CELTIC-NEXT
Eureka Cluster

Project Report

CISSAN

Collective intelligence supported by security aware nodes

D6.2 Interface for 3rd parties' applications

Editor: Ilgin Safak, University of Jyväskylä

Abstract

This report describes the interfaces of third-party applications integrated into the CISSAN platform and explains how these applications interact with the CISSAN platform by means of clearly defined and interoperable interfaces. A general overview of the interfaces is provided, which includes the overall role of each integration within the CISSAN platform, and how these interfaces allow for data exchange and operations between these connected systems. The key interface specifications are provided as confidential annexes to this report, which includes: (1) Councilbox Custom Metadata blockchain API specification, which is part of the blockchain-based IoT network security framework; (2) specification of the integration of Mattersoft's public transportation vehicles' GNSS location information into the CISSAN platform by means of MQTT; (3) API specification of the integration between the Arctos Labs optimization solver and the CISSAN platform; and (4) specification of the Clavister smart grid integration into the CISSAN platform by means of MQTT.

Project **CISSAN**

Public

March 2026

Participants in project CISSAN are:

- University of Jyväskylä (coordinator)
- Affärsverken Karlskrona AB
- Arctos Labs Scandinavia AB
- Bittium Wireless Ltd
- Bittium Biosignals Ltd
- Blekinge Tekniska Högskolan
- Blue Science Park
- Clavister AB
- Councilbox Ltd
- Geodata ZT GmbH
- Mattersoft
- Mint Security Ltd
- Netox Ltd
- Nodeon Ltd
- Savantic AB
- Scopesensor Ltd
- Techinova AB
- Wirepas Ltd

CISSAN-Collective intelligence supported by security aware nodes

D6.2 Interface for 3rd parties' applications

Editor: Ilgin Safak, University of Jyväskylä

Project coordinator: Ilgin Safak, University of Jyväskylä

CELTIC published project result

Executive Summary

As a multi-domain and interoperable ecosystem, the ability of the CISSAN platform to integrate third-party applications in a consistent and secure manner is becoming ever more important for the achievement of scalable deployment and adoption. This report aims to meet this need by describing the interfaces for third-party applications and explaining how these applications are integrated into the CISSAN platform through well-defined and standardized interfaces. This report aims to provide an overview of the interfaces that are made available and their associated roles, with technical specifications included in the annexes for implementation purposes.

The CISSAN platform has four key integrations with partner systems, namely the API for the blockchain system that underpins the blockchain-based IoT network security framework, the Message Queuing Transport Telemetry (MQTT)-based integration of public transport Global Navigation Satellite System (GNSS) location data, the MQTT-based integration of smart grid data, and the API for the interaction between the optimization solver and the CISSAN platform. The interfaces that are made available through these four key integration domains are designed to allow heterogeneous partner systems to interact with each other in a cohesive and collective intelligence-driven security environment.

While the CISSAN platform does not provide a universal plug-and-play interface that can be used for all external systems due to security reasons, future partners can reduce their integration efforts by leveraging the reference interfaces defined in this report. Existing CISSAN interfaces could be reused in future integrations, which would help minimize design costs, development time, and technical uncertainty. This would help in the systematic integration of third-party applications with the CISSAN platform.

This report lays the foundation for interoperable integration in the CISSAN domain by presenting validated interfaces and integration patterns between major partner systems. This report creates value for CISSAN stakeholders by reducing technical risks and improving the efficiency of interoperability based on standards. This will ultimately contribute to the creation of robust and trustworthy cybersecurity solutions in the European Union (EU) in accordance with standards and regulations, enhancing cross-sectoral cooperation and digital resilience in the EU.

List of Authors

In alphabetic order by partner name:

- Lars-Göran Magnusson, Arctos Labs
- Anders Liden, Clavister
- Rodrigo Martínez, Councilbox
- Ilgin Safak, University of Jyväskylä
- Teemu Kemppainen, Mattersoft
- Oliver Bölin, Techinova

Table of Contents

Abbreviations

API	Application Programming Interface
ECDSA	Elliptic Curve Digital Signature Algorithm
HTTPS	Hypertext Transport Protocol Secure
GDPR	General Data Protection Regulation
GNSS	Global Navigation Satellite System
GUI	Graphical User Interface
IEC	International Electrotechnical Commission
IoT	Internet of Things
ISO	International Organization for Standardization
JWT	JSON Web Token
NIS	Network and Information Systems
REST	Representational State Transfer
TLS	Transport Layer Security
VPN	Virtual Private Network

Definitions

Metadata API	RESTful API layer providing device lifecycle management on top of the Eventchain blockchain

1 Introduction

1.1 Purpose and Scope

This report describes the interfaces between the CISSAN system and the systems of its partners that are integrated into the system, with a clear description of how these systems interact with each other through well-defined and standardized integration means. The discussion of the interfaces will focus on their use and application at the architectural level; however, technical details will be provided in the annexes of this document. The interfaces to be discussed include: (i) the metadata API of the Councilbox blockchain system underlying the blockchain-based IoT network security system, (ii) the Message Queuing Transport Telemetry (MQTT)-based interface for public transport Global Navigation Satellite System (GNSS) location data, (iii) the MQTT-based interface for smart grids data, and (iv) the Application Programming Interface (API) for the interaction between the optimization solver and the CISSAN system.

This report will focus on interfaces that are currently implemented and being used by the CISSAN platform; thus, the document will not aim to define a generic interface for any arbitrary system but will instead document existing, validated interfaces and will provide guidelines for reference use for future extensions of the system. The target audience of this document includes both technical and non-technical individuals who will benefit from understanding the integration landscape and the interface specifications available for use with the CISSAN platform.

1.2 Context in the CISSAN Platform

Third-party applications and systems are a key element of the CISSAN platform for providing data, services, and decision-making support to facilitate collective intelligence, automated security operations, and disaster recovery operations. The CISSAN platform is a modular and interoperable system where different components interact with each other through specific interfaces. The interfaces documented in this report define the specific points of integration between third-party systems and the CISSAN management server for the exchange of data and control information. By presenting the interfaces in the context of the CISSAN platform architecture, this report provides a description of how third-party systems assist with data ingestion, trust management, decision-making support, and disaster recovery operations. Technical details of the interfaces are provided in the annexes of this report.

1.3 Document Structure

This report is intended to provide a clear understanding of the way the CISSAN platform interfaces with other systems, the specifications of which are provided in annexes. Section 1 presents the purpose, scope, and context of this report within the CISSAN platform. Section 2 presents an overview of the approach that has been followed for third-party integration and provides an overview of the interfaces that have currently been implemented and how they can be reused and extended in future integrations. The conclusion section provides a brief summary of the main points that have been covered in the report.

2 Overview of Third-Party Integration

2.1 Integration Principles

CISSAN partner systems interact with the CISSAN platform based on a set of pragmatic principles that ensure reliability, interoperability, and maintainability, while minimizing integration costs and risks. Standardized and widely adopted technologies are used for integration, such as RESTful APIs and MQTT, to ensure that the CISSAN platform can reuse existing technologies, skills, and infrastructures. Well-defined interface contracts are used for integration, and detailed specifications are provided for better understanding and minimizing integration mistakes. Additionally, a modular approach is adopted for integration, where partner systems interact with core services through well-defined boundaries. Integrations were designed based on real-world use cases, including transportation, smart grids and automated disaster recovery, and interface definitions have been based on real-world interfaces and interaction patterns within the CISSAN platform.

The interfaces defined for integration, as described in this report, conform to industry standards that are widely accepted and followed, such as RESTful API principles, MQTT protocol for messaging-based data exchange, and API description standards such as OpenAPI. From a security and compliance perspective, the integration interfaces defined for this project conform to security and compliance requirements, as well as various security and standardization frameworks, such as Network and Information Systems (NIS) 2, General Data Protection Regulation (GDPR), and information and industrial security standards, as defined in the CISSAN D7.1 standardization action plan.

2.2 Security and Access Considerations

Security and access control are at the very center of the integration of the CISSAN partners' systems with the CISSAN platform, given the nature of the data and the services involved. The interfaces presented in this report are designed to adhere to the security-by-design and zero-trust models that the project is founded upon, allowing only authorized systems to have access to the platform’s services. There is a consistent application of security, especially in terms of authentication, authorization, and integrity, in all the APIs and messaging interfaces exposed. There are also tighter security measures in place for especially sensitive operations, such as device governance, trust state updates, and orchestration requests.

The security requirements, compliance, and implementation of the project are documented in the deliverable reports, CISSAN deliverable D2.3 - Implementation definition of the CISSAN architecture and distributed system elements and interfaces and CISSAN D7.1 - Standardization action plan, which are not repeated in this section.

Arctos Labs

The focus from Arctos Labs within CISSAN is technology development of core optimization modeling capabilities. In the context of CISSAN this concerns optimal distribution of security tasks over a CISSAN network. Therefore, aspects such as authentication, authorization, and accounting as well as cryptographic protocols in the context of distributed components have been purposely put aside.

The architectural decision to have a separate optimization solver server external to CISSAN Platform is primarily targeted at shortening the turnaround time and ease collaboration between involved parties.

In a hypothetical product environment, the optimization solver functionality could be wrapped within a software package and installed locally within e.g., the CISSAN Management Server thereby being subject to a different environment from security and access considerations.

In another hypothetical product environment, where the optimization solver in fact is deployed externally as a separate entity, the presumption is that similar mechanisms, addressing security and access control, as demonstrated by other partners can be applied without interfering with the core functionality.

Councilbox

The Metadata API enforces JSON Web Token (JWT) Bearer token authentication (HS256) with bcrypt password hashing and constant-time credential comparison to prevent timing attacks. Rate limiting is applied to authentication and event submission endpoints to mitigate brute-force and denial-of-service risks, and all input is validated against strict patterns to prevent injection attacks. All blockchain transactions are signed with Elliptic Curve Digital Signature Algorithm (ECDSA) secp256k1 and hashed with SHA3-256, ensuring authenticity, integrity, and non-repudiation. Client-to-API communication is protected with Hypertext Transport Protocol Secure (HTTPS)/Transport Layer Security (TLS).

The messaging layer follows a zero-trust architecture with dual RabbitMQ brokers (external for hub-to-master, internal isolated from the hub network) and per-hub queue credentials with regex-restricted permissions, preventing cross-hub access.

No personally identifiable information is stored on the blockchain: device identifiers are technical, and trust scores and anomaly data contain no personal data, ensuring GDPR compliance by design. A transaction content deletion mechanism allows the node administrator to erase the content of specific transactions while preserving the hash chain and Merkle tree integrity, supporting the right to erasure without breaking cryptographic verification.

Clavister

In the Clavister smart grid integration, security and access control are treated as core design requirements due to the criticality of OT environments and the sensitivity of security-relevant intelligence. The integration is implemented as a tightly scoped MQTT interface, where access is limited to CISSAN-specific client identities and constrained to only the topics and operations required for the exchange of correlated anomaly/fault events, in line with the principle of least privilege. Communication support protection using TLS, and authorization can be enforced through broker-side topic-level access control, ensuring that only approved parties can publish or subscribe to the relevant topics and that the interface does not expose unnecessary privileges or functionality beyond what is required for the integration.

Mattersoft

In the Mattersoft transportation integration, security and access control are implemented as core design requirements to ensure that public transport GNSS location data can be provided to the CISSAN platform without increasing operational risk to critical infrastructure systems. The integrated GNSS location information represents non-sensitive operational telemetry and largely corresponds to public vehicle positioning data; nevertheless, the interface is secured to protect data integrity, prevent misuse, and avoid the creation of unnecessary attack surfaces. The interface does not expose passenger data, ticketing data, or any personally identifiable information. The integration is implemented as a strictly read-only MQTT interface, where the CISSAN platform is authorized only to subscribe to predefined GNSSLocation and Runmonitoring topics and is explicitly denied any publish, retain, or administrative permissions in accordance with the principle of least privilege. All communication is protected using TLS, and access is restricted to CISSAN-specific client identities with topic-level Access Control Lists enforced at the broker. Authentication and authorization events (including failed attempts and access violations) are logged to support auditability, incident investigation, and compliance evidence. The upstream GNSS data pipeline up to the MQTT broker operates under an International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27001-certified information security management system, ensuring that established controls for risk management, access management, secure communications, monitoring, and incident handling are applied. These measures align with the security-by-design and zero-trust principles defined in the CISSAN architecture and enable secure integration of real-world transport telemetry into the platform for collective GNSS anomaly detection research.

Techinova

In the Techinova smart grid integration, IEC 62443 is strictly followed when considering development and deployment. Since the hardware and operating sytstem is low-level and tightly controlled, the ingration aligns naturally with IEC 62443 principles such as secure-by-design development. To align with strict zone and conduit seperation, a seperate firewall placement above NodeEye is used, and as an additional enforcement, a Virtual Private Network (VPN) tunnel is used to encrypt the NodeEye data. From an access perspective, NodeEye can only send data to the configured broker, it does not receive any data except 3 phase current and voltage data. It can also not act on any of the substation

equipment but only receive data to analyze, and runs fully bare metal, meaning no shells can be used from the device.

2.3 Summary of Available Interfaces

This section provides a brief summary of the interfaces currently implemented between the CISSAN platform and its partners, with a focus on their position with respect to the overall integration landscape. The interfaces (see interfaces list in Table 1) implemented concern: (i) the API of the blockchain system underlying the governance and management of the security state of devices for trust and device management purposes; (ii) the integration of public transport GNSS location data via MQTT for obtaining the GPS data needed for performing anomaly detection on the buses locations via the CISSAN platform; (iii) the API enabling the communication between the optimization solver and the platform for obtaining the optimal distribution of security tasks across the networked devices in the CISSAN platform; and (iv) the integration of smart grid telemetry data via MQTT for managing the smart grid devices' statuses on the CISSAN platform. The interfaces thus cover the key aspects of the ingestion, governance, and coordination of the data handled by the CISSAN platform. The technical specifications of the interfaces are provided in annexes; this section provides a brief overview of their role with respect to the CISSAN architecture.

Table 1. List of CISSAN interfaces

Interface	Partner name	Purpose	Technology	Specification
Custom metadata Blockchain API	Councilbox	Device ledger, trust, device governance	REST	Annex 1
GNSS (Transportation)	Mattersoft	Vehicle location data ingestion	MQTT	Annex 2
Optimisation Solver	Arctos Labs	Task distribution requests/results	REST	Annex 3
Smart Grid	Clavister	Grid telemetry ingestion	MQTT	Annex 4
Smart Grid	NodeEye	Grid telemetry ingestion	MQTT	Annex 5

Custom metadata Blockchain API (Councilbox)

The management server integrates with the Councilbox blockchain via a REST client. It uses token-based authentication and calls the API to register devices, update global trust scores, and send blacklist and unblock events and uses a deadband to limit traffic. The device registry syncs device status (registered, blacklisted, trust) from the blockchain on startup and when discovering devices; the trust analyzer pushes trust updates and blacklist/unblock events. Integration is optional and controlled by configuration.

GNSS (Transportation) (Mattersoft)

Vehicle location data from Mattersoft is ingested via MQTT. The management server connects to the Mattersoft broker to receive data. In the management server web interface, the coordinates are shown with their respective anomalies if any.

Optimisation Solver (Arctos Labs)

The management server uses a REST client to talk to the Arctos optimisation solver. The pipeline manager builds a payload (devices, tasks, constraints, optional telemetry), sends it with HTTP POST then creates a job with HTTP POST request and polls for the result. The returned task–device assignment is turned into a deployment manifest and enacted via the CISSAN Orchestrator. The solver URL and job timeout are set in configuration.

Smart Grid (Clavister)

Clavister grid telemetry and anomaly events are published to the shared MQTT broker over a VPN tunnel. The management server daemon does not subscribe to or process these topics; the management Graphical User Interface (GUI) subscribes to them and displays them. Integration is therefore at the broker and web interface level, not inside the daemon.

Smart Grid (Techinova)

NodeEye grid telemetry is published to the shared MQTT broker. The CISSAN Management Server daemon does not ingest or process NodeEye data; instead, the CISSAN Management GUI subscribes to the NodeEye topics and displays them. Integration is at the broker and web interface level.

2.4 Reuse and Extension of the Integration Interfaces

Integration patterns, technologies, and interface structures in the underlying CISSAN partner integrations are designed with reusability in mind, allowing them to be adapted for future extensions of the CISSAN platform. With standard technologies such as REST APIs and MQTT, as well as well-structured data models, it is possible for new partners to align their systems with the existing interfaces, rather than creating a new integration from scratch. Future integrations can leverage the existing specifications as a real-world template, adapting message structures, interfaces, or workflows as needed for their specific domain, while still allowing them to leverage the core services of the CISSAN platform.

For instance, a new partner with IoT telemetry from another domain can reuse the current MQTT-based integration specification by mapping their message formats and topics to the patterns described, without requiring modifications to any of the current services. Similarly, a new optimization component can be integrated with the system by mapping to the established REST API patterns defined for the optimization solver interface, adjusting only their respective data models to fit their unique capabilities.

3 Conclusion

This report describes the third-party interfaces to connect partner systems to the CISSAN platform and gives a general overview of all current integration points, where the specifications are presented in its annexes. Through the description of APIs and interfaces using MQTT protocol to connect to the blockchain system, public transports GNSS data, smart grids data, and the optimisation solver, this report shows how different systems are currently integrated in the CISSAN platform and how these integrations can help to improve data ingestion, device governance, and decision-making processes. This structure of this document has been chosen to ensure that all stakeholders, regardless of their technical level, can easily understand the integration landscape without being exposed to implementation details in the main body of this document. Moreover, this document also shows how these interfaces and integration patterns can be reused as a basis to design and implement new integrations of third-party applications to the CISSAN platform in the future. This document therefore establishes a solid foundation to ensure consistent, safe, and sustainable integration of third-party applications to the CISSAN platform.

References

[1] D4.4 Updated Network Logging System, CISSAN Project, 2025

[2] RFC 7519 - JSON Web Token (JWT), IETF, 2015

Annexes

D6.2 Annex 1 - Metadata API Specification

D6.2 Annex 2 – Public transport vehicle GNSS location data integration with the CISSAN platform

D6.2 Annex 3 – Optimisation API Specification

D6.2 Annex 4 – Smart grid data integration

D6.2 Annex 5 – Smart grid data integration