УДК 004.7.032.2:004.056.5

МОДЕЛЬ ФУНКЦІОНУВАННЯ ЦИФРОВОЇ ІДЕНТИЧНОСТІ ТА ЗАСОБИ ЇЇ ВТІЛЕННЯ

Гаража Р. Ю.
Науковий керівник – к.т.н. Мельникова О.А.
Харківський національний університет радіоелектроніки, каф. БІТ
м. Харків, Україна
тел. +38(099) 760-91-52

This work is devoted to the research of the digital identity model and the identification of means capable of ensuring its functioning in accordance with the specified requirements. The main requirements for the implementation of digital identity are its privacy and the flexibility of its expansion. Flexibility can be achieved through the use of a three-participant identity model. Such participants are the owner of the identity, the postulator of the statements about the owner, and the verifier. Privacy is achieved by using zero-knowledge proofs. The resulting system allows participants to edit, verify and submit digital identity instances for verification using the unified identity standard and protocols.

Зважаючи на загальносвітову тенденцію до цифровізації послуг, зокрема і таких, що надає держава (яскравим прикладом є український застосунок Дія та система електронного урядування Естонії), питання втілення цифрової ідентичності набуває значної актуальності. При цьому на перший план виходять проблеми забезпечення конфіденційності та цілісності даних, що становлять ідентичність, а також масштабованості ідентичності як можливості вільно її доповнювати.

Метою роботи є виявлення існуючих засобів, що здатні забезпечити функціонування цифрової ідентичності гнучким і конфіденційним чином.

Згідно визначення, ідентичність — це якості, характеристики та досвід певної персони. До них можуть відноситися вік, стать, зовнішність, етнічна приналежність, громадянство або підданство, набуті навички, права, освіта та інше.

Цифрова ідентичність — це дані, що застосовуються для позначення певного суб'єкту в інформаційній системі. Вони можуть відображати характеристики, що складають ідентичність суб'єкту поза інформаційною системою. В мережі до цих даних зазвичай відносяться [1] логін, пароль, історія активності і т. п.

Розглянемо модель функціонування ідентичності. Учасників, що приймають участь у функціонуванні ідентичності як такої, умовно можна поділити на трьох суб’єктів: суб’єкт, що володіє ідентичністю, суб’єкт, що перевіряє ідентичність та суб’єкт, що постулює щодо першого певні твердження, що складають його ідентичність. Умовно позначимо учасників як володіючого, перевіряючого та постулюючого. При цьому ролі володіючого та постулюючого можуть, в окремих випадках, співпадати.

Можна проілюструвати цю модель наступним прикладом: магазин, що продає квитки на концерт, є постулюючим; людина, що придбала квиток — володіючим; а охорона на вході в клуб є перевіряючим. Таким чином, ідентичність володіючого містить твердження, що він має право відвідати концерт.

Застосування такої моделі функціонування ідентичності та розподілення ролей учасників може мати користь для забезпечення гнучкості функціонування цифрової ідентичності. Так, держава, надаючи певним суб'єктам (як власним, так і недержавним) дозвіл розширювати та доповнювати цифрову ідентичність громадянина за рахунок постулювання тверджень щодо його особистості (таких, як володіння дипломом про вищу освіту, водійськими правами, правами на нерухоме майно, тощо), може реалізувати загальнонаціональний проект цифрової ідентичності, що забезпечить одночасно гнучкість і уніфікованість.

Іншим важливим елементом функціонування цифрової ідентичності є забезпечення її конфіденційності та цілісності. Це може бути досягнуто за рахунок застосування доказів із нульовими знаннями [2] (також відомих як докази із нульовим розголошенням), що дозволяють підтвердити певне твердження, не розкриваючи зайвої чутливої інформації. Так, застосовуючи їх, володіючий ідентичністю може довести певне твердження щодо себе перевіряючому, не розкриваючи при цьому зміст інших тверджень, що стосуються його ідентичності.

Досягти водночас масштабованості та конфіденційності можна за рахунок застосування доказів із нульовими знаннями на базі дерев Меркла. Окремі заґешовані твердження будуть складати листи дерева, а корінь (кінцевий ґеш) буде унікальним ідентифікатором окремої цифрової ідентичності. Щоб підтвердити, що певне твердження входить до дерева, достатньо публічно зберігати лише корінь дерева, підтверджуючи володіння ним засобами асиметричної криптографії, і надавати для перевірки невелику кількість елементів (логарифм від кількості вузлів дерева [3]).

Отже, цифрова ідентичність має перспективи розвитку у децентралізованій, уніфікованій, довіреній і водночас безпечній з точки зору криптології манері.

Список використаних джерел:

1. What is a Digital Identity ? — Definition from Techopedia. https://www.techopedia.com/definition/23915/digital-identity

2. What is a zero - knowledge proof and why is it useful ? https://www.expressvpn.com/blog/zero-knowledge-proofs-explained/

3. Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016). Introduction to Cryptography & Cryptocurrencies. In Bitcoin and Cryptocurrency Technologies (p. 35). Princeton University Press.