**Оглавление**

[Введение 4](#_Toc9256503)

[1 Анализ предметной области 5](#_Toc9256504)

[1.1 Описание предметной области 5](#_Toc9256505)

[1.2 Формулировка проблемы и актуальность 11](#_Toc9256506)

[1.3 Обзор аналогов 12](#_Toc9256507)

[2 Программная документация 13](#_Toc9256508)

[2.1 Техническое задание на программное обеспечение 13](#_Toc9256509)

[2.1.1 Общие сведения 13](#_Toc9256510)

[2.1.1.1 Наименование программы 13](#_Toc9256511)

[2.1.1.2 Плановые сроки начала и окончания работ 13](#_Toc9256512)

[2.1.1.3 Порядок оформления и предъявления заказчику результатов работ 13](#_Toc9256513)

[2.1.1.4 Перечень нормативно-технических документов, методических материалов, использованных при разработке ТЗ 14](#_Toc9256514)

[2.1.1.5 Определения, обозначения, сокращения 14](#_Toc9256515)

[2.1.2 Назначение и цели создания системы 14](#_Toc9256516)

[2.1.2.1 Назначение системы 14](#_Toc9256517)

[2.1.2.2 Цели создания системы 15](#_Toc9256518)

[2.1.3 Характеристика объектов автоматизации 15](#_Toc9256519)

[2.1.3.1 Краткие сведения об объекте автоматизации 15](#_Toc9256520)

[2.1.3.2 Существующие программное обеспечение 15](#_Toc9256521)

[2.1.4 Требования к системе 15](#_Toc9256522)

[2.1.4.1 Требование к структуре и функционированию системы 15](#_Toc9256523)

[2.1.4.1.1 Перечень подсистем, их назначение и основные характеристики 15](#_Toc9256524)

[2.1.4.1.2 Требования к способам и средствам связи для информационного обмена между компонентами системы 16](#_Toc9256525)

[2.1.4.1.3 Требования к режимам функционирования системы 16](#_Toc9256526)

[2.1.4.1.4 Перспективы развития, модернизации системы 16](#_Toc9256527)

[2.1.4.2 Требования к надежности 16](#_Toc9256528)

[2.1.4.3 Требования к безопасности 16](#_Toc9256529)

[2.1.4.4 Требования к эргономике и технической эстетике 17](#_Toc9256530)

[2.1.4.5 Требования к интерфейсу 17](#_Toc9256531)

[2.1.4.6 Требования к защите информации от несанкционированного доступа 17](#_Toc9256532)

[2.1.4.7 Требования по сохранности информации при авариях 17](#_Toc9256533)

[2.1.4.8 Требования по стандартизации и унификации 17](#_Toc9256534)

[2.1.4.9 Дополнительные требования 17](#_Toc9256535)

[2.1.5 Требования к функциям (задачам), выполняемым системой 17](#_Toc9256536)

[2.1.6 Требования к видам обеспечения 18](#_Toc9256537)

[2.1.6.1 Требования к лингвистическому обеспечению системы 18](#_Toc9256538)

[2.1.6.2 Требования к программному обеспечению системы 18](#_Toc9256539)

[2.1.6.3 Требования к техническому обеспечению 18](#_Toc9256540)

[2.2 Пояснительная записка к программному обеспечению 18](#_Toc9256541)

[2.2.1 Назначение и область применения 18](#_Toc9256542)

[2.2.2 Технические решения 18](#_Toc9256543)

[2.2.2.1 Постановка задачи на разработку программы 18](#_Toc9256544)

[2.2.2.2 Описание структуры программной системы 18](#_Toc9256545)

[2.2.2.3 Описание технологии программирования 18](#_Toc9256546)

[2.2.2.4 Описание взаимодействия с другими программами 18](#_Toc9256547)

[2.2.2.5 Описание и обоснование выбора метода организации входных и выходных данных 18](#_Toc9256548)

[2.2.2.6 Описание алгоритмов и функционирования программы 18](#_Toc9256549)

[2.2.3 Ожидаемые технико-экономические показатели 18](#_Toc9256550)

[2.3 Описание программы 19](#_Toc9256551)

Введение

В современном мире, с его бурным развитием информационных технологий, с каждым днём становится всё больше и больше сфер подверженных автоматизации с помощью программных продуктов.

Количество информации растёт, её ценность повышается. Вопрос защиты информации от несанкционированного доступа важен как никогда. Кроме того, увеличение количества инструментов на основе программных продуктов требует усовершенствования механизмов доступа к ним пользователей с целью повышения удобства и безопасности.

Особенно это актуально в сфере коммерческого программного обеспечения, в которой необходимо обеспечение защищённости информации как от внешних угроз, так и поддержание ограничений на доступ к данным по причине разделения полномочий внутри круга доверенных лиц.

Для решения этих проблем существуют различные протоколы аутентификации и авторизации. Каждый из них имеет свои преимущества и недостатки, а подходы к реализации могут кардинально отличатся. Поэтому в условиях сложной инфраструктуры, большого количества пользователей и разнообразных ресурсов, а также наличия устаревших решений, несколько протоколов могут существовать одновременно. А это, в свою очередь усложняет работу пользователей из-за необходимости иметь несколько учётных записей.

1 Анализ предметной области

1.1 Описание предметной области

Процессы аутентификации и авторизации позволяют реализовать разделения прав доступа и защиту конфиденциальной информации от внешних угроз. Это необходимо в большинстве программных продуктов, особенно коммерческих. Также реализация конкретной системы может значительно повысит удобство работы пользователей, что зачастую ведёт ещё большему увеличению безопасности.

Для успешного прохождения авторизации необходимо пройти несколько этапов:

1) Идентификация – заявление о том, кем является пользователь, обычно выражается в предоставлении своего уникального идентификатора-имени.

2) Аутентификация – проверка подлинности пользователя. То есть действительно ли пользователь тот, за кого себя выдаёт. Самый распространённый способ — это подтверждение с помощью секретного пароля. Кроме того, аутентификация может быть односторонней и двусторонней (взаимной). При односторонней, проверки требует только тот, кто запрашивает доступ. При двусторонней запрашиваемый ресурс тоже должен подтвердить себя.

3) Авторизация – выдача соответствующих прав доступа к запрашиваемому ресурсу. Этот процесс позволяет использовать результаты работы аутентификации и выдать пользователю только то, что ему разрешается согласно его статусу.

Успешное последовательное прохождение этих этапов позволяет гарантировать защищённость информации, к которой осуществляется доступ.

Но, так как информация имеет ценность, то найдутся люди, желающие ей завладеть. При этом они могут использовать различные методы чтобы нарушить нормальное функционирование этапов авторизации или получить доступ к конфиденциальной информации напрямую. Поэтому появляется необходимость в полной защите данных: как при хранении, так и при передаче.

На практике процессы авторизации обычно происходят с использованием компьютерной сети, которая не может быть полностью ограждена от физического доступа злоумышленника. В таком случае приходится учитывать, что любая информация, передаваемая по сети может быть известна кому угодно. Следовательно, необходимо использовать методы, позволяющие преобразить данные так, что даже при их перехвате неавторизированным пользователем конфиденциальность не будет нарушена.

Такие методы предоставляет криптография. Криптография - это наука об обеспечении безопасности данных. Она занимается поисками решений четырех важных проблем безопасности - конфиденциальности, аутентификации, целостности и контроля участников взаимодействия. Основным способом решения этих проблем является шифрование. Шифрование. Шифрование - это преобразование данных определённым способом-алгоритмом в нечитабельную форму, с возможностью возвращения исходного состояния, используя специальные ключи шифрования.

На практике приходится считаться со сложными структурами данных и с аппаратные ограничениями, поэтому отдельных алгоритмов шифрования недостаточно. Нужны комплексные решения описывающие все этапы передачи данных, способные надёжно и эффективно решать проблему защиты информации. Такими решениями являются криптосистемы.

Они включают в себя набор правил и алгоритмов, регламентирующих манипуляции с данными, а также способы создания и распространения ключей. Криптографические системы можно классифицировать по типу используемых алгоритмов шифрования:

1. На основе симметричных алгоритмов.
2. На основе асимметричных алгоритмов.

Симметричные криптосистемы, также называемые системами с секретным ключом – способ шифрования, в котором один ключ используется как для шифрования, так и для расшифровывания. Является первым подходом к сокрытию информации изобретённым человеком.

Главной особенностью симметричной криптосистемы является то, что что ключ алгоритма шифрования должен оставаться в секрете от посторонних. Поэтому должна обеспечиваться защита ключа на протяжении всего его существования.

Кроме возможности потери конфиденциальности ключа, также существует опасность применения криптоанализа к зашифрованным данным. Поэтому выбранный алгоритм шифрования должен быть достаточно стойким, для недопущения расшифровки информации за приемлемое время.

Для симметричных алгоритмов уровень криптостойкости, обычно, определяется размером ключа шифрования, что эквивалентно полному перебору его значений.

Для современных систем желателен ключ длинной не менее 128 двоичных разрядов (128 бит).

Асимметричные криптосистемы в своей работе используют пару ключей: закрытый и открытый. Открытый ключ применяется для шифрования и может передаваться по незащищённому каналу связи. Расшифровка производится с помощью закрытого ключа, который должен оставаться в секрете.

Реализация асимметричных алгоритмов шифрования основана на применении односторонних функций, то есть таких функций, что, зная несложно найти значение F(x), но вычисление x по F(x) невозможно за приемлемое время. Теоретически, зная F(x), x можно подобрать, перебирая все возможные значения x и применять к ним функцию, до тех пор, пока результат не совпадёт с F(x). Однако практически, при достаточной размерности множества X, выполнить такой перебор, за приемлемое время, невозможно.

Классический пример такой функции – это функция основанные на принципе обратного модульного возведения в степень, также называемые задаче дискретного логарифмирования.

Но получается, что односторонняя функция не может использоваться в качестве функции шифрования. Так как хоть она и позволяет надёжно зашифровать данные, но расшифровать их некто не сможет. Для решения этой проблемы используются односторонние функции с секретом. Это особый вид функций, которые имеют некоторый секрет, позволяющий быстро вычислить обратное значение функции. Именно на этом принципе основаны большинство асимметричных криптографических систем.

(Вывод о необходимости подтверждения источников и шифровании ключей) В итоге оба подхода имеют свои преимущества и недостатки. Симметричные системы проще в реализации, за счёт более простых операций, а скорость шифрования в среднем на несколько порядков выше, чем у аналогичных по защищённости систем с открытым ключом. Единственным серьёзным недостатком является сложность обмена секретного ключа. Поэтому для применения симметричных систем на практике необходимо решить проблему надёжного распределения ключей между участниками процесса передачи данных.

При работе в публичных сетях, требуется быть уверенным в подлинности ключа. А именно в том, что полученный от пользователя ключ действительно сгенерирован им. Такой функционал может предоставить механизм Электронной подписи.

Обычно, в большинстве реальных систем, электронная подпись основана на принципах асимметричного шифрования, только применяет их иначе. Так же генерируется пара ключей: открытый, закрытый. Но для шифрования (подписи) данных применяется закрытый, соответственно для расшифровки (проверки подписи) открытый. Такой подход позволяет любому владельцу открытого ключа проверять подпись, а возможность подписать остаётся только за хранителем закрытого ключа. Таким образом проведя подписание каких-либо информации, мы генерируем электронную подпись и можем отправлять её вместе с исходными данными. Далее, зная отправителя и его открытый ключ, можно применить его к подписи и получить исходный файл.

Но получается, что каждый обладатель открытого ключа может получить из подписи оригинальные данные, а они должны быть секретны. Кроме того, подписанный файл по размеру будет сопоставим с оригинальным, что удвоит нагрузку на передающую среду. Поэтому в электронная подпись невозможна без хеш-функций.

Хеш-функция – осуществляет преобразование (хеширование) набора входных данных произвольной длинны, в выходную последовательность определённой длинны. При этом для каждого набора результат хеширования будет уникальным, а провести обратное преобразование невозможно.

Таким образом подписывая не сами данные, а их хеш, общедоступным окажется именно хеш, что безопасно. И размер подписи теперь возможно уменьшить, выбрав подходящую хещ-функцию.

Одной только проверки подлинности ключей недостаточно для сохранения конфиденциальности информации. Кроме этого, очевидно, необходимо скрывать сами значения ключей. Это можно сделать если использовать асимметричное шифрование на ключи. Так как размеры ключей небольшие, то потеря ресурсов на зашифровку-расшифровку будет незначительной.

Используя цифровую подпись и асимметричное шифрование можно реализовать безопасное распределение ключей для симметричных криптосистем.

Но такая система связи остаётся уязвимой для злоумышленника, который представляется доверенным пользователем, но отдаёт свой открытый ключ асимметричного шифрования, таким образом подменяя его.

Для решения этой проблемы открытый ключ доверенного пользователя вместе с сопроводительной информацией: именем, сроком действия и прочим подписывается центром сертификации. Предполагается, что центр сертификации честный и не подпишет ключ злоумышленника. А также то, что центр сертификации распространяет свой открытый ключ максимально широко, и желающие пройти аутентификацию, ещё до инициализации процесса обмена ключами, будут иметь открытый ключ такого центра, и злоумышленник ничего не сможет с этим поделать.

Этот процесс называется сертификацией. А подписанные центром сертификации открытые ключи, включающие в себя также прочие данные о владельце, называются цифровыми сертификатами. (добавить про центры сертификации)

(В итоге про Kerberos (OpenID connect?

), как про всё вместе)

OpenId Connect – это надстройка над протоколом авторизации OAuth 2.0, предоставляющая функции аутентификации. OIDC предполагает наличие отдельного доверенного сервера аутентификации, благодаря чему поддерживает технологию SSO, позволяет отделить функционал по аутентификации от конкретных приложений и гарантирует безопасность. Очень популярный протокол, поддерживается практически всеми крупными компаниями, например: Google, Facebook.

Для передач данных в процессе аутентификации используется стандарт JSON Web Token (JWT). Это открытии стандарт, описывает формат сообщений в виде JSON файлов, называемых токенами. Согласно нему токен состоит из заголовка, хранящего собственное описание, основной части, в которой хранится пользовательская информация, а также электронной подписи, удостоверяющей весь файл.

Процесс авторизации, в общем случае, выглядит следующим образом:

1. Пользователь запрашивает ресурс.
2. Ресурс перенаправляет пользователя на сервер аутентификации.
3. Пользователь вводит свои учётные данные на форме сервера аутентификации.
4. Сервер аутентификации проверяет данные пользователя по своей базе, и вы даёт токен доступа (access token).
5. Имея access token пользователь может получить доступ к ресурсу.

(дописать)

1.2 Формулировка проблемы и актуальность

Проблематика заключается в необходимость ООО «БиАйВи» в агрегации различных протоколов аутентификации в одну систему. С предоставлением пользователям этих протоколов единого интерфейса аутентификации.

Актуальность состоит в потребности ООО «БиАйВи» в повышении гибкости системы аутентификации. А также повышенные безопасности путём внедрения современных протоколов аутентификации.

1.3 Обзор аналогов

Для того, чтобы провести сравнение аналогов необходимо выделить объективные критерии:

1. Поддерживаемые протоколы.

KeyCloak - это open-source сервер аутентификации и управления учетными записями, построенный на базе спецификаций OAuth 2.0, Open ID Connect, JSON Web Token и SAML 2.0. Разрабатывается JBoss.

Преимущества:

* Встроенный механизм управления учетными записями
* Поддержка большого количества платформ
* Поддержка каталогов LDAP
* Поддержка протоколов SAML 2 и OpenID Connect

Недостатки:

* Не поддерживает Kerberos
* Ограниченные возможности по расширению функционала

OpenidDict – это open-sour библиотека, позволяющая разворачивать сервер аутентификации. Поддерживает OAuth 2.0, Open ID Connect.

Преимущества:

* Легко расширяется и дополняется
* Поддержка механизма управления учётными записями

Недостатки:

* Поддерживает только OpenID Connect
* Поддерживает только платформу ASP.NET

2 Программная документация

2.1 Техническое задание на программное обеспечение

2.1.1 Общие сведения

2.1.1.1 Наименование программы

Полное наименование программы: Система централизованной авторизации на основе LDAP, с использованием протоколов аутентификации Kerberos и OpenID connect.

Краткое наименование: Системы централизованной авторизации.

2.1.1.2 Плановые сроки начала и окончания работ

Плановый срок начала работ по созданию системы централизованной авторизации – 01 ноября 2018 года. Плановый срок окончания работ по разработке системы централизованной авторизации – 15 июня 2019 года.

2.1.1.3 Порядок оформления и предъявления заказчику результатов работ

Система передается в виде функционирующего приложения-клиента и серверной части, установленного на оборудование Заказчика в сроки, установленные договором. Совместно с системой производится сдача разработанного комплекта документации с руководством пользователя.

2.1.1.4 Перечень нормативно-технических документов, методических материалов, использованных при разработке ТЗ

При разработке автоматизированной системы и создании проектно-эксплуатационной документации Исполнитель должен руководствоваться требованиями следующих нормативных документов:

* ГОСТ 19.201-78. ТЕХНИЧЕСКОЕ ЗАДАНИЕ. ТРЕБОВАНИЯ К СОДЕРЖАНИЮ И ОФОРМЛЕНИЮ.
* ГОСТ 34.601-90. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания.
* ГОСТ 34.201-89. Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплексность и обозначение документов при создании автоматизированных систем.

2.1.1.5 Определения, обозначения, сокращения

Таблица 1 - Расшифровка определений, обозначений, сокращений

|  |  |  |
| --- | --- | --- |
| № | Наименование | Расшифровка |
| 1 | KDC | Key Distribution Center – центр выдачи ключей |
| 2 | ТЗ | Техническое задание |
| 3 | TGT | Ticket granting ticket – Билет на получение билета |

2.1.2 Назначение и цели создания системы

2.1.2.1 Назначение системы

Система централизованной авторизации предназначена для реализации процессов аутентификации и авторизации в сервисах, через доверенный сервер.

2.1.2.2 Цели создания системы

Основной целью создания системы централизованной авторизации является оптимизация процессов авторизации и аутентификации в инфраструктуре сервисов компании ООО «БиАйВи».

Для реализации поставленных целей система должна решать следующие задачи:

* Хранение учётных данных в каталоге LDAP
* Поддержка протокола Kerberos
* Поддержка протокола OpenId Connect

2.1.3 Характеристика объектов автоматизации

2.1.3.1 Краткие сведения об объекте автоматизации

* Система реализует технологию Single Sign-On.
* Используемые протоколы аутентификации реализуют концепцию доверенной третьей стороны.
* Данные о пользователях разных сервисов хранятся в одной базе данных на KDC.

2.1.3.2 Существующие программное обеспечение

На момент начала работы было…

2.1.4 Требования к системе

2.1.4.1 Требование к структуре и функционированию системы

2.1.4.1.1 Перечень подсистем, их назначение и основные характеристики

В состав системы централизованной авторизации должны входить следующие подсистемы:

* 1
* 2

2.1.4.1.2 Требования к способам и средствам связи для информационного обмена между компонентами системы

Система централизованной авторизации должна взаимодействовать со своими компонентами с использованием канала Интернет, используя протокол HTTP. Настройки приложения должны храниться в локальном хранилище каждого из компонентов.

2.1.4.1.3 Требования к режимам функционирования системы

Для системы централизованной авторизации определены следующие режимы:

* 1
* 2

2.1.4.1.4 Перспективы развития, модернизации системы

В дальнейшем планируется увеличение числа поддерживаемых протоколов.

2.1.4.2 Требования к надежности

Система должна сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

* 1
* 2

2.1.4.3 Требования к безопасности

Безопасность

2.1.4.4 Требования к эргономике и технической эстетике

Следование стандартам реализации?

2.1.4.5 Требования к интерфейсу

Требования?

2.1.4.6 Требования к защите информации от несанкционированного доступа

Описание надёжности протоколов?

2.1.4.7 Требования по сохранности информации при авариях

Данные на сервере должны иметь резервные копии?

2.1.4.8 Требования по стандартизации и унификации

Требования?

2.1.4.9 Дополнительные требования

Пока нет?

2.1.5 Требования к функциям (задачам), выполняемым системой

Система централизованной авторизации должна обеспечивать:

1. Регистрацию нового пользователя на KDC.
2. Регистрацию нового сервиса на KDC.
3. Проведение аутентификации зарегистрированных пользователей.
4. Проведение авторизации аутентифицированных пользователей на зарегистрированных сервисах.
5. Управление политикой авторизации со стороны сервисов.
6. Фоновую поддержку авторизации.
7. …

2.1.6 Требования к видам обеспечения

2.1.6.1 Требования к лингвистическому обеспечению системы

В системе должны присутствовать русский или английский языковые пакеты.

2.1.6.2 Требования к программному обеспечению системы

Для работы системы необходим сервер аутентификации с установленным Windows Server 2008 и выше.

2.1.6.3 Требования к техническому обеспечению

Требования к техническим характеристикам сервера:

* 8 Гб ОЗУ
* 2 ядерный процессор
* …

2.2 Пояснительная записка к программному обеспечению

2.2.1 Назначение и область применения

2.2.2 Технические решения

2.2.2.1 Постановка задачи на разработку программы

2.2.2.2 Описание структуры программной системы

2.2.2.3 Описание технологии программирования

2.2.2.4 Описание взаимодействия с другими программами

2.2.2.5 Описание и обоснование выбора метода организации входных и выходных данных

2.2.2.6 Описание алгоритмов и функционирования программы

2.2.3 Ожидаемые технико-экономические показатели

2.3 Описание программы

2.3.1

2.3.1.1

2.3.1.2

2.3.2

2.

LDAP – база данных для учётных данных (логины, права, и структура) (иерархическая (дерево)) + стандартные способы доступа.

Kerberos, OIDC… - протоколы (набор соглашений) по передаче данных между участниками(определёнными) сети.

НУЖНО – Сервер(KDC) реализующий(исполняющий) ПРОТОКОЛ, и хранящий данный в LDAP. (KDC выдаёт билеты и всё) (ИНФОРМАЦИЯ О РАСПОЛОЖЕНИИ KDC, алгоритмах шифрования в файле КОНФИГУРАЦИИ)

НУЖНО – Клиентская сторона способная создать нового USER’а и зарегистрироваться на KDC (ИНФОРМАЦИЯ О РАСПОЛОЖЕНИИ KDC, алгоритмах шифрования в файле КОНФИГУРАЦИИ)

НУЖНО – Пристройка(?!) к сервисам, которая может регистрироваться в KDC и принимать сформированные ПРОТОКОЛОМ билеты (ещё есть refresh ticket).

Какой сервер?? Как общаться с сервером?

(OIDC - общается json, Kerberos – не определенно (а как тогда? (GSSAPI ??)))

Критерии сравнения систем авторизации

1. Безопасность: количество участков системы, на которых возможен доступ третьих лиц, который может привести к потере безопасности (нужно описать все участки системы)
2. Удобство для пользователя (наличие SSO?) (кол-во действий для авторизации и необходимость повторной авторизации)
3. Удобство для ресурса (кол-во манипуляций, масштабируемость)
4. Стоимость?
5. Оборудование?
6. Поддержка работы? (выдача учёток)
7. Перспективность технологий (год? Популярность?)

Цель

Цель – оптимизация процессов авторизации и аутентификации в инфраструктуре сервисов компании ООО «БиАйВи»

Описание

Предметной областью является аутентификация/авторизация.

Это неотъемлемая часть всех современных программных продуктов. Необходима и для реализации конфиденциальности, и для безопасности, и для удобства пользователей.

Для успешного прохождения авторизации необходимы:

1. Идентификация – заявление о том, кем является пользователь
2. Аутентификация – проверка подлинности пользователя
3. Авторизация – выдача соответствующих прав доступа к запрашиваемому ресурсу

Одна из основных функций авторизации безопасность. Так как все процессы авторизации происходят удалённо, в рамках компьютерной сети, и защита таких сетей от несанкционированного доступа на сто процентов невозможна. Следовательно, необходимо обеспечить конфиденциальность данных с учётом этих уязвимостей. Первым этапом для решения этой задачи является выделение всех таких небезопасных участков системы.

* Программа, производящая авторизацию со стороны пользователя
* Каналы передачи данных
* Устройство (сервер) и программа производящие авторизацию
* ???

На каждом таком участке системы злоумышленник может производить:

1. Пассивное наблюдение - злоумышленник, перехватывая данные использует их для получения конфиденциальной информации.
2. Воздействие на обменную информацию - злоумышленник, перехватывая и манипулируя информацией, способен получить доступ к конфиденциальным данным/системам.
3. Пароли или иные удостоверяющие данные никогда не пересылаются по сети. Подразумевается, что сетевой трафик может быть прослушан, может произойти подмена сообщения или любая другая пакость.
4. Выдвигается обязательное требование, что информация о паролях/удостоверяющих данных хранится в единственном защищённом месте (Центре распределения ключей Kerberos). Поэтому удостоверяющие данные никогда не сохраняются на том хосте, который пользователь использует для входа/логина. После того, как произошёл первоначальный обмен в рамках аутентификации, этот хост должен забыть сведения о пароле.
5. Хосты/серверы приложений должны быть в состоянии подтвердить свою идентификационную сущность любому, кто запрашивает подобные доказательства.
6. Все коммуникации между аутентифицированными пользователями (клиентами) и сервисами приложений должны иметь возможность быть зашифрованными. С этой целью поддерживаются и могут применяться различные алгоритмы шифрования (все [симметричные](https://pro-ldap.ru/tr/zytrax/tech/encryption.html#symmetric)).

Для

Терминология Kerberos

Как и у всех серьёзных систем, у Kerberos есть своя уникальная терминология, а кое-какие общие термины в контексте Kerberos обретают новый смысл. Постараемся раскрыть их простыми словами (во возможности):

|  |  |
| --- | --- |
| Область действия (Realm) | Realm просто означает совокупность пользователей и серверов приложений, которые охватывает (или имеет о них информацию) Центр распределения ключей (KDC). Так, для того чтобы пользователь подсоединился (или вошёл) в Realm, у Сервера аутентификации (Authentication Server) этой области Realm должны быть сведения об удостоверяющих данных этого пользователя (и другая информация о нём), хранящиеся в защищённой базе данных безопасности того или иного вида (форма хранения не определяется в RFC). В терминологии Microsoft это будет называться Доменом (Domain). Области Realm могут доверять другим Realm, в этом случае доверяющие друг другу области должны быть взаимно аутентифицированными (Cross-Authenticated).  Форма имени Realm — ...@REALM (регистр символов имеет значение). Например, если Realm называется JOE, то его Realm-имя будет @JOE (что отличается от Realm-имени @joe), а если Realm называется EXAMPLE.COM, то его Realm-имя будет @EXAMPLE.COM. (Примечание: Согласно текущей рекомендации ([раздел 6.1 RFC 4120](http://tools.ietf.org/html/rfc4120#section-6.1)) в качестве имени REALM следует использовать доменное имя, которое часто преобразуется в верхний регистр.) Несмотря на то, что последняя форма может напоминать адрес электронной почты, никакого отношения к электронной почте она не имеет. Если буквы большие, это наверняка REALM, а не почта. |
| Принципал (Principal) | Принципал — это строка, полностью идентифицирующая пользователя службы Kerberos. Он имеет форму thing@REALM. Принципал может быть именем сервиса, выполняющегося на хосте (мы будем называть его принципалом сервиса (Service-Principal)), или именем пользователя (мы будем называть его принципалом пользователя (User-Principal)). Принципалы формируют индексное поле для информации об объекте, хранящейся в базе данных безопасности Kerberos (в Центре распределения ключей или KDC). Форматы принципалов для пользователей и сервисов различаются.  Имя принципала пользователя — это приблизительный эквивалент имени пользователя или имени учётной записи. Оно имеет форму principal-name[/instance-name]@REALM (где часть */instance-name* является опциональной). Например, если имя пользователя в принципале пользователя — alice, а Realm — joe, то полный принципал будет alice@joe. Расширение instance-name позволяет любому пользователю иметь более одного принципала. Так, если alice является администратором области Realm joe, имя её принципала будет alice/admin@joe, и у этого принципала будут другие права (и удостоверяющие данные).  Если речь идёт о принципале сервиса, то форма имени принципала становится service-name/QDN@REALM, где QDN — это доменное имя хоста (без точки в конце, как того требует FQDN), на котором работает сервис, а service-name — это специфичная для приложения строка, идентифицирующая сервис на этом хосте. Некоторые типы сервисов используют ключевое слово host. Так, для сервиса ftp, работающего на хосте с именем fileserver.example.com в области Realm @EXAMPLE.COM, имя принципала сервиса будет ftp/fileserver.example.com@EXAMPLE.COM. |
| Разрешение (Ticket) | Разрешение — это структура данных, содержимое которой известно только издателю этого разрешения, и какой-либо стороне или сторонам, к которым это разрешение имеет отношение. Промежуточные хосты, такие как клиентский хост, рассматривают эти разрешения как неразбираемый набор бит и просто передают их на конечный пункт назначения. В Kerberos разрешения могут быть либо Разрешениями на получение разрешения (Ticket Granting Tickets, TGT), — по сути представляют собой доказательства успешно пройденной аутентификации, — либо Сервисными разрешениями (Service Tickets, ST), — выдаются Службой выдачи разрешений (Ticket Granting Service, TGS) и позволяют пользователю получить доступ к требуемому Сервису приложений (Application Service). |

Полезные штуки

1. <https://pro-ldap.ru/tr/zytrax/tech/kerberos.html> - немного теории по Kerberos есть схема (С ссылками. Годно)
2. [http://asupro.com/gps-gsm/data-protection/classification-authentication-processes.html?utm\_source=yandex.ru#](http://asupro.com/gps-gsm/data-protection/classification-authentication-processes.html?utm_source=yandex.ru) - теория по аутентификации.
3. <https://www.intuit.ru/studies/courses/3580/822/lecture/30592?page=2> – Теория по криптографическим системам.
4. <https://it.wikireading.ru/59914> - про распределение ключей в Kerberos (+ там много всего)
5. <https://web.mit.edu/Kerberos/krb5-1.13/doc/admin/pkinit.html> - PKINIT (англ.)
6. <https://pro-ldap.ru/tr/zytrax/tech/ssl.html> - о x.509 и сертификатах.