UVC.one Technical Whitepaper

Federated Trust Architecture for Verified UV-C Disinfection

Version 1.0 | August 2025

Abstract

UVC.one presents a novel federated trust architecture for healthcare disinfection verification, built on the Refinio federated platform. This paper details the technical implementation of a multi-platform ecosystem comprising embedded sensors, mobile applications, desktop software, and server infrastructure that collectively provide cryptographically verifiable proof of UV-C disinfection operations.

Unlike traditional centralized verification systems, UVC.one employs a distributed trust model where multiple independent devices create unforgeable verification records through W3C Verifiable Credentials, enabling healthcare facilities to prove compliance without relying on external authorities.

---

1. Introduction

Healthcare facilities globally struggle with verifying UV-C disinfection effectiveness and maintaining compliance documentation. Current solutions rely on manual logging, trust-based systems, or isolated equipment monitoring that cannot provide cryptographic proof of actual disinfection events.

UVC.one addresses this challenge through a federated trust architecture that distributes verification across multiple independent devices, creating a tamper-resistant record of disinfection activities while maintaining operational simplicity for healthcare staff.

1.1 Problem Statement

Traditional UV-C verification faces three critical limitations:

- **Trust Gap**: No cryptographic proof that disinfection actually occurred
- **Isolation**: Equipment operates independently with no cross-verification

- **Centralization Risk**: Single points of failure in verification systems

1.2 Solution Overview

UVC.one implements a federated verification ecosystem where:

- Multiple independent devices create redundant verification records
- W3C Verifiable Credentials provide cryptographic proof of operations
- Distributed trust eliminates single points of failure
- Cross-platform accessibility ensures operational continuity

---

2. Federated Platform Architecture

2.1 Refinio Foundation

UVC.one is built upon the Refinio federated platform (refinio.net), which provides the underlying infrastructure for distributed data management and cryptographic verification. Refinio enables:

- **Decentralized Identity Management**: Using W3C Decentralized Identifiers (DIDs)
- **Verifiable Credentials**: Cryptographically signed attestations
- **Federated Data Storage**: Distributed across network nodes
- **Cross-Platform Synchronization**: Seamless data access across devices

2.2 Trust Model

The federated trust architecture operates on the principle of independent attestation through verifiable credentials within each healthcare facility:

- Facility Trust Network = {Light Source$_1$, Sensor$_1$, Sensor$_2$, ..., SensorN, Witness$_1$, ..., WitnessM}

Each device maintains its own cryptographic identity and independently issues verifiable credentials attesting to its interactions with other devices during disinfection events. Rather than requiring consensus, each device cryptographically signs its own observations and interactions, creating an unforgeable record of the verification process. Trust emerges from the cryptographic integrity of individual device attestations, not from agreement between devices.

2.3 Minimum Device Requirements

While UVC.one can operate with any number of devices, the minimum viable configuration requires three distinct types:

1. **Light Source Device**: UV-C lamp with embedded monitoring
2. **Environmental Sensor**: Independent radiation detection
3. **Witness Device**: Facility-owned verification node

Additional devices enhance verification confidence but are not architecturally required.

---

3. Multi-Platform Strategy

3.1 Platform Ecosystem Overview

UVC.one implements a comprehensive multi-platform strategy ensuring universal accessibility and operational continuity:

- **Embedded Devices**: Multi-platform embedded sensors and actors
- **Mobile Application**: iOS/Android native applications
- **Desktop Application**: Windows/macOS/Linux desktop software
- **Web Application**: Browser-based interface
- **Server Infrastructure**: Cloud and on-premise deployment options

3.2 Data Flow Architecture

- [Embedded Devices] ↔ [Local Refinio Node] ↔ [Facility Federated Network]
- ↕ ↕
- [Mobile/Desktop Apps] ← [BLE Configuration] → [Other Facility Nodes]
- ↕ ↕
- [Server Infrastructure] ← [Federated Trust Network] → [Cross-Facility Verification]

True Federated Architecture:

- **Facility Nodes**: Each facility operates its own Refinio federated node
- **Direct Federation**: Facilities connect directly to each other, not through centralized servers
- **Autonomous Operation**: Each facility maintains complete operational independence
- **Cross-Facility Trust**: Verification and attestation happens peer-to-peer between facility nodes

Data Sovereignty: Server infrastructure provides optional services (analytics, backup, compliance reporting) but facilities retain complete control over their verification data and can operate independently of any central authority.

---

4. Embedded Device Implementation

4.1 Multi-Platform Embedded Architecture

UVC.one supports a wide range of embedded hardware platforms, providing deployment flexibility based on specific facility requirements and existing infrastructure.

Common Capabilities Across Platforms:

- **Multi-Protocol Connectivity**: WiFi, Bluetooth Low Energy (BLE), and mesh networking
- **Secure Configuration**: WLAN credentials provisioned via Verifiable Credentials over BLE
- **Cryptographic Processing**: Hardware or software-accelerated encryption
- **Real-Time Operations**: Immediate verification and attestation capabilities
- **Network Flexibility**: Operates in encrypted mesh or integrated with existing infrastructure

4.2 Device Types and Functions

Light Source Devices

- Monitor UV-C lamp power consumption
- Measure actual UV-C radiation emission
- Generate timestamped operation records
- Create signed attestations of disinfection attempts

Environmental Sensors

- Independent UV-C radiation detection
- Room occupancy sensing
- Environmental condition monitoring
- Cross-verification of light source claims

Witness Devices

- Facility-owned verification nodes
- Aggregate data from multiple sources
- Generate compliance documentation
- Maintain local verification history

4.3 Hardware Platform Selection

Platform selection is based on specific deployment requirements including processing needs, connectivity requirements, environmental constraints, power considerations, integration complexity, and cost optimization. The architecture abstracts hardware differences, ensuring consistent operation regardless of underlying platform choice.

4.4 Verification Protocol

Each disinfection cycle follows a standardized verification protocol regardless of underlying hardware platform:

1. **Initiation**: Light source device begins operation logging
2. **Detection**: Environmental sensors confirm radiation presence
3. **Monitoring**: Continuous measurement throughout cycle
4. **Attestation**: All devices issue verifiable credentials describing their observations and interactions during the disinfection cycle
5. **Documentation**: Individual device attestations are aggregated into comprehensive verification records
6. **Compliance**: Verifiable credentials provide cryptographic proof for regulatory compliance

Cross-Platform Compatibility: The verification protocol operates consistently across all supported platforms - embedded devices, Linux, Windows, macOS, iOS, and Android - ensuring seamless interoperability between different hardware types and operating systems within the same facility.

---

5. Application Layer Implementation

5.1 Mobile Applications

Native mobile applications provide real-time monitoring and control:

Features:

- Live disinfection status dashboard
- Room-by-room verification display
- Push notifications for cycle completion
- Offline operation with later synchronization
- QR code scanning for device identification

Technical Implementation:

- React Native for cross-platform development

- Refinio SDK integration for data access
- Background synchronization services
- Encrypted local data storage

5.2 Desktop Applications

Desktop software offers comprehensive facility management:

Features:

- Multi-facility monitoring dashboard
- Detailed analytics and reporting
- Configuration management interface
- Data export and compliance reporting
- Windows filesystem integration (data accessible as folder structure)

Technical Implementation:

- Electron framework for cross-platform compatibility
- Direct Refinio node integration
- Local database synchronization
- File system abstraction layer

5.3 Web Applications

Browser-based interface ensures universal accessibility:

Features:

- Zero-installation access
- Role-based user management
- Real-time updates via WebSockets
- Mobile-responsive design
- Integration with existing hospital IT systems

Technical Implementation:

- Progressive Web Application (PWA)
- WebAssembly Refinio client
- Service worker for offline capability
- RESTful API with GraphQL subscriptions

---

6. Server Infrastructure

6.1 Hybrid Deployment Model

UVC.one supports flexible deployment options:

Cloud-First Architecture:

- Multi-region deployment for global access
- Auto-scaling based on facility count
- Managed service with 99.9% uptime SLA
- Automatic backup and disaster recovery

On-Premise Options:

- Private cloud deployment for sensitive data
- Air-gapped operation for high-security facilities
- Custom integration with existing IT infrastructure
- Local data sovereignty compliance

6.2 API Architecture

Comprehensive API layer enables integration:

RESTful APIs:

- Device management and configuration
- Verification data access
- User authentication and authorization
- Compliance reporting endpoints

GraphQL Interface:

- Real-time subscription updates
- Flexible data querying
- Batch operation support
- Schema-driven development

WebSocket Connections:

- Live facility monitoring
- Instant notification delivery
- Bi-directional device communication
- Low-latency status updates

---

7. Security and Compliance

7.1 Cryptographic Implementation

Device Identity:

- Each device generates unique Ed25519 key pairs
- Device identities registered with facility witness nodes
- Regular key rotation for enhanced security
- Hardware security module integration where available

Data Integrity:

- All verification records cryptographically signed
- Merkle tree structures for tamper detection
- Immutable audit trails with timestamp verification
- Multi-signature requirements for critical operations

7.2 Privacy Protection

Data Minimization:

- Only essential disinfection data collected
- Personal information excluded from verification records
- Anonymized analytics and reporting
- Configurable data retention policies

Access Control:

- Role-based permissions system
- Multi-factor authentication requirements
- API key management and rotation
- Audit logging for all access attempts

7.3 Regulatory Compliance

Healthcare Standards:

- HIPAA compliance for patient data protection
- HITECH security requirements
- ISO 27001 information security management
- FDA medical device software guidelines

International Standards:

- GDPR compliance for European operations
- SOC 2 Type II certification
- ISO 14155 clinical investigation standards
- IEC 62304 medical device software lifecycle

8. Federated Network Operations

8.1 Intra-Facility Federated Trust

Within-Facility Verification Network: The core innovation of UVC.one is establishing federated trust within a single healthcare facility through multiple independent verification nodes:

Device-Level Federation:

- Multiple embedded devices within each room form independent verification nodes
- Each device maintains its own cryptographic identity and verification capability
- Trust emerges from consensus among independent devices, not from a central authority
- No single device can falsify verification records without detection by peer devices

Room-Level Verification:

- Light source devices, environmental sensors, and witness devices independently attest to disinfection events
- Each device issues verifiable credentials describing its specific observations and interactions
- Multiple independent attestations create a comprehensive verification record
- Failed or conflicting attestations are preserved as part of the verification record for audit purposes

Facility-Wide Integrity:

- Witness devices aggregate verification data from multiple rooms and device types
- Cross-room verification patterns detect systematic failures or tampering attempts
- Distributed verification eliminates single points of failure within the facility
- Complete audit trail of all verification activities with cryptographic proof

8.2 Inter-Facility Federation Extension

Scaling to Multi-Facility Networks: The intra-facility federated trust architecture naturally extends to inter-facility verification networks:

Facility-as-Node:

- Each facility operates as a single federated node in the broader network
- Facility witness devices represent the facility's consensus in inter-facility communications
- Cross-facility verification builds on the established intra-facility trust foundation

- Multi-facility organizations can create private federated networks

Network Growth Patterns:

- **Hospital Systems**: Multiple facilities within the same healthcare organization
- **Regional Networks**: Independent facilities sharing verification standards
- **Research Collaborations**: Academic medical centers with verified data sharing
- **Supply Chain Verification**: Equipment manufacturers and healthcare facilities

Federated Benefits at Scale:

- Distributed compliance verification across facility networks
- Benchmarking and best practice sharing with cryptographic proof
- Network-wide reputation and trust scoring
- Resilient operation during individual facility network outages

8.3 Network Configuration and Security

Secure Provisioning:

- WLAN credentials distributed via W3C Verifiable Credentials
- Bluetooth Low Energy (BLE) for initial device configuration
- Zero-touch deployment with encrypted credential exchange
- Automatic network discovery and secure joining

Dual Network Architecture:

- **Encrypted Mesh**: Self-forming mesh network with end-to-end encryption
- **Infrastructure Integration**: Direct connection to facility WiFi/Ethernet
- **Automatic Failover**: Seamless switching between mesh and infrastructure modes
- **Bridge Nodes**: Devices can relay between mesh and infrastructure networks

Network Security:

- WPA3 encryption for infrastructure connections
- AES-256 encryption for mesh communications
- Certificate-based device authentication
- Network segmentation and traffic isolation

---

9. Implementation Considerations

9.1 Migration Strategy

Phased Deployment:

- Pilot installation with minimal device count
- Gradual expansion to additional rooms/facilities
- Integration with existing UV-C equipment where possible
- Staff training and change management support

Legacy Integration:

- API bridges to existing facility management systems
- Data export in standard formats (HL7, CSV, XML)
- Custom integration development services
- Backward compatibility maintenance

9.2 Operational Requirements

Network Infrastructure:

- **Flexible Network Configuration**: WLAN credentials configured via Verifiable Credentials and Bluetooth Low Energy (BLE)
- **Encrypted Mesh Operation**: Self-contained mesh network for isolated deployment
- **Full Infrastructure Integration**: Seamless integration with existing facility networks
- **Hybrid Deployment**: Support for both standalone mesh and integrated modes simultaneously

Maintenance:

- Quarterly device calibration recommended
- Annual security certificate renewal
- Software updates via over-the-air deployment
- 24/7 technical support availability

---

10. Future Development

10.1 Technology Roadmap

Short-term (6-12 months):

- Machine learning integration for predictive maintenance
- Advanced analytics dashboard with AI insights
- Integration with major facility management platforms
- Enhanced mobile application features

Medium-term (1-2 years):

- IoT sensor expansion beyond UV-C verification

- Artificial intelligence for optimal disinfection scheduling
- Integration with robotic disinfection systems

Long-term (2-5 years):

- Autonomous disinfection protocol optimization
- Predictive compliance risk assessment
- Integration with building management systems
- Expansion to other verification domains

10.2 Research Collaboration

UVC.one actively collaborates with academic institutions and research organizations to advance the state of federated verification systems in healthcare environments.

Our platform partner Refinio has e.g. contributed to

https://www.sciencedirect.com/science/article/pii/S2589750023001565

---

11. Conclusion

UVC.one represents a paradigm shift from trust-based to verification-based disinfection monitoring in healthcare facilities. By leveraging the Refinio federated platform and implementing a comprehensive multi-platform strategy, UVC.one provides healthcare organizations with cryptographically verifiable proof of disinfection operations while maintaining operational simplicity.

The federated trust architecture eliminates single points of failure while enabling cross-facility verification and compliance documentation that meets the highest regulatory standards. The multi-platform implementation ensures universal accessibility and seamless integration with existing healthcare IT infrastructure.

As healthcare facilities increasingly recognize the importance of verifiable infection control measures, UVC.one provides the technical foundation for a new generation of compliance and safety systems built on cryptographic proof rather than institutional trust.

References

1. Refinio Federated Platform: https://refinio.net
2. W3C Verifiable Credentials Data Model: https://www.w3.org/TR/vc-data-model/
3. W3C Decentralized Identifiers (DIDs): https://www.w3.org/TR/did-core/
4. UV-C Disinfection Guidelines, CDC: https://www.cdc.gov/coronavirus/2019-ncov/community/guidance.html
5. Medical Device Software Lifecycle Processes, IEC 62304
6. Health Insurance Portability and Accountability Act (HIPAA)
7. General Data Protection Regulation (GDPR)

Document Information:

- **Authors**: UVC.one Technical Team
- **Version**: 1.0
- **Date**: August 2025
- **Classification**: Public Technical Documentation
- **Contact**: technical@uvc.one