1. Какие задачи позволяет решать PKI.

**PKI (Public Key Infrastructure)**, или инфраструктура открытых ключей, – это система, которая позволяет использовать асимметричное шифрование и цифровые подписи на практике. Она включает в себя **выпуск, управление и хранение цифровых сертификатов**. Эти сертификаты, основанные на стандарте **X.509**, удостоверяют владение публичным ключом, связывая его с определенным лицом или организацией.

1. Основные компоненты PKI и их функции.

Основные компоненты PKI (Public Key Infrastructure) и их функции включают:

1. **Центр сертификации (CA)**:
   * Выдает цифровые сертификаты и управляет ими.
   * Проверяет идентичность организаций и пользователей перед выдачей сертификатов.
   * Участвует в процессе отзыва сертификатов.
2. **Центр регистрации (RA)**:
   * Проверяет запросы на получение сертификатов и аутентифицирует пользователей.
   * Передает запросы на сертификаты в CA для их выдачи.
   * Может управлять процессами регистрации и обновления сертификатов.
3. **Цифровые сертификаты**:
   * Содержат информацию о ключах, идентификаторе владельца и CA, который их выдал.
   * Используются для аутентификации и шифрования данных.
4. **Ключи (открытые и закрытые)**:
   * Открытые ключи используются для шифрования данных и проверки цифровых подписей.
   * Закрытые ключи хранятся в секрете и используются для дешифрования данных и создания подписей.
5. **Системы управления сертификатами**:
   * Обеспечивают автоматизацию процессов выдачи, обновления и отзыва сертификатов.
   * Поддерживают базы данных для хранения информации о сертификатах.
6. **Списки отозванных сертификатов (CRL)**:
   * Содержат информацию о сертификатах, которые были отозваны до истечения срока их действия.
   * Позволяют проверять актуальность сертификатов.
7. **Протоколы и стандарты**:
   * Определяют правила и процедуры для взаимодействия между компонентами PKI.
   * Включают такие протоколы, как X.509 для сертификатов и OCSP (Online Certificate Status Protocol) для проверки статуса сертификатов.

Эти компоненты работают совместно, обеспечивая безопасность и доверие в цифровых взаимодействиях.

1. Что такое – электронная цифровая подпись?

**Электронная подпись** – это способ использования вашего уникального приватного ключа для подтверждения вашей идентичности и гарантии неизменности отправленных данных. Это как цифровой аналог вашей рукописной подписи на документе, но с дополнительными преимуществами безопасности. Имеет следующие ключевые характеристики:

1. **Подтверждение подлинности**: ЭЦП позволяет удостовериться, что документ или сообщение подписаны конкретным пользователем. Это достигается с помощью закрытого ключа, который известен только подписчику.
2. **Целостность данных**: С помощью ЭЦП можно проверить, что содержимое документа не было изменено после его подписания. Если данные были изменены, подпись станет недействительной.
3. **Неотказуемость**: Подписав документ, автор не может впоследствии отрицать свою подпись, так как для её создания использовался его уникальный закрытый ключ.
4. **Использование криптографии**: ЭЦП основана на асимметричной криптографии, где используются пара ключей: открытый (для проверки подписи) и закрытый (для её создания).
5. **Широкое применение**: ЭЦП используется в различных сферах, включая электронный документооборот, онлайн-банкинг, подписание контрактов и заявок.

Электронная цифровая подпись обеспечивает безопасность и доверие в электронных взаимодействиях, позволяя избежать подделок и манипуляций с данными.

1. Что включает в себя сертификат?

Содержит публичный ключ и информацию о владельце ключа, а также подпись ЦС, подтверждающую подлинность данных.

Вот основные элементы, входящие в состав сертификата:

1. **Субъект (Subject)**:
   * Идентификация владельца сертификата (например, имя, организация, адрес).
2. **Открытый ключ (Public Key)**:
   * Открытый ключ, который используется для шифрования данных и проверки подписи.
3. **Центр сертификации (Issuer)**:
   * Название центра сертификации, который выдал сертификат. Это обеспечивает доверие к сертификату.
4. **Срок действия (Validity Period)**:
   * Дата начала и окончания действия сертификата. После окончания срока сертификат становится недействительным.
5. **Идентификатор сертификата (Serial Number)**:
   * Уникальный номер, присвоенный сертификату для его идентификации.
6. **Алгоритм подписи (Signature Algorithm)**:
   * Метод, используемый для создания подписи, например, SHA-256 с RSA.
7. **Цифровая подпись (Digital Signature)**:
   * Подпись центра сертификации, подтверждающая подлинность сертификата и его содержимого.
8. **Расширения (Extensions)** (опционально):
   * Дополнительная информация, которая может включать такие данные, как ограничения на использование сертификата (например, для шифрования или подписи), указания на допустимые альтернативные имена и другие параметры.

Эти элементы вместе обеспечивают целостность, подлинность и доверие к сертификату, позволяя использовать его для безопасных коммуникаций и аутентификации в цифровом мире.

1. Основное назначение сертификата открытого ключа?

Основное назначение сертификата открытого ключа заключается в обеспечении доверия к открытому ключу, который используется в криптографических операциях. Вот основные функции:

1. **Аутентификация**: Сертификат подтверждает, что открытый ключ принадлежит конкретному субъекту (пользователю, организации или устройству), что позволяет избежать подделок.
2. **Шифрование**: Сертификаты открытых ключей используются для шифрования данных, гарантируя, что только владелец соответствующего закрытого ключа сможет расшифровать эти данные.
3. **Целостность данных**: Использование сертификатов помогает убедиться, что данные не были изменены в процессе передачи, что особенно важно для электронных подписей и транзакций.
4. **Управление идентификацией**: Сертификаты служат важным элементом в системах управления идентификацией, позволяя централизованно управлять пользователями и их доступом к ресурсам.

Таким образом, сертификат открытого ключа является критически важным инструментом для обеспечения безопасности и доверия в цифровых взаимодействиях.