«Реализация юридически значимого документооборота с применением средств электронной цифровой подписи»

ТОО НИЛ «ГАММА ТЕХНОЛОГИИ»
2009 год

Электронная Цифровая Подпись (ЭЦП) – это аналог собственноручной подписи

Подпись – это рукописное и иногда стилизованное графически имя или другой графический знак под документом, идентифицирующий подписанта и означающий его согласие с текстом документа. Проверяется обычная подпись визуально (сличаем оригинал с подписью поставленной на документе).

В мире электронных документов подписание документа с помощью графических символов теряет смысл, т.к. подделать и скопировать графический символ можно бесконечное количество раз. ЭЦП является полным электронным аналогом обычной подписи на бумаге, но реализуется не с помощью графических изображений, а с помощью математических преобразований над содержимым документа.

Очевидные преимущества ЭЦП

- Особенности математического алгоритма создания и проверки ЭЦП гарантируют невозможность подделки такой подписи посторонними лицами (неопровержимость авторства). Надежность и удобство использования ЭЦП не вызывает сомнений.
  Процедура проверки ЭЦП выполняется компьютером безошибочно, что позволяет избежать человеческого фактора, при проверке обычной подписи.

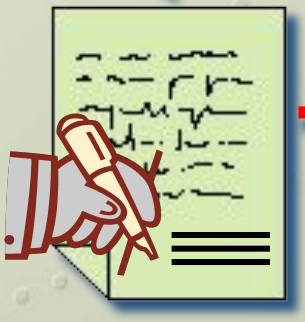
- ЭЦП дает информацию не только о лице, подписавшем документ, но и позволяет удостовериться, что сам документ не был изменен или подделан после подписания (аутентичность и целостность документа). Удобство в обмене, хранении и работе с электронными документами, имеющими юридическую силу.

Защищенность обычного документа

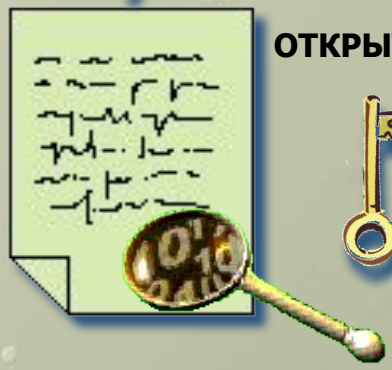
Схема формирования и проверки ЭЦП

ЭЦП

H5KL5R853N485J6RTU
8FN55MTM654676M443
734GJ56U67N567N67N
67474



СЕКРЕТНЫЙ



ОТКРЫТЫЙ

Сфера применения ЭЦП

Электронная цифровая подпись может применяться в разных областях:

- ЭЦП используется, как ответственная подпись на электронном документе – то есть в качестве аналога собственноручной подписи и/или печати на бумажном документе. Именно в этой ипостаси ЭЦП используется в системах электронного документооборота, в частности Государственных органов (ЕСЕДО).
- ЭЦП – это надежный инструмент, который позволяет установить авторство и подтвердить целостность любых данных в электронном виде. Например, полученное вами от руководителя письмо без ЭЦП, может оказаться на самом деле поддельным или содержать искаженную после его отправления информацию. Использование ЭЦП такую возможность исключает. При проверке ЭЦП будет установлено, что документ был изменен после его подписания.

Сфера применения ЭЦП

Электронная цифровая подпись может применяться в разных областях:

- ЭЦП может быть использована как ответственная подпись на электронном документе – то есть в качестве аналога собственноручной подписи и/или печати на бумажном документе. В частности, именно в этой ипостаси ЭЦП используется в системах электронного документооборота, в частности Государственных органов (ЕСЕДО).
- ЭЦП – это надежный инструмент, который позволяет установить авторство и подтвердить целостность любых данных в электронном виде. Например, полученное вами от руководителя письмо без ЭЦП, может оказаться на самом деле поддельным или содержать искаженную после его отправления информацию. Использование ЭЦП такую возможность исключает. При проверке ЭЦП будет установлено, что документ был изменен после его подписания.

Что нужно сделать для использования ЭЦП?

Перед тем как практически начать применять ЭЦП в своей работе, надо создать файлы сертификата и закрытого ключа. Сертификат будет использоваться для проверки подлинности данных подписанных ЭЦП любым человеком, использующим эти данные. А закрытый ключ нужен человеку для формирования ЭЦП подписываемых им данных.

Для того чтобы создать и в дальнейшем использовать сертификат, которому будут доверять все, кто будет проверять подлинность ЭЦП, нужна организация, которая обеспечит нормативную, организационную и правовую основу использования выпущенных ею сертификатов. Такой организацией является Национальный Удостоверяющий Центр (или АО НИТ с НУЦ).

Что нужно сделать для использования ЭЦП?

Создание закрытого ключа и получение сертификата:

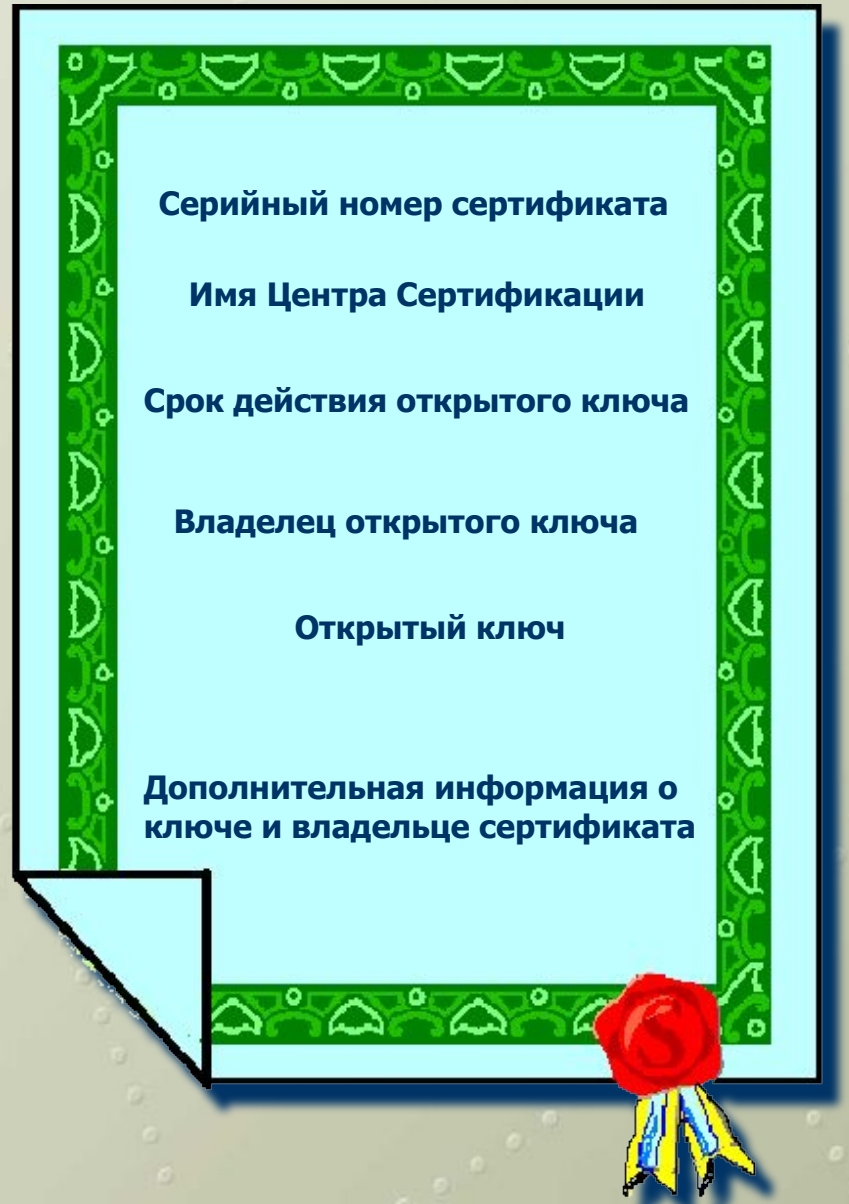
Ключи должны создаваться только на рабочем месте пользователя, а открытая часть ключа пересылаться в Удостоверяющий центр для последующего изготовления сертификата и получения его по e-mail.

Для того, чтобы никто, кроме владельца подписи, не мог воспользоваться закрытым ключом, его обычно записывают на съемный носитель. Данные устройства, также как банковские карточки, для дополнительной защиты снабжают PIN кодом. И точно также как при операциях с картой, перед тем как воспользоваться ключом для создания ЭЦП надо ввести правильное значение PIN кода.

Именно надежное сохранение пользователем своего закрытого ключа гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего документ подписанта.

Что нужно сделать для использования ЭЦП?

Сертификат содержит всю необходимую информацию для проверки ЭЦП. Данные сертификата открыты и публичны. Поэтому обычно сертификаты хранятся в хранилище операционной системы (в каждом компьютере, в общем сетевом хранилище, в базе данных и т.п.).


Серийный номер сертификата
Имя Центра Сертификации
Срок действия открытого ключа
Владелец открытого ключа
Открытый ключ
Дополнительная информация о ключе и владельце сертификата

Что нужно сделать для использования ЭЦП?

Все сертификаты всегда хранятся и в Национальном Удостоверяющем центре, точно так же, как и нотариус хранит всю необходимую информацию о человеке, выполнившем у него нотариальное действие.

ГЛОБАЛЬНОЕ ХРАНИЛИЩЕ

ЦЕНТР СЕРТИФИКАЦИИ

Криптопровайдер – основа безопасности

Создание ЭЦП представляет собой сложную математическую процедуру и ее выполняют специальные программы – криптопровайдеры. В современных операционных системах криптопровайдеры уже включены в их состав.

Однако в нашем случае законодательство требует применение сертифицированных государственными органами криптопровайдеров. В этом случае их придется покупать и устанавливать на всех машинах, на которых будут подписываться или проверяться ЭЦП. Создание же ключей и получение сертификатов будет возможно только после установки соответствующих криптопровайдеров, так как они будут использоваться в процессе создания ключей и дальнейших процессов формирования и проверки ЭЦП.

Криптопровайдер – Tumar CSP

Криптографический комплекс TUMAR CSP – набор механизмов для проведения полного комплекса мероприятий по защите информации при ее хранении, обработке и передаче по каналам связи

TUMAR CSP – сертифицирован на соответствие требованиям безопасности (качества) по всем 4 уровням, установленным в «СТ РК 1073 – 2002. Средства криптографической защиты информации»

TUMAR CSP - сертифицированное Microsoft программное средство защиты информации. TUMAR CSP реализует казахстанские криптографические алгоритмы и разработан в соответствии с криптографическим интерфейсом компании Microsoft - Cryptographic Service Provider (CSP)

Программно аппаратный комплекс CERTEX HSM

Программно-аппаратный комплекс CERTEX HSM предназначен для защиты секретных криптографических ключей и выполнения криптографической обработки данных
Устройство обеспечивает выполнение следующих криптографических функций:
генерация криптографических ключей;
шифрование/расшифровывание данных;
вычисление и проверка электронной цифровой подписи (ЭЦП);
вычисление значения хэш-функции (вычисление контрольной суммы).

АПК CERTEX HSM – сертифицирован на соответствие требованиям безопасности (качества) по 2 и 3 уровню безопасности, установленному в
«СТ РК 1073 – 2007(2002). Средства криптографической защиты информации»

Программно-аппаратный комплекс CERTEX HSM

Программно-аппаратный комплекс CERTEX HSM предназначен для защиты секретных криптографических ключей и выполнения криптографической обработки данных

Устройство обеспечивает выполнение следующих криптографических функций:

- генерация криптографических ключей;
- шифрование/расшифровывание данных;
- вычисление и проверка электронной цифровой подписи (ЭЦП);
- вычисление значения хэш-функции (вычисление контрольной суммы).

АПК CERTEX HSM – сертифицирован на соответствие требованиям безопасности (качества) по 2 и 3 уровню безопасности, установленному в «СТ РК 1073 – 2002. Средства криптографической защиты информации» «СТ РК 1073 – 2007. Средства криптографической защиты информации»

Программно-аппаратный комплекс CERTEX HSM

Программно-аппаратный комплекс CERTEX HSM предназначен для защиты секретных криптографических ключей и выполнения криптографической обработки данных

Устройство обеспечивает выполнение следующих криптографических функций:

- генерация криптографических ключей;
- шифрование/расшифровывание данных;
- вычисление и проверка электронной цифровой подписи (ЭЦП);
- вычисление значения хэш-функции (вычисление контрольной суммы).

АПК CERTEX HSM – сертифицирован на соответствие требованиям безопасности (качества) по 2 и 3 уровню безопасности, установленному в «СТ РК 1073 – 2002. Средства криптографической защиты информации» «СТ РК 1073 – 2007. Средства криптографической защиты информации»

Gamma technologies