ХАРАКТЕРИСТИКА СЕРТИФІКАТІВ ЕВРОСТАНДАРТУ ТА СТАНДАРТУ СЕРТИФІКАТА X509

Фоков В. И.
Науковий керівник — Вінокурова О.А.
Харківський національний університет радіоелектроніки
(61166, Харків, пр. Леніна, 14. каф. БІТ, тел. (057) 702-14-25)

Electronic digital signature can be used by any person as the hand made signature to make electronic document Law powerful . The law power of electronic document signed by Electronic digital signature is the same as the signature on the paper, signed by hand law active person or make a stamp on it.

Електронно цифровий підпис може бути використаний юридичними так і фізичними особами як аналог власноручного підпису для придання

електронному документу юридичної сили. Юридична сила електронного документа, підписаного ЕЦП, еквівалентна юридичній силі документа на паперовому носії, підписаного власноручним підписом право здібної особи та підкріпленого печаттю.

Видавець сертифікатів привласнює кожному сертифікату, що випускається, серійний номер Certificate Serial Number, який має бути унікальний. Комбінація імені видавця і серійного номера однозначно ідентифікує кожен сертифікат.

У полі Signature Algorithm Identifier вказується ідентифікатор алгоритму ЕЦП, який використовувався видавцем сертифікату для підпису сертифікату, наприклад ГОСТ Р 34.10-94


Имя пользователя: C = RU, org = ACME, cn = UserName
Имя издателя: C = RU, org = ACME
Номер сертификата: #12345678
Открытый ключ пользователя:
Алгоритм: GOST open key
Значение ключа: 01001110100100101000000 1
Сертификат действует с: 01.01.2006 00:00:00
Сертификат действует до: 31.12.2008 23:59:59
Дополнительная информация (X.509 v3 Extensions)
Регламент использования сертификата: Только для платежей
Секретный ключ действует с: 31.12.2006 23:59:59
Секретный ключ действует до: 31.12.2007 23:59:59
Область применения ключа: Идентификатор 1
Область применения ключа: Идентификатор i
Область применения ключа: Идентификатор N
Права и полномочия: Администратор
Атрибуты пользователя: IP, DNS, URI, RFC822, Номер счета, Адрес
...
Подпись Удостоверяющего Центра:
Алгоритм: GOST P 34.10-94 sign algorithm
Значение: 01001110100100101000000 1

У докладі буде сформульована характеристика Держ. стандарту Х509 та формат сертифіката євростандарту.