УДК 681.3.06: 519.248.681

ПРОЦЕДУРИ ТА КРИТЕРІЇ ПЕРЕХРЕСНОЇ СЕРТИФІКАЦІЇ PKI

Ю. М. ІЩЕНКО

Визначаються процедури та критерії, що повинні застосовуватися при здійсненні перехресної сертифікації в системі інфраструктури відкритих ключів (ІВК) та пояснюються додаткові вимоги, що висуваються для забезпечення довіреної взаємодії між різними мостами перехресної сертифікації.

The paper determines procedures and criteria that must be used in realizing cross-sectional certification in the system of public key infrastructure and explains additional requirements put forward for ensuring trusted interaction between bridges of cross-sectional certification.

ВСТУП

У цій статті визначаються процедури та критерії, що повинні застосовуватися при здійсненні перехресної сертифікації в системі інфраструктури відкритих ключів (ІВК) із залученням державного органу вповноваженого на перехресну сертифікацію (ДОУПС).

Розглянемо критерії перехресної сертифікації, які мають враховуватися посадовими особами відповідальними за обробку запиту на здійснення перехресної сертифікації (далі – запит). Процес надання відповіді складається з чотирьох етапів:

1. Ініціювання;
2. Зіставлення політик застосування сертифікатів;
3. Тест технічної інтероперабельності;
4. Укладання угоди;
5. П'ятий етап (підтримка) ми виключимо з опису, оскільки він не є частиною критеріїв перехресної сертифікації.

Обов'язковою вимогою до державних претендентів є їх сертифікації та акредитація згідно вимог чинного законодавства та інших політик в сфері захисту інформації.

Усі претенденти на здійснення перехресної сертифікації з ДОУПС повинні отримати унікальні об'єктні ідентифікатори Політики в стандартному реєстрі об'єктних ідентифікаторів ISO за допомогою відповідного комерційного або національного центру реєстрації.

1. УМОВИ, ЩО ПОВИННІ ВИКОНУВАТИСЯ ПРИ ЗДІЙСНЕННІ ПЕРЕХРЕСНОЇ СЕРТИФІКАЦІЇ

При здійсненні процесу перехресної сертифікації, орган, що вповноважений з питань політики державної ІВК, в будь-який момент може прийняти рішення щодо продовження перехресної сертифікації (умовне або безумовне).

1.1. Ініціювання (етап 1)

При отриманні запиту на здійснення перехресної сертифікації орган, що вповноважений з питань політики державної ІВК, має попередньо визначитися щодо того чи є запит повним і чи надано всю необхідну документацію, як того вимагає *інструкція з надання запиту на здійснення перехресної сертифікації*. Відповідне рішення є основою для визначення думки щодо коректності запиту.

Для іноземних претендентів, обов'язковим є заповнення пункту, в якому пояснюється намір здійснити перехресну сертифікацію із застосуванням ДОУПС. Пояснення можуть складатися з письмового пояснення, що має бути підписане вищим державним службовцем об'єкта та містити причини надання запиту.

Запити мають бути підписані таким представником вищого керівництва (директором або президентом) організації, що відповідає за ІВК, що має право подавати заяву на здійснення процесів перехресної сертифікації організації. Подача заяви має передбачати можливі витрати організації на здійснення перехресної сертифікації та дозвіл на надання інформації, необхідної від претендента.

Зовнішні претенденти, якщо інше непередбачено, мають надавати свідчення щодо поточного правового статусу об'єкта відповідального за ІВК. Також для підтвердження легітимності діяльності організації може вимагатися надати сертифікат від уповноважених органів влади в межах юрисдикції, яких було створено організацію.

Від іноземних претендентів може вимагатися надати свідчення щодо своїх фінансових можливостей та стану управління ризиками, пов'язаними із експлуатацією ІВК. Фінансові можливості можуть підтверджуватися шляхом надання організацією копії гарантій виконання контракту, акредитивного листа від фінансового інституту або листа, що вказує на відповідну страховку, або лист від компанії зі страхування поручительського зобов'язання, фінансової компанії чи страхової компанії.

Метою цієї вимоги є підтвердження можливості організації виконати будь-які фінансові зобов'язання, які пов'язані із експлуатацією УС, в тому числі, відповідальність перед абонентами або іншими об'єктами, що покладаються на випущені сертифікати та електронні цифрові підписи, які перевіряються через застосування сертифікатів відкритих ключів. Природа та достатність необхідних фінансових можливостей визначається органом уповноваженим з політики.

Правовий статус та фінансові можливості є критеріями доказовості, що складають основу довіри між урядом України та претендентами. Деякі претенденти звільняються від цих критеріїв доказовості.

Заява не вважається повною до того часу, доки орган, що вповноважений з питань політики державної ІВК, не визначить, що усю необхідну документацію було надано.

У загальному випадку, надається рекомендації продовжувати перехресну сертифікацію, якщо орган, який вповноважений з питань політики державної ІВК, вважає, що виконуються нижче перераховані умови, претендент може керувати ІВК, і має:

– Політику (-и) (або її (їх) еквівалент);

– Звід практик сертифікації;

– Політику безпеки (або її еквівалент), щодо захисту УС;

– Проведено аудит відповідності кореневого УС претендента;

– Здійснюються процеси підтримки політики застосування сертифікатів претендента;

– Надано усю інформацію (з урахуванням технологій, що використовуються претендентом), згідно переліку документів, що подаються із заявою, який визначено ДОУПС;

– Технології, що використовуються претендентом, та ДОУПС є сумісними (відповідність стандартів);

– ІВК претендента забезпечує рівень гарантій, що надається ДОУПС;

– Надано адекватну (правовому статусу) інформацію щодо організації, яка відповідає за ІВК претендента;

– Надано адекватну (фінансовим можливостям) інформацію щодо претендента та фінансові можливості дозволяють забезпечити надійне функціонування ІВК претендента.

– Якщо розглядається питання здійснення перехресної сертифікації для державного претендента, він має зобов'язаний пройти сертифікацію та акредитацію згідно вимог чинного законодавства та інших політик в сфері захисту інформації.

ІВК претендента має надати представника, що має надавати органу, що вповноважений з питань політики державної ІВК, допомогу в частині оцінювання заяви претендента. Заява претендента оцінюється з точки зору безпечності, конфіденційності та умов експлуатації.

Документи політики застосування сертифікатів можуть підтримувати різні рівні гарантій. Також можуть знадобитися додаткові оцінювання для зіставлення ІВК претендента та відповідного рівня гарантій в політиці застосування сертифікатів ДОУПС.

1.2. Зіставлення політик застосування сертифікатів (етап 2)

Зіставлення політик є процесом порівняння політик застосування сертифікатів претендента та ДОУПС та оцінювання міри, якою політики, практики та процедури ІВК претендента відповідають до таких, що застосовуються ДОУПС. Категорії, що мають використовуватися, знаходяться в матриці відповідності. Будь-яка перевірка/розгляд політики застосування сертифікатів ІВК претендента містить порівняння кожного розділу документа з відповідним розділом політики застосування сертифікатів ДОУПС з метою виявлення їх еквівалентності або можливості порівняння.

Результати зіставлення політик заносяться до матриці відповідності. Усі категорії та елементи, які не знайдено в політиці застосування сертифікатів ІВК претендента, мають бути перераховані у висновках до матриці відповідності. Якщо висувається вимога щодо підтримки додаткової інформації, що доповнює коментарії, то впродовж коректності посилання на цю інформацію може використовуватися додаткова документація.

Зіставлення політик є суб'єктивною задачею. Однакові ступені захисту можуть бути забезпечені з використанням різних засобів та заходів захисту. Задача зіставлення політик полягає у визначенні «еквівалентності» різних засобів захисту, для встановлення того, що політики забезпечуються порівнянний рівень гарантій (або встановлення міри відмінності рівнів гарантій). Після встановлення еквівалентності, вважається, що перехресні сертифікати відбивають довіру однієї ІВК до іншої. Очікується, що ІВК претендента буде виконувати зіставлення своєї політики застосування сертифікатів та політики ДОУПС з метою визначення рівня гарантій, що надаються останньою.

З метою здійснення перехресної сертифікації має бути перевірена надійність ІВК претендента. Це потребує, щоб ІВК претендента здійснювала процес спостереження за політикою застосування сертифікатів. Головним елементом процесу спостереження є проведення аудитів відповідності, згідно визначеної в ІВК претендента політики застосування сертифікатів. ІВК претендента має надати докази того, що процес спостереження виконується належним чином. Наприклад, докази можуть включати додаткові звіти з результатів аудиту різних компонентів ІВК претендента, таких, які підпорядковані УС та центри реєстрації.

Оскільки стандарти аудиту інфраструктури відкритих ключів/органів уповноважених на сертифікацію набувають подальшого попиту, то перевірка відповідності міжнародним стандартам, що перевірена в ході незалежного аудиту із залученням кваліфікованих експертів, може стати обов'язковою для здійснення перехресної сертифікації з ДОУПС. З причини відсутності таких стандартів, на цей час, результати аудиту приймаються, якщо вони виконані незалежними третіми сторонами, що мають досвід в сфері застосування та оцінювання систем ІВК, та використовують прийнятні методології аудиту.

1.3. Тест технічної інтероперабельності (етап 3)

Технічне тестування інтероперабельності проводиться для перевірки технічної сумісності ДОУПС та кореневого УС претендента. Метою проведення тестування є визначення можливості здійснення успішного обміну перехресними сер-

тифікатами та перевірка інтероперабельності каталогів. ДОУПС не має право випускати перехресні сертифікати до отримання позитивних результатів тестів. Орган, що вповноважений з питань політики державної ІВК, експлуатує прототип ДОУПС від імені уряду України. Його конфігурування виконано так, щоб він був копією виробничого ДОУПС. Для закінчення тесту технічної інтероперабельності може потребуватися залучення технічного персоналу УС претендента.

Для проведення тестування, ІВК претендента може використовувати обладнання дослідної моделі, що налаштована ідентично до УС або використовувати власний виробничий УС. Претендент несе фінансову відповідальність за всі витрати, що є наслідком тестування технічної інтероперабельності.

При підготовці звіту з технічної інтероперабельності, підрозділ державної ІВК описує результати тестів та надає їх до органу, що вповноважений з питань політики державної ІВК.

Звіт також має містити опис недоліків, які було викрито при тестуванні. Перелік недоліків може містити як недоліки технічної інтероперабельності, так і потенційно можливі проблеми, які не було викрито тестовими критеріями. Звіт також має містити очікувані наслідки від викритих недоліків та рекомендації від органу, що вповноважений з питань політики державної ІВК.

Успішне завершення тесту технічної інтероперабельності та заповнення переліку документів, що подаються із заявою, який визначено ДОУПС для ІВК претендентів має визначити технічні вимоги до перехресної сертифікації.

1.4 Укладання угоди (етап 4)

Обговорення угоди з перехресної сертифікації

Комплексне оцінювання відповідності ІВК претендента включає оцінювання інформації, зібраної протягом тестування технічної інтероперабельності та результатів зіставлення політик. Якщо отримані результати вказують на те, що ІВК претендента відповідає рівню гарантій ДОУПС та претендент погоджується з цими результатами, то орган, що вповноважений з питань політики державної ІВК, може ініціювати обговорення з метою укладання меморандуму про угоду.

Взаємовідносини між урядом України та організацією, що експлуатує ІВК, регламентуються меморандумом про угоду, та мають бути підписаними на основі рекомендацій органу, який вповноважений з питань політики державної ІВК (головою цього органу). Для підписання будь-яких рекомендацій органу, що вповноважений з питань політики державної ІВК, виконується додаткова перевірка заяви претендента, обговорення проекту меморандуму про угоду у прийнятному для органу, що вповноважений з питань політики державної ІВК, вигляді. Угода також має бути підписана вповноваженим органом з боку претендента.

Процедура визначення того, чи подана угода в прийнятному вигляді не може бути абстрактно описана. На сайті органу, що вповноважений з питань політики державної ІВК, має розміщатися макет меморандуму про угоду. З метою укладання угоди допускаються внесення змін до цього макету.

1.5. Підтримка взаємодії, продовження та припинення (етап 5)

Після укладання меморандуму про угоду з перехресної сертифікації та випуску перехресних сертифікатів, ДОУПС та претендент (тепер вже філія) входять у певні взаємовідносини, що є предметом для періодичного розгляду. В угоді має визначатися період повторного розгляду.

Орган, що вповноважений з питань політики державної ІВК, може припинити дію угоди та скасувати перехресні сертифікати, якщо з'ясується, що перехресна сертифікація філії не співпадає з національними інтересами України.

2. ВЗАЄМНА ПЕРЕХРЕСНА СЕРТИФІКАЦІЇ ДВОХ МОСТІВ

Якщо два мости перехресної сертифікації приймають рішення взаємодіяти, то мають бути застосовані спеціальні правила. Це обумовлюється тим, що в такому випадку перехресній сертифікації підлягають не два чи більше ІВК, а два домени довіри. Цей розділ присвячено поясненню додаткових вимог, що висуваються для забезпечення довіреної взаємодії між різними мостами перехресної сертифікації.

2.1. Загальні положення

Як наслідок того, що кожен з мостів є незалежним, їх вимоги є взаємними та двобічними. Для забезпечення взаємодії двох мостів, необхідно щоб кожен з них ясно розумів правила експлуатації іншого. Отже, новими вимогами є двобічне оцінювання критеріїв та методології та нормативних документів з метою розуміння бізнес планів, правил експлуатації та головного уповноваженого органу моста.

При оцінюванні необхідно відповісти на такі питання:

– Хто є вповноваженим органом для моста?

– Якщо міст є легітимним, від імені якого уповноваженого органу він спілкується та від чийого імені діє? Чи можуть сторони вступи в правові або квазіправові відносини?

– Яка природа взаємовідносин між ІВК членами та мостом (наприклад, якщо ІВК член також експлуатує міст, або керує мостом ІУП, ДОУПС має знати про ці стосунки; інший приклад, чи ухиляється ІУП від виконання вимог, і чи може це підірвати довіру до деяких ІВК за певних обставин)?

– Якій державі служить міст та чи дійсно ІВК, що були перехресно сертифіковані цим мостом, мають таку бізнесову необхідність взаємодіяти з членами іншого моста-кандидата, що це виправдовує ризики взаємодії двох мостів?

– Які існують процеси та процедури розв'язання конфліктів та хто відповідає за їх виконання?

– Які до ІВК застосовуються критерії, з метою визначення його інтероперабельності з мостом та визначення можливості його перехресної сертифікації?

– Які існують процедури перехресної сертифікації ІВК?

– Яким чином проводиться оцінювання ІВК для здійснення перехресної сертифікації?

– Яким чином органи, що вповноважені з питань політики/ управління повноваженнями ОУПС перевіряють, що його ІВК експлуатуються відповідно до угод укладених з ОУПС?

– Чи дозволяє аудит ОУПС повною мірою оцінити надійність операцій та процедур ОУПС? Що аудит робить стосовно всіх елементів політики застосування сертифікатів?

У дійсний час для органу, що вповноважений з питань політики державної ІВК, лише розробляються процедури взаємної перехресної сертифікації з іншими мостами.

2.2. Процедури здійснення перехресної сертифікації двох мостів

Незважаючи на методологію та процедури, що затверджені, органу, що вповноважений з питань політики та органу, що вповноважений на управління повноваженнями, необхідно відповісти на наведені нижче питання, це робиться за для того, щоб процес перехресної сертифікації забезпечив кожній стороні довіру до ІВК, що є членами іншої сторони. Усі процедури, що наведені нижче, спрямовані на отримання інформації, яка необхідна для кращого розуміння операційних та бізнес ризиків іншої сторони.

З метою забезпечення вдалої перехресної сертифікації, пропонується розробити відповідні процедури. Оскільки мости є незалежними, вони мають узгодити вибір методології перехресної сертифікації. Нижче наведено пропозиції, що є пропозиціями державної ІВК:

1. Наданням кожним з мостів заяви на здійснення перехресної сертифікації до органу, що вповноважений з питань політики іншої сторони;

2. Виконання двобічного зіставлення політик застосування сертифікатів з метою перевірки інтероперабельності локальним уповноваженим органом;

3. Двобічне оцінювання статутів (або їх еквівалентів) органу, вповноваженого за питань політики / органу вповноваженого на управління повноваженнями;

4. Двобічне оцінювання документів з методології та критеріїв перехресної сертифікації (або їх еквівалентів);

5. Виконання двобічного тестування технічної інтероперабельності із залученням відповідного уповноваженого органу (або його аналогу);

6. Обмін листами з результатами аудиту відповідності, які підтверджують, що мости експлуатуються відповідно до зводу практик сертифікації, а він у свою чергу не суперечить вимогам політики застосування сертифікатів;

7. Обговорення МПУ, з метою з'ясування того, як перехресна сертифікація ОПУС впливатиме (обмежувати або керуватиме) транзитивною довірою до інших об'єктів, що перехресно сертифіковані із залученням ОУПС;

8. Проведення щорічних перевірок та незалежного аудиту функціонування кожного з мостів.

ВИСНОВКИ

Таким чином, можна зробити висновок, що найбільш повні переваги застосування криптографії з відкритим ключем може бути отримано шляхом здійснення перехресної сертифікації інфраструктур відкритих ключів. Зважаючи на вимоги відповідного розподілення ресурсів держави, деякі параметри мають встановлюватися таким чином, щоб визначати пріоритетність дій з перехресної сертифікації.

Література.

[1] *D.Richard Kuhn, Vincent C. Hu, W.Timothy Polk, Shu-Jen Chang.* «Introduction to Public Key Technology and the Federal PKI Infrastructure». NIST SP 800-32. 2001.

[2] *C. Adams, P. Cain, D. Pinkus, R. Zuechenato.* Internet X.509 public key infrastructure – Time Stamp Protocol.

[3] Постанова КМУ від 28.10.2004 №1451 „Положення про центральний засвідчувальний орган»

[4] *Горбатов В.С., Полянская О.Ю.* Основы технологии PKI. – М.: Горячая линия – Телеком, 2004 – 246с.

[5] Основной ISO/IEC 9594-8, Information technology – Open systems interconnection – The Directory: public-key and attribute certificate frameworks

Надійшла до редколегії 24.09.2008

Іщенко Юлія Михайлівна, асистент кафедри Безпеки інформаційних технологій ХНУРЕ. Область наукових досліджень: системи захисту інформації.