Федеральное агентство связи

Ордена Трудового Красного Знамени федеральное государственное

бюджетное образовательное учреждение высшего образования

«Московский Технический Университет Связи и Информатики»

Кафедра «Информатика»

Курсовая работа по дисциплине «Основы программирования»

На тему: «Инфраструктуры открытых ключей»

Выполнил:

студент 1 курса

Максимов И. А

Научный руководитель:

Доцент,

Кандидат педагогических наук,

Заместитель заведующего кафедрой,

Писать надо то, что говорили Гуриков С. Р

Москва-2020

**Оглавление**

Введение…………………………………………………………………………………3

Техническое задание……………………………………………………………………5

Глава 1. Изучение темы «Инфраструктуры открытых ключей» ……………………8

* 1. Структура PKI………………………………………………………………...8
  2. Сервисы безопасности PKI…………………………………………………16

Глава 2.???..........................................................................................................................?

Заключение………………………………………………………………………………?

Библиография……………………………………………………………………………?

Приложения………………………………………………………………………………?

Приложение 1……………………………………………………………………...?

Приложение 2……………………………………………………………………...?

**~~Общая характеристика работы~~ НАЗВАНИЕ??**

**Актуальность темы.** Бурное развитие компьютерных технологий вызвало быстрый рост аудитории. С ростом числа пользователей также увеличился рост программ для взлома паролей и приложений, что приводит к риску потери информации. Обеспечение безопасной аутентификации и конфиденциальности информации стало актуальной проблемой в наше время.

Почти каждая компьютерная система требует, чтобы в начале сеанса работы пользователь идентифицировал себя. Обычно пользователю предлагается ввести имя и пароль. Аутентификация при помощи паролей - наиболее распространенный вид аутентификации. Но злоумышленник с помощью программы-анализатора, или сниффера, может перехватить пароль пользователя и тем самым получить доступ к его приватной информации. Это как раз-таки и сподвигло к эволюции механизмов аутентификации. **Очевидно**, что должна была появиться защита от этих атак в виде шифрования. Шифрование предотвращает раскрытие пароля при передаче. Но если все пользователи используют один и тот же ключ шифрования, то любой из них может использовать анализатор, получить чужой пароль и расшифровать его тем же способом, что и сервер. **В связи с этим** разработка новых способов шифрования и реализация их на практике стала одной из главной задачей современности. ТЕБЕ НЕ ПРО СОВРЕМЕННОСТЬ НАДО

Я НЕ ВИЖУ, ЧТО ИСПОЛЬЗОВАЛСЯ ОБРАЗЕЦ ВВЕДЕНИЯ ГОВОРИЛИ НА ЧТО ОБРАЩАТЬ ВНИМАНИЕ

**Объектом исследования** являются механизмы аутентификации.

**Предметом исследования** является инфраструктура открытых ключей.

**Цели работы и задачи исследования.** Цель работы–исследовать инфраструктуру открытых ключей и разработать программу на базе C++ в которой будет содержаться краткая информация о предмете исследования. Поставленная цель определила следующие основные задачи исследования:

1. Анализ существующих методов механизмов аутентификации.

2. Исследование инфраструктуры открытых ключей.

3. Разработка программы, в которой будет содержаться краткая информация ЭТО КАКАЯ ЖЕ КРАТКАЯ??по теме исследования.

**Методы исследования.** Для решения поставленных задач были использованы теоретические методы исследования. Теоретическую основу исследования составил труд в области инфраструктуры открытых ключей Ю. Полянской и С. Горбатова.

**Техническое задание**

**1. Основание для разработки**

**ЗДЕСЬ И ДАЛЕЕ НАДО ЧИТАТЬ ГОСТ В ЧАСТИ ОФОРМЛЕНИЯ ЗАГОЛОВКОВ**

Программный продукт «Курсовая работа по теме Инфраструктуры открытых ключей» разработан в соответствии с заданием, выданным от кафедры «Информатика» Московского технического университета связи и информатики и утверждён научным руководителем доцентом кафедры «Информатика» к.п.н Гуриковым С.Р. дата утверждения 29 октября 2020 года.

**2.ВАМ НА ЛЕКЦИИ ГОВОРИЛИ ПУНКТЫНазначение разработки**

Разработанный продукт предназначен для ознакомления с основными теоретическими положениями по теме инфраструктуры открытых ключей и проверки знаний пользователя по пройденному материалу.

**3. Требования к программе**

Разработанный программный продукт будет отвечать следующим требованиям:

??????

3.1. Требования надёжности.

Разрабатываемая программа должны отвечать следующим требованиям надёжности:

* Защита от некорректных действий пользователя и ошибочных исходных данных.
* Программа не должна во время работы модифицировать свой код или коды других программ.
* Диалоговый интерфейс программы должен строиться на основе оконного интерфейса операционной системы Microsoft Windows.
* Для доступа к программе пользователь должен аутентифицировать себя.
* Обеспечение сохранности программы при её удалении.

3.2. Требования к составу и параметрам технических средств.

**3.2.1 Минимальные технические средства для использования программы**

* Процессор с тактовой частотой 1,8 ГГц.
* 2 ГБ оперативной памяти.
* Видеокарта, поддерживающая минимальное разрешение экрана 720p (1280 на 720 пикселей)
* Пространство на жестком диске: минимум 800 МБ до 210 ГБ доступного пространства.

**3.2.2 Дополнительные требования**

* .NET Framework 4.5.2 или выше
* Необходимы права администратора

3.3. Требования к информационной и программной совместимости

Создаваемая программа должна легко инсталлироваться, функционировать и корректно работать при наличии операционных систем следующего типа:

* Windows 10 версии 1703 или выше: Home, Professional, Education и Enterprise.
* Windows 8.1 (с обновлением 2919355): Core, Professional и Enterprise.
* Windows 7 SP1 (с последними обновлениями Windows): Home Premium, Professional, Enterprise, Ultimate.
* Windows Server 2019: Standard и Datacenter.
* Windows Server 2016: Standard и Datacenter.????????

3.4. Требования к программной документации.

К программе должна прилагаться следующая документация:

* Текст кода программы.
* Описание программы.
* Методика испытаний.
* Руководство пользователя.

3.5. Стадии и этапы разработки.

Чтобы выполнить поставленную задачу нужно пройти следующие этапы разработки продукта:

**ЗДЕСЬ И ДАЛЕЕ НАДО ЧИТАТЬ ГОСТ В ЧАСТИ ОФОРМЛЕНИЯ ТАБЛИЦ**

Таблица 1 – Стадии разработки

|  |  |  |  |
| --- | --- | --- | --- |
| Номер этапа | Название этапа | Срок выполнения | Отчет |
| 1 | Утверждение темы | До 02.10.2020 |  |
| 2 | Написание введения | До 12.10.2020 |  |
| 3 | Составление ТЗ и написание теоретической части | До 29.10.2020 |  |

**Глава 1. Изучение темы «Инфраструктуры открытых ключей»ЭТО КАК??**

**§ ЧЕГО ЭТО??1.1 Структура PKI**

Для удовлетворения требований аутентификации в распределенной среде механизмы на базе сертификатов используют криптографию с открытыми ключами. Они созданы на основе многих свойств своих предшественников и добавляют новые возможности. Инфраструктура открытых ключей (PKI) — это современная технология аутентификации, использующая для идентификации субъектов криптографию с открытыми ключами вместе со следующими механизмами:

* Механизмом установления доверия на базе определенной модели доверия.
* Механизмом присваивания субъектам имен, уникальных в данной среде.
* Механизмом распространения информации, характеризующей правильность связывания определенной пары ключей (открытого и секретного) с определенным именем субъекта в данной среде(такая информация фиксируется и предоставляется центром, которому доверяет верификатор информации).

**Конечно**, аутентификация — это только один из необходимых сервисов безопасности. Многие приложения также требуют конфиденциальности, целостности и невозможности отказаться от участия в обмене информацией. Технология PKI обеспечивает поддержку всех этих сервисов.

**Основные компоненты PKI**

Нельзя утверждать, что PKI сама по себе является инфраструктурой безопасности, но она может быть основой всеобъемлющей инфраструктуры безопасности. Инфраструктура открытых ключей представляет собой комплексную систему, сервисы которой реализуются и предоставляются с использованием технологии открытых ключей. Цель PKI состоит в управлении ключами и сертификатами, посредством которого корпорация может поддерживать надежную сетевую среду. PKI позволяет использовать сервисы шифрования и выработки цифровой подписи согласованно с широким кругом приложений, функционирующих в среде открытых ключей. Основными компонентами эффективной PKI являются:

* Удостоверяющий центр.
* Регистрационный центр.
* Репозиторий сертификатов.
* Архив сертификатов.
* Конечные субъекты (пользователи).

Взаимодействие компонентов PKI иллюстрирует рис. 1.



Рис. 1. Основные компоненты PKI

ДАВАЙТЕ ТАК, ХОТИТЕ СДАТЬ РАБОТУ, ЗНАЧИТ НУЖНО СЛУШАТЬ И СЛЫШАТЬ, ЧТО ГОВОРИТ ПРЕПОДАВАТЕЛЬ, ЧИТАТЬ ГОСТ

ДАЛЬШЕ Я НЕ СМОТРЮ, ЗДЕСЬ ОДНИ ЗАМЕЧАНИЯ

**Удостоверяющий центр**

Фундаментальная предпосылка криптографии с открытыми ключами заключалась в том, что два незнакомых субъекта должны иметь возможность безопасно связываться друг с другом. Например, если пользователь А желает отправить конфиденциальное сообщение пользователю В, с которым он ранее не встречался, то для шифрования сообщения он должен иметь возможность связать каким-либо образом пользователя В и его открытый ключ. Для сообщества потенциальных пользователей, объединяющего сотни тысяч или миллионов субъектов, наиболее практичным способом связывания открытых ключей и их владельцев является организация доверенных центров. Этим центрам большая часть сообщества или, возможно, все сообщество доверяет выполнение функций связывания ключей и идентификационных данных (идентичности) пользователей.

Такие доверенные центры в терминологии PKI называются удостоверяющими (УЦ); они сертифицируют связывание пары ключей с идентичностью, заверяя цифровой подписью структуру данных, которая содержит некоторое представление идентичности и соответствующего открытого ключа. Эта структура данных называется сертификатом открытого ключа (или просто сертификатом). **По сути**, сертификат представляет собой некое зарегистрированное удостоверение, которое хранится в цифровом формате и признается сообществом пользователей PKI законным и надежным. Для заверения электронного сертификата используется электронная цифровая подпись УЦ- в этом смысле удостоверяющий центру уподобляется нотариальной конторе, так как подтверждает подлинность сторон, участвующих в обмене электронными сообщениями или документами.

Хотя УЦ не всегда входит в состав PKI, он является критически важным компонентом многих крупномасштабных PKI. Непосредственное использование открытых ключей требует дополнительной их защиты и идентификации для установления связи с секретным ключом. Без такой дополнительной защиты злоумышленник может выдавать себя как за отправителя подписанных данных, так и за получателя зашифрованных данных, заменив значение открытого ключа или нарушив его идентификацию. Все это приводит к необходимости проверки подлинности, то есть верификации открытого ключа.

**Таким образом** удостоверяющий центрявляется главным управляющим компонентом PKI

**Регистрационный центр**

Регистрационный центр (РЦ) является необязательным компонентом PKI. Обычно РЦ получает от удостоверяющего центра полномочия регистрировать пользователей, обеспечивать их взаимодействие с УЦ и проверять информацию, которая заносится в сертификат. Сертификат может содержать информацию, которая предоставлена субъектом, подающим заявку на сертификат и предъявляющим документ (паспорт, водительские права, чековую книжку и т.п.) или третьей стороной (например, кредитным агентством - о кредитном лимите пластиковой карты). Иногда в сертификат включается информация из отдела кадров или данные, характеризующие полномочия субъекта в компании (например, право подписи документов определенной категории). РЦ агрегирует эту информацию и предоставляет ее УЦ.

УЦ может работать с несколькими регистрационными центрами, в этом случае он поддерживает список аккредитованных регистрационных центров, то есть тех, которые признаны надежными. УЦ выдает сертификат РЦ и отличает его по имени и открытому ключу. РЦ выступает как объект, подчиненный УЦ, и должен адекватно защищать свой секретный ключ. Проверяя подпись РЦ на сообщении или документе, УЦ полагается на надежность предоставленной РЦ информации.

РЦ объединяет комплекс программного и аппаратного обеспечения и людей, работающих на нем. В функции РЦ может входить генерация и архивирование ключей, уведомление об аннулировании сертификатов, публикация сертификатов и САС в каталоге LDAP и др. Но РЦ не имеет полномочий выпускать сертификаты и списки аннулированных сертификатов. Иногда УЦ сам выполняет функции РЦ. **В связи с этим** РЦ можно назвать расширением, которое увеличивает функционал программы

**Репозиторий сертификатов**

Репозиторий- специальный объект инфраструктуры открытых ключей, база данных, в которой хранится реестр сертификатов Репозиторий значительно упрощает управление системой и доступ к ресурсам. Он предоставляет информацию о статусе сертификатов, обеспечивает хранение и распространение сертификатов и САС, управляет внесениями изменений в сертификаты. К репозиторию предъявляются следующие требования:

* простота и стандартность доступа;
* регулярность обновления информации;
* встроенная защищенность;
* простота управления;
* совместимость с другими хранилищами (необязательное требование).

Репозиторий обычно размещается на сервере каталогов, организованных в соответствии с международным стандартом X.500 и его подмножеством. Большинство серверов каталогов и прикладное программное обеспечение пользователей поддерживают упрощенный протокол доступа к каталогам LDAP (Lightweight Directory Access Protocol). Такой унифицированный подход позволяет обеспечивать функциональную совместимость приложений PKI и дает возможность доверяющим сторонам получать информацию о статусе сертификатов для верификации цифровых подписей.

**Архив сертификатов**

На архив сертификатов возлагается функция долговременного хранения (от имени УЦ) и защиты информации обо всех изданных сертификатах. Архив поддерживает базу данных, используемую при возникновении споров по поводу надежности электронных цифровых подписей, которыми в прошлом заверялись документы. Архив подтверждает качество информации в момент ее получения и обеспечивает целостность данных во время хранения. Информация, предоставляемая УЦ архиву, должна быть достаточной для определения статуса сертификатов и их издателя. Архив должен быть защищен соответствующими техническими средствами и процедурами.

**Конечные субъекты**

Конечные субъекты, или пользователи, PKI делятся на две категории: владельцы сертификатов и доверяющие стороны. Они используют некоторые сервисы и функции PKI, чтобы получить сертификаты или проверить сертификаты других субъектов. Владельцем сертификата может быть физическое или юридическое лицо, приложение, сервер ит. д. Доверяющие стороны запрашивают и полагаются на информацию о статусе сертификатов и открытых ключах подписи своих партнеров по деловому общению.

**Физическая топология**

Система PKI, помимо выполнения целого ряда функций – выпуска сертификатов, генерации ключей, управления безопасностью, аутентификации, восстановления данных, - должна обеспечивать интеграцию с внешними системами. PKI необходимо взаимодействовать с множеством самых разных систем и приложений -это и программное обеспечение групповой работы, и электронная почта, и системы управления доступом, и каталоги пользователей, и виртуальные частные сети, и разнообразные операционные системы, и службы безопасности, и web-приложения, и широкий спектр корпоративных систем.

Функциональные компоненты PKI (УЦ, РЦ и др.) могут быть реализованы программно и аппаратно различными способами, например, располагаться на одном или нескольких серверах. Системы, выполняющие функции удостоверяющего и регистрационного центров, часто называют серверами сертификатов и регистрации соответственно.

**Серверные компоненты PKI**

Основными серверными компонентами PKI являются сервер сертификатов, сервер каталогов и сервер восстановления ключей, опциональными компонентами – сервер регистрации, OCSP–сервер, обслуживающий запросы пользователей по онлайновому протоколу статуса сертификата Online Certificate Status Protocol и сервер проставления меток времени.

На сервер сертификатов возлагаются функции выпуска и управления сертификатами, защищенного хранения секретного ключа удостоверяющего центра, поддержки жизненного цикла сертификатов и ключей, восстановления данных, ведения контрольного журнала и регистрации всех операций удостоверяющего центра.

Сервер каталогов содержит информацию о сертификатах и атрибутах субъектов сертификатов открытых ключей. Через протокол LDAP приложения стандартным образом обращаются к записям каталогов, например, к адресам электронной почты, номерам телефонов, полномочиям и сертификатам пользователей.

Сервер каталогов должен обеспечивать:

* Сетевую аутентификацию через IP–адреса или DNS-имена и аутентификацию конечных субъектов по именам и паролям или по сертификатам открытых ключей;
* Управление доступом субъектов к информации в зависимости от их прав на выполнение операций чтения, записи, уничтожения, поиска или сравнения;
* Конфиденциальность (посредством протокола SSL) и целостность сообщений для всех видов связи.

Сервер восстановления ключей поддерживает создание резервных копий и восстановление ключей шифрования конечных субъектов. Среди всех компонентов PKI сервер восстановления ключей должен быть наиболее защищен и обеспечивать сильную аутентификацию администратора и пользователей, поддержку конфиденциальности и целостности сообщений, безопасное хранение всех компонентов ключей.

PKI управляет ключами и сертификатами, используемыми для реализации криптографических операций в web-браузерах, web–серверах, приложениях электронной почты, электронного обмена сообщениями и данными, в приложениях, поддерживающих защищенные сетевые транзакции и сеансы связи через World Wide Web или в виртуальных частных сетях на базе протоколов S/MIME, SSL и IPsec, а также для заверения цифровой подписью электронных документов или программного кода. Наряду с перечисленными выше приложениями, PKI-совместимыми могут быть и корпоративные приложения, разработанные внутри организации.

Приложения электронной почты и обмена сообщениями используют пары ключей для шифрования сообщений и файлов и заверения их цифровыми подписями. Системы электронного обмена данными поддерживают транзакции, требующие аутентификации сторон, обеспечения конфиденциальности и целостности данных. Браузеры и web–серверы используют шифрование для аутентификации, обеспечения конфиденциальности, а также в приложениях электронной коммерции и онлайнового предоставления банковских услуг. Шифрование и аутентификация применяются также для создания виртуальных частных сетей (Virtual Private Networks—VPN) на основе сетей общего пользования, для защиты коммуникаций между сайтами или удаленного доступа (клиент-сервер). Заверение цифровой подписью программных кодов и файлов дает возможность пользователям подтвердить источник получаемых по Интернету программ и файлов и целостность их содержания, это важно и для контроля вирусного заражения.

**§1.2 Сервисы безопасности PKI**

Сервис безопасности представляет собой совокупность механизмов, процедур и других средств управления для снижения рисков, связанных с угрозой утраты или раскрытия данных [2]. В основном считается, что PKI должна предоставлять три основных сервиса безопасности: аутентификацию, целостность и конфиденциальность.

Сервис идентификация и аутентификация обеспечивает аутентификацию участников коммуникации и аутентификацию источника данных.

Сервис целостности предотвращает преднамеренное или случайное несанкционированное изменение данных, в том числе их ввод, уничтожение или модификацию (изменение, сокращение или дополнение), в процессе передачи по сети. Для гарантирования целостности система должна обнаруживать несанкционированную модификацию информации. Цель получателя информации - убедиться в том, что данные при передаче не были изменены.

Сервис конфиденциальности обеспечивает защиту от несанкционированного получения информации: разрешает доступ к конфиденциальным данным только пользователям, имеющим соответствующие права, и предотвращает несанкционированное раскрытие информации не имеющими полномочий пользователями или процессами.

**Идентификация и аутентификация**

Идентификацией субъекта называется процесс сопоставления введенной им своей характеристики с некоторым идентификатором, хранимым системой. В дальнейшем идентификатор субъекта используется для предоставления субъекту определенного уровня прав и полномочий. Аутентификацией субъекта называется процедура проверки принадлежности идентификатора субъекту. Аутентификация осуществляется на основании того или иного секретного элемента (аутентификатора), которым располагают как субъект, так и информационная система.

Обычный способ идентификации - ввод имени пользователя при входе в систему. Для аутентификации пользователей, то есть проверки подлинности их личности, чаще всего используются пароли. При аутентификации источника данных подтверждается подлинность источника отдельной порции данных. Функция не обеспечивает защиты против повторной передачи данных. Аутентификация обычно находит применение в двух основных контекстах: идентификации субъекта и идентификации источника данных.

Идентификация субъекта служит просто для распознавания субъекта независимо от его последующих действий. Очевидно, что одной идентификации недостаточно, поскольку субъект, как правило, не только называет себя, но и желает получить возможность выполнять некоторые действия. На практике результат идентификации субъекта позволяет ему связываться с другими субъектами или выполнять определенные виды активности. Например, в результате идентификации субъект может получить секретный ключ, которым он затем может воспользоваться для расшифрования файла, а также для установления защищенной связи с другим субъектом. Идентификационные данные субъекта, который прошел аутентификацию, также могут быть связаны с некоторыми полномочиями доступа, на основании которых принимаются решения по контролю доступа.

Все приведенные замечания были сделаны вовсе не для того, чтобы преуменьшить важность идентификации субъекта. Защищенная система не может существовать без строгого механизма аутентификации. Аутентификация — это критически важный и необходимый шаг к работе защищенной системы, но это только первый шаг. Аутентификация сама по себе не является конечной целью.

Идентификация источника данных выполняется с намерением стационарно и окончательно связать идентифицированного субъекта с некоторыми определенными данными независимо от его любых дальнейших действий. Такой процесс может обеспечить поддержку сервиса неотказуемости.

По степени приближенности субъекта к среде различают следующие процедуры идентификации:

1. Начальную идентификацию субъекта в локальной среде, то есть на персональном, физически приближенном к субъекту устройстве без связи с другими устройствами в сети;

2. Идентификацию субъекта в удаленной среде или при доступе к удаленному устройству

В процедуре локальной аутентификации, или начальной аутентификации субъекта в локальной среде, почти всегда явно и непосредственно участвует пользователь, который должен ввести пароль или предъявить биометрические характеристики (отпечатки пальцев, рисунок радужной оболочки глаза). Удаленная аутентификация, или аутентификация субъекта в некоторой удаленной среде, может выполняться как с участием, так и без участия пользователя. Обычно, более сложные системы аутентификации явным образом не включают пользователя. Это происходит по двум причинам:

1. Трудно защитить систему аутентификации, которая получает секретную информацию, идентифицирующую субъекта (например, пароль или отпечатки пальцев), и передает ее на расстояние по незащищенным каналам, где она может быть скопирована с мошенническими целями недобросовестной стороной.

2. Пользователям неудобно вводить аутентифицирующую информацию всякий раз, когда они желают получить доступ к удаленной сети.

Таким образом, более рациональным решением является передача на расстояние результата процесса локальной аутентификации без передачи самой фактической информации, аутентифицирующей субъекта. Субъект может получить доступ к удаленной среде на основании положительного результата его аутентификации в локальной среде, если между локальной и удаленной средами установлена защищенная связь. В этом случае нет необходимости передавать на расстояние пароль, PIN-код или биометрические характеристики. Отметим, что такое решение может использоваться для последующей аутентификации (после успешно завершившейся начальной аутентификации) для работы с другими приложениями в локальной среде, то есть для защищённой однократной регистрации.

Существует много способов доказательства идентичности субъекта, но любой способ предусматривает предъявление одного из четырех возможных идентифицирующих признаков:

1. Того, что субъект имеет (например, смарт-карты или аппаратного ключа);

2. Того, что субъект знает (например, пароля или PIN-кода);

3. Того, чем субъект является (например, отпечатков пальцев, параметров ладони или рисунка радужной оболочки глаза);

4. Того, что субъект делает (например, клавиатурного почерка).

При однофакторной идентификации используется только один из перечисленных методов, при многофакторной идентификации- более одного метода (двухфакторная идентификация использует два метода, трехфакторная - три и т.д.). Известным примером двухфакторной аутентификации является процесс однократной регистрации при пользовании банкоматом, когда пользователь вставляет карту со встроенным чипом (то, что пользователь имеет) и вводит PIN-код (то, что пользователь знает), чтобы получить доступ к своему банковскому счету. Очевидно, что системы многофакторной идентификации требуют больших затрат усилий от пользователя, но более эффективны в смысле безопасности и практически лишают злоумышленника возможности выдать себя за легитимного пользователя.

Сервисы PKI обычно не используются для начальной (безразлично -однофакторной или многофакторной) аутентификации в локальной среде, но необходимы для аутентификации в удаленной среде (или последующей аутентификации в локальной среде), которая выполняется на базе сложных протоколов запроса-подтверждения и подписанных цифровой подписью сообщений. Важным преимуществом удаленной аутентификации на базе открытых ключей перед механизмами, которые имитируют аутентификацию в локальной среде, является то, что секретная информация, идентифицирующая субъекта, никогда не передается по сети. Если пользователь А хранит копию пароля или отпечатка пальца пользователя В, то пользователь В должен пройти аутентификацию, доказывая, что он знает или имеет эту информацию; это обычно выполняется путем передачи этой информации пользователю А в процессе регистрации. Если пользователь А владеет копией открытого ключа подписи пользователя В, то может попросить пользователя В подписать сообщение-запрос своим секретным ключом подписи (который известен только В). Если подписанный запрос возвращается, то пользователь В аутентифицировал себя без раскрытия какой-либо секретной информации. По сети не передается та информация, которая может быть использована злоумышленником для маскировки под пользователя В. Более того, пользователям А и В нет необходимости участвовать в дорогом и неудобном процессе предварительного создания разделяемого секрета (например, в передаче пользователю А копии пароля или отпечатка пальца пользователя В ).Пользователь А может просто воспользоваться опубликованной в репозитории УЦ или присланной по электронной почте самим пользователем В копией его открытого ключа.

Преимуществом сервиса аутентификации PKI является возможность однократной регистрации через PKI-совместимые устройства (и возможно, через серверы шлюзов локальной сети к другим устройствам тоже). Пользователь сначала однократно регистрируется в локальной сети (используя однофакторную или многофакторную аутентификацию), после чего получает локальный доступ к своим секретным ключам. Затем секретный ключ подписи может быть использован для автоматической и прозрачной аутентификации пользователя другими серверами и устройствами сети независимо оттого, желает ли пользователь использовать их для коммуникации. Пользователь может свободно использовать локальную и удаленную среды без необходимости каждый раз вводить пароль или предъявлять для считывания отпечаток пальца.

**Таким образом** в первой главе мы познакомились с основными методами аутентификации пользователя, а также рассмотрели инфраструктуру открытых ключей (PKI), которые позволяют обеспечить безопасность файлов в системе, а также позволяют устроить удалённую идентификацию пользователя с помощью ключей безопасности.

**Список используемых источников**

1. Полянская, О. Ю. Инфраструктуры открытых ключей: учебное пособие / О. Ю. Полянская, В. С. Горбатов. — 3-е изд. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 452 c. — ISBN 978-5-4497-0382-8. URL: (<http://www.iprbookshop.ru/89439.html>) (дата обращения: 29.10.2020). — Текст: электронный.

2.ГОСТ 19.201-78 Техническое задание, требования к содержанию и оформлению. URL: (http://docs.cntd.ru/document/gost-19-201-78) (дата обращения: 29.10.2020).