КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (6), 2019
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2019.6.1931
УДК 004.738.5

Курбатов Олександр Сергійович
Харківський національний університет радіоелектроніки, кафедра безпеки інформаційних технологій, Харків, Україна
ORCID ID: 0000-0002-8237-4377
olkurbatov@gmail.com

Кравченко Павло Олександрович
кандидат технічних наук
Distributed Lab, Харків, Україна
ORCID ID: 0000-0002-0456-3295
pavel@distributedlab.com

Полуяненко Микола Олександрович
кандидат технічних наук
доцент кафедри безпеки інформаційних систем і технологій Харківського національного університету імені. В. Н. Каразіна, Харків, Україна
ORCID ID: 0000-0001-9386-2547
nlfsr01@gmail.com

Олексій Шаповал
Харківський національний університет імені В.Н. Каразіна, кафедра безпеки інформаційних систем і технологій, Харків, Україна
ORCID ID: 0000-0003-4478-3193
alex.shapoval@protonmail.com

Кузнєцова Тетяна Юрьевна
науковий співробітник науково-дослідної частини Харківського національного університету імені В.Н. Каразіна, Харків, Україна
ORCID ID: 0000-0001-6154-7139
kuznetsova.tatiana17@gmail.com

ДЕЦЕНТРАЛІЗОВАНА СИСТЕМА ІДЕНТИФІКАЦІЇ ТА СЕРТИФІКАЦІЇ

Анотація. Ця стаття описує підхід до ідентифікації та сертифікації у децентралізованому середовищі. Протокол визначає шлях інтеграції блокчейн-технології та концепції web-of-trust для створення децентралізованої інфраструктури відкритих ключів зі зручним керуванням ідентифікаторами користувачів. Сутність схеми полягає у розмежуванні усієї інфраструктури на 2 рівня: рівень центрів сертифікації (постачальників послуг), які сумісно ведуть історію подій, що пов'язані з сертифікатами користувачів; та рівень кінцевих користувачів, систем та додатків. При створенні, оновленні та відкликанні сертифікатів, учасники вищого рівня досягають консенсусу відносно підтвердження пов'язаних з цим транзакцій, що забезпечує більш високий рівень валідності сертифікатів та синхронізацію їх стану між центрами сертифікації. У свою чергу учасникам нижчого рівня не потрібно виконувати складні процедури верифікації окремого сертифікату: на відміну від класичної X.509 архітектури та web-of-trust підходу, максимальна кількість перевірок у ланцюжці може дорівнювати - двом. Важливою особливістю в такій системі є її здатність до відмови центрів сертифікації: у випадку відмови та/чи компрометації ключів одного центру сертифікації, інші учасники мережі продовжують безперебійно працювати з іншими, а технологія блокчейн може забезпечити неможливість додавання сертифікату центром, ключі якого були

ISSN 2663 - 4023

скомпрометовані, так як всі події в системі зв'язані за допомогою криптографічних методів. Зокрема, така система може використовуватися у Інтерні Речей (Internet of Things). Кожен індивідуальний сенсор повинен правильно комунікувати з іншими компонентами системи в цілому. Для надання безпечної взаємодії цих компонентів, вони повинні обмінюватися зашифрованими повідомленнями з можливістю перевірки їх цілісності та автентичності, схема надання котрих знаходиться в описаній схемі.

Ключові слова: технологія блокчейн; інфраструктура відкритих ключів; цілісність; автентичність; децентралізована система; ідентифікація; сертифікація.

1. ВСТУП

Традиційна схема інфраструктури відкритих ключів полягає у використанні централізованих сервісів, що виконують обслуговування клієнтів та випуску їх сертифікатів відкритих ключів [1-10]. З іншої сторони схема web-of-trust полягає у індивідуальному підписі сертифікатів користувачів іншими користувачами [11-16]. Отже існують такі основні підходи для побудування інфраструктури: використовуючи стандарт X.509 [17] та повністю децентралізований підхід, що спирається на web-of-trust [18].

Перший підхід широко застосовується у існуючих системах, тому що він є дуже ефективним з точки зору продуктивності такої системи [1-3]: процеси отримання, оновлення, відкликання сертифікатів не потребують великої кількості часу [19-24]. До того ж така модель може швидко реагувати на компрометацію ключів центрів сертифікації нижнього рівня [25-27].

Однак, така модель побудування інфраструктури відкритих ключів має декілька проблем:

- вразливість до централізованого цензурування [28, 29];
- центри сертифікації віщого рівня потребують повної довіри користувачів [1, 2];
- необхідність перевірки ланцюжка сертифікатів до корневого центра сертифікації [28];
- проблеми, що пов’язані з синхронізацією OCSP (Online Certificate Status Protocol) серверів [19];
- кореневий центр сертифікації є точкою відмови системи (проблеми з компрометацією ключів кореневого центру сертифікації) [20].

Інфраструктура відкритих ключів, що базується на web-of-trust є повністю децентралізованою моделлю, тому що кожен з учасників системи виконує як сертифікацію інших учасників, так і валідацію їхніх сертифікатів [11-14]. Таких підхід дозволяє вирішити проблеми ієрархічної моделі. Однак це менш гнучкий підхід, так як кожна дія в мережі, що пов’язана з функціонуванням сертифікату (оновлення, відгук) повинна бути провалідована вузлами, що зберігають даний сертифікат [14-16]. Одним додатковим обмеженням є складність побудування ланцюжка сертифікатів з високим рівнем довіри.

У цій роботі ми опишемо принципи побудови децентралізованої інфраструктури ідентифікації та сертифікації, що пропонує використання технології блокчейн у

ISSN 2663 - 4023

сукупності з гібридною моделлю: дворівневою ієрархічною структурою. Її верхній рівень складається з місцевих органів сертифікації, які організовані в мережу довіри і досягають консенсусу щодо стану реєстру; нижній рівень — це кінцеві користувачі. Органи сертифікації виконують роль посередництва між серверами та кінцевими користувачами та гарантують справжність останніх.

2. КОМПОНЕНТИ ДЕЦЕНТРАЛІЗОВАНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ТА СЕРТИФІКАЦІЇ

Децентралізована система ідентифікації та сертифікації складається з наступних компонентів:

- CA - центр сертифікації (Certificate authority);
- RA - центр реєстрації (Registration authority);
- Сховища персональних даних (ПД);
- Сховище сертифікатів;
- Кінцеві користувачі, системи та додатки.

Схематично, розташування компонентів та їх зв’язки можно зобразити на рис. 1.

Центри сертифікації є одними з головних компонентів інфраструктури відкритих ключів. CA випускають сертифікати відкритих ключів для підтвердження прав користувачів, систем та додатків, які потребують цього. У процесі створення сертифікату CA підписує його власним ключем для підтвердження його автентичності [30-35]. Відкритий ключ кожного CA є загальнодоступним для всіх функціонуючих суб’єктів.

Центри сертифікації також виконують роль валідаторів платформи, тобто вони перевіряють транзакції и досягають згоди щодо актуального стану реєстру. Реєстр організований у вигляді ланцюжка блоків. Це гарантує цілісність усієї історії транзакцій (випуску, оновлення, відклику сертифікатів). Для цього пропонується використовувати Федеративну Візантійську Угоду (Federated Byzantine Agreement) в якості алгоритму досягнення консенсусу [36].

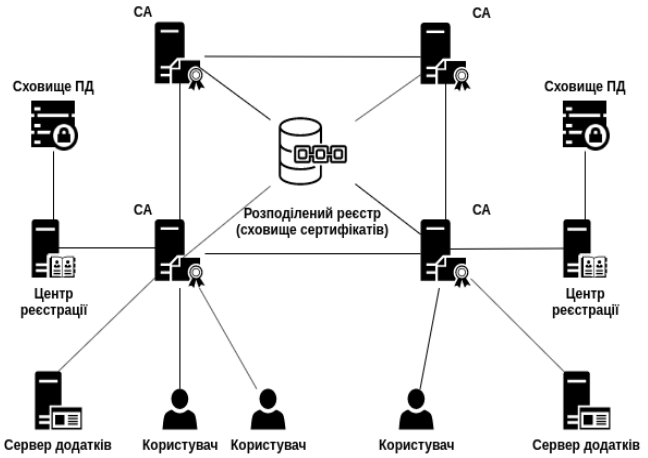

Рис. 1. Компоненти інфраструктури відкритих ключів

RA виконують початкову ідентифікацію та реєстрацію користувачів. Для отримання сертифікату користувачу необхідно звернутися безпосередньо до RA. RA обробляє запит користувача та надані разом з ним дані. Після обробки RA передає дані до CA. При цьому варто зазначити, що RA обробляє різні дані, до яких входять і персональні. Оскільки персональні дані користувачів не можуть бути передані третім сторонам (та оброблятися ними) без згоди користувача на це, потрібно забезпечити їхню конфіденційність. Протягом передачі запиту від RA до CA, передаються тільки відкриті дані та геш-значення усього набору даних, що були надані. Ці значення повинні бути додані до сертифікату відкритого ключа так як і користувач (той, хто передав запит) і інша сторона повинні мати можливість перевірки цілісності збережених даних (що RA обробив їх правильно та не модифікував). Відзначимо, що RA повністю відповідає за збереження конфіденційності при обробці та зберіганні персональних даних користувачів, тому він має бути оснащений комплексною системою захисту інформації та дотримуватися політики безпеки відносно зберігання, обробки та резервування даних.

Сховища персональних даних зберігають усі дані, які користувачі надали RA. Дані користувачів зашифровуються за допомогою секретного ключа RA і тільки він може отримати прямий доступ до них. Усі ці дані повинні зберігатися впродовж усього життєвого циклу сертифікату користувача. Якщо користувач змінює ці дані, RA також повинен оновити запис у сховищі даних (і відправити оновлене геш-значення до CA). Стороння організація може відправити запит до RA для отримання даних конкретного користувача (наприклад перевірити що дані відповідають занесеному до сертифікату геш-значенню). У цьому випадку, сторона, що звертається повинна отримати дозвіл користувача на доступ та обробку його персональних даних (дозвіл повинен містити які дані можуть бути передані, відкритий ключ сторони, що звертається для шифрування цих даних, а також цифровий підпис самого користувача).

Як ми зазначали раніше, сховище сертифікатів є розподіленим реєстром, якій зберігають CA. Сертифікати організовані у вигляді впорядкованого ланцюжку блоків, кожен з яких містить посилання на попередній. Блоки містять транзакції, кожна з яких, у свою чергу, містить операції, що пов’язані з конкретним сертифікатом. Кожна дія (випуск, оновлення, відклик) повинна бути ініційована за допомогою відповідної транзакції. Кінцеві користувачі, системи та додатки також можуть мати локальну копію бази даних. Це підвищує рівень прозорості дій валідаторів платформи та незворотність історії транзакцій.

3. ПРИНЦИПИ ФУНКЦІОНУВАННЯ СИСТЕМИ

По-перше, центри сертифікації повинні обмінятися відкритими ключами один з одним. Кожен з них формує сертифікати відкритих ключів усіх інших. Також, кожен з центрів сертифікації визначає рівень довіри по відношенню до іншого центру сертифікації. Якщо рівень довіри максимальний, то CA повністю довіряє іншому CA проводити сертифікацію кінцевих користувачів, систем та додатків [37].

ISSN 2663 - 4023

Після того, як такі сертифікати сформовані, кожен СА генерує транзакцію, яка містить набір операцій випуску сертифікатів з відповідними деталями. Усі ці транзакції об'єднуються до одного блоку, який має назву "genesis block". Уся подальша історія сертифікатів базуватиметься на цьому блоці.

Кількість транзакцій у генезіс блоці дорівнює початковій кількості валідаторів (СА). Кількість випущених сертифікатів у цьому блоці дорівнює $n(n-1)$, де n — початкова кількість СА.

Варто зазначити, що початковий стан довіри між органами сертифікації може бути неоднорідним. Залежно від рівня довіри одного СА до іншого, сертифікати кінцевих користувачів можуть мати різний рівень довіри для інших СА, користувачів, систем та додатків.

СА можу бути доданий вже після ініціалізації системи ідентифікації та сертифікації. Для цього, новий центр сертифікації повинен отримати згоду інших СА на це та повідомити їм значення свого відкритого ключа. Відзначимо, що кожен СА незалежно приймає рішення щодо довіри новому центру сертифікації.

Для отримання права сертифікації користувачів, систем та додатків, СА повинен отримати сертифікати свого відкритого ключа від кожного іншого активного СА. На протязі випуску сертифікату, кожен центр сертифікації визначає рівень довіри до нового центру сертифікації. Якщо рівень довіри максимальний (100), то всі користувачі, які отримали сертифікат від СА будуть гарантовано довіряти сертифікатам, що були випущені новим центром сертифікації. Якщо ж рівень довіри до нового СА буде нульовий, то сертифікати від цього СА будуть вважатись недійсними користувачами центра сертифікації, який видав відповідний сертифікат.

У цьому випадку рівень довіри сертифікату, що був випущений іншим СА буде дорівнювати:

$$Validity\ level = STLCAproxy(cert.\ CAforeign)\ SVLCAforeign(cert.\ object),$$

де $STLCAproxy(cert.\ CAforeign)$ — рівень довіри СА по відношенню до іншого СА; $SVLCAforeign(cert.\ object)$ — рівень валідності кінцевої сторони по відношенню до іншого СА.

Варто також зазначити, що рівень довіри між центрами сертифікації може змінюватися під час роботи системи. Кожна зміна рівня довіри сертифіката повинна бути ініційована відповідною транзакцією. Зауважимо, що кожен користувач самостійно визначає необхідний поріг довіри, якому сертифікат повинен відповідати, щоб використовуватись для взаємодії.

Після формування генезисного блоку, кінцеві користувачі, системи та програми отримують сертифікати від СА. Щоб отримати сертифікат відкритого ключа, суб'єкт звертається до RA для завершення початкової ідентифікації та реєстрації. RA вимагає від суб'єкта необхідні дані, обробляє їх і зберігає у захищеному сховищі. Після цього RA надає СА геш-значення отриманих даних, публічні дані суб'єкта (які вбудовані в

ISSN 2663 - 4023

сертифікат) та відкритий ключ суб'єкта ідентифікації. CA отримує ці дані та формує сертифікат відкритого ключа. Процес отримання сертифікатів показаний на рис. 2.

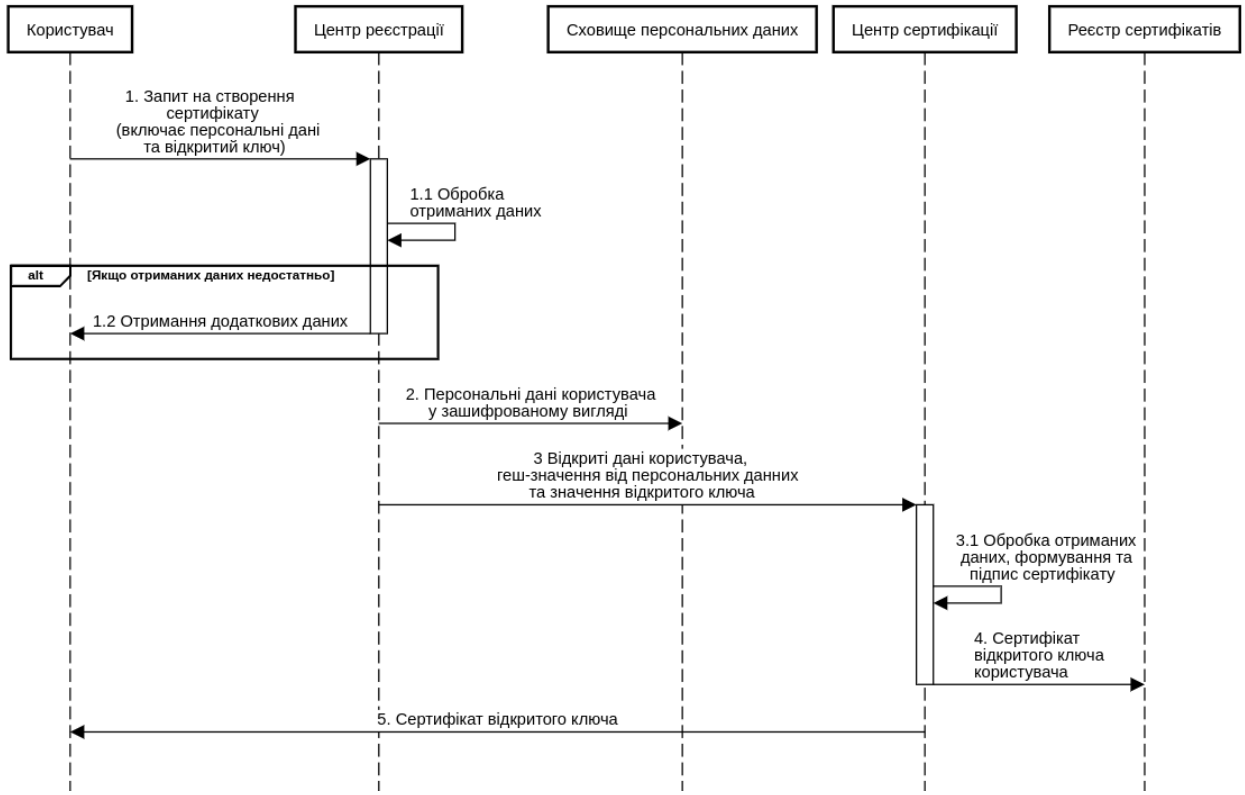

Рис. 2. Процес отримання сертифікату відкритого ключа

Користувач надсилає свої особисті дані та згенерований відкритий ключ до RA. Усі дані передаються у зашифрованому вигляді (направлене шифрування на RA). RA обробляє запит (ідентифікує користувача). Оскільки мета отримання ключа вказана в запиті, для ідентифікації можуть знадобитися різні набори необхідних даних. Якщо наданих даних недостатньо, RA вимагає додаткових даних. Якщо користувач надає дані, процес продовжує, якщо ні, в запиті буде відхилено.

Після цього, RA шифрує особисті дані користувача та зберігає їх у захищеному сховищі. Лише RA може отримати прямий доступ до особистої інформації. Якщо третя сторона хоче отримати доступ до персональних даних, їй потрібно отримати дозвіл користувача. RA передає набір даних в CA, що включає: публічні дані користувача, які повинні бути включені в сертифікат, відкритий ключ користувача та його особисті дані. Варто зазначити, що всі дані передаються в зашифрованому вигляді (спрямовані на відкритий ключ CA) і підписуються RA.

Після цього CA обробляє дані, отримані від RA, і використовує їх для формування сертифіката відкритого ключа користувача. CA формує транзакцію, яка містить операцію створення сертифіката та розподіляє її серед інших CA. Вузли перевіряють транзакцію та досягають консенсусу щодо оновлення сховища сертифікатів. Коли транзакція додається до сховища, CA передає користувачеві його сертифікат відкритого

ISSN 2663 - 4023

ключа. З цього часу користувач може застосовувати свою пару ключів для взаємодії з іншими користувачами, системами та додатками.

4. ПРОЦЕС ВЕРИФІКАЦІЇ СЕРТИФІКАТУ

Суб'єкт верифікації повинен встановити зв'язок між відкритим ключем та об’єктом сертифікату. Це робиться шляхом перевірки того, що отриманий сертифікат виданий уповноваженим органом з достатньою довірою. Перевірка сертифікату може проводитися двома способами, залежно від того, хто видав сертифікат відкритого ключа.

Одиночна перевірка проводиться лише в тому випадку, якщо верифікатор повністю довіряє центру сертифікації, який видав цей сертифікат для підтвердження. У цьому випадку для перевірки відкритого ключа верифікатор звертається до сховища сертифікатів (яке доступне для всіх) та отримує відповідний сертифікат. Після цього він перевіряє всі поля сертифіката: час дійсності, рівень дійсності, що повинен бути більше 0 (це означає, що сертифікат не відкликаний) тощо. Після цього він перевіряє, чи був цей сертифікат підписаний повністю довіреним CA (наприклад, якщо верифікатор є клієнтом саме цього CA).

Якщо сертифікат перевірки був підписаний CA, якому верифікатор не довіряє (безпосередньо), то він перевіряє ланцюжок сертифікатів. На відміну від мережі довіри та стандарту X.509, максимальна кількість сертифікатів у ланцюжку, що перевіряються при такому підході, дорівнює 2. Щоб перевірити сертифікат, верифікатор звертається до сховища сертифікатів і отримує два сертифікати: сторони, що проходить верифікацію (сертифікат, який підписується іншим CA) та сертифікат цього CA (який підписаний CA, якому верифікатор довіряє). Якщо обидва сертифікати є дійсними і рівень довіри достатньо високий, верифікатор вважає сертифікат дійсним.

Важливо також врахувати, як поводиться мережа, коли ключ одного з CA скомпроментовано. У разі відклику сертифіката стандарт X.509, надається можливість його повторного випуску вищим рівнем CA. При цьому учасники нижчого рівня протягом певного періоду часу втрачають здатність повноцінно функціонувати (в контексті компрометації ключів кореневого центру сертифікації це стає серйозною проблемою). У разі ж використання web-of-trust відклик сертифікату будь-якого користувача не впливає на функціонування інших користувачів. Однак це повільний і складний процес (по-перше, велика кількість вузлів має бути переконана, що саме власник сертифіката хоче його відкликати і що це не зловмисник, який намагається обмежити можливості користувача). У запропонованому підході відклик сертифікату одного з CA не вплине на функціонування інших користувачів (лише обмежить можливість оновлення сертифікатів підпорядкованих користувачів). При цьому можна достатньо швидко відновити сертифікат, але для повного його прийняття, потрібно звернутися до всіх інших валідаторів платформи.

ISSN 2663 - 4023

5. ВИСНОВКИ

Система ідентифікації та сертифікації на основі технології блокчейн може бути єдиним джерелом інформації щодо сертифікатів користувачів, систем та додатків, оскільки вся історія операцій із сертифікатами зберігатиметься та обробляється різними незалежними сторонами (упорядковано у часі).

Архітектура, описана в цьому документі, дозволяє будь-якому кінцевому користувачеві або додатку зберігати повну базу даних сертифікатів відкритого ключа (та їхні поточні статуси) з надійною синхронізацією та можливістю перевіряти дії всіх органів сертифікації відповідно до правил протоколу.

Описана схема дозволяє кожному члену системи самостійно визначати рівень довіри до всіх інших учасників системи. Таким чином, рівень об'єктивності та прозорості процесів ідентифікації та сертифікації підвищується, оскільки кожен член перевіряє дії інших та самостійно приймає рішення щодо довіри окремому суб'єкту.

Використання такої системи дозволяє організувати інфраструктуру між користувачами та окремими серверами додатків. Основна особливість такої структури — використання єдиного ідентифікатора (відкритого ключа) для отримання послуг з усіх серверів додатків у децентралізованій системі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] S. F. Mjølsnes, S. Mauw, and S. K. Katsikas, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2008.
[2] A. Maeda, “PKI Solutions for Trusted E-Commerce: Survey of the De Facto Standard Competition in PKI Industries,” Information Technology Policy and the Digital Divide.
[3] D. Chadwick and G. Zhao, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2005.
[4] V. Dolgov and I. Ishchenko, "Proposals of using chameleon-signature in Ukrainian prototype of combined PKI," 2010 International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Lviv-Slavske, 2010, pp. 303-303.
[5] J. Lopez, P. Samarati, and J. L. Ferrer, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2007.
[6] J. Davies, “Implementing SSL/TLS Using Cryptography and PKI,” Dec. 2010.
[7] A. S. Atzeni and A. Lioy, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2006.
[8] Krasnobayev V. A. Method for realization of transformations in public-key cryptography. Telecommunications and Radio Engineering. - Volume 66, 2007 Issue 17, pp. 1559-1572.
[9] A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov, "Code-based public-key cryptosystems for the post-quantum period," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 125-130. DOI: 10.1109/INFOCOMMST.2017.8246365.
[10] W. T. Polk and K. Seamons, “6th annual PKI R&D workshop ‘Applications-Driven PKI’ proceedings,” September 2007.
[11] B. Schneier, “Applied Cryptography, Second Edition,” John Wiley & Sons, Inc. Oct. 2015.
[12] N. Ferguson, B. Schneier, and T. Kohno, “Cryptography Engineering,” Oct. 2015.
[13] G. Guo, J. Zhang, and J. Vassileva, “Improving PGP Web of Trust through the Expansion of Trusted Neighborhood,” 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, Aug. 2011.

[14] D. Wueppelmann, “PGP Auth: Using Public Key Encryption for Authentication on the Web.” A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of master of computer science. Ottawa, Ontario September, 2015.

[15] K. Portz, J. M. Strong, and L. Sundby, “To Trust Or Not To Trust: The Impact Of WebTrust On The Perceived Trustworthiness Of A Web Site,” Review of Business Information Systems (RBIS), vol. 5, no. 3, p. 35, Jul. 2011.

[16] M. Zhu and Z. Jin, “Trust Analysis of Web Services Based on a Trust Ontology,” Lecture Notes in Computer Science, pp. 642–648.

[17] RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile. [online] Available at: https://tools.ietf.org/html/rfc5280.

[18] J. Callas, "OpenPGP Message Format", IETF RFC 4880, Nov. 2007, [online] Available: www.ietf.org/rfc/rfc4880.txt.

[19] RFC 4158: Internet X.509 Public Key Infrastructure - Certification Path Building. [online] Available at: https://tools.ietf.org/html/rfc4158.

[20] RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. [online] Available at: https://tools.ietf.org/html/rfc6960.

[21] K. Isirova and O. Potii, "Decentralized public key infrastructure development principles," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kiev, 2018, pp. 305-310.

[22] A. A. Kuznetsov, Yu. I. Gorbenko, D. I. Prokopovych-Tkachenko, M. S. Lutsenko, M. V. Pastukhov. “NIST PQC: Code-Based Cryptosystems.” Telecommunications and Radio Engineering, Volume 78, 2019, Issue 5, pp. 429-441. DOI: 10.1615/TelecomRadEng.v78.i5.50.

[23] Yu.V.Stasev, A.A.Kuznetsov, “Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes.” Cybernetics and Systems Analysis, vol. 41, Issue 3, pp. 354-363, May 2005. DOI: 10.1007/s10559-005-0069-9.

[24] B. Rajendran, "Evolution of PKI ecosystem," 2017 International Conference on Public Key Infrastructure and its Applications (PKIA), Bangalore, 2017, pp. 9-10.

[25] I. Gorbenko, M. Yesina and V. Ponomar, "Anonymous electronic signature method," 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 47-50.

[26] H. Nanang, A. F. Misman and Z. Zulkifli, "Trust, risk and public key infrastructure model on e-procurement adoption," 2017 5th International Conference on Cyber and IT Service Management (CITSM), Denpasar, 2017, pp. 1-6.

[27] A. Kuznetsov, A. Pushkar'ov, N. Kiyan and T. Kuznetsova, "Code- based electronic digital signature," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 331-336. DOI: 10.1109/DESSERT.2018.8409154.

[28] S. Farrell, "Not Reinventing PKI until We Have Something Better," in IEEE Internet Computing, vol. 15, no. 5, pp. 95-98, Sept.-Oct. 2011.

[29] I. M. Rodiana, B. Rahardjo and W. Aciek Ida, "Design of a Public Key Infrastructure-based Single Ballot E-Voting System," 2018 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung - Padang, Indonesia, 2018, pp. 6-9.

[30] O. Potii, Y. Gorbenko and K. Isirova, "Post quantum hash based digital signatures comparative analysis. Features of their implementation and using in public key infrastructure," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 105-109.

[31] A. Kuznetsov, M. Lutsenko, N. Kiian, T. Makushenko and T. Kuznetsova, "Code-based key encapsulation mechanisms for post- quantum standardization," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 276-281. DOI: 10.1109/DESSERT.2018.8409144.

[32] Yu.V. Stasev, A.A. Kuznetsov. “Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes”. Kibernetika i Sistemnyi Analiz, No. 3, pp. 47-57, May-June 2005.

[33] P. Landrock, "PKI, past, present and future," 2005 The IEE Seminar on Quantum Cryptography: Secure Communications for Business (Ref. No. 2005/11310), London, 2005, pp. 0_12-2/17.

[34] A. Kuznetsov, A. Kiian, M. Lutsenko, I. Chepurko and S. Kavun, "Code based cryptosystems from NIST PQC," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 282-287. DOI: 10.1109/DESSERT.2018.8409145.

[35] M. Pala, S. Cholia, S. A. Rea and S. W. Smith, "Extending PKI Interoperability in Computational Grids," 2008 Eighth IEEE International Symposium on Cluster Computing and the Grid (CCGRID), Lyon, 2008, pp. 645-650.

[36] David Mazieres. "The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus". [online] Available: https://www.stellar.org/papers/stellar-consensus-protocol.pdf.

[37] X.1254: Entity authentication assurance framework - ITU. [online] Available: https://www.itu.int/rec/T-REC-X.1254.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (6), 2019
ISSN 2663 - 4023

Oleksandr S. Kurbatov
Kharkiv National University of Radioelectronics, Department of Information System Security, Kharkiv, Ukraine
ORCID ID: 0000-0002-8237-4377
olkurbatov@gmail.com

Pavlo O. Kravchenko
Doctor of Philosophy
Distributed Lab, Kharkiv, Ukraine
ORCID ID: 0000-0002-0456-3295
pavel@distributedlab.com

Nikolay A. Poluyanenko
Candidate of Engineering Sciences
Associate Professor at the Department of Information Systems and Technologies Security
V.N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID ID: 0000-0001-9386-2547
nlfsr01@gmail.com

Oleksiy V. Shapoval
V.N. Karazin Kharkiv National University, Department of Information Systems and Technologies Security, Kharkiv, Ukraine
ORCID ID: 0000-0003-4478-3193
alex.shapoval@protonmail.com

Tetiana Kuznetsova
Researcher at the research part of V. N. Karazin Kharkiv National University, Kharkiv, Ukraine
ORCID ID: 0000-0001-6154-7139
kuznetsova.tatiana17@gmail.com

DECENTRALIZED IDENTITY AND CERTIFICATION SYSTEM

Abstract. This article describes an approach to identification and certification in a decentralized environment. The protocol defines the way to integrate blockchain technology and web-of-trust concepts to create a decentralized public key infrastructure with easy user ID management. The essence of the scheme is to differentiate the entire infrastructure into 2 levels: the level of certification authorities (service providers) that jointly keep track of events related to user certificates; and the level of end users, systems and applications. During creating, updating, and revoking certificates, higher-level members reach a consensus on the confirmation of transactions associated with them, which ensures a higher level of validity of the certificates and synchronization of their status between certification centers. In turn, lower-level members do not need to perform complex verification procedures for a corresponding certificate: unlike the classic X.509 architecture and web-of-trust approach, the maximum number of checks in a chain can be two. An important feature of such a system is its ability to refuse certification centers: in the case of failure and / or compromise of the keys of one certification center, other network members continue to work seamlessly with others, and blockchain technology may make it impossible to add a certificate to a center whose keys have been compromised, because all the events in the system are connected by cryptographic methods. In particular, such a system can be used on the Internet of Things. Each individual sensor must communicate properly with other components of the system as a whole. In order to enable the secure interaction of these components, they must exchange encrypted messages to verify their integrity and authenticity, the provisioning scheme of which is in the described scheme.

Keywords: blockchain technology; public key infrastructure; integrity; authenticity; decentralized system; identification; certification.

ISSN 2663 - 4023

REFERENCES

[1] S. F. Mjølsnes, S. Mauw, and S. K. Katsikas, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2008.
[2] A. Maeda, “PKI Solutions for Trusted E-Commerce: Survey of the De Facto Standard Competition in PKI Industries,” Information Technology Policy and the Digital Divide.
[3] D. Chadwick and G. Zhao, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2005.
[4] V. Dolgov and I. Ishchenko, "Proposals of using chameleon-signature in Ukrainian prototype of combined PKI," 2010 International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Lviv-Slavske, 2010, pp. 303-303.
[5] J. Lopez, P. Samarati, and J. L. Ferrer, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2007.
[6] J. Davies, “Implementing SSL/TLS Using Cryptography and PKI,” Dec. 2010.
[7] A. S. Atzeni and A. Lioy, Eds., “Public Key Infrastructure,” Lecture Notes in Computer Science, 2006.
[8] Krasnobayev V. A. Method for realization of transformations in public-key cryptography. Telecommunications and Radio Engineering. - Volume 66, 2007 Issue 17, pp. 1559-1572.
[9] A. Kuznetsov, I. Svatovskij, N. Kiyan and A. Pushkar'ov, "Code-based public-key cryptosystems for the post-quantum period," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 125-130. DOI: 10.1109/INFOCOMMST.2017.8246365.
[10] W. T. Polk and K. Seamons, “6th annual PKI R&D workshop ‘Applications-Driven PKI’ proceedings,” September 2007.
[11] B. Schneier, “Applied Cryptography, Second Edition,” John Wiley & Sons, Inc. Oct. 2015.
[12] N. Ferguson, B. Schneier, and T. Kohno, “Cryptography Engineering,” Oct. 2015.
[13] G. Guo, J. Zhang, and J. Vassileva, “Improving PGP Web of Trust through the Expansion of Trusted Neighborhood,” 2011 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology, Aug. 2011.
[14] D. Wueppelmann, “PGP Auth: Using Public Key Encryption for Authentication on the Web.” A thesis submitted to the Faculty of Graduate and Postdoctoral Affairs in partial fulfillment of the requirements for the degree of master of computer science. Ottawa, Ontario September, 2015.
[15] K. Portz, J. M. Strong, and L. Sundby, “To Trust Or Not To Trust: The Impact Of WebTrust On The Perceived Trustworthiness Of A Web Site,” Review of Business Information Systems (RBIS), vol. 5, no. 3, p. 35, Jul. 2011.
[16] M. Zhu and Z. Jin, “Trust Analysis of Web Services Based on a Trust Ontology,” Lecture Notes in Computer Science, pp. 642–648.
[17] RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile. [online] Available at: https://tools.ietf.org/html/rfc5280.
[18] J. Callas, "OpenPGP Message Format", IETF RFC 4880, Nov. 2007, [online] Available: www.ietf.org/rfc/rfc4880.txt.
[19] RFC 4158: Internet X.509 Public Key Infrastructure - Certification Path Building. [online] Available at: https://tools.ietf.org/html/rfc4158.
[20] RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. [online] Available at: https://tools.ietf.org/html/rfc6960.
[21] K. Isirova and O. Potii, "Decentralized public key infrastructure development principles," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kiev, 2018, pp. 305-310.
[22] A. A. Kuznetsov, Yu. I. Gorbenko, D. I. Prokopovych-Tkachenko, M. S. Lutsenko, M. V. Pastukhov. “NIST PQC: Code-Based Cryptosystems.” Telecommunications and Radio Engineering, Volume 78, 2019, Issue 5, pp. 429-441. DOI: 10.1615/TelecomRadEng.v78.i5.50.

[23] Yu.V.Stasev, A.A.Kuznetsov, “Asymmetric Code-Theoretical Schemes Constructed with the Use of Algebraic Geometric Codes.” Cybernetics and Systems Analysis, vol. 41, Issue 3, pp. 354-363, May 2005. DOI: 10.1007/s10559-005-0069-9.

[24] B. Rajendran, "Evolution of PKI ecosystem," 2017 International Conference on Public Key Infrastructure and its Applications (PKIA), Bangalore, 2017, pp. 9-10.

[25] I. Gorbenko, M. Yesina and V. Ponomar, "Anonymous electronic signature method," 2016 Third International Scientific-Practical Conference Problems of Infocommunications Science and Technology (PIC S&T), Kharkiv, 2016, pp. 47-50.

[26] H. Nanang, A. F. Misman and Z. Zulkifli, "Trust, risk and public key infrastructure model on e-procurement adoption," 2017 5th International Conference on Cyber and IT Service Management (CITSM), Denpasar, 2017, pp. 1-6.

[27] A. Kuznetsov, A. Pushkar'ov, N. Kiyan and T. Kuznetsova, "Code- based electronic digital signature," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 331-336. DOI: 10.1109/DESSERT.2018.8409154.

[28] S. Farrell, "Not Reinventing PKI until We Have Something Better," in IEEE Internet Computing, vol. 15, no. 5, pp. 95-98, Sept.-Oct. 2011.

[29] I. M. Rodiana, B. Rahardjo and W. Aciek Ida, "Design of a Public Key Infrastructure-based Single Ballot E-Voting System," 2018 International Conference on Information Technology Systems and Innovation (ICITSI), Bandung - Padang, Indonesia, 2018, pp. 6-9.

[30] O. Potii, Y. Gorbenko and K. Isirova, "Post quantum hash based digital signatures comparative analysis. Features of their implementation and using in public key infrastructure," 2017 4th International Scientific-Practical Conference Problems of Infocommunications. Science and Technology (PIC S&T), Kharkov, 2017, pp. 105-109.

[31] A. Kuznetsov, M. Lutsenko, N. Kiian, T. Makushenko and T. Kuznetsova, "Code-based key encapsulation mechanisms for post- quantum standardization," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 276-281. DOI: 10.1109/DESSERT.2018.8409144.

[32] Yu.V. Stasev, A.A. Kuznetsov. “Asymmetric code-theoretical schemes constructed with the use of algebraic geometric codes”. Kibernetika i Sistemnyi Analiz, No. 3, pp. 47-57, May-June 2005.

[33] P. Landrock, "PKI, past, present and future," 2005 The IEE Seminar on Quantum Cryptography: Secure Communications for Business (Ref. No. 2005/11310), London, 2005, pp. 0_12-2/17.

[34] A. Kuznetsov, A. Kiian, M. Lutsenko, I. Chepurko and S. Kavun, "Code based cryptosystems from NIST PQC," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), Kyiv, Ukraine, 2018, pp. 282-287. DOI: 10.1109/DESSERT.2018.8409145.

[35] M. Pala, S. Cholia, S. A. Rea and S. W. Smith, "Extending PKI Interoperability in Computational Grids," 2008 Eighth IEEE International Symposium on Cluster Computing and the Grid (CCGRID), Lyon, 2008, pp. 645-650.

[36] David Mazieres. "The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus". [online] Available: https://www.stellar.org/papers/stellar-consensus-protocol.pdf.

[37] X.1254: Entity authentication assurance framework - ITU. [online] Available: https://www.itu.int/rec/T-REC-X.1254.