НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

Інформаційні технології

МЕТОДИ ЗАХИСТУ КЕРУВАННЯ КЛЮЧАМИ

Частина 1. Загальні положення

(ISO/IEC 11770-1:1996, IDT)

ДСТУ ISO/IEC 11770-1:2009

Видання офіційне

БЗ № 3–2009/464

Київ
ДЕРЖСПОЖИВСТАНДАРТ УКРАЇНИ
2010

ПЕРЕДМОВА

1 ВНЕСЕНО: Технічний комітет стандартизації ТК 105 «Банківські та фінансові системи та технології», ЗАТ «Інститут інформаційних технологій»

ПЕРЕКЛАД І НАУКОВО-ТЕХНІЧНЕ РЕДАГУВАННЯ: **І. Горбенко,** д-р техн. наук (науковий керівник); **І. Івченко,** канд. техн. наук; **М. Карнаух; О. Потій,** канд. техн. наук; **А. Лєншин,** канд. техн. наук; **Д. Шевченко; І. Остапенко**

2 НАДАНО ЧИННОСТІ: наказ Держспоживстандарту України від 12 березня 2009 р. № 108 з 2010–06–01

3 Національний стандарт відповідає ISO/IEC 11770-1:1996 Information technology — Security techniques — Key management — Part 1: Framework (Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Загальні положення)

Ступінь відповідності — ідентичний (IDT)

Переклад з англійської (en)

4 УВЕДЕНО ВПЕРШЕ

ЗМІСТ

НАЦІОНАЛЬНИЙ ВСТУП

Цей стандарт є тотожний переклад ISO/IEC 11770-1:1996 Information technology — Security techniques — Key management — Part 1: Framework (Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Загальні положення).

Технічний комітет, відповідальний за цей стандарт в Україні, — ТК 105 «Банківські та фінансові системи і технології».

Стандарт містить вимоги, які відповідають чинному законодавству України.

До стандарту внесено такі редакційні зміни:

— слова «ця частина ISO/IEC 11770», «цей документ» замінено на «цей стандарт»;

— структурні елементи стандарту: «Титульний аркуш», «Передмову», «Національний вступ», «першу сторінку», «Терміни та визначення понять» і «Бібліографічні дані» — оформлено відповідно до вимог комплексу стандартів «Національна стандартизація»;

— у розділах «Нормативні посилання» та «Бібліографія» наведено «Національне пояснення», виділене в тексті рамкою;

— до підрозділу 3.2 долучено «Національну примітку», виділену в тексті рамкою.

Додатки А, В, С, Д — інформативні.

Копії документів, на які є посилання в тексті цього стандарту, можна замовити в Головному фонді нормативних документів.

НАЦІОНАЛЬНИЙ СТАНДАРТ УКРАЇНИ

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

МЕТОДИ ЗАХИСТУ. КЕРУВАННЯ КЛЮЧАМИ

Частина 1. Загальні положення

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

МЕТОДЫ ЗАЩИТЫ. УПРАВЛЕНИЕ КЛЮЧАМИ

Часть 1. Основные положения

INFORMATION TECHNOLOGY

SECURITY TECHNIQUES. KEY MANAGEMENT

Part 1. Framework

Чинний від 2010–06–01

1 СФЕРА ЗАСТОСУВАННЯ

Цей стандарт:

1) установлює мету керування ключами;

2) описує загальну модель керування ключами, яка є основою для механізмів керування ключами;

3) визначає основні поняття щодо керування ключами, загальні для всіх частин стандарту;

4) визначає послуги керування ключами;

5) установлює властивості механізмів керування ключами;

6) висуває вимоги щодо керування ключовими даними протягом їхнього життєвого циклу;

7) описує схему керування ключовими даними протягом їхнього життєвого циклу.

Цей стандарт визначає загальну модель керування ключами, незалежну від використання будь-якого окремого криптографічного алгоритму. Однак певні механізми розподілення ключів можуть залежати від окремих властивостей алгоритмів, наприклад від властивостей асиметричних алгоритмів.

Окремі механізми керування ключами розглянуто в інших частинах стандарту ISO/IEC 11770. Симетричні механізми розглянуто в ISO/IEC 11770–2. Асиметричні механізми розглянуто в ISO/IEC 11770–3. Цей стандарт є основоположним для зазначених вище стандартів. Приклади використання механізмів керування ключами містять стандарти ISO 8732 та ISO 11166. Якщо для керування ключами потрібна неспростовність, треба використовувати стандарти ISO/IEC 13888.

У цьому стандарті розглянуто як автоматизовані, так і неавтоматизовані аспекти керування ключами, в тому числі структури елементів даних і послідовності операцій, які використовують для отримання послуг керування ключами. Однак деталі протоколу обміну, які можуть знадобитися, цим стандартом не визначено.

Як і у випадку інших послуг щодо безпеки, керування ключами може забезпечуватися тільки в контексті визначеної політики безпеки. Означення політики безпеки не належить до сфери застосування цього стандарту.

Видання офіційне

2 НОРМАТИВНІ ПОСИЛАННЯ

Наведені нижче нормативні документи містять положення, які через посилання в цьому тексті становлять положення цього стандарту. На час опублікування цього стандарту зазначені нормативні документи були чинними. Усі нормативні документи підлягають перегляду, і учасникам угод, базованих на цьому стандарті, необхідно визначити можливість застосування найновіших видань нормативних документів, наведених нижче. Члени IEC та ISO впорядковують каталоги чинних міжнародних стандартів.

ISO 7498-2:1989 Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture

ISO/IEC 9798-1:1991 Information technology — Security techniques — Entity authentification mechanisms — Part 1: General model

ISO 10181-1:1996 Information Technology — Open Systems Interconnection — Security frameworks for open systems: Overview.

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

ISO 7498-2:1989 Системи оброблення інформації. Взаємодія відкритих систем. Базова еталонна модель. Частина 2. Архітектура безпеки

ISO/IEC 9798-1:1991 Інформаційні технології. Методи захисту. Механізми автентифікування об'єктів. Частина 1. Загальна модель

ISO 10181-1:1996 Інформаційні технології. Взаємодія відкритих систем. Схеми безпеки для відкритих систем. Огляд.

3 ТЕРМІНИ ТА ВИЗНАЧЕННЯ ПОНЯТЬ

Наведені нижче терміни вжито згідно з визначеннями, наведеними в ISO 7498-2:
цілісність даних (*data integrity*);
автентифікація джерела даних (*data origin authentication*);
цифровий підпис (*digital signature*).
Наведені нижче терміни вжито згідно з визначеннями, наведеними в ISO 9798-1:
автентифікація об'єкта (*entity authentication*).
Наведені нижче терміни вжито згідно з визначеннями, наведеними в ISO/IEC 10181-1:
повноважний з безпеки (*security authority*);
домен безпеки (*security domain*);
третя довірча сторона (TTP) (*trusted third party* (TTP)).
У цьому стандарті вжито такі терміни та визначення позначених ними понять.

3.1 асиметричний криптографічний метод (*asymmetric cryptographic technique*)

Криптографічний метод, який використовує два взаємозв'язані перетворення: відкрите (з використанням відкритого ключа) і секретне (з використанням особистого ключа); ці перетворення мають таку властивість, що за наданим відкритим перетворенням не можна в результаті обчислень вивести секретне перетворення

3.2 повноважна організація з сертифікування (CA) (*certification authority*) (CA)

Центр, якому довірено формувати і призначати сертифікати відкритих ключів; CA може формувати і призначати ключі об'єктам (необов'язково).

Національна примітка

В Україні повноважною організацією з сертифікування є Центр сертифікування ключів, Засвідчувальний центр, Центральний засвідчувальний орган

3.3 розшифровування (*decipherment*)

Обернення відповідного перетвору зашифровування

3.4 зашифровування (*encipherment*)

(Зворотне) перетворення даних за допомогою криптографічного алгоритму для одержання шифротексту, тобто для приховування інформаційного змісту даних

3.5 ключ (*key*)

Послідовність кодів, яка керує виконанням криптографічного перетворення (наприклад, зашифровування, розшифровування, обчислення криптографічної перевіркової функції, формування підпису або верифікація цього підпису)

3.6 узгодження ключів (*key agreement*)

Процес установлювання спільного таємного ключа між об'єктами так, що жоден з них не може попередньо визначити значення цього ключа

3.7 підтвердження ключа (*key confirmation*)

Засвідчення одному із об'єктів, що інший ідентифікований об'єкт володіє правильним ключем

3.8 контроль ключа (*key control*)

Спроможність вибрати ключ або параметри, використовувані для обчислення ключа

3.9 центр розподілення ключів (ЦРК) (*key distribution center*) (KDC)

Об'єкт, якому довірено генерування (або придбання) і розподілення ключів об'єктам, кожен з яких має ключовий взаємозв'язок із ЦРК

3.10 ключові дані (*key material*)

Дані (а саме: ключі, значення для ініціалізації), потрібні для встановлення і підтримування криптографічного ключового взаємозв'язку

3.11 керування ключами (*key management*)

Адміністрування і використання генерування, реєстрування, сертифікування, скасування, розподілення, інсталювання, зберігання, архівування, відкликання, виведення і знищення ключових даних відповідно до політики безпеки

3.12 центр передавання ключів (ЦПК) (*key translation center*) (KTC)

Об'єкт, якому довірено передавання ключів між об'єктами, кожен з яких має ключовий взаємозв'язок із ЦПК

3.13 особистий ключ (*private key*)

Ключ пари асиметричних ключів об'єкта, який повинен використовувати тільки цей об'єкт.

Примітка. Особистий ключ зазвичай не повинен розкриватися.

3.14 відкритий ключ (*public key*)

Ключ пари асиметричних ключів об'єкта, який може бути загальнодоступний

3.15 сертифікат відкритого ключа (*public key certificate*)

Інформація щодо відкритого ключа об'єкта, підписана повноважною організацією з сертифікування, внаслідок чого вона стає непідробною

3.16 інформація щодо відкритого ключа (*public key information*)

Певна інформація окремого об'єкта, яка містить щонайменше розрізнювальний ідентифікатор об'єкта і щонайменше один його відкритий ключ. Може бути доповнена іншою інформацією щодо повноважної організації з сертифікування, об'єкта і відкритого ключа, який міститься в інформації щодо відкритого ключа, а саме: строк чинності відкритого ключа, строк чинності відповідного особистого ключа або ідентифікатор застосованого алгоритму

3.17 випадкове число (*random number*)

Змінюваний з часом параметр, значення якого не можна передбачити

3.18 таємний ключ (*secret key*)

Ключ, який використовує у симетричних криптографічних методах тільки наперед визначена множина об'єктів

3.19 порядковий номер (*sequence number*)

Змінюваний з часом параметр, значення якого вибирають із визначеної послідовності, який не повторюється протягом певного періоду часу

3.20 симетричний криптографічний метод (*symmetric cryptographic technique*)
Криптографічний метод, який використовує однаковий таємний ключ для перетворення даних як відправника, так і одержувача Без знання таємного ключа не можна в результаті обчислень вивести перетворення даних ні відправника, ні одержувача

3.21 познака часу (*time stamp*)
Змінюваний з часом параметр, який відмічає момент часу щодо загальноприйнятого еталону часу

3.22 змінюваний з часом параметр (*time variant parameter*)
Одиниця даних, яку використовує об'єкт для верифікування неповторюваності повідомлення, а саме випадкове число, номер із послідовності або познака часу

4 ЗАГАЛЬНІ ПОЛОЖЕННЯ ПРО КЕРУВАННЯ КЛЮЧАМИ

Керування ключами — це адміністрування та використання послуг щодо генерування, реєстрування, сертифікування, скасування, розподілення, інсталювання, зберігання, архівування, відкликання, виведення та знищення ключових даних

Метою керування ключами є безпечне адміністрування та використання зазначених послуг щодо керування ключами і тому захист ключів є надзвичайно важливим

Процедури керування ключами залежать від основних криптографічних механізмів, передбачуваного використання ключа та чинної політики безпеки Керування ключами охоплює також функції, виконувані в криптографічному обладнанні.

4.1 Захист ключів

Ключі є критичною частиною будь-якої системи захисту, основаної на криптографічних методах Належний захист ключів залежить від низки чинників, а саме типу програмного застосунку, для якого використовують ключі, загроз, з якими вони стикаються, різних станів, у яких можуть перебувати ключі тощо Головним чином ключі мають бути захищені від розкриття, модифікування, знищення і повторного використання (залежно від криптографічних методів) Приклади можливих загроз ключам наведені в додатку А Чинність ключа має бути обмежена часом і кількістю використань Ці обмеження визначаються часом і кількістю даних, потрібних для проведення атаки з розкриття ключа, та стратегічною цінністю захищеної інформації протягом часу Ключі, використовувані для генерування інших ключів потребують більшого захисту, ніж ключі, які генеруються Іншим важливим аспектом захисту ключів є унеможливлення їхнього помилкового використання, а саме використання ключа шифрування для ключа шифрування даних

4.1.1 *Захист криптографічними методами*

Деяким загрозам ключовим даним можна протидіяти використанням криптографічних методів Наприклад, шифрування протидіє розкриттю і несанкціонованому використанню ключа, механізми цілісності даних протидіють модифікуванню, механізми автентифікування джерела даних, цифрові підписи та механізми автентифікування об'єктів протидіють імітуванню

Криптографічні механізми розділення протидіють помилковому використанню Таке розділення функційного використання можна виконувати зв'язуванням інформації з ключем Наприклад, зв'язування контролівної інформації з ключем забезпечує використання спеціальних ключів для спеціальних задач (а саме для шифрування ключа, цілісності даних) контроль ключів потрібний для неспростовності у симетричних методах

4.1.2 *Захист некриптографічними методами*

Познаки часу можна використовувати для обмеження використання ключів певними допустимими періодами часу Разом із порядковими номерами вони також захищають від повторення записаної інформації узгодження ключа

4.1.3 *Захист фізичними засобами*

Кожний криптографічний пристрій у межах захищеної системи потребує захисту ключової інформації, яку він використовує, від загроз модифікування, знищення і розкриття, за винятком відкритих ключів Такий пристрій зазвичай забезпечує безпечну область зберігання ключів їхнього використання та виконання криптографічного алгоритму Він може надавати засоби

— уведення ключової інформації з окремого захищеного пристрою зберігання ключа,

— взаємодії з криптографічними алгоритмами, реалізованими в окремих інтелектуальних засобах захисту (а саме в інтелектуальних картках картках із пам'яттю),

— зберігання ключової інформації у вигляді файлів (а саме на дискеті)

Області безпеки зазвичай захищають фізичними механізмами безпеки

4.1.4 ***Захист організаційними засобами***

Одчим із засобів захисту ключів є організація їх в ієрархію ключів Окрім найнижчого рівня ієрархії, ключі одного рівня ієрархії використовують винятковно для захисту ключів у наступному нижньому рівні ієрархії Тільки ключі найнижчого рівня ієрархії використовують безпосередньо для забезпечення послуг захисту даних Такий ієрархічний підхід дозволяє обмежити використання кожного ключа, обмежуючи таким чином розкриття й ускладнюючи проведення атаки Наприклад, компрометація окремого сеансового ключа обмежена тільки компрометацією інформації, захищеної цим ключем

Використання безпечних областей стосується загроз розкриття ключів, іхнього модифікування та знищення неуповноваженими суб єктами Однак залишається загроза, що системні адміністратори уповноважені на виконання окремих функцій керування компонентами послуги керування ключами, можуть зловживати своіми спеціальними привілеями доступу Зокрема, вони можуть спробувати отримати головний ключ (ключ найвищого рівня ієрархії) Розкриття головного ключа потенційно дає змогу заволодіти, розкрити або маніпулювати всіма іншими ключами, захищеними цим ключем (тобто всіма іншими ключами в тій конкретній ключовій ієрархії) Отже, бажано мінімізувати доступ до цього ключа можливо вжити таких заходів, щоб жодна окрема особа не мала доступу до його значення Таку вимогу можна задовольнити розподіленням ключа (подвійний або навіть n-кратний контроль) або використанням спеціальних криптографічних схем (Схеми Поділу Таємниці)

4.2 Загальна модель життєвого циклу ключа

Криптографічний ключ проходить через послідовність станів, що визначають його життєвий цикл Головними є три стани

— очікування активності (очікування) у цьому стані ключ треба згенерувати, але не вводити в дію з метою використання,

— активний у цьому стані ключ використовують для криптографічного перетворення інформації,

— постактивний у цьому стані ключ треба використовувати тільки для розшифровування або верифікування

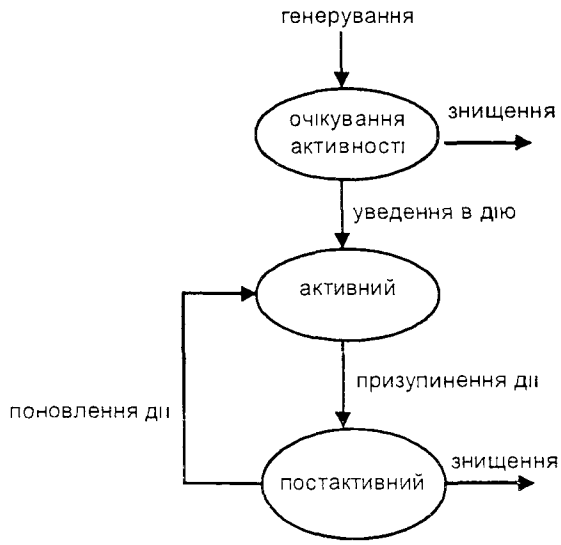

Рисунок 1 — Життєвий цикл ключа

Примітка Користувач постактивного ключа повинен мати гарантію що дані криптографічно оброблено до того як ключ став постактивним Цю гарантію зазвичаи забезпечує довірчии змінниии у часі параметр

Ключ, про який відомо, що його скомпрометовано, має відразу набути постактивного стану і може потребувати спеціального поводження. Ключ уважають скомпрометованим, якщо відомо або підозрюють його неуповноважене використання.

На рисунку 1 проілюстровано стани і відповідні переходи між ними.

На рисунку 1 наведено узагальнену модель життєвого циклу ключа. Інші моделі життєвого циклу можуть мати додаткові деталі, які можуть бути підстанами поданих вище трьох станів. Більшість життєвих циклів потребує дій стосовно архівування. Ці дії можуть бути асоційовані з будь-яким із станів залежно від окремих деталей життєвого циклу.

4.2.1 ***Переходи між станами ключа***

Під час переходів ключа від одного стану до іншого він підлягає одному з таких перетворень, що відображено також на рисунку 1:

— **генерування** — це процес генерування ключа. Генерування ключа треба здійснювати згідно з встановленими правилами генерування ключів. Процес генерування ключів може містити випробувальні процедури для верифікування дотримання цих правил:

— **уведення в дію** — робить ключ чинним для криптографічних операцій;

— **призупинення дії** — обмежує використання ключа. Це може статися внаслідок закінчення строку дії ключа або його відкликання;

— **поновлення дії** — дозволяє знову використовувати постактивний ключ для криптографічних операцій;

— **знищення** — закінчує життєвий цикл ключа. Воно охоплює логічне знищення ключа і може містити його фізичне знищення.

Переходи можуть бути спричинені такими подіями: потреба нових ключів, компрометація ключа, закінчення строку дії ключа та завершення життєвого циклу ключа. Усі ці переходи містять низку послуг керування ключами. Взаємовідносини між переходами і послугами наведено у таблиці 1. Ці послуги пояснено у розділі 5.

Будь-який окремий криптографічний підхід потребуватиме лише підмножини послуг, наведених у таблиці 1.

Таблиця 1 — Переходи і послуги

Переходи	Послуга	Примітка
Генерування	генерування ключа	обов'язкова
	реєстрування ключа	необов'язкова, тут або під час активізування
	формування сертифіката ключа	необов'язкова
	розподілення ключа	необов'язкова
	зберігання ключа	необов'язкова
Уведення в дію	формування сертифіката ключа	необов'язкова
	розподілення ключа	необов'язкова
	виведення ключа	необов'язкова
	інсталювання ключа	обов'язкова
	зберігання ключа	необов'язкова
	реєстрування ключа	необов'язкова, тут або під час генерування
Призупинення дії	зберігання ключа	необов'язкова
	архівування ключа	необов'язкова, тут або під час знищення
	відкликання ключа	необов'язкова
Поновлення дії	формування сертифіката ключа	необов'язкова
	розподілення ключа	необов'язкова
	виведення ключа	необов'язкова
	інсталювання ключа	обов'язкова
	зберігання ключа	необов'язкова

Кінець таблиці 1

Переходи	Послуга	Примітка
Знищення	скасування ключа	обов язкова якщо реєстрований
	знищення ключа	обов язкова
	архівування ключа	необов'язкова, тут або під час деактивізування

4.2.2 *Переходи, послуги і ключі*

Ключі для окремих криптографічних методів використовують різні комбінації послуг протягом їхнього життєвого циклу Нижче наведено два приклади

Для симетричних криптографічних методів після генерування ключа перехід від очікування активності до активного стану містить інсталювання ключа, а також може містити реєстрування та розподілення ключа У деяких випадках інсталювання також може містити виведення спеціального ключа Життєвий цикл ключа має бути обмежений фіксованим періодом Активний стан закінчується призупиненням дії зазвичай, після закінчення строку дії ключа Якщо відбулася або підозрюють компрометацію ключа в активному стані, відкликання також спричиняє його перехід у постактивний стан Постактивний ключ можна заархівувати Якщо знову потрібен заархівований ключ, його буде поновлено і він може знову потребувати інсталювання або розподілення перш ніж стане повністю активним У протилежному випадку після призупинення дії ключ може бути скасовано і знищено

Для асиметричних криптографічних методів генерують пару ключів (відкритий та особистий) і обидва ключі переходять у стан очікування активності Зауважимо, що життєві цикли обох ключів пов'язані між собою, але неідентичні Перш ніж перейти в активний стан, особистий ключ буде зареєстровано (необов язково), розподілено його користувачу (необов'язково) і завжди інстальовано Переходи особистого ключа з активного стану в постактивний стан, зокрема призупинення дії, поновлення дії і знищення подібні до описаних для симетричних ключів У разі сертифікування відкритого ключа зазвичай сертифікат, що містить відкритий ключ, створює повноважна організація з сертифікування з метою засвідчення чинності та особи власника відкритого ключа Цей сертифікат відкритого ключа може бути розміщений у довіднику або в іншій подібній службі, або вернений власнику для розподілення Коли власник розсилає інформацію, що підписана його особистим ключем, він може додати свій сертифікат Пара ключів стає активною після сертифікування відкритого ключа Якщо пару ключів використовують для цифрового підпису, відкритий ключ може залишатися в активному або в постактивному стані протягом невизначеного часу після того, як призупинено дію або знищено відповідний йому особистий ключ Доступ до відкритого ключа може бути потрібний для верифікування цифрових підписів, зроблених до первинної дати закінчення строку дії відповідного особистого ключа Якщо для шифрування використовують асиметричні методи і призупинено дію або знищено ключ, використаний для зашифровування, відповідний особистий ключ пари може залишатися в активному або постактивному стані для подальшого розшифровування

Певне використання ключа або застосунок можуть визначати послуги для цього ключа Наприклад у системі може бути прийнято рішення не реєструвати сеансові ключі тому, що процес реєстрування може бути довшим, ніж їх життєвий цикл Навпаки, потрібно реєструвати таємний ключ у разі використання для цифрового підпису симетричних методів

5 ПОНЯТТЯ ПРО КЕРУВАННЯ КЛЮЧАМИ

5 1 Послуги щодо керування ключами

Для кращого розуміння послуг щодо керування ключами у цьому розділі описано загальну структуру керування ключами, як послуги скомбіновано одна з одною та як їх підтримують

Керування ключами спирається на основні послуги щодо генерування реєстрування сертифікування розподілення інсталювання зберігання, виведення, архівування, відкликання скасування та знищення Ці послуги можуть бути частиною системи керування ключами або надаватися іншими постачальниками послуг Залежно від виду послуги постачальник послуги повинен виконувати визначений мінімум вимог щодо безпеки (безпека обміну тощо) для того, щоб йому довіряли всі залучені об єкти Наприклад постачальником послуги може бути третя довірча сторона

На рисунку 2 показано, що послуги щодо керування ключами розташовані на одному рівні і можуть бути використані множиною різних користувачів (особами або процесами). Ці користувачі можуть застосовувати різні засоби керування ключами в різних застосунках, використовуючи послуги залежно від своїх потреб. Послуги керування ключами наведені в таблиці 1.

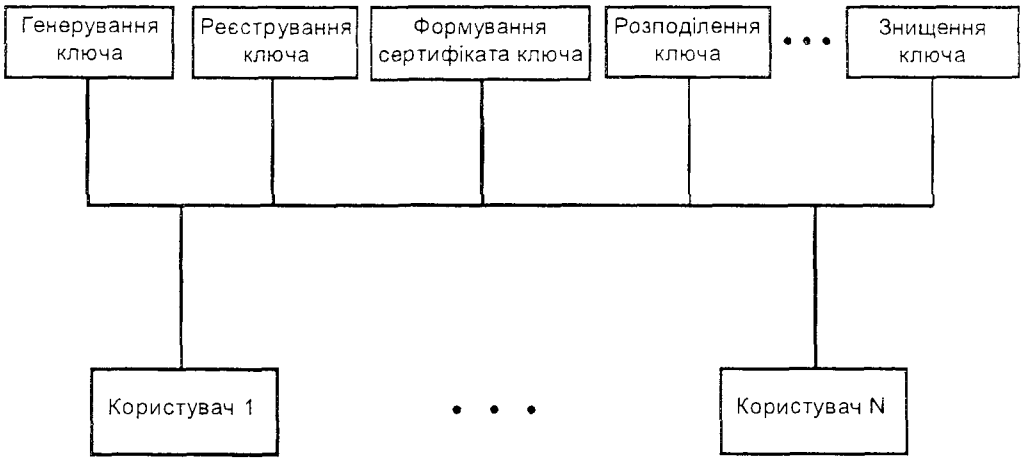

Рисунок 2 — Послуги щодо керування ключами

5.1.1 ***Послуга щодо генерування ключа***

Послуга щодо генерування ключа — це послуга, яку активізують для генерування ключів у захищеному режимі для окремого криптографічного алгоритму. Це означає, що генерування ключів не може бути підроблене, ключі генерують згідно із заданим розподілом і таким чином, що результат не можна передбачити. Цей розподіл залежить від криптографічного алгоритму, для якого його використовують, і потрібним рівнем криптографічного захисту. Генерування деяких ключів, а саме головних ключів, потребує особливої уваги, оскільки знання цих ключів надає доступ до залежних від них або породжених ними ключів.

5.1.2 ***Послуга щодо реєстрування ключа***

Послуга щодо реєстрування ключа зв'язує ключ із об'єктом. Її надає повноважний реєстратор і зазвичай застосовують тоді, коли використовують симетричні методи. Коли об'єкт бажає зареєструвати ключ, він має зв'язатися з повноважним реєстратором. Реєстрування ключа охоплює запит на реєстрування та підтвердження цього реєстрування.

Повноважний реєстратор веде реєстр ключів і відповідної інформації з належним рівнем захисту. У додатку В надано детальну інформацію щодо керування ключами.

Повноважний реєстратор ключів забезпечує операції реєстрування і скасування.

5.1.3 ***Послуга щодо формування сертифіката ключа***

Послуга щодо формування сертифіката ключа засвідчує зв'язок відкритого ключа з об'єктом і надається повноважною організацією з сертифікування. Після одержання запиту на сертифікацію ключа повноважна організація з сертифікування створює сертифікат ключа. Сертифікати відкритих ключів описані детальніше в ISO/IEC 11770-3.

5.1.4 ***Послуга щодо розподілення ключа***

Розподілення ключа — це множина процедур для надійного забезпечення авторизованих об'єктів інформаційними об'єктами керування ключами (відповідно до прикладу в додатку В). Особливим випадком розподілення ключів є передавання ключа, в якій ключові дані встановлюють між об'єктами з використанням центра передавання ключів (відповідно до 6.2).

ISO/IEC 11770-2 пропонує різні механізми встановлення ключів між об'єктами. ISO/IEC 11770-3 визначає механізми узгодження таємних ключів і механізми пересилання таємних і відкритих ключів.

5.1.5 ***Послуга щодо інсталювання ключа***

Послуга щодо інсталювання ключа завжди необхідна перед використанням ключа. Інсталювання ключа означає створення ключа всередині засобу керування ключем із захистом від розкриття.

5.1.6 ***Послуга щодо зберігання ключа***

Послуга щодо зберігання ключа забезпечує безпечне зберігання ключів, призначених для поточного чи короткострокового використання або для резервування. Зазвичай корисно забезпечувати фізично відокремлене зберігання ключів. Наприклад, це забезпечує конфіденційність та цілісність ключових даних або цілісність відкритих ключів.

Зберігання ключів можливе в усіх станах життєвого циклу ключа (а саме: в очікуванні активності, в активному і в постактивному). Залежно від важливості ключів вони можуть бути захищені одним із таких механізмів:

— фізичний захист (а саме: зберігання ключа всередині тривких до пошкоджень пристроїв або на зовнішніх носіях, як дискета або картка з пам'яттю);

— шифрування з використанням ключів, які самі фізично захищені;

— захист доступу до них за допомогою паролів або персонального ідентифікаційного номера (ПІН).

Для всіх ключових даних кожна спроба розкриття має бути виявленою.

5.1.7 ***Послуга щодо виведення ключа***

Послуга щодо виведення ключа створює потенційно велику кількість ключів із використанням таємного первинного ключа, що називають ключем виведення, нетаємних змінюваних даних та процесу перетворення (який так само не потребує таємності). Результатом такого процесу є похідний ключ. Виведення ключа потребує спеціального захисту. Процес виведення має бути незворотним і непередбачуваним, щоб забезпечити неможливість у разі розкриття похідного ключа розкриття ключа виведення або іншого похідного ключа.

5.1.8 ***Послуга щодо архівування ключа***

Архівування ключа забезпечує процес безпечного довгострокового зберігання ключів після нормального використання. Архівування може використовувати послугу зберігання ключів, але допускається також їхнє автономне зберігання. Заархівовані ключі можуть потребувати відновлення значно пізнішою датою з ціллю доведення або спростування певних позовів після припинення нормального користування ключами.

5.1.9 ***Послуга щодо відкликання ключа***

Якщо є припущення або відома компрометація ключа послуга щодо відкликання ключа гарантує безпечне призупинення дії ключа. Ця послуга потрібна для ключів, строк дії яких вичерпано. Відкликання ключа також буде мати місце, коли змінюються обставини у власника ключа. Після відкликання ключа його може бути використано тільки для розшифровування і верифікування. Відкликання ключа не застосовне для схем, заснованих на сертифікатах, в яких життєвий цикл ключа контролюється строком дії сертифіката.

Примітка. Деякі застосунки для цієї послуги використовують строк «вилучити ключ».

5.1.10 ***Послуга щодо скасування ключа***

Послуга щодо скасування ключа — це процедура, яку надає повноважний реєстратор ключів і усуває зв'язок ключа з об'єктом. Вона є частиною процесу знищення ключа (відповідно до 5.1.11). Для скасування ключа об'єкт повинен зв'язатися з повноважним реєстратором.

5.1.11 ***Послуга щодо знищення ключів***

Послуга щодо знищення ключа забезпечує процес безпечного знищення ключів, які вже не потрібні. Знищування ключа означає видалення всіх записів цього інформаційного об'єкта керування ключем таким чином, що не залишається жодної нформації після проведення знищення і жодними засобами неможливо відновити знищений ключ. Це стосується знищування усіх заархівованих копій. Однак до знищування заархівованих ключів має бути виконано перевіряння, щоб упевнитись, що жодний заархівований матеріал, захищений цими ключами, вже ніколи не знадобиться.

Примітка. Деякі ключі можуть зберігатися поза електронним пристроєм або системою Знищення таких ключів потребує додаткових адміністративних заходів.

5.2 Послуги щодо підтримування

Для підтримки дії щодо керування ключами можуть знадобитися інші послуги.

5.2.1 *Послуги засобів керування ключами*

Послуги щодо керування ключами можуть використовувати інші послуги, що стосується захисту. До них належать:

— **контроль доступу.** Ця послуга може бути використана для забезпечення доступу до ресурсів системи керування ключами тільки авторизованим об'єктам і авторизованим чином;

— **аудит.** Відстежування дій, що стосуються безпеки і виникають у системі керування ключами Журнали аудиту можуть допомогти визначити ризики та порушення безпеки;

— **автентифікація.** Цю послугу треба використовувати для встановлення об'єкта як авторизованого члена домена безпеки;

— **криптографічні послуги.** Ці послуги треба використовувати для забезпечення цілісності, конфіденційності, автентифікування та неспростовності послуги керування ключами;

— **послуга фіксування часу.** Ця послуга потрібна для генерування змінюваних із часом параметрів, таких як строк вірогідності.

5.2.2 *Послуги, орієнтовані на користувача*

Криптографічні системи і пристрої можуть потребувати інших послуг, потрібних для адекватного функціювання, таких як послуги реєстрування користувачів. Ці послуги залежать від особливостей реалізацій не належать до сфери застосування цього стандарту.

6 КОНЦЕПТУАЛЬНІ МОДЕЛІ РОЗПОДІЛЕННЯ КЛЮЧІВ

Розподілення ключів між об'єктами може бути складним. На це впливає характер каналів зв'язку, залучені довірчі взаємовідносини та використовувані криптографічні методи. Об'єкти можуть зв'язуватися безпосередньо або опосередковано, можуть належати до одного або різних доменів безпеки, можуть використовувати або ні послуги довірчих органів. Наведені нижче концептуальні моделі показують, як ці різні випадки впливають на розподілення ключів та інформації.

6.1 Розподілення ключів між зв'язаними об'єктами

На взаємодію об'єктів впливають канали зв'язку, ступінь довіри між ними та використовувані криптографічні методи.

Існують канали зв'язку між об'єктами А і В, які бажають обмінятися інформацією з використанням криптографічних методів. Ці канали зв'язку показано на рисунку 3. Взагалі розподілення ключа має здійснюватися через безпечний канал, який логічно відрізняється від каналу передавання.

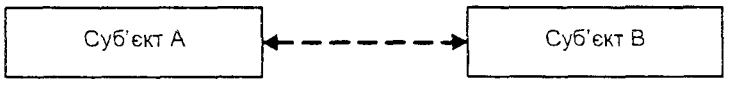

Рисунок 3 — Лінія зв'язку між двома об'єктами

Випадками безпосередньої взаємодії об'єктів є узгодження ключів, контролювання ключів та підтвердження ключів. Детальніше цей випадок наведено в ISO/IEC 11770-2 та ISO/IEC 11770-3.

6.2 Розподілення ключів у межах одного домена

Наведену нижче модель засновано на концепції домена безпеки з повноважним із безпеки згідно з ISO/IEC 10181-1.

Цей повноважний з безпеки може пропонувати такі послуги керування ключами, як передавання ключів. За умови використання об'єктами асиметричних методів для безпечного обміну інформацією можливі такі випадки:

— для цілісності або автентифікування джерела даних одержувач потребує відповідного сертифіката відкритого ключа відправника;

— для конфіденційності відправник потребує чинного сертифіката відкритого ключа одержувача;

— для автентифікування, конфіденційності та цілісності кожний партнер потребує сертифіката відкритого ключа іншої сторони. Це забезпечує засоби взаємної неспростовності.

Кожен об'єкт може потребувати взаємодії зі своєю повноважною організацією з сертифікування для одержання відповідного сертифіката відкритого ключа. Якщо пов'язані партнери довіряють одне одному і можуть провести взаємну автентифікацію сертифікатів їхніх відкритих ключів, то жодна повноважна організація з сертифікування не потрібна.

Примітка. Існують криптографічні застосунки, в яких не застосовують жодної повноважної організації з сертифікування. У цьому випадку пов'язані партнери можуть лише здійснити безпечний обмін спеціальною відкритою інформацією замість сертифікатів їхніх відкритих ключів

У разі використання симетричних методів між двома такими партнерами генерування ключів розпочинається одним із таких способів:

1) генеруванням ключа одним із об'єктів і відсиланням його до центру передавання ключів (ЦПК);

2) запитом одного із об'єктів до центру передавання ключів стосовно генерування ключа для подальшого розподілення.

Якщо генерування ключів виконує один із об'єктів, безпечне розподілення ключа може виконуватися центром передавання ключів як показано на рисунку 4. Цифри зображують кроки обміну. ЦПК одержує зашифрований ключ від об'єкта А (1), розшифровує його і повторно зашифровує його, використовуючи ключ, розподілений між ним та об'єктом В. Потім він може або переслати зашифрований ключ об'єкту В (2), або відправити його назад об'єкту А (3), який перешле його об'єкту В (4).

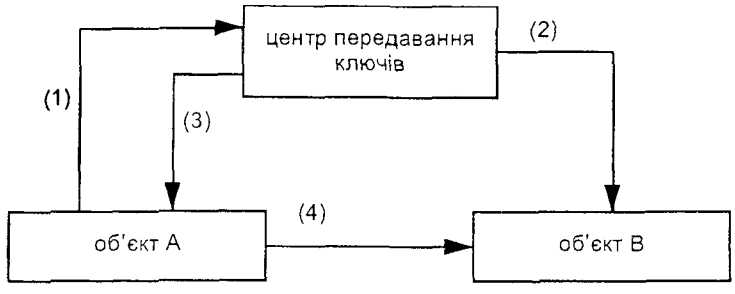

Рисунок 4 — Центр передавання ключів

Якщо генерування ключів здійснює третя довірча сторона, то існують два варіанти подальшого розподілення ключа пов'язаним партнерам. Ці випадки проілюстровані на рисунку 5 «Концептуальна модель центра розподілення ключів» та на рисунку 6 «Розподілення ключів пересиланням ключа від об'єкта А до об'єкта В». На рисунку 5 проілюстровано випадок, коли центр розподілення ключів спроможний безпечно зв'язуватися з обома об'єктами. У цьому випадку, як тільки ключ згенеровано за запитом одного з об'єктів, центр розподілення ключів несе відповідальність за безпечне розподілення ключа обом об'єктам. (1) — зображення запиту розподіленого ключа, а (2а) і (2в) — розподілення ключа пов'язаним партнерам.

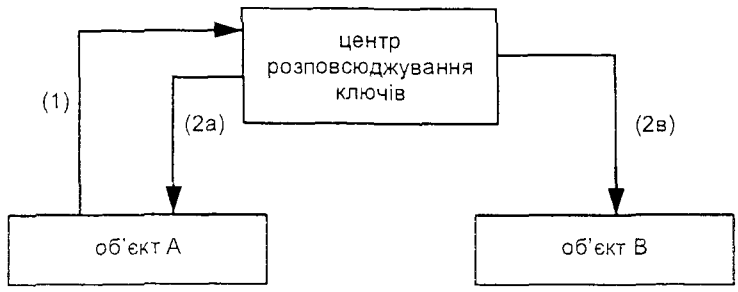

Рисунок 5 — Концептуальна модель центру розподілення ключів

Якщо тільки об єкт А формує запит розподілення таємного ключа між об'єктами А і В, орган може діяти двома різними способами Якщо він може безпечно зв'язатися з обома об'єктами, він може розповсюдити таємний ключ обом об'єктам, як це зазначено вище Якщо орган може зв'язатися тільки з об'єктом А, то об'єкт А відповідає за розподілення ключа об'єкту В На рисунку 6 зображено цей спосіб розподілення ключа (1) зображує запит розподіленого ключа , а (2) — його розподілення об'єкту А (3) зображує пересилання ключа від А до В

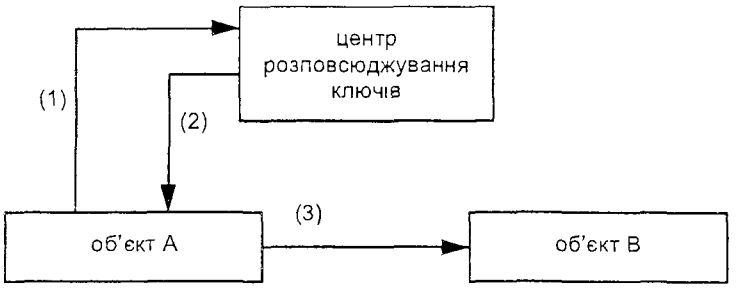

Рисунок 6 — Розподілення ключа пересиланням ключа від об'єкта А до об'єкта В

6.3 Розподілення ключів між доменами

Ця модель містить два об'єкти А і В, що належать двом різним доменам безпеки, які поділяють принаймні один криптографічний метод (тобто симетричний або асиметричний) Кожний домен безпеки має свого власного повноважного з безпеки одного, якому довіряє А, іншого, якому довіряє В Якщо А і В або довіряють один одному, або кожний довіряє повноважному іншого домена, то ключі розподіляють відповідно до 6 1 або 6 2

Розрізняють два випадки встановлення ключа між А і В

— одержання сертифіката відкритого ключа В (якщо застосовне),

— встановлення розподіленого таємного ключа між А і В

Між цими компонентами можливі різні ключові відносини, що відображають сутність довіри між компонентами

У випадку використання об'єктами для обміну інформацією асиметричних методів і відсутності доступу до загальної послуги довідників, яка надає сертифікати відкритих ключів, кожний об'єкт має зв'язуватися зі своїм відповідним повноважним для одержання сертифіката відкритого ключа партнера (відповідно до рисунку 7 (1)) Повноважні об'єктів А і В обмінюються сертифікатами відкритих ключів об єктів А і В (2) і пересилають їх до А і В (3) Після цього А і В можуть безпосередньо здійснювати безпечний зв'язок (4)

Іншим підходом до обміну сертифікатами відкритих ключів є перехресне сертифікування (відповідно до додатка D)

Якщо об єкти зв'язуються з використанням симетричних методів, кожний об єкт має також безпечно взаємодіяти із своїм відповідним повноважним (1) для одержання таємного ключа, який дозволить їм зв'язатися Повноважні з безпеки домовляються про спільний таємний ключ (2), який використовуватимуть об єкти Один повноважний розподіляє таємний ключ обом об'єктам, використовуючи іншого повноважного як центр розподілення Останній може також забезпечити пересилання ключа ((2) і (3))

Якщо тільки об єкт А формує запит таємного ключа для зв'язку з об'єктом В то повноважний з безпеки може діяти двома способами Якщо він може зв язатися з обома об'єктами він може розподілити таємний ключ їм обом, як це зазначено вище Якщо повноважний з безпеки може зв язатися тільки з одним об єктом, то об'єкт що одержує ключ, несе відповідальність за пересилання ключа іншому об єкту

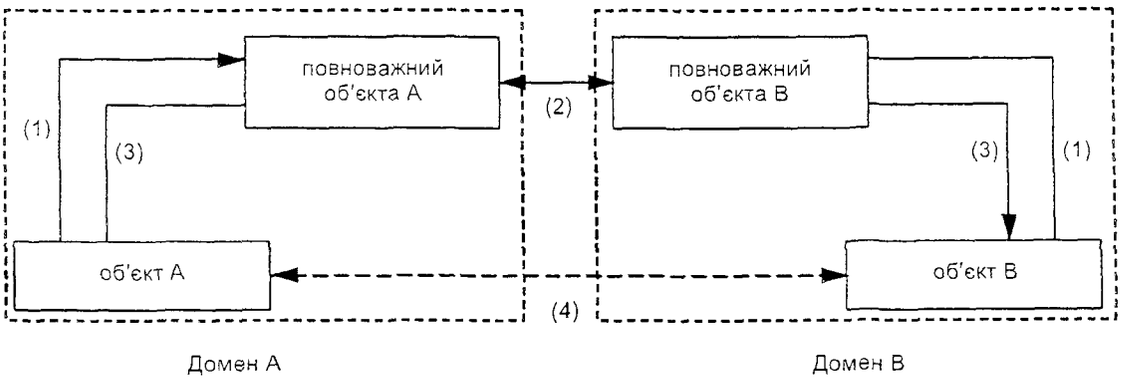

Рисунок 7 — Розподілення ключів між двома доменами

Інколи повноважні об'єктів А і В не мають ані взаємних довірчих відносин, ані безпосередніх каналів зв'язку. В цьому випадку вони мають залучити повноважного з безпеки X, якому вони обоє довіряють, як це показано на рисунку 8 (стрілки (2a) і (2b)). Повноважний X може згенерувати ключ і розподілити його повноважним об'єктів А і В (рисунок 8, стрілки (3a) і (3b)). Або повноважний X може переслати одержаний таємний ключ, або сертифікат відкритого ключа (2a) від повноважного з безпеки об'єкта А до повноважного з безпеки об'єкта В (3b). Повноважні мають потім переслати одержаний ключ їхнім відповідним об'єктам (згідно з рисунком 8, (4a) і (4b)), які потім можуть безпечно обмінюватися інформацію (5). Можливо, для встановлення ланцюга довіри треба буде провести пошук повноважних із безпеки, які б задовольняли вимогам.

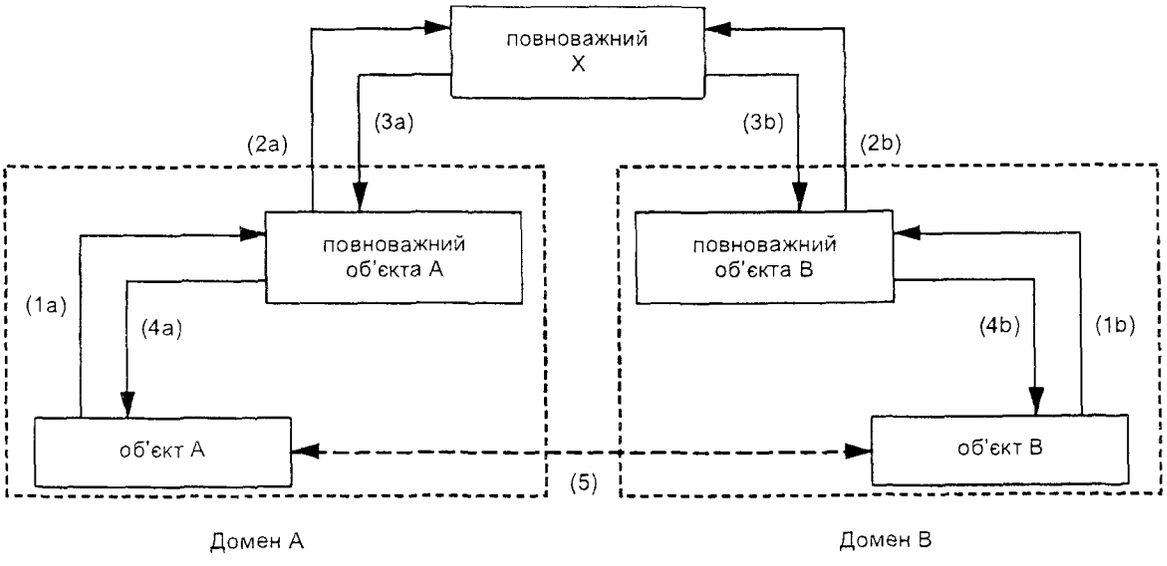

Рисунок 8 — Ланцюг довіри між органами

7 СПЕЦІАЛЬНІ ПОСТАЧАЛЬНИКИ ПОСЛУГ

Деякі послуги, яких потребує система керування ключами, можуть бути надані зовнішнім постачальником послуг. Такі послуги можуть надавати:

— повноважний реєстратор ключів або повноважна організація з сертифікування ключів;
— центр розподілення ключів згідно з ISO/IEC 8732;
— центр пересилання ключів згідно з ISO/IEC 8732.

ДОДАТОК А
(довідковий)

ЗАГРОЗИ КЕРУВАННЮ КЛЮЧАМИ

Керування ключами вразливе до низки загроз, перелік яких наведено нижче

Розкриття ключових даних: ключові дані або є відкритим текстом, незахищеним і до нього може бути здійснено доступ, або його зашифровано, але його можна розшифрувати

Модифікування ключових даних: зміна ключових даних таким чином, що їх не можна використовувати так, як передбачено

Неавторизоване знищення ключових даних: знищення ключа або пов язаних із ним даних

Неповне знищення ключових даних: це може спричинити компрометацію поточних або майбутніх ключів

Неавторизоване відкликання: безпосереднє або опосередковане вилучення чинного ключа або ключових даних

Імітування: знеособлювання авторизованого користувача або об'єкта

Затримування виконання функцій керування ключами: це може спричинити відмову генерування, розподілення, відкликання або реєстрування ключа, відмову вчасного оновлення сховища ключів або відмову підтримування рівнів авторизації користувача тощо Загроза затримування може виникати через будь-яку із зазначених вище загроз або через фізичну відмову ключового обладнання

Зловживання ключами:

— використання ключа в неавторизованих цілях, а саме використання ключа шифрування для ключа шифрування даних,

— використання засобу керування ключами в неавторизованих цілях, а саме неавторизоване зашифровування або розшифровування даних,

— використання ключа після закінчення строку його дії,

— надмірне використання ключа,

— надання ключів неавторизованим одержувачам

ДОДАТОК В
(довідковий)

ІНФОРМАЦІЙНІ ОБ'ЄКТИ КЕРУВАННЯ КЛЮЧАМИ

Інформаційний об'єкт керування ключами містить ключ (або ключі) разом із необов'язково, іншою інформацією, що контролює можливе використання ключів Скоріше ніж у явній формі інформація контролю може зумовлюватися домовленостями, які контролюють використання інформаційних об єктів керування ключами (Наприклад, використання одного ключа асиметричної шифрувальної пари контролюється узгодженим використанням іншого одного — для зашифровування, а іншого — для розшифровування)

За допомогою контролівної інформації можна відстежувати таке

— тип об єкта, який може захищати ключ (а саме дані або інформаційний об єкт керування ключем)

— допустимі операції (а саме зашифровування, розшифровування),

— допущеного користувача,

— середовище, у якому може бути використано ключ,

— інші аспекти, особливі для певного методу контролювання або застосунку, які використовують інформаційний об єкт керування ключем

Для оптимізування інформаційний об єкт керування ключем може частково або повністю бути створений у процесі генерування ключа

Конкретним прикладом інформаційного об єкта керування ключем є сертифікат ключа Він містить щонайменше підписані повноважною організацією з сертифікування

— ключові дані

— ідентифікатор користувача який може використовувати відповідний інформаційний об єкт керування ключем,

— операції, що виконує відповідний інформаційний об єкт керування ключем (можуть бути задачі в неявному вигляді),

— строк дії;

— ідентифікатор повноважної організації з сертифікування.

Наведені нижче ASN.1 — визначення є прикладом інформаційного об'єкта керування ключем, хоча він може містити інші параметри залежні від застосування.

```
Key          ::=  PROTECTED {KeyContents, protectionType};
KeyContents  ::=  SEQUENCE     {
                  key ID           [0]  Key_Identity,
                  keyValue         [1]  Key_Value,
                  checkValue       [2]  Check_Value,
                  cryptoMethod     [3]  Cryptographic_Method,
                  timeStamp        [4]  Time_Stamp,
                  generAuthority   [5]  Generating_Authority,
                  certiAuthority   [6]  Certification_Authority,
                  issuer           [7]  Issuer,
                  validity         [8]  Validity_of_Key};
```

Він складається з параметрів KeyID (однозначний ідентифікатор), KeyValue (значення ключа) і CheckValue (контролювальне значення), де обов'язковим є тільки KeyValue. Параметри CryptoMethod, Issuer і Validity контролюють використання ключа, обмежуючи його спеціальними алгоритмами, часом використання і певними користувачами. Ці параметри є важливі для контролювання використання ключа, але необов'язкові. Параметри GenerAuthority, CertiAuthority і TimeStamp важливі для доказу авторства джерела ключа, строку дії, але також є необов'язкові. Для сертифіката ключа обов'язковим є параметр Issuer.

ДОДАТОК С
(довідковий)

КЛАСИ КРИПТОГРАФІЧНИХ ЗАСТОСУНКІВ

Загальну класифікацію криптографічних систем визначають два основні використовувані методи, а саме: симетричний і асиметричний. Внаслідок того що керування ключами має обслуговувати обидва методи, непотрібен інший підхід. Тому в наступному розділі криптографічні системи класифіковано відповідно до функційності, яку забезпечує метод.

У загальному випадку криптографічна система пропонує два різні типи криптографічних послуг: послуги автентифікування та послуги шифрування. Послуги шифрування використовують для криптографічного захисту інформації, тобто вони забезпечують конфіденційність даних. Послуги автентифікування переважно використовують для автентифікування об'єктів, автентифікування джерела даних, цілісності даних та неспростовності. Типи криптографічних систем та відповідні операції показано на рисунку С.1.

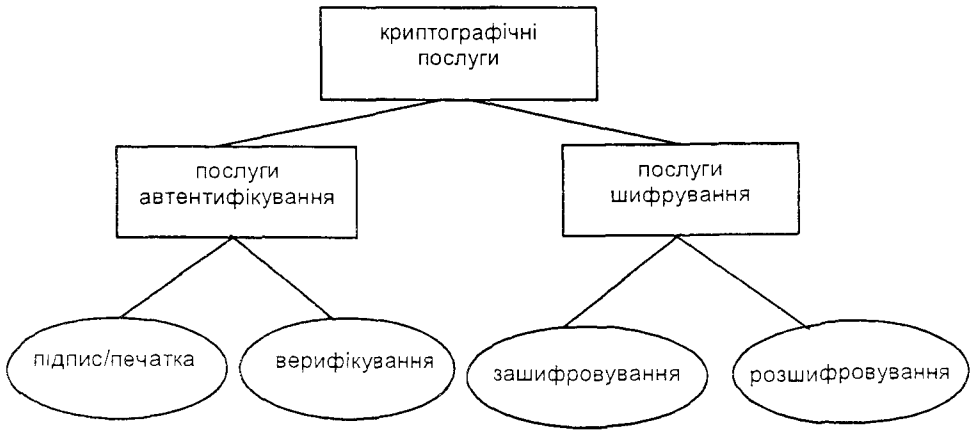

Рисунок С.1 — Криптографічні послуги і відповідні механізми

С.1 Послуги автентифікування та ключі

Послуги автентифікування забезпечують автентифікування зв'язаних об єктів (автентифікування об єктів) автентифікування джерела даних (автентифікування походження даних), неспростовність та цілісність даних Ця послуга може використовувати такі механізми

— **"запечатати блок даних",** який для цілісності даних містить правило виведення криптографічної контролювальної величини даних, а саме генерування за допомогою симетричного алгоритму коду автентифікування повідомлення (MAC),

— **"підписати блок даних",** який містить генерування цифрового підпису для автентифікування джерела даних, цілісності даних та (або) неспростовності,

— **"верифікування запечатаного блоку даних",** який містить обчислення криптографічної контролювальної величини даних, та порівняння її з еталонною контролювальною величиною (доказ цілісності даних),

— **"верифікування підписаного блоку даних",** який містить верифікацію цифрового підпису для виявлення, чи був він вироблений заявленим відправником і (або) доказ цілісності даних

У послугах автентифікування процеси підписування та запечатування використовують інформацію, яка є або особистою (тобто унікальною і конфіденційною) інформацією відправника, або таємною і відомою тільки відправнику і одержувачу, процес верифікування використовує або процедури та інформацію, які є загальнодоступними, але з яких не може бути виведена особиста інформація відправника, або розподілену таємну інформацію відправника і одержувача Істотною характеристикою підписування є те, що підпис може бути вироблений лише з використанням особистої інформації відправника, його особистого ключа Таким чином, якщо підпис верифікують із використанням відкритого ключа джерела, то потім можна довести третій стороні (повноважному нотаріусу), що тільки єдиний власник особистої інформації міг виробити цей підпис

Послуга автентифікування використовує два з трьох типів ключів

— **ключ запечатування** — розподілений таємний ключ,

— **ключ підписування** — унікальний особистий ключ, асоційований з джерелом;

— **ключ верифікації** — або відкритий ключ, або таємний ключ

У симетричних методах послуга автентифікування використовує ключ запечатування і ключ верифікації, подані тим самим таємним ключем, в асиметричних методах вона використовує ключ підписування та ключ верифікації, подані ключовою парою, яка складається з відкритого та особистого ключів

С.2 Послуги шифрування та ключі

Послуги шифрування забезпечують в основному конфіденційність інформації, але також і цілісність даних Залежно від використовуваних методів застосовують послуги щодо безпеки автентифікування і неспростовність

Використовують два основних механізми:

— **зашифровування,** виробляє зашифрований текст за вхідними даними

— **розшифровування,** виробляє відкритий текст із відповідного зашифрованого тексту

Послуга шифрування може бути охарактеризована використаним криптографічним методом а саме симетричним або асиметричним Якщо використовують симетричний метод операції зашифровування і розшифровування виконують з одним ключем (розподілений таємний ключ) Якщо використовують асиметричний метод, операції зашифровування і розшифровування виконують із двома різними, але взаємопов язаними ключами, тобто відкритим і особистим ключами

ДОДАТОК D
(довідковий)

КЕРУВАННЯ ЖИТТЄВИМ ЦИКЛОМ СЕРТИФІКАТА

Цей довідковий додаток описує вимоги та процедури, застосовні в керуванні життєвим циклом сертифіката відкритого ключа.

D.1 Повноважна організація з сертифікування (CA)

CA є довірчою стороною своїх абонентів. Така довіра основана на використанні адекватних криптографічних механізмів і обладнання та на досвіді професійного керування і контролювання. Ця довіра має підтверджуватися незалежним аудитом (внутрішнім, зовнішнім чи обома), результати якого мають бути доступними для абонентів.

CA має нести відповідальність за:

1) ідентифікування об'єктів, інформацію про відкритий ключ яких надано для сертифікування;

2) забезпечення якості пари асиметричних ключів, використовуваних для формування сертифіката відкритого ключа;

3) захист процесу сертифікування, а також особистого ключа, використовуваного для підписування інформації щодо відкритого ключа;

4) керування системно-залежними даними, які мають містити інформацію щодо відкритого ключа — порядковий номер сертифіката відкритого ключа, ідентифікатор CA тощо;

5) призначення та перевіряння строку дії;

6) оповіщення об'єкта, ідентифікованого інформацією відкритого ключа, що сертифікат відкритого ключа видано. Засоби, використані для пересилання цього повідомлення, мають бути незалежними від методу, використаного для пересилання до CA інформації відкритого ключа;

7) забезпечення того, що два різних об'єкти не будуть тотожними і зможуть належним чином розпізнаватися;

8) супроводження та видання списків відкликання;

9) внесення до журналу всіх кроків процесу генерування сертифіката відкритого ключа.

Одна CA для видання сертифіката відкритого ключа може сертифікувати інформацію відкритого ключа іншої CA. Отже, автентифікування може містити ланцюг сертифікатів відкритих ключів. Перший сертифікат відкритого ключа в цьому ланцюгу має бути одержаним і автентифікованим деякими способами, відмінними від сертифікатів відкритих ключів.

D.1.1 *Асиметрична ключова пара повноважної організації з сертифікування*

CA повинен мати засіб безпечного керування ключами, спроможний генерувати асиметричну ключову пару для використання цією CA. Процес генерування має забезпечувати непередбачуваність ключових даних. Жоден зловмисник не повинен одержувати переваги від знання процесу генерування.

Особистий ключ CA використовують для підписування інформації відкритого ключа об'єкта. Має бути забезпечений високий рівень захисту особистого ключа CA, оскільки володіння ним дало б змогу зловмиснику маскуватися під CA і генерувати підроблені сертифікати відкритих ключів. Отже, особистий ключ CA має бути добре захищений під час використання всередині засобу керування ключами. Його треба вводити або виводити із засобу керування ключами захищеним та під контролем самої CA.

Суттєвою для безпеки системи сертифікування відкритих ключів є цілісність відкритого ключа верифікації CA. Якщо сертифікат відкритого ключа не містить відкритий ключ CA, то треба вжити спеціальних заходів для забезпечення його автентифікованого розподілення. На місцях користувачів має бути вжито заходи для забезпечення автентичності збереженої копії відкритого ключа CA.

Відкритий ключ верифікації CA використовують для підтвердження сертифікатів відкритих ключів інших користувачів. Перед кожним використанням відкритого ключа CA, користувач повинен упевнитися, що ключ верифікації є чинним на поточний момент.

D.2 Процес сертифікування

Цей розділ описує вимоги та процедури, застосовні в процесі сертифікування.

D.2.1 *Модель сертифікування відкритого ключа*

Цей розділ визначає базову модель сертифікування відкритих ключів. Модель розподіляє основні функції за логічними об'єктами (рисунок D.1):

1) повноважна організація з сертифікування (СА) — об єкт, що несе відповідальність за сертифікування інформації відкритого ключа об'єкта — користувача,

2) довідник (ДОВ) — об єкт, що несе відповідальність за надання інтерактивного доступу до сертифікатів відкритих ключів для оперативного використання їх об'єктами — користувачами,

3) генератор ключів (ГК) — об'єкт, що несе відповідальність за генерування асиметричної ключової пари,

4) повноважний реєстратор (ПР) — об'єкт, що несе відповідальність за забезпечення СА засвідченими ідентифікаторами користувачів,

5) об'єкт — користувач (А)

Нижче розглянуто відносини між логічними об єктами моделі та відповідні вимоги щодо безпеки стосовно цих відносин Логічні об'єкти можуть бути суміщеними Наприклад А і ГК можна об єднати, якщо об'єкт-користувач сам генерує асиметричну ключову пару, або СА і ГК можна об'єднати якщо СА генерує ключову пару для об'єкта — користувача

Примітка Треба подбати щоб сертифікат згенеровании об єднаними ПР і СА був однаковим із сертифікатом створеним розподіленими різними ПР і СА

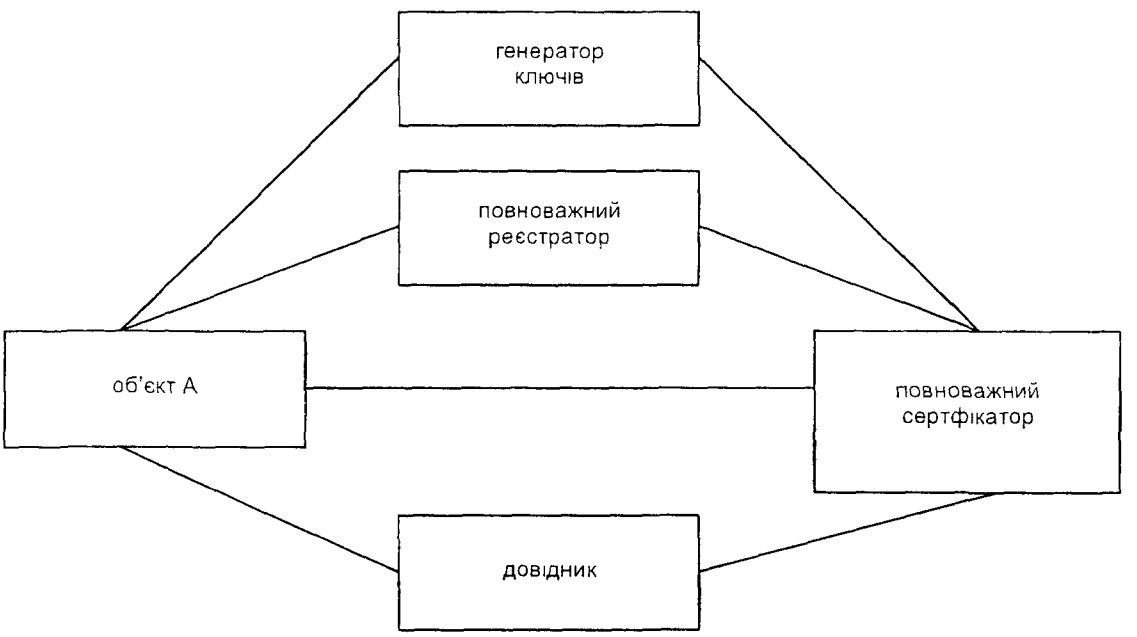

Рисунок D 1 — Базова модель сертифікування відкритих ключів

D.2.1.1 *Сертифікаційні відносини*

Цей розділ надає опис деяких сертифікаційних відносин базової моделі й відповідні вимоги щодо безпеки В окремій системній реалізації не всі відносини мають бути активними Наприклад, завдання ПР, СА і ГК можна об єднувати

А-ГК Об єкт А просить генератора ключів ГК згенерувати асиметричну ключову пару ГК довірене генерування асиметричних ключових пар високої якості ГК генерує ключову пару (S_A,V_A) таким чином, що S_A є ключем підписуванням, а V_A є ключем верифікації, і вертає їх А Це пересилання треба виконувати з автентифікуванням і конфіденційно ГК і А мають бути абсолютно впевненими в тому що під час пересилання третя сторона не зможе модифікувати асиметричну ключову пару та прочитати її значення

А-ПР Об'єкт А замовляє реєстрування у повноважного реєстратора ПР Об єкт А повинен подати свою особисту інформацію ПР ПР перевіряє автентичність інформації А і можливо додає деякі системно-залежні дані Інформацію після цього передають до СА безпечним шляхом

А-СА Об єкт А просить повноважну організацію з сертифікування сертифікувати його інформацію відкритого ключа (або її підмножину), зокрема його відкритий ключ та розпізнавальне ім я Подавання

інформації відкритого ключа до СА треба здійснювати із забезпеченням автентифікування і конфіденційності таким чином, щоб забезпечити його автентичність і цілісність. СА перевіряє автентичність інформації відкритого ключа А, можливо, додає системно-залежні дані й потім підписує повну інформацію відкритого ключа для виготовлення сертифіката відкритого ключа А. Сертифікат відкритого ключа потім може бути пересланий до А.

Після одержання виданого сертифіката відкритого ключа А верифікує його коректність із використанням відкритого ключа верифікації V_{CA} повноважної організації з сертифікування. Доступ А до цього відкритого ключа верифікації V_{CA} має бути автентифікованим. Починаючи з цього часу, відкритий ключ А можна розповсюджувати як сертифікат відкритого ключа і використовувати кожному, хто має доступ до відкритого ключа верифікації СА.

Проте, якщо повноважна організація з сертифікування просить ГК згенерувати асиметричну ключову пару для об'єкта А, то ключову пару об'єкта А має бути переслано від ГК до А. Вимогами щодо безпеки для пересилання є конфіденційність, цілісність та автентичність. Крім того, СА довірено зберігати конфіденційність, цілісність та автентичність усіх асиметричних ключових пар протягом оброблення та зберігання. І, нарешті, СА має пересилати до А його особистий ключ, будучи абсолютно впевненою у тому, що третя сторона не може ні модифікувати, ні прочитати величину, що пересилається.

А-ДОВ Об'єкт А пересилає сертифікат свого відкритого ключа в довідник ДОВ і реєструє його в довіднику. Для реєстрування сертифіката відкритого ключа в довіднику потрібно автентифікування об'єкта та контролювання доступу. Між А і ДОВ має бути узгоджено, хто уповноважений керувати записом стосовно цього об'єкта в довіднику. В одних застосунках довідник керує всіма довідниковими записами. В інших — кожний об'єкт Х відповідає за керування своїм довідниковим записом.

ПР-СА ПР просить СА сертифікувати інформацію відкритого ключа А. Пересилання інформації відкритого ключа А від ПР до СА треба виконувати з автентифікацією. СА верифікує автентичність інформації відкритого ключа А, можливо, додає системно-залежні дані й потім підписує повну інформацію відкритого ключа, щоб виробити сертифікат відкритого ключа А. СА повідомляє ПР про сертифікацію.

СА-ГК Повноважна Організація з сертифікування СА просить генератора ключів ГК згенерувати асиметричну ключову пару для об'єкта А. ГК довірено генерувати асиметричні ключові пари високої якості. ГК генерує ключову пару і пересилає її до СА. Це пересилання треба виконувати з автентифікуванням і конфіденційно. ГК і СА має бути абсолютно впевненими в тому, що третя сторона не може ні модифікувати асиметричну ключову пару, ні прочитати величини під час пересилання. СА довірено зберігати конфіденційність і автентичність усіх асиметричних ключових пар протягом оброблення і зберігання.

СА-ДОВ СА пересилає вироблені сертифікати відкритих ключів безпосередньо в довідник ДОВ і реєструє їх у довідникові. Для реєстрування сертифікатів відкритих ключів у довіднику потрібно автентифікування об'єкта і контролювання доступу.

D.2.2 ***Реєстрування***

Реєстрування ключа об'єкта охоплює подання об'єктом запиту на сертифікування та його підтвердження ПР або СА. У наступних підпунктах наведено вимоги щодо подання об'єктом запиту на сертифікацію. Запит на сертифікування може містити чи не містити величину відкритого ключа.

D.2.2.1 *Подання запиту на сертифікування фізичними особами*

Для застосунків із низьким ступенем ризику прийняття запиту на сертифікування має базуватися на ідентифікуванні особи, яка звернулася за сертифікатом відкритого ключа. Самі запити на сертифікування не треба подавати особисто, але треба використовувати прийнятну ділову практику для ідентифікування цих осіб.

Для застосунків із високим ступенем ризику прийняття запиту на сертифікування має базуватися на особистій появі (або на появі повноважного агента) особи, що звертається за сертифікатом відкритого ключа, і використанні прийнятних комерційних стандартів для ідентифікування особи (і агента цієї особи, за потреби) Це може передбачати верифікування тотожності третьою довірчою стороною.

D.2.2.2 *Подання юридичною особою запиту на сертифікацію*

Приймання запиту на сертифікування повинно базуватися на доставленні інформації запиту на сертифікування врученням її принаймні одним представником об'єкта і:

1) Підписі й печатці (якщо застосовне) на титульному аркуші, якими завірено запит на сертифікат відкритого ключа

2) Використанні прийнятної комерційної практики ідентифікування підпису і печатки (якщо застосовне) об єкта

3) Використанні прийнятної комерційної практики ідентифікування представників які доставили інформацію запиту на сертифікування

D.2.3 ***Взаємовідносини між юридичними особами***

У юридичних осіб може виникнути потреба у встановленні договірних відносин з іншими юридичними особами Це може бути влаштовано різними способами

1) Службовці компанії мають власні асиметричні ключові пари Юридична особа діє як СА для своїх службовців Транзакції авторизуються службовцями з використанням їхніх персональних ключів, сертифікованих СА компанії Одержувачі перевіряють, що джерело сертифіковане компанією, відкритий ключ якої, в свою чергу сертифікований СА вищого рівня ієрархії

2) Службовці компанії не мають власних асиметричних ключових пар Тільки юридична особа має одну або більше асиметричних ключових пар Одержувачі відкритим ключем компанії перевіряють узгодженість транзакцій Одержувачі не повинні обтяжувати себе ієрархією і політикою повноважень компанії-джерела

D.2.4 ***Генерування сертифіката***

Будь-якому використанню асиметричної ключової пари передує процес генерування сертифіката відкритого ключа

Процес генерування сертифіката має містити такі кроки

1) Перевіряння інформації відкритого ключа для виявлення помилок

2) Прийняття інформації відкритого ключа (вимоги стосовно приймання інформації відкритого ключа відповідно до D 2 2)

3) Підготовляння та долучення даних потрібних для керування сертифікатом відкритого ключа СА може генерувати асиметричну(і) ключову(і) пару(и) для об єкта (необов язково)

4) Обчислення підпису для сертифіката відкритого ключа Може містити геш-функцію

5) Запис до журналу аудиту Дії СА щодо генерування сертифіката відкритого ключа мають бути занесені до журналу

Для застосунків із високим ступенем ризику може бути бажаним до (1) вимагати декількох підписів СА на сертифікаті відкритого ключа, які містять підписи, виконані незалежними криптографічними засобами (з різними особистими ключами), або до (2) вимагати декількох підписів інформації відкритого ключа різними СА

D.2.5 ***Відновлення/Життєвий цикл***

Життєвий цикл сертифіката відкритого ключа зазначено строком дії, встановленим у сертифікаті відкритого ключа або визначено іншим чином політикою керування СА

D.3 Розподілення та використання сертифікатів відкритих ключів

Цей розділ описує вимоги та процедури, застосовні до розподілення та використання сертифікатів відкритих ключів

D.3.1 ***Розподілення та зберігання сертифікатів відкритих ключів***

Після генерування сертифіката відкритого ключа не треба спеціальних заходів для забезпечення його конфіденційності або цілісності Сертифікати відкритих ключів можуть зберігатися у відкритому довіднику для зручного доступу до них користувачів

D.3.2 ***Верифікування сертифікатів відкритих ключів***

Для підтвердження сертифіката відкритого ключа суб'єкт В який виконує верифікування має принаймні перевірити підпис СА на сертифікаті відкритого ключа Якщо сертифікат відкритого ключа має призначений строк дії то В має упевнитися що інформація відкритого ключа суб єкта А чинна на поточний момент (відповідно до D 5) Для верифікування сертифіката відкритого ключа верифікатор повинен мати чинну копію відкритого ключа верифікації СА

D 4 Способи сертифікування

Не має потреби знати всі СА та їхніх абонентів як немає потреби знати всю ієрархію СА Бажано щоб для забезпечення гнучкого використання і обміну сертифікатами відкритих ключів СА серти-

фікували один одного (перехресне сертифікування). Це перехресне сертифікування треба виконувати з використанням високих рівнів гарантій і точних регламентів. Якщо наявна мережа перехресних сертифікатів відкритих ключів, то можуть бути побудовані шляхи їх підтвердження. Користувач повинен тільки мати довіру до ключа верифікації одного органу сертифікування. Через сертифікаційний шлях ця довіра поширюється на відкриті ключі партнерів, виготовлені невідомим органом сертифікування.

D.5 Відкликання сертифіката

Сертифікати можуть бути відкликані повноважною організацією з сертифікування, що їх виготовила, до закінчення строку дії. Це може статися через низку причин, в тому числі таких:

1) Компрометація особистого ключа об'єкта.
2) Запит об'єкта про скасування.
3) Зміна приналежності об'єкта.
4) Припинення дії об'єкта.
5) Помилкова ідентифікація об'єкта.
6) Компрометація особистого ключа СА.
7) Припинення дії СА.

Відповідно мають існувати процедури і засоби швидкого зв'язку для полегшення безпечного і автентифікованого скасування:

1) Одного або більше сертифікатів відкритих ключів одного або кількох об'єктів.

2) Множини всіх сертифікатів відкритих ключів, виданих СА на базі одної пари асиметричних ключів, яку повноважна організація з сертифікування використала для підписування інформації відкритого ключа.

3) Усіх сертифікатів відкритих ключів, виданих СА безвідносно до використаних пар асиметричних ключів.

Дві останні вимоги забезпечують засоби відкликання сертифікатів відкритих ключів, якщо сталася або підозрюють компрометацію особистого ключа СА, або коли змінено пару асиметричних ключів, використовуваних для підписування сертифікатів відкритих ключів. Якщо строк дії сертифікатів відкритих ключів вичерпано або вони відкликані, їхні копії має зберігати третя довірча сторона протягом часу, встановленого практикою використання, законами і нормативними актами.

Коли особистий ключ об'єкта або СА відкликано з будь-яких причин, СА-видавець цього сертифіката відкритого ключа повинен негайно вжити заходів для оповіщення всіх суб'єктів системи щодо відкликання будь-яких відповідних сертифікатів відкритих ключів. Це може мати місце у формі автентифікованого СА повідомлення, розісланого всім суб'єктам, повідомлення, автентифікованого іншим СА, веденням третьою довірчою стороною інтерактивного списку відкликаних сертифікатів відкритих ключів або навіть опублікуванням списку відкликаних чи дійсних сертифікатів.

Коли сертифікат відкритого ключа відкликаний через підозру або фактичну компрометацію особистого ключа, особистий ключ не треба більше ніколи використовувати. Сертифікат відкритого ключа можна використовувати лише з метою верифікування із забезпеченням того факту, що дані підписані до відкликання. Більше того, будь-які ключові дані, зашифровані цим сертифікатом відкритого ключа (безвідносно до типу), мають бути негайно скасованим.

Якщо закінчився строк дії сертифіката відкритого ключа або він відкликаний з причин, непов'язаних із підозрою або фактичною компрометацією, особистий ключ не треба більше ніколи використовувати. Сертифікат відкритого ключа все ще можна використовувати для верифікування та розшифровування. Всі відправлені і захищені цим сертифікатом відкритого ключа ключові дані (безвідносно до типу) мають бути замінені якнайшвидше.

D.5.1 *Списки відкликання*

Список відкликання містить список із часовими познаками серійних номерів або ідентифікатори тих сертифікатів відкритих ключів, що були відкликані СА. У списку відкликання можна використовувати два види часових познак:

1) Дата і час видання відкликання СА;

2) Дата і час підозрюваної або фактичної компрометації.

Остання дата (якщо вона відома) полегшує аудит підозрілих повідомлень. Сертифікат відкритого ключа залишають у списку відкликання щонайменше, до закінчення строку його дії. Часова познака важлива, тому що має бути відомо, в який час зв'язок відкритого ключа і об'єкта був розірваний.

Після відкликання з причини підозрюваної або фактичної компрометації, інформацію, підписану з використанням відповідного особистого ключа, не можна більше вважати чинною, якщо підпис був виконаний після дати можливої компрометації, або дата підпису не може бути надійно встановлена Інформацію не можна шифрувати з використанням відкликаного відкритого ключа

Список відкликань має.

1) Бути датованим і підписаним СА так, щоб об єкти могли підтвердити цілісність списку і дату розповсюдження,

2) Регулярно видаватися СА, навіть якщо не сталося змін з моменту останнього видання,

3) Бути доступним для всіх об'єктів системи, за винятком можливих перешкод, а саме законам нормативним актам або припису суду

Для розподілення списків відкликання можливі різні механізми в тому числі

1) доставлення кожному користувачеві повідомлення/транзакції третьою довірчою стороною

2) запити користувача до третьої довірчої сторони щодо поточного статусу певного сертифіката відкритого ключа,

3) запит до СА щодо його поточного списку відкликання

Повноважна організація з сертифікування має періодично публікувати і розповсюджувати новий список відкликань

ДОДАТОК Е
(довідковий)

БІБЛІОГРАФІЯ

ISO 8732 1988 Banking — Key management (wholesale)

ISO/I EC 9594-8 1990 Information technology — Open Systems Interconnection — The Directory — Part 8 Authentication framework

ISO/IEC 10116 1991 Information technology — Modes of operation for an n-bit block cipher algorithm

ISO 11166-1 1994 Banking — Key management by means of asymmetric algorithms — Part 1 Principles, procedures and formats

ISO 11568-1 1994 Banking — Key management (retail) — Part 1 Introduction to key management

ISO 11568-2 1994 Banking — Key management (retail) — Part 2 Key management techniques for symmetric ciphers

ISO 11568-3 1994 Banking — Key management (retail) — Part 3 Key life cycle for symmetric ciphers

ISO 11568-4[1)] Banking — Key management (retail) — Part 4 Key management techniques for public key cryptosystems

ISO 11568-5[1)] Banking — Key management (retail) — Part 5 Key life cycle for public key cryptosystems

ISO/IEC 11770-2 1996 Information technology — Security techniques — Key management — Part 2 Mechanisms using symmetric techniques

ISO/IEC 11770-3[1)] Information technology — Security techniques — Key management — Part 3 Mechanisms using asymmetric techniques

ISO/IEC 13888[1)] Information technology— Security requirements — Non-repudiation (all parts)

НАЦІОНАЛЬНЕ ПОЯСНЕННЯ

ISO 8732 1988 Банківська справа Керування ключами (опт)

ISO/IEC 9594-8 1990 Інформаційні технології Взаємодія відкритих систем Каталоги Частина 8 Схема автентифікування

ISO/IEC 10116 1991 Інформаційні технології Види операцій алгоритму шифрування n-бітового блоку

ISO 11166-1 1994 Банківська справа Керування ключами за допомогою асиметричних алгоритмів Частина 1 Принципи, процедури і формати

ISO 11568-1 1994 Банківська справа Керування ключами (роздріб) Частина 1 Вступ до керування ключами

[1)] Буде опубліковано

ISO 11568-2:1994 Банківська справа. Керування ключами (роздріб). Частина 2. Методи керування ключами для симетричного шифрування

ISO 11568-3:1994 Банківська справа. Керування ключами (роздріб). Частина 3. Життєвий цикл ключів для симетричного шифрування

ISO 11568-4:1994 Банківська справа. Керування ключами (роздріб). Частина 4. Методи керування ключами для криптосхем з відкритим ключем

ISO 11568-3:1994 Банківська справа. Керування ключами (роздріб). Частина 5. Життєвий цикл ключів для криптосхем із відкритим ключем

ISO/IEC 11770-2.1996 Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням симетричних методів

ISO/IEC 11770-3 Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми з використанням асиметричних методів

ISO/IEC 13888 Інформаційні технології. Вимоги щодо безпеки. Неспростовність (всі частини).

Код УКНД 35.040

Ключові слова: захист інформації, керування ключами, криптографія, методи захисту, обмін інформацією оброблення даних.