yubico

ключ до хмари

Інструкція з розробки модуля автентифікації YubiKey

Примітка до програми Yubico

Версія 1.0

7 травня 2012 року

Вступ

Yubico є провідним постачальником простого, відкритого онлайн-захисту особистих даних. Флагманський продукт компанії, YubiKey®, унікально поєднує бездрайверне USB-апаратне забезпечення з відкритим кодом. Понад мільйон користувачів у 100 країнах покладаються на сильну двофакторну автентифікацію YubiKey для захисту доступу до комп'ютерів, мобільних пристроїв, мереж та онлайн-сервісів. Клієнти варіюються від окремих користувачів інтернету до електронних урядів і компаній зі списку Fortune 500. Заснована у 2007 році, Yubico є приватною компанією з офісами в Каліфорнії, Швеції та Великобританії.

Застереження

Зміст цього документа може бути змінено без попередження через постійний прогрес у методології, дизайні та виробництві. Yubico не несе відповідальності за будь-які помилки чи збитки будь-якого роду в результаті використання цього документа.

Програмне забезпечення Yubico, згадане в цьому документі, надається вам згідно з положеннями та умовами, що супроводжують програмне забезпечення, або за іншою домовленістю між Yubico і вами чи компанією, яку ви представляєте.

Торгові марки

Yubico та YubiKey є торговельними марками Yubico Inc.

Контактна інформація

Yubico Inc
228 Гамільтон авеню, 3-й поверх
Пало-Альто, Каліфорнія 94301
США
info@yubico.com

ТОВ "Зе Кернел" — Офіційний дистриб'ютор YubiKey в Україні

Відділ продажів – sales@yubikey.com.ua
Технічна підтримка – support@yubikey.com.ua

Адреса:
01001, м. Київ, вул. Михайла Грушевського 10, офіс №212

Адміністрація компанії
Телефон: +38 (044) 35 81 888

Зміст

1. Інформація про документ

1.1 Призначення

Модулі автентифікації YubiKey розроблені для додавання потужних двофакторних можливостей автентифікації на базі YubiKey до програм на стороні сервера.

Зростаюча популярність і впровадження YubiKey призвели до появи ряду партнерських корпоративних рішень і проєктів з відкритим вихідним кодом, які пропонують модулі YubiKey на стороні сервера, щоб задовольнити потребу в надійній автентифікації.

Однак компанія Yubico та її клієнти помітили велику різницю в можливостях розгортання, керування, автентифікації та відновлення, які пропонують ці модулі. Тому, ґрунтуючись на відгуках клієнтів і досвіді Yubico, ми пропонуємо розробникам модулів дотримуватися набору загальних вказівок щодо дизайну своїх модулів, які допоможуть покращити взаємодію з клієнтами.

У цьому документі містяться загальні вказівки щодо розробки модуля автентифікації YubiKey, щоб він безперебійно працював у більшості випадків використання, з якими ми стикалися. Він охоплює можливості, які ми рекомендуємо підтримувати, і міркування, які слід враховувати при проєктуванні та розробці комплексного та налаштовуваного модуля автентифікації YubiKey для програм на стороні сервера. У документі також містяться рекомендації щодо впровадження, адміністрування та підтримки модуля.

У документі не розглядаються жодні деталі конкретної платформи чи мови програмування.

1.2 Аудиторія

Цей документ призначений для розробників додатків і модулів, зацікавлених у розробці модуля автентифікації YubiKey для забезпечення надійної двофакторної автентифікації за допомогою YubiKey.

1.3 Супутня документація

- Посібник YubiKey – Використання, налаштування та ознайомлення з основними поняттями
- Початок роботи з клієнтами
- Протокол перевірки OTP YubiKey версії 2.0

1.4 Визначення

Термін	Визначення
Пристрій YubiKey або YubiKey	Пристрій автентифікації Yubico для підключення до порту USB
USB	Універсальна послідовна шина
OTP	Одноразовий пароль
YubiCloud	Онлайн-сервіс перевірки OTP Yubico

2. Вступ і передумови

YubiKey — це унікальний USB-ключ для безпечного, легкого та доступного входу в мережі та сервіси. Завдяки своїй здатності емулювати клавіатуру USB, він працює з будь-якого комп'ютера для будь-якої кількості програм із правами лише на рівні користувача та без необхідності клієнтського програмного забезпечення.

Розроблений для будь-якої програми, де ім'я користувача/пароль уже недостатньо безпечний, загалом його набагато легше використовувати та розгортати/інтегрувати, ніж традиційні токени або смарт-картки на основі відображення.

YubiKey пропонується з безплатним сервером валідації та клієнтськими компонентами з відкритим вихідним кодом, безплатною службою автентифікації/валідації, яка відповідає вимогам сучасних розробників, підприємств, електронних послуг і споживачів, що швидко змінюються. Yubico також підтримує відкриті стандарти ідентифікації (SAML, OpenID тощо). Безплатна хмарна служба валідації дозволяє використовувати один ключ YubiKey для кількох програм. Це призвело до зростання кількості партнерських корпоративних рішень і проектів з відкритим вихідним кодом, які пропонують потужні можливості автентифікації на базі сервера YubiKey для багатьох стандартних фреймворків додатків і служб.

Кілька відкритих модулів автентифікації YubiKey були розроблені для різних програм і фреймворків з відкритим кодом як Yubico, так і спільнотою відкритих програм.

Деякі приклади програм і фреймворків, для яких були розроблені модулі автентифікації YubiKey, включають Crasman, Drupal, Joomla, MediaWiki, phpBB, osCommerce, WordPress тощо. Щоб отримати докладний список, відвідайте http://wiki.yubico.com.

Однак клієнти Yubico помітили велику різницю в тому, як модулі реалізують підтримку розгортання, керування, автентифікації та можливостей відновлення. Тому, щоб допомогти розробникам модулів легше створювати всеосяжну функціональність і гнучкий, але потужний контроль керування в модулі автентифікації, ми склали ці рекомендації та найкращі практики, які також покращать взаємодію з клієнтами.

Базуючись на досвіді Yubico та відгуках наших клієнтів, у цьому документі обговорюються різні міркування, які необхідно врахувати, і надаються вказівки щодо найкращих практик для розробників додатків і модулів, щоб забезпечити комплексну функціональність і потужне, але просте у використанні розгортання + керування, яке є досить гнучким, щоб відповідати різним потребам розгортання в реальному житті для надійного двофакторного рішення автентифікації за допомогою YubiKey.

Документ передбачає, що читач знайомий з наступним:

- Технологія Yubico OTP (генерація та валідація OTP).
- Протокол валідації OTP YubiKey версії 2.0.

3. Огляд

Двофакторна система автентифікації автентифікує користувача на основі двох факторів, чогось, що користувач знає, що зазвичай є комбінацією його імені користувача та/або пароля, і того, що користувач має у своєму фізичному розпорядженні, яким у нашому випадку є YubiKey. Двофакторна автентифікація забезпечує високий рівень безпеки та часто потрібна для відповідності нормам. Однак є випадки використання, коли однофакторна автентифікація потрібна для спрощеного доступу або зручності з помірним рівнем безпеки. Ми розглянемо розробку як двофакторного, так і однофакторного режимів автентифікації.

3.1 Однофакторна та двофакторна автентифікація YubiKey

YubiKey видає одноразовий пароль (OTP) із 44 символів, перші 12 символів якого є унікальним загальнодоступним ідентифікатором самого YubiKey, а наступні символи є динамічною частиною OTP. Зразок виведення з YubiKey, де кнопку було натиснуто тричі, може виглядати так:

Public ID **OTP**

fifjgjgkhchb**irdrfdnlnghhfgrtnnlgedjlftrbdeut**

fifjgjgkhchb**gefdkbbditfjrlniggevfhenublfnrev**

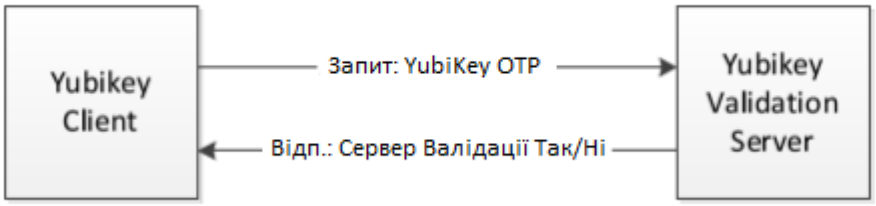
fifjgjgkhchb**lechfkfhiiuunbtnvgihdfiktncvlhck**

Той факт, що YubiKey видає як статичну частину ідентифікатора, так і динамічну частину OTP, що постійно змінюється, дозволяє розробляти комбінації двофакторної автентифікації та системи однофакторної автентифікації.

3.2 Базові компоненти

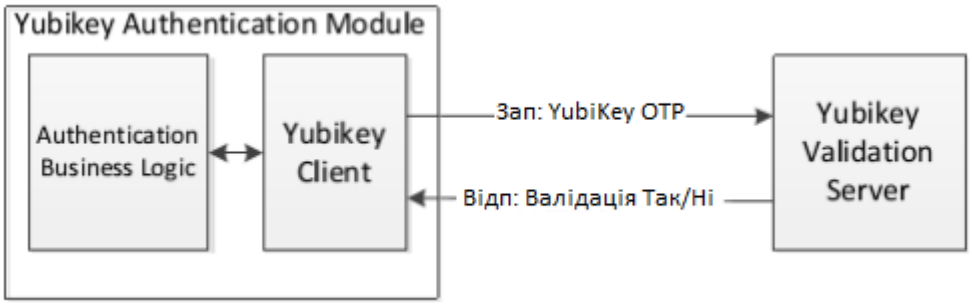
Серверні компоненти фреймворку автентифікації Yubico доступні з відкритим кодом. Базові компоненти забезпечують перевірку одноразового пароля YubiKey, пов'язуючи його з тим, який ключ YubiKey використовувався, і чи був дійсним надісланий OTP.

Базовими компонентами типової системи автентифікації YubiKey є так званий «клієнтський» модуль, відповідальний за реалізацію транспортного протоколу OTP і розбір відповіді від другого компонента, Сервера Валідації, який виконує фактичну валідацію OTP.



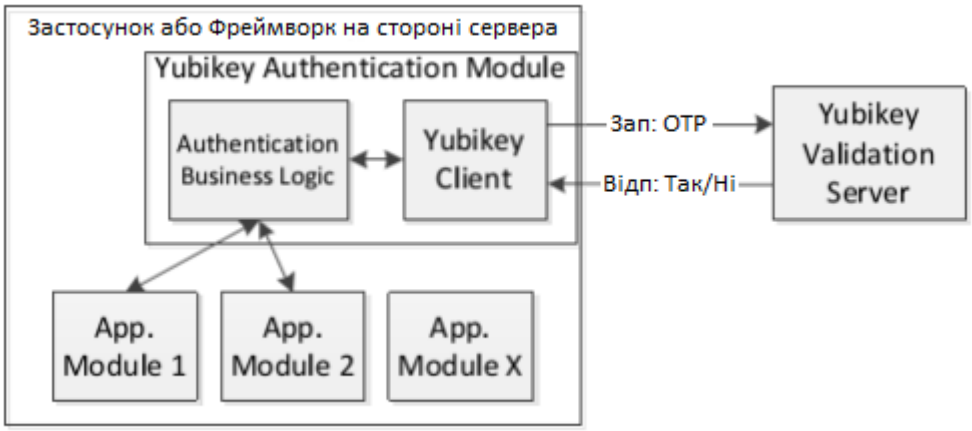
Клієнтський модуль YubiKey — це те, що ви інтегруєте в модуль автентифікації YubiKey на стороні сервера. Клієнти доступні багатьма мовами програмування http://www.yubico.com/web-api-clients, і ви також можете написати власного клієнта (див. посилання вище в розділі 1.3).

YubiKey Клієнт, реалізований у модулі автентифікації YubiKey, на високому рівні зазвичай виглядатиме приблизно так:



Бізнес-логіка автентифікації реалізує YubiKey і прив'язки користувачів, а також керування YubiKey.

Потім модуль Валідації стає частиною інфраструктури або програми на стороні сервера, де модуль автентифікації взаємодіє з іншими модулями та компонентами програми, такими як база даних і модуль керування користувачами та модуль входу в систему.



Залежно від характеру програми або фреймворка, розробник повинен враховувати масштабування, техніку надання YubiKey, встановлення, видалення модулів і постійне керування.

3.3 Сервер валідації та онлайн-служба валідації

Модуль автентифікації YubiKey може перевірити OTP на власному Сервері Валідації або на Онлайн-службі Валідації Yubico. Ви повинні вирішити, яка модель найкраще підходить для вашої програми.

Головною перевагою власного сервера є те, що ви повністю контролюєте всі ключі AES, запрограмовані в YubiKey.

Основна перевага використання Онлайн-сервісу Валідації Yubico полягає в тому, що ключі YubiKey уже готові до використання разом з Онлайн-сервісом Валідації (не потребує додаткового обслуговування).

3.3.1 Використання локального сервера валідації

Під час валідації на власному сервері ви контролюєте внутрішні ключі YubiKey. Ключі AES можна запрограмувати за допомогою інструменту персоналізації (доступного безплатно на сайті Yubico), і кожен ключ AES YubiKey буде записаний у файл, який потім, своєю чергою, можна буде імпортувати в базу даних сервера валідації. Перевага полягає в тому, що ви повністю контролюєте свої власні ключі.

3.3.2 Використання онлайн-служби валідації Yubico

Основна перевага використання Служби Валідації полягає в тому, що ключі YubiKey уже готові до використання з Онлайн-службою Валідації. Це також означає, що користувач може використовувати ключ як з вашою службою, так і з іншими сторонніми програмами та службами, такими як Google Apps для бізнес-користувачів і LastPass для керування паролями споживачів. Це також дає змогу користувачам, які вже мають YubiKey, зареєструватися на вашій службі.

3.4 Режими автентифікації, масштабування, забезпечення та адміністрування

Під час розробки модуля ви повинні враховувати режими автентифікації, масштабування, забезпечення (надання) YubiKey і адміністрування.

3.4.1 Режими автентифікації

Для відповідності багатьом галузевим законодавствам потрібна двофакторна автентифікація. Ви можете обрати підтримку лише режимів двофакторної автентифікації. Однак, якщо ви розробляєте модуль автентифікації YubiKey, який планується зробити частиною фреймворку, ми наполегливо рекомендуємо вам підтримувати чотири основні режими автентифікації, описані нижче, і надати адміністратору можливість примусово застосовувати бажаний режим для кожної групи користувачів на основі потреб безпеки та вимог політики:

A. Ім'я користувача + Пароль + OTP YubiKey.
B. Ім’я користувача або YubiKey OTP + пароль.
C. Лише YubiKey OTP.
D. Ім'я користувача + пароль.

3.4.2 Масштабування

Залежно від того, створюєте ви програму чи модуль для роботи в більшій структурі, ви можете знати або не знати, на скільки користувачів вам доведеться розраховувати. Для такої структури як Drupal можуть існувати сайти лише з кількома користувачами, але також — сайти з мільйонами користувачів. Навіть якщо ви не плануєте екстремального проєктування, будь ласка, розгляньте модулі, що працюють у фреймворках для підтримки як мінімум 10 000 користувачів.

Також для масштабування (якщо це доречно) розгляньте ієрархічну структуру для функцій адміністрування та служби підтримки.

Як найкращу практику Yubico рекомендує розробити модуль автентифікації YubiKey таким чином, щоб він жодним чином не обмежував і не впливав негативно на масштабованість, адміністрування та функцію служби підтримки (якщо вона є) оригінальної структури/програми.

3.4.3 Забезпечення

Надання YubiKey має виконуватися як мінімум адміністратором.

Адміністратор повинен мати можливість призначити користувачеві YubiKey. Адміністратор повинен мати можливість керувати всіма іншими аспектами, наприклад, зіставляти один або кілька ключів YubiKey з користувачем.

Якщо використовується самостійне налаштування (необов'язкова вимога, але настійно рекомендується у разі великої бази користувачів), спроєктуйте модуль так, щоб він міг підтримувати як великі споживчі сайти, так і сайти з більш обмеженою користувацькою базою.

Дивіться більше інформації в розділі деталей нижче.

3.4.4 Адміністрування

Адміністрування модуля має бути зведене до мінімуму. Слід розглянути можливість самостійного забезпечення та самостійного керування користувачами, щоб мінімізувати навантаження на адміністрування, особливо для великих сайтів.

Дивіться більше інформації в розділі деталей нижче.

4. Можливості та функціональність

У цьому розділі описуються різні підтримувані можливості та міркування, які слід враховувати при розробці модуля автентифікації YubiKey для програм на стороні сервера.

4.1 Надання YubiKey

Зазвичай користувачі можуть мати один або кілька ключів YubiKey, пов’язаних зі своїми обліковими записами. Однак в якості надійної практики безпеки настійно рекомендується, щоб модуль не дозволяв призначати той самий YubiKey більш ніж одному користувачеві.

Перша частина (фіксовані 12 символів) YubiKey OTP є унікальним ідентифікатором для YubiKey і відома як YubiKey ID. Його слід використовувати для підтримки зв’язку Користувач – YubiKey у модулі.

Щоб пов’язати ключі YubiKey з обліковими записами користувачів, модуль має реалізувати підтримку однієї або обох з наступних двох моделей надання залежно від потреб і розміру програми/сервісу:

1. Надання адміністратором (це завжди має підтримуватися).
2. Самоналаштування користувачем (необов’язкове, але чудово підходить для масштабування служби).

У наступних підрозділах описано ці моделі забезпечення більш детально.

4.1.1 Надання адміністратором (обов'язково)

Згідно з цією моделлю надання, адміністратор повинен мати можливість пов’язувати ключі YubiKey з обліковими записами користувачів.

Ця модель ініціалізації забезпечує жорсткіший контроль над користувачами, які отримують доступ до програми, і рекомендована для програм з вищими потребами в безпеці та невеликою базою користувачів. Однак, якщо база користувачів програми велика, надання YubiKey адміністратором може стати досить громіздким.

4.1.2 Самоналаштування користувачем (необов’язково)

Згідно з цією моделлю надання, окремий користувач має можливість пов’язати один або декілька ключів YubiKey зі своїм обліковим записом.

У моделі самоналаштування модуль повинен дозволяти користувачеві зареєструвати YubiKey як частину процесу реєстрації або під час першого використання програми/сервісу після встановлення та ввімкнення модуля. До того моменту, коли користувач успішно призначить перший YubiKey, модуль повинен застосовувати оригінальний метод (наприклад, зазвичай ім’я користувача + пароль) для автентифікації користувача.

Ця модель надання зменшує адміністративне навантаження та рекомендована для програм із великою базою користувачів.

4.2 Режими автентифікації

Модуль автентифікації YubiKey має бути дуже гнучким. Базуючись на відгуках клієнтів і досвіді Yubico, ми рекомендуємо, щоб модуль підтримував такі чотири режими автентифікації, які охоплюють більшість випадків використання YubiKey.

Підтримувані режими автентифікації:

1. Ім'я користувача + пароль + OTP YubiKey (найбільш безпечний).
2. Пароль + OTP YubiKey.
3. (Ім'я користувача або YubiKey OTP) + Пароль (зручний режим).
4. Лише YubiKey OTP.

Адміністратор повинен мати можливість вибрати один із наведених вище режимів автентифікації YubiKey як глобальний обраний режим автентифікації користувача для програми. Обраний режим автентифікації має бути обов'язковим для всіх користувачів усіх типів.

У наступних підрозділах більш детально описуються можливі режими автентифікації (як визначено вище).

4.2.1 Ім'я користувача + пароль + OTP YubiKey

Цей режим автентифікації вимагає від користувача ввести ім'я користувача, пароль і OTP YubiKey для входу в програму.

Це найбезпечніший режим із чотирьох, і його зазвичай слід установлювати як стандартний для модуля (після встановлення).

Ми наполегливо рекомендуємо вам розглянути параметр адміністративної конфігурації «Зробити OTP необов'язковим, доки YubiKey не буде призначено обліковому запису користувача», якщо існує можливість розгортання модуля автентифікації YubiKey для програм, які вже знаходяться у виробництві та мають базу користувачів від середньої до великої, оскільки розповсюдження та призначення YubiKey користувачам може зайняти час. Ця опція дозволить адміністраторам створити проміжок часу, щоб забезпечити безперебійне обслуговування для користувачів, поки вони отримують і призначають свої ключі YubiKey, а після розумного періоду переходу перейти до суворіших заходів безпеки.

4.2.2 Пароль + YubiKey OTP

За допомогою цього режиму автентифікації користувачі можуть входити в програму, використовуючи свій пароль і YubiKey OTP.

YubiKey ID можна використовувати для ідентифікації/відповідності імені користувача, щоб спростити процес входу в систему та покращити взаємодію з користувачем.

4.2.3 (Ім'я користувача або YubiKey OTP) + Пароль

За допомогою цього режиму автентифікації користувачі можуть входити в програму, використовуючи свої (ім'я користувача та пароль) або (YubiKey OTP та пароль).

Цей режим не забезпечує додаткової безпеки. Натомість це чиста зручність, оскільки користувач може вибрати ім'я користувача та пароль без використання YubiKey.

Однак це може бути корисним на етапі переходу під час розгортання YubiKey для всіх користувачів. У такому випадку адміністратор може пізніше перейти до першого режиму, де для входу потрібні всі три фактори.

4.2.4 Лише YubiKey OTP

Використовуючи цей режим автентифікації, користувачі можуть увійти в програму, просто вказавши свій OTP YubiKey.

YubiKey ID можна використовувати для ідентифікації/відповідності імені користувача, щоб спростити процес входу в систему та покращити взаємодію з користувачем. Цей режим пропонує зручну однофакторну автентифікацію за допомогою YubiKey. Але це не так безпечно, як двофакторна автентифікація, оскільки якщо YubiKey буде втрачено або вкрадено, тоді (до вимкнення) YubiKey може використовуватися для входу в службу будь-ким, просто натисканням кнопки (за умови, що неавторизований користувач знає про сервіс, для якого ввімкнено YubiKey).

4.3 Валідація YubiKey OTP

Yubico надає онлайн-сервіс валідації OTP (під назвою YubiCloud) для перевірки OTP, згенерованих YubiKey. Крім того, організації можуть вибрати розміщення власних серверів валідації YubiKey OTP.

Модуль автентифікації YubiKey має бути розроблений для підтримки як перевірки одноразових паролів YubiKey за допомогою Онлайн-служби Валідації (OTP) Yubico (YubiCloud), так і внутрішньої служби валідації YubiKey OTP.

4.3.1 YubiCloud – Онлайн-служба Валідації Yubico

YubiCloud — онлайн-сервіс валідації одноразових паролів Yubico, який можна використовувати для перевірки одноразових паролів, згенерованих YubiKey. За попередньою опцією ключі YubiKey запрограмовано для використання з YubiCloud («працює з коробки»).

YubiCloud використовує звичайний дворівневий підхід Yubico (інтерфейс сервера Валідації та сервер KSM). Він заснований на реплікованій архітектурі та працює з декількома серверами валідації в різних географічних місцях, щоб уникнути єдиної точки збою, зменшити затримки мережі та підвищити доступність.

4.3.2 Внутрішній сервер Валідації OTP YubiKey

Організації та постачальники програм/послуг можуть розмістити свої сервери валідації OTP YubiKey. Таким чином, модуль автентифікації YubiKey повинен містити підтримку для перевірки одноразових паролів YubiKey за допомогою внутрішнього серверу(ів) валідації YubiKey OTP.

Ми рекомендуємо вибрати між внутрішньою та зовнішньою валідацією як параметр конфігурації в глобальній конфігурації.

4.4 Керування YubiKey

Керування YubiKeys є важливою частиною підтримки YubiKey. У найпростішому випадку адміністратор здійснював би все керування, коли це необхідно. Для великих сайтів це не масштабується, тому ви можете розглянути можливість виконання певних завдань користувачем або створення ієрархії адміністраторів і персоналу служби підтримки.

4.4.1 Керування YubiKey адміністратором

Модуль має дозволити адміністраторам керувати ключами YubiKey, пов’язаними з обліковими записами користувачів. Адміністратор повинен мати можливість активувати/деактивувати та видаляти ключі YubiKey, пов’язані з користувачами. Тільки ключі YubiKey зі статусом «активний» можуть увійти до програми.

Адміністратор повинен завжди мати можливість призначити ключі YubiKey обліковим записам користувачів. Це особливо важливо – і обов’язково – якщо самоініціалізація ключів YubiKey не підтримується.

4.4.2 Керування YubiKey користувачем

Якщо реалізована підтримка самостійної підготовки ключів YubiKey, то зазвичай модуль повинен дозволяти користувачам керувати ключами YubiKey, пов’язаними з їхніми обліковими записами. Це можна реалізувати

по-різному, залежно від типу послуг, які ви надаєте.

Для бізнесу керування YubiKey користувачами може бути обмежене повідомленням про втрачений або вкрадений ключ (автоматичне призупинення зв'язаного YubiKey) і впровадженням способу для користувачів тимчасово отримати доступ до послуги або деяких її частин за допомогою деяких тимчасових засобів, поки користувач не отримає новий YubiKey.

Для споживчих послуг (і якщо це дозволяє ваша політика безпеки), користувачі повинні мати можливість додавати нові ключі YubiKey до своїх облікових записів. Користувач також повинен мати можливість активувати/деактивувати та видаляти ключі YubiKey, пов'язані з обліковим записом, а також повідомляти про втрачені або вкрадені ключі YubiKey. Залежно від вашої служби може знадобитися або не знадобитися підтримка користувачів, які отримують тимчасовий доступ до послуг, якщо ключ позначено як втрачений або вкрадений (див. розділ нижче). У деяких випадках наявність кількох ключів, пов'язаних з одним і тим самим обліковим записом, вирішує цю проблему, особливо для пов'язаних з фінансами послуг.

4.5 Обробка втрачених, викрадених або пошкоджених ключів YubiKey

Модуль має містити механізм для ефективної обробки випадків втрати або пошкодження YubiKey. Модуль має допомогти користувачеві повідомити та підтвердити втрату/пошкодження YubiKey, щоб заблокувати будь-який доступ до серверної програми неавторизованою особою, яка знайшла втрачений YubiKey. І якщо ввімкнуто самоініціалізацію користувачем, то модуль має дозволити користувачеві, чий YubiKey втрачено/пошкоджено, додати новий YubiKey до свого облікового запису, щоб користувач міг увійти в програму.

5 Рекомендації щодо впровадження

Модуль автентифікації YubiKey повинен бути розроблений і реалізований як плагін (за можливості). Модуль не слід впроваджувати шляхом зміни основних файлів основної платформи. Це допомагає гарантувати, що модуль не буде зламано під час оновлення базової платформи додатків.

У цьому розділі наведено рекомендації щодо впровадження та обслуговування модуля автентифікації YubiKey.

5.1 Встановлення

Адміністратор повинен мати можливість встановити, налаштувати та увімкнути модуль автентифікації YubiKey з консолі адміністратора.

Встановлення модуля має бути простим і виконуватися як частина процесу встановлення модуля; повинні бути проведені такі заходи:

1. Необхідно визначити параметри конфігурації для модуля за попередньою опцією.
2. Усі модифікації бази даних, такі як створення нових таблиць, визначення конфігурацій модулів тощо, слід виконувати без впливу на інші модулі.
3. Базуючись на вимогах базової платформи програми, модуль має бути зареєстрований у програмі.

Рекомендується, щоб сценарій встановлення забезпечував підтримку всіх систем баз даних, які підтримуються базовою платформою додатків.

5.2 Видалення

У більшості випадків модуль повинен підтримувати спосіб елегантного видалення модуля, якщо це необхідно. У такому випадку перед видаленням модуль має запропонувати адміністратору створити резервну копію даних, які використовує модуль, у файлі, який можна буде відновити пізніше, якщо це буде потрібно.

Резервне копіювання не обов'язково реалізовувати як частину процесу видалення, натомість це може бути опція, яку адміністратор може вибрати на звичайному екрані адміністрування модуля. Видалення модуля автентифікації YubiKey не повинно залишати інші модулі в стані, коли вони не працюватимуть як зазвичай.

5.3 Конфігурація

Після встановлення та ввімкнення модуля автентифікації YubiKey адміністратор зможе налаштувати глобальні параметри для модуля.

Модуль має надавати інтерфейс конфігурації модуля, де адміністрація може налаштувати наступні глобальні параметри для модуля:

- Режим Автентифікації YubiKey.
- Служба Валідації для використання.
- Увімкнення/Вимкнення модуля.

У наступних підрозділах детально описуються різні параметри, які можна налаштувати.

5.3.1 Вибір режиму автентифікації

Можливо, усі запропоновані режими автентифікації не повинні підтримуватися для всіх програм, оскільки вимоги можуть диктувати, що лише деякі режими є сумісними, і тому лише ці режими можуть бути реалізовані. Однак для фреймворків (наприклад, Drupal), які використовуватимуться для багатьох цілей, ми рекомендуємо запровадити

всі режими та залишити адміністратору сайту право вирішувати, які режими використовувати.

В інтерфейсі конфігурації модуля адміністратор повинен мати можливість вибрати один із наступних чотирьох режимів автентифікації як вибраний режим автентифікації користувача:

1. Пароль + OTP YubiKey.
2. (Ім'я користувача або YubiKey OTP) + Пароль.
3. Лише YubiKey OTP.
4. Ім'я користувача + пароль + YubiKey.

Для режиму автентифікації «Ім'я користувача + пароль + YubiKey OTP» в інтерфейсі також має бути можливість вибору опції «Зробити OTP необов'язковим, доки не призначено». Якщо вибрано цей параметр, користувачі повинні мати можливість входити в програму за допомогою імені користувача та пароля, доки YubiKey не призначено для їхнього облікового запису. Після того, як YubiKey призначено певному обліковому запису користувача, цей користувач, щоб увійти, має бути змушений надати одноразовий пароль із призначеного YubiKey на додаток до імені користувача та пароля.

Ця опція полегшує плавне розгортання рішення суворої автентифікації YubiKey для існуючих екземплярів програми, що має активних користувачів. Для великої бази користувачів адміністратори потенційно можуть використовувати цю опцію, щоб забезпечити безперервний доступ користувачам протягом певного обмеженого періоду часу (наприклад, 15 днів), доки ключі YubiKey не будуть призначені та розповсюджені всім користувачам, а потім адміністратор може вимкнути цю опцію або вибрати інший режим автентифікації.

Виходячи з вибраного режиму автентифікації користувача, інтерфейс входу в програму також слід змінити, щоб уникнути плутанини користувача. Наприклад, якщо вибрано режим автентифікації «Ім'я користувача + пароль + OTP YubiKey» з вибраною опцією «Зробити OTP необов'язковим до призначення», тоді інтерфейс входу повинен мати три поля введення, а саме «Ім'я користувача», «Пароль» і «OTP YubiKey» — у такій послідовності, і потрібно чітко зазначити, що поле «YubiKey OTP» є необов'язковим, поки його не призначено. Так само, якщо вибрано режим автентифікації «Пароль + YubiKey OTP», тоді інтерфейс входу має мати два поля введення, а саме «Пароль» і «YubiKey OTP».

5.3.2 Налаштування Служби Валідації

В інтерфейсі конфігурації модуля адміністратор повинен мати можливість вибирати між онлайн-службою валідації OTP Yubico та внутрішньою службою валідації YubiKey OTP. За попередньою опцією модуль має використовувати онлайн-сервіс валідації Yubico.

Щоб використовувати службу валідації OTP YubiKey, модуль повинен отримати власний ключ Yubico API та ідентифікатор API. Розробник (розробники) модуля може (можуть) згенерувати ключ API за допомогою онлайн-генератора ключів API Yubico за таким посиланням:

https://upgrade.yubico.com/getapikey/

У інтерфейсі адміністратор повинен мати можливість налаштувати такі параметри служби перевірки:

- Ключ API – це спільний симетричний ключ, який використовується для підпису запиту на валідацію OTP і для перевірки відповіді на валідацію OTP.
- Ідентифікатор API – це унікальний ідентифікатор API, який використовується сервером валідації для отримання правильного спільного секрету для підпису відповіді.
- HTTPs – це позначка, яка вказує на те, що модуль хоче використовувати HTTPs для доступу до служби валідації.
- Тайм-аут – кількість секунд для очікування відповіді автентифікації до закінчення часу очікування запиту.

Якщо адміністратор вирішує використовувати внутрішню службу валідації OTP YubiKey, тоді інтерфейс має дозволяти адміністратору налаштовувати URL-адреси внутрішніх примірників сервера валідації.

5.4 Інтеграція пакета Yubico

Онлайн-служба валідації одноразового пароля Yubico доступна через API веб-служб. Щоб спростити інтеграцію з YubiCloud, Yubico пропонує кілька готових до використання реалізацій API веб-служб (так звані Yubico Клієнти) на різних мовах програмування. Клієнтські бібліотеки доступні на C, PHP, Java, .Net, Ruby, PERL, Python тощо. Для отримання додаткової інформації про ці клієнтські бібліотеки відвідайте http://www.yubico.com/web-api-clients.

Настійно рекомендується, щоб розробник модуля використовував останню версію однієї з цих клієнтських бібліотек для інтеграції валідації OTP YubiKey у Модуль Автентифікації YubiKey.

5.5 Керування YubiKey

5.5.1 Керування YubiKey адміністратором

Модуль має забезпечувати простий у використанні інтерфейс для керування YubiKey за допомогою адміністратора на консолі адміністратора.

Інтерфейс слід розробляти та впроваджувати, пам'ятаючи про те, що може бути велика кількість користувачів із пов'язаними ключами YubiKey у програмі чи середовищі, яке використовує модуль.

Ми рекомендуємо, щоб інтерфейс мав перераховувати інформацію про користувача YubiKey у табличному форматі з такими стовпцями:

1. Ім'я користувача.
2. Ідентифікатор YubiKey.
3. Статус – Активний/Деактивований.
4. Дії – Активувати/Деактивувати, Видалити.

Модуль може також перераховувати додаткові деталі, як-от інформацію про дату й час «Останнє використання», додаткові поля для використання служби підтримки тощо. Інтерфейс має відображати фіксовану кількість записів за раз і має реалізовувати відповідну функціональність сторінок для зручної навігації.

Адміністратор також повинен мати можливість шукати певного користувача/YubiKey за допомогою імені користувача/YubiKey ID або його початкового фрагмента у функції пошуку.

5.5.2 Керування YubiKey користувачем

Якщо вимоги дозволяють, ми рекомендуємо, щоб модуль надавав (простий у використанні) інтерфейс для керування YubiKey користувачем на консолі користувача.

Ми рекомендуємо, щоб в інтерфейсі відображалися відомості про користувача YubiKey у табличному форматі з наступними стовпцями:

1. Ідентифікатор YubiKey.
2. Статус – Активний/Деактивований.
3. Дії – Активувати/Деактивувати, Видалити.

Модуль також має надати форму для додавання нового YubiKey до облікового запису користувача. Користувача слід попросити надати YubiKey OTP. Перед додаванням YubiKey до облікового запису користувача модуль повинен виконати такі перевірки:

1. OTP є дійсним YubiKey OTP.
2. YubiKey OTP успішно перевірено за допомогою служби валідації.
3. YubiKey ID не належить жодному іншому наявному користувачу (якщо вимоги однакові, YubiKey не можна використовувати для декількох облікових записів).

Примітка: модуль має переконатися, що кожного разу, коли він отримує YubiKey OTP від кінцевого користувача; він повинен використовувати цей OTP (шляхом надсилання запиту валідації на сервер), таким чином гарантуючи, що той самий OTP не може бути використаний повторно.

5.6 Повідомлення про втрачений/пошкоджений YubiKey

Якщо користувач втратить свій YubiKey, модуль повинен забезпечувати механізм легкого блокування YubiKey, щоб запобігти будь-якому доступу до сайту неавторизованої особи, яка може знайти втрачений YubiKey. В інтерфейсі входу модуль має надавати посилання, за яким користувачі можуть повідомити про втрату свого YubiKey.

Рекомендується, щоб механізм був розроблений як триетапний процес:

1. Звітність.
2. Підтвердження (щоб уникнути зловмисного/випадкового блокування інших облікових записів користувачів).
3. Скидання.

У наступних підрозділах описано вищезазначені кроки більш детально.

5.6.1 Повідомлення про втрату Yubikey

Щоб повідомити про втрату YubiKey, користувача слід попросити надати ім'я користувача/електронну адресу та пароль (необов'язково, якщо користувач забув свій пароль), пов'язані з його/її обліковим записом.

Після успішної перевірки імені користувача/адреси електронної пошти та пароля (якщо вони надані) на зареєстровану адресу електронної пошти користувача слід надіслати одноразове посилання для підтвердження.

5.6.2 Підтвердження

Щоб підтвердити втрату YubiKey, користувач повинен перейти за посиланням для одноразового підтвердження, надісланим у листі з підтвердженням.

Коли користувач підтверджує втрату свого YubiKey, необхідно виконати наступні дії:

- Усі ключі YubiKey, пов'язані з обліковим записом користувача, мають бути тимчасово заблоковані.
- Якщо самостійна ініціалізація YubiKey підтримується, тоді користувач повинен бути перенаправлений до інтерфейсу «Скинути YubiKey».
- Якщо самостійна ініціалізація YubiKey не підтримується, необхідно надіслати сповіщення електронною поштою всім зацікавленим особам (зазвичай адміністраторам), а користувача слід сповістити, чи може він/вона увійти до системи, перш ніж йому буде призначено новий YubiKey.

а. І якщо дозволено увійти, то — як, тобто який тимчасовий метод можна використовувати до отримання нового YubiKey.

5.6.3 Скидання

Скидання повинно дозволити користувачеві додати новий YubiKey до облікового запису або активувати один із існуючих YubiKey.

Користувача слід попросити надати YubiKey OTP з YubiKey. Під час скидання YubiKey необхідно виконати такі дії:

1. YubiKey OTP має бути підтверджено за допомогою служби валідації.
2. Необхідно перевірити ідентифікатор YubiKey, щоб переконатися, що YubiKey не належить жодному іншому користувачеві.
3. Якщо YubiKey вже належить користувачеві, активуйте цей YubiKey.

4. Якщо YubiKey не належить користувачеві, пов’яжіть YubiKey з обліковим записом користувача та увімкніть його.

5.7 Журнали та звіти

Модуль повинен реєструвати всі події на основі YubiKey з відповідним рівнем серйозності для регулярного моніторингу адміністраторами.

Модуль повинен надавати різноманітні звіти для адміністратора, як мінімум такі:

- Відображення YubiKey-користувача.
- Користувачі без ключів YubiKey.
- Дезактивовані ключі YubiKey.
- Журнал активності – запис дати/часу, публічного ідентифікатора та активності (успіх/невдача) для кожної спроби автентифікації (успішної або ні).

5.8 Документація

Модуль має надати детальний покроковий посібник із налаштування для адміністраторів і розробників додатків, зацікавлених у забезпеченні надійної двофакторної автентифікації користувача за допомогою YubiKey. У цьому документі читачі повинні ознайомитися з кроками, необхідними для встановлення та налаштування модуля автентифікації YubiKey для програми, щоб увімкнути потужну двофакторну автентифікацію користувача на основі YubiKey. Він також має описувати адміністрування модуля високого рівня.

Посібник з конфігурації має детально описувати наступні елементи:

Передумови до модуля:

- Можливості модуля.
- Інструкції зі встановлення.
- Інструкції з налаштування.
- Інструкції з видалення.
- Адміністрування модуля (Користувачі та ключі YubiKey).

6 Контрольний список

У цьому розділі наведено контрольний перелік можливостей, які необхідно підтримувати, і міркування, які слід враховувати при розробці модуля автентифікації YubiKey для програм на стороні сервера.

№	Розгляд проєктування	Ваш вибір (позначте все, що підходить)
1	Встановлення	☐ Так ☐ Ні
2	Видалення	☐ Так ☐ Ні
3	Параметри конфігурації • Режими автентифікації YubiKey • Служба Валідації для використання • Підтримка увімкнення/вимкнення модуля	 ☐ Ім'я користувача + Пароль + OTP ☐ Пароль + OTP ☐ (Ім'я користувача або OTP) + Пароль ☐ Лише OTP ☐ Зробіть OTP необов'язковим, доки YubiKey не буде призначено обліковому запису користувача ☐ Служба Валідації YubiCloud ☐ Ваш локальний сервер валідації ☐ Так ☐ Ні
4	Використання клієнта валідації з відкритим кодом Yubico	☐ Так ☐ Ні
5	Керування YubiKey • Адміністратором сайту • Користувачами сайту • Підтримка самостійного забезпечення	 ☐ Так ☐ Ні ☐ Так ☐ Ні ☐ Так ☐ Ні
6	Призначати користувачам кілька ключів YubiKey	☐ Так ☐ Ні
7	Повідомляти про втрату ключів YubiKey користувачами	☐ Так ☐ Ні
8	Журнали та звіти	☐ Так ☐ Ні
9	Документація модуля	☐ Так ☐ Ні

Скопіюйте цей контрольний список на сторінку Yubico Wiki, де ви описуєте свій модуль. Таким чином зацікавлені користувачі отримають швидкий огляд підтримуваних функцій ще до встановлення модуля.