Электронная цифровая подпись является реквизитом документа, с помощью которого можно установить, произошло ли искажение информации, содержащейся в электронном документе, с момента факта формирования подписи, а также позволяет подтвердить принадлежность того или иного документа владельцу.

Технология электронной подписи реализуется на связке открытого и закрытого ключа.

Открытый ключ – известен всем пользователям системы и необходим для проверки электронной подписи. С его помощью получатель документа устанавливает авторство документа и неизменность документа после подписания.

Закрытый ключ – уникальная последовательность символов, с помощью которой формируется каждая электронная подпись. Закрытый ключ хранится на ключевом носителе (токене) и защищен паролем, который известен только владельцу.

По моему мнению, оба вида этих ключей имеют свои преимущества и недостатки, однако я считаю, что закрытый ключ всё же является менее надёжным.

Основное назначение закрытого ключа – само создание электронной подписи. Он является конфиденциальной частью пары и не сообщается никому. Именно поэтому он гораздо более уязвим в сравнении с открытым ключом: взломав носитель, злоумышленник имеет возможность подписать любой документ вашей подписью, и доказать свою непричастность будет крайне сложно. Кроме того, в соответствии с положениями закона 63-ФЗ, ответственность за сохранение носителя ключа ЭЦП лежит на его владельце. В том случае, если вы потеряли носитель или заметили следы взлома, сертификат рекомендуется отозвать.