# X.509 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ВЗАЄМОЗВ'ЯЗОК ВІДКРИТИХ СИСТЕМ КАТАЛОГ: ОСНОВНІ ПОЛОЖЕННЯ СЕРТИФІКАЦІЇ ВІДКРИТОГО КЛЮЧА ТА СЕРТИФІКАЦІЇ АТРИБУТІВ

# ОСНОВИ ДЛЯ ВИКОРИСТАННЯ КАТАЛОГОМ ТАКИХ ЗАСОБІВ

- Технологія відкритого ключа, що включає сертифікати відкритого ключа, використовується Каталогом для виконання суворої автентификації, операцій підпису та/або зашифровування і для збереження підписаних та/або зашифрованих даних у Каталозі.

- Сертифікати атрибутів можуть використовуватися Каталогом для здійснення управління доступом на базі правил.

# ФУНКЦІЇ СТАНДАРТУ X.509

- визначає форму подання інформації автентифікації, яка зберігається Каталогом;
- описує, як інформація автентифікації може бути отримана з Каталогу;
- встановлює припущення, які зроблено щодо способу формування та розміщення інформації автентифікації у Каталозі;
- визначає три способи використання додатками такої інформації автентифікації для виконання автентифікації та описує, як шляхом автентифікації можуть підтримуватися інші послуги захисту.

# ДОДАТКИ X.509

- У **Додатку А** надається модуль ASN.1, який містить всі визначення, пов'язані з основними положеннями.
- У **Додатку Б** надаються правила генерації та обробки списків скасування сертифікатів (ССС).
- У **Додатку В** надаються приклади випуску дельта-ССС.
- У **Додатку Г** надаються приклади синтаксисів політики застосування повноважень та атрибутів повноважень.
- **Додаток Д** є введенням у криптографію відкритого ключа.
- **Додаток Е** визначає ідентифікатори об’єктів, які присвоюються алгоритмам автентификації та шифрування, за відсутністю формального реєстру.
- **Додаток Ж** містить приклади використання обмежень на шляхи сертифікації.
- **Додаток З** містить упорядкований за алфавітом список визначень інформаційних елементів у цій Специфікації.

# ВИЗНАЧЕННЯ

- **Сертифікат атрибутів** Структура даних, підписана цифровим способом уповноваженим з атрибутів, що пов'язує деякі значення атрибутів з інформацією ідентифікації утримувача атрибутів.
- **Базовий ССС .** ССС, що використовується як основа при формуванні дельта-ССС.
- **Список скасування сертифікатів (ССС).** Підписаний список, що визначає набір сертифікатів, які емітентом в подальшому не вважаються чинними. В доповнення, до звичайних ССС, визначені деякі спеціальні типи ССС, які охоплюють конкретні галузі.
- **Дельта-ССС.** Частковий список скасування, що містить тільки перелік сертифікатів, статус скасування яких було змінено з моменту випуску базового ССС, на який посилається цей частковий список.
- **Повний ССС.** Повний список скасування для заданої області дії, що містить перелік всіх сертифікатів, які були скасовані.
- **Непрямий ССС.** Список скасування, що містить, принаймні, перелік сертифікатів, що випущені іншими уповноваженими органами, ніж той хто випустив цей ССС.
- **Інфраструктура управління повноваженнями (ІУП).** Інфраструктура, яка у взаємодії з інфраструктурою відкритого ключа, здатна забезпечувати управління повноваженнями для підтримки послуги авторизації.
- **Сертифікат відкритого ключа.** Структура даних, що містить відкритий ключ користувача та деяку іншу інформацією, на яку накладено цифровий підпис за допомогою особистого ключа уповноваженого на сертифікацію, що випустив цей сертифікат відкритого ключа.
- **Інфраструктура відкритого ключа (ІВК).** Інфраструктура, що здійснює управління відкритими ключами, з метою надання послуг цілісності, справжності (автентифікації), неспростовності та конфіденційності.

# ПЕРЕВІРКА ЧИННОСТІ СВК ВКЛЮЧАЄ:

- встановлення довіреного шляху сертифікації між користувачем сертифіката та суб'єктом сертифіката;
- перевірку цифрових підписів на кожному сертифікаті на шляху сертифікації;
- перевірку чинності всіх сертифікатів на такому шляху.

# ПЕРЕВІРКА ЧИННОСТІ СЕРТИФІКАТУ АТРИБУТІВ ВКЛЮЧАЄ:

- гарантію того, що повноважень у сертифікаті у порівнянні з політикою застосування повноважень достатньо;
- встановлення за необхідністю довіреного шляху делегування;
- перевірку цифрового підпису на кожному сертифікаті на шляху делегування;
- гарантію того, що кожний емітент санкціонований для делегування  повноважень;
- перевірку того, що у сертифікатів не минув строк чинності або, що вони не були скасовані емітентами.

# ВЛАСТИВОСТІ СЕРТИФІКАТУ

- будь-який користувач, що має доступ до відкритого ключа уповноваженого на сертифікацію може відновити відкритий ключ, який був сертифікований;

- жодна сторона, крім уповноваженого на сертифікацію, не може з наперед заданою ймовірністю змінювати сертифікат без наступного виявлення цієї зміни.

# СТРУКТУРА СЕРТИФІКАТУ

**CA<<A>> = CA{V,SN,AI,CA,UCA,A,UA,Ap,TA},**

- V – версія сертифіката,
- SN – реєстраційний номер сертифіката,
- AI – ідентифікатор алгоритму, який використовувався для підписання сертифіката,
- UCA – довільний унікальний ідентифікатор CA,
- UA – довільний унікальний ідентифікатор користувача,
- Ap – відкритий ключ користувача A,
- TA – зазначає строк чинності сертифіката та складається із двох дат, першої та останньої, за якими визначається строк чинності сертифіката.

# СТРУКТУРА СЕРТИФІКАТУ У НОТАЦІЇ ASN.1

- **Certificate ::= SIGNED { SEQUENCE {**
- **version [0] Version DEFAULT v1,**
- **serialNumber CertificateSerialNumber,**
- **signature AlgorithmIdentifier,**
- **issuer Name,**
- **validity Validity,**
- **subject Name,**
- **subjectPublicKeyInfo SubjectPublicKeyInfo,**
- **issuerUniqueIdentifier [1] IMPLICIT UniqueIdentifier OPTIONAL,**
- *-- якщо присутній, то має використовуватися v2 або v3*
- **subjectUniqueIdentifier [2] IMPLICIT UniqueIdentifier OPTIONAL,**
- *-- якщо присутній, то має використовуватися v2 або v3*
- **extensions [3] Extensions OPTIONAL**
- *-- якщо присутній, то має використовуватися v3 --*

# ТИПИ СЕРТИФІКАТІВ ВІДКРИТОГО КЛЮЧА

Сертифікат кінцевого об'єкта – це сертифікат, випущений УС для суб'єкта, що не є емітентом інших сертифікатів відкритого ключа.

Сертифікат уповноваженого на сертифікацію – це сертифікат, випущений уповноваженим на сертифікацію для суб'єкта, що сам є уповноваженим на сертифікацію і тому спроможний випускати сертифікати відкритого ключа.

# ТИПИ СЕРТИФІКАТІВ УС

- **САМОВИПУЩЕНИЙ СЕРТИФІКАТ** - це сертифікат, в якому емітент і суб'єкт є тим самим УС. УС може використовувати самовипущені сертифікати, наприклад, під час операції зміни старих ключів на нові;

- **САМОПІДПИСАНИЙ СЕРТИФІКАТ** - це окремий випадок самовипущених сертифікатів, коли особистий ключ, що використовується уповноваженим на сертифікацію для підписання сертифіката, відповідає відкритому ключу, сертифікованому у даному сертифікаті.

- **ПЕРЕХРЕСНИЙ СЕРТИФІКАТ** (крос-сертифікат) - це сертифікат, у якому емітент сертифіката та суб'єкт є різними уповноваженими на сертифікацію.

# СПИСКИ СКАСУВАННЯ

- список скасування сертифікатів;
- список скасування уповноважених органів;
- дельта-список скасування;
- список скасування сертифікатів атрибутів;
- список скасування уповноважених з атрибутів.

# СПИСКИ СКАСУВАННЯ В ASN.1:

- **CertificateList ::= SIGNED { SEQUENCE {**
- **version Version OPTIONAL,**
- *-- якщо присутній, то має використовуватися v2*
- **signature AlgorithmIdentifier,**
- **issuer Name,**
- **thisUpdate Time,**
- **nextUpdate Time OPTIONAL,**
- **revokedCertificates SEQUENCE OF SEQUENCE {**
- **serialNumber CertificateSerialNumber,**
- **revocationDate Time,**
- **crlEntryExtensions Extensions OPTIONAL } OPTIONAL,**
- **crlExtensions [0] Extensions OPTIONAL }}**

# РОЗШИРЕННЯ

1) *інформація про ключі та політику*: ці розширення сертифіката та ССС містять додаткову інформацію про використовувані ключі, включаючи ідентифікатори ключів для ключів суб'єкта та емітента, покажчики призначення або обмежень на використання ключів та покажчики політики застосування сертифікатів;

2) *атрибути суб'єкта та емітента*: ці розширення сертифіката та ССС підтримують альтернативні імена з різними формами імені, для суб'єкта сертифіката, емітента сертифіката, або емітента ССС. Ці розширення також можуть нести додаткову атрибутну інформацію про суб'єкта сертифіката, щоб дати можливість користувачу сертифіката переконатися в тому, що суб'єкт сертифіката є конкретною особою або об'єктом;

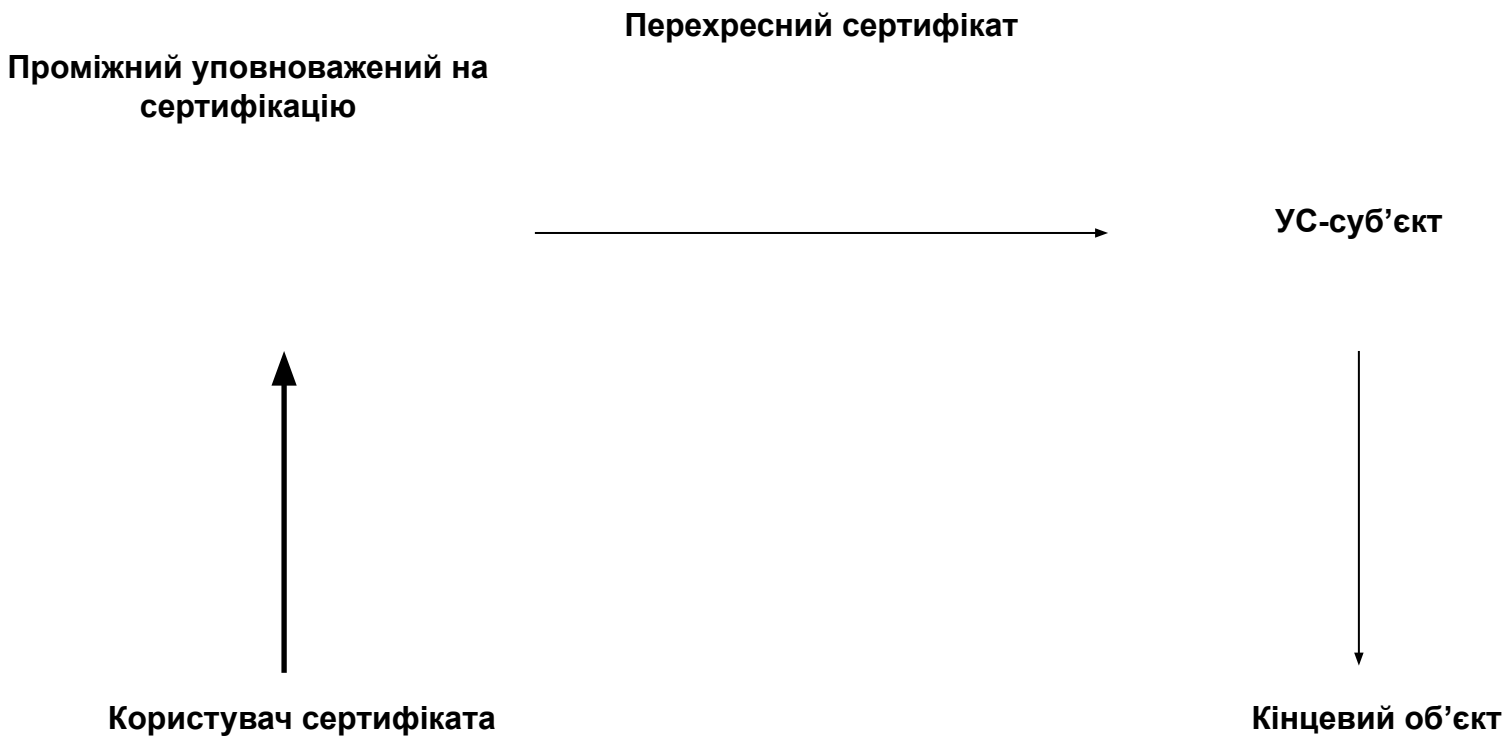
3) *обмеження шляху сертифікації*: ці розширення сертифіката дозволяють включити специфікації обмежень у сертифікати УС, (тобто сертифікати для уповноважених на сертифікацію, які були випущені іншими уповноваженими на сертифікацію) для полегшення автоматизованої обробки шляхів сертифікації, коли задіяна множина політик застосування сертифікатів.

# РОЗШИРЕННЯ

1) *базові розширення ССС*: ці розширення допускають включення в ССС покажчиків причини скасування, для тимчасового припинення дії сертифіката, та включення порядкових номерів випусків ССС;

2) *пункти розповсюдження ССС та дельта-ССС*: ці розширення сертифіката та ССС дозволяють розбивати повну множину інформації скасування від одного УС на окремі ССС та дозволяє поєднувати інформацію від множини УС в одному ССС.

# ПЕРЕХРЕСНА СЕРТИФІКАЦІЯ



# СИТУАЦІЇ, ЗА ЯКИХ УС МОЖЕ ВИПУСТИТИ СЕРТИФІКАТ САМОМУ СОБІ:

- як зручний спосіб кодування свого відкритого ключа для зв'язку зі своїми користувачами сертифікатів та збереження його ними;
- для сертифікації ключів, що використовуються не для підписання сертифіката та ССС (наприклад для позначки часу);
- для заміни своїх власних сертифікатів, у яких закінчився строк чинності.

# ВИМОГИ ДО РОЗШИРЕНЬ ДЛЯ ІНФОРМАЦІЇ ПРО КЛЮЧІ ТА ПОЛІТИКУ

- оновлення ключової пари УС може проводитися регулярно або в особливих випадках.
- звичайно суб'єкт сертифіката має різні відкриті ключі та, відповідно, різні сертифікати для різних цілей, наприклад, для цифрового підпису або узгодження ключів шифрування.
- оновлення ключової пари суб'єкта може проводитися регулярно або в особливих випадках.

# ВИМОГИ ДО РОЗШИРЕНЬ ДЛЯ ІНФОРМАЦІЇ ПРО КЛЮЧІ ТА ПОЛІТИКУ

- можливість зазначення строку використання особистого ключа в сертифікаті;
- має бути оговорена умова для включення інформації про політику застосування сертифікатів у сертифікати;
- відображення політики;
- користувач системи шифрування або цифрових підписів, що використовує сертифікати, повинен вміти заздалегідь визначати алгоритми, які підтримуються іншими користувачами.

# ПОЛЯ РОЗШИРЕННЯ ДЛЯ СВК ТА ССС

- ідентифікатор ключа уповноваженого органу;
- ідентифікатор ключа суб'єкта;
- використання ключа;
- розширене використання ключа;
- строк використання особистого ключа;
- політика застосування сертифіката;
- відображення політики.

# РОЗШИРЕННЯ „ІДЕНТИФІКАТОР КЛЮЧА УПОВНОВАЖЕНОГО ОРГАНУ”

(завжди некритичне )

- **authorityKeyIdentifier EXTENSION ::= {**
- **SYNTAX AuthorityKeyIdentifier**
- **IDENTIFIED BY id-ce-authorityKeyIdentifier }**
- **AuthorityKeyIdentifier ::= SEQUENCE {**
- **keyIdentifier [0] KeyIdentifier OPTIONAL,**
- **authorityCertIssuer [1] GeneralNames OPTIONAL,**
- **authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL }**
- **( WITH COMPONENTS {..., authorityCertIssuer PRESENT,**
- **authorityCertSerialNumber PRESENT} |**
- **WITH COMPONENTS {..., authorityCertIssuer ABSENT,**
- **authorityCertSerialNumber ABSENT} )**
- **KeyIdentifier ::= OCTET STRING**

# РОЗШИРЕННЯ „ІДЕНТИФІКАТОР КЛЮЧА СУБ'ЄКТА”

(завжди некритичне )

- **subjectKeyIdentifier EXTENSION ::= {**
- **SYNTAX S subjectKeyIdentifier**
- **IDENTIFIED BY id-ce subjectKeyIdentifier**

**}**

- **SubjectKeyIdentifier ::= KeyIdentifier**

# РОЗШИРЕННЯ „ВИКОРИСТАННЯ КЛЮЧА”
## (може бути критичним або некритичним)

- keyUsage EXTENSION ::= {
- SYNTAX KeyUsage
- IDENTIFIED BY id-ce-keyUsage }
- KeyUsage ::= BIT STRING {
- digitalSignature (0),
- nonRepudiation (1),
- keyEncipherment (2),
- dataEncipherment (3),
- keyAgreement (4),
- keyCertSign (5),
- cRLSign (6),
- encipherOnly (7),
- decipherOnly (8) }

# РОЗШИРЕННЯ „РОЗШИРЕНЕ ВИКОРИСТАННЯ КЛЮЧА”

(може бути критичним або некритичним)

- **extKeyUsage EXTENSION ::= {**
- **SYNTAX SEQUENCE SIZE (1..MAX) OF KeyPurposeId**
- **IDENTIFIED BY id-ce-extKeyUsage }**
- **KeyPurposeId ::= OBJECT IDENTIFIER**

# РОЗШИРЕННЯ „СТРОК ВИКОРИСТАННЯ ОСОБИСТОГО КЛЮЧА”

(некритичне)

- **privateKeyUsagePeriod EXTENSION ::= {**
- **SYNTAX PrivateKeyUsagePeriod**
- **IDENTIFIED BY id-ce-privateKeyUsagePeriod }**
- **PrivateKeyUsagePeriod ::= SEQUENCE {**
- **notBefore [0] GeneralizedTime OPTIONAL,**
- **notAfter [1] GeneralizedTime OPTIONAL }**
- **( WITH COMPONENTS {..., notBefore PRESENT} |**
- **WITH COMPONENTS {..., notAfter PRESENT} )**

# Розширення „Політика застосування сертифікатів”

(може бути критичним або некритичним)

- **certificatePolicies EXTENSION ::= {**
- **SYNTAX CertificatePoliciesSyntax**
- **IDENTIFIED BY id-ce-certificatePolicies }**
- **CertificatePoliciesSyntax ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation**
- **PolicyInformation ::= SEQUENCE {**
- **policyIdentifier CertPolicyId,**
- **policyQualifiers SEQUENCE SIZE (1..MAX) OF**
- **PolicyQualifierInfo OPTIONAL }**
- **CertPolicyId ::= OBJECT IDENTIFIER**
- **PolicyQualifierInfo ::= SEQUENCE {**
- **policyQualifierId CERT-POLICY-QUALIFIER.&id**
- **({SupportedPolicyQualifiers}),**
- **qualifier CERT-POLICY-QUALIFIER.&Qualifier**
- **({SupportedPolicyQualifiers}{@policyQualifierId})**
- **OPTIONAL }**
- **SupportedPolicyQualifiers CERT-POLICY-QUALIFIER ::= { ... }**

# РОЗШИРЕННЯ „ВІДОБРАЖЕННЯ ПОЛІТИКИ”

(може бути критичним або некритичним )

- **policyMappings EXTENSION ::= {**
- **SYNTAX PolicyMappingsSyntax**
- **IDENTIFIED BY id-ce-policyMappings }**
- **PolicyMappingsSyntax ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {**
- **issuerDomainPolicy CertPolicyId,**
- **subjectDomainPolicy CertPolicyId }**

# Вимоги, які пов'язані з атрибутами суб'єкта сертифіката та емітента сертифіката

- необхідно, щоб сертифікати могли використовуватися додатками, які використовують різноманітні форми імен, включаючи імена електронної пошти Internet, імена доменів Internet, адреси відправника/одержувача у форматі X.400 та імена EDI.

- користувач сертифіката може мати потребу в захищеному наданні певної ідентифікуючої інформації про суб'єкта, щоб бути впевненим у тому, що суб'єкт дійсно є очікуваною особою або об'єктом.

# ПОЛЯ РОЗШИРЕННЯ ДЛЯ СЕРТИФІКАТА ТА ССС

- альтернативне ім'я суб'єкта;
- альтернативне ім'я емітента;
- атрибути Каталогу суб'єкта.

# РОЗШИРЕННЯ „АЛЬТЕРНАТИВНЕ ІМ'Я СУБ'ЄКТА"

(може бути критичним або некритичним )

- **subjectAltName EXTENSION ::= {**
- **SYNTAX GeneralNames**
- **IDENTIFIED BY id-ce-subjectAltName }**
- **GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName**
- **GeneralName ::= CHOICE {**
- **otherName [0] INSTANCE OF OTHER-NAME,**
- **rfc822Name [1] IA5String,**
- **dNSName [2] IA5String,**
- **x400Address [3] ORAddress,**
- **directoryName [4] Name,**
- **ediPartyName [5] EDIPartyName,**
- **uniformResourceIdentifier [6] IA5String,**
- **iPAddress [7] OCTET STRING,**
- **registeredID [8] OBJECT IDENTIFIER }**
- **OTHER-NAME ::= TYPE-IDENTIFIER**
- **EDIPartyName ::= SEQUENCE {**
- **nameAssigner [0] DirectoryString {ub-name} OPTIONAL,**
- **partyName [1] DirectoryString {ub-name} }**

# РОЗШИРЕННЯ „АЛЬТЕРНАТИВНЕ ІМ’Я СУБ’ЄКТА”

- **otherName** – ім'я будь-якої форми, яке визначене як примірник класу інформаційного об'єкта **OTHER-NAME**;
- **rfc822Name** – адреса електронної пошти Internet, яка визначена згідно з Internet RFC 822;
- **dNSName** – ім'я домена Internet, яке визначене згідно з Internet RFC 1035;
- **x400Address** - адреса O/R, яка визначена згідно з ITU-T Rec. X.411 | ISO/IEC 10021-4;
- **directoryName** – ім'я Каталогу, яке визначене згідно з ITU-T Rec. X.501 | ISO/IEC 9594-2;
- **ediPartyName** – ім'я форми, погодженої між партнерами, що спілкуються, за обміном електронними даними; компонент **nameAssigner** ідентифікує уповноважений орган, що уповноважений присвоювати унікальні значення імен у компоненті **partyName**;
- **uniformResourceIdentifier** – уніфікований ідентифікатор ресурсів (Uniform Resource Identifier) для WWW, який визначений згідно з Internet RFC 1630;
- **iPAddress** – IP адреса, яка визначена згідно з Internet RFC 791, подана у вигляді бінарного рядка;
- **registeredID** – ідентифікатор будь-якого зареєстрованого об'єкта, присвоєного згідно з CCITT Rec. X.660 | ISO/IEC 9834-1.

# РОЗШИРЕННЯ „АЛЬТЕРНАТИВНЕ ІМ'Я ЕМІТЕНТА"

(може бути критичним або некритичним )

- **issuerAltName EXTENSION ::= {**
- **SYNTAX GeneralNames**
- **IDENTIFIED BY id-ce-issuerAltName }**

# РОЗШИРЕННЯ „АТРИБУТИ КАТАЛОГУ СУБ’ЄКТА”

(завжди є некритичним)

- **subjectDirectoryAttributes EXTENSION ::= {**
- **SYNTAX AttributesSyntax**
- **IDENTIFIED BY id-ce-subjectDirectoryAttributes }**
- **AttributesSyntax ::= SEQUENCE SIZE (1..MAX) OF Attribute**

# ВИМОГИ
# ДО ОБРОБКИ ШЛЯХУ СЕРТИФІКАЦІЇ

- сертифікати кінцевого об'єкта мають відрізнятися від сертифікатів УС.

- УС має бути спроможний точно зазначити обмеження, які дозволяють користувачу сертифіката перевіряти, що менш довірені УС на шляху сертифікації не порушують довіру до себе шляхом випуску сертифікатів суб'єктам у невідповідному просторі імен.

- обробка шляху сертифікації має реалізовуватися в автоматизованому та автономному модулі. Необхідно, щоб були реалізовані довірені апаратні або програмні модулі, які виконують функції обробки шляху сертифікації.

# ВИМОГИ ДО ОБРОБКИ ШЛЯХУ СЕРТИФІКАЦІЇ (продовження)

- має існувати можливість реалізації обробки шляху сертифікації без залежності від взаємодій у реальному часі з локальним користувачем;
- має бути можливість реалізації обробки шляху сертифікації без залежності від використання довірених локальних баз даних інформації опису політик;
- шляхи сертифікації мають діяти в середовищах, де розпізнається множина політик застосування сертифікатів.

# ВИМОГИ ДО ОБРОБКИ ШЛЯХУ СЕРТИФІКАЦІЇ (продовження)

- потрібно забезпечення достатньої гнучкості в моделях довіри.;
- структури іменування не мають бути обмежені необхідністю використання імен у сертифікатах, тобто структура імен Каталогу, що вважається звичайною для організацій або географічних зон, не має коректуватися з метою адаптації до вимог УС;
- поля розширення сертифіката мають бути зворотно-сумісними із системою необмеженого зближення шляхів сертифікації, як зазначено в більш ранніх редакціях ITU-T Rec. X.509 | ISO/IEC 9594-8;
- необхідно, щоб УС був спроможний забороняти використання відображення політик і вимагати присутності явних ідентифікаторів політики застосування сертифікатів у наступних сертифікатах на шляху сертифікації;

# ПОЛЯ РОЗШИРЕННЯ ДЛЯ СЕРТИФІКАТІВ

- базові обмеження;
- обмеження імені;
- обмеження політики;
- заборона будь-якої політики.

# ВИМОГИ, ЩО СТОСУЮТЬСЯ ССС

- для кожного скасованого сертифіката ССС містить дату оголошення скасування, яке було здійснено уповноваженим органом;
- користувачі сертифіката повинні бути здатні визначати із самого ССС додаткову інформацію, яка включає область дії сертифікатів, що охоплюється цим списком, порядок повідомлень про скасування та потік ССС, у якому номер ССС є унікальним;
- емітенти повинні бути здатні динамічно змінювати розбивку ССС на частини й направляти користувачів сертифікатів у нове місце розташування відповідних ССС, якщо розбивка змінилася;
- дельта-ССС також можуть бути доступні, щоб обновити заданий базовий ССС. Користувачі сертифіката повинні бути здатні визначати із заданого ССС таке: чи доступні дельта-ССС, де вони розміщені й коли буде випущений наступний дельта-ССС.

# ПОЛЯ РОЗШИРЕННЯ ССС ТА ЗАПИСІВ ССС

- **номер ССС;**
- код причини;
- код команди блокування
- дата втрати чинності;
- **область дії ССС;**
- **передача статусу на розгляд;**
- **ідентифікатор потоку ССС;**
- **упорядкований список;**
- **дельта-інформація.**

# РОЗШИРЕННЯ „НОМЕР ССС”

- **cRLNumber EXTENSION ::= {**
- **SYNTAX CRLNumber**
- **IDENTIFIED BY id-ce-cRLNumber }**
- **CRLNumber ::= INTEGER (0..MAX)**

# РОЗШИРЕННЯ „КОД ПРИЧИНИ”
## (завжди некритичне )

- reasonCode EXTENSION ::= {
- SYNTAX CRLReason
- IDENTIFIED BY id-ce-reasonCode }
- CRLReason ::= ENUMERATED {
- unspecified (0),
- keyCompromise (1),
- cACompromise (2),
- affiliationChanged (3), (змінена інформація)
- superseded (4), (сертифікат був замінений
- cessationOfOperation (5), (сертифікат більше не потрібний для зазначених цілей)
- certificateHold (6), (заблокований)
- removeFromCRL (8),
- privilegeWithdrawn (9), (скасування повноважень)
- aACompromise (10) }

# РОЗШИРЕННЯ „КОД КОМАНДИ БЛОКУВАННЯ”

**(завжди некритичне )**

- **holdInstructionCode EXTENSION ::= {**
- **SYNTAX HoldInstruction**
- **IDENTIFIED BY id-ce-instructionCode }**
- **HoldInstruction ::= OBJECT IDENTIFIER**

# РОЗШИРЕННЯ „ДАТА ВТРАТИ ЧИННОСТІ”
## (завжди некритичне )

- **invalidityDate EXTENSION ::= {**
- **SYNTAX GeneralizedTime**
- **IDENTIFIED BY id-ce-invalidityDate }**

# РОЗШИРЕННЯ „ОБЛАСТЬ ДІЇ ССС”

## (завжди критичне )

```
crlScope EXTENSION ::= {
  SYNTAX          CRLScopeSyntax
  IDENTIFIED BY   id-ce-cRLScope }
CRLScopeSyntax ::=      SEQUENCE SIZE (1..MAX) OF PerAuthorityScope
PerAuthorityScope ::= SEQUENCE {
  authorityName          [0]   GeneralName OPTIONAL,
  distributionPoint  [1] DistributionPointName OPTIONAL,
  onlyContains           [2]   OnlyCertificateTypes OPTIONAL,
  onlySomeReasons        [4]   ReasonFlags OPTIONAL,
  serialNumberRange      [5]   NumberRange OPTIONAL,
  subjectKeyIdRange      [6]   NumberRange OPTIONAL,
  nameSubtrees           [7]   GeneralNames OPTIONAL,
  baseRevocationInfo     [9]   BaseRevocationInfo OPTIONAL
 }
OnlyCertificateTypes ::= BIT STRING {
  user        (0),
  authority   (1),
  attribute   (2) }
NumberRange ::= SEQUENCE {
  startingNumber   [0]   INTEGER OPTIONAL,
  endingNumber     [1]   INTEGER OPTIONAL,
  modulus                INTEGER OPTIONAL }
BaseRevocationInfo ::= SEQUENCE {
  cRLStreamIdentifier    [0]   CRLStreamIdentifier OPTIONAL,
  cRLNumber              [1]   CRLNumber,
  baseThisUpdate         [2]   GeneralizedTime }
```

# РОЗШИРЕННЯ „ПЕРЕДАЧА СТАТУСУ НА РОЗГЛЯД”

- забезпечує механізм для випуску довіреного „списку ССС”, включаючи всю важливу інформацію для допомоги сторонам, що довіряють, у визначенні, чи мають вони достатньо інформації скасування для своїх потреб;

- забезпечує механізм для переадресації сторони, що довіряє, з попереднього місця розташування (наприклад, зазначеного в розширенні „Пункту розповсюдження ССС”, або запису Каталогу уповноваженого органу на випуск ССС) на інше місце розташування інформації скасування..

# РОЗШИРЕННЯ „ПЕРЕДАЧА СТАТУСУ НА РОЗГЛЯД” (завжди критичне )

```
• statusReferrals EXTENSION ::= {
•   SYNTAX        StatusReferrals
•   IDENTIFIED BY     id-ce-statusReferrals }
• StatusReferrals ::= SEQUENCE SIZE (1..MAX) OF StatusReferral
• StatusReferral ::= CHOICE {
•   cRLReferral     [0]    CRLReferral,
•   otherReferral   [1]    INSTANCE OF OTHER-REFERRAL}
• CRLReferral ::= SEQUENCE {
•   issuer                 [0]    GeneralName OPTIONAL,
•   location               [1]    GeneralName OPTIONAL,
•   deltaRefInfo           [2]    DeltaRefInfo OPTIONAL,
•   cRLScope                      CRLScopeSyntax,
•   lastUpdate             [3]    GeneralizedTime OPTIONAL,
•   lastChangedCRL         [4]    Generalized
• DeltaRefInfo ::= SEQUENCE {
•   deltaLocation          GeneralName,
•   lastDelta        GeneralizedTime OPTIONAL }
• OTHER-REFERRAL ::= TYPE-IDENTIFIER
```

# РОЗШИРЕННЯ „ІДЕНТИФІКАТОР ПОТОКУ ССС”

(завжди некритичне )

- **cRLStreamIdentifier EXTENSION ::= {**
- **SYNTAX CRLStreamIdentifier**
- **IDENTIFIED BY id-ce-cRLStreamIdentifier }**
- **CRLStreamIdentifier ::= INTEGER (0..MAX)**

# РОЗШИРЕННЯ „УПОРЯДКОВАНИЙ СПИСОК”

(завжди некритичне )

- **orderedList EXTENSION ::= {**
- **SYNTAX OrderedListSyntax**
- **IDENTIFIED BY id-ce-orderedList }**
- **OrderedListSyntax ::= ENUMERATED {**
- **ascSerialNum (0), (**послідовність скасованих сертифікатів у ССС сформована в порядку зростання реєстраційного номера сертифіката**)**
- **ascRevDate (1) } (**послідовність скасованих сертифікатів у ССС сформована в порядку зростання дати скасування сертифікатів**)**

# РОЗШИРЕННЯ „ДЕЛЬТА-ІНФОРМАЦІЯ”

(завжди некритичне )

- **deltaInfo EXTENSION ::= {**
- **SYNTAX DeltaInformation**
- **IDENTIFIED BY id-ce-deltaInfo }**
- **DeltaInformation ::= SEQUEsNCE {**
- **deltaLocation GeneralName,**
- **nextDelta GeneralizedTime OPTIONAL }**

# Вимоги до розширень для пунктів розповсюдження ССС та дельта-ССС

- для управління розмірами ССС необхідно, щоб була можливість виділення підмножин з множини всіх сертифікатів, випущених одним уповноваженим органом, для різних ССС. Це може бути досягнуте шляхом зв'язування кожного сертифіката з пунктом розповсюдження ССС, яким є:

- для підвищення швидкості бажано зменшити кількість ССС, які мають бути перевірені при перевірці чинності множини сертифікатів, наприклад, для шляху сертифікації;

- існує вимога розділяти ССС, що містять скасовані сертифікати УС та скасовані сертифікати кінцевих об'єктів. Це спрощує обробку шляхів сертифікації, оскільки очікується, що ССС для скасованих сертифікатів уповноважених органів будуть дуже коротким (звичайно порожнім).

# Вимоги до розширень для пунктів розповсюдження ССС та дельта-ССС

- для різних ССС необхідно застосування запобіжних заходів для ситуацій потенційної компрометації (коли існує ризик зловживання особистим ключем);
- також необхідні запобіжні заходи для часткових ССС (відомих як дельта-ССС), які містять тільки записи для сертифікатів, які були скасовані з моменту випуску базового ССС;
- для дельта-ССС необхідно зазначити дату/час, після якої цей список міститиме оновлення;
- висувається вимога вказувати в межах сертифіката, де можна знайти найновіший ССС (наприклад, найостанніший дельта-ССС).

# Поля розширення для пунктів розповсюдження ССС та дельта-ССС

- пункти розповсюдження ССС;
- випускаючий пункт розповсюдження;
- емітент сертифіката;
- покажчик дельта-ССС;
- оновлення бази;
- найновіший ССС.

# РОЗШИРЕННЯ „ПУНКТИ РОЗПОВСЮДЖЕННЯ ССС”

(може бути критичним або некритичним )

- **cRLDistributionPoints EXTENSION ::= {**
- **SYNTAX CRLDistPointsSyntax**
- **IDENTIFIED BY id-ce-cRLDistributionPoints }**
- **CRLDistPointsSyntax ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint**
- **DistributionPoint ::= SEQUENCE {**
- **distributionPoint [0] DistributionPointName OPTIONAL,**
- **reasons [1] ReasonFlags OPTIONAL,**
- **cRLIssuer [2] GeneralNames OPTIONAL }**
- **DistributionPointName ::= CHOICE {**
- **fullName [0] GeneralNames,**
- **nameRelativeToCRLIssuer [1] RelativeDistinguishedName }**
- **ReasonFlags ::= BIT STRING {**
- **unused (0),**
- **keyCompromise (1),**
- **cACompromise (2),**
- **affiliationChanged (3),**
- **superseded (4),**
- **cessationOfOperation (5),**
- **certificateHold (6),**
- **privilegeWithdrawn (7),**
- **aACompromise (8) }**

# РОЗШИРЕННЯ „ВИПУСКАЮЧИЙ ПУНКТ РОЗПОВСЮДЖЕННЯ”

(завжди критичне )

- **issuingDistributionPoint EXTENSION ::= {**
- **SYNTAX IssuingDistPointSyntax**
- **IDENTIFIED BY id-ce-issuingDistributionPoint }**
- **IssuingDistPointSyntax ::= SEQUENCE {**
- **distributionPoint [0] DistributionPointName OPTIONAL,**
- **onlyContainsUserCerts [1] BOOLEAN DEFAULT FALSE,**
- **onlyContainsAuthorityCerts [2] BOOLEAN DEFAULT FALSE,**
- **onlySomeReasons [3] ReasonFlags OPTIONAL,**
- **indirectCRL [4] BOOLEAN DEFAULT FALSE,**
- **onlyContainsAttributeCerts [5] BOOLEAN DEFAULT FALSE }**

# РОЗШИРЕННЯ „ЕМІТЕНТ СЕРТИФІКАТА”

(завжди критичне )

- **certificateIssuer EXTENSION ::= {**
- **SYNTAX GeneralNames**
- **IDENTIFIED BY id-ce-certificateIssuer }**

# РОЗШИРЕННЯ „ПОКАЖЧИК ДЕЛЬТА-ССС”

(завжди критичне )

- **deltaCRLIndicator EXTENSION ::= {**
- **SYNTAX BaseCRLNumber**
- **IDENTIFIED BY id-ce-deltaCRLIndicator }**
- **BaseCRLNumber ::= CRLNumber**

# РОЗШИРЕННЯ „ОНОВЛЕННЯ БАЗОВОЇ ІНФОРМАЦІЇ СКАСУВАННЯ”

(завжди некритичне )

- **baseUpdateTime EXTENSION ::= {**
- **SYNTAX GeneralizedTime**
- **IDENTIFIED BY id-ce-baseUpdateTime }**

# РОЗШИРЕННЯ „НАЙНОВІШИЙ ССС”

(може бути як критичним, так і некритичним )

- **freshestCRL EXTENSION ::= {**
- **SYNTAX CRLDistPointsSyntax**
- **IDENTIFIED BY id-ce-freshestCRL }**

# ВХІДНІ ДАНІ ОБРОБКИ ШЛЯХУ

- набір сертифікатів, що становлять шлях сертифікації;
- довірене значення відкритого ключа або ідентифікатор ключа (якщо ключ зберігається всередині модуля обробки шляху сертифікації), для використання при перевірці першого сертифіката в шляху сертифікації;
- значення покажчика *initial-policy-set*, що містить один або більше ідентифікаторів політик застосування сертифікатів, які зазначають, що кожна із цих політик буде припустимою для користувача сертифіката з метою обробки шляху сертифікації; ці вхідні дані можуть також приймати спеціальне значення *any-policy*;
- значення покажчика *initial-explicit-policy*, який вказує на необхідність вказівки явного ідентифікатора політик у полі розширення „Політика застосування сертифікатів” всіх сертифікатів на шляху;
- значення покажчика *initial-policy-mapping-inhibit*, що зазначає, чи заборонено відображення політики на шляху сертифікації;
- значення покажчика *initial-inhibit-any-policy*, що зазначає, чи вважається спеціальне значення **anyPolicy**, якщо воно присутнє в розширенні „Політика застосування сертифікатів”, співпадаючим із будь-яким конкретним значенням політики застосування сертифікатів в обмеженому наборі;
- поточна дата/час (якщо вони внутрішньо не доступні для модуля обробки шляху сертифікації).

# ВИХІДНІ ДАНІ ОБРОБКИ ШЛЯХУ

- покажчик успіху або невдачі перевірки дійсності шляху сертифікації;
- діагностичний код, що зазначає причину невдачі, якщо перевірка дійсності завершилася невдачею;
- набір політик, обмежених уповноваженим органом, та пов'язані з ними описи, відповідно до яких шлях сертифікації є дійсним, або спеціальне значення *any-policy*;
- набір політик, обмежених користувачем, сформованих у результаті перетинання *authorities-constrained-policy-set* та *initial-policy-set*;
- покажчик *explicit-policy-indicator*, який зазначає, чи вимагає користувач сертифіката або уповноважений орган на шляху, щоб припустима політика ідентифікувалася в кожному сертифікаті в шляху сертифікації;
- деталі відображення будь-якої політики, що виникає під час обробки шляху сертифікації.

# ЗМІННІ ОБРОБКИ ШЛЯХУ

- *authorities-constrained-policy-set*: таблиця ідентифікаторів політик та описів із сертифікатів шляху сертифікації (рядки зазначають політики, їхні описи та історію відображення, а стовпці зазначають сертифікати в шляху сертифікації);

- *permitted-subtrees*: набір специфікацій піддерева, що визначають піддерева, у які мають потрапляти всі імена суб'єктів у наступних сертифікатах в шляху сертифікації, або вони можуть приймати спеціальне значення *unbounded*;

- *excluded-subtrees*: набір (можливо порожній) специфікацій піддерева (кожен містить базове ім'я піддерева та покажчики максимального та мінімального рівнів), що визначають піддерева, в які не можуть потрапляти ніякі імена суб'єктів у наступному сертифікаті в шляху сертифікації;

- *required-name-forms*: набір (можливо порожній) із множини форм імені. Для кожного набору форм імені кожний наступний сертифікат має містити ім’я із форм  імені з цього набору;

# ЗМІННІ ОБРОБКИ ШЛЯХУ (продовження)

- *explicit-policy-indicator*: зазначає, чи повинна припустима політика явно ідентифікуватися в кожному сертифікаті в шляху сертифікації;

- *path depth*: ціле число, значення якого дорівнює числу сертифікатів на шляху сертифікації плюс одиниця, для яких обробка завершена;

- *policy-mapping-inhibit-indicator*: зазначає, чи заборонено відображення політики;

- *inhibit-any-policy-indicator*: зазначає, чи вважається спеціальне значення **anyPolicy** співпадаючим з будь-якою конкретною політикою застосування сертифікатів;

- *pending-constraints*: деталі обмежень явного або забороненого відображення політик і/або будь-якої забороненої політики, які зазначені, але ще не мають чинності. Існує три однобітових покажчики, які називаються *explicit-policy-pending*, *policy-mapping-inhibit-pending* та *inhibit-any-policy-pending*. Для кожного покажчика встановлюється значення, яке має назву *skip-certificates* та зазначає число сертифікатів, які необхідно пропустити до того, як обмеження набудуть чинності.