Розділ 8

ІНФРАСТРУКТУРИ ВІДКРИТИХ КЛЮЧІВ ТА СЕРТИФІКАЦІЇ АТРИБУТІВ РОЗВИНЕНИХ ДЕРЖАВ

8.1. СТАН СТВОРЕННЯ, СТРУКТУРА ТА ЗАСТОСУВАННЯ ІВК В США

8.1.1. Історична довідка, стан і загальні проблемні питання впровадження ІВК в США

США є однією з перших країн, яка створила та почала широко використовувати системи ІВК на рівні федеральних агенцій, відомств, великих корпорацій тощо. Ще в 1994 році з метою визначення підходів до побудови федеральної ІВК корпорація MITRE за замовленням NIST провела перші фундаментальні дослідження різних систем ІВК [221]. За результатами досліджень було встановлено, що під час створення федеральної ІВК необхідно вирішити ряд проблем щонайменше в шести напрямках, різного характеру та спрямованості, на різних рівнях представлення.

До першого напрямку належать проблеми законодавчого та нормативно-правового врегулювання взаємовідносин сторін, що беруть участь у створенні та застосуванні ІВК. До них безпосередньо необхідно віднести розробників, постачальників і користувачів послуг сертифікації, а також третіх довірчих сторін.

До другого напрямку належать проблеми загальносистемного рівня, перш за все щодо обґрунтування вибору архітектури ІВК з урахуванням завдань, що вирішуються на рівні держави, відомств, федеральних агенцій та організацій, установ тощо. До них з часом долучилися проблеми загальносистемного рівня, що виникли на міжнародному та міждержавному рівнях.

До третього напрямку можна віднести проблеми процедурно-функціонального рівня, які здебільшого полягають у визначенні та закріпленні основних функціональних вимог до системи сертифікації, політик (правил) обробки сертифікатів, надання відповідних послуг виготовлення та обслуговування сертифікатів відкритих ключів тощо.

До четвертого напрямку можна віднести проблеми функціонально-технічного рівня, перш за все в частині визначення функціональної структури центрів сертифікації, їх фізичної та структурної топології, визначення функціональних вимог безпеки у відповідності з вимогами гарантій якості надання послуг сертифікації.

П'ятий напрям пов'язаний із вирішенням сугубо технічних проблем, які належать до вибору й ефективної реалізації апаратних, програмно-апаратних і програмних засобів та устаткування центрів сертифікації, засобів криптографічного захисту інформації, криптографічних протоколів і технічних специфікацій.

Шостий напрям пов'язаний із проблемами несумісності, які по суті виникли в процесі впровадження ІВК у федеральних і комерційних відомствах та організаціях і зводиться здебільшого до неузгодженості технічних специфікацій і криптографічних протоколів та параметрів криптографічних перетворень.

Результати аналізу вирішення проблем за визначеними напрямками надані в технічному звіті корпорації MITRE [221]. У звіті розглянуто альтернативні варіанти архітектури ІВК та центрів сертифікації, класифікація процедур обробки сертифікатів. Важливим результатом є дослідження вартості експлуатації системи ІВК США в загальнодержавному масштабі.

Щодо стандартизації, то вже з 1994 року США орієнтується на побудову федеральної ІВК на основі відкритих стандартів. Структури даних визначаються стандартом X.509, що детально розглянутий у 7 розділі цієї роботи [13, 14].

У 2001 році агенцією U.S. General Accounting Office США підготовлено звіт про стан впровадження технологій ІВК у федеральних структурах. У звіті зазначається, що «за 7 років федеральні відомства не наблизилися до будь-якого загальнодержавного стандарту розроблення й управління ІВК» [51, 65, 66, 68, 81].

Також необхідно відзначити, що федеральні відомства США на перших етапах вибору структури відомчої ІВК мали достатню свободу. При цьому федеральна ІВК будувалася способом об'єднання різноманітних систем ІВК, які знаходились у власності різних відомств, агенцій та організацій. Указаний підхід дозволив створювати ефективні корпоративні й відомчі системи, які оперативно вводилися в дію, але при цьому суттєво ускладнювалася можливість і строки побудови загальнодержавної ІВК.

Основними проблемами й протиріччями, що виникли та до цих пір перешкоджають впровадженню ІВК на федеральному рівні [65–66, 68, 81, 221–222], стали такі:

– забезпечення інтероперабельності різних систем ІВК, що експлуатуються у відомствах та агенціях;

– достатньо висока вартість створення й експлуатації ІВК;

– взаємодія відомчих ІВК та федерального мостового центру сертифікації;

– недостатня узгодженість політик і принципів функціонування ІВК;

– необхідність постійної підготовки та перепідготовки персоналу та користувачів систем ІВК.

Під *інтероперабільністю* взагалі розуміють здатність систем здійснювати обробку інформації між собою та використовувати оброблену відповідним чином інформацію. Проблема інтероперабельності виникає через те, що розробники й постачальники продуктів ІВК використовують стандарти та специфікації, які не завжди чітко й повністю визначені, або взагалі не узгоджені. Основним засобом вирішення цієї проблеми є врахування постачальниками продуктів ІВК вимог відкритих стандартів. Так, для визначення структур даних рекомендується використовувати стандарт X.509 (ISO/IEC 9594-8) з мінімальними змінами та максимально використовувати механізми розширень сертифіката. Такий підхід значно поліпшує інтероперабельність систем ІВК від різних постачальників, підвищує

інтероперабельність сертифікатів, які відповідають формату X.509 та федеральному профілю. Для виключення несумісності через неоднозначність інтерпретації даних у сертифікаті NIST розробив федеральний профіль сертифіката, який можуть використовувати відомства, що взаємодіють з федеральним мостовим центром сертифікації (Federal Bridge Certification Authority, FBCA) [68, 81].

Для об'єднання відомчих ІВК в США створено федеральний мостовий центр сертифікації – FBCA. Він формує сертифікати, що є дійсними для ІВК одного відомства та які будуть прийнятними в ІВК іншого відомства. При цьому передбачається, що відомства укладають угоду про те, що їх відомчі ІВК зв'язуються через FBCA [68,81]. Він забезпечує інтероперабельність шляхом трансляції інформації з відомчих сертифікатів у загальний сертифікат, який є прийнятним для інших учасників сертифікації. Тобто застосовується процес відображення політики застосування сертифікатів у відповідності до ISO/IEC 9594-8 (X.509). Однак повна промислова версія FBCA поки що не функціонує у повному обсязі. Тому вирішення проблеми інтероперабельності в загальнодержавному масштабі в США на цей час не досягнуто.

У цілому, станом на грудень 2003 року у 24 відомствах уряду США було започатковано 89 ініціативних проектів зі створення відомчих ІВК (табл. 1.1). Більшість систем у 2003 р. були пілотними проектами, а ті системи, що були реалізовані, працювали на відносно малій множині додатків. Так, із 89 проектів систем ІВК – 25 знаходились на стадії планування, 8 – на стадії проектування, 10 – на стадії розробки, 5 – на стадії випробувань. Тільки 35 систем експлуатувались, а 6 проектів були призупинені.

У цілому, досвід США показав, що впровадження технологій ІВК у фінансовому й матеріальному сенсі є надто витратними. На кінець 2003 загальна вартість усіх проектів склала більш ніж один мільярд доларів США.

Досвід США дозволяє визначити більшість проблемних задач, серед яких необхідно відзначити:

– забезпечення інтероперабельності систем і продуктів ІВК;

– впровадження міжнародних і промислових стандартів;

– створення систем ІВК, які підтримують потенційно велику кількість користувачів;

– зменшення вартості побудови систем ІВК;

– встановлення загальноприйнятих політик і процедур, що підтримують комплексний рівень довіри між відомствами;

– розробка та здійснення відомчих і загальнодержавних програм навчання користувачів і перепідготовки спеціалістів.

Першочерговими завданнями, що сформовані урядом США на 2001–2005 роки, були:

– розробка державної політики функціонування ІВК з метою сприяння у використанні систем ІВК, забезпечення комплексного рівня безпеки відомчих ІВК, зменшення загального ризику уряду під час розробки ІВК;

– забезпечення розробки й періодичного перегляду технічних положень, умов і стандартів у галузі створення й експлуатації систем ІВК;

– забезпечення постійного нагляду за виконанням відомствами державної політики у сфері ІВК, включаючи юридичне обґрунтування відмови у співпраці з FBCA.

8.1.2. Архітектура федеральної ІВК США

Аналіз досвіду експлуатації ІВК в США дозволив виявити два основних принципи, на основі яких будується архітектура ІВК в США [51, 65–66, 221].

По-перше, це незалежність побудови відомчих і комерційних систем та елементів ІВК. Більшість федеральних відомств у комерційних розробках реалізують власні проекти ІВК, головною метою яких є вирішення своїх корпоративних завдань.

По-друге, максимальне використання комерційних продуктів і послуг комерційних провайдерів послуг сертифікатів.

Головною проблемою Федеральної ІВК США, що виникла, є створення шляхів сертифікації між федеральними відомствами, які забезпечать високий рівень довіри під час виконання трансакцій. Її можна розглядати як перехресну сертифікацію в межах держави. Також проблемними для США залишилися задачі забезпечення взаємодії Федеральної ІВК з корпоративними ІВК приватних компаній, ІВК іноземних держав тощо. З цією метою в США уже впроваджена технологія Федерального моста сертифікації (FBCA).

На рис. 8.1 подана загальна архітектура ІВК США. Вона складається з двох великих доменів: федеральна ІВК і нефедеральна ІВК. Кожний домен об'єднує мережі центрів сертифікації, які побудовані за ієрархічною, комірчасто-сітчастою або змішаною структурою [221].

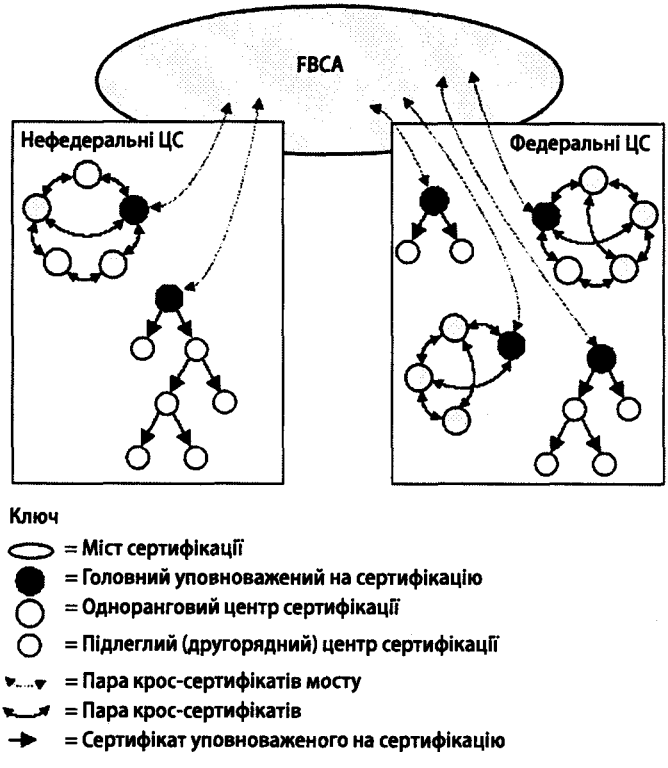

Рис. 8.1. Загальна архітектура ІВК США

Федеральний мостовий центр сертифікації (FBCA) є уніфікованим елементом [68, 81], який забезпечує зв'язок між відомчими ІВК. FBCA не є кореневим центром сертифікації, а є «мостом довіри». Він не є початком шляху сертифікації, а тільки з'єднує довірчі домени через крос-сертифікати між FBCA та головними центрами сертифікації. FBCA функціонує під управлінням Уповноваженого органу з управління федеральною політикою (Federal policy menegement authority (FPMA)). Федеральні (або нефедеральні) центри сертифікації, які виконують вимоги FPMA, мають можливість користуватися послугами FBCA. Такий шлях значно простіший у порівнянні з узгодженням усіх центрів між собою за допомогою крос-сертифікатів.

8.1.3. Федеральний профіль сертифіката США

У США введено загальне поняття, що характеризує структури даних, які використовуються у федеральній ІВК – федеральний ІВК-профіль (рис. 8.2) [81, 61]. Цей профіль здебільшого складається з федерального профілю сертифіката та федерального профілю списків скасування сертифіката (див. розділ 7).

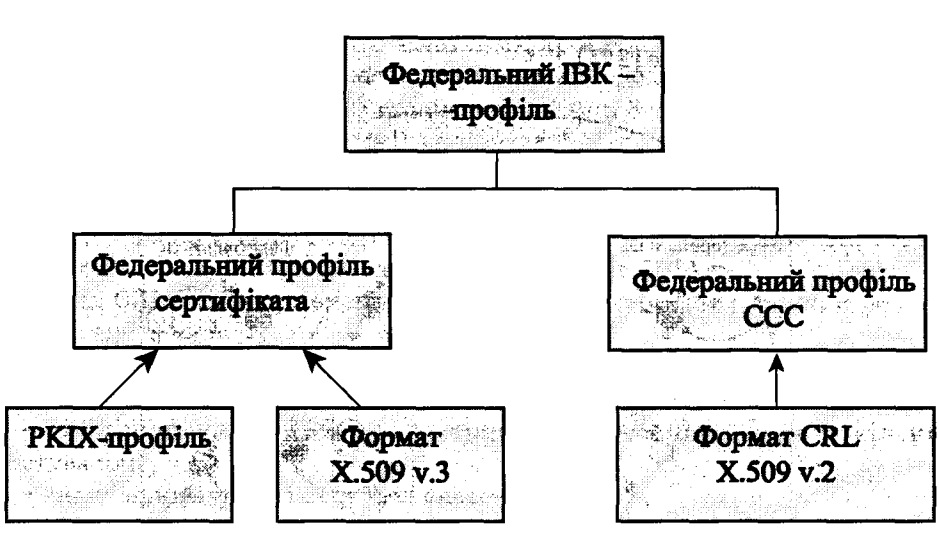

Рис. 8.2. Федеральний ІВК-профіль

Федеральний профіль сертифіката базується на «стандартному профілі», який містить унікальні параметри, що встановлені для федеральних систем. Федеральний профіль розроблений на основі PKIX-профілю та формату сертифіката X.509 v.3. Він служить доповненням до чинного PKIX-профілю та враховує всі розбіжності між стандартним і федеральним профілем. Якщо необхідно забезпечити реалізацію всіх федеральних доповнень до стандартного сертифіката та списку скасованих сертифікатів, то організація має адаптувати свій X.509 сертифікат з використанням параметрів, що введені у федеральний профіль, та параметрами, які введені у профіль PKIX. При цьому, параметри федерального профілю мають переваги. Федеральний профіль сертифіката описує зміст п'яти типів сертифікатів X.509:

1) сертифікат цифрового підпису кінцевого суб'єкта;
2) сертифікат управління ключами кінцевого суб'єкта;
3) сертифікат центру сертифікації;
4) сертифікат мостового центру сертифікації;
5) самопідписаний сертифікат центру сертифікації.

Сертифікат цифрового підпису кінцевого суб'єкта обов'язково містить відкритий ключ, який призначений для перевірки його цифрового підпису.

Сертифікат управління ключами обов'язково містить відкритий ключ, який призначений для перевірки ключів під час їх транспортування.

Сертифікат центру сертифікації – сертифікат, що випущений одним центром сертифікації для іншого центру сертифікації.

Сертифікат моста сертифікації випускається FBCA для головних уповноважених із сертифікації.

Самопідписаний сертифікат центру сертифікації формується центром для безпечного розподілу серед своїх користувачів.

У таблиці 8.1 надані основні й додаткові розширення для кожного класу сертифікатів.

Таблиця 8.1. **Розширення сертифіката у Федеральній ІВК**

Розширення сертифіката	Обов'язкове чи необов'язкове	Зміст
1	2	3
Key Usage	Для всіх сертифікатів	Розширення використання ключа визначає призначення ключа, що міститься в сертифікаті. Для користувачів ключ може використовуватись для підпису документів, автентифікації, управління ключами або шифрування даних. Для центрів сертифікації – перевірка підпису на сертифікатах та ССС
Basic constraints	Для всіх сертифікатів ЦС	Указує, що суб'єкт являє собою ЦС. Може містити кількість додаткових сертифікатів на шляху сертифікації
Authority Key Identifier	Для всіх сертифікатів	Геш (за алгоритмом SHA-1) відкритого ключа, яким перевіряється підпис сертифіката. Служить для вибору потрібного ключа
Subject Key Identifier	Для всіх сертифікатів ЦС. Може бути присутнє і в сертифікатах кінцевих об'єктів	Геш (за алгоритмом SHA-1) відкритого ключа

Закінчення табл. 8.1

1	2	3
Subject alternative name	Необов'язково, але використовується	Дозволяє додатково ідентифікувати суб'єкт сертифіката. Визначені опції включають адресу електронної пошти, DNS-ім'я, IP-адресу
Certificate policies	Для всіх сертифікатів	У сертифікатах кінцевих об'єктів тут представлені політики, що описують рівень довіри. У сертифікатах ЦС цей список описує діапазон політик, для яких цей сертифікат є довірчим
Policy mapping	Для всіх сертифікатів ЦС. Присутнє тільки, коли суб'єкт і емітент діють на основі різних політик	Описує, які політики ЦС відповідають політикам суб'єкта
Name constraints	Для всіх сертифікатів ЦС	Використовується для обмеження набору довірчих сертифікатів на основі імен
Policy constraints	Для всіх сертифікатів ЦС	Використовується для нав'язування політики або заборони відображення політики
CRL distribution points	Необов'язково. Тільки в сертифікатах, чий статус скасування визначається непрямими ССС	Використовується для ідентифікації ССС, який включає цей сертифікат

8.1.4. Федеральний профіль списку скасованих сертифікатів

Федеральний ІВК-профіль визначає два профілі списку скасованих сертифікатів:

1) профіль для FBCA;

2) профіль для всіх інших центрів сертифікації федеральної ІВК.

Обидва профілі базуються на форматі CRL X.509 v.2.

Перший тип профілю вводить розширення, які вводять додаткову інформацію про скасовані сертифікати. Розширення запису ССС, ідентифіковані в профілі, являють розширення емітента сертифіката та кодів причини. За замовчуванням, емітентом ССС є ЦС, що випустив сертифікат; якщо це не так, то в ССС указується емітент. Коди причини вказують причини скасування сертифіката. Сторона, що довіряє, може прийняти сертифікат з кодом «замінений», але не може прийняти з кодом «компрометація ключа». Другий тип розширень являє собою розширення, що вказують інформацію про весь ССС. За федеральним профілем це ідентифікатор ключа уповноваженого, альтернативне ім'я емітента, номер ССС і пункт розподілу ССС. У наступних таблицях наводяться розширення ССС за федеральним профілем. Усі розширення повинні відповідати RFC 2459 та профілю.

Таблиця 8.2. **Розширення ССС у Федеральній ІВК**

Розширення ССС	Обов'язкове чи необов'язкове	Зміст
CRL number	Для всіх ССС	Передає номер, який послідовно і монотонно збільшується. Необхідне для швидкого виявлення, у якій групі знаходиться ССС
Authority Key Identifier	Для всіх ССС	Геш-значення (за алгоритмом SHA-1) відкритого ключа, яким перевіряється підпис сертифіката. Служить для вибору потрібного ключа
Issuer alternative name	Необов'язкове	Дозволяє додатково ідентифікувати адресу електронної пошти емітента
Issuing distribution points	Для всіх непрямих ССС	Відповідає "CRL distribution points" у сертифікаті

Таблиця 8.3. **Розширення запису ССС у Федеральній ІВК**

Розширення ССС	Обов'язкове чи необов'язкове	Зміст
Reason code	Для всіх сертифікатів, крім сертифікатів ЦС без інформації	Визначає причину скасування сертифіката
Certificate issuer	Для всіх ССС	Ідентифікує емітента для набору сертифікатів, наведених у цьому ССС

8.1.5. Основні напрями підвищення інтероперабельності компонентів ІВК

Визнання Федерального профілю сертифіката та списку скасованих сертифікатів не вирішує всіх проблем інтероперабельності систем ІВК. Тому під керівництвом NIST десять американських компаній (AT&T, BBN, Certicom, Cylink, DynCorp, Northern Telecom, IRE, Motorola, Spyrus Inc., VeriSign Inc.), що посідають провідні позиції на ринку послуг ЕЦП, розробили мінімальні вимоги до специфікації для компонентів ІВК – MISPC [66].

Ці рекомендації визначають основи для взаємодії між компонентами ІВК, що постачаються різними постачальниками й підтримують інтероперабельність широкого кола систем та засобів ІВК. Здебільшого цей документ визначає:

1) процедури генерації, відновлення та скасування сертифікатів відкритого ключа;

2) процедури генерації та верифікації цифрового підпису;

3) процедури перевірки сертифікатів і шляхів сертифікації.

Специфікація також містить розширений профіль сертифіката та ССС, а також типові трансакції: запит на сертифікацію, на відновлення та скасування сертифіката, на повернення сертифікатів і ССС з репозиторію.

Рекомендації базуються на форматах сертифіката X.509 v.3 та CCC v.2. Окрім цього, документ використовує формати даних, що встановлюються в стандартах ITU-T X.509, ANSI X9.55, X9.57 та X.9.62, IETF PKIX тощо.

Спираючись на міжнародні та національні стандарти в MISPC надається специфікація таких компонентів:

– уповноваженого на сертифікацію (центру сертифікації);
– уповноваженого на реєстрацію (центру реєстрації);
– утримувача сертифікатів;
– клієнта ІВК.

Окрім цього, уточнюються формати даних:

– формат сертифіката;
– формат CCC;
– формати службових повідомлень.

Аналіз цього документа дозволяє зробити висновок, що компанії, які підтримують MISPC, базуються на використанні стандартного формату сертифіката X.509 і не змінюють критичних полів, а використовують можливості розширень сертифіката.

8.2. СТАН ЗАСТОСУВАННЯ ТА РОЗВИТКУ ІВК В КАНАДІ

8.2.1. Загальні підходи до створення ІВК

Роботи з проектування та побудови ІВК уряду Канади (Government of Canada PKI) [9] були розпочаті в 1995 році. Нормативною базою створення ІВК Уряду Канади (УК) стали документи Консультативної Ради з Інформаційної комунікації (Information Highway Advisory Council) [70]. У названих документах визначені концептуальні підходи до створення ІВК. Сутність їх зводиться до такого.

1. Федеральні, провінційні й територіальні уряди співпрацюють з метою законодавчого врегулювання, контролю та вирішення проблем забезпечення безпеки інформації у сфері електронної комерції на рівнях уряду, приватного сектора та міжнародної торгівлі;

2. Уряд Канади працює у співробітництві з провінціями, територіями, приватним сектором та іншими зацікавленими сторонами у сфері розробки стандартів безпеки та їх поширення як у Канаді, так і серед міжнародних партнерів з метою поліпшення обміну інформацією;

3. Уряд, постачальники послуг у приватному секторі, користувачі та інші учасники інформаційної комунікації взаємодіють та працюють у сфері розробки політик та основ інфраструктури безпеки Канади, що підтримує інформаційні комунікації.

Згідно вказаних концептуальних положень основним напрямком досягнення зазначених цілей є створення ІВК. Консультативна рада перша започаткувала роботи з розробки політики ІВК, а також процедур крос-сертифікації з метою забезпечення сумісності та інтероперабельності державної ІВК з міжнародними системами.

У 1995 році розпочалися роботи зі створення ІВК Уряду Канади, до яких було залучено 6 відомств. Основною метою робіт було забезпечення більшої ефектив-

ності надання послуг громадянам Канади; високого рівня безпеки електронної комерції, а також забезпечення більш високого рівня конфіденційності інформації, що використовується у федеральному уряді.

8.2.2. Архітектура ІВК Уряду Канади

Уряд Канади (УК), на відміну від США, пішов стратегією побудови урядової ІВК за визначеною однозначно ієрархічною структурою.

На рисунку 8.3 наведений спрощений варіант архітектури ІВК Уряду Канади.

Основними елементами ІВК Уряду Канади є:

1) уповноважений орган з управління політикою (Policy Management Authority – PMA);

2) головний центр сертифікації (Canadian Central Facility – CCF);

3) центри сертифікації (Certificate Authority – CA);

4) локальні центри реєстрації (Local Registration Authority – LRA).

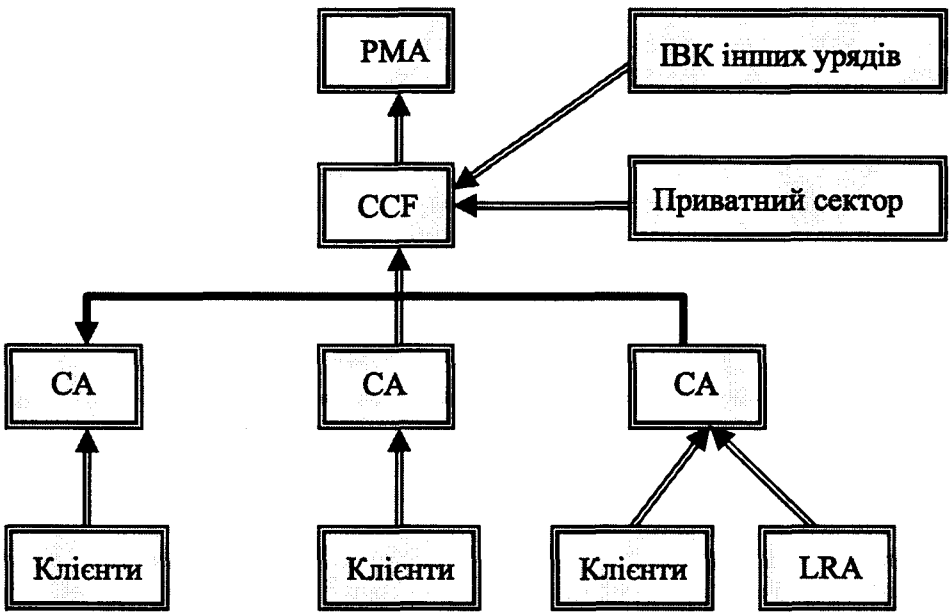

Рис. 8.3. Основні елементи ІВК Уряду Канади

Уповноважений орган PMA є міжвідомчим комітетом, який підпорядковується казначейству (Treasury Board Secretariat). Основним завданням PMA є нагляд за додержанням політики функціонування ІВК УК.

Головний центр сертифікації CCF є центральним уповноваженим органом із сертифікації, який реалізує та впроваджує політику ІВК УК та забезпечує здійснення крос-сертифікації із зовнішніми організаціями, наприклад, урядами інших країн, відомствами й корпораціями тощо. CCF є центром сертифікації ніби «нульового» рівня. Він розміщений в Оттаві.

До основних функцій головного центру сертифікації CCF належать:

1) випуск сертифікатів для всіх центрів сертифікації ІВК УК 1-го рівня;

2) випуск сертифікатів для зовнішніх ІВК, у відповідності до вимог PMA;

3) підтримка списків скасованих сертифікатів;

4) архівування всіх сертифікатів і списків скасованих сертифікатів, випущених в ІВК УК;

5) архівування журналів аудиту головного центру сертифікації та, за необхідністю, центрів сертифікації 1-го рівня.

Центри сертифікації функціонують у відомствах та урядових департаментах. Кожний центр сертифікації відповідає за адміністрування визначеної множини об'єктів шифрування/ вироблення електронного цифрового підпису, локальних центрів реєстрації та підпорядкованих йому центрів сертифікації.

Відповідальність за функціонування центру сертифікації несе керівник департаменту, організації, агенції, групи або відділу.

Центри сертифікації першого рівня безпосередньо підпорядковуються головному центру сертифікації. Центри сертифікації другого рівня безпосередньо підпорядковуються центрам сертифікації першого рівня та можуть бути розгорнуті залежно від завдання кожного департаменту або відомства.

Основною функцією локальних центрів реєстрації є ідентифікація та реєстрація сертифікатів відкритих ключів своїх користувачів. Центри реєстрації функціонують у департаментах і відомствах. Локальний центр реєстрації підпорядковується центру сертифікації. Залежно від вимог відомства, може бути створена будь-яка кількість локальних центрів реєстрації. До основних функцій центра реєстрації належать:

1) реєстрація, зняття з реєстрації та зміна атрибутів об'єктів і суб'єктів;

2) підтвердження дійсності користувачів, пов'язаних з об'єктами;

3) авторизація запитів на відновлення ключів і сертифікатів;

4) прийом та авторизація запитів на скасування сертифікатів;

5) розподіл носіїв особистих ключів (токенів, дискет тощо), а також виведення з обігу старих носіїв тощо;

6) реєстрація, зняття з реєстрації та призначення привілеїв персоналу, що обслуговує центр реєстрації.

Таким чином, урядова ІВК будується за ієрархічним принципом. Причому Уряд Канади відразу прийняв стратегію побудови державної ІВК під наглядом державного контролюючого органу з метою уникнути проблем взаємодії між ІВК різних відомств. Такий підхід прийнятий і в Україні.

8.2.3. Особливості побудови ІВК УК

ІВК Уряду Канади побудована на продуктах компанії Entrust Technology Inc. Сімейство продуктів цієї компанії забезпечує повну автоматизацію виготовлення сертифікатів відкритих ключів, управління ключами, цифрового підпису та шифрування. Продукти забезпечують єдину архітектуру безпеки, можуть застосовуватися в мережах типу «клієнт – сервер» на платформах Windows, Macintosh або Unix.

Базовим продуктом ІВК є Entrust/Authority та Entrust/RA v.5.1 [223–225], що згідно ISO/IEC 15408 [108] мають рівень гарантій EAL 4+ та відповідають вимогам міжнародного профілю захисту на систему виготовлення й обслуговування сертифікатів [71]. Постачання продуктів виконують ще дві компанії – SAGUS Security Inc. та Chrysalis–ITS. Продукти компанії SAGUS реалізують рішення щодо забезпечення безпеки на робочих станціях, у додатках «клієнт – сервер», локальних мережах і взаємодіють з продуктами Entrust.

Основним продуктом компанії Chrysalis-ITS є урядова карта – апаратно-програмний засіб КЗІ. Засіб КЗІ являє собою модуль КЗІ – Type II PCMCIA. Він забезпечує зашифрування, розшифрування та цифровий підпис всередині приладу. Модуль задовольняє вимогам FIPS 140-1 Level II, є сумісним з продуктами Entrust і може використовуватись на робочих станціях і мобільних комп'ютерах через PCMCIA інтерфейс. Компанія також поставляє модуль GSEC, при використанні якого забезпечується більш високий рівень захисту, оскільки всі криптографічні операції виконуються тільки всередині модуля. GSEC підтримує криптографічні алгоритми симетричного й асиметричного шифрування, гешування та генерацію ключів. Як симетричні шифри можуть застосовуватись алгоритми CAST, DES, TDES, RC2, RC4 та AES. Ключі генеруються тільки всередині модуля. Несиметричне шифрування здійснюється з використанням RSA та алгоритмів, що визначені в ISO/IEC 18033-2. Асиметричні ключові пари генеруються тільки всередині картки й особисті ключі зберігаються тільки всередині картки. Гешування виконується з використанням алгоритмів MD5, SHA-1 та SHA-2. Застосування апаратно-програмних модулів дозволило реалізувати в ІВК УК вищий рівень гарантій.

8.2.4. Перелік стандартів, алгоритмів і протоколів, що підтримуються ІВК УК

Урядова ІВК Канади спирається на відкриті стандарти, протоколи та технічні специфікації, що здебільшого визнані на міжнародному рівні. Застосовуються та підтримуються такі стандарти.

Безпека криптографічних засобів

1. FIPS 140-1 та FIPS 140-2 – вимоги безпеки до криптографічних модулів (національні стандарти США) [116–117].

2. CEAD – програма оцінки й підтвердження відповідності криптографічних засобів вимогам.

Стандарти та криптографічні алгоритми

1. Симетричні алгоритми:
Entrust Technologies CAST (128 бітів); RC2, TDES, AES.

2. Асиметричні алгоритми:
– RSA/MD5 та RSA/SHA-1 для ЕЦП із 1024-бітовими ключами;
– FIPS PUB 180-1 та FIPS PUB: DSA/SHA;
– FIPS PUB 186-1 та FIPS PUB 180-1: DSA/SHA;
– FIPS PUB 186-2 та FIPS PUB 180-1: EC DSA/SHA-1;

– FIPS PUB 186-3 та FIPS PUB 180-2: RSA/SHA-1 для ЕЦП із 2048 та 3072-бітовими ключами;

– FIPS PUB 186-3 та FIPS PUB 180-2: EC DSA/SHA-1;

– ISO/IEC 15946-2(14888-3) та ISO/IEC 10118:EC DSA, EC G DSA/ SHA-1, SHA-2.

3. Комунікаційні протоколи:

– RFC 1777 LDAP (Lightweight Directory Access Protocol);

– ISO/IEC 8824 та 8825 ASN.1 нотація;

– S/MIME Message Specification: PKCS Security Services to MIME;

– PEM (Privacy Enhanced Mail);

– MSP (Message Security Protocol);

– Independent Data Unit Protection (IDUP), GSS API, Internet–чорновик; та GSS API, RFC 1508.

4. Мережеві протоколи:

– підтримка TCP/IP.

5. Інфраструктура:

– X.500 служба Каталогу та підтримка інших каталогів і (ре)депозитаріїв з інтерфейсом LDAP.

6. Інфраструктура відкритих ключів:

– сертифікати ITU-T Rec. X.509 | ISO/IEC 9594-8, v3;

– Simple Public Key GSS-API Mechanism (SPKM), RFC 2025;

– MISPC (Minimum Interoperability Specification for PKI Components);

– Secure Exchange Protocol (SEP);

IETF PKIX:

– Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile;

– Internet Public Key Infrastructure Part III: Certificate Management Protocols; Certificate Policies and Certification Practice Statements Framework; and CertificateManagement Services Application Programming Interface (CMS-API), Issue 2.0.

Таким чином, у Канаді, з урахуванням досвіду США, як основну для урядових систем реалізовано ієрархічну архітектуру ІВК. Формати даних повністю підтримують формат сертифіката ITU–T Rec. X.509 | ISO/IEC 9594-8, v3. У Канаді надійно функціонує державна ІВК, яка має ієрархічну структуру. За розвиток ІВК відповідає Секретаріат ІВК (The Public Key Infrastructure Secretariat), що управляється Головним відділом інформації Секретаріату Казначейства Канади (Chief Information Officer Branch of the Treasury Board Secretariat of Canada).

Головний (кореневий) ЦСК називається «The Canadian Central Facility, CCF» (Канадська Центральна Установа), яка розміщена в Communications Security Establishment (Установі безпеки комунікацій) в Оттаві. Цей центр виконує і роль «мосту», тобто здійснює крос-сертифікацію між державними і приватними установами.

8.3. СТАН ЗАСТОСУВАННЯ ТА РОЗВИТКУ ІВК У ЄВРОПЕЙСЬКОМУ СОЮЗІ

Аналіз нормативно-правових документів, що регулюють питання використання ЕЦП у ЄС [5, 226–228], дозволяє стверджувати, що в ЄС не існує концепції створення єдиної європейської ІВК. Кожна країна – член ЄС має створювати власну інфраструктуру, але при цьому дотримуватися вимог європейського законодавства з метою забезпечення інтероперабельності.

На електронному диску, що додається до монографії, в другому розділі наводяться дані стану та проблемні питання впровадження та застосування ІВК в ЄС. При викладенні ми здебільшого орієнтувались на [228].

8.3.1. Аналіз вимог європейського законодавства щодо ЕЦП

Проблемним поточним завданнями ЄС щодо правового регулювання відносин у сфері електронного документообігу є розвиток та прийняття однакових законів у державах з дуже різними правовими системами та традиціями. Мета ЄС полягає не у створенні однакового законодавчого порядку, а в сприянні торгівлі, розвитку інвестиційної діяльності та свободи пересування громадян. Найбільш важливим законодавчим інструментом, який використовується ЄС для надання законної сили своїм рішенням, є Директиви ЄС [5]. Особливістю Директив ЄС є те, що вони містять обов'язкові завдання (результат), який держави – члени ЄС повинні досягти протягом указаного строку, але форми та методи досягнення результату визначаються кожною державою самостійно. При цьому держави – члени ЄС мають визначені зобов'язання в частині впровадження та використання послуг ІВК з необхідним рівнем гарантій.

У сфері електронного документообігу прийнято дві Директиви: Директива про електронну комерцію 2000 року (ДЕК), що імплементована в національне законодавство державами-членами ЄС до 17 лютого 2002 року, і Директива про електронні підписи 1999/93 ЄС, що набула чинності 19 липня 2001 року [5]. Вони впроваджені в національне законодавство державами – членами ЄС повною мірою.

Директива про електронну комерцію 2000 встановлює загальні основи для розвитку та застосування електронної комерції. Так, стаття 9 Директиви вимагає від держав надання законної сили договорам в електронній формі, усунення бар'єрів при їхньому використанні та забороняє заперечення їхньої юридичної чинності виняткова на підставі електронної форми. Зобов'язання та вигоди, що досягаються при застосуванні Директиви дійсні тільки в межах ЄС.

Директива про електронні підписи 1999/93 ЄС є більш деталізованою і встановлює основи для юридичного визнання електронних підписів і вимоги до держав-членів в області їхньої сертифікації. Так, стаття 5 визначає [5], що вдосконалені електронні підписи, які засновані на чинних сертифікатах і створені за допомогою безпечних механізмів створення підпису, повинні:

– задовольняти юридичним вимогам щодо підписів стосовно даних, поданих в електронній формі, так само, як і підпис, написаний власноруч задовольняє вимогам стосовно даних, написаних на папері;

– прийматися як докази в судочинстві.

При цьому країни-члени ЄС повинні забезпечити неможливість позбавлення електронного підпису юридичної сили та прийнятності як доказу в судочинстві лише на тій підставі, що ЕЦП:

1) був виконаний в електронній формі;

2) не заснований на чинному сертифікаті;

3) не заснований на чинному сертифікаті, виданому акредитованим постачальником послуг із сертифікації;

4) не створений за допомогою безпечного механізму створення підпису.

Директива ЄС 1999/93 ЄС встановлює ряд вимог до чинних сертифікатів. Так, чинні сертифікати повинні містити:

1) вказівку про те, що сертифікат виданий як чинний сертифікат;

2) ідентифікацію постачальника послуг із сертифікації та держави, в якій засноване його підприємство;

3) ім'я особи, що підписалася, чи її псевдонім, який ідентифікується як такий;

4) забезпечення особливої ознаки особи, що підписується, яка включається в сертифікат, залежно від мети, на яку орієнтований сертифікат;

5) дані для перевірки підпису, які відповідають даним, що створюють підпис, під контролем особи, що підписалася;

6) вказівка на початок і закінчення терміну чинності сертифіката;

7) ідентифікаційний код сертифіката;

8) вдосконалений електронний підпис постачальника послуг із сертифікації;

9) обмеження сфери використання сертифіката, якщо таке застосовується;

10) обмеження вартості операцій, при здійсненні яких може використовуватись сертифікат, якщо такі застосовуються.

Також Директива визначає вимоги до постачальників послуг із сертифікації, які повинні:

1) демонструвати надійність, необхідну для постачання послуг із сертифікації;

2) забезпечувати функціонування швидкого та безпечного надання довідкових послуг і невідкладне й безпечне анулювання послуг;

3) забезпечувати чітке визначення дати й часу видачі та анулювання сертифіката;

4) перевіряти за допомогою відповідних засобів згідно з внутрішнім законодавством ідентичність та, якщо таке застосовується, будь-які особливі ознаки особи, якій видається сертифікат;

5) наймати штат осіб, що мають спеціальні знання, досвід і кваліфікацію, необхідну для послуг, що надаються, зокрема, компетентних осіб на рівні управління, експертизи в технології електронних підписів та обізнаних із правилами безпеки; вони також повинні застосовувати адміністративні правила та правила процедури, адекватні й такі, що відповідають визнаним стандартам;

6) використовувати достовірні системи та продукцію, захищені від модифікацій і забезпечувати технічну та криптографічну безпеку процесу, що ними забезпечується;

7) вживати заходів проти підробки сертифікатів та в разі, якщо постачальник послуг із сертифікації виробляє дані, що створюють підпис, гарантувати конфіденційність під час вироблення таких даних;

8) підтримувати достатні фінансові ресурси для здійснення діяльності відповідно до вимог, передбачених цією Директивою, зокрема, нести ризик відповідальності за шкоду, заподіяну, наприклад, шляхом отримання відповідного страхування;

9) зберігати всю інформацію, що стосується видачі чинних сертифікатів протягом відповідного періоду часу, зокрема з метою надання доказів сертифікації в цілях судочинства. Такі записи можуть здійснюватись електронним шляхом;

10) до того, як вступати в договірні відносини з особою, яка прагне отримати сертифікат, що засвідчує її електронний підпис, повідомляє таку особу через надійні засоби зв'язку про точні терміни та умови використання сертифіката, включаючи будь-які обмеження його використання, існування системи добровільної акредитації та процедури подання скарг і врегулювання спорів. Така інформація, що може надаватися в електронному вигляді, повинна бути подана в письмовому вигляді та викладена добре зрозумілою мовою. Відповідні частини цієї інформації також мають бути доступними на запит третіх сторін, які покладаються на сертифікат;

11) використовувати надійні системи зберігання сертифікатів у такій формі, яка підлягає перевірці, з тим, щоб:

– лише уповноважені особи могли здійснювати введення даних та їх змінювати,

– забезпечувалась можливість перевірки інформації на достовірність; сертифікати відкриті для внесення в них коригувань лише в тих випадках, у яких отримано згоду власників сертифікатів;

– будь-які технічні зміни, що загрожують цим вимогам безпеки, були очевидні для оператора.

Аналіз Директив ЄС дозволяє зробити висновок, що головною метою висування вимог є забезпечення гарантії того, що під час використання ЕЦП досягнуто максимальну безпеку. При цьому вказівок на конкретні пристрої, методи або технічні вимоги до формування ЕЦП немає.

8.3.2. Стандартизація ЄС в галузі ІВК

З метою підвищення координації національних, регіональних і міжнародних органів зі стандартизації в галузі ІВК, Європейський Інститут Комп'ютерних Технологій (ІСТ), за підтримкою Європейської Комісії, створив Європейську Ініціативу Стандартизації Електронного Підпису (EESSI).

Основними принципами роботи EESSI є такі:

1) узгодження рішень, які дозволяють уникнути дублювання роботи в межах ЄС;

2) ефективне залучення всіх сторін у галузі ЕЦП до процесів стандартизації ЄС;

3) відкритість і прозорість механізмів і взятих ініціатив, що використовуються.

У 1999 році в рамках EESSI була розроблена робоча програма зі стандартизації в галузі ЕЦП та ІВК [226]. У робочій програмі були визначені як критичні три ключові напрямки стандартизації:

1) стандартизація якості та функціонування постачальників послуг із сертифікації (ППС);

2) стандартизація якості та функціонування механізмів вироблення та перевірки ЕЦП;

3) стандартизація вимог до ЕЦП.

Основною технологією для підтримки ЕЦП визначено технологію ІВК. Під час створення та використання технологій ІВК пріоритетне значення повинні мати:

– вимоги безпеки для механізмів ЕЦП;

– сертифікація/ реєстрація відповідності механізмів і послуг ЕЦП;

– управління безпекою та політикою сертифікації під час випуску сертифікатів;

– механізми вироблення та перевірки підпису;

– синтаксис і формати даних, а також технічні аспекти політик підпису;

– протоколи взаємодії з Уповноваженим щодо відмітки часу.

EESSI активно взаємодіє з іншими ініціативами на глобальному рівні, розробляє рішення, які гарантують можливість взаємодії додатків електронного підпису.

Основні роботи зі стандартизації в галузі ЕЦП та ІВК в рамках EESSI здійснюють ICT, CEN та ETSI (рис. 8.4) у тісній взаємодії з національними органами зі стандартизації.

На рис. 8.5 показано розподіл напрямків роботи робочих груп ETSI ESI та CEN E-SIGN.

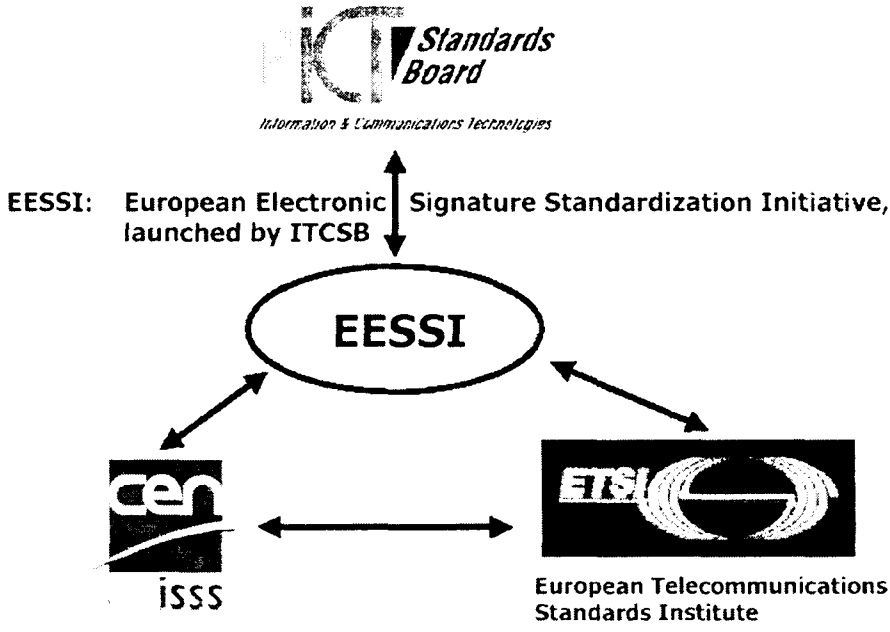

Рис. 8.4. Схема взаємодії робочих груп EESSI

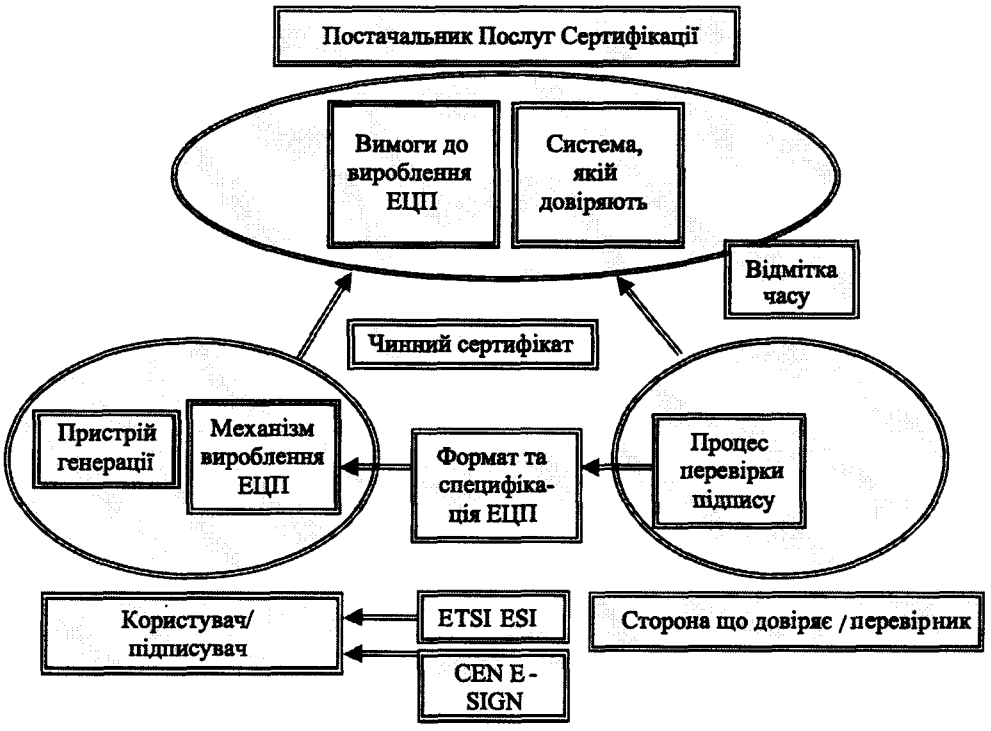

Рис. 8.5. Розподіл напрямків роботи робочих груп

ETSI ESI є технічним органом, що відповідає за інфраструктури та послуги безпеки в телекомунікаційних середовищах.

ETSI ESI займається розробкою таких питань:

1) Використання сертифікатів відкритого ключа X.509 як чинного сертифіката;

2) Управління Безпекою і Політика Сертифікації для Постачальників послуг із сертифікації (ППС), які випускають чинні сертифікати;

3) Синтаксис і формати кодування для електронного підпису та технічні аспекти для політик підпису;

4) Протокол, що дозволяє взаємодію з Уповноваженим на Позначку часу.

ETSI ESI створив можливість обговорення поточних чернеток стандартів, допоміжних матеріалів і можливість обміну ідеями.

Результатом роботи ETSI ESI стало опублікування нормативних документів (табл. 8.4).

Організація CEN's Information Society Standardization System (CEN/ISSS) відповідає за частину робочої програми EESSI, що пов'язана зі стандартами якості й функціонування для Постачальників Послуг із Сертифікації (CSPs) і за стандарти якості та функціонування для механізмів вироблення й перевіряння підпису.

Таблиця 8.4. **Нормативні документи ETSI ESI**

1	2
CWA 14167-1	Вимоги щодо захисту сертифікатів управління надійними системами для електронних підписів – частина 1: Вимоги системного захисту
CWA 14167-2	Вимоги щодо захисту сертифікатів управління надійними системами для електронних підписів – частина 2: Криптографічний модуль для CSP операції підписання з резервуванням – Профіль захисту (CMCSOB-PP)
CWA 14167-3	Вимоги щодо захисту сертифікатів управління надійними системами для електронних підписів – частина 3: Криптографічний модуль для CSP послуг генерації ключів – профіль захисту (CMCKG-PP)
CWA 14167-4	Вимоги щодо захисту сертифікатів управління надійними системами для електронних підписів – частина 4: Криптографічний модуль для CSP операції підписання – профіль захисту – CMCSO-PP
CWA 14169	Пристрої створення безпечного підпису "EAL 4+"
CWA 14170	Вимоги захисту для застосувань щодо створення підпису
CWA 14171	Загальні керівництва для верифікації електронного підпису
CWA 14172-1	EESSI керівництво оцінки відповідності – частина 1: Загальне введення
CWA 14172-2	EESSI керівництво оцінки відповідності – частина 2: Послуги та процеси центру сертифікації
CWA 14172-3	EESSI керівництво оцінки відповідності – частина 3: Сертифікати управління надійними системами для електронних підписів
CWA 14172-4	EESSI керівництво оцінки відповідності – частина 4: Застосування створення підпису та загальне керівництво для верифікації електронного підпису
CWA 14172-5	EESSI керівництво оцінки відповідності – частина 5: Пристрої створення безпечних підписів
CWA 14172-6	EESSI керівництво оцінки відповідності – частина 6: Пристрій створення підпису, що підтримує підписи, окрім кваліфікованих
CWA 14172-7	EESSI керівництво оцінки відповідності – частина 7: Криптографічні модулі, що використовуються постачальниками послуг сертифікації для операції підписання та послуг генерації ключів
CWA 14172-8	EESSI керівництво оцінки відповідності – частина 8: Послуги та процеси центрів тимчасової розмітки

Закінчення табл. 8.4

1	2
CWA 14355	Керівництво щодо реалізації пристроїв створення безпечного підпису
CWA 14365-1	Керівництво щодо використання електронних підписів – частина 1: Правові й технічні аспекти
WA 14365-2	Керівництво щодо використання електронних підписів – частина 2: Профіль захисту для програмних пристроїв створення підпису
CWA 14890-1	Прикладний інтерфейс для старт-карт, що використовуються як пристрої створення безпечного підпису – частина 1: Базові вимоги
CWA 14890-2	Прикладний інтерфейс для старт-карт, що використовуються як пристрої створення безпечного підпису – частина 2: Додаткові послуги

Таблиця 8.5. **Нормативні документи CEN/ISSS**

1	2	3
TS 101 903 v1.2.2	Квітень 2004	XML Розширені електронні підписи (XAdES)
TS 101 903 v1.2.1	Березень 2004	XML Розширені електронні підписи (XAdES) (*вилучений*)
TS 101 862 v1.3.1	Березень 2004	Кваліфікований профіль сертифікації
TS 102 280	Березень 2004	X.509 v.3 профіль сертифікації для сертифікатів, виданих реальним персонам
TR 102 047	Лютий 2004	Міжнародна гармонізація форматів електронного підпису
TR 102 040 v1.2.1	Лютий 2004	Міжнародна гармонізація вимог щодо політики для центрів сертифікації, що випускають сертифікати
TS 101 733 v1.5.1	Грудень 2003	Формати електронного підпису
TR 102 272	Грудень 2003	ASN.1 формат для політик підпису
TS 102 231	Жовтень 2003	Гармонізована TSP інформація статусу
TS 102 158	Жовтень 2003	Вимоги щодо політики для CSP, що випускають атрибутні сертифікати
TR 102 045	Березень 2003	Політика підпису для розширеної ділової моделі
SR 002 176	Березень 2003	Алгоритми та параметри для безпечних електронних підписів

Закінчення табл. 8.5

1	2	3
TR 102 153	Лютий 2003	Попередні дослідження з профілів сертифікації
TR 102 046	Лютий 2003	Підтримка ETSI стандартів з EESSI фази 2 і 3
TS 102 023 v1.2.1	Січень 2003	Вимоги щодо політики для центрів тимчасової розмітки
TR 102 044	Грудень 2002	Визначення вимог щодо атрибутної сертифікації
TS 101 733 v1.4.0	Вересень 2002	Версія форматів електронного підпису
TR 102 038	Квітень 2002	XML формат для політик підпису
TS 102 023	Квітень 2002	Вимоги щодо політики для центрів тимчасової розмітки
TS 102 042	Квітень 2002	Вимоги щодо політики для центрів сертифікації, що випускають сертифікати відкритого ключа
TS 101 456 v1.2.1	Квітень 2002	Вимоги щодо політики для центрів сертифікації, що випускають кваліфіковані сертифікати
TR 102 030	Квітень 2002	Забезпечення гармонізованої інформації про статус Постачальника довірчих послуг
TR 102 040	Березень 2002	Міжнародна гармонізація вимог щодо політики для центрів сертифікації, що випускають сертифікати
TS 101 861 v1.2.1	Березень 2002	Профіль тимчасової розмітки
TR 102 041	Лютий 2002	Звіт про політики підпису
TS 101 903	Лютий 2002	XML Розширені Електронні Підписи (XAdES)
TS 101 733 v1.3.1	Лютий 2002	Формати електронного підпису
TS 101 861 v1.1.1	Вересень 2001	Профіль тимчасової розмітки
TS 101 862 v1.2.1	Червень 2001	Профіль кваліфікованого сертифіката
TS 101 456 v1.1.1	Грудень 2000	Вимога щодо політики для центрів сертифікації, що випускають кваліфіковані сертифікати
TS 101 862 v1.1.1	Грудень 2000	Профіль кваліфікованого сертифіката
TS 101 733 v1.2.2	Грудень 2000	Формати електронного підпису
ES 201 733 v1.1.3	Травень 2000	Формати електронного підпису

CEN's Information Society Standardization System (CEN/ISSS) відповідає за частину робочої програми EESSI, що пов'язана зі стандартами якості та функціонування для Постачальників Послуг із Сертифікації (CSPs) і за стандарти якості й функціонування для механізмів вироблення та перевіряння підпису.

З метою виконання своєї частини робочої програми CEN/ISSS створила Відділ електронного підпису.

Він охоплює такі напрямки:

– вимоги щодо безпеки для довірчих механізмів і систем;

– вимоги щодо безпеки для безпечних механізмів вироблення підпису;

– операційне середовище створення підпису;

– механізми та середовище перевірки підпису;

– оцінка узгодженості механізмів і послуг електронного цифрового підпису.

Таким чином, у ЄС прийнятий загальний підхід, аналогічний до підходу в США: кожна країна будує свою ІВК, а потім вони будуть об'єднуватись. На цей час наведені нормативні документи набули чинності.

Необхідно також відзначити, що в Європі з 2000 року було розпочато спробу створити загальноєвропейську ІВК з назвою Euro PKI. Був створений ЦСК Вищого Рівня. Роботи щодо його створення розпочалися з проектів ICE-TEL та ICE-CAR. Засновником цих робіт була Європейська Комісія, яка працювала за програмою Телематика для Дослідження (European Commission under the Telematics for Research programme).

На сьогодні EuroPKI має центри сертифікації в багатьох країнах Європи. Структура наведена у табл. 8.6.

8.4. СТАН СТВОРЕННЯ ТА ЗАСТОСУВАННЯ ІВК В РОСІЙСЬКІЙ ФЕДЕРАЦІЇ

У Російській Федерації ІВК визначається як «комплекс організаційно-технічних заходів та програмно-апаратних засобів, необхідних для використання технології з відкритими ключами» [229, 232].

З організаційної точки зору інфраструктура відкритих ключів Російської Федерації включає:

– центри сертифікації відкритих ключів різного призначення;

– центри реєстрації власників сертифікатів відкритих ключів;

– власників сертифікатів відкритих ключів;

– користувачів сертифікатів або осіб, що покладаються на сертифікати відкритих ключів.

Юридичною та технологічними основами взаємодії учасників ІВК є законодавча й нормативна бази, технічні стандарти та специфікації, спеціальні програмні й апаратні засоби та експлуатаційна документація.

Спрощена інфраструктура відкритих ключів Російської федерації наведена на рис. 8.6. Розгляд інфраструктури підтверджує, що в основу її побудови покладено принцип ієрархії.

Таблиця. 8.6. **Структура загальноєвропейської ІВК**

	EuroPKI Top Level CA		
*		EETIC CA (European Entrapreneurs Telematics Initiatives Committee)	
*		Italian CA (EuroPKI)	
*	*		CSP CA Centro di Supercalcolo Piemonte
*	*		Politecnico di Torino CA
*	*		CA del comune di Roma (discontinued)
*	*		CA del comune di Modena
*	*		Provincia di Macerata CA
*	*		CA UniMoRe (Universit di Modena e Reggio Emilia)
*		Slovenian CA	
*	*		Trade Point Slovenia CA
*		Polish CA	
*	*		Research and Academic Computer Network EuroPKI CA – NASK EuroPKI
*	*		Certification Authority EuroPKI «CKPL_LODMAN_CA» Technical University Computer Center
*		Romanian CA	
*		Norwegian CA (UNINETT)	
*		British CA (University College of London)	
*		Irish CA (Trinity College of Dublin)	
*		Austrian CA (Institute for Applied Information Processing and Communications)	
*		Lithuanian CA	
*		Spanish CA (IRIS–PCA)	

Ключовими елементами інфраструктури відкритих ключів Російської Федерації є засвідчувальні центри – федеральний засвідчувальний центр, засвідчувальні центри суб'єктів федерації, засвідчувальні центри федеральних відомств, а також регіональні засвідчувальні центри суб'єктів федерації та федеральних відомств. Особливими функціями наділені регіональні та відомчі центри реєстрації користувачів.

Федеральний закон РФ «Об электронной цифровой подписи» виділяє два типи засвідчувальних центрів: відкритий, тобто такий, що працює в рамках інформаційної системи загального користування, і корпоративний, що надає послуги в корпоративній інформаційній системі.

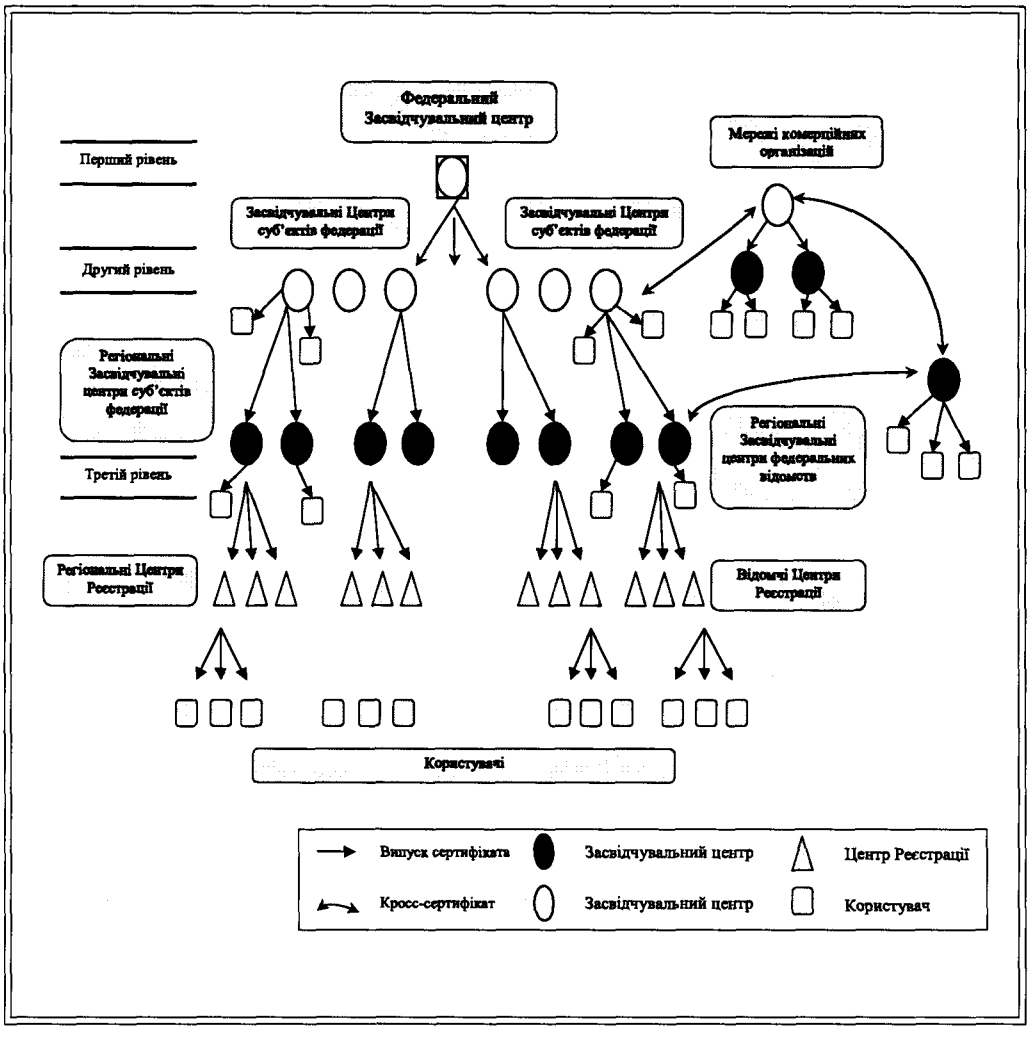

Рис. 8.6. Схема побудови федеральної інфраструктури відкритого ключа РФ

Таблиця 8.7. **Функції засвідчувального центру**

Функції засвідчувального центру	Характер функцій
Прийом запитів на видачу сертифіката від користувачів Перевірка інформації про користувачів Реєстрація користувачів Формування шаблонів сертифікатів Видача сертифікатів	Реєстраторські функції
Ведення бази виданих сертифікатів Підтвердження сертифікатів на запити користувачів Публікація довідників сертифікатів Формування та публікація списків скасування сертифікатів (ССС)	Ведення баз сертифікатів
Організація та підтримка схем оповіщення користувачів про події, що відбуваються в системі Прийом та обробка повідомлень про компрометацію ключів користувачів Розбір конфліктних ситуацій	Підтримка користувачів
Зберігання ключів Зберігання електронних документів Незалежне посвідчення документів Простановка позначки часу Крос-сертифікація з іншими системами	Надання додаткових послуг

Аналіз функцій засвідчувальних центрів дозволяє згрупувати їх за принципами, наведеними в таблиці 8.7.

Організація роботи засвідчувального центру покроково виглядає так:

1. *Користувач.* Подає в паперовому або електронному вигляді, залежно від типів сертифікатів і вимог системи, заявку на одержання сертифіката в засвідчувальний центр.

Під подачею заявки розуміють виконання всіх необхідних формальностей щодо укладання договору, у разі його потреби, заповнення анкети користувача та надання необхідних документів/ їхніх засвідчених копій. Перелік документів, що вимагаються, залежить від того, є користувач фізичною чи юридичною особою, а також від типу та призначення сертифіката, що передбачається одержати. У разі одержання сертифікатів з мінімальним рівнем безпеки/ надійності можливий спрощений порядок, що припускає обмін інформацією винятково в електронній формі.

2. *Засвідчувальний центр* виконує такі операції:

– перевіряє інформацію, що надана користувачем;

– заносить інформацію про користувача в інформаційну систему;

– формує та фізично передає користувачеві ключі й сертифікати реєстрації користувача;

– передає користувачеві спеціальне програмне забезпечення, необхідне для генерації особистих і відкритих ключів (за необхідності), а також програмно-апаратні засоби для наступної роботи із сертифікатами;

– інструктує користувача про порядок формування, реєстрації ключів і подальшої роботи з електронним цифровим підписом.

3. *Користувач* виконує такі дії:

– встановлює програмно-технічні засоби на своєму комп'ютері;

– генерує секретний і відкритий ключі електронного цифрового підпису;

– передає відкритий ключ, що підписаний за допомогою ключа реєстрації у засвідчувальний центр.

4. *Засвідчувальний центр* робить такі операції:

– на основі інформації, що отримана від користувача, формує шаблон сертифіката відкритого ключа;

– на основі отриманого від центра реєстрації шаблона формує та передає у центр реєстрації сертифікат відкритого ключа користувача;

– безпосередньо видає сертифікат користувачеві.

5. *Засвідчувальний центр* також:

– інформує користувача про події в системі;

– здійснює технічну підтримку користувача;

– бере участь у розборі конфліктних ситуацій;

– публікує довідники сертифікатів;

– публікує списки скасування сертифікатів;

– при запитах користувача та третіх осіб підтверджує дію сертифіката;

– одержує й обробляє повідомлення про компрометацію ключа користувача, а також виконує дії щодо відновлення компрометованого ключа користувача;

– одержує й обробляє повідомлення про зміни в інформації щодо користувача;

– у разі необхідності також надає інші додаткові послуги.

Взаємодію між засвідчувальним центром та користувачами/ власниками сертифікатів можна здійснювати двома способами. У першому випадку сам засвідчувальний центр веде роботу з користувачами напряму, що описано вище.

За наявності великої кількості користувачів або їх значного географічного розподілу по території це не завжди зручно з технічної точки зору, оскільки передбачається, що під час реєстрації користувача виникає необхідність не тільки приймати від нього паперові документи, але в ряді випадків буде потрібен і особистий візит користувача до засвідчувального центру. Другий спосіб полягає в тому, що засвідчувальний центр передає частину функцій реєстрації користувачів третій стороні – центру реєстрації. При цьому взаємодія центру реєстрації та засвідчувального центру здійснюється в такий спосіб.

1. *Користувач* подає в паперовому чи електронному вигляді, залежно від типів сертифікатів і вимог системи, заявку на одержання сертифіката в центр реєстрації.

2. *Центр реєстрації* виконує такі дії:

– перевіряє інформацію, що надана користувачем;

– формує та фізично передає користувачеві ключі й сертифікати реєстрації користувача;

– у разі необхідності передає користувачеві спеціальне програмне забезпечення, що необхідне для генерації секретних і відкритих ключів, а також для наступної роботи із сертифікатами;

– інструктує користувача про порядок формування та реєстрації ключів.

3. *Користувач* виконує таке:

– установлює на своєму комп'ютері програмно-технічні засоби;

– генерує особистий і відкритий ключі;

– передає відкритий ключ, що підписаний за допомогою ключа реєстрації, у центр реєстрації.

4. *Центр реєстрації* виконує такі операції:

– на основі інформації, що отримана від користувача, формує шаблон сертифіката відкритого ключа;

– передає шаблон сертифіката в засвідчувальний центр.

5. *Засвідчувальний центр* на основі отриманого від центра реєстрації шаблону формує та передає в центр реєстрації сертифікат відкритого ключа користувача.

6. *Центр реєстрації* видає користувачеві сертифікат відкритого ключа.

Далі він виконує функції, що можуть здійснюватися як центром реєстрації, так і засвідчувальним центром, а деякі також третіми організаціями – сервісними компаніями, виробниками та продавцями програмного забезпечення, у тому числі:

– інформує користувача про події в системі;

– здійснює технічну підтримку користувача;

– одержує та передає в засвідчувальний центр повідомлення про компрометацію ключа користувача;

– бере участь у розв'язанні конфліктних ситуацій;

– публікує довідники сертифікатів і списки відкликаних сертифікатів;

– на запит користувача та третіх осіб підтверджує дію сертифіката;

– одержує й обробляє повідомлення про компрометацію ключа користувача та бере участь у його відновленні;

– одержує й обробляє повідомлення про зміни в інформації про користувача;

– надає інші додаткові послуги.

Наведена схема організації взаємодії сторін представляється досить обґрунтованою, оскільки вона передбачає чіткий розподіл функцій, що вимагають великої частки участі людини (реєстрація), і функцій, що допускають переважно автоматичну комп'ютерну обробку інформації (усі інші). Причому функції істотно розрізняються за своєю природою та вимагають різних підходів до їхньої організації та управління ними.

Окрім функцій реєстрації, засвідчувальний центр може передати третім особам і частину інших своїх функцій, наприклад, функції з технічної підтримки користувачів, розв'язання конфліктних ситуацій тощо.

Припускається, що варіант з виділенням функцій реєстрації користувачів буде активно використовуватися у федеральній системі керування сертифікатами, оскільки технічно складно та нерентабельно створювати таку кількість засвідчувальних центрів, що відповідала б числу територіальних одиниць Російської Федерації [230]. Подібну ж схему будуть використовувати великі відкриті системи

сертифікації, які захочуть забезпечити собі широку регіональну присутність, а крім того й корпоративні засвідчувальні центри, які зможуть використовувати таку схему для розвитку свого бізнесу.

Відповідно до визначення згідно зі ст. 3 Закону РФ «Об электронной цифровой подписи», «Сертифікат ключа підпису – документ на паперовому носії або електронний документ із електронним цифровим підписом уповноваженої особи засвідчувального центру, що включає в себе відкритий ключ ЕЦП, який видається засвідчувальним центром учаснику інформаційної системи для підтвердження дійсності електронного цифрового підпису та ідентифікації власника сертифіката ключа підпису».

Закон РФ «Об электронной цифровой подписи» також встановлює перелік інформації, що повинна міститися в сертифікаті (ст. 6), а саме:

– унікальний реєстраційний номер сертифіката ключа підпису в реєстрі засвідчувального центру;

– дати початку і закінчення строку його дії;

– прізвище, ім'я та по батькові власника сертифіката ключа підпису або псевдонім власника;

– відкритий ключ ЕЦП;

– найменування засобу ЕЦП, з яким використовується даний відкритий ключ ЕЦП;

– найменування та місце розташування засвідчувального центру, що видав сертифікат ключа підпису;

– відомості про відносини, у рамках яких електронний документ із електронним цифровим підписом буде мати юридичне значення.

Закон допускає внесення інших відомостей до тексту сертифіката, у тому числі за заявою власника сертифіката. Власник сертифіката є власником відкритого ключа ЕЦП, підтвердженого сертифікатом.

Користувач сертифіката – це особа, що покладається на сертифікат при здійсненні певних дій або, словами Федерального Закону «Об электронной цифровой подписи» (ст. 3), «фізична особа, що використовує отримані в засвідчувальному центрі відомості про сертифікат ключа підпису для перевірки приналежності електронного цифрового підпису власникові сертифіката ключа підпису».

На сьогодні в Російській Федерації не встановлений який-небудь стандарт, що визначає формат сертифіката. Однак аналіз продуктів російських компаній-виробників дозволяє зробити висновок про те, що в Росії схиляються до розробки національного профілю на основі формату X.509.

8.5. ОСОБЛИВОСТІ ЗАСТОСУВАННЯ ІВК В АВСТРАЛІЇ

ІВК в Австралії почала свій розвиток у 1990 році як частина сектора «Технології комунікацій та інформації» (Information and Communications Technology, ICT). Розпочали розробляти продукти для ІВК приватні компанії Security Domain та Signet Systems, які з часом були викуплені міжнародними компаніями (Baltimore Technologies та Spyrus відповідно). Перший ЦСК почав працювати в 1990 році і був розроблений Security Domain разом з Поштою Австралії (Australia Post) [233 – 234].

В Австралії ЕЦП підтримується законодавчими актами, які не накладають ніяких обмежень на технології ЕЦП. Закон про Електронні транзакції (Electronic Transactions Act 2000) ґрунтується на моделі закону про електронну комерцію, що дозволяє сторонам використовувати будь-які технології ЕЦП (за попередньою домовленістю).

У 2003 році федеральний уряд створив регулюючий орган, названий «Сторож» ("Gatekeeper"), для управління цифровими сертифікатами в урядових цілях. У рамках цього проекту було запущено декілька ЦСК.

На цей момент популярність ІВК в Австралії не велика, але зростає. За статистикою на 2005 рік у країні існує дві значні ІВК: ІВК Податкової служби (100000 сертифікатів) та ІВК медичної сфери (7000 сертифікатів).

У 2006 році запущено програму з випуску цифрових сертифікатів на смарт-картках, які будуть використовуватись як посвідчення водія. Планується випустити близько 2 млн. сертифікатів.

Висновки та проблемні питання

1. Аналіз досвіду створення та експлуатації ІВК у різних країнах дозволяє визначити сутність проблем створення ІВК на різних рівнях.

На правовому рівні – це регулювання взаємовідносин між учасниками процесів сертифікації.

На системному рівні – обґрунтування доцільності архітектури ІВК з урахуванням задач, що вирішуються на рівні держави, відомств, державних і правових підприємств, суспільних організацій.

На процедурно-функціональному рівні – визначення та закріплення основних функціональних вимог до системи сертифікації, встановлення переліку послуг центрів сертифікації.

На функціонально-технічному – визначення функціональності й організації центрів сертифікації та висування вимог безпеки до центрів з метою забезпечення необхідної якості, надійності та безпеки надання послуг.

На технічному рівні – вибір та ефективна реалізація апаратних, програмно-апаратних засобів центрів сертифікації, у тому числі криптографічних засобів.

2. Основними проблемами, що стримують широке застосування технологій ІВК, є:

– проблеми інтероперабельності різних систем ІВК;

– недостатній досвід роботи систем ІВК у відомствах і корпораціях;

– висока вартість реалізації рішень;

– недостатня визначеність та узгодженість політик застосування сертифікатів;

– високі вимоги до рівня підготовки обслуговуючого персоналу та користувачів.

3. Найбільш поширеним типом архітектури ІВК є ієрархічна архітектура, особливо у державному секторі. Такі архітектури дозволяють здійснювати управління з єдиного державного органу.

4. Усі країни при створенні національних ІВК та визначенні основних структур даних спираються на міжнародний стандарт ISO/IEC 9594-8 | ITU-T Rec.

X.509:2005. На основі вимог цього стандарту розробляються національні профілі сертифіката та списку скасування сертифікатів.

5. Цілком зрозуміло, що під час створення ІВК в Україні виникли схожі проблеми. С точки зору архітектурної побудови ІВК для державного сектора України найбільш прийнятним є підхід побудови ієрархічної структури центрів. Причому побудова ІВК має йти зверху. Такий підхід виключає виникнення можливих розбіжностей на різних проблемних рівнях ІВК, а також дозволить оптимізувати витрати державних коштів на побудову ІВК.

Для вирішення проблем функціональної сумісності найбільш прийнятним підходом є стандартизація функцій, структур даних, протоколів обробки тощо. Побудову комплексу стандартів у цій галузі доцільно почати із застосування гармонізованого в Україні міжнародного стандарту ДСТУ ISO/IEC 9594-8:2006. На основі цього стандарту слід розвивати інші напрямки стандартизації в цій галузі.

6. Однією з найбільших проблем, що явно постала в ЄС, США, РФ та на міжнародному рівні в цілому, є забезпечення взаємодії користувачів різних ЦСК, у тому числі різних держав та ЄС. Особливо гострою ця проблема виявилася для внутрішнього застосування в ЄС та США, а також для взаємодії на міжнародному рівні практично всіх користувачів ІВК. Не виключенням щодо цього є й Україна. Як показав попередній аналіз, для України ця проблема є більш гострою, оскільки в ній недопущеними до використання є стандарти цифрового підпису та направленого шифрування, що базуються на перетвореннях в кільцях – RSA криптографічні перетворення.

У той же час RSA криптографічні перетворення на сьогодні використовуються як основні в США, ЄС, Канаді, Австралії та інших провідних країнах світу.