

image not found or type unknown



Электронная цифровая подпись (ЭЦП) сейчас на слуху. Многие современные компании переходят на электронный документооборот. Да и в повседневной жизни, вы, наверняка, сталкивались с этим. Если в двух словах, суть ЭЦП очень проста: есть удостоверяющий центр, есть генератор ключей, еще немного магии, и вуаля — все документы подписаны. Осталось разобраться, что же за магия позволяет цифровой подписи работать.

Если вспомнить формальное определение, то ЭЦП — это реквизит электронного документа. Другими словами, последовательность битов, вычисленная уникально для каждого конкретного сообщения. Подпись может быть вычислена, как с применением секретного ключа, так и без него. Без секретного ключа подпись представляет собой просто код, который может доказать, что документ не был изменен. С использованием секретного ключа подпись докажет целостность сообщения, позволит убедиться в его подлинности и аутентифицировать источник.

С использованием ЭЦП увеличиваются возможности электронного документооборота.