Автентифікація кінцевого користувача при наданні доступу до онлайнових інформаційних ресурсів

При наданні послуги доступу до інформаційних ресурсів постачальник послуг повинен

1) **ідентифікувати** акаунт кінцевого користувача, тобто з'ясувати, хто намагається отримати доступ до ресурсу,
2) **автентифікувати** кінцевого користувача, тобто перевірити, чи дійсно людина, яка намагається отримати доступ, є власником цього акаунта,
3) **авторизувати** доступ (чи відмовити в ньому), перевіривши, чи має право цей користувач на отримання послуги згідно з наявними угодами.

При доступі до онлайнових інформаційних ресурсів, що надаються за договорами цілим організаціям, постачальнику послуг не потрібна персоналізація кінцевого користувача – йому достатньо знати, що цей користувач належить до певної організації-клієнта, яка сплачує за послуги. Тому виконання пп. 1 та 2 перекладається зазвичай безпосередньо на організацію-клієнта, що звільнює постачальника послуг від необхідності утримувати базу даних кінцевих користувачів (для деяких постачальників мова може йти про бази з багатьма мільйонами записів) та управляти записами цієї бази (наприклад, додавати та вилучати з неї дані про студентів, які вступають або випускаються з університету).

Перевірка приналежності користувача до певної організації може проводитись у два основних способи:

1) **За IP-адресою.** Доступ надається будь-якому користувачу, що робить запит на послугу з певного діапазону IP-адрес, закріплених за організацією-клієнтом.
2) **Через Shibboleth**. Ідентифікація та автентифікація кінцевого користувача проводиться на сервері організації-клієнта за допомогою акаунта і пароля. Тільки після такої автентифікації запит перенаправляється до постачальника послуг. Ця технологія реалізується за допомогою програмного забезпечення Shibboleth (або аналогічного), встановленого на серверах організації-клієнта (який в даному контексті іменується постачальником посвідчень, Identity Provider, IdP) та постачальника послуг (Service Provider, SP).

Опис принципів такої взаємодії серверів постачальників посвідчень та постачальників послуг див. на сайті Федерації Посвідчення Електронних Акаунтів для Науки та Освіти ПЕАНО www.peano.uran.ua, що підтримується Асоціацією УРАН.

Перевага способу доступу за IP-адресою:

- простота реалізації. Технічно для цього потрібно лише виділення певного діапазону IP-адрес Інтернет провайдером, а організаційно – реєстрація ним цього діапазону в базі даних RIPE і закріплення за певною організацією-клієнтом.

Недоліки надання доступу за IP-адресою:

- неможливість доступу до сервісу для кінцевого користувача з іншого місця, крім свого робочого (наприклад, з дому або перебуваючи у відрядженні);
- неможливість застосовувати гнучкі умови для придбання ліцензій у постачальників послуг, класифікуючи своїх співробітників і надаючи різним категоріям різні права доступу (наприклад, у такий спосіб неможливо надати доступ до ресурсу викладачам університету і відмовити в доступі студентам);
- неможливість відслідковування статистики, хто з користувачів користувався якими інформаційними сервісами;
- необхідність переналаштування сервісу з боку постачальника послуг при зміні IP-адрес користувача (наприклад, в разі зміни інтернет-провайдера).

Переваги способу доступу через Shibboleth:

- повна підтримка такої технології з боку більшості сучасних постачальників онлайнових послуг;
- можливість доступу до сервісу з будь-якого місця;
- можливість збирання персональної статистики в організації-клієнті, хто зі співробітників або студентів користувався якими інформаційними сервісами;
- можливість надавати різним категоріям користувачів доступ до різних ресурсів;

Недоліки способу доступу через Shibboleth:

- потреба в кваліфікованому персоналі для підтримки програмного забезпечення IdP Shibboleth, або,
- розгортання Shibboleth в сторонньому датацентрі, що потребуватиме додаткових витрат на користь оператора датацентру на хостинг та технічну підтримку віртуального комп'ютера та системи IdP Shibboleth.

Асоціація УРАН, маючи досвід у впровадженні технології Shibboleth, протягом 2016-2018 організовуватиме низку навчальних семінарів для системних адміністраторів університетів стосовно розгортання програмного забезпечення IdP Shibboleth на їх серверах.

Інша альтернатива – виділити клієнту віртуальний комп'ютер з хостингом на технічному майданчику УРАН з уже згенерованою системою IdP Shibboleth для управління базою даних кінцевих користувачів певної стандартизованої конфігурації. Наповнення та актуалізація такої бази даних здійснюється віддалено відповідним менеджером організації-клієнта.

В будь-якому випадку, Асоціація УРАН проведе також для менеджерів баз даних кінцевих користувачів навчальні семінари стосовно правил управління цими базами.

Таку послугу надає ДП «Мережевий оператор УРАН». Її орієнтовна вартість складає 2100 грн./міс. (включно з ПДВ), проте, якщо організація-клієнт має договір з ДП «Мережевий оператор УРАН» про надання телекомунікаційних послуг, то його щомісячна абонплата становитиме лише різницю між 2100 грн. та абонплатою за телекомунікаційні послуги. Якщо ж вартість телекомунікаційних послуг перевищує 2100 грн./міс, то послуги з хостингу та технічної підтримки віртуального комп'ютера та системи IdP Shibboleth надаватимуться безкоштовно.