену данными*** обеспечивает следующие функциональные возможности:

1) получать от компонента *управления политикой обмена данными* уведомления с новой информацией по обмену данными; 2) публиковать новую информацию по обмену данными; 3) уведомлять компонент *подписки на информацию по обмену данными* о публикации новой информации по обмену данными.

– Компонент ***подписки на информацию по обмену данными*** обеспечивает следующие функциональные возможности:

1) получать от компонента *управления информацией по обмену данными* уведомления с новой информацией по обмену данными; 2) рассылать новую информацию по обмену данными подписчикам.

– Компонент ***управления токенами*** обеспечивает следующие функциональные возможности:

1) получать от компонента *управления доступом к предоставляемым данным* уведомления о необходимости создания токена доступа; 2) создавать токены доступа; 3) передавать созданные токены доступа в компонент *управления доступом к предоставляемым данным*.

– ***Интерфейс прикладного программирования (API) для доступа к функциям обмена данными*** позволяет пользователям управлять перечисленными выше услугами обмена данными и получать доступ к ним.

6.2.3 Сервер хранения ключей

Ниже описаны функциональные возможности каждого компонента сервера хранения ключей.

– Компонент ***управления хранением ключей*** обеспечивает следующие функциональные возможности:

1) принимать от *поставщика данных* запросы на хранение ключей;
2) выполнять аутентификацию *поставщика данных*;
3) обеспечивать надежное хранение ключей, например в виде зашифрованных данных и/или в изолированном хранилище;
4) уведомлять *поставщика данных* о хранении ключа;
5) получать от компонента *проверки токенов* уведомления с результатом проверки токена доступа;
6) передавать ключи *потребителю данных*.

– Компонент ***проверки токенов*** обеспечивает следующие функциональные возможности:

1) получать токен доступа от потребителя данных;
2) проверять полученный токен доступа;
3) передавать результат проверки в компонент *управления хранением ключей*.

– ***API для доступа к функциям управления ключами*** позволяет пользователям управлять ключами шифрования данных и получать доступ к ним.

6.2.4 Сервер хранения данных

Ниже описаны функциональные возможности каждого компонента сервера хранения данных.

– Компонент ***управления хранением данных*** обеспечивает следующие функциональные возможности:

1) принимать от *поставщика данных* запросы на сохранение шифротекста;
2) выполнять аутентификацию *поставщика данных*;
3) хранить шифротекст;
4) уведомлять *поставщика данных* о хранении шифротекста.

– Компонент ***распространения данных*** обеспечивает следующие функциональные возможности:

1) получать запросы от *потребителя данных*;
2) выполнять аутентификацию *потребителя данных*;
3) передавать *потребителю данных* шифротекст.

– ***API для доступа к функциям управления данными*** позволяет пользователям управлять предоставляемыми данными и получать доступ к ним.

7 Архитектура безопасности управления обменом данными на основе DLT

В соответствии с функциональной архитектурой, представленной на рисунке 1, потребители данных запрашивают и получают ключ шифрования данных, с помощью которого они затем расшифровывают данные шифротекста и в результате получают предоставляемые данные в виде открытого текста. После этого данные, представленные в виде открытого текста, уже не могут контролироваться с помощью системы управления обменом данными на основе DLT. Потребители могут переслать данные в виде открытого текста другим пользователям, не имеющим разрешения на доступ к ним.

Для того чтобы поставщики данных могли безопасно обмениваться данными с другими, а у потребителей данных не было возможности переслать полученные данные другим пользователям

в виде открытого текста, функциональная архитектура, представленная на рисунке 1, должна содержать дополнительные средства безопасности, как показано на рисунке 2.

7.1 Обзор архитектуры безопасности

На рисунке 2 показана архитектура безопасности системы управления обменом данными на основе DLT, которая обеспечивает условия для того, чтобы:

– соединения между функциональными компонентами, представленными на рисунке 1, были безопасными;

– поставщики данных осуществляли шифрование данных и выдавали разрешения на доступ к ним, прежде чем они попадут в другие руки;

– потребители данных расшифровали данные, полученные в шифротексте, в соответствии с имеющимся у них разрешением, чтобы получить доступ к ним;

– потребители данных по завершении работы с полученными данными шифровали их так же, как это делают поставщики данных, чтобы полученные данные хранились у потребителей данных в виде шифротекста;

– потребители данных передавали их другим только в виде шифротекста.

Таким образом, даже если пользователи получают данные, пересылаемые другими, они должны запрашивать разрешение на доступ к ним через систему управления обменом данными на основе DLT.

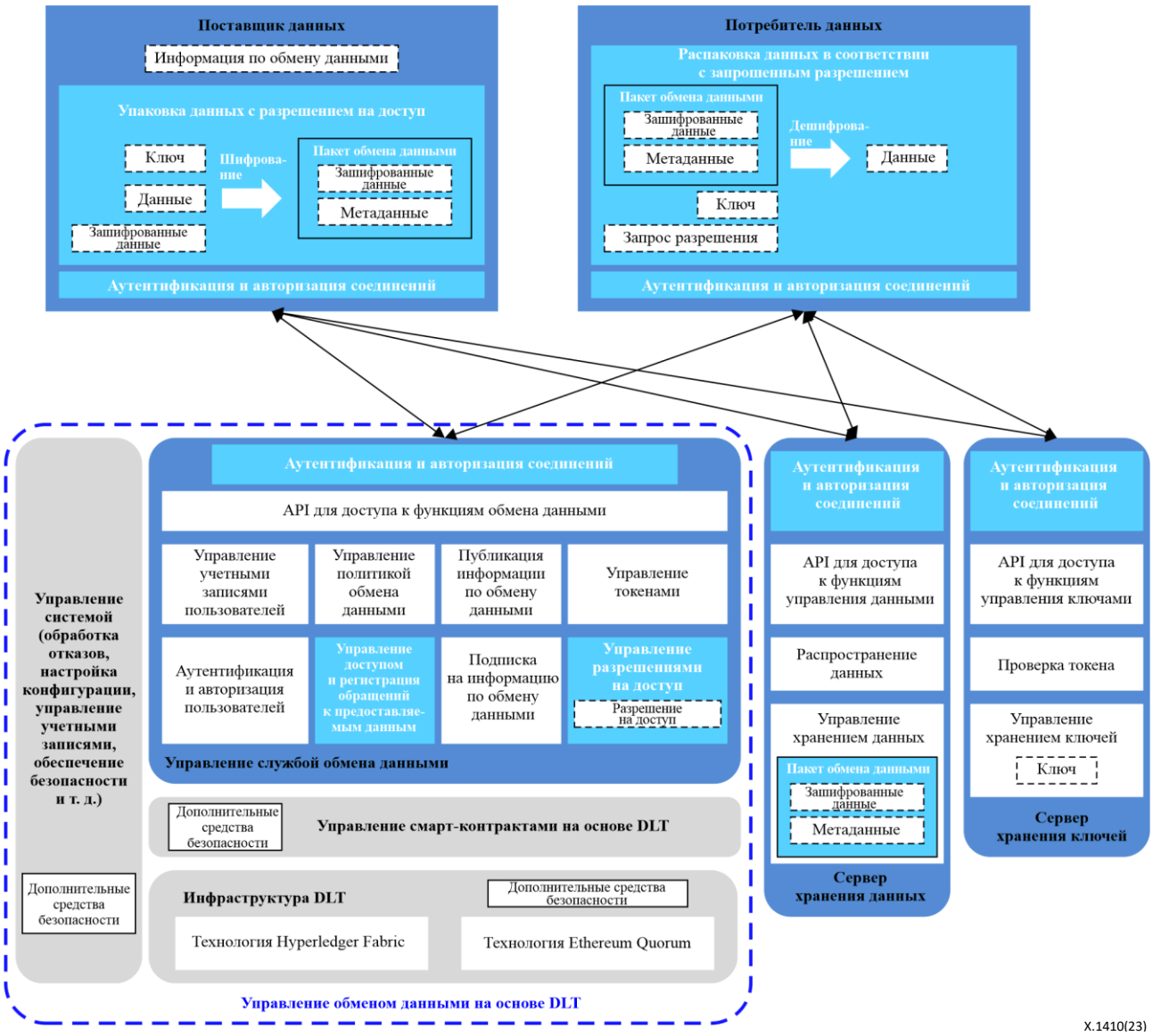

Рисунок 2 – Архитектура безопасности системы управления обменом данными на основе DLT

В отличие от рисунка 1, рисунок 2 содержит блоки функциональных компонентов голубого цвета, соответствующие логическим функциям безопасности, которые подробно описаны в пункте 7.2.

Дополнительные средства обеспечения безопасности трех функциональных компонентов, представленных на рисунке 2 блоками серого цвета, в настоящей Рекомендации не рассматриваются; см. [b-ITU-T X.1402].

7.2 Функциональные компоненты обеспечения безопасности

7.2.1 Упаковка данных с разрешением на доступ

Чтобы пользователи могли оформлять разрешения на доступ к предоставляемым данным, *поставщик данных*, представленный на рисунке 1, должен ввести новую логическую функцию безопасности – *упаковку данных с разрешением на доступ*, которая обеспечивает следующие функциональные возможности:

– создание ключей симметричной системы шифрования для шифрования предоставляемых данных;

– установление соединения с *сервером хранения ключей* для регистрации идентификатора и адреса ключа;

– установление соединения с *сервером хранения данных* для регистрации идентификатора и адреса пакета обмена данными;

– оформление разрешений на доступ к предоставляемым данным, которые содержат информацию о времени доступа и сроке действия, метку "только для чтения", идентификатор ключа и адрес его хранения, а также идентификатор пакета обмена данными и адрес его хранения;

– создание метаданных, содержащих идентификатор пакета обмена данными, идентификатор поставщика данных, открытый ключ поставщика данных и подпись предшествующей информации;

– создание пакетов обмена данными, содержащих зашифрованные данные и метаданные;

– загрузка ключей на *сервер хранения ключей* по защищенному каналу передачи;

– загрузка пакетов обмена данными на *сервер хранения данных* по защищенному каналу передачи;

– загрузка разрешений на доступ к данным в систему *управления службой обмена данными* по защищенному каналу передачи.

7.2.2 Распаковка данных в соответствии с запрошенным разрешением

Чтобы пользователи могли обращаться к предоставленным им данным в соответствии с запрошенным разрешением, *потребитель данных,* представленный на рисунке 1, должен ввести новую логическую функцию безопасности – *распаковку данных в соответствии с запрошенным разрешением*, которая обеспечивает следующие функциональные возможности:

– получение адреса для исполнения смарт-контракта обмена данными;

– установление соединения с системой *управления службой обмена данными*, исполнение смарт-контрактов обмена данными и получение запрошенных разрешений, которые содержат информацию о времени доступа и сроке действия, метку "только для чтения", идентификатор ключа и адрес его хранения, а также идентификатор пакета обмена данными и адрес его хранения;

– установление соединения с *сервером хранения ключей* для получения ключа шифрования;

– установление соединения с *сервером хранения данных* для получения пакета обмена данными, содержащего зашифрованные данные и метаданные;

– проверка принятых пакетов обмена данными с применением подписи, содержащейся в метаданных;

– дешифрование зашифрованных данных с применением ключа шифрования;

– представление пользователям полученных данных в виде открытого текста в соответствии с запрошенным разрешением;

– по завершении работы с полученными данными – зашифровывание их тем же способом, каким пользуются поставщики данных.

7.2.3 Управление разрешениями на доступ

Чтобы пользователи могли оформить разрешение на доступ к предоставляемым им данным или обращаться к полученным данным в соответствии с запрошенным разрешением, система *управления службой обмена данными*, показанная на рисунке 1, должна быть дополнена новой логической функцией безопасности – *управлением разрешениями на доступ*, которая обеспечивает следующие функциональные возможности:

– поддержка пользователей, оформляющих разрешение на доступ к предоставляемым данным:

  • получение от компонента *управления политикой обмена данными* разрешения на доступ, оформленного *поставщиком данных*;

  • сохранение разрешения на доступ;

  • передача ответа в компонент *управления политикой обмена данными*;

– поддержка пользователей, обращающихся к полученным данным в соответствии с запрошенным разрешением:
  - получение от компонента *управления доступом и регистрации обращений к предоставляемым данным* разрешения, запрошенного *потребителем данных*;
  - создание запрошенного разрешения;
  - передача запрошенного разрешения в компонент *управления доступом и регистрации обращений к предоставляемым данным.*

7.2.4 Управление доступом и регистрация обращений к предоставляемым данным

Чтобы пользователи могли отслеживать обращения к их данным, компонент *управления доступом и регистрации обращений к предоставляемым данным*, показанный на рисунке 2, должен быть дополнен следующими возможностями:

– установление соединения с компонентом *управления разрешениями на доступ* для получения запрошенного разрешения;

– регистрация обращений к предоставленным данным на основе запрошенного разрешения.

7.2.5 Аутентификация и авторизация соединений

Для обеспечения безопасности соединений пять функциональных компонентов, показанных на рисунке 1 (*поставщик данных, потребитель данных,* компонент *управления службой обмена данными, сервер хранения ключей и сервер хранения данных*), должны быть дополнены новой логической функцией безопасности – *аутентификацией и авторизацией соединений*.

Когда *поставщик данных* или *потребитель данных* направляет запрос компоненту *управления службой обмена данными, серверу хранения ключей* или *серверу хранения данных*, компонент *аутентификации и авторизации соединений* обеспечивает следующие функциональные возможности:

– аутентификация *поставщика данных/потребителя данных* в системе *управления службой обмена данными/на сервере хранения ключей/сервере хранения данных* с применением сертификатов [b-IETF RFC 4306], [b-IETF RFC 5246] или предварительно переданного ключа [b-IETF RFC 4279], [b-IETF RFC 4306];

– аутентификация системы *управления службой обмена данными/сервера хранения ключей/сервера хранения данных поставщиком данных/потребителем данных* с применением сертификатов [b-IETF RFC 4306], [b-IETF RFC 5246];

– аутентификация *поставщика данных/потребителя данных* в системе *управления службой обмена данными/на сервере хранения ключей/сервере хранения данных* с применением белого/черного списков [b-IETF RFC 5782], [b-IETF RFC 5851] или списка управления доступом [b-IETF RFC 4314], [b-IETF RFC 4949];

– генерирование сеансового ключа, используемого для защиты соединений между *поставщиком данных/потребителем данных* и системой *управления службой обмена данными/сервером хранения ключей/сервером хранения данных*.

7.3 Процедуры безопасного обмена данными

7.3.1 Процедура предоставления данных поставщиками данных с оформлением разрешения на доступ

Процедура предоставления данных поставщиками данных с оформлением разрешения на доступ иллюстрируется на рисунке 3.

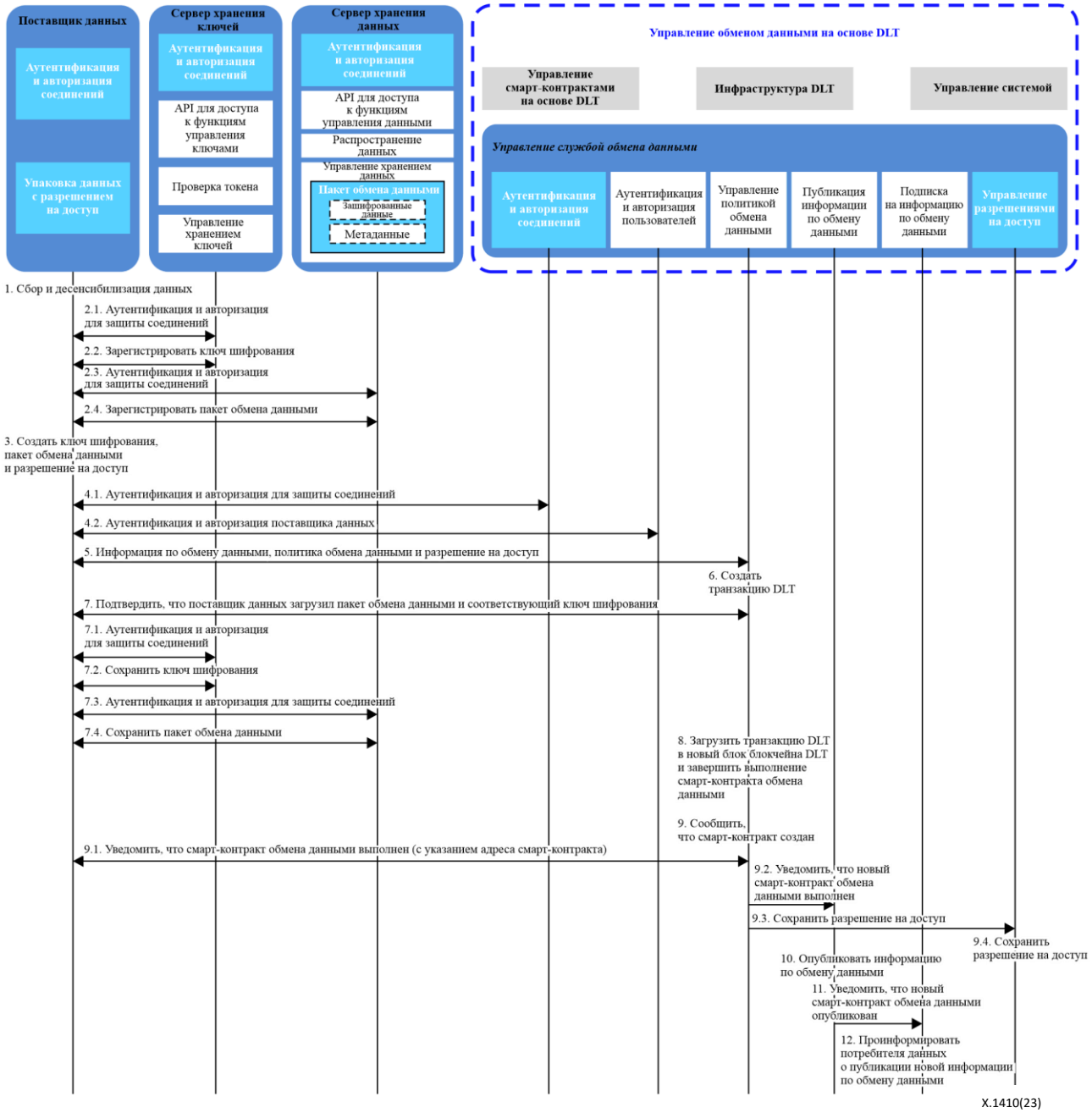

Рисунок 3 – Процедура предоставления данных поставщиками данных с оформлением разрешения на доступ

Как показано на рисунке 3, процедура производится следующим образом.

1) *Поставщик данных* собирает исходные данные и десенсибилизирует их, не оказывая при этом негативного влияния на качество предоставляемых данных.

2) *Поставщик данных* регистрирует пакет обмена данными и его ключ на локальном или удаленном сервере хранения ключей и сервере хранения данных следующим образом:

   2.1) *поставщик данных* и компонент *аутентификации и авторизации соединений сервера хранения ключей* проводят взаимную аутентификацию и получают сеансовый ключ, который будет использоваться для защиты последующих сеансов связи между ними;

   2.2) *поставщик данных* устанавливает соединение с *сервером хранения ключей* и регистрирует идентификатор ключа и адрес, по которому его можно получить;

2.3) *поставщик данных* и компонент *аутентификации и авторизации соединений сервера хранения данных* проводят взаимную аутентификацию и получают сеансовый ключ, который будет использоваться для защиты последующих сеансов связи между ними;

2.4) *поставщик данных* устанавливает соединение с *сервером хранения данных* и регистрирует идентификатор пакета обмена данными и адрес, по которому его можно получить.

3) *Поставщик данных* создает информацию по обмену данными, в том числе идентификатор поставщика данных, открытый ключ поставщика данных, идентификатор пакета обмена данными и адрес его хранения, идентификатор ключа и адрес его хранения, перечень отраслей, организациям которых разрешен доступ, перечень пользователей, которым разрешен доступ, и другие атрибуты данных (такие, как категория, характеристика, условия использования и цена данных).

Поставщик данных создает ключ, используемый для шифрования предоставляемых данных.

Поставщик данных оформляет разрешения на доступ к данным, которые содержат информацию о времени доступа и сроке действия, метку "только для чтения", идентификатор ключа и адрес его хранения, а также идентификатор пакета обмена данными, подлежащего передаче, и адрес его хранения.

Поставщик данных создает метаданные, содержащие идентификатор пакета обмена данными, идентификатор поставщика данных, открытый ключ поставщика данных и подпись предшествующей информации.

Поставщик данных создает пакет обмена данными, содержащий зашифрованные данные и метаданные.

4) Перед публикацией предоставляемых данных необходимо, чтобы:

4.1) *поставщик данных* и компонент *аутентификации и авторизации соединений* системы *управления службой обмена данными* провели взаимную аутентификацию и получили сеансовый ключ, который будет использоваться для защиты последующих сеансов связи между ними;

4.2) *поставщик данных* и компонент *аутентификации и авторизации пользователей* системы *управления службой обмена данными* провели взаимную аутентификацию. После успешной взаимной аутентификации компонент *аутентификации и авторизации пользователей* проверяет, имеет ли поставщик данных право публиковать предоставляемые данные.

5) *Поставщик данных* предоставляет информацию по обмену данными в соответствии с требованиями компонента *управления политикой обмена данными* системы *управления службой обмена данными*. *Поставщик данных* создает политику обмена данными с информацией по обмену данными и другой информацией. *Поставщик данных* передает информацию по обмену данными, политику обмена данными, разрешение на доступ и свою цифровую подпись в компонент *управления политикой обмена данными.*

6) Получив от *поставщика данных* информацию по обмену данными, политику обмена данными, разрешение на доступ и соответствующую цифровую подпись, компонент *управления политикой обмена данными* проверяет цифровую подпись и создает транзакцию DLT.

7) Компонент *управления политикой обмена данными* подтверждает *поставщику данных*, что ключ и пакет обмена данными сохранены соответственно на *сервере хранения ключей* и *сервере хранения данных*. В противном случае необходимо предпринять следующие шаги:

7.1) *поставщик данных* и компонент *аутентификации и авторизации соединений сервера хранения ключей* проводят взаимную аутентификацию и получают сеансовый ключ, который будет использоваться для защиты последующих сеансов связи между ними;

7.2) *поставщик данных* устанавливает соединение с *сервером хранения ключей* и сохраняет на нем ключ;

7.3) *поставщик данных* и компонент *аутентификации и авторизации соединений сервера хранения данных* проводят взаимную аутентификацию и получают сеансовый ключ, который будет использоваться для защиты последующих сеансов связи между ними;

7.4) *поставщик данных* устанавливает соединение *с сервером хранения данных* и сохраняет на нем пакет обмена данными.

8) Компонент *управления политикой обмена данными* передает одну или несколько транзакций DLT вместе с их цифровыми подписями в нижележащие компоненты *инфраструктуры DLT* и компонент *управления смарт-контрактами на основе DLT* для формирования нового блока, содержащего один или несколько смарт-контрактов обмена данными. Вновь сгенерированный блок распространяется среди соответствующих узлов DLT. Загрузка транзакций DLT в блокчейн DLT зависит от конкретной технологии реализации (например, Hyperledger Fabric, Ethereum Quorum), рассмотрение которой выходит за рамки данной Рекомендации.

9) Компонент *управления политикой обмена данными* информирует соответствующие компоненты о создании смарт-контракта обмена данными.

9.1) Компонент *управления политикой обмена данными* уведомляет *поставщика данных* о том, что смарт-контракт обмена данными выполнен. Уведомление включает адрес для исполнения смарт-контракта.

9.2) Компонент *управления политикой обмена данными* уведомляет компонент *публикации информации по обмену данными* о том, что смарт-контракт обмена данными выполнен. Уведомление включает адрес для исполнения смарт-контракта и информацию по обмену данными.

9.3) Компонент *управления политикой обмена данными* уведомляет компонент *управления разрешениями на доступ* о том, что смарт-контракт обмена данными выполнен. Уведомление включает адрес для исполнения смарт-контракта и разрешение на доступ.

9.4) Компонент *управления разрешениями на доступ* сохраняет разрешение на доступ.

10) Получив уведомление от компонента *управления политикой обмена данными,* компонент *публикации информации по обмену данными* публикует вновь полученную информацию по обмену данными.

11) Компонент *публикации информации по обмену данными* информирует компонент *подписки на информацию по обмену данными* о том, что смарт-контракт обмена данными выполнен. Уведомление включает адрес для исполнения смарт-контракта и новую информацию по обмену данными.

12) Получив уведомление от компонента *публикации информации по обмену данными,* компонент *подписки на информацию по обмену данными* рассылает подписчикам адрес для исполнения смарт-контракта и новую информацию по обмену данными.

7.3.2 Процедура обращения потребителей данных к предоставляемым данным в соответствии с запрошенным разрешением

Процедура обращения потребителей данных к предоставляемым данным в соответствии с запрошенным разрешением иллюстрируется на рисунке 4.

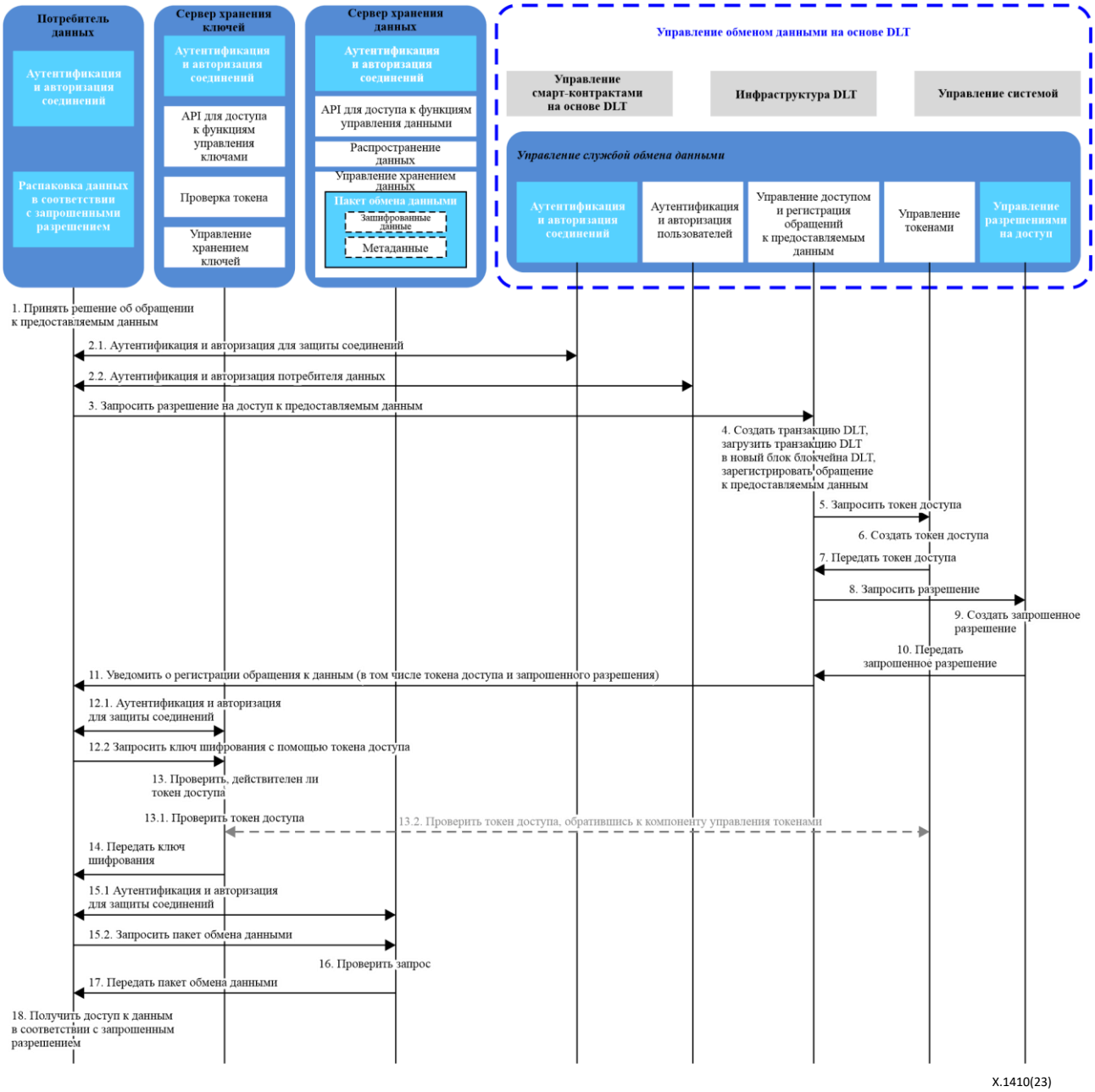

Рисунок 4 – Процедура обращения потребителей данных к предоставляемым данным в соответствии с запрошенным разрешением

Как показано на рисунке 4, процедура обращения потребителей данных к предоставляемым данным в соответствии с запрошенным разрешением производится следующим образом.

1) *Потребитель данных* получает информацию по обмену данными, выполняя поиск в компоненте *публикации информации по обмену данными*, подписавшись на публикуемую информацию либо получая ее от других. *Потребитель данных* решает обратиться к предоставляемым данным и исполняет смарт-контракт обмена данными.

2) Перед исполнением смарт-контракта обмена данными для обращения к предоставляемым данным выполняются следующие операции.

   2.1) *Потребитель данных* и компонент *аутентификации и авторизации соединений* системы *управления службой обмена данными* проводят взаимную аутентификацию и получают сеансовый ключ, который будет использоваться для защиты последующих сеансов связи между ними.

2.2) *Потребитель данных* обеспечивает взаимную аутентификацию с компонентом *аутентификации и авторизации пользователей* системы *управления службой обмена данными*. После успешной взаимной аутентификации компонент *аутентификации и авторизации пользователей* проверяет, имеет ли потребитель данных право обращаться к предоставляемым данным.

3) *Потребитель данных* передает свою идентификационную информацию (например, идентификатор, открытый ключ) и информацию по обмену данными вместе со своей цифровой подписью в компонент *управления доступом и регистрации обращений к предоставляемым данным.*

4) Получив идентификационную информацию *потребителя данных*, информацию по обмену данными и цифровую подпись, компонент *управления доступом и регистрации обращений к предоставляемым данным* проверяет цифровую подпись, а затем проверяет, разрешен ли потребителю данных доступ к данным в соответствии с политикой обмена данными (например, доступ к предоставляемым данным может получить только потребитель данных из определенной отрасли или страны). Если все требования для получения доступа к предоставляемым данным выполнены, компонент *управления доступом и регистрации обращений к предоставляемым данным* создает транзакцию DLT в соответствии с информацией, полученной от потребителя данных. Компонент *управления доступом и регистрации обращений к предоставляемым данным* передает одну или несколько транзакций DLT вместе со своей цифровой подписью в нижележащие компоненты *инфраструктуры DLT* и компонент *управления смарт-контрактами на основе DLT* для формирования нового блока, содержащего одну или несколько записей об обращении к данным. Вновь сгенерированный блок распространяется среди соответствующих сетевых узлов DLT. Загрузка транзакций DLT в блокчейн DLT зависит от конкретной технологии реализации (например, Hyperledger Fabric, Ethereum Quorum), рассмотрение которой выходит за рамки данной Рекомендации.

5) Компонент *управления доступом и регистрации обращений к предоставляемым данным* информирует компонент *управления токенами* о необходимости создания токена доступа.

6) Получив уведомление от компонента *управления доступом и регистрации обращений к предоставляемым данным*, компонент *управления токенами* создает токен доступа.

7) Компонент *управления токенами* передает созданный токен доступа в компонент *управления доступом и регистрации обращений к предоставляемым данным*.

8) Компонент *управления доступом и регистрации обращений к предоставляемым данным* информирует о создании запрошенного разрешения компонент *управления разрешениями на доступ*.

9) Получив уведомление от компонента *управления доступом и регистрации обращений к предоставляемым данным,* компонент *управления разрешениями на доступ* создает запрошенное разрешение.

10) Компонент *управления разрешениями на доступ* передает запрошенное разрешение в компонент *управления доступом и регистрации обращений к предоставляемым данным.*

11) Получив токен доступа и запрошенное разрешение, компонент *управления доступом и регистрации обращений к предоставляемым данным* регистрирует обращение к предоставляемым данным и передает *потребителю данных* токен доступа, запрошенное разрешение, информацию о ключе (например, идентификатор и адрес хранения), информацию о пакете обмена данными (например, идентификатор и адрес хранения) и другую информацию (например, цифровые сертификаты *сервера хранения ключей* и *сервера хранения данных*).

12) Получив от компонента *управления доступом и регистрации обращений к предоставляемым данным* токен доступа, запрошенное разрешение, информацию о ключе и информацию о пакете обмена данными, *потребитель данных* выполняет следующие операции:

12.1) *потребитель данных* и компонент *аутентификации и авторизации соединений сервера хранения ключей* проводят взаимную аутентификацию и получают сеансовый ключ, который будет использоваться для защиты последующих сеансов связи между ними;

12.2) *потребитель данных* передает токен доступа в компонент *проверки токенов сервера хранения ключей* в соответствии с адресом хранения ключа для получения ключа шифрования.

13) Компонент *проверки токенов сервера хранения ключей* проверяет, действителен ли токен доступа.

13.1) Компонент *проверки токенов сервера хранения ключей* получает от *потребителя данных* токен доступа и проверяет его.

13.2) В процессе проверки токена компонент *проверки токенов* факультативно может установить связь с компонентом *управления токенами* системы *управления обменом данными на основе DLT*.

14) Компонент *проверки токенов* передает результат проверки в компонент *управления хранением ключей сервера хранения ключей*. Получив результат проверки токена от компонента *проверки токенов*, компонент *управления хранением ключей сервера хранения ключей* передает ключ *потребителю данных*.

15) Получив ключ от компонента *управления хранением ключей сервера хранения ключей, потребитель данных* выполняет следующие операции:

15.1) *потребитель данных* и компонент *аутентификации и авторизации соединений сервера хранения данных* проводят взаимную аутентификацию и получают сеансовый ключ, который будет использоваться для защиты последующих сеансов связи между ними;

15.2) *потребитель данных* подает в *сервер хранения данных* запрос на получение пакета обмена данными.

16) Получив запрос от *потребителя данных,* компонент *распространения данных сервера хранения данных* аутентифицирует *потребителя данных*.

17) Компонент *распространения данных сервера хранения данных* передает пакет обмена данными *потребителю данных*.

18) *Потребитель данных* обращается к предоставляемым данным в соответствии с запрошенным разрешением. Закончив работу с данными, *потребитель данных* зашифровывает полученные данные тем же способом, что и *поставщик данных*.

Приложение A

Процедуры управления обменом данными на основе DLT

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

В этом Приложении описаны две основные процедуры: 1) процедура публикации данных поставщиком данных в процессе обмена данными на основе DLT и 2) процедура обращения потребителя данных к данным, предоставляемым в процессе обмена данными на основе DLT.

При описании процедур управления обменом данными на основе DLT предполагается, что соблюдены следующие предварительные условия:

– каждый пользователь (например, *поставщик данных, потребитель данных*) получил цифровой сертификат и соответствующий секретный ключ, сгенерированный им самостоятельно или полученный из CA;

– каждый пользователь выполнил надлежащие настройки конфигурации (такие, как цифровой сертификат узла DLT, параметры сетевого соединения DLT, подготовка сети);

– пользователи (например, поставщик данных, потребитель данных) могут использовать симметричные системы шифрования. Эти системы обеспечивают криптографическую стойкость, достаточную для обеспечения конфиденциальности данных;

– *инфраструктура DLT* и компонент *управления смарт-контрактами на основе DLT* функционируют надлежащим образом;

– сеть DLT функционирует надлежащим образом;

– *сервер хранения ключей* и *сервер хранения данных* функционируют надлежащим образом.

A.1 Процедура публикации данных поставщиком данных в процессе обмена данными на основе DLT

Процедура публикации данных поставщиком данных в процессе обмена данными на основе DLT иллюстрируется на рисунке A.1.

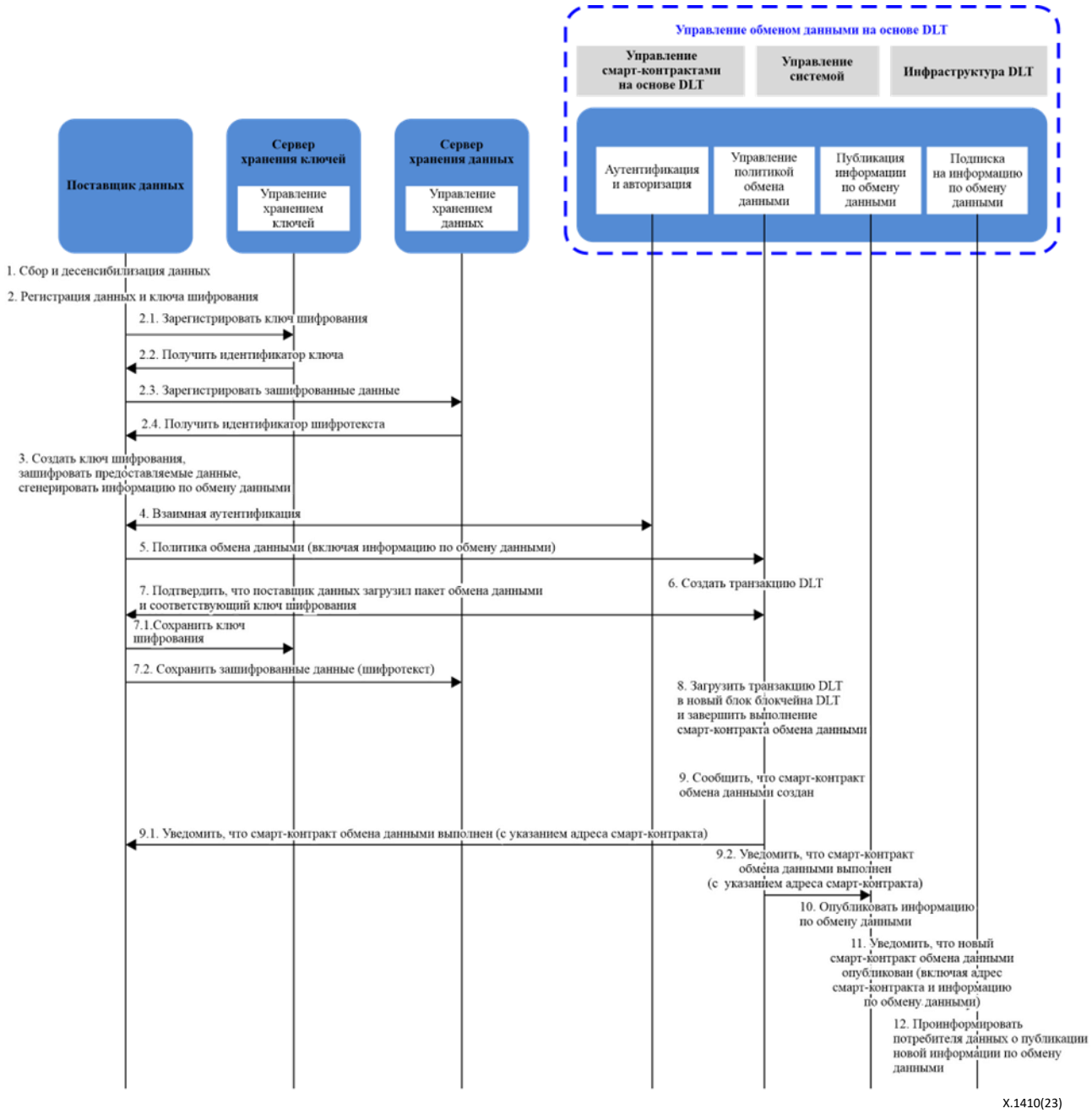

Рисунок A.1 – Процедура публикации данных поставщиком данных в процессе обмена данными на основе DLT

Как показано на рисунке A.1, процедура производится следующим образом.

1) *Поставщик данных* собирает исходные данные и десенсибилизирует их, не оказывая при этом негативного влияния на качество предоставляемых данных.

2) *Поставщик данных* регистрирует предоставляемые данные и ключ системы симметричного шифрования на локальном или удаленном сервере хранения ключей и сервере хранения данных следующим образом:

   2.1) генерирует ключ шифрования данных, используемый для системы симметричного шифрования;

   2.2) получает идентификатор ключа и адрес его хранения от *сервера хранения ключей*;

   2.3) шифрует данные с помощью ключа, используя систему симметричного шифрования, и регистрирует зашифрованные данные, т. е. шифротекст;

2.4) получает от *сервера хранения данных* идентификатор шифротекста и адрес его хранения.

3) *Поставщик данных* генерирует ключ шифрования данных и с его помощью шифрует данные, подлежащие публикации. Зашифрованные данные представляют собой шифротекст. *Поставщик данных* создает информацию по обмену данными, в том числе идентификатор поставщика данных, открытый ключ поставщика данных, идентификатор шифротекста и адрес его хранения, идентификатор ключа шифрования данных и адрес его хранения, перечень отраслей, организациям которых разрешен доступ, перечень пользователей, которым разрешен доступ, и другие атрибуты данных (такие, как категория, характеристика, условия использования и цена данных).

4) Перед публикацией предоставляемых данных *поставщик данных* обеспечивает взаимную аутентификацию с компонентом *аутентификации и авторизации пользователей* системы *управления обменом данными на основе DLT*. Для взаимной аутентификации может использоваться цифровой сертификат учетных данных. После успешной взаимной аутентификации компонент *аутентификации и авторизации пользователей* проверяет, имеет ли поставщик данных право публиковать предоставляемые данные.

5) После успешной аутентификации и авторизации *поставщик данных* предоставляет информацию по обмену данными в соответствии с требованиями компонента *управления политикой обмена данными* системы *управления обменом данными на основе DLT*. *Поставщик данных* создает политику обмена данными с помощью информации по обмену данными и другой информации. *Поставщик данных* передает политику обмена данными и свою цифровую подпись в компонент *управления политикой обмена данными*.

6) Получив от *поставщика данных* политику обмена данными и соответствующую цифровую подпись, компонент *управления политикой обмена данными* проверяет цифровую подпись и создает транзакцию DLT.

7) Компонент *управления политикой обмена данными* подтверждает *поставщику данных*, что ключ и шифротекст сохранены соответственно на *сервере хранения ключей* и *сервере хранения данных*. В противном случае необходимо предпринять следующие шаги:

7.1) *поставщик данных* сохраняет ключ на *сервере хранения ключей*;

7.2) *поставщик данных* сохраняет шифротекст на *сервере хранения данных*.

8) Компонент *управления политикой обмена данными* передает одну или несколько транзакций DLT вместе с их цифровыми подписями в нижележащие компоненты *инфраструктуры DLT* и компонент *управления смарт-контрактами на основе DLT* для формирования нового блока, содержащего один или несколько смарт-контрактов обмена данными. Вновь сгенерированный блок распространяется среди соответствующих узлов DLT. Загрузка транзакций DLT в блокчейн DLT зависит от конкретной технологии реализации (например, Hyperledger Fabric, Ethereum Quorum), рассмотрение которой выходит за рамки данной Рекомендации.

9) Компонент *управления политикой обмена данными* информирует соответствующие компоненты о создании смарт-контракта обмена данными.

9.1) Компонент *управления политикой обмена данными* уведомляет *поставщика данных* о том, что смарт-контракт обмена данными выполнен. Уведомление включает адрес исполнения смарт-контракта.

9.2) Компонент *управления политикой обмена данными* уведомляет компонент *публикации информации по обмену данными* о том, что смарт-контракт обмена данными выполнен. Уведомление включает адрес для исполнения смарт-контракта и информацию по обмену данными.

10) Получив уведомление от компонента *управления политикой обмена данными*, компонент *публикации информации по обмену данными* публикует вновь полученную информацию по обмену данными.

11) Компонент *публикации информации по обмену данными* информирует компонент *подписки на информацию по обмену данными* о том, что смарт-контракт обмена данными выполнен. Уведомление включает адрес для исполнения смарт-контракта и новую информацию по обмену данными.

12) Получив уведомление от компонента *публикации информации по обмену данными,* компонент *подписки на информацию по обмену данными* рассылает подписчикам адрес для исполнения смарт-контракта и новую информацию по обмену данными.

A.2 Процедура обращения потребителей данных к данным, предоставляемым на основе DLT

Процедура обращения потребителей данных к данным, предоставляемым на основе DLT, иллюстрируется на рисунке A.2.

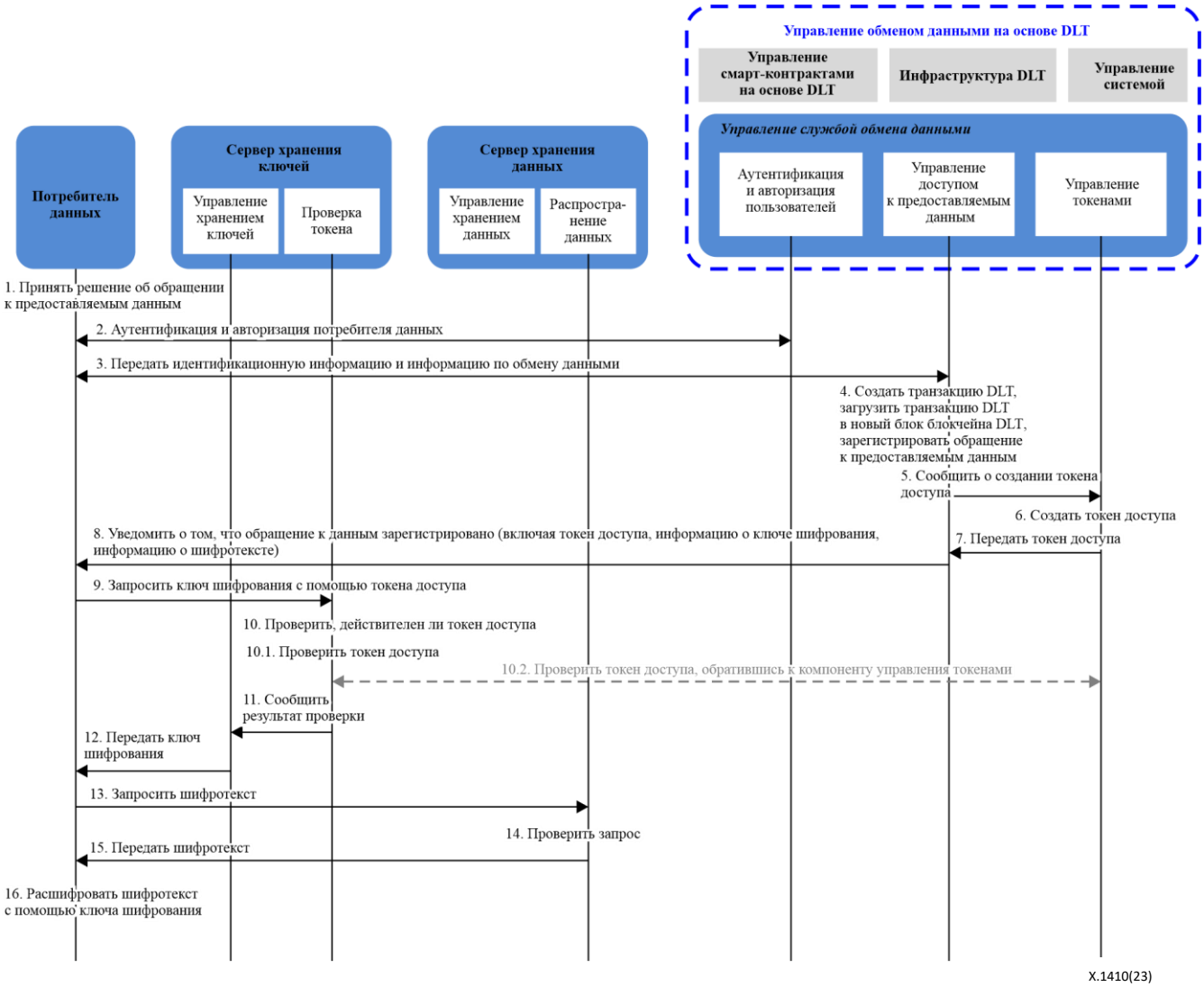

Рисунок A.2 – Процедура обращения потребителей данных к данным, предоставляемым на основе DLT

Как показано на рисунке A.2, процедура производится следующим образом.

1) *Потребитель данных* получает информацию по обмену данными, выполняя поиск в компоненте *публикации информации по обмену данными*, подписавшись на публикуемую информацию либо получая ее от других. *Потребитель данных* решает обратиться к предоставляемым данным и исполняет смарт-контракт обмена данными.

2) Перед исполнением смарт-контракта обмена данными для получения доступа к предоставляемым данным *потребитель данных* производит взаимную аутентификацию с компонентом *аутентификации и авторизации пользователей* системы *управления обменом данными на основе DLT*. Для взаимной аутентификации рекомендуется использовать цифровой сертификат учетных данных. После успешной взаимной аутентификации компонент *аутентификации и авторизации пользователей* проверяет, имеет ли потребитель данных право обращаться к предоставляемым данным.

3) После успешной взаимной аутентификации и авторизации *потребитель данных* передает в компонент *управления доступом к предоставляемым данным* свою идентификационную информацию (например, идентификатор, открытый ключ) и информацию по обмену данными вместе со своей цифровой подписью.

4) Получив идентификационную информацию потребителя данных, информацию по обмену данными и цифровую подпись, компонент *управления доступом к предоставляемым данным* проверяет цифровую подпись и разрешение потребителя данных на доступ к данным в соответствии с политикой обмена данными (например, доступ к предоставляемым данным может получить только потребитель данных из определенной отрасли или страны). Если все требования для получения доступа к предоставляемым данным выполнены, компонент *управления доступом к предоставляемым данным* создает транзакцию DLT в соответствии с информацией, полученной от потребителя данных. *Компонент управления доступом к предоставляемым данным* передает одну или несколько транзакций DLT вместе со своей цифровой подписью в нижележащие компоненты *инфраструктуры DLT* и компонент *управления смарт-контрактами на основе DLT* для формирования нового блока, содержащего одну или несколько записей об обращении к данным. Вновь сгенерированный блок распространяется среди соответствующих узлов DLT. Загрузка транзакций DLT в блокчейн DLT зависит от конкретной технологии реализации (например, Hyperledger Fabric, Ethereum Quorum), рассмотрение которой выходит за рамки данной Рекомендации.

5) Компонент *управления доступом к предоставляемым данным* информирует компонент *управления токенами* о необходимости создания токена доступа.

6) Получив уведомление от компонента *управления доступом к предоставляемым данным*, компонент *управления токенами* создает токен доступа.

7) Компонент *управления токенами* передает созданный токен доступа в компонент *управления доступом к предоставляемым данным*.

8) Получив токен доступа, компонент *управления доступом к предоставляемым данным* передает *потребителю данных* токен доступа, информацию о ключе (например, идентификатор и адрес его хранения), информацию о шифротексте (например, идентификатор и адрес его хранения), другую информацию (например, цифровые сертификаты *сервера хранения ключей* и *сервера хранения данных*).

9) Получив от компонента *управления доступом к предоставляемым данным* токен доступа, информацию о ключе и информацию о шифротексте, *потребитель данных* передает токен доступа в компонент *проверки токенов сервера хранения ключей* в соответствии с адресом хранения ключа для получения ключа шифрования, который используется для расшифровки шифротекста.

10) Компонент *проверки токенов* проверяет, действителен ли токен доступа.

    10.1) Компонент *проверки токенов сервера хранения ключей* получает от *потребителя данных* токен доступа и проверяет его.

    10.2) В процессе проверки токена компонент *проверки токенов* факультативно может установить связь с компонентом *управления токенами* системы *управления обменом данными на основе DLT*.

11) Компонент *проверки токенов* передает результат проверки в компонент *управления хранением ключей*.

12) Получив результат проверки токена от компонента *проверки токенов*, компонент *управления хранением ключей* передает *потребителю данных* ключ шифрования.

13) Получив ключ шифрования от компонента *управления хранением ключей, потребитель данных* подает запрос на *сервер хранения данных*, чтобы получить шифротекст.

14) Получив запрос от *потребителя данных,* компонент *распространения данных сервера хранения данных* аутентифицирует *потребителя данных*.

15) Компонент *распространения данных сервера хранения данных* передает *потребителю данных* шифротекст.

16) *Потребитель данных* расшифровывает шифротекст с помощью ключа шифрования и получает доступ к предоставляемым данным в виде открытого текста.

Библиография

[b-ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection − The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1400] Recommendation ITU-T X.1400 (2020), *Terms and definitions for distributed ledger technology*.

[b-ITU-T X.1402] Recommendation ITU-T X.1402 (2020), *Security framework for distributed ledger technology*.

[b-ITU-T FG DLT D1.1] Technical Specification ITU-T FG DLT D1.1 (2019), *Distributed ledger technology terms and definitions*.

[b-ISO/IEC 18033-1] ISO/IEC 18033-1:2021, *Information security − Encryption algorithms − Part 1: General*.

[b-ISO/IEC 20944-1] ISO/IEC 20944-1:2013, *Information technology – Metadata registries interoperability and bindings (MDR-IB) – Part 1: Framework, common vocabulary, and common provisions for conformance*.

[b-ISO/IEC 29100] ISO/IEC 29100:2011, *Information technology − Security techniques − Privacy framework*.

[b-ISO/IEC/IEEE 15939] ISO/IEC/IEEE 15939:2017, Syst*ems and software engineering − Measurement process.*

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-shared key ciphersuites for transport layer security (TLS)*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet key exchange (IKEv2) protocol*.

[b-IETF RFC 4314] IETF RFC 4314 (2005), *IMAP4 access control list (ACL) extension*.

[b-IETF RFC 4949] IETF RFC 4949 (2007), *Internet security glossary, version 2*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The transport layer security (TLS) protocol: Version 1.2.*

[b-IETF RFC 5782] IETF RFC 5782 (2010), *DNS blacklists and whitelists*.

[b-IETF RFC 5851] IETF RFC 5851 (2010), *Framework and requirements for an access node control mechanism in broadband multi-service networks*.

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, 2023 г.