

image not found or type unknown



Электронная подпись - это схема, ее используют для отображения подлинности электронных сообщений либо документов. Цифровая подпись предоставляет все для получателя полагать, что сообщение было создано с помощью известного отправителя, что оно действительно отправлено (аутентификация и безотказность), а также то, что письмо не изменили в процессе передачи (целостность). Отвечая на вопрос: «ЭЦП – что это такое?» - стоит отметить, что цифровые подписи являются стандартным элементом большинства криптографических наборов протоколов и обычно используются для распространения ПО, совершения финансовых операций, а также во многих иных случаях, когда это важно для определения подделки или фальсификации.

Цифровые подписи применяются для реализации электронных подписей. Но не каждая подпись является цифровой. подписи используют асимметричную криптографию. Цифровые подписи предоставляют нам проверку и безопасность для сообщений, которые были отправлены по незащищенному каналу. Подпись помогает нам понять, что сообщение было отправлено с помощью заявленного отправителя.

Также я хочу отметить, что ЭЦП могут также реализовать принцип безотказности. Это значит, что подписчик не может утверждать, что он не подписывал сообщение. Некоторые схемы предлагают временную метку для цифровой подписи и даже если закрытый ключ подвергается воздействию, подпись остается действительной. Исходя из своего изучения могу сказать следующее: ЭЦП могут быть в виде битовой строки и могут быть применены в электронной почте, контрактах или сообщении, отправленном с помощью какого-либо криптографического протокола.