**Керування статусами сертифікатів, інфраструктура керування привілеями**

*- Керування статусами сертифікатів*

Статус сертифіката (діє / не діє) (булева змінна) не зберігається всередені.

Питання: де його зберігати?  
1) Не зберігаємо взагалі.

2) Використовувати короткі терміни дії.

3) Статуси зберігаються зовні.

Коли не потрібно збарігати статуси?

1) Короткі терміни дії.

2) Конфігурація «зірка».

*- Інфраструктура керування привілеями (PMI – Privilege Management Infrastructure)*

Нова довірена сторона: Атрибутний центр (AA - Attribute Authority).

PMI – надбудова над PKI (Public Key Infrastructure).

Повноваження – у атрибутних сертифікатах.

Атрибутні сертифікати прив’язані до сертифікатів відкритих ключів.

Атрибутні сертифікати вмирають швидко.

Використання:

- інтернет-протоколи;

- динамічне керування доступом;

- grid-системи.

- ... .

Зауваження: Для підвищення безпеки рекомендовано розносити СА (Центр сертифікації ключів) та АА.

Сертифікат ключа === паспорт

Атрибутний сертифікат === віза

Міжнародні стандарти: XS09, ISO 9594-8 2009, RFC 5755

***Attribute Cert Info*** = SEQ {

Version: INTEGER OPT, //V.2

holder: Holder, //owner

issuer: [0] V2Form,

signal: AlgId,

serial Number: INTEGER,

aCValidity: SEQ {

not Before

GeneralizedTime

not After

}

Attributes: Attributes,

issuerUniqueId: OCTET STRING OPT,

extensions: Extensions

*Holder* = SEQ {

baseCertId: [0] IsuerSerial OPT,

entityName: [1] GeneralNames OPT,

objectDigest: [2] ObjectDigestInfo OPT

}

*IssuerSireal* = SEQ {  
 issuer: GeneralNames,

serial: INTEGER,

issuerUniqueId: OCTET STRING OPT  
}

*ObjectDigestInfo* = SEQ {  
 objectType: ENUMERATED, // 0 – public key(subject PK), 1 – holder cert, 2 – «інше»   
 otherType: OID OPT,

digestAlg: AlgId,

digest: BIT STRING  
}

*V2Form* = SEQ {  
 issuerName: GeneralNames OPT,

baseCertId: [0] IssuerSerial OPT,

objectDigest: [1] ObjectDigestInfo OPT  
}

Особливості АА та його ключа:

1) сертифікат ключа – за X.509v3.

2) не використовується для перевірки підписів.

3) АА !== СА => Basic Constraints is CA = false

4) не допускаються жодних ланцюгів довіри.