

UVC.one Технічний Документ

Федеративна Архітектура Довіри для Верифікованої УФ-С Дезінфекції

Версія 1.0 | Серпень 2025

Анотація

UVC.one представляє нову федеративну архітектуру довіри для верифікації дезінфекції в охороні здоров'я, побудовану на федеративній платформі Refinio. Цей документ детально описує технічну реалізацію багатоплатформної екосистеми, що включає вбудовані датчики, мобільні додатки, настільне програмне забезпечення та серверну інфраструктуру, які разом забезпечують криптографічно перевірювані докази операцій УФ-С дезінфекції.

На відміну від традиційних централізованих систем верифікації, UVC.one використовує розподілену модель довіри, де декілька незалежних пристроїв створюють невідомі записи верифікації через W3C Verifiable Credentials, дозволяючи медичним закладам доводити відповідність вимогам без покладання на зовнішні органи.

1. Вступ

Медичні заклади по всьому світу стикаються з проблемою верифікації ефективності УФ-С дезінфекції та ведення документації відповідності. Існуючі рішення покладаються на ручне ведення журналів, системи на основі довіри або ізольоване моніторинг обладнання, що не може забезпечити криптографічний доказ фактичних подій дезінфекції.

UVC.one вирішує цю проблему через федеративну архітектуру довіри, що розподіляє верифікацію між декількома незалежними пристроями, створюючи стійкий до підробки запис діяльності з дезінфекції, зберігаючи при цьому операційну простоту для медичного персоналу.

1.1 Постановка Проблеми

Традиційна УФ-С верифікація стикається з трьома критичними обмеженнями:

- **Розрив Довіри:** Відсутність криптографічного доказу того, що дезінфекція дійсно відбулася
- **Ізоляція:** Обладнання працює незалежно без перехресної верифікації
- **Ризик Централізації:** Єдині точки відмови в системах верифікації

1.2 Огляд Рішення

UVC.one реалізує федеративну екосистему верифікації, де:

- Декілька незалежних пристроїв створюють резервні записи верифікації
- W3C Verifiable Credentials забезпечують криптографічний доказ операцій
- Розподілена довіра усуває єдині точки відмови
- Міжплатформна доступність забезпечує операційну безперервність

2. Федеративна Архітектура Платформи

2.1 Основа Refinio

UVC.one побудований на федеративній платформі Refinio (refinio.net), яка забезпечує базову інфраструктуру для розподіленого управління даними та криптографічної верифікації. Refinio дозволяє:

- **Децентралізоване Управління Ідентичністю:** Використання W3C Decentralized Identifiers (DIDs)
- **Verifiable Credentials:** Криптографічно підписані атестації
- **Федеративне Зберігання Даних:** Розподілене між вузлами мережі
- **Міжплатформна Синхронізація:** Безперебійний доступ до даних через пристрої

2.2 Модель Довіри

Федеративна архітектура довіри працює на принципі незалежної атестації через verifiable credentials в межах кожного медичного закладу:

Мережа Довіри Закладу = {Джерело Світла₁, Датчик₁, Датчик₂, ..., Датчик_N, Свідок₁, ..., Свідок_M}

Кожен пристрій підтримує свою власну криптографічну ідентичність та незалежно видає verifiable credentials, що засвідчують його взаємодії з іншими пристроями під час подій дезінфекції. Замість вимоги консенсусу, кожен пристрій криптографічно підписує свої власні спостереження та взаємодії, створюючи невідомий запис процесу верифікації.

Довіра виникає з криптографічної цілісності індивідуальних атестацій пристроїв, а не з угоди між пристроями.

2.3 Мінімальні Вимоги до Пристроїв

Хоча UVC.one може працювати з будь-якою кількістю пристроїв, мінімальна життєздатна конфігурація вимагає три різні типи:

1. **Пристрій Джерела Світла:** УФ-С лампа з вбудованим моніторингом
2. **Датчик Навколишнього Середовища:** Незалежне виявлення радіації
3. **Пристрій-Свідок:** Пристрій верифікації, що належить закладу

Додаткові пристрої підвищують довіру до верифікації, але не є архітектурно необхідними.

3. Багатоплатформна Стратегія

3.1 Огляд Екосистеми Платформ

UVC.one реалізує комплексну багатоплатформну стратегію, що забезпечує універсальну доступність та операційну безперервність:

- **Вбудовані Пристрої:** Багатоплатформні вбудовані датчики та актуатори
- **Мобільний Додаток:** Нативні додатки для iOS/Android
- **Настільний Додаток:** Програмне забезпечення для Windows/macOS/Linux
- **Веб-Додаток:** Інтерфейс на основі браузера
- **Серверна Інфраструктура:** Хмарні та локальні варіанти розгортання

3.2 Архітектура Потoku Даних

Потік Даних в Межах Закладу:

- Вбудовані пристрої комунікують безпосередньо з локальним вузлом Refinio закладу
- Мобільні та настільні додатки підключаються до того ж локального вузла Refinio
- BLE використовується для безпечної конфігурації пристроїв та провізіювання облікових даних
- Всі дані верифікації залишаються під контролем закладу

Міжзакладна Федерація:

- Вузол Refinio кожного закладу може підключатися безпосередньо до вузлів інших закладів

- Peer-to-peer верифікація та атестація між закладами
- Центральний орган не потрібен для міжзакладної довіри
- Серверна інфраструктура надає додаткові послуги аналітики та резервного копіювання

Мережеві Режими:

- **Зашифрована Mesh:** Пристрої формують самодостатню мережу з власною підключеністю
 - **Інтеграція Інфраструктури:** Пряме підключення до WiFi/Ethernet закладу
 - **Гібридна Операція:** Одночасна mesh та інфраструктурна підключеність
-

4. Реалізація Вбудованих Пристроїв

4.1 Багатоплатформна Вбудована Архітектура

UVC.one підтримує широкий спектр вбудованих апаратних платформ, забезпечуючи гнучкість розгортання на основі специфічних вимог закладу та існуючої інфраструктури.

Загальні Можливості Через Платформи:

- **Багатопротокольна Підключеність:** WiFi, Bluetooth Low Energy (BLE) та mesh-мережі
- **Безпечна Конфігурація:** Облікові дані WLAN надаються через Verifiable Credentials по BLE
- **Криптографічна Обробка:** Апаратне або програмне прискорення шифрування
- **Операції в Реальному Часі:** Негайна верифікація та атестація
- **Мережева Гнучкість:** Працює в зашифрованій mesh-мережі або інтегрується з існуючою інфраструктурою

4.2 Типи Пристроїв та Функції

Пристрої Джерела Світла

- Моніторинг споживання енергії УФ-С лампи
- Вимірювання фактичного випромінювання УФ-С радіації
- Генерація записів операцій з позначками часу
- Створення підписаних атестацій спроб дезінфекції

Датчики Навколишнього Середовища

- Незалежне виявлення УФ-С радіації

- Сенсинг присутності в кімнаті
- Моніторинг умов навколишнього середовища
- Перехресна верифікація заяв джерела світла

Пристрої-Свідки

- Вузли верифікації, що належать закладу
- Агрегація даних з декількох джерел
- Генерація документації відповідності
- Ведення локальної історії верифікації

4.3 Вибір Апаратної Платформи

Вибір платформи базується на специфічних вимогах розгортання, включаючи потреби обробки, вимоги підключення, екологічні обмеження, міркування живлення, складність інтеграції та оптимізацію витрат. Архітектура абстрагує апаратні відмінності, забезпечуючи послідовну роботу незалежно від вибору базової платформи.

4.4 Протокол Верифікації

Кожен цикл дезінфекції слідує стандартизованому протоколу верифікації незалежно від базової апаратної платформи:

1. **Ініціація:** Пристрій джерела світла починає ведення журналу операцій
2. **Виявлення:** Датчики навколишнього середовища підтверджують присутність радіації
3. **Моніторинг:** Безперервне вимірювання протягом циклу
4. **Атестація:** Всі пристрої видають verifiable credentials, що описують їх спостереження та взаємодії під час циклу дезінфекції
5. **Документація:** Індивідуальні атестації пристроїв агрегуються в комплексні записи верифікації
6. **Відповідність:** Verifiable credentials надають криптографічний доказ для регуляторної відповідності

Міжплатформна Сумісність: Протокол верифікації працює послідовно через всі підтримувані платформи - вбудовані пристрої, Linux, Windows, macOS, iOS та Android - забезпечуючи безперебійну сумісність між різними типами апаратного забезпечення та операційними системами в межах одного закладу.

5. Реалізація Рівня Додатків

5.1 Мобільні Додатки

Нативні мобільні додатки забезпечують моніторинг та контроль в реальному часі:

Функції:

- Жива панель статусу дезінфекції
- Відображення верифікації по кімнатах
- Push-сповіщення про завершення циклу
- Офлайн-операція з подальшою синхронізацією
- Сканування QR-кодів для ідентифікації пристроїв

Технічна Реалізація:

- React Native для міжплатформної розробки
- Інтеграція Refinio SDK для доступу до даних
- Служби фонові синхронізації
- Зашифроване локальне зберігання даних

5.2 Настільні Додатки

Настільне програмне забезпечення пропонує комплексне управління закладом:

Функції:

- Панель моніторингу багатьох закладів
- Детальна аналітика та звітність
- Інтерфейс управління конфігурацією
- Експорт даних та звітність відповідності
- Інтеграція з файловою системою Windows (дані доступні як структура папок)

Технічна Реалізація:

- Фреймворк Electron для міжплатформної сумісності
- Пряма інтеграція вузла Refinio
- Синхронізація локальної бази даних
- Рівень абстракції файлової системи

5.3 Веб-Додатки

Інтерфейс на основі браузера забезпечує універсальну доступність:

Функції:

- Доступ без встановлення
- Управління користувачами на основі ролей
- Оновлення в реальному часі через WebSockets
- Мобільно-адаптивний дизайн
- Інтеграція з існуючими ІТ-системами лікарень

Технічна Реалізація:

- Progressive Web Application (PWA)
 - WebAssembly клієнт Refinio
 - Service worker для офлайн-можливостей
 - RESTful API з GraphQL підписками
-

6. Серверна Інфраструктура

6.1 Гібридна Модель Розгортання

UVC.one підтримує гнучкі варіанти розгортання:

Хмарна Архітектура:

- Багаторегіональне розгортання для глобального доступу
- Автомасштабування на основі кількості закладів
- Керована послуга з 99.9% SLA безвідмовної роботи
- Автоматичне резервне копіювання та відновлення після аварій

Локальні Варіанти:

- Приватне хмарне розгортання для чутливих даних
- Відключена від мережі операція для високозахищених закладів
- Користувачька інтеграція з існуючою ІТ-інфраструктурою
- Локальне дотримання суверенітету даних

6.2 API Архітектура

Комплексний рівень API дозволяє інтеграцію:

RESTful APIs:

- Управління пристроями та конфігурація
- Доступ до даних верифікації
- Автентифікація та авторизація користувачів
- Ендпоінти звітності відповідності

GraphQL Інтерфейс:

- Оновлення підписок в реальному часі
- Гнучке запитування даних
- Підтримка пакетних операцій
- Розробка на основі схеми

WebSocket З'єднання:

- Живий моніторинг закладу
 - Миттєва доставка сповіщень
 - Двостороння комунікація пристроїв
 - Оновлення статусу з низькою затримкою
-

7. Безпека та Відповідність

7.1 Криптографічна Реалізація

Ідентичність Пристрою:

- Кожен пристрій генерує унікальні пари ключів Ed25519
- Ідентичності пристроїв реєструються з вузлами-свідками закладу
- Регулярна ротація ключів для підвищеної безпеки
- Інтеграція модуля апаратної безпеки де доступно

Цілісність Даних:

- Всі записи верифікації криптографічно підписані
- Структури дерева Меркла для виявлення підробки

- Незмінні аудиторські сліди з верифікацією позначок часу
- Вимоги багатопідписів для критичних операцій

7.2 Захист Приватності

Мінімізація Даних:

- Збирається тільки необхідна інформація про дезінфекцію
- Персональна інформація виключена з записів верифікації
- Анонімізована аналітика та звітність
- Налаштовувані політики зберігання даних

Контроль Доступу:

- Система дозволів на основі ролей
- Вимоги багатофакторної автентифікації
- Управління та ротація API ключів
- Аудиторське логування всіх спроб доступу

7.3 Регуляторна Відповідність

Стандарти Охорони Здоров'я:

- Відповідність HIPAA для захисту даних пацієнтів
- Вимоги безпеки HITECH
- Управління інформаційною безпекою ISO 27001
- Рекомендації FDA щодо програмного забезпечення медичних пристроїв

Міжнародні Стандарти:

- Відповідність GDPR для європейських операцій
 - Сертифікація SOC 2 Type II
 - Стандарти клінічних досліджень ISO 14155
 - Життєвий цикл програмного забезпечення медичних пристроїв IEC 62304
-

8. Операції Федеративної Мережі

8.1 Внутрізакладна Федеративна Довіра

Мережа Верифікації в Межах Закладу: Основна інновація UVC.one полягає у встановленні федеративної довіри в межах одного медичного закладу через декілька незалежних вузлів верифікації:

Федерація на Рівні Пристроїв:

- Декілька вбудованих пристроїв в кожній кімнаті формують незалежні вузли верифікації
- Кожен пристрій підтримує свою власну криптографічну ідентичність та можливість верифікації
- Довіра виникає з криптографічної цілісності індивідуальних атестацій пристроїв, а не з центрального органу
- Жоден окремий пристрій не може підробити записи верифікації без виявлення реєр-пристроями

Верифікація на Рівні Кімнати:

- Пристрої джерела світла, датчики навколишнього середовища та пристрої-свідки незалежно засвідчують події дезінфекції
- Кожен пристрій видає verifiable credentials, що описують його специфічні спостереження та взаємодії
- Декілька незалежних атестацій створюють комплексний запис верифікації
- Невдалі або конфліктні атестації зберігаються як частина запису верифікації для аудиторських цілей

Цілісність на Рівні Закладу:

- Пристрої-свідки агрегують дані верифікації з декількох кімнат та типів пристроїв
- Шаблони верифікації між кімнатами виявляють систематичні відмови або спроби підробки
- Розподілена верифікація усуває єдині точки відмови в межах закладу
- Повний аудиторський слід всіх діяльностей верифікації з криптографічним доказом

8.2 Розширення Міжзакладної Федерації

Масштабування до Багатозакладних Мереж: Внутрізакладна архітектура федеративної довіри природно розширюється до міжзакладних мереж верифікації:

Заклад-як-Вузол:

- Кожен заклад працює як окремий федеративний вузол у ширшій мережі
- Пристрої-свідки закладу представляють консенсус закладу в міжзакладних комунікаціях
- Міжзакладна верифікація будується на встановленій основі внутрізакладної довіри
- Багатозакладні організації можуть створювати приватні федеративні мережі

Шаблони Зростання Мережі:

- **Лікарняні Системи:** Декілька закладів в межах однієї організації охорони здоров'я
- **Регіональні Мережі:** Незалежні заклади, що поділяють стандарти верифікації
- **Дослідницькі Співпраці:** Академічні медичні центри з верифікованим обміном даними
- **Верифікація Ланцюга Постачання:** Виробники обладнання та медичні заклади

Федеративні Переваги в Масштабі:

- Розподілена верифікація відповідності через мережі закладів
- Бенчмаркінг та обмін найкращими практиками з криптографічним доказом
- Оцінка репутації та довіри на рівні мережі
- Стійка операція під час відключень мережі окремих закладів

8.3 Конфігурація Мережі та Безпека

Безпечне Провізіювання:

- Облікові дані WLAN розподіляються через W3C Verifiable Credentials
- Bluetooth Low Energy (BLE) для початкової конфігурації пристрою
- Розгортання без дотику з зашифрованим обміном обліковими даними
- Автоматичне виявлення мережі та безпечне приєднання

Подвійна Мережева Архітектура:

- **Зашифрована Mesh:** Самоформуюча mesh-мережа з end-to-end шифруванням
- **Інтеграція Інфраструктури:** Пряме підключення до WiFi/Ethernet закладу
- **Автоматичне Переключення:** Безперебійне переключення між mesh та інфраструктурними режимами
- **Мостові Вузли:** Пристрої можуть ретранслювати між mesh та інфраструктурними мережами

Мережева Безпека:

- WPA3 шифрування для інфраструктурних з'єднань
 - AES-256 шифрування для mesh-комунікацій
 - Автентифікація пристроїв на основі сертифікатів
 - Сегментація мережі та ізоляція трафіку
-

9. Міркування Реалізації

9.1 Стратегія Міграції

Поетапне Розгортання:

- Пілотна установка з мінімальною кількістю пристроїв
- Поступове розширення на додаткові кімнати/заклади
- Інтеграція з існуючим УФ-С обладнанням де можливо
- Навчання персоналу та підтримка управління змінами

Інтеграція Спадщини:

- API мости до існуючих систем управління закладом
- Експорт даних у стандартних форматах (HL7, CSV, XML)
- Користувацькі послуги розробки інтеграції
- Підтримка зворотної сумісності

9.2 Операційні Вимоги

Мережева Інфраструктура:

- **Гнучка Конфігурація Мережі:** Облікові дані WLAN налаштовуються через Verifiable Credentials та Bluetooth Low Energy (BLE)
- **Операція Зашифрованої Mesh:** Самодостатня mesh-мережа для ізольованого розгортання
- **Повна Інтеграція Інфраструктури:** Безперебійна інтеграція з існуючими мережами закладу
- **Гібридне Розгортання:** Підтримка як автономних mesh, так і інтегрованих режимів одночасно

Обслуговування:

- Рекомендується щоквартальне калібрування пристроїв
- Щорічне оновлення сертифікатів безпеки
- Оновлення програмного забезпечення через over-the-air розгортання

- Цілодобова технічна підтримка
-

10. Майбутній Розвиток

10.1 Технологічна Дорожня Карта

Короткостроково (6-12 місяців):

- Інтеграція машинного навчання для прогнозного обслуговування
- Просунута аналітична панель з AI інсайтами
- Інтеграція з основними платформами управління закладами
- Розширені функції мобільного додатку

Середньостроково (1-2 роки):

- Інтеграція блокчейну для незмінних записів відповідності
- Розширення IoT датчиків поза верифікацію УФ-С
- Штучний інтелект для оптимального планування дезінфекції
- Інтеграція з роботизованими системами дезінфекції

Довгостроково (2-5 років):

- Автономна оптимізація протоколу дезінфекції
- Прогнозна оцінка ризику відповідності
- Інтеграція з системами управління будівлями
- Розширення на інші домени верифікації

10.2 Дослідницька Співпраця

UVC.one активно співпрацює з академічними установами та дослідницькими організаціями для просування стану федеративних систем верифікації в медичних середовищах.

11. Висновок

UVC.one представляє парадигмальний зсув від моніторингу дезінфекції на основі довіри до верифікаційного в медичних закладах. Використовуючи федеративну платформу Refinio та реалізуючи комплексну багатоплатформну стратегію, UVC.one надає організаціям охорони здоров'я криптографічно перевірювані докази операцій дезінфекції, зберігаючи при цьому операційну простоту.

Федеративна архітектура довіри усуває єдині точки відмови, дозволяючи міжзакладну верифікацію та документацію відповідності, що відповідає найвищим регуляторним стандартам. Багатоплатформна реалізація забезпечує універсальну доступність та безперебійну інтеграцію з існуючою ІТ-інфраструктурою охорони здоров'я.

Оскільки медичні заклади все більше визнають важливість верифікованих заходів контролю інфекцій, UVC.one надає технічну основу для нового покоління систем відповідності та безпеки, побудованих на криптографічному доказі, а не на інституційній довірі.

Посилання

1. Федеративна Платформа Refinio: <https://refinio.net>
2. Модель Даних W3C Verifiable Credentials: <https://www.w3.org/TR/vc-data-model/>
3. W3C Decentralized Identifiers (DIDs): <https://www.w3.org/TR/did-core/>
4. Рекомендації CDC щодо УФ-С Дезінфекції:
<https://www.cdc.gov/coronavirus/2019-ncov/community/guidance.html>
5. Процеси Життєвого Циклу Програмного Забезпечення Медичних Пристроїв, IEC 62304
6. Закон про Переносимість та Підзвітність Медичного Страхування (HIPAA)
7. Загальний Регламент Захисту Даних (GDPR)

Інформація про Документ:

- **Автори:** Технічна Команда UVC.one
- **Версія:** 1.0
- **Дата:** Серпень 2025
- **Класифікація:** Публічна Технічна Документація
- **Контакт:** technical@uvc.one