Содержание:

Введение

Цифровая подпись – это математический алгоритм, обычно используемый для проверки подлинности и целостности сообщения (например, электронной почты, транзакции по кредитной карте или цифрового документа). Цифровые подписи создают виртуальный отпечаток пальца, который является уникальным для физического или юридического лица и используется для идентификации пользователей и защиты информации в цифровых сообщениях или документах. В электронных письмах содержимое электронной почты само становится частью цифровой подписи. Цифровые подписи значительно более безопасны, чем другие формы электронных подписей.

Причины использования цифровой подписи

Цифровые подписи повышают прозрачность онлайн-взаимодействия и развивают доверие между клиентами, деловыми партнерами и поставщиками.

Работа цифровой подписи

Цифровые подписи работают с помощью следующих функций:

- **Хэш** – функция (также называемая “хэш”)-это строка чисел и букв фиксированной длины, генерируемая математическим алгоритмом и файлом произвольного размера, таким как электронная почта, документ, изображение или другой тип данных. Эта сгенерированная строка уникальна для хэшируемого файла и является односторонней функцией-вычисленный хэш не может быть обращен вспять, чтобы найти другие файлы, которые могут генерировать то же самое хэш-значение. Некоторые из наиболее популярных алгоритмов хеширования, используемых сегодня, являются Secure Hash Algorithm-1 (SHA-1), семейство Secure Hashing Algorithm-2 (SHA-2 и SHA-256) и

Message Digest 5 (MD5).

- **Криптография** с открытым ключом – Криптография с открытым ключом (также известная как асимметричное шифрование) - это криптографический метод, использующий систему пар ключей. Один ключ, называемый открытым ключом, шифрует данные. Другой ключ, называемый закрытым ключом, расшифровывает данные. Криптография с открытым ключом может использоваться несколькими способами для обеспечения конфиденциальности, целостности и подлинности. Криптография с открытым ключом может
    - Обеспечьте целостность, создав цифровую подпись сообщения с использованием закрытого ключа отправителя. Это делается путем хэширования сообщения и шифрования хэш-значения их закрытым ключом. Таким образом, любые изменения в сообщении приведут к другому хэш-значению.
    - Обеспечьте конфиденциальность, зашифровав все сообщение открытым ключом получателя. Это означает, что только получатель, обладающий соответствующим закрытым ключом, может прочитать сообщение.
    - Проверьте личность пользователя с помощью открытого ключа и сверьте его с центром сертификации.
- **Инфраструктура открытых ключей (PKI)** – PKI состоит из политик, стандартов, людей и систем, которые поддерживают распространение открытых ключей и проверку подлинности физических или юридических лиц с цифровыми сертификатами и центром сертификации.
- **Центр сертификации (CA)** – ЦС-это доверенная третья сторона, которая проверяет личность человека и либо генерирует пару открытых/закрытых ключей от его имени, либо связывает существующий открытый ключ, предоставленный этим человеком этому человеку. Как только центр сертификации проверяет чью-либо личность, он выдает цифровой сертификат, который имеет цифровую подпись центра сертификации. Затем цифровой сертификат может быть использован для проверки лица, связанного с открытым ключом, по запросу.
- **Цифровые сертификаты** – цифровые сертификаты аналогичны водительским удостоверениям в том, что их целью является идентификация владельца сертификата. Цифровые сертификаты содержат открытый ключ физического лица или организации и имеют цифровую подпись центра сертификации. В сертификат также может быть включена другая информация об организации, физическом лице и ЦС.

- **Конфиденциальность (PGP)/OpenPGP** – PGP/OpenPGP является альтернативой PKI. С PGP/OpenPGP пользователи «доверяют» другим пользователям, подписывая сертификаты людей с проверяемыми удостоверениями. Чем более взаимосвязаны эти подписи, тем выше вероятность верификации конкретного пользователя в интернете. Эта концепция называется «паутиной доверия»

Цифровые подписи работают, доказывая, что цифровое сообщение или документ не были изменены намеренно или непреднамеренно с момента его подписания. Цифровые подписи делают это, генерируя уникальный хэш сообщения или документа и шифруя его с помощью закрытого ключа отправителя. Созданный хэш является уникальным для сообщения или документа, и изменение любой его части полностью изменит хэш.

После завершения работы сообщение или цифровой документ подписывается цифровой подписью и отправляется получателю. Затем получатель генерирует свой собственный хэш сообщения или цифрового документа и расшифровывает хэш отправителя (включенный в исходное сообщение) с помощью открытого ключа отправителя. Получатель сравнивает созданный им хэш с расшифрованным хэшем отправителя; если они совпадают, сообщение или цифровой документ не были изменены, и отправитель аутентифицируется.

Заключение

Использование цифровых подписей в сочетании с PKI или PGP укрепляет их и уменьшает возможные проблемы безопасности, связанные с передачей открытых ключей, путем проверки того, что ключ принадлежит отправителю, и проверки личности отправителя. Безопасность цифровой подписи почти полностью зависит от того, насколько хорошо защищен закрытый ключ. Без PGP или PKI доказать чью-либо личность или отозвать скомпрометированный ключ невозможно; это может позволить злоумышленникам выдавать себя за кого-либо без какого-либо метода подтверждения.

Благодаря использованию доверенной третьей стороны цифровые подписи могут использоваться для идентификации и проверки отдельных лиц и обеспечения целостности сообщения.

Поскольку безбумажные онлайн-взаимодействия используются все шире, цифровые подписи могут помочь вам обезопасить и защитить целостность ваших данных. Понимая и используя цифровые подписи, вы можете лучше защитить свою информацию, документы и транзакции.