Розділ 12

ОСНОВНІ ПОЛОЖЕННЯ РЕАЛІЗАЦІЇ ПЕРСПЕКТИВНОЇ ПОЛІТИКИ СЕРТИФІКАЦІЇ X-509

12.1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

12.1.1. Початкові положення

Нині можна говорити про початок нового етапу розвитку та вдосконалення ІВК. Цей етап, на наш погляд, розпочався вдосконаленням Політик сертифікації X-509. Перш за все на розгляд заслуговують результати та пропозиції, отримані при вдосконаленні Інфраструктури управління ключами (ІУК) Міністерства оборони США [236] (надалі – відомства). Вона призначена для забезпечення системних та інженерних рішень у вигляді продуктів і послуг захисту інформаційно-телекомунікаційних систем, заснованих на комп'ютерних мережах. Суттєвою частиною ІУК є Інфраструктура відкритого ключа (ІВК, PKI). Вона складається з продуктів і послуг, за допомогою яких забезпечують управління сертифікатами згідно X-509, тобто при застосуванні асиметричної криптографії. Сертифікати забезпечують ідентифікацію індивідуума, що зазначений у сертифікаті, а також зв'язують його з конкретною парою відкритого/ особистого ключів і видавником сертифікату.

Щодо програм, які здійснюють або підтримують відомства, вимагається надання таких послуг, як конфіденційність, автентичність, технічна невідмовність (надійність) та управління доступом. Указані послуги забезпечуються з використанням таких компонентів мережевого захисту, як робочі станції, охоронні пристрої, брандмауери, маршрутизатори, вбудовані мережеві шифратори (INE) та довірчі сервери баз даних тощо. Дії із захисту вказаних компонентів підтримуються та доповнюються з використанням ІВК, тобто сертифікатів відкритих ключів X-509.

Послуги управління захистом, що забезпечуються з використанням ІВК, включають таке:

1) генерація/ зберігання/ відновлення ключів;

2) генерація, модифікація, відновлення, перекодування та розповсюдження сертифікатів;

3) генерація списку скасувань (CRL) і розповсюдження сертифікатів;

4) директивне управління елементами сертифікації;

5) ініціалізація/ програмування/ керування засобами, що містять сертифікати;

6) управління привілеями та санкціонуванням;

7) функції системного адміністрування (наприклад, аудит захисту, управління конфігурацією, архівування тощо).

Якісне надання вказаних послуг гарантується виконанням вимог щодо ІВК, включаючи такі:

1) ідентифікація абонента й перевірка його повноважень;

2) управління комп'ютерними та криптографічними системами;

3) експлуатація комп'ютерних і криптографічних систем;

4) використання ключів і сертифікатів відкритого ключа абонентами та залежними сторонами;

5) визначення правил для обмеження зобов'язань і забезпечення вищого ступеня впевненості в дотриманні умов цієї політики.

Надійність частини рішень захисту, що засновані на асиметричній криптографії, безпосередньо визначається безпечністю та надійністю функціонування ІВК, що використовується, включаючи устаткування, засоби, персонал і процедури.

Положення, що застосовуються в такій політиці, мають бути обґрунтованими щодо мінімальних вимог, а органи акредитації можуть вимагати вищих рівнів гарантій, ніж зазначено в конкретній політиці сертифікації для відповідних застосувань.

Політика Сертифікації відомства (СР) – це об'єднана політика, згідно з якою встановлюється та діє Центр Сертифікації (СА) ключів, який керується компонентом відомства. Така Політика не визначає конкретні реалізації PKI, не містить конкретних планів майбутніх реалізацій чи майбутніх Політик Сертифікації. Вона також не визначає політику сертифікації для СА, керування якими здійснюється зовнішніми об'єктами від імені відомства, досвіду експлуатації, загроз, що змінюються. Політика повинна переглядатись і модифікуватись з урахуванням досвіду експлуатації, зміни моделей загроз і порушників, а також за результатами подальшого аналізу.

Політика, що розглядається в цьому розділі, визначає порядок створення й управління X-509 сертифікатами відкритого ключа Версії 3 для використання в застосуваннях, що вимагають зв'язку між елементами мережевих комп'ютерних систем. Такі застосування включають:

– електронну пошту;

– передачу несекретної і секретної інформації;

– підпис електронних форм;

– підписи електронних договорів;

– автентифікацію таких компонентів інфраструктури як Web-сервери, брандмауери і каталоги. Телекомунікаційні системи в них можуть бути як незахищеними мережами, наприклад, Інтернет або несекретна мережа маршрутизатора Інтернет-протоколу (NIPRNET), а також захищеними мережами, наприклад такими як секретна мережа маршрутизатора Інтернет-протоколу (SIPRNET).

12.1.2. Рівні гарантій

Рівні гарантій, що можуть бути забезпечені

Однією з базових вимог Політики є забезпечення певних рівнів гарантій. Відомство, тобто Міністерство оборони США, зареєструвало дев'ять рівнів гарантій. Кожному рівню гарантій призначений ідентифікатор об'єкта (OID), що вказується в сертифікатах, випущених CA, зв'язаних із цим рівнем, відповідно до умов політики.

Ідентифікатор об'єкта OID реєструється під id-infosec позначкою як:

{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) certificate-policy(11)}

id-US-dod-basic ID::= {id-certificate політика 2}

id-US-dod-medium ID::= {id-certificate політика 5}

id-US– dod-medium-2048 ID::= {id-certificate політика 18}

id-US– dod-medium Hardware ID::= {id-certificate політика 9}

id-US-dod-medium Hardware-2048 ID::= {id-certificate політика 19}

id-US-dod-PIV-auth ID::= {id-certificate політика 10}

id-US-dod-PIV-auth-2048 ID::= {id-certificate політика 20}

id-US-dod-high ID::= {id-certificate політика 4}

id-US-dod-type1 ID::= {id-certificate політика 6}

Політика, що розглядається, стосується тільки тих політик, які потрібні для PKI, що затверджені як DoD Medium {5}, Medium-2048 {18}, Medium Hardware {9}, Medium Hardware-2048 {19}, PIV-Auth {10}, PIV-Auth-2048 {20} або High {4} Гарантійні OID.

Умови, представлені в цій Політиці, можуть застосовуватись до семи рівнів гарантійних (Medium, Medium-2048, Medium Hardware, Medium Hardware-2048, PIV-Auth, PIV-Auth-2048 і High), якщо не вказано інше.

Якщо не вказано інше, всі посилання на «Середню Гарантію» стосуються Medium, Medium-2048, Medium Hardware, Medium Hardware-2048, PIV-Auth і PIV-Auth-2048 сертифікатів.

За винятком розміру ключа, вимоги Політики ідентичні для таких пар OID:

1) Medium і Medium-2048;

2) Medium Hardware і Medium Hardware-2048;

3) PIV-Auth і PIV-Auth-2048.

Сертифікати, що вказують PIV-auth OID, задовольняють усім вимогам для Medium Assurance Hardware (апаратних засобів із середньою гарантією), за винятком лише того, що сертифікати, які вказують PIV-auth OID, повинні також вказувати використання ключів digital Signature і ніщо інше. Сертифікати, що вказують PIV-auth-2048 OID, задовольняють всім вимогам Medium Assurance Hardware (Medium Hardware-2048), за винятком лише того, що сертифікати, у яких вказують PIV-auth-2048 OID, повинні також вказувати використання ключів digital Signature і ніщо інше.

12.1.3. Учасники ІВК

Учасниками ІВК є центри сертифікації (CA), центри реєстрації (RA) та користувачі. Центр Управління Політикою відомства (PMA) є органом, що призначений для виконання таких функцій:

– нагляд за створенням і відновленням політик сертифікації, включаючи оцінку змін, що визначені службами й відомствами Міністерства, і плани щодо реалізації будь-яких прийнятих змін;

– своєчасне забезпечення відповідної координації служби і відомства Міністерства щодо його CP через процес досягнення консенсусу;

– перегляд технологій сертифікації (CPS) Міністерства шляхом аналізу документів CPS щодо гарантії, що технологія CMA, призначена для обслуговування Міністерства, відповідає DoD Політикам Сертифікації;

– перегляд результатів CMA перевірок з метою визначення відповідності CMA затверджених CPS документів, а також вироблення рекомендацій до CMA стосовно дій або заходів, таких як скасування CMA сертифікатів;

– встановлення придатності Політик, що не відповідають вимогам DoD політик, для використання в межах Міністерства (наприклад, у випадках, де розглядається технічний механізм «політики відображення»);

– розробка рекомендацій для DoD Програмних і Проектних Адміністраторів і DoD Центрів Акредитації Інформаційних Систем щодо доцільності сертифікатів, зв'язаних з DoD політиками сертифікації для конкретних застосувань.

Повноваження центру управління політикою з прийняття рішень належать Директору з Інформаційних технологій комітету DoD та його фахівцям. PMA може делегувати повноваження у відповідні DoD політики й інструкції.

Як Центри сертифікації, так і Центри реєстрації (RA) є «Центрами управління сертифікатами» (CMA). Будемо використовувати термін CMA, коли функція може бути призначена для CA або для RA або коли вимога застосована як до CA, так і до RA. Термін «Центр реєстрації» включає такі об'єкти, як локальні центри реєстрації. Розділення зобов'язань з реєстрації абонентів між CA і RA може змінюватися при реалізації певної політики сертифікації. Це розділення зобов'язань повинне бути описано в CPS положеннях CA.

12.1.4. Характеристика об'єктів ІВК

Учасниками ІВК є центри сертифікації (CA), центри реєстрації (RA) та абоненти (користувачі).

Центр сертифікації (CA) – це об'єкт, акредитований PMA для виготовлення та обслуговування сертифікатів відкритого ключа. CA відповідальний за всі аспекти видання й управління сертифікатами, включаючи управління процесами реєстрації, ідентифікації й автентифікації, виготовлення сертифікатів, видання сертифікатів, відкликання сертифікатів та їх перекодування. Також він відповідальний за гарантію, що всі аспекти надання послуг центром і виконання операцій, пов'язаних із сертифікатами, виданими згідно з діючою Політикою, виконуються відповідно до вимог і гарантій Політики. CA є інклюзивним і включає всі типи CA. Будь-яка вимога CA, що міститься в Політиці, може застосовуватись до всіх типів CA, якщо тільки явно не визначено інше.

У разі ієрархічної ІВК СА повинні підкорятися Кореневому СА (і максимум проміжному СА). Природа підпорядкування має бути описана. Реалізація такої ієрархії повинна здійснюватися через процедуру розширення сертифікату. Центр СА, для якого другий СА є підпорядкованим, називається *вищим* СА.

Центр реєстрації (RA) – це об'єкт, який вступає в угоду з СА для збору інформації, а також верифікації особи й інформації абонентів, яка має бути введена в сертифікати відкритого ключа. Центр RA повинен виконувати свої функції відповідно до регламенту CPS, затвердженого PMA.

Абонент – це об'єкт, чиє ім'я міститься в сертифікаті і який підтверджує відповідним чином, що він використовує свій ключ і сертифікат згідно з політикою сертифікації.

12.1.5. Використання сертифікатів

Сертифікати, що вказують OID Політики, які визначаються, повинні використовуватися тільки для транзакцій, пов'язаних з діями відомства. Центр СА повинен заявити цю вимогу у своїх CPS і накладати на Абонентів вимогу дотримання цього обмеження.

Відомча ІВК (PKI) повинна підтримувати такі послуги захисту: конфіденційність, цілісність, автентифікацію (справжність) і надійність (технічна невідмова). ІВК підтримує ці послуги захисту через забезпечення ідентифікації й автентифікації, цілісності й технічної надійності через застосування цифрових підписів, а конфіденційність через узгодження ключів. Ці основні послуги захисту забезпечують довгострокову цілісність підписаних даних, але не можуть забезпечити цілісність для всіх прикладних застосувань. Наприклад, коли існує вимога для верифікації достовірності підпису поза періодом достовірності сертифіката, що встановлений контрактом, наприклад, довірча тимчасова мітка.

ІВК повинна забезпечувати підтримку для широкої різноманітності застосувань, у яких забезпечується обробка таких видів інформації як:

– адміністративна й фінансова Інформація;
– інформація системи національної безпеки;
– інформація цільової категорії гарантії;
– інформація цільової категорії гарантії різних рівнів конфіденційності;
– секретна інформація аж до надсекретної;
– електронна комерція тощо.

Здається, що мета може бути реалізована через підтримку кожного із застосувань, але через різні правові вимоги, національну політику й політику захисту різних категорій інформації, економічно найефективнішим є рішення, що ґрунтується на підтримці всієї множини гарантій різних рівнів.

Рівень гарантій пов'язується із сертифікатом відкритого ключа, що ґрунтується на довірі до СА, який абонент може обґрунтовано встановлювати засобом зв'язування свого відкритого ключа з особою та привілеями, які заявлені в сертифікаті. При цьому рівень гарантій залежить від належної реєстрації абонентів і належної генерації й управління асиметричною парою ключів відповідно до вимог Політики. Також персонал, фізичні, процедурні й технічні

засоби керування захистом впливають на рівень гарантій сертифікатів, випущених системою ІВК.

Ступінь довіри до сертифіката, що приймається користувачем, визначається різноманітними чинниками ризику. Особливо, видом інформації, моделлю загроз і порушника.

Зміст інформації необхідно відокремлювати від важливості інформації щодо досягнення цілей і завдань відомства, особливо для бойових військових завдань та електронної комерції. Обов'язковими є такі послуги як конфіденційність інформації, критичність інформації відомства або критичність інформації, що визначається грошовими сумами в електронній комерції.

Загроза – це будь-яка обставина чи подія, що може призвести або призводить до нанесення шкоди. У термінах інформаційних систем термін «шкода» включає знищення, розголошування або модифікацію даних, процесів або оброблювальних компонентів. Загрози для системи включають екологічні лиха, фізичне руйнування, проникнення в систему, несанкціонований доступ, помилку людини та спостерігання чи підробку комунікаційних зв'язків. Під час оцінки загроз, що створюються порушником, необхідно враховувати його можливості, стійкість до ризиків і доступність. У результаті досліджень відомство може дійти висновку, що значна більшість компрометацій відбувалася через здійснення загроз з боку інсайдерів, тобто фізичних або юридичних осіб, які завдяки своєму службовому становищу або привілеям мали вільний доступ до банківської інформації.

Відомчі мережі даних, у яких використовуватимуться сертифікати, що описані в політиці, повинні мати різні рівні захисту. Механізми, які реалізуються для захисту в мережах, повинні забезпечувати різні рівні захисту. Прикладами механізмів, що забезпечують мережевий захист, можуть бути мережеве шифрування, фізична ізоляція, високогарантійні охоронні пристрої та брандмауери. Ці механізми використовуються для створення високозахищених мереж і анклавів. Імовірність здійснення атаки в такі захищені мережі може бути зменшена завдяки:

1) обмеженню доступу при використанні мережі й точок зв'язку з іншими мережами, наприклад, за рахунок застосування охоронних пристроїв або міжмережевих екранів (навіть відносно тих, хто має санкціонований доступ, стійкість до ризиків має бути висока високою);

2) утрудненню здатності зловмисника до дій усередині мережі через захист від хакерів і трудністю внесення засобів їх здійснення іззовні.

Дійсна оцінка зменшення ризику, що пов'язана з використанням механізмів послаблення ризиків, може бути визначена тільки конкретною оцінкою рівня захищеності на системному рівні.

Для середовищ, що захищаються, необхідно мати можливість захисту з такими рівнями – *високий, нормальний* (*помірний*) *та задовільний* (*мінімальний*).

У середовищах, де потрібен високий рівень захисту, необхідно, щоб:

– у мережах конфіденційність забезпечувалась за допомогою пристроїв шифрування, що затверджені до використання спеціальною службою для захисту секретної інформації;

– здійснювалась фізична ізоляція мереж, що застосовуються для обробки даних з високим рівнем секретності, доступ до яких може бути тільки через відповідний допуск до секретних матеріалів з боку держави.

У середовищах, де потрібен нормальний рівень захищеності, необхідно застосовувати ізольовані несекретні мережі, а також повинне здійснюватись затверджене шифрування інформації. За деяких обмежень до такої інформації доступ можуть мати іноземні громадяни.

У середовищах, де потрібен задовільний рівень захищеності, під'єднання до Інтернету повинне здійснюватись через брандмауер або спеціально допущені засоби, шифрування інформації в таких мережах є необов'язковим.

12.1.6. Сутність основних рівнів гарантій використання сертифікатів

У відомстві при використанні сертифікатів за запитами має забезпечуватись 9 рівнів гарантій. Основна увага повинна приділятися наданню таких послуг, як цілісність і управління доступом до інформації, що вважається для відомства конфіденційною, а також до інформації, що пов'язана з електронними фінансовими транзакціями й іншою електронною комерцією. Завжди кінцевий вибір механізмів захисту, рівня стійкості та гарантій вимагає управління ризиками, що стосується конкретного завдання й середовища. Орган, відповідальний за затвердження кожного специфічного рівня гарантій, звичайно повинен бути органом, що має права здійснення акредитації. Основні вимоги до рівнів гарантій такі:

1 рівень – Базовий рівень гарантій (DoD Basic Assurance). Цей рівень призначений для застосувань, які обробляють несекретну інформацію низького некритичного значення в мінімально або помірно захищеному середовищі. Відомчий СА не може випускати базові сертифікати, він повинен випускати виключно сертифікати середньої та високої гарантії. Доступ до відомчих інформаційних ресурсів ніколи не повинен дозволятися на підставі базових сертифікатів. Базові сертифікати (або відомчі еквівалентні сертифікати) можуть застосовуватись взаємодіючим з відомством з метою автентифікації або шифрування інформації при її передачі в телекомунікаційній системі, щоб запобігти несанкціонованому доступу або несанкціонованій обробці відомчої інформації (наприклад, координація зустрічей, доступ до інформації Web сайту, яка була дозволена для необмеженого розповсюдження). Базові сертифікати можуть, наприклад, бути випущені не відомчими, а комерційними об'єктами (центрами).

2 рівень – Середній відомчий рівень гарантій (DoD Medium Assurance). Цей рівень призначений для застосувань сертифікатів, що використовуються для обробки несекретної інформації середнього значення в помірно захищених середовищах, несекретної інформації вищого значення у високозахищених середовищах, а також для контролю за розмежуванням доступу до секретної інформації в високо захищених середовищах.

3 рівень – Середній відомчий рівень гарантій 2048 (DoD Medium-2048 Assurance). Цей рівень призначається для того ж використання сертифікатів, що й 2 рівень (DoD Medium Assurance), але має більший розмір ключа, як вимагається

керівництвом від Національного Інституту Стандартів і Технологій, тобто не менше 2048 бітів при криптографічних перетвореннях у кільцях і полях.

4 рівень – Середній відомчий апаратний рівень гарантій (DoD Medium Assurance Hardware). Цей рівень призначений для використання сертифікатів у застосуваннях, які обробляють несекретну інформацію середнього значення в мінімально захищених середовищах, несекретну інформацію вищого значення в помірно захищених середовищах і контролю за розмежуванням доступу до секретної інформації в високо захищених середовищах. Цей рівень також призначений для всіх застосувань, що діють у середовищах 2 рівня, але вимагають вищого ступеня гарантії і технічної невідмови.

5 рівень – Середній відомчий апаратний рівень 2048 гарантій (DoD Medium Assurance Hardware-2048). Цей рівень призначений для того ж використання сертифікатів, що й 2 рівень (DoD Medium Assurance), але має більший розмір ключа, як вимагається керівництвом Національного Інституту Стандартів і Технологій, не менше 2048 бітів при криптографічних перетвореннях в кільцях і полях.

6 рівень – PIV відомчий рівень справжніх гарантій (DoD PIV-Auth Assurance). Цей рівень призначений для будь-якого використання сертифікатів, що придатні для 4 рівня (DoD Medium Assurance Hardware), у яких немає вимог до рівня послуги невідмови.

7 рівень – PIV відомчий рівень справжніх гарантій 2048 (DoD PIV-Auth-2048 Assurance). Цей рівень призначений для того ж використання сертифікатів, що й 6 рівень (DoD PIV-Auth Assurance), але має більший розмір ключа, як вимагається керівництвом Національного Інституту Стандартів і Технологій, не менше 2048 бітів при криптографічних перетвореннях у кільцях і полях.

8 рівень – високий відомчий рівень гарантій (DoD High Assurance). Цей рівень призначений для застосувань, що обробляють несекретну інформацію вищого значення (цільова гарантійна категорія I) у мінімально захищених середовищах. Цей рівень придатний і для застосування щодо сертифікатів середньої гарантії, у тому числі:

– надання послуг цифрового підпису для несекретної інформації з гарантією категорії I;

– для захисту інформації, що стосується національної безпеки, у мережах у яких інформація не шифрується;

– забезпечення захисту (автентифікації та конфіденційності) інформації, що перетинає межі класифікації, коли такий перетин уже дозволений згідно з політикою системного захисту (наприклад, пересилка несекретної інформації через HAG від SIPRNET до NIPRNET);

– для забезпечення технічної невідмови для фінансових або електронних комерційних застосувань високого значення.

9 рівень гарантій – (Type 1). Цей рівень призначений для застосунків, що обробляють секретну інформацію в мінімально захищених середовищах, та автентифікації інформації, що може впливати на захищеність секретної системи.

Загальне використання сертифікатів подано в таблиці 12.9, де перелічені всі рівні гарантій. Будь-яке застосування, яке вимагає інформації для перетину межі класифікації, вимагає високого рівня гарантії.

Таблиця 12.9. **Загальне використання сертифікатів**

Значимість інформації	Захищеність мережі		
	Висока	Середня	Мінімальна
Низька	Середній рівень	Середній рівень	Середній рівень
Середня	Середній рівень	Середній рівень	Середній апаратний рівень
Висока	Середній рівень	Середній апаратний рівень	Високий рівень

Організація, що володіє технологією сертифікації (CPS), повинна представляти її до центру управління політикою (PMA) для аналізу відповідності цієї політики сертифікації (CP) заданому рівню гарантій. Центр PMA доручає проведення аналізу відповідності та надає підсумковий письмовий звіт, у якому вказується перелік областей, у яких CPS не може або не забезпечує дотримання цій CP. Центр PMA повинен представити результати аналізу до затвердження CPS. Центр управління сертифікатами CMA повинен мати затверджену центром PMA технологію сертифікації CPS і відповідати всім вимогам CP/CPS до початку надання послуг. У деяких випадках характер системних функцій, тип зв'язків або операційне середовище можуть вимагати додаткового затвердження.

12.1.7. Репозиторії та публікації

Репозиторій є первинним джерелом сертифікатів центра сертифікації CA і/або списків скасування сертифікатів CRL. Він має бути доступним абонентові цілодобово, 7 днів на тиждень з мінімальною повною доступністю 99 % щорічно, включаючи плановані простої, які не повинні перевищувати 0,5 % на рік. При обчисленні доступності репозиторію не враховуються простої, що визначаються простоями мережі.

Репозиторії, які підтримують CA в частині реєстрації інформації згідно з цією Політикою, повинні:

1) підтримувати доступність до інформації, яка вимагається діючою політикою, щодо реєстрації та пошуку сертифікатів та інформації, що належить до послуг CA;

2) забезпечувати механізми управління доступом, що є достатнім для захисту інформації депозиторію згідно з вимогами.

Сертифікати повинні видаватись згідно з діючим регламентом і за умови повідомлення абонента щодо володіння особистим ключем, який разом із відкритим ключем сертифіката є асиметричною ключовою парою. Списки відкликаних сертифікатів CRL повинні видаватися згідно з діючим регламентом. Уся інформація, що міститься в репозиторії, повинна негайно бути доступною та видаватись абонентам після того, як вона стає доступною для центра сертифікації, а також тимчасові межі видання різних типів інформації. Інформація репозиторіїв має бути захищеною від несанкціонованої модифікації та розголошування.

12.2. ІДЕНТИФІКАЦІЯ ТА АВТЕНТИФІКАЦІЯ В ІВК

12.2.1. Іменування в СА

Розглянемо основні концептуальні питання іменування в ІВК, ґрунтуючись на результатах [236].

По-перше, у всіх сертифікатах повинні використовуватися для полів емітента та імені абонента відмітні імена DN форми. Взагалі, центр СА не повинен призначати DN імена. Абоненти повинні мати DN, призначені ним через організації, згідно з прийнятою системою іменувань. Центр управління сертифікатами СМА повинен досліджувати й виправляти імена абонентів, якщо необхідно брати до уваги будь-які можливі колізії імен. При цьому, якщо це можливо, то СМА повинен координувати й виконувати вимоги відповідного центру іменування. Для деяких сертифікатів можуть додатково встановлюватися альтернативні форми імен.

Також для абонентів із середнім і вищим рівнем гарантій ім'я суб'єкта повинне бути не нульовим, і опціональне альтернативне ім'я, якщо воно відмічено як некритичне. Імена, що використовуються в межах відомства, повинні однозначно ідентифікувати персону або об'єкт, яким вони призначені. Центр управління сертифікатами СМА повинен гарантувати, що існує зв'язок між абонентом і будь-якою організацією, яка ідентифікується будь-яким компонентом будь-якого імені в його сертифікаті. Коли використовуються відмітні DN імена, ім'я повинне представляти абонента таким чином, щоб воно було легко зрозумілим для інших абонентів. Для людей-абонентів це зазвичай буде законне ім'я. Для устаткування це може бути ім'я моделі та серійний номер, або назва прикладного процесу (наприклад, Поштовий Список Організації X тощо). Відомство повинне встановити один або більше повноважних органів, відповідальних за створення та підтримку системи DN імен. Центр управління сертифікатами СМА, який використовує DN, повинен координувати роботу з такими повноважними органами для визначення належного іменування для кожного абонента.

Окрім того, кожен кореневий центр СА, який затверджує політику, повинен підписувати тільки сертифікати з підлеглими іменами зсередини простору імен, затвердженого центром управління РМА. У разі якщо один СА засвідчує інший, старший СА повинен накладати обмеження на простір імен, який застосовується в підлеглому СА. Обмеження імен щонайменше повинні бути такими, як і його власні обмеження імен.

Коли для накладення цих обмежень існують технічні засоби (такі наприклад, як розширення сертифіката обмеження імен), вони повинні використовуватися в першу чергу. Інакше обмеження імен повинні накладатися процедурним або договірним способом.

Центр СА не повинен випускати анонімні сертифікати, сертифікати не повинні містити анонімні або псевдонімні посвідчення особи.

При цьому правила інтерпретації форм імені повинні міститись у відповідному профілі сертифіката і встановлюються органом іменування, якщо такий існує, або самим центром СА. Орган іменування повинен бути ідентифікований у договірній формі або в технології CPS. Повинна забезпечуватись унікальність імен в середовищі відомства. Там, де практично повинне використовуватися іменування X.500 DN, – СА і RA повинні забезпечувати унікальність імені в межах

X.500 простору імен. Коли використовуються інші форми імен, вони також повинні бути розміщені таким чином, щоб гарантувати унікальність імені в середовищі відомства. Центр CA повинен документувати у своїй технології CPS, які форми імен використовуються, як CA і RA взаємодіятимуть з органами іменування відомства і як вони розмістять імена для гарантування унікальності імен, у тому числі серед поточних і минулих абонентів.

Також центр управління сертифікатами CMA не може видавати ім'я, яке має обмеження через торгову марку. CMA не повинен випускати сертифікат, знаючи, що він включає ім'я, яке визнане судом компетентної юрисдикції як посягання на торгову марку інших. Центр CMA не зобов'язаний досліджувати торгові марки або вирішати суперечки щодо торгової марки.

12.2.2. Порядок початкового посвідчення особи

Вимоги, що викладаються, стосуються всіх абонентів, включаючи довірчі ролі.

У всіх випадках, коли абонент генерує ключі, йому потрібно довести центру управління сертифікатами CMA, що він володіє особистим ключем, який є парою до відповідного відкритого ключа, що міститься в сертифікаті. Для ключів підпису це може бути зроблено, наприклад, шляхом підпису запиту. Для ключів управління ключами CA або RA це можна зробити за шифруванням сертифіката абонента в повідомленні запиту підтвердження. Потім абонент може розшифрувати і повернути сертифікат до CA або RA у повідомленні підтвердження. Центр управління політикою PMA може визначити інші механізми, які щонайменше є такими ж захищеними, як ті, що вказані як допустимі.

У випадку, коли ключ генерується безпосередньо абонентом, наприклад, в апаратному генераторі ключів, який з високим рівнем захисту записує особистий ключ до електронного ключа абонента, особистий ключ є захищеним від його компрометації. Якщо абонент не володіє електронним ключем, коли генерується асиметрична пара, то він повинен бути доставлений абонентові захищеним шляхом.

Запити сертифікатів від імені організації повинні включати ім'я, адресу організації і статутні документи щодо існування й правочинності організації. Центр CMA повинен верифікувати цю інформацію, окрім встановлення достовірності представника, а також санкції такого представника діяти від імені організації. Використання сертифікатів організації повинно розглядатися у відповідному CMA, і ці CMA повинні запобігати використанню сертифікатів організації, де потрібна неспростовність абонента.

Сертифікати відкритого ключа повинні випускатися від імені індивідуума, як тільки це можливо, а особисті ключі, що зв'язані з такими сертифікатами, ніколи не повинні розділятися з будь-якою іншою особою. Для тих випадків, коли вони діють в одній ролі або в групі, сертифікат може випускатися з відмітним іменем, яке ідентифікує групу або роль. Нижче, у порядку переваг, перелічені альтернативні механізми видачі сертифікатів ролі або групи. Менш безпечні опції повинні використовуватися тільки тоді, якщо опції вищої переваги не можуть бути здійснені.

Унікальні особисті ключі цифрового підпису й шифрування та зв'язані з ними сертифікати, що містять ім'я групи або ролі, повинні бути видані тим особам, що діють від імені або як посередники для групи або ролі.

Кожен індивідуум, що діє в тій самій ролі, повинен мати окремий особистий ключ підпису та сертифікат, що вказує роль. Індивідууми, що діють в одній і тій самій ролі або групі, можуть розділяти один і той самий сертифікат шифрування і зв'язаний особистий ключ.

Сертифікат підпису, що містить відмітне ім'я, яке вказує на роль, може бути виданий, і зв'язаний особистий ключ підпису може розділятися персонами, що діють у цій ролі. (Відзначимо, що відсутність технічно-наказної індивідуальної відповідальності й довіри до процедурних механізмів, як описано у вимогах нижче, являє більший ризик захисту для систем і даних, захищених за допомогою цих сертифікатів, і тому повинна бути обмежена до максимально можливого ступеня. Оскільки послуга невідмови може більше не забезпечуватись, то сертифікати, які відповідають особистим ключам, що тримаються множиною абонентів, не повинні використовуватися для укладення договорів або застосувань в електронній комерції.)

Місцевий повноважний орган повинен санкціонувати створення групових або ролевих сертифікатів.

У таких випадках:

– спонсор (відповідальний) групи/ ролі повинен бути відповідальний за забезпечення управління особистим ключем і відстеження, хто володіє особистим ключем весь час, включаючи підтримку поточного списку абонентів, які мають доступ до використання особистого ключа, а також перелік, який абонент мав право на управління ключем і в який час;

– спонсор (відповідальний) групи/ ролі повинен переслати початковий список і періодично пересилати всі відновлення до локального керівника із системного захисту, з часу останнього представлення цього списку.

Керівник є відповідальним за періодичний перегляд списку спонсора з поглядом на ідентифікацію аномалій. Список тих, хто тримає загальний особистий ключ, повинен бути доступним для CA і RA, за запитом.

Процедури випуску електронних ключів (токенів) для використання загального ключа повинні відповідати всім іншим умовам Політики, що застосовується (наприклад, генерація ключа, захист особистого ключа, обов'язки абонента).

Також центр CMA повинен гарантувати, що ідентифікаційна інформація заявника та відкритий ключ адекватно зв'язані. Кожен CMA повинен вказувати у своїй технології CPS процедури з автентифікації особи абонента. Додатково центр CMA повинен реєструвати процес, якого потрібно дотримуватися щодо кожного сертифіката. Щонайменше технологічна документація повинна включати:

1) засвідчення персони, що виконує ідентифікацію;

2) підписану заяву персони, який верифікував особу абонента, згідно з цією політикою сертифікації;

3) метод, що використовується для автентифікації особи індивідуума, включаючи тип ідентифікації й унікальний числовий або буквено-цифровий ідентифікатор, якщо такий застосовно;

4) дату перевірки.

Додатково технологічна документація повинна включати заяву особи. Заява повинна бути підписана власноруч або за допомогою цифрового підпису, якщо достатньо якісні відбитки пальців або інші дані біометрики зібрані й можуть бути зв'язані з особою абонента. Кожен підпис має бути застосований у присутності персони, що здійснює автентифікацію особи.

Для заявників середньої та високої гарантії доказ особи заявника вимагає надання заявниками щонайменше одного федерального урядового офіційного фотографічного ідентифікаційного посвідчення особи (такого, як DoD ідентифікаційна картка або паспорт) або двох нефедеральних урядово випущених офіційних ідентифікаційних посвідчень особи, щонайменше одне з яких має бути фото-ID, таким, як водійські права. Як альтернатива представленню ідентифікаційних посвідчень особи можуть використовуватися інші механізми еквівалентної або більшої гарантії (такі, як порівняння біометричних даних з посвідченнями особи, заздалегідь перевіреними згідно із стандартами цієї політики і отриманими через засвідчену взаємодію із захищених баз даних).

Для середньої гарантії посвідчення особи заявника має бути персонально верифікованим перед уведенням в дію сертифіката заявника. Заявник повинен персонально пред'являтися для підтвердження особи нотаріусу, засвідченому Федеральним Урядом Сполучених Штатів або урядом штату як санкціонований, наприклад Notaries Public, яка використовує штамп, друк або інший механізм для засвідчення свого підтвердження особи. Крім того, CPS повинен вказувати, яким чином надаватиметься повідомлення про виникнення цієї перевірки особи і як верифікуватиметься виконання відповідним фахівцем перевірки особи

Для Середньої Гарантії посвідчення особи заявника має бути персонально верифікованим перед введенням в дію сертифіката заявника. Заявник повинен персонально пред'являтися таким органам, як:

– CMA;

– довірчому Агенту (TA), що особисто затверджений CMA або призначений ім'ям в документі до CMA від Керівника/ Завідувача організації, яку вони представляють;

– персоні, засвідченій Федеральним Урядом Сполучених Штатів або урядом штату як санкціонований для підтвердження осіб, наприклад такій, як Notaries Public, яка використовує штамп, друк або інший механізм для засвідчення свого підтвердження особи. Крім того, CPS повинен вказувати яким чином надаватиметься повідомлення про виникнення цієї перевірки особи і як верифікуватиметься виконання відповідним фахівцем перевірки особи.

Заявник повинен з'явитися перед одним з потрібних засвідчувачів осіб не пізніше 30 днів до приєднання підпису CA до сертифіката заявника, або альтернативно, коли особисті ключі постачаються абонентам з використанням апаратних токенів (електронних ключів). Абоненти повинні персонально з'явитися перед TA CMA або CMA для отримання своїх токенів або даних активації токенів.

Для Medium Assurance Hardware або High Assurance рівнів CMA повинен персонально засвідчувати особу заявника до введення в дію сертифіката заявника. Існує два шляхи здійснення цієї вимоги:

1) заявник повинен персонально з'явитися перед CMA або TA, персонально затвердженим CMA або призначеним ім'ям в документі до CMA від Керівника/

Завідувача організації, яку вони представляють, у будь-який час до приєднання підпису CA до сертифіката заявника;

2) коли особисті ключі постачаються абонентам з використанням електронних ключів, абоненти повинні персонально з'являтися перед CMA для отримання своїх токенів або даних активації токенів. Проте, карти передачі ключів, які містять тільки особистий ключ шифрування для використання у FORTEZZA/CAW видаленому перекодуванні, можуть постачатися Абонентові від TA для полегшення випуску робочих сертифікатів Абонента відповідно до вимог цієї політики.

Молодші фахівці та інші, не компетентні для виконання прямої реєстрації поодинці, повинні супроводжуватися персоною, вже засвідченою PKI, яка представлятиме інформацію, достатню для реєстрації на рівні вимог до сертифіката як для самого себе, так і для супровідної персони (табл. 12.10).

Таблиця 12.10. **Вимоги до заявника**

Medium Assurance	Повинен пред'являтися персонально до TA, нотаріуса (або його еквівалента) або CMA і представляє офіційний фото-I
Medium Assurance Hardware або High Assurance	Повинен прибути персонально до CMA або TA і представляє офіційний фото-ID

Medium Assurance, Medium Assurance Hardware або High Assurance сертифікати можуть випускатися на основі електронно засвідчених (з використанням поточного, дійсного DoD PKI сертифіката підпису і зв'язаного особистого ключа) запитів Абонента, що підлягають таким обмеженням:

– гарантійний рівень нового сертифіката має бути таким самим або нижче, ніж гарантійний рівень існуючого сертифіката, що використовується як автентифікований мандат;

– DN нового сертифіката має бути ідентичним DN сертифіката підпису, при цьому інформація в новому сертифікаті, який може бути використаний для санкціонування доступу, має бути ідентичною імені сертифіката підпису;

– термін завершення дії нового сертифіката має бути не пізнішим, ніж дата наступної потрібної персональної автентифікації, зв'язаної із сертифікатом підпису;

– дата персональної автентифікації, що пов'язана з новим сертифікатом, має бути не пізнішою, ніж дата персональної автентифікації, зв'язаної із сертифікатом підпису, що використовується для автентифікації;

– період достовірності нового сертифіката має бути не більшим, ніж максимальний період достовірності, встановлений вимогами цієї CP для цього типу сертифіката.

Такий електронно засвідчений випуск потрібен для засвідчення перекодування, за винятком того, що новий сертифікат є дійсним паралельно з існуючим сертифікатом, але можливо з іншим терміном завершення дії.

Деякі обчислювальні та комунікаційні компоненти (наприклад, маршрутизатори, брандмауери) будемо називати як суб'єкти сертифікації. У таких

випадках компонент повинен мати людський PKI спонсор, причому PKI спонсор є відповідальним за надання CMA, або до CMA, затверджений TA, правильної інформації щодо:

– ідентифікації устаткування;

– відкритих ключів устаткування;

– контактної інформації для забезпечення зв'язку CMA із PKI спонсором, коли потрібно санкціонування;

– верифікацію підписаних у цифровій формі повідомлень, посланих від PKI спонсорів (з використанням сертифікатів еквівалентної або більшої гарантії, ніж запитана)

Поштова адреса абонента, що входить до сертифіката (наприклад, у розширенні підлеглого альтернативного імені), не верифікується.

Сертифікати, які містять явні або неявні філіали організації, повинні випускатися тільки після встановлення, що абонент має санкції для дії від імені організації з відповідно призначеною компетенцією. Прикладами цього можуть бути групові і ролеві сертифікати, і CA і RA сертифікати.

Федеральна інфраструктура відкритого ключа (FPKI) США і CRL профіль, FPKI профіль сумісності каталогів і DoD X.509 CP повинні формувати основу для оцінки сумісності з DoD PKI. Проте рішення з перехресної сертифікації із зовнішнім PKI повинно прийматися PMA.

12.2.3. Ідентифікація й автентифікація для перекодування запитів

Що довше й частіше ключ використовується, то більш вразливим він стає до втрати або розкриття. Це послаблює надану абонентові гарантію щодо дійсності унікальної прив'язки між ключем і його власником. Тому важливо, щоб абонент періодично отримував нові ключі і перевстановлював їх. Перекодування сертифіката означає створення нового сертифіката, ідентичного старому сертифікату, за виключенням того, що:

– новий сертифікат має новий, інший відкритий ключ (що відповідає новому, іншому особистому ключу);

– інший серійний порядковий номер;

– може мати інший призначений період дійсності.

Сертифікати абонента можуть перекодуватися на підставі існуючих сертифікатів абонента, за таких умов:

– період чинності нового сертифіката не перевищить максимальний період часу між безпосередніми сертифікаціями;

– максимальний термін дії нового сертифіката не перевищить 3 роки;

– гарантійний рівень нового сертифіката такий самий або менше, ніж гарантійний рівень сертифіката, що використаний для автентифікації запиту;

– вся інша інформація Абонента залишається дійсною.

Якщо вищесказане не виконується, то абонент повинен виконати вимоги початкового посвідчення особи. Будь-який CA, який включає санкціонування в сертифікаті, включаючи все, що супроводжує або мається на увазі відмітним DN, повинен задокументувати у своєму CPS механізмі повідомлення CA про відміну санкцій. Відміна санкцій повинна призводити до скасування старого сертифіката

і, якщо необхідно, випуск нового сертифіката з іншим відкритим ключем і відповідними санкціями.

Особисті ключі підпису та сертифікати абонентів мають максимальний термін дії три роки. Сертифікати управління ключами абонента мають максимальний термін дії три роки, але використання особистих ключів управління ключами абонента для розшифрування є необмеженим.

Запити перекодування для сертифікатів можуть бути автентифіковані на підставі поточних дійсних сертифікатів абонента, поки період дійсності нового сертифіката не перевищить значень, наведених у таблиці 12.11.

Таблиця 12.11. **Періоди дійсності сертифікатів**

Гарантійний рівень	Вимога до періоду персональної автентифікації
Medium Assurance Software	Кожні 9 років
Medium Assurance Hardware	Кожні 4 роки
High Assurance	Кожні 3 роки

Працездатність СА повинна перевірятися через використання ключа підпису або процесу початкової реєстрації. Вона повинна проводитись через процес початкової реєстрації щонайменше один раз на три роки. Перекодування, після скасування для всіх гарантійних рівнів, має бути здійснено шляхом використання персональної автентифікації.

Запити скасування повинні бути автентифіковані. Запити відміни сертифіката можуть бути автентифіковані за допомогою зв'язаного особистого ключа сертифіката, незалежно від компрометації особистого ключа.

12.3. ВИМОГИ ДО ПЕРІОДУ ДІЇ СЕРТИФІКАТА

12.3.1. Порядок подання заяви на сертифікат

Основним наміром цієї Політики є визначення мінімальних вимог і процедур, необхідних для підтримки довіри до PKI, а також мінімізація вимог на окремі реалізації центра управління сертифікатами (CMA), абонентів і залежних сторін.

Заявник і CMA повинні під час подачі заяви на сертифікат виконати такі дії:

1) встановити і зареєструвати особу абонента;

2) отримати асиметричну пару відкритого/ особистого ключів, що потрібні для виготовлення кожного сертифіката;

3) встановити, що з відкритого ключа формується сертифікат відкритого ключа, а особистий ключ є конфіденційним і використовується тільки абонентом (власником);

4) визначити спосіб контакту для верифікації ролей або санкцій, що запитуються.

Указані дії можуть виконуватися в будь-якому порядку, що є зручним для CMA і абонентів, але вони не повинні нести в собі будь-які загрози. Крім того, дії

повинні бути здійснені до видачі сертифіката. Також усі взаємодії всередині CMA, що підтримують подачу заяви на сертифікат і процес його видачі, повинні бути автентифіковані й захищені від модифікації за допомогою механізмів, сумірних з вимогами до даних, які захищаються виготовленими сертифікатами. Наприклад, комунікації, що підтримують випуск Medium Assurance сертифікатів, повинні бути захищені за допомогою Medium Assurance сертифікатів або деяких інших еквівалентних механізмів. Окрім того, будь-яка передача загальних секретів за допомогою електронних засобів має бути захищеною (наприклад, зашифрованою) за допомогою засобів, які сумірні або не гірше з вимогами до даних, що захищаються сертифікатами, які випускаються.

Центр CA, що здійснює цю CP, повинен засвідчити інші CA (для включення перехресної сертифікації) тільки як санкціоновані DoD PMA.

Запити CA на CA сертифікати мають подаватися до DoD PMA на відповідну контактну адресу, а також повинні супроводжуватися CPS згідно з форматом структури політики сертифікації й технології сертифікації Інтернет X.509 Інфраструктури Відкритого Ключа (RFC 3647).

DoD PMA повинен оцінювати подані CPS на допустимість для застосування. PMA також може вимагати проведення початкового аудиту відповідності обох сторін вимогам. Це потрібно для гарантії того, що CMA готовий реалізувати всі аспекти поданих CPS, перш ніж DoD PMA санкціонує CMA для випуску й управління сертифікатами. CA повинен випускати тільки такі сертифікати, що відповідають DoD CPS. Для цього необхідно отримати письмове санкціонування від DoD PMA, і тільки потім сертифікати можуть бути виготовлені з урахуванням обмежень, що накладені PMA або його представниками.

Заява на сертифікат може подаватися до CA абонентом або центром реєстрації RA/ LRA від імені абонента.

Отримавши запит, CMA або TA повинні:

1) перевірити ідентичність запитувача;

2) перевірити повноваження запитувача й цілісність інформації в запиті сертифіката.

Хоча абонент в запиті може вказувати все правильно, однак відповідальність за верифікацію правильності й точності інформації покладається на CMA. Це може здійснюватися засобом реалізації системного підходу до компонування баз даних, які містять персональну інформацію, або через персональний контакт з центром атрибутів (як це встановлено в CPS положеннях CMA). Якщо бази даних або інші джерела використовуються для підтвердження атрибутів абонента, то ці джерела і зв'язана інформація, що посилається до CMA, повинні бути захищені від несанкціонованого модифікування з рівнем, який повинен бути сумірний з рівнем, встановленим для сертифікатів. Також CMA повинен верифікувати всі санкціонування й іншу інформацію щодо атрибутів, яка отримана від заявника. У більшості випадків RA є відповідальним за верифікацію даних заявника, але якщо CA приймає дані заяви безпосередньо від заявників, то CA є відповідальним за верифікацію даних заяви. Інформація щодо атрибутів має бути верифікуваною через ті відомства або ролі, які мають повноваження призначати інформацію або атрибут. Стосунки з цими відомствами або ролями мають встановлюватися перед початком виконання CA своїх функцій і описуватися в CPS.

12.3.2. Процес подачі заяви на сертифікат

CA і RA безпосередньо несуть відповідальність за те, що інформація в заявах на сертифікат є точною. У їх CPS повинні бути визначеними процедури верифікації інформації в заявах на сертифікат.

Ідентифікація й автентифікація абонента повинні виконуватися CA, RA, LRA або TA від імені цих сторін.

Кожна заява на сертифікат може відхилятися від того, що вимагається, з різних причин. Це неточна інформація або відсутність місії (права), потрібної для виготовлення сертифіката для абонента. Центри CA, RA, LRA або TA можуть відхиляти заяву на сертифікат, але до відхилення вони повинні працювати з відповідними сторонами для вирішення протиріч і неточностей.

Заява на сертифікат вважається прийнятою тільки тоді, коли CA прийняв заяву і вирішив видати сертифікат.

Час для обробки заяв на сертифікат не обумовлюється.

12.3.3. Випуск сертифіката

Дії CA в процесі видачі сертифіката. CA повинен автентифікувати запит на виготовлення сертифіката, забезпечити гарантію, що відкритий ключ зв'язаний з відповідним (правильним) абонентом, отримати від абонента доказ володіння особистим ключем, і тільки після цього виготовити сертифікат і видати його абонентові. CA також повинен подати сертифікат в репозиторій.

Абонент повинен бути також повідомлений про видачу сертифіката.

12.3.4. Прийняття сертифіката

Процедура прийняття сертифіката. Для персональної автентифікації підпис абонента про прийняття сертифіката та визнання форми відповідальності (наприклад, DD Form 2842) повинні містити вимоги до процедури прийняття сертифіката. Підпис абонента щодо сертифіката повинен отримуватися до того, як CA дозволить абонентові реальне використання свого особистого ключа.

Для електронної автентифікації запит абонента для отримання нових сертифікатів і виключення можливості заперечення відносно сертифіката або його змісту повинна виконуватись процедура прийняття абонентом виготовленого сертифіката.

12.3.5. Ключова пара та використання сертифіката

Особистий ключ і використання сертифіката. Щодо особистого ключа має бути унеможливлений несанкціонований доступ до нього інших об'єктів і суб'єктів. Абонент не повинен використовувати особистий ключ підпису після скасування або завершення терміну дії зв'язаного з ним сертифіката. Абонент може продовжувати використовувати свій особистий ключ розшифрування після скасування або завершення терміну дії зв'язаного з ним сертифіката тільки для розшифрування раніше зашифрованої інформації. Також абонент

повинен використовувати свій особистий ключ тільки для DoD діяльності. Використання особистого ключа має бути також обмежене згідно з розширенням використання ключів у сертифікаті. Якщо мається розширення використання ключів і мається на увазі будь-яке обмеження з використання особистого ключа, то ці обмеження також повинні виконуватись. Наприклад, особистий ключ OCSP відповідача повинен використовуватися тільки для підписання OCSP відповідей.

12.3.6. Відкритий ключ і використання сертифіката

Залежні сторони повинні гарантувати, що відкритий ключ у сертифікаті використовується тільки в цілях, указаних в розширеннях використання ключа, якщо таке наявне.

Якщо розширене розширення використання ключа наявне і мається на увазі будь-яке обмеження з використання сертифіката, то ці обмеження також повинні враховуватися.

12.3.7. Відновлення сертифіката

Під відновленням сертифіката розуміють створення нового сертифіката з тим самим ім'ям, ключем і санкціями, як у попереднього (старого) сертифіката, але з розширеним періодом чинності та новим серійним номером. Сертифікат може бути відновлений для управління CRL розміром. Сертифікат також може бути відновлений, якщо відкритий ключ не досяг терміну завершення своєї дії, зв'язаний особистий ключ не був скомпрометований, а ім'я й атрибути абонента правильні. Тому CMA може дозволяти перекодування з початковим випуском і двома відновленнями на рік. Але попередній сертифікат не повинен скасовуватися, не повинен надалі перекодовуватися, відновлюватися або модифікуватися.

Сертифікат може відновлюватися, якщо він не досяг терміну завершення дії, не був скасований, повний життєвий час сертифікатів, випущених (включаючи новий сертифікат) для цього відкритого ключа, не перевищує допустимого строку, а ім'я й атрибути абонента все ще правильні.

Абонент, RA або LRA можуть робити запит на відновлення сертифіката абонента.

Процес відновлення може бути споріднений процесу початкового випуску сертифіката.

Також, альтернативно, сертифікат може автоматично відновлюватися CA на підставі електронного запиту, автентифікованого відповідним чином.

12.3.8. Перекодування сертифіката

Перекодування засобів сертифікації, що створюють новий сертифікат з тим самим ім'ям і санкціями, як і попередній, але з новим ключем, розширює період дії та вводить новий серійний номер. Після перекодування сертифіката, попередній сертифікат може або не може скасовуватися, але не повинен надалі перекодовуватися, відновлюватися або модифікуватися.

Сертифікат повинен перекодовуватися, коли він більше не може відновлюватися. Скасований сертифікат не повинен перекодовуватися.

Абонент, RA або LRA можуть запитувати дозвіл на перекодування сертифіката абонента.

Процес перекодування може бути споріднений процесу початкової видачі сертифіката. Альтернативно, сертифікат може автоматично перекодуватися центром CA на підставі електронного автентифікованого запиту від абонента.

12.3.9. Модифікування сертифіката

При модифікації (відновленні) засобів сертифікації створюється новий сертифікат, який має той самий або інший ключ, інший серійний номер і відрізняється від попереднього сертифіката одним або більше іншими полями. Наприклад, CA може вирішити модифікувати сертифікат абонента, який набуває санкціонування. Попередній сертифікат може скасовуватися або не скасовуватися, але він не повинен надалі перекодовуватися, відновлюватися або модифікуватися.

CA повинен автентифікувати достовірність будь-яких санкціонувань за допомогою тих самих засобів, як і для початкового санкціонування або засобів такого самого або вищого рівня захисту й гарантії.

Сертифікат може модифікуватися, якщо частина інформації, окрім відмітного DN, наприклад, поштова адреса або санкціонування, повинні бути перевірені CA, RA або LRA.

Процес модифікації сертифіката може бути споріднений процесу початкової сертифікації. Альтернативно, сертифікат може автоматично модифікуватися CA на підставі електронного автентифікованого запиту від Абонента. Проте, достовірність будь-яких змін у процесі санкціонування повинна бути перевірена CA, RA або LRA.

12.3.10. Скасування та припинення дії сертифіката

Сертифікат повинен бути скасований, коли прив'язка між суб'єктом і відкритим ключем суб'єкта, що визначена в сертифікаті, більше не вважається дійсною. Прив'язка визнається недійсною, наприклад, за таких обставин:

– коли ідентифікація інформаційних компонентів або компонентів належності будь-яких імен у сертифікаті стає недійсною;

– при зменшені атрибутів привілей, що затверджені в сертифікаті абонента;

– при виявленні порушення абонентом умов своєї абонентської угоди;

– при виникненні підозри компрометації особистого ключа;

– коли абонент або інша санкціонована сторона (як визначено в CPS положеннях CMA) просить скасувати його сертифікат.

У межах ІВК, CMA може негайно скасувати сертифікати в межах свого домену. Письмова заява та стисле пояснення про скасування мають згодом надаватися абоненту. RA може запитувати скасування сертифіката абонента від імені будь-якої санкціонованої сторони, як визначено в його CPS.

Будь-який формат, що використовується для запиту скасування, повинен ідентифікувати скасований сертифікат, пояснювати причину скасування і дозволяти автентифікацію запиту (наприклад, підписаного в цифровій формі або власноруч). Для скасування потрібна необхідна дія CMA, тобто абонент не може через автоматизований процес скасувати свій власний сертифікат або змінювати попередню причину скасування без втручання CMA. Автентифікація запитів скасування сертифіката важлива для запобігання зловмисного скасування сертифікатів несанкціонованими сторонами.

Зокрема, якщо скасування запитується внаслідок компрометації ключа або підозрюваного шахрайського використання, то запит скасування абонента і RA повинен бути вказаний. Якщо RA виконує це від імені абонента, то повинен застосовуватися формат формального підписаного повідомлення, відомий CA. Усі запити повинні бути автентифіковані, причому для підписаних запитів від суб'єкта сертифікації або від RA достатньо верифікації підпису.

При отриманні запиту скасування від Абонента або іншої санкціонованої сторони, CMA повинен автентифікувати запит скасування. CMA може, на свій розсуд, приймати розумні заходи для верифікації потрібності скасування. Якщо запит скасування виявляється дійсним, CMA повинен скасувати сертифікат шляхом розміщення свого серійного номера й іншої ідентифікаційної інформації на CRL.

Під час реалізації ІВК за допомогою апаратних ключів абоненти, що залишають організації, які спонсують їх участь в ІВК, повинні передавати своєму CMA (через будь-який зрозумілий механізм) усі криптографічні апаратні ключі, випущені під керівництвом спонсорської організації, до залишення організації. Електронний ключ повинен бути обнулений або знищений негайно після передачі та захищений від зловмисного використання між передачею та обнуленням або знищенням.

Згідно з цією політикою не повинно бути ніякого пільгового періоду для скасування сертифіката. Абоненти й санкціоновані об'єкти ІВК повинні запитувати скасування сертифікатів як тільки перед ними виникає потреба в скасуванні. CA повинен обробляти всі запити скасування в межах однієї години після отримання запиту.

Використання скасованих сертифікатів може призвести до руйнуючих або катастрофічних наслідків. Визначення частоти отримання нових даних скасування покладається на залежну сторону і системний орган акредитації. Якщо це тимчасово нездійсненно, то залежна сторона повинна або відмовитися від використання сертифіката, або прийняти інформоване рішення прийняття ризику. Таке використання може бути іноді необхідне для виконання надзвичайних експлуатаційних вимог.

CRL списки періодично випускаються і доводяться у репозиторій, навіть якщо не потрібно робити ніяких змін або відновлень. CRL можуть випускатися частіше, якщо це потрібно.

CA повинен гарантувати, що замінені CRL видалені з репозиторію при реєстрації найостаннішого списку CRL.

DoD CA повинні узгоджувати списки CRL з частотою їх випуску CRL згідно з наведеним у таблиці 12.12.

Таблиця 12.12. **Періодичність випуску CRL**

CA	Нормальна періодичність випуску CRL	Максимальний час очікування випуску CRL з причини компрометації ключа або CA
Кореневий CA – середньої гарантії – середньої апаратної гарантії	Щонайменше один раз на кожні 28 днів	У межах 18 годин повідомлення
CA підпису – середньої гарантії – середньої апаратної гарантії	Щонайменше один раз на день	У межах 18 годин повідомлення
Кореневий CA високої гарантії	Щонайменше один раз на кожні 28 днів	У межах 6 годин повідомлення
CA підпису високої гарантії	Щонайменше один раз на день	У межах 6 годин повідомлення
Апаратні засоби, наприклад, FORTEZZA PAA, PCA, CAW	Щонайменше один раз на кожні 28 днів	У межах 6 годин повідомлення

Сертифікати абонента високої гарантії, якщо вони скасовуються внаслідок компрометації ключа, повинні бути перелічені в списку непрямого скасування сертифікатів (ICRL) згідно з деяким механізмом еквівалентної функціональності та своєчасності у межах шести годин після отримання запиту скасування компонентом інфраструктури (RA або CA). CA сертифікат високого рівня гарантії, що скасований з будь-якої причини, також повинен бути розміщений у ICRL списку високої гарантії або деякого механізму еквівалентної функціональності та своєчасності у межах шести годин після отримання запиту скасування.

CA повинен видати опис того, як отримати інформацію скасування для виданих ними сертифікатів, і пояснення наслідків використання інформації скасування, строк якої минув. Ця інформація повинна надаватися абонентам протягом запиту або видачі сертифіката і бути легко доступною для будь-якої потенційної залежної сторони.

У разі скасування будь-якого DoD PKI CA, DoD кореневий CA повинен повідомляти всі перехресно-сертифіковані або DoD затверджені зовнішні PKI з урахуванням обмежень вищевказаної таблиці.

CRL повинен відстрочуватися під час генерації, але не пізніше чотирьох годин після генерації. Окрім того, новий CRL повинен видаватися не пізніше часу, вказаного в nextUpdate полі найостаннішого виданого CRL для тієї ж CRL області застосування.

СА та клієнтське програмне забезпечення залежної сторони опціонально можуть підтримувати on-line перевірку стану. Оскільки DoD діє в деяких середовищах, які не можуть забезпечувати on-line зв'язки, всім СА потрібно підтримувати CRL. Клієнтському програмному забезпеченню з використанням on-line перевірки скасування не потрібно отримувати або обробляти CR. OCSP відповідачі повинні функціонувати в такий спосіб, який гарантує, що використовується точна й сучасна інформація від санкціонованих центрів СА для забезпечення стану скасування.

Характеристики стану скасування забезпечують послуги автентифікації й цілісності, сумірні з гарантійним рівнем сертифіката, що перевіряється.

Залежні сторони опціонально можуть використовувати on-line перевірку стану. Оскільки DoD може діяти в деяких середовищах, які не можуть застосувати on-line комунікації, усім центрам СА потрібно підтримувати CRL. Якщо клієнти функціонують у режимі on-line перевірки, то обробляти CRL не потрібно. DoD залежні сторони (включаючи CMA) повинні залежати тільки від OCSP відповідачів, затверджених згідно з вимогами. Центри СА можуть також використовувати інші методи для оголошування про скасування сертифікатів. Але будь-який альтернативний метод повинен відповідати таким вимогам:

1) альтернативний метод повинен бути описаний у СА, затверджених CPS;

2) альтернативний метод має забезпечити послуги автентифікації й цілісності та сумірні з гарантійним рівнем сертифіката, що верифікується;

3) альтернативний метод повинен відповідати вимогам видачі й часу очікування для CRL.

CMA, що використовує спеціальні коди, повинен мати здатність переходу будь-якого спеціального коду до компрометації.

DoD PKI не повинен підтримувати припинення скасування сертифікатів. Сертифікати, які випускаються згідно з цією політикою, і ті, що розміщено в CRL, не повинні згодом вважатися дійсними (наприклад, через їх видалення з подальшого CRL).

DoD PKI не підтримує повноваження стану сертифікації, наприклад, простий протокол перевірки достовірності сертифіката (SCVP).

Абонування є синонімом періоду чинності сертифіката. Абонування завершується при скасуванні або завершенні терміну дії сертифіката.

12.3.11. Депонування та відновлення ключів

DoD політика відновлення й депонування ключів повинна описуватись у політиці відновлення ключів (KRP) для відомства. Згідно [KRP] операції депонування й відновлення ключів повинні відповідати затвердженій технології відновлення ключів.

DoD PKI зараз підтримує депонування й відновлення особистих ключів шифрування. DoD PKI не підтримує відновлення ключів за допомогою методів інкапсуляції ключів.

12.4. ГЕНЕРАЦІЯ ТА ІНСТАЛЯЦІЯ КЛЮЧОВИХ ПАР

12.4.1. Генерація ключових пар

Усі ключі та проміжні ключі й псевдовипадкові числа, що використовуються для генерації всіх ключів, повинні генеруватися за допомогою FIPS затвердженого методу. Наприклад, просте число для використання за допомогою RSA алгоритму, визначеного в RSA Криптографічному Стандарті [PKCS 1], повинне генеруватися та перевірятися згідно з [PKCS 1]. Особистий ключ вважається генерованим PKI об'єктом, який першим вступає у володіння ним: Абонентом, RA або CA.

Випадкові числа для ключового матеріалу Високої Гарантії повинні генеруватися в апаратному криптографічному модулі, атестованому згідно FIPS 140 Рівня 2.

Особистий ключ не повинен з'являтися за межами модуля, у якому він генерувався, якщо тільки він не зашифрований для транспортування (Див. Розділ 6.2.6), або для обробки чи зберігання за допомогою механізму відновлення ключів.

CA криптографічний ключовий матеріал повинен генеруватися в апаратному криптографічному устаткуванні, атестованому згідно з FIPS 140 Рівня 2.

Генерація CA ключів повинна здійснюватися під управлінням двох персон. Процедури, що використовувалися для генерації CA ключів, повинні бути задокументовані й підписані двома або більше особами для забезпечення контрольованого доказу дотримання задокументованих процедур. Документація процедури має бути деталізована, достатньо для демонстрації використання відповідного розділення ролей. Незалежна третя сторона (наприклад, аудитор відповідності) повинна перевіряти достовірність процедур генерації ключів або через свідчення або через дослідження підписаних і задокументованих процедур.

Криптографічний ключовий матеріал OCSP відповідача повинен генеруватися в криптографічних модулях, атестованих згідно з FIPS 140 Рівня 2. Апаратний криптографічний модуль, атестований згідно з FIPS 140 Рівня 2, повинен використовуватися для OCSP високоємких відповідачів.

Ключові пари Середньої Гарантії повинні генеруватися в криптографічних модулях, атестованих згідно з FIPS 140 Рівня 1.

Medium Assurance Hardware і High Assurance ключові пари підпису повинні генеруватися на Абонентському токені, який має бути апаратним криптографічним модулем, атестованим згідно з FIPS 140 Рівня 2. Високогарантійні FORTEZZA CAW центри можуть генерувати пари відкритих/ особистих ключів підпису від імені Видаленого Користувача/ Абонента. Такі ключові пари генеруватимуться тільки на FORTEZZA PCMCIA карті або T2CSS платі FIPS 140 Рівня 2 або вищого рівня. Якщо ключова пара повинна витягуватися з токену, на якому він був генерований (інших, ніж визначено в Розділі 6.2.2), для передачі до Видаленого Користувача/ Абонента або для вставки в Сервер криптографічної підтримки типу 2 (T2CSS), ключі повинні безпечно витягуватися способом, який гарантує, що тільки належний токен Видаленого Користувача/ Абонента може розшифровувати та здійснювати доступ до нового ключа підпису. Модуль, на якому була генерована ключова пара, повинен негайно обнулятися після витягування, і затверджений процес повинен мати місце для гарантії неможливості створення ніяких додаткових копій ключа.

Medium Assurance Hardware ключові пари шифрування повинні генеруватися в апаратних криптографічних модулях, атестованих згідно з FIPS 140 Рівня 2. Ключові пари можуть генеруватися з токенів, поки існує гарантія, що ніякі копії, окрім санкціонованих копій ключового депонування ключів, не продовжують існування після завершення процесів генерації та вставки.

Пара ключів шифрування Високої Гарантії повинна генеруватися на апаратному криптографічному модулі, атестованому згідно з FIPS 140 Рівня 2. Апаратному модулю не потрібно бути токеном Абонента, поки існує гарантія, що ніякі копії, окрім санкціонованих копій ключового депонування особистого ключа шифрування, не продовжують існування після завершення процесів генерації та передачі.

12.4.2. Постачання особистих ключів абонентам

У більшості випадків особистий ключ генеруватиметься й залишатиметься в межах криптографічної межі криптографічного модуля. Якщо власник модуля генерує ключове у визначеному місці, то немає ніякої необхідності постачати особистий ключ Абонента. Якщо ключ генерується на апаратному криптографічному модулі де-небудь в іншому місці, то апаратний криптографічний модуль треба постачати Абонентові. Відповідальність за розташування й стан апаратного криптографічного модуля має підтримуватися, поки модуль не буде у володінні абонента. Абонент повинен визнати паспорт апаратного криптографічного модуля.

Особисті ключі, зв'язані з Medium Assurance (за виключенням Medium Hardware) сертифікатами, можуть генеруватися й зберігатися в програмних криптографічних модулях. Коли Абонент генерує ці ключі у визначеному місці, то немає необхідності їх постачання. Якщо особисті ключі генеруються де-небудь в іншому місці, вони повинні передаватися або постачатися до Абонента в зашифрованій формі, і метод шифрування повинен гарантувати, що тільки Абонент може володіти особистими ключами підпису відкритого тексту. Шифрування повинне мати стійкість, сумірну зі стійкістю захисту ключа. Абонент повинен підтвердити прийняття особистого ключа підпису. Початково генерований особистий ключ підпису потрібно знищити. Механізми повинні гарантувати, що додаткові копії програмних ключів не підтримуються, якщо тільки це не дозволено цією Політикою Сертифікації

Тільки ті, що санкціоновані DoD політикою відновлення ключів, можуть мати доступ до особистих ключів, зв'язаних із сертифікатами шифруванням

Для всіх гарантійних рівнів, коли кодовані апаратні токени постачаються Абонентам, постачання повинно здійснюватися способом, який гарантує, що правильні токени й дані активації надаються саме тому Абонентові. CMA повинен підтримувати запис отримання токену Абонентом. Коли використовується будь-який механізм, який включає загальний секрет (наприклад, пароль або Персональний Ідентифікаційний Номер (PIN)), цей механізм повинен гарантувати, що тільки заявник і CMA є користувачами цього загального секрету.

12.4.3. Постачання відкритих ключів до емітента сертифікатів

Загальні ключі повинні постачатися до емітента сертифіката способом, який зв'язує верифіковану ідентифікацію заявника з відкритим ключем, що засвідчується. Ця прив'язка повинна здійснюватися за допомогою засобів, які захищені

до того ж рівня захисту, забезпеченого ключами, що засвідчуються. Прив'язка повинна здійснюватися за допомогою криптографічних, фізичних, процедурних і інших відповідних методів. Методи, використовувані для постачання відкритих ключів, повинні бути обумовлені в CPS.

У тих випадках, де пари відкритих/ особистих ключів генеруються CMA від імені Абонента, CMA повинен здійснювати механізми захисту для гарантії, що токен, на якому тримається пара відкритих/ особистих ключів, безпечно відправлений належному Абонентові і що токен не активізується до отримання належним Абонентом.

Як указано в пункті 6.1.1 розділу 6, FORTEZZA CAW може безпечно витягувати пари відкритих/ особистих ключів з токену, на якому вони були генеровані, для передачі до видаленого Користувача/ Абонента. У таких випадках механізми захисту, застосовані до витягнутих ключів, також мають відповідати п. 6.2.6 розділу 6, і сертифікат неможна активувати до отримання належним Видаленим Користувачем/ Абонентом

12.4.4. Постачання відкритих ключів залежним сторонам

PKI і залежні сторони повинні працювати разом для гарантії автентифікованого й цілісного постачання Довірчих Сертифікатів. Придатні методи для постачання Довірчих Сертифікатів включають, але не обмежені:

– CA або RA, що завантажують Довірчі Сертифікати в токені, що постачаються залежним сторонам через захищені механізми;

– захищене розповсюдження Довірчих Сертифікатів через захищені зовнішні механізми;

– порівняння геш-значень сертифікатів або відбитків з геш-значень або відбитками Довірчого Сертифіката, доступними через автентифіковані зовнішні джерела (відзначимо, що відбитки або геш-значень, які внутрішньо зареєстровані разом із сертифікатом, не допустимі як механізми автентифікації);

– завантаження сертифікатів з Web сайтів, захищених за допомогою чинного DoD сертифіката рівного або більшого гарантійного рівня, ніж сертифікат, що завантажується.

Системи, що використовують High Assurance сертифікати, повинні зберігати Довірчі Сертифікати так, щоб легко виявляти несанкціоновану зміну або заміну.

12.4.5. Розміри ключів

Для FORTEZZA Високогарантійного PKI ключі Стандарту Цифрового Підпису (DSS), випущені DoD PKI Сполучених Штатів, повинні використовувати щонайменше 160-бітовий особистий ключ (x) і щонайменше 1024-бітовий простий модуль (p). Мінімальні розміри відкритого ключа Абонента мають становити 1024 бітів для Алгоритму Ключового Обміну (KEA).

Для Середньогарантійних ключів (за винятком Medium-2048, Medium Hardware-2048 і PIV-Auth-2048) RSA (Рівест, Шамір, Адлеман), випущених DoD PKI, мають становити 1024 бітів. Розмір ключа Кореневого CA має становити 2048 бітів. (Для цього не потрібно скасування DoD Root 1 сертифіката, але DoD Root 1

сертифікат повинен використовувати свій ключ підписання тільки для випуску CRL). Мінімальний розмір відкритого ключа для всіх Medium-2048, Medium Hardware-2048 і PIV-Auth-2048 RSA ключів має становити 2048 бітів. Мінімальний розмір відкритого ключа для Високогарантійних RSA ключів має становити 2048 бітів. Усі RSA ключі, випущені після 31 грудня 2010, мають становити 2048 бітів. OCSP відповідачі повинні підписувати відповіді за допомогою алгоритму підпису, розміру ключа й алгоритму гешування рівної або більшої криптографічної стійкості, ніж використовується CA для підписання CRL.

Для Середньої Гарантії ключове просте поле Алгоритму Криптографії Еліптичної Кривої (*//p//*) має бути не менше ніж 224, і Бінарне Поле (*m*) повинне бути не менше ніж 233. Для Високої Гарантії ключове просте поле Алгоритму Криптографії Еліптичної Кривої (*//p//*) повинне бути не менше ніж 384, і Бінарне Поле (*m*) повинне бути не менше ніж 409.

Використання SSL або іншого протоколу для передачі реєстраційної інформації чи постачання особистого ключа повинне вимагати щонайменше використання довжини симетричного ключа й алгоритму показника трудовитрат, який дорівнює або перевищує показник трудовитрат, пов'язаний з ключовими парами Абонента.

12.4.6. Генерація загальних параметрів та перевірка якості ключів

Параметри відкритого ключа завжди повинні генеруватися й перевірятися згідно із стандартом, який визначає криптоалгоритм, у якому мають використовуватися параметри. Наприклад, параметри відкритого ключа для використання з алгоритмами, визначеними в Стандарті Цифрового Підпису FIPS 186-2, повинні генеруватися й тестуватися згідно з FIPS 186-2.

Кожного разу, коли криптоалгоритм описується у FIPS 186-2, вимоги та рекомендації щодо генерації та перевірки параметрів FIPS 186-2 потрібні всім об'єктам, що генерують ключові пари, чиї відкриті компоненти мають бути сертифіковані DoD PKI.

12.4.7. Області використання ключів (цілі використання ключів)

Відкриті ключі, зв'язані із сертифікатами, які встановлюють Середньогарантійні або Високогарантійні політики, повинні бути сертифіковані для використання в підписанні або шифруванні, але не для обох. Використання конкретного ключа позначається розширенням використання ключа в X.509 сертифікаті. Це обмеження не призначено для заборони використання протоколів (подібно Рівню Безпечних Сокетів), що забезпечують автентифіковані з'єднання з використанням сертифікатів шифрування. Формати CA і сертифікатів кінцевих об'єктів, включаючи спосіб заповнення keyUsage розширення в цих сертифікатах, описані в DoD PKI Специфікації та Рекомендаціях Функціонального Інтерфейсу [INT-SPEC].

Відкриті ключі Абонентів, що зв'язані із сертифікатами, які встановлюють PIV-Auth або PIV-auth-2048 гарантію, повинні заявляти розширення ключового використання «digitalSignature» і не повинні заявляти будь-яке інше розширення ключового використання.

12.5. ЗАХИСТ ОСОБИСТИХ КЛЮЧІВ І ОСОБЛИВОСТІ ПРОЕКТУВАННЯ КРИПТОГРАФІЧНИХ МОДУЛІВ

12.5.1. Стандарти й засоби управління криптографічними модулями

Кращим стандартом, що визначає вимоги до захисту криптографічних модулів, на наш погляд, є федеральний стандарт Модулів FIPS 140-3 [123]. Також PMA може визначати, які інші зіставні стандарти атестації, сертифікації або верифікації є достатніми для застосування. Ці стандарти видаватимуться PMA. Криптографічні модулі повинні бути атестовані згідно з FIPS 140 та відповідати рівню, що визначений нижче, або повинні бути атестовані, сертифіковані чи верифіковані з використанням стандарту, що виданий PMA. Абоненти, які мають ключі, сертифіковані згідно з Medium Assurance політикою, повинні використовувати криптографічні модулі, які відповідають щонайменше критеріям, встановленим для Рівня 1. Абоненти, які мають ключі, сертифіковані згідно з Medium Assurance Hardware политикою, повинні використовувати апаратні криптографічні модулі, які відповідають щонайменше критеріям, встановленим для Рівня 2. Сертифікати з високим рівнем гарантій можуть формуватися на основі апаратних криптографічних модулів рівня 2. Високий рівень може використовуватись, якщо він доступний або необхідний згідно з вимогами. У PKI для полегшення управління сертифікатами абонента має бути забезпечене використання будь-якого придатного криптографічного модуля. Сертифікати із середнім і високим рівнем гарантій повинні бути підписані за допомогою апаратного криптографічного модуля, що відповідає 2-му рівню.

Для OCSP користувачі низького рівня можуть використовувати криптографічні модулі й апаратне устаткування або програмне забезпечення. Усі OCSP високоємких користувачів повинні використовувати FIPS 140 з рівнем захисту 2 або апаратні криптографічні модулі з більш високим рівнем.

Центри реєстрації RA із середнім і високим рівнями гарантій повинні використовувати апаратні криптографічні модулі з 2-им рівнем захищеності.

Усі криптографічні модулі повинні функціонувати таким чином, щоб особисті асиметричні ключі ніколи не виводилися зовні у відкритому вигляді. Особистий ключ не повинен ні за яких умов видаватись за межі CA устаткування у незашифрованому вигляді. Також ніхто не повинен мати доступу до особистого ключа підпису, окрім абонента власника. Особисті ключі направленого розшифрування також повинні бути доступними тільки сторонам, що санкціоновані у відповідності з діючою політикою. Ключі направленого розшифрування повинні триматися в найжорсткішій секретності й управлятися згідно з діючою політикою.

Особисті ключі ЕЦП, призначені для виготовлення сертифікатів, повинні бути захищеними на тому ж рівні, як і сертифікат, що виготовляється. У разі коли CA не задає явно рівень захищеності особистих ключів RA, указана вище вимога розповсюджується й на RA особисті ключі.

Як правило, 2-й (апаратний) рівень захищеності повинен застосовуватись і для OCSP високоємких користувачів.

12.5.2. Багатостороннє управління особистим ключем

Для апаратних засобів FORTEZZA CAW центр CA може використовувати одностороннє управління для підпису ключів. Для інших CA процедури генерації, активації та резервування ключів повинні виконуватись у присутності двох суб'єктів з довірчими ролями. Для цих дій одна з довірчих ролей повинна бути адміністратором системи, а інша сторона не повинна мати роль ISSO або аудитора.

Для OCSP високоємких користувачів генерація, активація та резервування ключів повинні вимагати присутності двох довірчих ролей.

Доступ до ключів, що підписані для CA або OCSP і зарезервованих для відновлення після форс-мажорних обставин, повинен бути щонайменше під двостороннім управлінням.

Запит сертифіката CA або OCSP користувача (включаючи генерацію та постачання відкритого ключа) для генерації CA або OCSP сертифіката повинен здійснюватися під двостороннім управлінням. Імена сторін, що задіюються для двостороннього управління, повинні підтримуватися згідно зі списком, який має бути доступним для перевірки протягом терміну контролю відповідності.

12.5.3. Депонування особистих ключів

Особисті ключі CA ніколи не повинні депонуватися. Ні за яких умов ключ, що призначений для підтримки послуги неспростовності, не повинен довірятися нікому, крім абонента-користувача. Для деяких цілей, наприклад таких, як направлене розшифрування даних, необхідно забезпечувати доступ до особистого ключа асиметричної пари шифрування. Для забезпечення цього в ІВК має забезпечуватися можливість депонування ключів. Метод, процедури й засоби управління, що призначені для зберігання, запиту, витягування та/або пошуку, постачання, захисту й знищення запитаної копії депонованого ключа, мають бути описані в політиці відновлення ключів (KRP), яка повинна стати обов'язковою складовою цієї CP політики.

12.5.4. Резервування особистих ключів

Для абонентів середнього рівня гарантій дозволено резервування тільки своїх власних особистих ключів шифрування (але не підпису). Резервування особистих ключів підпису абонента з метою відновлення робити не треба. Абонентам дозволено робити операційні копії особистих ключів, що постійно знаходяться в програмних криптографічних модулях, для кожного із застосувань абонента або у разі коли ключ повинен бути в іншому місці або іншому форматі. Для середнього рівня гарантій, за винятком Medium Assurance Hardware, компонентам ІВК дозволяється створення єдиної резервної копії особистих ключів у випадках, коли неправильне використання компонентів призводить до псування ключів. Усі передачі ключів повинні бути зроблені із затвердженого криптографічного модуля, і ключ повинен передаватись тільки в зашифрованому вигляді. Абонент (ІВК користувач) є відповідальним за гарантування, що всі копії особистих ключів, включаючи ті, що можуть бути вбудовані в засоби з метою резервування, захищені,

включаючи захист від будь-якої робочої станції, на якій розміщуються будь-які з його особистих ключів.

Центр СА може копіювати тільки апаратний криптографічний модуль абонента у відповідь на дійсний початковий запит резервування або в результаті запиту типу адміністративної дії, підписаного Абонентом. Кожне санкціонування доступу потрібно задокументовувати, і кожен результуючий доступ має бути зареєстрований. Тільки СА й абоненти повинні мати можливість резервування особистих ключів (наприклад, RA не повинен резервувати особисті ключі).

Резервні копії особистих ключів підпису центру СА повинні створюватися й оброблятися тільки під тим же багатостороннім управлінням, що й основний ключ підпису. При цьому можуть бути зроблені не більше ніж дві резервні копії особистих ключів підпису центру СА. Одна резервна копія повинна утримуватися в резервному розташуванні, тобто в приміщенні, призначеному для зберігання резервних компонентів.

Особисті ключі підпису OCSP користувача повинні резервуватися як визначено нижче. При цьому може бути зроблено не більше двох резервних копій особистого ключа підпису OCSP користувача. Якщо створені резервні копії, то тільки одна копія будь-якого ключа підпису має бути збережена в розташуванні OCSP користувача. Якщо зроблена друга копія, то вона повинна зберігатися в місці розташування резервних компонентів. Резервний модуль також повинен відповідати вимогам криптографічного модуля для OCSP користувача.

FORTEZZA CAW центри високої гарантії можуть вимагати резервування СА компонентів відповідно до плану відновлення після лиха й інших ситуацій, що вимагають додаткового резервування. DoD Центр підтримки політики (PCA) може бути санкціонований для створення аж до двох копій СА ключа для головного розташування та додаткової копії для кожного з двох затверджених резервних розташувань, але це має бути затверджено його службовим або відомчим CAW центром затвердження. При цьому місце резервного розташування не потрібно розголошувати в запиті. Окрім того, при отриманні дійсного запиту від CAW центру та затвердженні його службовим або відомчим CAW центром затвердження щодо знищення однієї з основних створених резервних копій PCA санкціонується створення додаткової копії для заміни знищеної. Інші запити CAW СА даних понад затверджені повинні додатково вимагати дозволу та затвердження PCA. Як RA, так і абоненти не повинні резервувати особисті ключі високого рівня гарантій.

12.5.5. Запис або зчитування особистих ключів з криптографічного модуля

Особисті ключі мають генеруватися криптографічним модулем і в криптографічному модулі. У випадку необхідності транспортування особистого ключа з одного криптографічного модуля до іншого особистий ключ під час транспортування має бути зашифрованим. Особисті ключі не повинні ніколи існувати у відкритому вигляді за межами криптографічного модуля. Транспортування особистого ключа повинно виконуватися тільки до санкціонованого об'єкта (тільки абонентові у випадку ключа підпису), і стійкість шифрування має бути щонайменше сумірна зі стійкостю ключа, що транспортується. Особисті або симетричні

ключі, призначені для шифрування інших особистих ключів при їх транспортуванні, мають бути захищені від розголошування. Рівень захисту цих ключів повинен бути сумірний з рівнем захисту, що забезпечується відносно даних, які захищаються за допомогою сертифіката, зв'язаного з особистим ключем.

12.5.6. Зберігання особистого ключа в криптографічному модулі

Особистий ключ, що зберігається в криптографічному модулі, має бути захищеним від несанкціонованого доступу до нього та його використання. Рівень захищеності особистого ключа визначається згідно з вимогами FIPS 140 [117, 123].

12.5.7. Метод активації особистого ключа

Для активації особистого ключа в криптографічному модулі можуть застосовуватись паролеві фрази, PIN коди, біометричні дані, ключі автентифікації або інші механізми, що забезпечують еквівалентну автентичність. Дані активації можуть розповсюджуватися персонально або надсилатись абонентам поштою, але окремо від криптографічних модулів, які вони активізують. Уведення даних активації повинно здійснюватись з необхідним рівнем захисту від розголошення, наприклад, дані не можна відображати, поки вони вводяться.

12.5.8. Метод дезактивації особистого ключа

Криптографічні модулі, які були активізовані, не повинні залишатися без нагляду, і, таким чином, відкритими для несанкціонованого доступу. Після використання їх потрібно вимкнути, наприклад, через процедуру logout, або через пасивний тайм-аут. Апаратні криптографічні модулі, що не використовуються, мають бути видалені із засобу та збережені відповідно до прийнятої політики.

12.5.9. Метод знищення особистого ключа

Особистий ключ, який користувачеві більше не потрібен, або коли сертифікат, якому він відповідає, втрачає термін дії або скасований, повинен бути знищений. Для програмних криптографічних модулів знищення можна здійснити перезаписом даних. Для апаратних криптографічних модулів можуть бути виконані певні команди, наприклад, команда «обнуління» особистого ключа. Фізичне знищення апаратних засобів є необов'язковим (не повинне вимагатися).

12.5.10. Інші аспекти управління ключовими парами

Відкритий ключ архівується як частина архівації сертифікатів. Термін чинності особистих ключів підпису не повинен перевищувати 13 місяців. Термін дії зв'язаних сертифікатів відкритого ключа не повинен перевищувати шість років. Термін дії ключів, які використовуються для захисту ключового матеріалу, визначається окремо.

12.6. ДАНІ АКТИВАЦІЇ

12.6.1. Генерування та інсталяція даних активації

Дані активації можуть бути вибрані абонентом. Парольна фраза, PIN код, ключ, біометричні дані або інші механізми, що забезпечують еквівалентний рівень автентичності, повинні використовуватися для захисту від несанкціонованого доступу до особистого ключа. Дані активації повинні відповідати вимогам «стійкості механізму автентифікації» згідно з FIPS 140 [117, 123].

PIN код абонента (для включення CMA) має бути довжиною щонайменше 6–8 цифр. Якщо можливо, то краще генерувати PIN коди з використанням випадкових механізмів. Якщо це неможливо, то абонент, який призначає свої власні PIN коди, повинен бути проінструктований відносно вибору PIN кодів. Так, вони не повинні бути пов'язаними з його персональною особою, історією або середовищем. Також не можна використовувати повторні числа, числа соціального страхування та календарні формати дат або інші дані, які легко вгадуються. Якщо застосовуються буквено-цифрові паролі, то краще використовувати розсіяну суміш із 8 символів, включаючи щонайменше дві розсіяні цифри. Дані активації не повинні містити слова словника. Вони мають відрізнятися від слів або імен щонайменше двома символами, які є не простою заміною чисел на букви і не повинні складатися зі слів або імен, що завершуються 1–4-ма цифрами. Дані активації не повинні містити послідовності повторних символів, календарні формати чи формати номерних знаків. Для верифікації відповідності даних активації всім вимогам повинні використовуватися технічні засоби.

Якщо для генерації PIN кодів або парольних фраз використовуються випадкові числа, то вони повинні відповідати всім вимогам FIPS 140 [117, 123]. Метод, що використовується для вироблення PIN коду або символів парольних фраз, повинен гарантувати, що всі дійсні символи для PIN коду або парольної фрази, вибираються з однаковою ймовірністю.

Якщо дані активації повинні передаватися, то це треба здійснювати з використанням каналу з відповідним захистом, у певний час і зі зв'язаного криптографічного модуля. Якщо це не можна зробити вручну, то абонентові необхідно рекомендувати дату відправлення й очікуваний термін постачання будь-яких даних активації. Для підтвердження постачання абоненти підписують і повертають квитанцію про постачання відповідних даних. Окрім того, абоненти повинні також отримувати (і підтверджувати, що отримали) рекомендаційну інструкцію абоненту щодо розуміння відповідальності за використання й управління криптографічного модуля.

12.6.2. Захист даних активації

Дані активації криптографічних модулів потрібно зберігати, але краще не записувати. Якщо все ж таки їх записують, то вони мають бути захищені на рівні даних, захищуваних відповідним криптографічним модулем, але вони не повинні зберігатися за допомогою криптографічного модуля.

Дані активації особистих ключів, зв'язаних з відповідними сертифікатами, що засвідчують індивідуальну вірогідність, ніколи не повинні розділятися. Дані

активації для особистих ключів, зв'язаних із сертифікатами, що засвідчують організаційну вірогідність, мають бути обмежені до даних в організації, санкціонованої для використання особистих ключів.

12.7. ЗАСОБИ УПРАВЛІННЯ КОМП'ЮТЕРНИМ ЗАХИСТОМ

12.7.1. Устаткування CA і OCSP користувача

Устаткування CA і OCSP користувача, що застовується для інфраструктур із середнім або вищим рівнем гарантій, повинні використовувати діючі системи, які вимагають:

– автентифікації на основі login;
– забезпечують управління з розмежуванням доступу;
– забезпечують можливість контролю рівня захисту;
– забезпечують ізоляцію процесів;
– підтримують відновлення з ключового або системного збою.

Устаткування CA і OCSP користувача, що використовується в інфраструктурах з вищим рівнем гарантій, треба розміщувати в операційних системах, які реалізують вимоги середнього рівня гарантій і довірчий шлях.

CA застосування, яке було розроблено згідно з вимогами методології розробки довірчих систем рівня 2, має бути оцінене на відповідність Профілю Захисту CIMC (Компоненту Видачі й Управління Сертифікатами). Для рівня 3 – на відповідність із зіставленням PMA затвердженого стандарту. OCSP користувача потрібно оцінити на відповідність гарантійному рівню 4 CC (Загальні Критерії) Оцінки (EAL) або зіставному PMA затвердженого стандарту.

Коли устаткування CA або OCSP користувача розміщене на оцінених платформах у підтримці вимог гарантії комп'ютерного захисту, то система (апаратні засоби, програмне забезпечення й операційна система) потрібно, якщо це можливо, оцінити в конфігурації. Щонайменше такі платформи повинні використовувати одну й ту саму версію комп'ютерної операційної системи, що відповідним чином оцінена.

12.7.2. Технічні засоби управління життєвим циклом

Засоби управління системою розробки

Центри CA повинні розроблятися за допомогою методології розробки довірчих систем (TSDM) рівня 2.

Засоби управління адмініструванням захисту

Устаткування CA і OCSP користувача має бути призначене для адміністрування інфраструктури управління ключами. Конфігурація систем CA і OCSP користувача, а також будь-які модифікації та відновлення треба задокументовувати. Системи CA і OCSP користувача не повинні мати встановлені застосування або компонентне програмне забезпечення, які не є частиною конфігурації CA і OCSP користувача. Формальна методологія управління конфігурацією повинна використовуватися для інсталяції та експлуатації систем CA і OCSP користувача.

Також повинен застосовуватись механізм виявлення несанкціонованих модифікацій щодо системного програмного забезпечення або конфігурації CA і OCSP користувача.

Розумну обережність потрібно проявляти для запобігання завантаженню зловмисного програмного забезпечення на RA устаткування. На RA комп'ютер мають бути завантажені тільки ті застосування, що потрібні для виконання організаційного завдання. Таке програмне забезпечення треба отримувати з джерел, санкціонованих локальною політикою. Дані на RA устаткуванні потрібно сканувати на зловмисний код при першому використанні й періодично пізніше.

Засоби управління захистом життєвого циклу

Устаткування (апаратне й програмне), забезпечення, що застосовуються в ІВ, для зменшення ймовірності підробки будь-якого конкретного компонента можуть купуватися випадково. Устаткування для ІВК повинне розроблятися в керованому середовищі. Для високого рівня гарантії процес розробки має бути визначений і задокументований.

Усі апаратні засоби та програмне забезпечення, які були ідентифіковані як підтримуючі OCSP критичного користувача або CA, повинні транспортуватися або постачатися через керовані середовища, що забезпечують безперервний ланцюжок відповідальності з місця, де вони були ідентифіковані. Програмне забезпечення CA і OCSP користувачів при первинному завантаженні повинне верифікуватися на предмет поставки санкціонованим джерелом, а також що воно є версією, призначеною для цього використання.

Відновлення устаткування повинне здійснюватись або розроблятися тим самим способом, що й основне устаткування, і встановлюватися визначеним способом навченим персоналом, що заслуговує довіру.

Для секретних застосувань CA устаткування і плати повинні постачатися спеціальним чином. Устаткування є секретним, якщо будь-яке секретне прикладне програмне забезпечення або будь-яка секретна інформація коли-небудь були завантажені на устаткуванні або платах.

Засоби управління мережевого захисту

CMA устаткування має бути розміщене на внутрішніх локальних мережах, позаду граничних мережевих засобів захисту й допустимих засобів захисту та узгоджене з політикою для мережевого захисту на рівні цільової гарантійної категорії I (MAC I). Послуги, що дозволені для устаткування CA і OCSP користувачів середнього й вищого рівнів гарантій, повинні бути обмежені до послуг, потрібних для виконання CMA функцій. Тобто CMA устаткування може допускати додаткові послуги, узгоджені з локальною політикою.

12.8. ПРОФІЛЬ ЗАХИСТУ

12.8.1. Номер версії

Політика, що розглядається в цьому розділі, призначена для управління тільки DoD X.509 сертифікатами Версії 3.

12.8.2. Розширення сертифіката

Правила включення, значення й обробка розширень визначені у профілях. Ці профілі призначені для управління інфраструктурою і є достатньо гнучкими для задоволення потреб різноманітних CA і суспільств. Інфраструктура з високим рівнем гарантій повинна обробляти розширення та шляхи, визначені у профілях X.509 сертифіката й списку скасування сертифікатів і правилах обробки шляхів сертифікації для MISSI [SDN 706]. Інфраструктури з середнім рівнем гарантій повинні використовувати технічні специфікації Федеральної ІВК Версії 1: Частина E – Профіль Розширень X.509 Сертифіката і CRL [FPKI-prof]. Будь-які зміни для цих профілів повинні бути затверджені DoD PKI технічною робочою групою та задокументовані в CPS. Кожного разу, коли використовуються особисті розширення, вони мають бути визначені в CPS. Критичні особисті розширення повинні бути сумісними з іншими.

Інформація управління доступом може бути внесена subjectDirectoryAttributes розширення. Синтаксис детально визначається в [SDN 702].

12.8.3. Алгоритмічні об'єктні ідентифікатори

У сертифікатах згідно з Політикою, що розглядається, для ЕЦП повинні використовуватись OID ідентифікатори з таблиці 12.13.

Таблиця 12.13. **OID ідентифікатори для сертифікатів**

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha1WithRSAEncryption	iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
ID-RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-SHA1	iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1}
ecdsa-with-SHA256	iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4}

Там, де сертифікати підписані за допомогою RSA з PSS доповненням, OID є незалежним від алгоритму гешування, причому алгоритм гешування визначається як параметр. RSA підписи з PSS доповненням можуть використовуватися з алгоритмами гешування й OID, що вказані в табл. 12.14.

Таблиця 12.14. **OID RSA з PSS доповненням**

id-sha256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}
id-sha512	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3}

Сертифікати згідно з цією Політикою повинні використовувати OID для визначення алгоритму, для якого був генерований підлеглий ключ, згідно з табл. 12.15.

Таблиця 12.15. **OID для визначення алгоритму**

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public key-type (2) 1}
id-ecDH	iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12)}
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

Там, де сертифікати містять відкритий ключ еліптичної кривої, параметри повинні бути вказані як одна з еліптичних кривих, наведених у табл. 12.16.

Таблиця 12.16. **Параметри еліптичних кривих**

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34}
ansip521r1	iso(1) identified-organization(3) certicom(132) curve(0) 35}

З метою забезпечення криптографічної ізоляції для закритих застосувань, коли відкритий ключ є виду id-ecDH, особистий OID ідентифікатор може бути використаний для вказівки іншої базової точки на одній з вищевказаних еліптичних кривих.

Згідно з DoD політикою ІВК може виготовляти сертифікати тільки з відкритих ключів, які зв'язані безпосередньо з криптографічними алгоритмами, визначеними вище. Також для виготовлення сертифікатів, списків скасування сертифікатів і будь-якого іншого ІВК об'єкта дозволені тільки описані вище алгоритми ЕЦП.

12.8.4. Форми імен

Усі ІВК повинні мати здатність генерувати й обробляти DN імена. При відповідному обґрунтуванні можуть використовуватися й інші імена. Наприклад для сертифікатів, що використовуються для реалізації апаратного протоколу, найбільш корисними є адреси пристроїв. У такому разі альтернативна форма імені може бути включена в subjectAltName розширення. Якщо немає ніякого DN імені (але всі сертифікати високого рівня гарантії повинні мати DN імена), то підлегле поле базового сертифіката повинне бути порожньою послідовністю, і таке розширення має бути відмічене як критичне. Будь-яка форма імені, що визначає GeneralName у [13], може використовуватися згідно з відповідним профілем. Використання альтернативних форм імені має бути визначено в CPS, включаючи критичність, типи й обмеження імен.

12.8.5. Обмеження імен

CA сертифікати, випущені в ІВК високого рівня гарантії, повинні накладати обмеження імен і обмеження довжини шляху, як необхідно згідно з SDN 706.

12.8.6. Об'єктний ідентифікатор політики сертифікації

Сертифікати, випущені згідно з цією політикою, повинні затверджувати OID ідентифікатор у відповідності з рівнем гарантії, з яким він був випущений. Сертифікати, випущені згідно з цією політикою, не повинні містити специфікатори політики. Політика, що розглядається, не вимагає, щоб certificatePolicies розширення було критичним. Користувачі, чиє клієнтське програмне забезпечення не обробляє це розширення, піддаються ризику використання сертифікатів з порушенням встановленої політики.

12.8.7. CRL профіль

Номер версії

CRL списки, випущені згідно з цією політикою, повинні затверджувати номер версії, як описано в [113]. Списки CRL з високим рівнем гарантії повинні використовувати версію 2. Списки CRL із середнім рівнем гарантії можуть використовувати версію 1 або версію 2.

Розширення CRL елементів

Деталізовані CRL профілі, що охоплюють використання кожного розширення, доступні в [SDN 706]. Сертифікати, випущені ІВК з середнім рівнем гарантії, можуть альтернативно узгоджуватися з профільними рекомендаціями в [FPKI-prof] або можуть випускати CRL, що не використовують ніяких розширень. Будь-які зміни для цих профілів повинні бути затверджені DoD ІВК технічною робочою групою й задокументовані в CPS.

12.8.8. OCSP профіль

Номер версії

DoD PKI повинна використовувати OCSP версії 1.

OCSP-розширення

В OCSP запитах і відповідях можуть використовуватись розширення, визначені в RFC 2560. Якщо запит містить nonce, а відповідь не містить nonce, залежна сторона може обробляти відповідь, якщо інформація вважається обґрунтованою.

12.9. УСТАТКУВАННЯ ТА ЗАСОБИ УПРАВЛІННЯ ЕКСПЛУАТАЦІЄЮ

12.9.1. Фізичні засоби управління

CA і OCSP високої ємкості повинні використовувати устаткування, призначене цим CMA функціям. Не повинні виконуватися функції, не зв'язані з CMA. Несанкціоноване використання CMA устаткування має бути заборонено. Повинні бути також реалізовані фізичні засоби управління, які захищають CMA апаратні засоби і програмне забезпечення від несанкціонованого використання. CMA криптографічні модулі повинні бути захищені від крадіжки, втрати й несанкціонованого використання.

Розташування та конструкція

Розташування та конструкція устаткування, в якому розміщуватимуться CMA устаткування, та операції мають відповідати DoD і локальній політиці захисту інформації з тим самим рівнем, як і інформація, що захищатиметься з використанням сертифікатів відкритого ключа.

Фізичний доступ

За винятком FORTEZZA CAW, устаткування й криптографічні модулі CA і OCSP користувача завжди:

1) мають бути захищені від несанкціонованого доступу;

2) вимагати присутності щонайменше двох довірчих посадових осіб для будь-якого доступу до устаткування CA або OCSP користувача або до криптографічного модуля CA або OCSP користувача;

3) FORTEZZA CAW і зв'язані криптографічні модулі мають бути захищені від несанкціонованого доступу;

4) RA устаткування має бути захищене від несанкціонованого доступу, поки криптографічний модуль встановлюється й активізується;

5) для скорочення ризику підробки устаткування RA має реалізовувати засоби управління фізичним доступом, навіть коли криптографічний модуль не встановлений і не активізований. Ці механізми захисту повинні бути сумірними з рівнем загрози в середовищі RA устаткування.

Якщо змінні криптографічні модулі CA і OCSP користувача та будь-яка інформація активації, що використовується для доступу або включення криптографічних модулів чи устаткування, не застосовуються, то їх потрібно розміщувати в замкнутих контейнерах. Контейнери повинні забезпечувати фізичний захист, достатній для розміщення устаткування й інформації, сумірної з класифікацією відносно конфіденційності або значущості інформації, що захищається сертифікатами, випущеними CA. Дані активації повинні або запам'ятовуватись або записуватися й зберігатися способом, сумірним із рівнем захисту, що забезпечується криптографічним модулем.

Перевірка захисту устаткування, що містить устаткування CA і OCSP користувача, повинна здійснюватись до залишення устаткування без нагляду. У процесі перевірки необхідно визначити, що:

– устаткування знаходиться в стані, що відповідає поточному режиму експлуатації (наприклад, що криптографічні модулі на своєму місці, коли «відкрито», і захищені, коли «закрито»);

– будь-які контейнери захисту захищені належним чином;

– системи фізичного захисту (наприклад, блокування дверей, кришки отвору) функціонують належним чином;

– область захищена від несанкціонованого доступу.

Персона або група персон повинні бути явно відповідальними за виконання таких перевірок. Повинен вестись журнал, який ідентифікує персону, що виконує перевірку в кожному зразку. Якщо устаткування не має безперервного нагляду, остання персона перед відходом повинна ініціювати журнал відходу, де вказується дата і час, і заявляється, що всі необхідні механізми фізичного захисту на місці й активізовані.

Устаткування, що містить обладнання CA і OCSP користувача середнього або високого рівня гарантії, якщо залишається без нагляду більше ніж 24 години, мають бути захищене системою виявлення вторгнення. Окрім того, перевірка повинна проводитися щонайменше один раз кожні 24 години для гарантії, що ніяких спроб зламу механізмів фізичного захисту не було зроблено.

Поточна NSA політика вимагає, щоб апаратний криптографічний модуль, що використовується для випуску сертифікатів, ключі яких будуть застосовуватись для захисту секретної інформації, був засекречений на рівні секретної інформації як під час використання, так і під час невикористання. Причому під час невикористання він повинен зберігатися в контейнері, затвердженому для зберігання секретних засобів КЗІ, доступ до якого дозволяється тільки для санкціонованих CMA операторів.

Зберігання носіїв

Носії повинні зберігатися для захисту їх від ненавмисного пошкодження (вода, вогонь, електромагнітне поле тощо). Носії, які містять конфіденційну інформацію, наприклад, інформацію аудиту захисту, архівації та резервну інформацію, мають бути захищені від несанкціонованого доступу.

У центрах СА із середнім і вищим рівнями гарантій, які експлуатуються безперервно (протягом одного тижня або довше), повне системне резервування повинне виконуватися раз на тиждень. Для періодично експлуатованих СА із середнім і вищим рівнями гарантій повне системне резервування повинне виконуватися кожного разу, коли система включається, або один раз на тиждень, але не рідше. Щонайменше одна резервна копія повинна зберігатися в зовнішньому розташуванні (окремо від СА устаткування). Потрібно зберігати тільки найостаннішу резервну копію. Резервна копія повинна зберігатися разом з фізичними і процедурними засобами управління, сумірними із засобами управління операційної СА системи.

12.9.2. Процедурні засоби управління

Довірчі ролі

Довірча роль – це роль, виконавець якої здійснює функції, які можуть призвести до порушень, якщо виконуються неналежним чином, випадково чи зловмисно. Персонал, обраний на ці ролі, повинен бути старанним і заслуговувати на довіру. Функції, що виконуються в цих ролях, формують основу довіри вцілому й до ІВК. Існують два підходи для збільшення ймовірності успішного здійснення цих ролей. Перший підхід гарантії полягає в тому, що персона, яка виконує роль, заслуговує на довіру і навчена належним чином. Другим підходом є покладання функцій ролі на декількох людей таким чином, щоб будь-яка зловмисна дія вимагала таємної угоди між ними на здійснення порушення. Також для уникнення помилок і протидії невідповідній поведінці повинні застосовуватись спеціальні механізми.

Первинні довірчі ролі, визначені політикою, що розглядається, є СА, OCSP і RA об'єкти.

Центр сертифікації

Усі сертифікати, які виготовляються згідно з DoD політикою сертифікації, повинні випускатися СА службою, що діє під керівництвом СА. Відповідальна персона або орган (наприклад, рада директорів), визначені як СА служба, повинні бути призначеними і мати право здійснювати контроль відповідності.

Будь-який СА, який має відповідний затверджений ідентифікатор політики, визначений для нього, підлягає умовам цієї політики. Роль СА і відповідні процедури СА мають бути визначені в CPS.

Перш за все, обов'язками СА, згідно з умовами цієї політики, є гарантія здійснення таких функцій:

1) RA функціонує, як описано в регламенті;

2) генерація та скасування сертифікатів;

3) реєстрація сертифікатів і CRL;

4) здійснення зовнішнього резервування згідно з періодичним графіком, яке достатнє для відновлення післясистемного збою;

5) виконання інкрементних резервувань бази даних;

6) адміністративні функції, такі як повідомлення про компрометацію та підтримка бази даних;

7) програмування та управління апаратним криптографічним модулем, якщо воно застосовується.

Центр реєстрації

Будь-який центр реєстрації RA, який діє згідно з цією політикою, підлягає умовам цієї політики і PMA затвердженому CPS, згідно з яким він діє.

Перш за все обов'язками RA є:

– засвідчення особи, згідно з вимогами;

– уведення інформації про абонента та верифікація коректності таких даних;

– захищеність передач запитів і відповідей від CA;

– отримання і розповсюдження сертифікатів абонента.

Роль RA значною мірою залежить від реалізацій ІВК та локальних вимог. Обов'язки й засоби управління для RA мають бути явно описані в CPS положеннях CA, якщо в CA використовуються RA.

Інші довірчі ролі

Для Інфраструктур із середнім і вищим рівнями гарантій CMA повинен, у своєму CPS, визначити інші довірчі ролі, на які повинні покладатися обов'язки, що гарантують належну, безпечну й захищену експлуатацію CMA устаткування та реалізації процедур. Ці обов'язки включають:

– установку нових облікових записів;

– конфігурацію початкового вузлового і мережевого інтерфейсу;

– призначення привілеїв захисту та засобів управління доступом для облікових записів і інших довірчих ролей;

– створення пристроїв для підтримки відновлення з катастрофічних системних ситуацій;

– виконання системного резервування, модернізацію і відновлення програмного забезпечення;

– виконання захищеного зберігання й розповсюдження резервних копій і модифікацій до зовнішнього розташування;

– зміну конфігурації вузлового або мережевого інтерфейсу.

Адміністратор безпеки (аудитор відповідності):

– виконання контролю відповідності вимогам;

– виконання функцій архівації та видалення контрольного журналу захисту й інших архівних даних;

– перегляд контрольного журналу захисту.

Для гарантії системної цілісності потрібно забороняти виконання вказаних обов'язків CMA відносно своїх власних CMA засобів. CMA повинен підтримувати списки, включаючи імена, організації й контактну інформацію про тих, хто діє в цих довірчих ролях, і повинен зробити їх доступними для контролю.

ІВК спонсор (адміністратор сертифікації) здійснює роль Абонента для нелюдських системних компонентів і організацій (включаючи групи і ролі), що називаються суб'єктами сертифікації відкритого ключа. ІВК спонсор працює з CMA і (коли це можливо) їх TA для реєстрування компонентів (наприклад, маршрутизаторів, брандмауерів) і є відповідальним за виконання обов'язків абонентів, визначених у цьому документі.

Протокол on-line стану сертифікації

Будь-який OCSP об'єкт, який діє згідно з цією політикою, підлягає умовам цієї політики, і PMA затвердженого CPS, згідно якому він діє. Перш за все, OCSP об'єкт є відповідальним за:

– забезпечення стану скасування сертифіката для залежних сторін;

– гарантію, що характеристики стану скасування містять послуги автентифікації й цілісності, сумірні з гарантійним рівнем сертифіката, що перевіряється.

Ідентифікація й автентифікація для кожної ролі

Персона, яка здійснює довірчу роль, повинна автентифікувати себе для локальної системи згідно з діючими вимогами (DoDI 8500.2).

Персона, яка здійснює довірчу роль, повинна автентифікувати себе для компонента видаленої інфраструктури DoD PKI за допомогою дійсного DoD X.509 сертифіката.

Ролі, що вимагають розділення обов'язків

Ні за яких умов виконавець CMA ролі не повинен здійснювати функцію свого власного контролю або функцію аудитора захисту. Аудитор контролю не повинен виконувати будь-яку іншу роль в CMA. Окрім того, у FORTEZZA PKI, ISSO не повинен виконувати будь-яку іншу роль в CMA. CMA не повинен виконувати ніякої ролі в центрі CA, включаючи роль ISSO або аудитора відповідності. RA не повинен виконувати обов'язки системного адміністратора ISSO на будь-якій системі.

Програмне забезпечення й апаратні засоби CA, RA і OCSP об'єктів повинні визначати ці розподілення обов'язків.

Ніякий індивідуум не повинен мати більш ніж одну ідентичність у будь-якій системі CA, RA або OCSP об'єктів.

12.9.3. Персональні засоби управління

Особи обслуговуючого персоналу повинні вибиратися для будь-якої CMA або іншої довірчої ролі на підставі лояльності до держави, їх надійності та вірогідності. Обслуговуючий персонал може бути із числа військовослужбовців або урядовими цивільними фахівцями будь-якої організації, санкціонованими PMA для виготовлення й обслуговування DoD IBK сертифікатів згідно з цією CP, або підрядчиками таких організацій. Усі особи CMA повинні бути громадянами держави. Усі персони, що здійснюють довірчі ролі, окрім CMA, повинні бути громадянами держави або мати допуск до урядових секретів.

Усі операції CA і OCSP потужні об'єкти повинні управлятися персоною або органом (наприклад Радою Директорів). Ця персона або орган повинні бути визначені як CA або OCSP об'єкт високого рівня гарантії та OCSP потужних об'єктів повинні управлятися спеціальним уповноваженим або офіцером, урядовим службовцем GS-7 або вище, або цивільним фахівцем підрядчика/ постачальника еквівалентної або більшої відповідальності й рівня. Оператори й устаткування для інсталяції CA і OCSP потужного об'єкта повинні діяти в межах адміністративного управління визначеного адміністратора.

Персонал, призначений для застосування CMA устаткування в межах DoD PKI, може бути військовим, цивільним або підрядчиками і повинен:

– успішно здійснити відповідну навчальну програму;

– продемонструвати здатність до виконання своїх обов'язків;

– бути надійним;

– не мати ніяких інших обов'язків, які впливали або суперечили б його обов'язкам як СМА;

– не бути раніше звільненим від СМА або COMSEC наглядачем за виконанням службових обов'язків з причин недбалості або невиконання своїх обов'язків;

– не відміняти або не скасовувати свій допуск до секретів;

– не бути визнаним винним у кримінальному злочині;

– бути призначеним у письмовій формі затверджувальним органом або бути договірною стороною для надання ІВК послуг.

СМА, що випускає або запитує сертифікати, які встановлюють рівень допуску до секретів (наприклад, конфіденційно, таємно, цілком таємно), повинен мати рівень допуску до секретів рівний або вище встановленого рівня допуску. Самим СМА не потрібно тримати інші санкції, встановлені в сертифікатах (наприклад, категорії захисту), якщо тільки цього не вимагає політика, зв'язана із цими санкціями.

Процедури біографічної перевірки

Місцеві служби, відомства або суспільні організації повинні виконувати біографічні перевірки. Такі перевірки мають виконуватися виключно для визначення придатності персони здійснювати ІВК роль, і не повинні бути скасовані, якщо тільки це не потрібно. Процедури біографічної перевірки мають бути описані в CPS.

Періодичність і вимоги перепідготовки

Ті, хто залучені в здійсненні ІВК ролей, повинні бути обізнані про зміни в СМА. Будь-яка істотна зміна в СМА операції повинна супроводжуватися планом навчання (усвідомлення), і виконання такого плану має бути задокументованим. Прикладами таких змін можуть бути СА програмні або апаратні відновлення, зміни в автоматизованій системі захисту й переміщення СА устаткування.

Періодичність та послідовність чергування робіт

Ця політика не робить ніякого обумовлення щодо частоти або послідовності чергування робот. Локальні політики, які накладають вимоги, повинні передбачати безперервність і цілісність ІВК послуг.

Санкції щодо несанкціонованих дій

СМА повинна приймати відповідні адміністративні та дисциплінарні дії проти персоналу, який порушує цю політику.

Вимоги до незалежного підрядчика

Персонал підрядчика, що залучається для використання будь-якої частини ІВК, повинен відповідати тим самим критеріям, що й урядовий фахівець держави, і допускатися до рівня інформації, захищеної сертифікатами, випущеними ІВК. ІВК постачальники, які забезпечують послуги для DoD, повинні встановлювати процедури для гарантії виконання будь-якими субпідрядниками своїх дій згідно з їх CPS і цією політикою.

Документація, що поставляється персоналу

Для кожної ролі персоналу, який здійснює цю роль, повинна бути надана документація, достатня для визначення обов'язків і процедур.

12.9.4. Процедури ведення контрольного журналу

До устаткування CA, OCSP і RA в частині реєстрації висуваються певні вимоги.

По-перше, будь-які здатності контролю захисту базової операційної системи СМА повинні перевірятися протягом інсталяції.

По-друге, щонайменше повинні бути зареєстровані такі СМА події:

– доступ до СМА застосування (наприклад, logon);

– повідомлення, що отримані з будь-якого джерела, що запрошують СМА до дії (запити сертифіката, підписання сертифіката, скасування сертифіката, повідомлення про компрометацію);

– OCSP об'єкти звільнені від вимоги аудиту;

– дії, що прийняті відповідно запитам СМА дій;

– для OCSP об'єктів, СМА ISSO повинен реєструвати результати аналізу щотижневої вибірки відповідей, надісланих кожним відповідачем;

– фізичний доступ, завантаження, обнуління, передача ключів, резервування, отримання або знищення СМА криптографічних модулів;

– прийняття, обслуговування (наприклад, кодування або інші маніпуляції з криптографічними механізмами та перетвореннями) і постачання апаратних криптографічних модулів;

– реєстрація будь-якого матеріалу в репозиторії;

– аномалії, помилкові стани, невдачі перевірки цілісності програмного забезпечення, прийняття неправильних або невірно маршрутизованих повідомлень;

– будь-які відомі або підозрілі порушення фізичного захисту, підозрілі або відомі спроби атакувати СМА устаткування через мережеві атаки, збої устаткування, енергетичні простої, мережеві збої або порушення цієї політики сертифікації.

Устаткування CA і OCSP потужних об'єктів повинні реєструвати інсталяцію серверів, доступ і модифікацію (для включення змін в конфігураційні файли, профілі захисту, привілеї адміністратора).

Для CA і OCSP потужних об'єктів обов'язкова реєстрація:

– доступу до устаткування (наприклад, доступ до кімнати);

– файлового маніпулювання й управління обліковими записами;

– будь-якого матеріалу в репозиторії;

– доступу до баз даних;

– будь-яке використання особистого ключа підпису.

Для кожної події, що належить контролю, СМА звіт з аудиту захисту повинен щонайменше включати:

– тип події;

– час виникнення події;

– для повідомлень з RA (або інших об'єктів), що запитують CA дії, джерело повідомлень, адресат і їх вміст;

– спроби підпису або скасування CA сертифіката – з реєстрацією успіху або невдачі;

– дії, що ініційовані оператором (включаючи доступ до устаткування й застосування);

– там, де можливо, дані контрою захисту повинні бути зібрані автоматично;

– коли це неможливо, повинен використовуватися журнал для службових записів, у паперовій формі, або інший фізичний механізм;

– усі журнали контрою захисту, як електронні, так і неелектронні, повинні зберігатися згідно з вимогами;

Періодичність обробки даних журналу

Для середнього рівня гарантій необхідно щонайменше 6 періодичних переглядів за рік, причому мінімум 25 відсотків даних контролю з дня проведення останнього перегляду. Для високого рівня гарантій щонайменше потрібно 12 (щомісячно) переглядів за рік, із них щонайменше 33 відсотки даних контролю захисту, починаючи з проведення останнього перегляду.

СМА повинен реалізувати гарантовано процедури передачі даних контролю захисту перед перезаписом або переповненням автоматизованих системних журналів контролю захисту.

Період зберігання контрольного журналу

Інформація, що формується на устаткуванні СМА, повинна утримуватися на устаткуванні СМА, поки інформація не буде видалена, і зберігатися згідно з цією політикою. Видалення даних контролю захисту з СМА устаткування повинно виконуватися відповідним об'єктом, але не СМА. Цей об'єкт має бути визначений у CPS положеннях СМА. Дані контролю захисту повинні бути внутрішньо доступні щонайменше протягом двох місяців або до їх перегляду, і потім зовні як архівні записи. Усі контрольні журнали захисту, як електронні, так і неелектронні, повинні зберігатися й бути доступними протягом перевірок.

Захист контрольного журналу

Дані контролю захисту не повинні бути доступними для читання або модифікації будь-якою людиною або будь-яким автоматизованим процесом, окрім тих, які виконують обробку контролю захисту. Конфігурація та процедури СМА системи повинні бути реалізовані разом для гарантії того, що тільки санкціоновані люди архівують або видаляють дані контролю захисту. Об'єкту, що виконує архівацію даних контролю захисту, не потрібно мати доступ «Модифікації», але процедури мають бути реалізовані для захисту архівованих даних від видалення або знищення до завершення періоду зберігання даних контрою захисту. Дані контролю захисту повинні бути переміщені в безпечне, захищене місце зберігання окремо від устаткування СМА.

Резервування контрольного журналу

Дані контролю захисту повинні підтримуватися щонайменше щомісячно. Копія даних контролю захисту повинна щомісячно передаватися та зберігатися назовні поза ЦСК, як визначено в CPS.

Система контролю

Процес контролю захисту повинен виконуватися незалежно і не повинен будь-яким шляхом бути під управлінням СМА. Процеси контролю захисту операційної системи повинні бути викликані в системному запуску і припиняються тільки при зупинці системи. Усі процеси контролю захисту застосувань повинні бути викликані в системному запуску і припиняються тільки при зупинці застосування. Як тільки стає очевидним збій автоматизованої системи контролю

захисту, CMA повинен припинити всі операції, за винятком обробки скасування, поки можливість контролю захисту не буде відновлена. При цих обставинах CMA повинен застосувати механізми для запобігання несанкціонованих CMA функцій. Ці механізми повинні бути описані в CPS положеннях CMA.

Повідомлення суб'єкта

Щодо повідомлення суб'єкта не висуваються вимоги, що подія була перевірена. Сповіщення в реальному часі цією політикою не вимагаються і не забороняються.

Оцінка вразливості

CMA, системний адміністратор і інший операційний персонал повинен спостерігати за спробами порушення цілісності системи управління сертифікацією, включаючи устаткування, фізичне розташування та персонал. Дані контролю захисту повинні переглядатися аудитором захисту (адміністратором безпеки) відносно таких подій як повторні невдалі дії, запити привілейованої інформації, спроби доступу до системних файлів і не автентифіковані відповіді. Аудитори захисту повинні перевіряти безперервність даних контролю захисту. Керівник захисту ISSO повинен документувати звітні результати періодичного перегляду контрольних журналів.

12.9.5. Архівація записів

Типи архівних записів

CMA архівні записи повинні бути достатньо деталізовані для верифікації управління ІВК належним чином, також як і верифікації достовірності будь-якого сертифіката протягом всього його періоду достовірності (наприклад, дійсний, скасований, призупинений). Принаймні повинні архівуватися такі дані.

Протягом CMA системної ініціалізації:

– CMA акредитація (якщо необхідно);

– CPS, CPS;

– будь-які договірні або інші угоди, з якими CMA зв'язаний або який стосується операцій;

– звіти перевірки відповідності;

– конфігурація системного устаткування.

Під час операції CMA для середнього та вищого рівнів гарантій:

– модифікації або відновлення для будь-якого з вищевказаних елементів даних;

– запити сертифікації та запити скасування;

– документація автентифікації особи абонента;

– документація отримання та прийняття сертифікатів;

– документація отримання токенів;

– усі сертифікати та CRL (або інша інформація скасування) як випущені, так і видані;

– дані контролю захисту;

– інші дані або застосування, достатні для верифікації архівного вмісту;

– усі робочі комунікації з PMA, іншими CMA й аудиторами контролю.

Період зберігання

Архівні записи, повинні зберігатися як визначено в затвердженому реєстрі записів згідно з DoD програмою управління записами DoDD 5015.2. Інакше архівні записи повинні зберігатися, без будь-якої втрати даних протягом періоду:

– щонайменше десять років, шість місяців для середнього рівня гарантій;
– щонайменше двадцять років, шість місяців для високого рівня гарантій;
– щонайменше одинадцять років для FORTEZZA/CAW PCA;
– щонайменше одинадцять років для FORTEZZA/CAW ICRLA;
– щонайменше до списання FORTEZZA/CAW PKI CA плюс один рік.

Застосування, що необхідні для читання цих архівів, повинні підтримуватися щонайменше протягом вищевказаного відповідного періоду зберігання.

CMA повинен підтримувати архівовані дані або забезпечувати архівовані дані та засоби їх застосування, які необхідні для читання архівів, для PMA затвердженої DoD архівної служби. Ця служба повинна зберігати ці засоби застосування, необхідні для читання цих архівованих даних, до завершення призначеного періоду архівації.

FORTEZZA PKI CA повинен підтримувати архівовані дані або забезпечувати архівовані дані та засоби їх застосування, необхідні для читання архівів. Для Сервісної/ Відомчої архівної служби, яка повинна зберігати ці засоби застосування, необхідні засоби для читання цих даних, до завершення призначеного періоду архівації.

Захист архіву

Ніякий несанкціонований оператор устаткування CMA не повинен бути здатний модифікувати або видаляти архів, але архівовані записи можуть переміщатися на інший носій. Якщо основний носій не може зберігати дані протягом необхідного періоду, центром архівації має бути визначений механізм для періодичної передачі архівованих даних на новий носій. Ніяка передача носія не повинна зробити недійсним CMA зроблені та приєднані підписи. CMA повинен підтримувати список людей, санкціонованих для модифікування або видалення архіву, і робити цей список доступним протягом контролю відповідності CP. Випуск конфіденційної архівної інформації повинен здійснюватися згідно з політикою. Архівні носії повинні зберігатися в окремому, безпечному, захищеному устаткуванні. До архівації архівні записи мають бути розмічені відмітним ім'ям, датою та класифікацією CMA.

Процедури детального опису створення, упакування та відправки архівної інформації мають бути видані в CMA методичному довіднику або CPS. Тільки санкціоновані оператори устаткування CMA можуть мати доступ до архіву.

12.9.6. Заміна ключів

CA використовує тільки особистий ключ підпису для створення сертифікатів. Проте користувачі використовують CA сертифікат протягом терміну дії сертифіката абонента. Тому CA не повинні випускати абонентські сертифікати, які продовжуються після терміну завершення їх власних сертифікатів і відкритих ключів, і період достовірності CA сертифіката повинен розширювати один період достовірності сертифіката абонента з урахуванням останнього використання CA

особистого ключа. Для мінімізації ризику відносно ІВК через компрометацію СА ключа особистий ключ підпису повинен змінюватися частіше, і тільки новий ключ треба використовувати в цілях підпису сертифіката з того часу. Попередній (старий), проте дійсний сертифікат має бути доступним для верифікації старих підписів, поки не завершиться термін дії всіх абонентських сертифікатів, що виготовлені з його використанням. Якщо старий особистий ключ використовується для підписання CRL, які містять сертифікати, підписані цим ключем, то старий ключ повинен бути збережений і захищений (див. також RFC 4210).

У таблиці 12.17 наведені максимальні періоди достовірності СА сертифіката підпису й максимальний термін дії особистого ключа підпису, відокремлені косою рискою. Термін дії RA ключа є таким, як описано для СА і для абонентів. Якщо СА сертифікат і термін дії особистого ключа вибрані коротшими, ніж абонентські, то термін дії RA сертифіката й ключа має бути не більше, ніж термін дії СА. Відзначимо, що особисті ключі підпису, які стали вже недійсними для виготовлення сертифіката, можуть ще використовуватися для CRL підпису. Усі значення подані в роках.

Таблиця 12.17. **Максимальні строки дійсності ключів**

Рівень гарантій	СА	СА автовипуску	Проміжний СА	Кореневий СА
Середній рівень гарантії	6/3	6/6	10/4	36/20
Високий рівень гарантій	6/3	6/6	10/4**	36/20**

Примітки

Стовпець СА автовипуску стосується СА, які використовують тільки автоматизований процес для випуску сертифікатів.

** PCA і PAA FORTEZZA ІВК високого рівня гарантій складає 11/5 і 36/25, відповідно.

12.9.7. Компрометація та відновлення після лиха

Якщо стає відомо про спробу потенційної компрометації СА, треба провести дослідження з метою визначення характеру й ступеня збитку. Якщо виникла підозра, що СА особистий ключ скомпрометовано, потрібно дотримуватися процедури встановлення виду компрометації. Інакше область дії потенційного збитку повинна бути оцінена з метою визначення, чи потрібно відновлення СА, чи потрібно скасування тільки деяких сертифікатів і/або потрібно оголошення скомпрометованим особистого ключа СА.

У разі компрометації ключа OCSP об'єкта СА, який випустив сертифікат, OCSP об'єкт повинен скасувати сертифікат такого OCSP об'єкта, а інформація скасування повинна бути негайно видана найшвидшим способом. Згодом, OCSP об'єкт повинен перекодуватися.

Також СА повинен підтримувати резервні копії системи, баз даних і особистих ключів з метою відновлення працездатності СА у разі зіпсування програмного

забезпечення і/або даних. Перед операціями відновлення CA повинен гарантувати, що цілісність системи була відновлена.

У разі компрометації особистого ключа CA старий CA повинен скасувати такий CA сертифікат, і інформація скасування повинна бути видана негайно найдоцільнішим способом. Згодом CA інсталяція повинна бути встановлена повторно. Якщо CA кореневий, то довірчий, самопідписаний сертифікат повинен бути видалений з кожного застосування користувача, а новий розповсюджений через захищені зовнішні механізми. Кореневий CA повинен описати свої підходи для реагування на компрометацію ключа кореневого CA у своїх CPS.

Центри CA середнього та високого рівнів гарантій повинні підтримувати відповідним чином затверджений план відбудови після лиха.

У разі лиха, у якому CA устаткування стає пошкодженим і недіючим, CA повинні щонайшвидше перевстановлюватися, надаючи пріоритет можливості скасування сертифікатів абонента. Якщо CA не може перевстановити можливості скасування раніше наступного періоду відновлення, указаного в найостаннішому CRL, випущеному CA, або одного тижня, то CA повинен повідомити про це PMA. PMA повинен прийняти рішення щодо оголошення компрометованим особистого ключа підписання CA і перевстановити CA ключі та сертифікати, усі перехресні сертифікати й усі абонентські сертифікати або дозволити додатковий час для повторного встановлення можливості скасування CA.

У разі лиха, внаслідок якого CA інсталяція стає фізично пошкодженою і в результаті всі копії CA підпису знищуються, CA повинен запитувати скасування своїх сертифікатів. Тоді CA інсталяція повинна бути повністю відновлена через повторне встановлення CA, генерацію нових особистих і відкритих ключів, їх повторну сертифікацію, а також зробити повторний випуск усіх перехресних сертифікатів. Нарешті, всі абонентські сертифікати мають бути виготовлені повторно. У таких випадках будь-які користувачі, які продовжують використання сертифікатів, підписаних за допомогою знищеного особистого ключа, ризикують самі й піддають ризику тих, кому вони пересилають дані.