История

Начало асимметричным шифрам было положено в работе «Новые направления в современной криптографии» Уитфилда Диффи и Мартина Хеллмана, опубликованной в 1976 году. Находясь под влиянием работы Ральфа Меркле (англ. Ralph Merkle) о распространении открытого ключа, они предложили метод получения секретных ключей, используя открытый канал. Этот метод экспоненциального обмена ключей, который стал известен как обмен ключами Диффи — Хеллмана, был первым опубликованным практичным методом для установления разделения секретного ключа между заверенными пользователями канала. В 2002 году Хеллман предложил называть данный алгоритм «Диффи — Хеллмана — Меркле», признавая вклад Меркле в изобретение криптографии с открытым ключом. Эта же схема была разработана Малькольмом Вильямсоном в 1970-х, но держалась в секрете до 1997 г. Метод Меркле по распространению открытого ключа был изобретён в 1974 и опубликован в 1978 году, его также называют загадкой Меркле.

В 1977 году учёными Рональдом Ривестом, Ади Шамиром и Леонардом Адлеманом из Массачусетского технологического института был разработан алгоритм шифрования, основанный на проблеме о разложении на множители. Система была названа по первым буквам их фамилий (RSA — Rivest, Shamir, Adleman). Эта же система была изобретена в 1973 году Клиффордом Коксом (англ. Clifford Cocks), работавшим в центре правительственной связи (GCHQ), но эта работа хранилась лишь во внутренних документах центра, поэтому о её существовании было неизвестно до 1977 года. RSA стал первым алгоритмом, пригодным и для шифрования, и для электронной подписи.

Объекты PKI

PKI реализуется в модели [клиент-сервер](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D0%B8%D0%B5%D0%BD%D1%82-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80), то есть проверка какой-либо информации, предоставляемой инфраструктурой, может происходить только по инициативе клиента.

**Основные компоненты PKI:**

* [**Удостоверяющий центр**](https://ru.wikipedia.org/wiki/%D0%A6%D0%B5%D0%BD%D1%82%D1%80_%D1%81%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8) (УЦ) является основной структурой, формирующей цифровые сертификаты подчиненных центров сертификации и конечных пользователей. УЦ является главным компонентом PKI:

1. он является [доверенной третьей стороной](https://ru.wikipedia.org/w/index.php?title=%D0%94%D0%BE%D0%B2%D0%B5%D1%80%D0%B5%D0%BD%D0%BD%D0%B0%D1%8F_%D1%82%D1%80%D0%B5%D1%82%D1%8C%D1%8F_%D1%81%D1%82%D0%BE%D1%80%D0%BE%D0%BD%D0%B0&action=edit&redlink=1) (trusted third party)
2. это сервер, который осуществляет управление жизненным циклом сертификатов (но не их непосредственным использованием).

* [**Сертификат открытого ключа**](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%82_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D0%BE%D0%B3%D0%BE_%D0%BA%D0%BB%D1%8E%D1%87%D0%B0) (чаще всего просто *сертификат*) — это данные пользователя и его открытый ключ, скреплённые электронной подписью удостоверяющего центра. Выпуская сертификат открытого ключа, удостоверяющий центр тем самым подтверждает, что лицо, поименованное в сертификате, владеет закрытым ключом, который соответствует этому открытому ключу.
* **Регистрационный центр** (РЦ) — необязательный компонент системы, предназначенный для регистрации пользователей. Для этих целей РЦ обычно предоставляет веб-интерфейс. Удостоверяющий центр доверяет регистрационному центру проверку информации о субъекте. Регистрационный центр, проверив правильность информации, подписывает её своим ключом и передаёт удостоверяющему центру, который, проверив ключ регистрационного центра, выписывает сертификат. Один регистрационный центр может работать с несколькими удостоверяющими центрами (то есть состоять в нескольких PKI), один удостоверяющий центр может работать с несколькими регистрационными центрами. Иногда, удостоверяющий центр выполняет функции регистрационного центра.
* **Репозиторий** — хранилище, содержащее сертификаты и [списки отозванных сертификатов](https://ru.wikipedia.org/wiki/%D0%A1%D0%BF%D0%B8%D1%81%D0%BA%D0%B8_%D0%BE%D1%82%D0%BE%D0%B7%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D1%85_%D1%81%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%82%D0%BE%D0%B2) (СОС) и служащее для распространения этих объектов среди пользователей. В Федеральном Законе РФ № 63 «Об электронной подписи» он называется *реестр сертификатов ключей подписей*.
* **Архив сертификатов** — хранилище всех изданных когда-либо сертификатов (включая сертификаты с закончившимся сроком действия). Архив используется для проверки подлинности электронной подписи, которой заверялись документы.
* **Центр запросов** — необязательный компонент системы, где конечные пользователи могут запросить или отозвать сертификат.
* **Конечные пользователи** — пользователи, приложения или системы, являющиеся владельцами сертификата и использующие инфраструктуру управления открытыми ключами.

Основные задачи

Основные задачи системы информационной безопасности, которые решает инфраструктура управления открытыми ключами:

* обеспечение конфиденциальности информации;
* обеспечение целостности информации;
* обеспечение аутентификации пользователей и ресурсов, к которым обращаются пользователи;
* обеспечение возможности подтверждения совершенных пользователями действий с информацией (неотказуемость, (неотрекаемость, апеллируемость) — англ. non-repudiation).

Основная идея

Упрощенно, PKI представляет собой систему, основным компонентом которой является удостоверяющий центр и пользователи, взаимодействующие между собой используя сертификаты, выданные этим удостоверяющим центром. Деятельность инфраструктуры управления открытыми ключами осуществляется на основе регламента системы. Инфраструктура открытых ключей основывается на использовании принципов [криптографической системы с открытым ключом](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0_%D1%81_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%BC_%D0%BA%D0%BB%D1%8E%D1%87%D0%BE%D0%BC). Инфраструктура управления открытыми ключами состоит из [центра сертификации](https://ru.wikipedia.org/wiki/%D0%A3%D0%B4%D0%BE%D1%81%D1%82%D0%BE%D0%B2%D0%B5%D1%80%D1%8F%D1%8E%D1%89%D0%B8%D0%B9_%D1%86%D0%B5%D0%BD%D1%82%D1%80) ([удостоверяющего центра](https://ru.wikipedia.org/wiki/%D0%A3%D0%B4%D0%BE%D1%81%D1%82%D0%BE%D0%B2%D0%B5%D1%80%D1%8F%D1%8E%D1%89%D0%B8%D0%B9_%D1%86%D0%B5%D0%BD%D1%82%D1%80) — УЦ), конечных пользователей и опциональных компонентов: центра регистрации и сетевого справочника.

***Основные функции удостоверяющего центра:***

* проверка личности будущих пользователей сертификатов;
* выдача пользователям сертификатов;
* аннулирование сертификатов;
* ведение и публикация списков отозванных сертификатов (Certificate Revocation List/CRL), которые используются клиентами инфраструктуры открытого ключа, когда они решают вопрос о доверии сертификату.

***Дополнительные функции удостоверяющего центра:***

* УЦ может производить генерацию пар ключей, один из которых будет включен в сертификат.
* По запросу, при разрешении конфликтов, УЦ может производить проверку подлинности электронной подписи владельца сертификата, выданного этим УЦ.

**Сертификат** — это электронный документ, который содержит электронный ключ пользователя (открытый ключ), информацию о пользователе, которому принадлежит сертификат, электронную подпись [центра выдачи сертификатов](https://ru.wikipedia.org/wiki/%D0%A3%D0%B4%D0%BE%D1%81%D1%82%D0%BE%D0%B2%D0%B5%D1%80%D1%8F%D1%8E%D1%89%D0%B8%D0%B9_%D1%86%D0%B5%D0%BD%D1%82%D1%80) (УЦ), информацию о сроке действия сертификата и другие атрибуты. Сертификат не может быть бессрочным, он всегда содержит дату и время начала и окончания своего действия.

Причины досрочного аннулирования сертификатов:

* компрометация закрытого ключа;
* изменение информации о владельце сертификата, содержащейся в этом сертификате;
* добровольное заявление владельца сертификата;
* изменения полномочий текущего владельца сертификата.

*Ключевая пара* — это набор, состоящий из двух ключей: закрытого ключа (private key) и открытого ключа (public key). Эти ключи создаются вместе, являются комплементарными по отношению друг к другу (то, что зашифровано с помощью открытого ключа можно расшифровать, только имея закрытый ключ, а электронную подпись, сделанную с помощью закрытого ключа, можно проверить, используя открытый ключ).

Ключевая пара создается либо [центром выдачи сертификатов (удостоверяющим центром)](https://ru.wikipedia.org/wiki/%D0%A3%D0%B4%D0%BE%D1%81%D1%82%D0%BE%D0%B2%D0%B5%D1%80%D1%8F%D1%8E%D1%89%D0%B8%D0%B9_%D1%86%D0%B5%D0%BD%D1%82%D1%80) по запросу пользователя, или же самим пользователем с помощью специального программного обеспечения. Пользователь делает запрос на сертификат, и после процедуры идентификации пользователя УЦ выдаёт ему сертификат, подписанный этим Удостоверяющим Центром. Электронная подпись УЦ свидетельствует о том, что данный сертификат выдан именно этим центром и никем другим.

Открытый ключ известен всем, в то время закрытый ключ хранится в тайне. Владелец закрытого ключа всегда хранит его в тайне и ни при каких обстоятельствах не должен допустить того, чтобы этот ключ стал известным злоумышленникам или другим пользователям. Если же закрытый ключ всё-таки станет известен злоумышленникам, то он считается [скомпрометированным](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%80%D0%BE%D0%BC%D0%B5%D1%82%D0%B0%D1%86%D0%B8%D1%8F_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)), поэтому сертификат со связанным с ним открытым ключом должен быть отозван. Только владелец закрытого ключа может подписать данные, а также расшифровать данные, которые были зашифрованы открытым ключом, связанным с закрытым ключом владельца. Действительная подпись гарантирует авторство информации и то, что информация в процессе передачи не подверглась изменениям. Подпись кода гарантирует, что данное программное обеспечение действительно произведено указанной компанией и не содержит вредоносного кода, если компания это декларирует.

Собственный закрытый ключ используется для подписи данных; собственный закрытый ключ, в свою очередь, используется для расшифрования данных, полученных от других участников PKI. Открытый ключ, извлеченный из сертификата другого участника Инфраструктуры Открытых Ключей, может использоваться для подтверждения корректности электронной подписи этого участника, а также для шифрования данных отправляемых этому участнику. Процесс шифрования с использованием асимметричной криптографии является медленным по сравнению с симметричными алгоритмами, поэтому использование его для шифрования данных не рекомендуется и по факту не производится в системах, где время является критическим фактором. При использовании сертификатов открытых ключей для защищенного взаимодействия с веб-сайтами (интернет-магазинами, банками), сертификаты используются только для установления защищенной связи; для последующего обмена информацией используются выбранные сторонами симметричные ключи.

*Одним из ключевых понятий ИОК является электронная подпись. В рамках этой статьи понятия подпись, электронная подпись (ЭП), цифровая подпись и электронная цифровая подпись (ЭЦП) взаимозаменяемы. В Федеральном Законе РФ № 1 «Об электронно-цифровой подписи» от 2001 года, существовало только понятие электронно-цифровой подписи. Федеральный Закон РФ № 63 «Об электронной подписи» от 2011 года расширил понятие подписи. В соответствии со статьей 5 «Виды электронных подписей», различают простую электронную подпись и усиленную электронную подпись. В текущей статье и практически во всех литературных источниках об Инфраструктуре Открытых Ключей, как англоязычных, так и русскоязычных, под понятием подписи понимается усиленная электронная подпись.*

Электронная подпись — это результат использования алгоритма электронной подписи на хэш данных (документа/сообщения/файла).

Подлинность электронной подписи проверяется следующим образом:

1. Получатель получает данные (зашифрованные или в открытом виде) и электронную подпись.
2. [Опциональный шаг, так как документ/сообщение/файл мог быть отправлен в открытом виде]. Данные расшифровываются с помощью либо заранее оговоренного симметричного ключа, либо с помощью закрытого ключа получателя (во втором случае данные были зашифрованы с помощью открытого ключа получателя, извлеченного из его сертификата).
3. Получатель вычисляет хэш расшифрованного документа/сообщения/файла (алгоритм хэш указан в сертификате).
4. Получатель применяет к электронной подписи алгоритм снятия подписи (алгоритм подписи указан в сертификате), в результате чего получает хэш исходного документа/сообщения/файла.
5. Получатель сравнивает хэши. Если они одинаковы — электронная подпись считается действительной, при условии, что сертификат действителен и был применен в соответствии с его политиками.

В число приложений, поддерживающих PKI, входят: защищённая [электронная почта](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D1%87%D1%82%D0%B0), протоколы платежей, электронные чеки, электронный обмен информацией, защита данных в сетях с протоколом [IP](https://ru.wikipedia.org/wiki/IP), электронные формы и документы с электронной [цифровой подписью](https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C) (ЭП).

**Краткое описание процесса работы с личными сертификатами**

Для того чтобы получить сертификат, нужно обратиться в Удостоверяющий Центр. Перед запросом на получение сертификата нужно удостовериться, что данный УЦ аккредитован в той сфере, где владелец сертификата будет его использовать. Для получения сертификата необходимо сгенерировать пару открытый-закрытый ключи; это производит либо пользователь, либо УЦ, в зависимости от политики Удостоверяющего Центра или договоренностей между клиентом и УЦ.

Для использования сертификатов (подписи или проверки подписи), пользователь должен установить на используемую Операционную систему криптографические средства, поддерживающие работу с данными сертификатами и алгоритмами электронной подписи.

После получения сертификата его нужно установить в свою систему. При использовании ОС семейства Windows, после установки сертификата его можно будет увидеть через оснастку «хранилище личных сертификатов» (Пуск -> Выполнить -> certmgr.msc -> OK). В свойствах можно увидеть время действия сертификата, кем он был выдан, кому был выдан, его уникальный номер и другие атрибуты. Для того, чтобы клиент мог работать с [удостоверяющим центром](https://ru.wikipedia.org/wiki/%D0%A3%D0%B4%D0%BE%D1%81%D1%82%D0%BE%D0%B2%D0%B5%D1%80%D1%8F%D1%8E%D1%89%D0%B8%D0%B9_%D1%86%D0%B5%D0%BD%D1%82%D1%80), необходимо включить центр в список доверенных. После включения в этот список, любой сертификат, выданный доверенным центром, считается достоверным, а его владелец — достойным доверия. Пользователи обмениваются сертификатами (таким образом происходит обмен открытыми ключами) и начинают взаимодействие.

**Архитектуры PKI**

В основном выделяют 5 видов архитектур PKI, это:

1. простая PKI (одиночный УЦ)
2. иерархическая PKI
3. сетевая PKI
4. кросс-сертифицированные корпоративные PKI
5. архитектура мостового УЦ

В основном PKI делятся на разные архитектуры по следующим признакам:

* количество УЦ (а также количество УЦ, которые доверяют друг-другу)
* сложность проверки пути сертификации
* последствия выдачи злоумышленника себя за УЦ

Рассмотрим более подробно каждую из архитектур PKI в отдельности.

**1. Простая PKI**[

Как уже говорилось выше, самая простая из архитектур, это архитектура одиночного УЦ. В данном случае все пользователи доверяют одному УЦ и переписываются между собой. В данной архитектуре, если злоумышленник выдаст себя за УЦ, необходимо просто перевыпустить все выписанные сертификаты и продолжить нормальную работу.

**2. Иерархическая PKI**[

Иерархическая структура — это наиболее часто встречающаяся архитектура PKI. В данном случае во главе всей структуры стоит один Головной УЦ, которому все доверяют и ему подчиняются нижестоящие УЦ. Кроме этого головного УЦ в структуре присутствуют ещё не один УЦ, который подчиняется вышестоящему, которому в свою очередь приписаны какие-либо пользователи или нижестоящие УЦ. Частный пример иерархической PKI — корпоративная PKI. В иерархической PKI, даже если злоумышленник выдал себя за какой — либо УЦ, сеть продолжает работать без него, а когда он восстанавливает нормальную работоспособность — он просто снова включается в структуру.

**3. Сетевая PKI**[

Сетевая архитектура PKI строится как сеть доверия, многочисленные удостоверяющие центры которой предоставляют PKI-сервисы и связаны одноранговыми, то есть равноправными, отношениями. Но в данном случае нет одного головного УЦ, которому все доверяют. В этой архитектуре все УЦ доверяют рядом стоящим УЦ, а каждый пользователь доверяет только тому УЦ, у которого выписал сертификат. Удостоверяющие центры выпускают сертификаты друг для друга; пара сертификатов описывает двусторонние отношения доверия. В данную архитектуру PKI легко добавляется новый УЦ, для этого ему нужно обменяться сертификатами, по крайней мере, с одним УЦ, который уже входит в сеть. В данной архитектуре наиболее сложное построение цепочки сертификации.

Сетевые PKI обладают большой гибкостью, так как имеют многочисленные пункты доверия. [Компрометация](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%80%D0%BE%D0%BC%D0%B5%D1%82%D0%B0%D1%86%D0%B8%D1%8F_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)) одного УЦ не отражается на сетевой PKI в целом: удостоверяющие центры, которые выпустили сертификаты для скомпрометированного УЦ, просто аннулируют их, тем самым удаляя из инфраструктуры ненадежный УЦ. В результате не нарушается работа пользователей, связанных с другими удостоверяющими центрами, — они по-прежнему могут полагаться на надежные пункты доверия и защищенно связываться с остальными пользователями своей PKI. Компрометация сетевой PKI приводит либо к тому, что сворачивается работа одного УЦ вместе с его сообществом пользователей, либо, если стали ненадежными несколько удостоверяющих центров, к тому, что PKI распадается на несколько меньших инфраструктур. Восстановление после компрометации сетевой PKI происходит проще, чем иерархической, прежде всего, потому что компрометация затрагивает меньше пользователей.

Построить путь сертификации в сети достаточно сложно, поскольку этот процесс не детерминирован и имеются многочисленные варианты формирования цепи сертификатов. Одни из них приводят к построению правильного пути, другие — заводят в тупик. По этой причине валидация пути сертификации часто выполняется одновременно с его построением, частью этого процесса является удаление неверных ветвей. Для построения правильного пути используется несколько дополнительных полей сертификатов.

**4. Архитектура кросс-сертифицированной корпоративной PKI**[

Данный вид архитектуры можно рассматривать как смешанный вид иерархической и сетевой архитектур. Есть несколько фирм, у каждой из которых организована какая-то своя PKI, но они хотят общаться между собой, в результате чего возникает их общая межфирменная PKI.В архитектуре кросс-сертифицированной корпоративной PKI самая сложная система цепочки сертификации.

**5. Архитектура мостового УЦ**[

Архитектура мостового УЦ разрабатывалась для того, чтобы убрать недостатки сложного процесса сертификации в кросс-сертифицированной корпоративной PKI. В данном случае все компании доверяют не какой-то одной или двум фирмам, а одному определённому мостовому УЦ, который является практически их головным УЦ, но он не является основным пунктом доверия, а выступает в роли посредника между другими УЦ.

Внедрение PKI[

Внедрение инфраструктуры управления открытыми ключами с учетом снижения затрат и сроков внедрения осуществляется в течение семи этапов.

* Этап 1. Анализ требований к системе.
* Этап 2. Определение архитектуры.
* Этап 3. Определение регламента.
* Этап 4. Обзор системы безопасности. Анализ и минимизация рисков.
* Этап 5. Интеграция.
* Этап 6. Развертывание.
* Этап 7. Эксплуатация.

Примеры использования PKI[

**Электронная подпись (ЭП)**[

Сторона А для документа вычисляет хеш-функцию, затем полученное значение шифруется с помощью закрытого ключа (private key) получая ЭП. Сторона Б получает документ, ЭП и сертификат (ссылку на сертификат) стороны А, верифицирует сертификат открытого ключа стороны А в удостоверяющем центре, дешифрует полученную ЭП при помощи публичного ключа (public key), вычисляет хеш-функцию документа и проверяет с расшифрованым значением. Если сертификат стороны А действителен и проверка прошла успешно, принимается, что документ был подписан стороной А.

**Шифрование сообщений**[ | ]

Сторона Б зашифровывает документ открытым ключом стороны А. Чтобы убедиться, что открытый ключ действительно принадлежит стороне А, сторона Б запрашивает сертификат открытого ключа у удостоверяющего центра. Если это так, то только сторона А может расшифровать сообщение, так как владеет соответствующим закрытым ключом.

**Авторизация**[ | ]

Сертификаты могут использоваться для подтверждения личности пользователя и задания полномочий, которыми он наделён. В числе полномочий субъекта сертификата может быть, например, право просматривать информацию или разрешение вносить изменения в материал, представленный на web-сервере.

Терминология PKI[ | ]

Из всего выше сказанного можно выделить некоторые пункты, а также добавить новые, для того чтобы определить основные термины, используемые в PKI. Итак, в PKI используются термины:

[**Сертификат открытого ключа**](https://ru.wikipedia.org/wiki/%D0%A1%D0%B5%D1%80%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%82_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D0%BE%D0%B3%D0%BE_%D0%BA%D0%BB%D1%8E%D1%87%D0%B0)

электронный документ удостоверенный электронной подписью удостоверяющего центра, содержащий открытый ключ, информацию о сроке его действия и владельце ключа.

[**Закрытый ключ**](https://ru.wikipedia.org/wiki/%D0%97%D0%B0%D0%BA%D1%80%D1%8B%D1%82%D1%8B%D0%B9_%D0%BA%D0%BB%D1%8E%D1%87)

ключ, известный только его владельцу, сгенерированный с помощью асимметричного криптографического алгоритма, использующийся для [электронной подписи](https://ru.wikipedia.org/wiki/%D0%AD%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%B0%D1%8F_%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C) данных и расшифровки данных зашифрованных на соответствующем этому закрытому ключу открытом ключе.

[**Открытый ключ**](https://ru.wikipedia.org/wiki/%D0%9A%D0%BB%D1%8E%D1%87_(%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%8F)#%D0%9A%D0%BB%D0%B0%D1%81%D1%81%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F_%D0%BA%D0%BB%D1%8E%D1%87%D0%B5%D0%B9)

ключ, создаваемый в паре с закрытым ключом с помощью асимметричного криптографического алгоритма, используется для шифрования данных и проверки электронной подписи.

[**Отпечаток открытого ключа**](https://ru.wikipedia.org/wiki/%D0%9E%D1%82%D0%BF%D0%B5%D1%87%D0%B0%D1%82%D0%BE%D0%BA_%D0%BE%D1%82%D0%BA%D1%80%D1%8B%D1%82%D0%BE%D0%B3%D0%BE_%D0%BA%D0%BB%D1%8E%D1%87%D0%B0)**(fingerprint/thumbprint)**

информация, по которой можно идентифицировать открытый ключ. Отпечаток создаётся путём применения [криптографической хеш-функции](https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%B0%D1%8F_%D1%85%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F) к значению открытого ключа.

**Подписанные данные**

данные, подписанные при помощи закрытого ключа пользователя.

**Зашифрованные данные**

данные, зашифрованные при помощи открытого ключа пользователя.

**Путь доверия**

цепочка документов, которая позволяет удостовериться, что предъявленный сертификат был выдан доверенным центром; последним звеном в этой цепочке является предъявленный сертификат, начальным — сертификат корневого доверенного центра сертификации, а промежуточными — сертификаты, выданные промежуточным центрам сертификации. Особенностью пути доверия является то, что при потере доверия к начальному звену цепочки (корневому центру сертификации) теряется доверие ко всей цепочке, то есть ко всем выданным данным центром сертификатам и к предъявленному в том числе.

**Личные сертификаты**

сертификаты которые хранятся у пользователя в личном хранилище сертификатов.

**Корневые центры сертификации**

центры сертификации, которым доверяют изначально все, либо руководствуясь политикой предприятия, либо из-за предустановленных настроек хранилища сертификатов, и которые могут находиться в начале пути доверия.

**Доверенные центры сертификации**

список центров сертификации, которым доверяют владельцы сертификатов. Чтобы сделать какой-либо центр доверенным, достаточно получить от него сертификат и внести его в список доверенных центров.