Setting up Western Balkans Electronic Register of Road Undertakings

WBRRU System Requirements

Transport Community Permanent Secretariat
Masarikova 5, 11000 Belgrade
Serbia

Table of Contents

List of Figures

List of Tables

No table of figures entries found.

List of Abbreviations

BPMN	Business Process Modelling and Notation
CA	Contracting Authority (TCT Permanent Secretariat)
EC	European Commission
EU	European Union
WBRRU	Western Balkans Register of Road Transport Undertakings
ICT	Information – Communication Technology
IT	Information Technology
ERRU	European Register of Road Transport Undertakings
MS	Member States (of EU)
RP	TCT Regional Partner/ Regional Party/ Regional Participant: Albania, Bosnia and Herzegovina, Kosovo*, Montenegro, North Macedonia, Serbia
SEE	South East Europe
TCT	Transport Community Treaty
TEN-T	Trans-European Transport Networks
TODIS	Transport Observatory Database/ Information System
WB	Western Balkans

* This designation is without prejudice to positions on status and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

1 Objectives of the WBRRU System

The Western Balkans Register of Road Transport Undertakings (WBRRU) is designed as a regional digital infrastructure platform to support structured data exchange among the six Western Balkan Regional Partners (WB6) – Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia – and to enable integration with the European Register of Road Transport Undertakings (ERRU).

The purpose of WBRRU is to serve as a regional interoperability gateway that mirrors the core principles and message structure of ERRU, while accommodating the diversity of national systems across the WB6 region. The platform will facilitate real-time, secure, and standardized electronic communication of regulatory data between competent transport authorities.

This specification outlines the technical and functional architecture of the WBRRU system, focusing on two major interfaces: the WBRRU Interface for National Registers, and the ERRU Interface for connectivity with the EU network. WBRRU will not maintain a centralized licensing register or perform risk scoring; instead, it acts as a compliant messaging and validation hub.

This document also addresses national configuration flexibility, digital permit exchange integration, normalization logic per RP (Regional Partner), security governance, access control, and technical monitoring required for cross-border compliance transparency. This specification is also targeted toward technical contractors and integrators, to enable consistent implementation in line with EU interoperability standards.

2 Architecture Overview

The WBRRU system is logically segmented into components that together enable seamless message transmission, transformation, validation, and monitoring. The architecture is cloud-native and based on microservices principles, ensuring modularity, scalability, and resilience.

At its core, WBRRU consists of two primary interfaces: the WBRRU Interface and the ERRU Interface. These interfaces manage inbound and outbound messages from WB6 national registers and from EU member state counterparts respectively.

Supporting these interfaces is a messaging engine responsible for schema validation, transformation, queueing, and retry logic. A normalization engine operates in tandem, allowing RP-specific data mappings to conform to ERRU standards. A system settings console, available only to WBRRU administrators, ensures flexible updates to normalization profiles, endpoint configurations, and rule enforcement.

The security and access control framework supports mutual TLS authentication, role-based permissions, and audit traceability. Technical monitoring is facilitated through a real-time dashboard displaying per-RP integration status, throughput, error rates, and exportable logs. Other modules, such as a digital permit exchange service, are incorporated to extend interoperability into customs and inspection domains like SEED+.

3 Stakeholders and Roles

The WBRRU platform is used by multiple stakeholders involved in regulating, maintaining, and exchanging data on road transport undertakings. The core roles are tailored to the structure and responsibilities outlined in the EU ERRU framework, adapted for regional deployment in the Western Balkans.

There are three main categories of stakeholders in the WBRRU system:

1. RP Authority Users: These users represent competent transport regulatory bodies in each WB6 RP. They are responsible for integrating their national systems with WBRRU, sending and receiving compliance messages, monitoring the status of interactions with other states, and configuring data normalization rules specific to their RP.
2. WBRRU System Administrators: Managed centrally by TCT, this role governs system-wide configurations, normalization mappings, security settings, and manages the connection with the EU ERRU node. Admins also perform monitoring, analytics, user management, and audit logging.
3. Auditors and Inspectors: These users can view records, logs, and validation statuses without modifying data. Their access is essential for transparency, EU reporting, and inspection processes.

User role definition is enforced through an access control module, which ensures that only authorized actors can initiate, update, or monitor system functions based on strict role-based permissions.

4 Functional Architecture

The WBRRU functional architecture is modular and focused on high-availability and compliance-driven messaging operations. Its design facilitates two-way, secure communication between WB6 national systems and the EU ERRU environment, through well-defined interfaces and message processing layers.

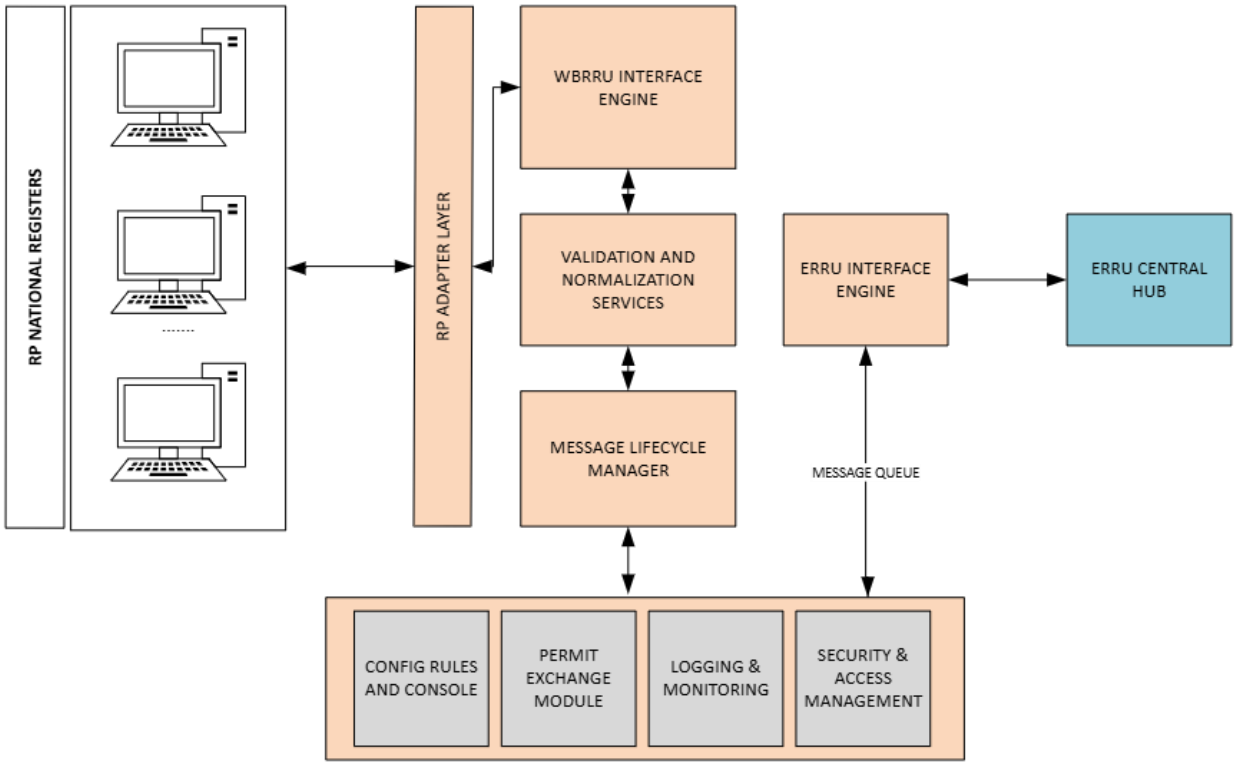
Core components include the WBRRU Interface for national data exchange, the ERRU Interface for EU compliance routing, a centralized Message Lifecycle Manager for validation and tracking, and a configuration module for defining RP-specific normalization rules. Supplementary modules support digital permit exchange, logging, monitoring, and access management.

Each national register communicates with WBRRU through its respective RP adapter. These adapters normalize input and output messages according to pre-defined schemas and transformation logic managed by the WBRRU settings console. WBRRU internally uses a message queue and validation engine to ensure consistency before further dispatching to the ERRU node.

Outbound messages to ERRU conform strictly to the OneWay and ReqRes patterns as defined in the latest ERRU WSDL and XML schemas. These include CGR (Check of Good Repute), NCR (Notification of Check Tesult), CTUD (Check Transport Undertaking Data), NU (Notification of Unfittness). The platform manages digital signing, error handling, and delivery receipts.

To accommodate legal, technical, and procedural variations across the WB6, the Normalization & Partner Configuration Module stores and applies field mapping rules for every RP. These configurations can be updated centrally without downtime and ensure that national differences do not impact EU interoperability.

Monitoring dashboards allow system administrators to track delivery status per RP, detect errors or message bottlenecks, and export reports for governance bodies. Security is enforced at every layer with TLS 1.2+, OAuth tokens, digital certificates, and full audit logging of system activity.



This modular and configurable architecture ensures that the WBRRU platform remains resilient, extensible, and aligned with evolving EU digital transport compliance mandates.

5 Functional Requirements

RP Adapter Layer

Handles protocol mediation, format translation, and secure connectivity with RP systems.

This architectural layer enables each RP to continue operating their existing infrastructure with minimal changes while achieving full interoperability through the WBRRU ecosystem

Functions:

- Inbound message receiver (REST/SOAP listener)
- Message schema mapping (RP XML -> Internal XML)
- Error detection & wrapping
- Secure channel establishment (HTTPS w/ client cert)
- Message enrichment (national context ID injection)

REQ-1	The RP Adapter Layer serves as the primary integration point between each Regional Partner's National Register and the WBRRU core system. It acts as a gateway that securely receives incoming messages using REST or SOAP protocols and manages all aspects of protocol translation and schema conversion.

REQ-2	Each adapter ensures the conformance of national messages with the internal WBRRU data model, transforming RP-specific XML into an intermediate canonical format. Security is enforced through HTTPS connections with mutual certificate authentication, guaranteeing the authenticity of each national sender.
REQ-3	The adapter also enriches messages with additional metadata, such as a national context identifier or unique RP code, which allows downstream systems to apply RP-specific processing rules.
REQ-4	Error detection routines within the adapter pre-validate structural correctness and flag invalid messages for review.
REQ-5	Faulty messages are wrapped in standardized error responses and logged for diagnostic purposes. This decouples the national systems from ERRU complexity while enabling seamless integration
REQ-6	The adapter's modular nature ensures maintainability and simplifies future updates to schema or communication protocols.

WBRRU Interface Engine

Normalizes inbound messages from RPs and prepares outbound messages.

This structured and rule-driven interface layer enables the rest of the WBRRU platform to handle messages efficiently, maintain message integrity, and ensure full compliance with both national and EU-level data exchange expectations.

Functions:

- Validation against RP schema (XSD/JSON Schema)
- Application of normalization rules via XSLT
- Tag transformation for ERRU compatibility
- Store original + normalized version for auditing

REQ-7	The WBRRU Interface Engine is responsible for accepting, processing, and preparing validated inbound messages from RP Adapters for further handling within the system. This component performs a series of structural and semantic checks, validating each incoming message against RP-specific XML Schema Definitions (XSD) and applying business logic to detect malformed or non-compliant content.
REQ-8	Once validated, the interface engine invokes the normalization process using transformation templates written in XSLT or another rule-execution engine to ensure the message conforms to the internal canonical WBRRU schema. This standardized format enables consistent internal processing and interoperability with downstream modules
REQ-9	The interface engine performs tag mapping and restructuring to align with ERRU semantics while preserving the traceability of the original message

	through versioned storage. Both the source message and the normalized version are securely stored to support future audits and diagnostics
REQ-10	The engine also categorizes messages based on their operational type (e.g., infringement report, license status change, license check) and tags them with metadata that determines routing priorities and processing deadlines.

ERRU Interface Engine

Translates normalized messages into ERRU-compliant formats and handles routing.

This component ensures WBRRU's full alignment with EU legal and technical interoperability requirements

Functions:

- XML generation using latest WSDL schema for CGR, NCR, CTUD, NU
- Message type dispatcher (OneWay, ReqRes handlers)
- Connection manager to ERRU central hub
- ERRU message response parser
- Retry queue with exponential backoff on failure

REQ-11	The ERRU Interface Engine enables compliant message routing between the WBRRU system and the EU's central ERRU node. Once a message has been normalized and processed internally, this component generates outbound XML messages conforming strictly to the latest ERRU WSDL specifications.
REQ-11	The engine supports both synchronous (ReqRes) and asynchronous (OneWay) messaging paradigms, allowing flexibility in how different message types (e.g., CGR, NCR, CTUD,NU) are transmitted and acknowledged
REQ-11	A message dispatcher classifies and queues each message accordingly and assigns it to the appropriate transmission pipeline. The interface engine features a connection management layer responsible for authenticating and maintaining sessions with the ERRU hub, handling retries using exponential backoff strategies in case of communication failures. Upon receiving responses from the ERRU hub, such as acknowledgments or validation errors, the engine parses the content and updates the status within the Message Lifecycle Manager
REQ-11	The ERRU Interface also supports transformation of response messages back into RP-compliant formats if needed. This ensures traceability and feedback consistency for Regional Partners. Built-in conformance validation tools test each message before transmission, ensuring that only structurally sound and semantically correct data is exchanged with the EU network

Message Lifecycle Manager (MLM)

Tracks and manages each message from origin to response.

This mechanism not only supports operational continuity but also reinforces the legal validity of cross-border data exchanges, offering both transparency and control in a high-compliance environment.

Functions:

- Message status tracking (ingested, validated, normalized, sent, acknowledged)
- Timestamped message journal entries
- Error routing and manual override mechanisms
- Correlation ID tagging for bilateral traceability

REQ-12	The Message Lifecycle Manager (MLM) is the central coordination service responsible for tracking every message processed by the WBRRU system. It maintains a stateful log of each message's journey—from initial receipt through validation, transformation, dispatch, and acknowledgment.
REQ-13	Every state transition is time-stamped and associated with a unique correlation ID, allowing administrators and national authorities to trace a message's status and history in real time. This function is critical for compliance with audit requirements and for resolving transmission or validation errors.
REQ-14	In the event of failure, the MLM logs the issue and invokes error handling mechanisms such as retry queues, notification alerts, and escalation workflows. Additionally, it enables manual override actions for competent users when automatic processing fails.
REQ-15	The MLM interfaces directly with both the ERRU and RP Adapter layers to ensure consistent bilateral traceability. By maintaining a canonical status model and providing API access to lifecycle queries, the MLM acts as the authoritative source of truth for message delivery accountability.

Validation and Normalization Services

Rule-based engine applying structural and content validation.

A dual-engine approach decouples national data specifics from internal logic and guarantees harmonized data exchange. Together, validation and normalization serve as the quality gate of the entire WBRRU ecosystem, ensuring that only complete, accurate, and conformant data flows into the ERRU and partner systems.

Functions:

- Syntactic validation (XSD, WSDL conformance)
- Semantic checks (e.g., valid license number range, operator status check)
- Normalization rule executor (per RP logic using rule DSL)

- Message rejection with detailed error codes

REQ-16	The Validation and Normalization Services component ensures that every message exchanged through WBRRU complies structurally and semantically with both EU-wide ERRU standards and RP-specific business rules.
REQ-17	It consists of two subsystems: the validation engine and the normalization engine. The validation engine applies syntactic rules such as XSD and WSDL conformance checks to confirm the message structure is correct.
REQ-18	It also runs semantic validations like ensuring that operator IDs exist, license statuses are permissible, and dates are logically consistent. If a message fails, detailed error codes are generated and routed back to the originating system with human-readable feedback.
REQ-19	Once validated, the normalization engine transforms RP-specific message formats into a standardized internal schema using transformation logic, usually implemented via XSLT or domain-specific language (DSL) rule scripts.
REQ-20	These transformations are dynamically driven by the RP code and allow each partner to maintain their data model while achieving interoperability. The service logs all validation attempts and outcomes for compliance monitoring.

Configuration & Rules Console

Admin interface to manage system and RP-level behavior.

The Configuration & Rules Console is a critical enabler of system flexibility, empowering central governance teams to manage a multi-jurisdictional architecture without jeopardizing operational continuity or compliance integrity.

Functions:

- RP normalization rules (load/update/test)
- Interface endpoint management (add/update/deprecate)
- Security certificate repository and lifecycle
- Toggle modules per RP (permit exchange on/off)
- Admin audit log and approval workflows

REQ-21	The Configuration & Rules Console is the administrative control panel for managing system-wide and RP-specific behavior within the WBRRU architecture. It provides a secure web-based interface through which authorized users can define, modify, and test normalization rules, schema mappings, and routing behaviors per Regional Partner.

REQ-22	This console is vital for system maintainability, allowing administrators to respond rapidly to legislative or procedural changes without altering backend code.
REQ-23	Key features include a rules editor with versioning support, endpoint registration and deprecation tools, and certificate lifecycle management for each RP's secure communication channel. It also allows toggling modules, such as enabling or disabling digital permit exchange for specific partners.
REQ-24	The console maintains a full audit trail of all configuration changes, including who made the change, when, and what the previous values were. An approval workflow ensures that any modifications are peer-reviewed before activation.
REQ-25	Built-in testing tools allow admins to simulate message processing with new rules before deployment, ensuring validation and transformation logic behaves as expected.

Logging & Monitoring Subsystem

Ensures observability and regulatory compliance.

Collectively, this component ensures system resilience, provides early warnings, supports root cause analysis, and enables efficient troubleshooting in a distributed, high-compliance environment.

Functions:

- Message log aggregator with filter/search API
- System health dashboards (latency, throughput, failure rate)
- User access logs (role, timestamp, IP, action)
- Alerting engine (email/SMS/Slack integration)

REQ-26	The Logging & Monitoring Subsystem is the backbone of observability and operational assurance within WBRRU. It collects, stores, and analyzes detailed logs and metrics from all functional components, ensuring transparency, traceability, and real-time awareness of system performance.
REQ-27	Message logs record every transaction, including sender, receiver, timestamp, processing state, and associated errors, with support for advanced filtering and querying via API or user interface. These logs are immutable and retained according to EU compliance requirements, enabling forensic audits and dispute resolution.
REQ-28	Monitoring functions leverage metrics from infrastructure (CPU, memory, network) and application-level indicators (message latency, queue length, success/failure ratios) visualized through dashboards. Prometheus and Grafana are typically used to provide dynamic monitoring, while alert rules trigger notifications via email, SMS, or collaboration platforms like Slack if thresholds are breached (e.g., failed message rate >5% over 5 minutes).

REQ-29	Anomaly detection rules flag unusual patterns such as traffic surges or recurrent validation errors. The subsystem also tracks user activity logs, noting login events, data access, and configuration changes to support accountability and GDPR logging.

Security & Access Management

Protects data, interfaces, and user access.

This component forms the foundation of trust for RP data exchange, enforcing both legal obligations and operational safeguards.

Functions:

- OAuth2 server with JWT tokens
- MFA enforcement on admin roles
- TLS/SSL across all internal/external communications
- RBAC enforcement (user group -> permission set)
- GDPR compliance support (data subject logs, deletion API)

REQ-30	The Security & Access Management component safeguards the integrity, confidentiality, and availability of all data and services within the WBRRU ecosystem. It enforces a multi-layered security model combining authentication, authorization, encryption, and audit mechanisms. User authentication relies on OAuth2 protocols with support for multi-factor authentication (MFA) for administrative roles.
REQ-31	Access control is role-based (RBAC), ensuring users can only view or modify data pertinent to their responsibilities. Permissions are assigned based on pre-defined user groups such as national register operators, system administrators, and compliance auditors. TLS/SSL encryption is mandatory for all internal and external communications, preventing man-in-the-middle attacks and ensuring message confidentiality during transit.
REQ-32	Additionally, sensitive data at rest (e.g., license numbers, infringement records) is encrypted using industry-standard algorithms. The module integrates with centralized certificate authorities and maintains lifecycle management for credentials per RP.
REQ-33	Audit trails capture every security-relevant action including logins, permission changes, and data access attempts. The system also supports GDPR compliance, enabling data subjects to request access logs or trigger deletion processes through a secure API.

REQ-34	Periodic security audits and automated vulnerability scans ensure compliance with evolving cybersecurity standards.

Digital Permits Exchange Module

The Digital Permit Exchange Module is a strategic component of the WBRRU architecture, designed to streamline the verification of international road transport permits, including Dangerous Goods transport across WB6 RPs.

Each Regional Partner (RP) may use this module for sharing existing transport permits through authenticated and structured electronic processes.

Core features of the module include:

REQ-35	Structured digital forms for permit metadata sharing and validation
REQ-36	PDF and XML document generation with embedded e-signatures compliant with eIDAS standards.
REQ-37	API endpoints for SEED+ or other validation systems to query permit status.
REQ-38	Lifecycle status tracking (issued, used, revoked, expired) with event timestamps
REQ-39	Dashboard view of permits by status and RP
REQ-40	Security and authenticity of permits are enforced via digital certificate integration, and the system supports both online validation via API and QR-code based offline verification tools. The permit registry remains national, but metadata is shared via WBRRU for cross-border visibility where agreements permit.
REQ-41	The module enables integration with customs and border control systems (e.g., SEED+) for permit validation during inspections.
REQ-42	This module enhances transparency and operational efficiency in managing international authorizations and aligns with EU expectations for digital document exchange in transport operations.

6 ERRU Interoperability

WBRRU is engineered to support complete interoperability with the EU ERRU system, following specifications defined by the European Commission and MOVEHUB messaging protocols. The ERRU Interface module enables bidirectional message exchange between WB6 registers and EU Member State counterparts.

This module forms the legal and operational backbone of the WBRRU system, ensuring that all WB6 Regional Partners remain interoperable with EU monitoring and compliance mechanisms under Regulation (EC) 1071/2009 and subsequent implementing acts.

Supported message types include:

REQ-43	NCR (Notify Check ResultNotify Check Result) CGR (Check Good Repute) CTUD (Check Transport Undertaking Data) NU (Notification of Unfittness)…
REQ-44	All messages are validated against the latest ERRU XML schema and must conform to the WSDL message catalogue defined in Annex II. Upon transmission, messages are digitally signed and routed over mutual TLS connections using certificate-based authentication.
REQ-45	The interface includes a message queue with delivery status labels (Pending, Sent, Acknowledged, Failed), ACK/NACK processing, and retry logic with configurable thresholds. Messages received from the EU are validated, parsed, and routed back to the appropriate RP using reverse transformation rules.
REQ-46	A dedicated error handler and notification submodule logs any failed transmissions and alerts system administrators. The interface supports message logging, archiving, and export in compliance with EU retention and audit regulations.
REQ-47	Interoperability is continuously tested against EU conformance testing environments to ensure ongoing compliance and reliability. As EU technical specifications evolve, WBRRU administrators are responsible for updating schema versions and adapter configurations using the built-in configuration tools.

7 National Register Integration

WBRRU is designed to operate in tandem with the National Electronic Registers (NERs) of the WB6 RPs. Since the maturity of these systems varies, the system provides flexible integration options to accommodate both developed electronic systems and RPs still using manual or semi-digital workflows.

This integration flexibility ensures that all WB6 Regional Partners, regardless of IT capacity, can participate in regional and EU-wide compliance frameworks and maintain sovereignty over their national registers.

REQ-48	Each WB6 RP will interact with WBRRU via a dedicated RP adapter, which transforms local data formats and service calls into a common messaging structure aligned with WBRRU and ERRU specifications. The adapters support both RESTful and SOAP-based interactions and provide customizable endpoint mappings and field normalization.
REQ-49	For RPs with operational NERs (e.g., Serbia, Bosnia and Herzegovina), WBRRU supports real-time message exchanges and queued message processing using secure, authenticated API calls. These Regional Partners can send messages directly and receive ACK/NACK feedback asynchronously. WBRRU also provides a secure web-based interface (frontend) for all WBRRU use cases.
REQ-50	For RPs still developing or lacking NERs (e.g., Kosovo, Montenegro), WBRRU provides a secure web-based interface for message composition, review, and dispatch. This ensures minimal disruption to cross-border operations and helps standardize workflows while full integration is developed.
REQ-51	The system includes tools providing Excel connectivity for bulk data import (e.g., from Excel or CSV), that is being digitally signed from within the WBRRU application and offers onboarding support such as schema validation testbeds, sample messages, and integration guides. Each partner is responsible for their national endpoint security, while WBRRU maintains centralized oversight of authentication tokens and message dispatch outcomes.

8 Access Control and User Management

WBRRU implements a robust and centralized access control framework to ensure the integrity and confidentiality of all transactions, records, and configuration settings within the system.

These requirements below, ensure that WBRRU can serve as a trusted and auditable interoperability platform, supporting lawful data exchange across borders while preserving national sovereignty and compliance with EU digital security standards.

REQ-52	Access to WBRRU is role-based and follows the principle of least privilege. Each user is assigned to one of the following roles: - NR_SYSTEM: Users from National Registers who are allowed to send, receive, validate, and query messages related to road transport undertakings. - WBRRU_ADMIN: System administrators responsible for partner configuration, message monitoring, normalization rule management, and audit oversight. - AUDITOR: Read-only access for third-party observers or EU-compliant auditors, with permission to export logs, view message trails, and access configuration states.

REQ-53	Authentication is handled through Firebase Auth or an equivalent SSO provider, supporting multi-factor authentication and periodic session revalidation. Each user action is logged with a timestamp, IP address, user ID, and description of the event. Logs are immutable and stored with encryption-at-rest.
REQ-54	Administrative rights are restricted to a small number of WBRRU administrators who use the system settings module to control normalization logic, message routing configurations, error thresholds, and queue management policies.
REQ-55	Access to WBRRU services is enforced through mutual TLS authentication, and all API calls must be signed and validated before acceptance. The system includes tools for role audit, user deactivation, and credential rotation to ensure long-term security compliance.

9 Data Model

The WBRRU data model underpins the integrity and traceability of all information exchanged between national registers and EU authorities. It is designed to support a decentralized but standardized architecture, ensuring that each national register can represent its legal entities while maintaining compatibility with EU data structures.

Core entities in the data model include Operator, Manager, Vehicle, Infringement, and Message. Each of these entities is stored as a record with associated attributes that conform to ERRU and national register schemas. Relationships between entities (e.g., operators and their vehicles or transport managers) are explicitly modeled and validated.

Key Fields by Entity[1]:

- Operator: WBRRU ID, legal name, national register ID, RP, license type, license status, repute status, contact information.
- Manager: Manager ID, name, nationality, CPC certificate ID, associated operator(s), employment status.
- Vehicle: Registration number, VIN, type, capacity, ownership, compliance certificates, linked operator.
- Infringement: Message ID, severity level, infringement code, issuer, date of incident, vehicle ID, enforcement body.
- Message: Message type (CTUD, CGR, etc.), originating RP, timestamp, status, retry count, signed payload.

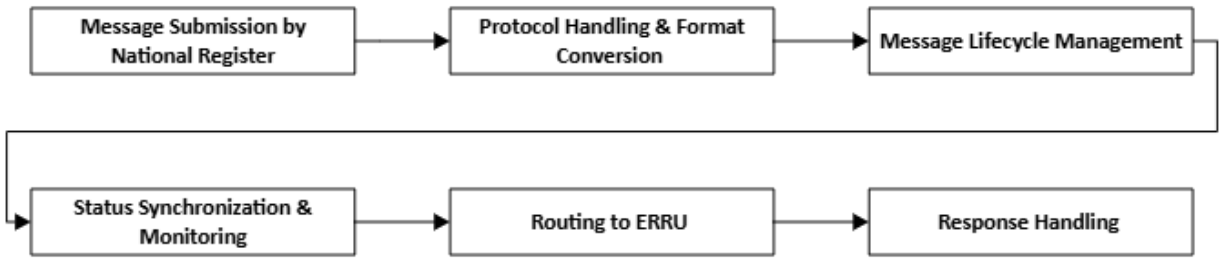
The data model is schema-driven and can be expanded or updated via migration scripts and schema registries. Field-level validations ensure that each record conforms to national and EU legal requirements. Cross-field checks are enforced to avoid conflicts (e.g., a manager assigned to multiple disqualified operators).

[1] See Annex I for full list of fields per message type.

All data is stored in an encrypted, cloud-based NoSQL or hybrid SQL/NoSQL format, optimized for message throughput, searchability, and reporting. Data models are versioned and documented using OpenAPI and XSD/JSON schema formats.

11.1 Data Flow

The WBRRU Data Flow below outlines the complete transactional lifecycle of a message exchanged between a Regional Partner (RP) and the European ERRU system. This structured sequence ensures accuracy, traceability, and legal compliance for every data exchange.



Message Submission by National Register: Each RP's national system sends a message to the WBRRU system through its designated RP Adapter. This submission may include a request (e.g., CGR, CTUD, or NCR) or an administrative update.

Protocol Handling & Format Conversion: The RP Adapter authenticates the incoming request using secure certificates, converts the protocol if necessary (e.g., REST to internal API), and transforms the RP-specific XML into WBRRU's internal canonical format. If schema validation fails, an error response is generated and returned immediately.

Validation & Normalization: The internal message undergoes two layers of checks—syntactic validation against structural rules (XSD/WSDL) and semantic validation based on business logic (e.g., license status, operator ID). After passing validation, the message is normalized through rule-based transformations tailored per RP.

Message Lifecycle Management: The validated and normalized message is passed to the Message Lifecycle Manager, where it is logged, assigned a unique message ID and correlation tag, and stored in the lifecycle journal.

Routing to ERRU: The ERRU Interface Engine generates an ERRU-compliant message in latest XML schema and selects the appropriate messaging pattern (OneWay for CGR, ReqRes for CTUD, etc.). It dispatches the message to the ERRU central hub using the pre-established secure channel.

Response Handling: Upon receipt of an acknowledgment (ACK) or a functional error (NACK), the system logs the response, updates the lifecycle status, and prepares a response message if needed. This message is converted back to RP-compliant format and returned to the originating national system.

Status Synchronization & Monitoring: The full interaction is recorded for traceability, while system health and processing status (e.g., queue time, round-trip latency) are tracked through the Logging & Monitoring Subsystem. Alerts are issued if anomalies are detected.

11.2 WBRRU Use Cases

❖ CHECKING THE GOOD REPUTE OF TRANSPORT MANAGERS

When verifying through WBRRU, whether a transport manager has been declared in one of the RPs as unfit to manage the transport activities of an undertaking, RPs shall perform a broadcast CGR search by sending a Check Good Repute Request. The responding RPs shall reply to the request by sending a Check Good Repute Response.

❖ NOTIFICATION OF CHECK RESULTS

For the notification of a serious infringement through ERRU, the RP or EU Member State of infringement shall send a Notification of Check Result to the RP or EU Member State of establishment with the information about the infringement. Infringements not categorised in Directive 2006/22/EC or in Regulation (EC) No 1071/2009 shall not be notified.

When no infringement has been detected during the check, a Notification of Check Result shall be sent to the RP or EU Member State of establishment consisting of the information about the clean check as set out in Annex I.

A check shall not be considered as a clean check when minor infringements have been detected. Where only minor infringements have been detected during the check, a Notification of Check Result shall be sent to the RP or EU Member State of establishment consisting of information about the date and number of minor infringements detected.

The Notification of Check Result shall be sent as soon as possible, and at the latest within 6 weeks of the final decision on the infringements detected, if any, providing the information set out in Annex I.

The RP or EU Member State of establishment shall reply to the Notification of Check Result by sending a Notification of Check Result Response, as soon as possible and at the latest within 6 weeks of the final decision on the matter, informing of which, if any, of the penalties imposed. If such penalties are not imposed, the Notification of Check Result Response shall include the reasons therefor. The Notification of Check Result Response shall not be necessary when the Notification of Check Result refers to a clean check.

In all cases, a Notification of Check Result and a Notification of Check Result Response shall be acknowledged by means of a Notification of Check Result Acknowledgement.

❖ CHECKING THE TRANSPORT UNDERTAKING DATA

When checking through WBRRU any of the transport undertaking data, an RP or an EU Member State shall send a Check Transport Undertaking Data Request to the RP or EU Member State of establishment.

The RP or EU Member State of establishment shall reply by sending a Check Transport Undertaking Data Response.

Queries sent through the CTUD functionality shall be carried out by entering either the name of the transport undertaking, its licence number or the number of any of the certified true copies, or the registration number

of any of its vehicles, without being necessary to perform a query by typing more than two of the aforementioned entries.

Responding RP or EU Member State, when searching in their registers the result of a CTUD request on the basis of either the licence or the registration number of a vehicle, shall take measures to adapt the format of the data in the search request to the format of the data in the national register.

In particular, responding RP or EU Member State, when searching in their registers the result of a CTUD request on the basis of either the licence or the registration number of a vehicle, shall ignore special characters such as hyphens or slashes. Blanks shall also be ignored.

Responding RP shall return to the requesting party all the information that is available through the XML messages defined in Annex I and II. If a part of the information requested has not been found, this shall not preclude responding RP to provide the rest of the information requested that is available in the register, including the registration number of vehicles.

❖ NOTIFYING THE UNFITNESS OF A TRANSPORT MANAGER

When a transport manager has been declared to be unfit in one RP, that RP may send a Notification of Unfitness to all other RPs.

In all cases, a Notification of Unfitness shall be acknowledged by means of a Notification of Unfitness Acknowledgement.

❖ CHECKING BILATERAL PERMITS VIA THE DIGITAL PERMIT MODULE

When checking bilateral permits through WBRRU DIGITAL PERMIT MODULE any of the transport undertaking data, an RP shall send a Check Transport Undertaking Data Request to the RP of establishment.

The RP of establishment shall reply by sending a Check Transport Undertaking Data Response.

Queries shall be sent through the Digital Permit Module being similar to CTUD functionality (CTUD-DP) and shall be carried out by entering either the name of the transport undertaking, its licence number or the number of any of the certified true copies, or the registration number of any of its vehicles, without being necessary to perform a query by typing more than two of the aforementioned entries.

Responding RP, when searching in their registers the result of a CTUD-DP request on the basis of either the bilateral permit or the registration number of a vehicle, shall take measures to adapt the format of the data in the search request to the format of the data in the national register.

In particular, responding RP, when searching in their registers the result of a CTUD-DP request on the basis of either the licence or the registration number of a vehicle, shall ignore special characters such as hyphens or slashes. Blanks shall also be ignored.

Responding RP shall return to the requesting RP all the information that is available through the XML messages defined. If a part of the information requested has not been found, this shall not preclude responding RP to provide the rest of the information requested that is available in the register, including the registration number of vehicles.

10 Technical Architecture

WBRRU is designed as a microservice-based cloud architecture, ensuring modularity, extensibility, and resilience. Each core function is encapsulated in a containerized service, with shared infrastructure components handling networking, security, and logging.

Major Components of Technical Architecture:

1. Gateway Services: REST and SOAP endpoint gateways accepting inbound messages and forwarding validated traffic to internal queues.
2. Message Processor: Central validation and dispatch engine for message routing, normalization, and queuing.
3. Normalization Engine: A rule-based transformer for adapting RP-specific data into ERRU-compliant schema.
4. Data Store: Firestore or a hybrid document-structured DB for storing all core records.
5. Messaging Bus: FIFO and dead-letter queues for reliable message delivery and retry mechanisms.
6. Audit Logger: Immutable ledger for logging user actions, message lifecycle events, and system updates.
7. Admin Console: Web-based UI for WBRRU administrators to manage configurations, monitor queues, and export reports.
8. Integration Connectors: RP-specific adapters for Serbia, Albania, etc., plus a MOVEHUB-compliant ERRU node connector.

Deployment and Infrastructure:

1. Hosted on a scalable, container-based cloud environment (e.g., Kubernetes on GCP or AWS).
2. All services support horizontal scaling and failover.
3. TLS 1.2 or higher enforced on all external and internal communications.
4. X.509 certificate-based authentication for mutual trust with national and EU nodes.

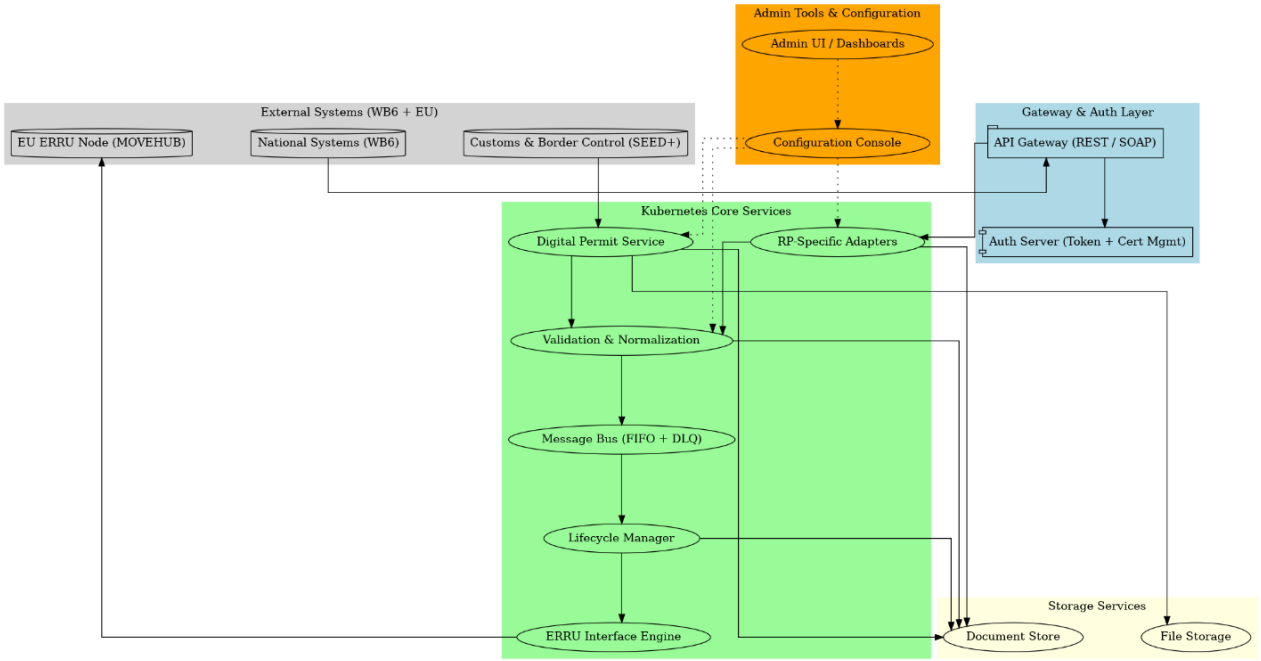


Figure 1: WBRRU Technical Architecture (deployment view)

The above architecture ensures that WBRRU remains agile and compliant with EU infrastructure guidelines, enabling seamless upgrades, patch deployments, and RP-specific customizations.

11 Security and Compliance

The WBRRU system shall adhere to EU and international standards for information security, ensuring that all data exchanges, user interactions, and system operations are protected against unauthorized access, manipulation, and breaches.

Security Principles to be Applied:

- Confidentiality: All data transmitted between national registers and WBRRU shall be encrypted using TLS 1.2 or higher and secure VPN connection. Internal services shall use mutual TLS with certificate-based authentication.
- Integrity: Messages must be digitally signed before being transmitted, ensuring that payloads cannot be altered in transit. All signed messages must be verified on receipt. National systems will use the PKI certificates provided by TCT for the purposes of securing the transmission of messages between the national system and WBRRU.
- Availability: System architecture shall include failover services, message retry logic, and queue monitoring to maintain service continuity.
- Accountability: All access and changes must be logged, including user identity, time, origin IP, and affected resource. Logs must be immutable and stored securely for a minimum of five years.

Access Control:

- User accounts must be protected by Firebase Authentication or equivalent, supporting MFA, token expiration, and user role management.
- Only users with proper roles from restricted infrastructure and VPN connection can perform operations such as configuration updates, message validation overrides, or system restarts.

GDPR and Data Sovereignty:

- The system enforces per-RP data compartmentalization, ensuring RP data is not accessed by third parties without legal basis.
- Personally identifiable information is minimized, encrypted at rest, and subject to national data privacy rules and GDPR compliance.

Regulatory Compliance:

- The system shall be built in alignment with Regulation (EU) 2016/679 (GDPR), Regulation (EU) 910/2014 (eIDAS), and the NIS Directive (EU) 2016/1148 on cybersecurity.

Ongoing security assessments, penetration testing, and audit reviews will be required to maintain compliance with evolving EU and national regulations.

12 System Scalability

WBRRU is architected for regional scalability to accommodate growth in data volume, participating authorities, and functional capabilities without service degradation.

Key Scalability Strategies:

1. Stateless Services: Core services (validation, messaging, normalization) are stateless and can scale horizontally using container orchestration platforms (e.g., Kubernetes).
2. Load Balancing: All external interfaces and critical services use load balancers to distribute incoming traffic and avoid overload.
3. Elastic Queues: The messaging system uses FIFO queues with autoscaling and dead-letter handling to support burst traffic and delivery retries.
4. Sharded Data Storage: National data can be partitioned into separate collections or databases per RP to ensure efficient access and data segregation.
5. Modular Expansion: New message types, digital workflows, or RP-specific integrations can be added as separate microservices without impacting existing operations.

Cloud-native deployment allows each RP to scale independently based on their volume of operations, while WBRRU's central coordination service ensures message orchestration remains consistent.

Performance is continuously monitored and benchmarked to maintain compliance with defined SLAs (e.g., <1s response time, 99.9% uptime). This scalability ensures the platform can adapt to include new RPs or additional modules such as risk analysis or mobility intelligence in future phases.

13 Monitoring and Logging

The WBRRU platform includes an integrated monitoring and logging framework that enables system administrators and auditors to maintain visibility into the health, performance, and integrity of the application and message workflows.

Monitoring Tools:

- Real-time dashboards track message throughput, queue sizes, system uptime, API latency, and error rates per RP.

- Notifications and alerts can be configured to inform system operators of issues such as failed message dispatch, unresponsive endpoints, or invalid message structures.
- System health checks are run periodically on each microservice, with results accessible via the admin panel and optionally integrated with third-party monitoring tools (e.g., Google Cloud Monitoring, Prometheus).

Logging Functions:

- Each user action, message state transition, and system configuration update is logged with a unique ID, timestamp, user reference, and operation summary.
- Logs are stored using an encrypted write-once, read-many (WORM) architecture, ensuring compliance with audit traceability requirements.
- Export functions allow filtered logs to be downloaded in CSV or JSON format for external inspection or reporting.
- Anomaly detection tools flag suspicious or unexpected patterns, such as repeated message failures or access attempts outside authorized hours.

The monitoring and logging module ensures operational reliability, supports auditing obligations, and provides a robust foundation for future automation and AI-driven analytics.

14 SEED+ Integration

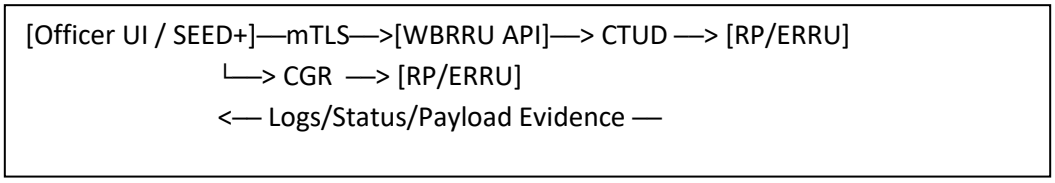
In this chapter, a concise implementation and operations view for integrating **SEED+ (Customs & Border)** with WBRRU to perform real-time permit verification using **CTUD** (undertaking data) and **CGR** (good repute) checks, is provided.

Actors & Systems

The flow involves SEED+, which starts the verification; WBRRU, which orchestrates the CTUD and CGR calls, applies retries and ordering where required, and records evidence; Regional Partners, which expose message endpoints for undertaking and transport-manager data; and the ERRU network, which carries authoritative messages between member-state nodes.

14.1 High-Level Architecture

SEED+ communicates with WBRRU over mutual TLS, with certificates governed through the administrator controls. Messaging follows the ERRU 3.5 SOAP/XML profile and uses asynchronous acknowledgments where the protocol expects them. WBRRU centralises the orchestration while preserving partner-specific behaviour such as retries, FIFO ordering, and dead-letter queues.



14.2 Border Sequence (Happy Path)

1. **SEED+** sends `VerifyPermit` with: Inspection/Crossing ID, Operator Name, Vehicle Plate, optional RP.
2. **WBRRU** returns `202 Accepted` (or equivalent) and writes a **Transaction Log** entry.
3. **CTUD** request dispatched → **CTUD Response** received (`statusCode=Found`).
4. **CGR** request dispatched → **CGR Response** received (`fitnessStatus=Fit`).
5. **WBRRU** aggregates results → returns **Final Status** to SEED+ and seals an **e-signature** summary with timestamps.

14.3 Minimal Data Set (from SEED+)

The request should carry a UUID-formatted inspectionId, the operatorName, the vehicleRegistration, and an optional requestedByRP using ISO-2 country codes; where available, officerId and location metadata can be included for traceability.

14.4 Interfaces (Indicative)

SEED+ calls an inbound WBRRU endpoint such as POST /api/seed/verify with a JSON payload and receives an immediate acceptance response, after which SEED+ can poll GET /api/seed/verify/{inspectionId} or register a webhook for completion events. WBRRU issues CTUD and CGR SOAP requests to partner endpoints over mTLS and stamps each message with technicalId, workflowId, sentAt, from, and to headers in line with ERRU conventions.

14.5 Timeouts & SLAs (operational targets)

The system must comply with the following performance objectives under normal operating conditions:

- **Initial Acceptance Response Time**:
  ≤ 300 ms
- **CTUD (Create/Update/Delete) Round Trip**:
  - P50 (median): ≤ 1.5 seconds
  - P95 (95th percentile): ≤ 4 seconds
- **CGR (Control/General Request) Round Trip**:
  - P50 (median): ≤ 1.5 seconds
  - P95 (95th percentile): ≤ 4 seconds
- **End-to-End Final Status Delivery** (including message processing and acknowledgment, subject to Regional Partner system availability):
  - P95: ≤ 8 seconds

14.6 Security & Compliance

Mutual TLS is enforced between SEED+ and WBRRU, with certificate lifecycles tracked and alerted on before expiry. Messages are signed in accordance with ERRU profiles, and both platforms should maintain accurate clocks via NTP to avoid signature drift. Data minimisation applies throughout: only the fields required to run CTUD and CGR are transmitted, and any exports or views surface redacted content. All events are logged immutably with workflow and technical identifiers and with hashes of payloads so that evidence can be verified without retaining full raw content.

14.7 Logging & Evidence

Every verification produces a linked sequence of transaction-log entries that show what was sent, what was received, and the resulting status. Authorised users can open a payload viewer to inspect content for troubleshooting; routine storage prefers a digest plus a location pointer, which provides auditability while reducing exposure of personal data.

14.8 Operations, Failures & Requirements

14.8.1 Operational Procedures

To start a check, officers confirm that SEED+ displays a connected state, submit the VerifyPermit request, and monitor the live transaction log until a final status is shown. If no match is returned, they try an alternative identifier such as a permit number or an explicit partner, and where results remain elusive they follow the local refusal or manual-inspection procedure. If the outcome indicates an unfit manager or an invalid licence, officers apply the refusal or secondary-check policy, capture evidence references, and inform their supervisor.

Initiate check: Ensure SEED+ shows **Connected** → send VerifyPermit → monitor **Transaction Log** → act on final status.

If No Match / Not Found

- Re-try with alternative identifier (Permit ID, RP). If still not found, follow refusal or manual inspection SOP.

If Unfit/Invalid

- Apply refusal/secondary check policy. Capture evidence IDs and notify supervisor.

14.8.2 Failure Modes & Standard Responses

When a CTUD timeout occurs, the likely cause is a slow or unavailable partner endpoint. WBRRU performs configured retries and moves the item to the dead-letter queue when attempts are exhausted; the officer is informed and advised to conduct a manual check while a ticket is raised with the partner. If a CGR search returns no record, the usual explanation is a mismatch in the name or date of birth; WBRRU returns a final Not Found status and the operator revalidates inputs before deciding whether to escalate. If mutual TLS fails, the most common reason is an expired or untrusted certificate; WBRRU rejects the connection, raises a critical alert, and the certificate is replaced before tests resume. If a schema is invalid because mandatory fields are missing or mis-shaped, WBRRU raises an Error Notification and quarantines the message; the sender fixes the payload and resubmits via SEED+. Where ordering is required and FIFO was not enabled, conflicting outcomes can arise; enabling FIFO for the affected partner resolves the discrepancy for subsequent traffic.

Failure	Likely Cause	WBRRU Behaviour	Operator Action
`CTUD timeout`	RP endpoint slow/down	Retries → DLQ on exhaust	Inform officer; advise manual check; create ticket to RP
`CGR not found`	Name/DOB mismatch	Return final status `NotFound`	Validate inputs; if persistent, escalate
`mTLS failure`	Expired/invalid cert	Reject inbound; raise Critical Alert	Replace cert; retest
`Schema invalid`	Missing fields	EN raised; message quarantined	Fix payload; re-submit via SEED+
`Ordering needed`	FIFO disabled	Conflicting outcomes	Enable FIFO for affected RP

The same failure modes and standard responses apply horizontally to

14.8.3 Data Protection Notes (Field Handling)

WBRRU retains the inspection identifier, the final decision, and the timestamps necessary for audit while avoiding persistent storage of full personal details unless a legal basis exists. Logs are subject to retention limits—such as one hundred and eighty days for routine records—with extended retention applied only when an incident investigation requires it.

14.8.4 Acceptance Criteria (SEED+)

- **AC-1** Given valid inputs, when SEED+ calls `/api/seed/verify`, then WBRRU returns **Accepted** within **300 ms** and a log entry appears.
- **AC-2** When CTUD and CGR both return `Found`, then final status is `` with consolidated summary.
- **AC-3** When CTUD returns `NotFound`, then final status is `` and CGR is skipped.
- **AC-4** When CGR returns `Unfit` or certificate `Invalid`, then final status is `` and reason is included.
- **AC-5** During RP outage, requests are **retried** and on exhaust moved to **DLQ** with actionable error text.
- **AC-6** Payload viewer displays **redacted** content or stored hash reference; access is role-restricted.
- **AC-7** All timestamps are ISO-8601 UTC; headers include `workflowId` and `technicalId`.

14.8.5 Functional Requirements — SEED+

Category	Requirement ID	Description
SEED+ GEN (General)	FR SEED GEN 01	The system shall expose an inbound verification endpoint for SEED+ (/api/seed/verify or equivalent) using mTLS.
	FR SEED GEN 02	The system shall persist a Transaction Log with entry types sent, received, and status, linked by workflowId.
	FR SEED GEN 03	The system shall compute and store payload digests (hashes) and locations for evidence.
SEED+ FLOW (CTUD→CGR Orchestration)	FR SEED FLOW 01	The system shall dispatch CTUD first; only dispatch CGR when CTUD statusCode=Found.
	FR SEED FLOW 02	The system shall aggregate CTUD and CGR outcomes into a single final status with reasons.
	FR SEED FLOW 03	The system shall allow configuration of target RP override per request or per partner default.
SEED+ RELIABILITY	FR SEED REL 01	The system shall apply configurable retries with exponential backoff for RP timeouts.
	FR SEED REL 02	After retry exhaustion, the system shall route the request to DLQ with the last error and metadata.
	FR SEED REL 03	The system shall support FIFO per RP when enabled to preserve message order.
SEED+ SECURITY	FR SEED SEC 01	The system shall enforce mutual TLS and reject connections with expired or untrusted certificates.
	FR SEED SEC 02	The system shall redact PII in logs and restrict payload viewer access by role.
	FR SEED SEC 03	The system shall timestamp all events in UTC and verify acceptable clock skew.
SEED+ UX (Operational UI)	FR SEED UX 01	The UI shall display Connected/Degraded/Down integration status.
	FR SEED UX 02	The UI shall require Inspection ID, Operator Name, and Vehicle Plate before enabling Initiate Border Check.
	FR SEED UX 03	The UI shall show a live transaction log with icons and allow opening a Payload Viewer dialog.

14.8.6 Test Cases

Test Case	Description
T1	Happy Path: Valid inputs → CTUD Found → CGR Fit → final = All Clear (<8s P95).
T2	Undertaking Not Found: CTUD NotFound → final = Not Found; CGR skipped.
T3	Unfit Manager: CTUD Found → CGR Unfit → final = Not Permitted.
T4	RP Timeout: Simulate RP down → retries → DLQ after exhaust; alert raised.
T5	mTLS Expired: Reject at edge; audit entry with reason; status = Security Error.

15 User Interfaces

The WBRRU system includes dedicated user interfaces tailored to different user groups, ensuring intuitive access to functionality, role-based visibility, and multilingual support across all participating Regional Partners.

Operator Dashboard (National Authority Users):

- Message queue tracking for in-progress and failed dispatches.
- Search and filtering tools for operators, vehicles, and transport managers.
- Inline document uploads for licenses, CPC certificates, and permits. Files are digitally signed and stored in a local folder within each Authority's infrastructure.

Operator Dashboard has the following additional operational and functional requirements:

Category	Requirement ID	Description
OP-GEN (General)	**FR-OP-GEN-01**	The system shall present three areas: Message Status, Undertaking Information (CTUD), and Good Repute (CGR).
	FR-OP-GEN-02	The system shall provide clear validation messages for incomplete or invalid inputs.
	FR-OP-GEN-03	The system shall use consistent visual indicators (badges) for success/error, risk bands, and statuses.
OP-MSG (Message Status)	**FR-OP-MSG-01**	The system shall provide filters for **Regional Partner**, **Message Type** (CTUD/CGR), and **Status** (Success/Error).
	FR-OP-MSG-02	The system shall display a table with **Message ID**, **Date & Time**, **Type**, **Requested By**, and **Status**
	FR-OP-MSG-03	The system shall allow selecting a message row to view **details** and the full **XML payload**
	FR-OP-MSG-04	The system shall provide a **Resend Message** action from the message details view.
	FR-OP-MSG-05	The system shall indicate the currently selected message in the list.
OP-CTUD (Undertaking Information)	**FR-OP-CTUD-01**	The system shall require at least **two** of the following before submission: Operator Name, Community Licence Number, Vehicle Licence Plate.
	FR-OP-CTUD-02	The system shall allow selecting a **Target Regional Partner/Country** for the query
	FR-OP-CTUD-03	Upon success, the system shall display an **Undertaking Profile** including name, legal form, address, country
	FR-OP-CTUD-04	The system shall display **Risk Band** and **Risk Rating** with appropriate visual indicators

Category	Requirement ID	Description
	FR-OP-CTUD-05	The system shall display **Statistics** including number of vehicles and employees per undertaking
	FR-OP-CTUD-06	The system shall present **Licence** details including number, type, status, validity dates, and issuing authority
	FR-OP-CTUD-07	Where infringements exist, the system shall display a **summary banner** and provide a dialog listing ID, final decision date, location, category, type, penalty, and execution status
	FR-OP-CTUD-08	Where no infringements exist, the system shall display a clear **None Found** confirmation
OP-CGR (Good Repute)	**FR-OP-CGR-01**	The system shall allow searching any field as per the minimum data requirements (Annex I and chapter 11.2).
	FR-OP-CGR-02	The system shall prevent any other submission until the search is comp
	FR-OP-CGR-03	Upon success, the system shall display **Fitness Status** (Fit/Unfit) and **Certificate Validity** (Valid/Invalid) with visual indicators
	FR-OP-CGR-04	The system shall display manager details (names, date of birth, CPC number) and summary of managed undertakings/vehicles when available
	FR-OP-CGR-05	When no record is found, the system shall present a neutral “Not Found” message
OP-NCR (Notification of Check Result)	**FR-OP-NCR-01**	The system provide fumctionality as described in NCR use case and as per the minimum data requirements (Annex I and chapter 11.2).
OP-AUD (Audit & Usability)	**FR-OP-AUD-01**	The system shall timestamp messages in the list and details view
	FR-OP-AUD-02	The system shall preserve entered form values within the session until cleared or a new search is performed
	FR-OP-AUD-03	The system shall provide accessible labels for inputs and buttons and support keyboard navigation within tables and dialogs

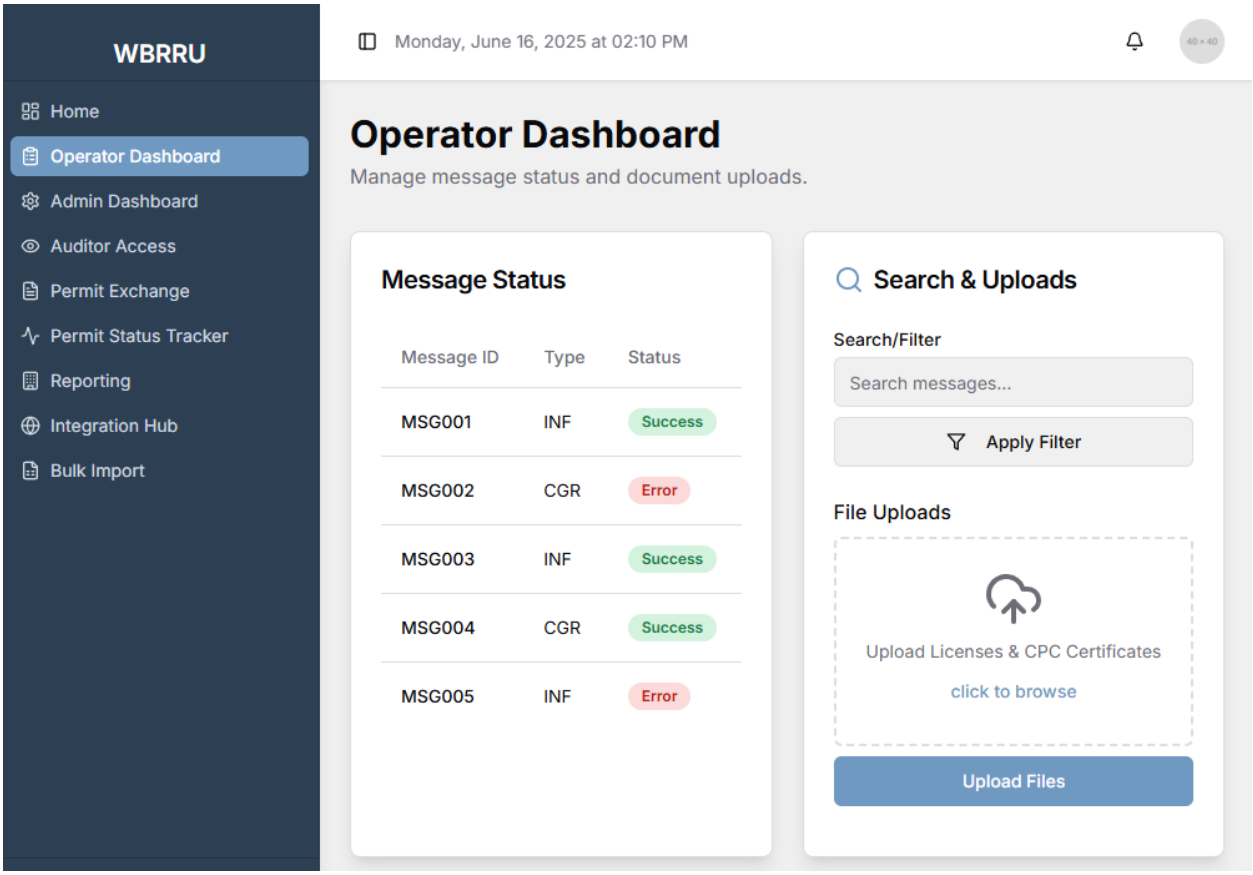


Figure 2: Regional Partner Operator Dashboard

Administrator Dashboard (WBRRU Admins):

- RP-level configuration settings including normalization profiles, endpoint URLs, enabled message types, and retry policies.
- Real-time message traffic monitor with error logging, status filters, and dispatch control tools.
- System-wide event log viewer and user management console.
- Alerts configuration panel and system health widget integration.

Operator Dashboard has the following additional operational and functional requirements:

Category	Requirement ID	Description
General & Cross-Cutting (GEN)	**FR-GEN-01**	The system shall allow the user to select a Regional Partner (RP) filter that applies consistently across all tabs.
	FR-GEN-02	The system shall reset dependent UI context when the selected RP changes (e.g., clear staged certificate uploads, reset mapping view to default message type).

Category	Requirement ID	Description
	FR-GEN-03	The system shall display status indicators (badges) for common states (Active/Paused, Connected/Pending/Error, Valid/Invalid/Warning, Risk band).
	FR-GEN-04	The system shall provide user-visible confirmations for key actions (e.g., Save, Retry, Delete) via on-screen notifications.
	FR-GEN-05	The system shall prevent irreversible actions without explicit user intent (e.g., require a click on Delete; no implicit destructive operations).
	FR-GEN-06	The system shall preserve unsaved edits within the current session until the user cancels or saves.
RP Configuration (RPC)	**FR-RPC-01**	The system shall allow toggling an RP Service Status between Active and Paused.
	FR-RPC-02	The system shall allow editing the RP Endpoint URL.
	FR-RPC-03	The system shall allow editing the Retry Count (integer) used for transient failures.
	FR-RPC-04	The system shall allow enabling/disabling FIFO processing per RP.
	FR-RPC-05	The system shall allow enabling/disabling Dead-Letter Queue (DLQ) per RP.
	FR-RPC-06	The system shall allow enabling/disabling individual message categories (e.g., CGR, CTUD, CCL, NCR, NU, NRR, NLM, NTM, ACK, EN, RSI, CTM, ADM) per RP.
	FR-RPC-07	The system shall allow enabling/disabling functional modules per RP (e.g., Permit Exchange, Good Repute, Customs Integration, Infringements).
	FR-RPC-08	The system shall provide a Save Changes action that commits RP configuration updates.
	FR-RPC-09	The system shall provide a Cancel action that discards unsaved RP configuration edits.
	FR-RPC-10	The system shall display current certificate metadata for the selected RP when a certificate is configured.
ERRU XML Mapping (MAP)	**FR-MAP-01**	The system shall allow selecting a message type for mapping (e.g., Common Header, CGR Request/Response, CTUD Request/Response, etc.).
	FR-MAP-02	The system shall display, for the selected type, a list of WBRRU fields with descriptions and grouping (Required/Request/Response/Acknowledgement).
	FR-MAP-03	The system shall allow editing a Partner Field value for each WBRRU field.
	FR-MAP-04	The system shall create a new mapping entry if a WBRRU field has no existing Partner Field mapping when edited.

Category	Requirement ID	Description
	FR-MAP-05	The system shall provide an Auto-map function that, given a JSON schema with a prefix, generates Partner Field names for all fields in the selected message type.
	FR-MAP-06	The system shall apply the auto-mapped values without altering fields that the user has subsequently edited within the same session.
	FR-MAP-07	The system shall persist in mapping edits when the user saves RP configuration.
Data Sources per RP (DS)	**FR-DS-01**	The system shall allow selecting a Source Type for National Registry and Permit Exchange (e.g., API, Excel File, MS Access, Not Configured).
	FR-DS-02	The system shall display a Status indicator for each data source (Connected, Pending, Error, Not Configured).
	FR-DS-03	The system shall allow editing a Connection String/URL/Path for each data source when the type is not “Not Configured”.
	FR-DS-04	The system shall disable editing of connection details when the data source type is “Not Configured” and clear any existing value on change to that state.
	FR-DS-05	The system shall provide a Test Connection action for each data source when it is configurable.
Certificate Management (CERT)	**FR-CERT-01**	The system shall display the current Issuer, Subject, Expiry Date, and Status (Active/Expired) for the RP certificate when present.
	FR-CERT-02	The system shall allow uploading a new certificate file in .pfx, .p12, or .cer format.
	FR-CERT-03	The system shall allow removing the current certificate from the RP configuration.
	FR-CERT-04	The system shall require Save Changes to commit any staged certificate upload or removal.
	FR-CERT-05	The system shall provide visual feedback when a certificate is Expired or missing.
Rules Console (RUL)	**FR-RUL-01**	The system shall allow filtering Rule Sets by RP or viewing All Partners.
	FR-RUL-02	The system shall display for each rule: Name, Module, Last Modified date, and Applicability (RP/Global).
	FR-RUL-03	The system shall allow selecting a rule to load its content into an editor view.
	FR-RUL-04	The system shall allow editing the rule content and saving changes.
	FR-RUL-05	The system shall update the rule’s Last Modified date upon successful save.

Category	Requirement ID	Description
	FR-RUL-06	The system shall provide Add New Rule with fields Name, Module, and Content, and shall assign the rule to the selected RP or Global if no RP is selected.
	FR-RUL-07	The system shall provide a Cancel action to exit rule editing without saving changes.
	FR-RUL-08	The system shall provide a Test Rule area to input sample data and request an evaluation (where implemented).
Live Traffic (LIV)	**FR-LIV-01**	The system shall display a line chart showing recent requests and errors over time.
	FR-LIV-02	The system shall allow filtering the chart by RP and show default aggregate data when no RP is selected.
	FR-LIV-03	The system shall display a legend and interactive tooltip with data values.
	FR-LIV-04	The system shall update the chart dataset when the RP filter changes.
Data Import (IMP)	**FR-IMP-01**	The system shall allow selecting an RP to associate with the imported data.
	FR-IMP-02	The system shall provide upload areas for (a) National Registry Data and (b) INF/CGR Messages supporting CSV/Excel file types.
	FR-IMP-03	The system shall allow clearing a selected file prior to import.
	FR-IMP-04	The system shall present a Validation Summary table with row number, field name, status (Valid/Warning/Invalid), and message.
	FR-IMP-05	The system shall present a Preview of parsed rows (at least 10) including key columns such as Registry ID, Entity Name, Licence Number, Risk Band, and RP.
	FR-IMP-06	The system shall support the actions Cancel, Validate Only, and Import Now.
	FR-IMP-07	The system shall provide a Connect Data Source panel with Source Type, connection details, and actions Test Connection and Connect and Preview.
	FR-IMP-08	The system shall display Import Guidelines & Resources including schema references and best-practice notes.
Logs (LOG)	**FR-LOG-01**	The system shall allow filtering Logs by RP and provide a text Search input.
	FR-LOG-02	The system shall display logs in a table with Level, Message, Timestamp, and Partner columns.
	FR-LOG-03	The system shall present a scrollable log view for extended lists.
	FR-LOG-04	The system shall provide a View All Logs action.
Users	**FR-USR-01**	The system shall allow filtering Users by RP.

Category	Requirement ID	Description
	FR-USR-02	The system shall display a user table including User ID, Name, Role, Partner, Status, and Actions.
	FR-USR-03	The system shall provide an Add New User action.
	FR-USR-04	The system shall provide an Edit action per user (where implemented).
	FR-USR-05	The system shall display user Status as a badge (Active/Inactive).
Alerts (ALT)	**FR-ALT-01**	The system shall allow filtering Alerts by RP.
	FR-ALT-02	The system shall display alerts with level (Critical/Warning), message, timestamp, and partner.
	FR-ALT-03	The system shall provide appropriate actions per severity (e.g., Acknowledge for Critical, View Details for Warning).
	FR-ALT-04	The system shall provide a Configure Alert Rules action.
Dead-Letter Queue (DLQ)	**FR-DLQ-01**	The system shall allow filtering DLQ items by RP.
	FR-DLQ-02	The system shall display DLQ items with Message ID, Partner, Error, Timestamp, and Actions.
	FR-DLQ-03	The system shall provide a View action to inspect the raw payload of a DLQ item.
	FR-DLQ-04	The system shall provide Retry and Delete actions for DLQ items.
	FR-DLQ-05	The system shall display an empty-state message when no DLQ items match the current filter.
Audit & Record-Keeping (AUD)	**FR-AUD-01**	The system shall timestamp configuration changes and rule updates and display the most recent update date where relevant.
	FR-AUD-02	The system shall provide sufficient context (e.g., RP name, rule name) in confirmations and views to support traceability.
	FR-AUD-03	The system shall surface certificate status (Active/Expired) conspicuously to support proactive renewal.

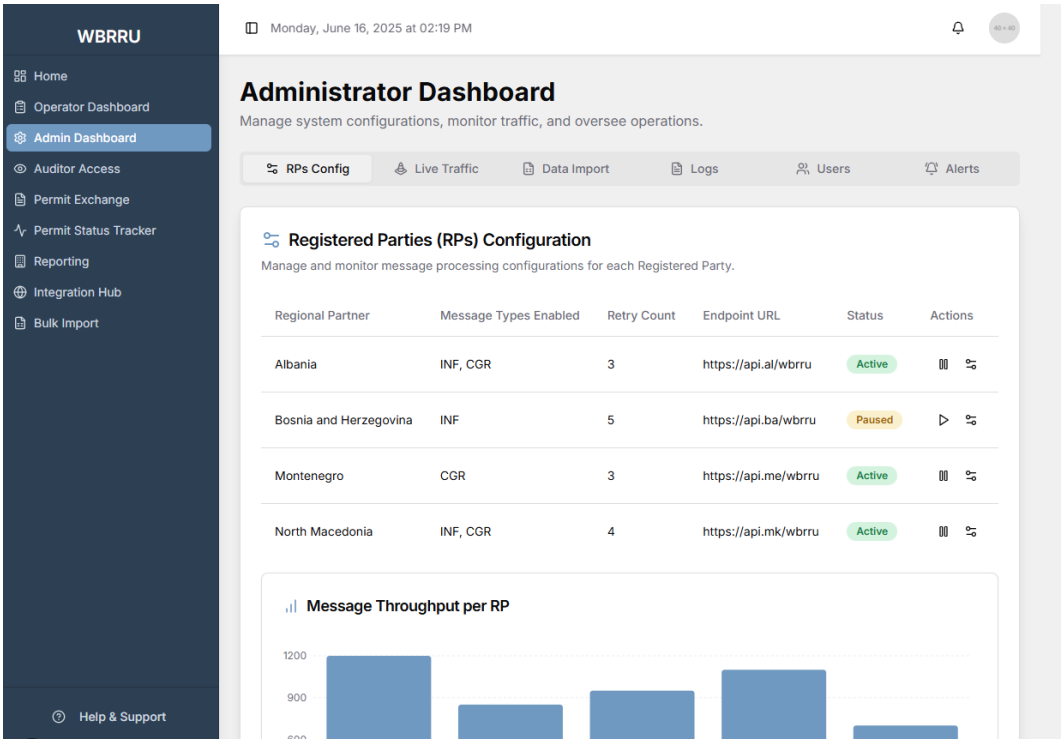


Figure 3:Administrator Dashboard (general overview)

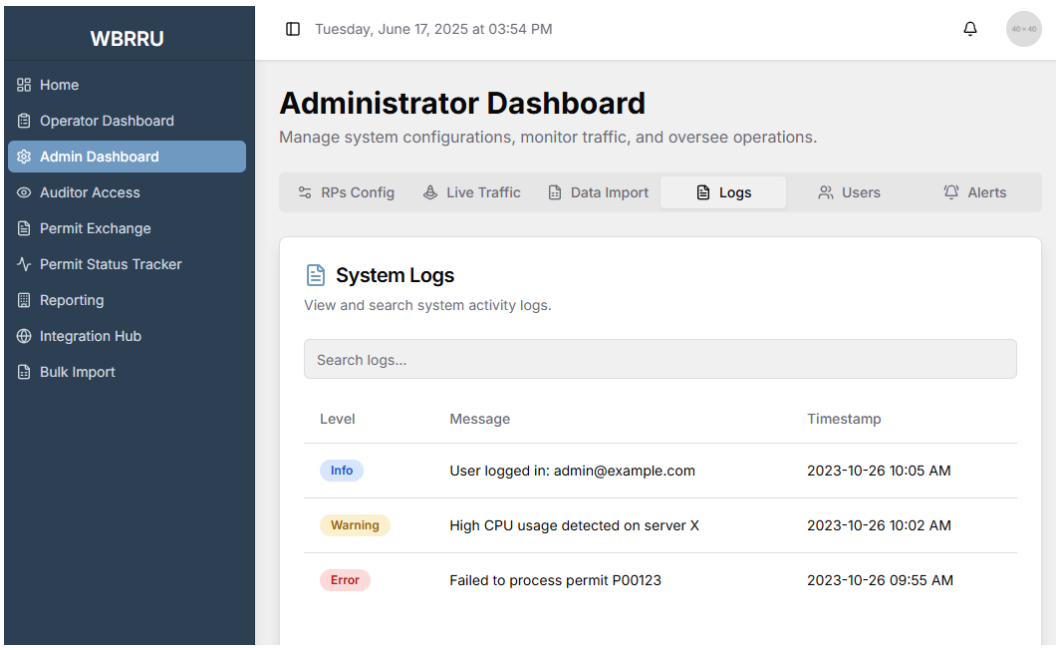


Figure 4: Administrator Dashboard (system logs)

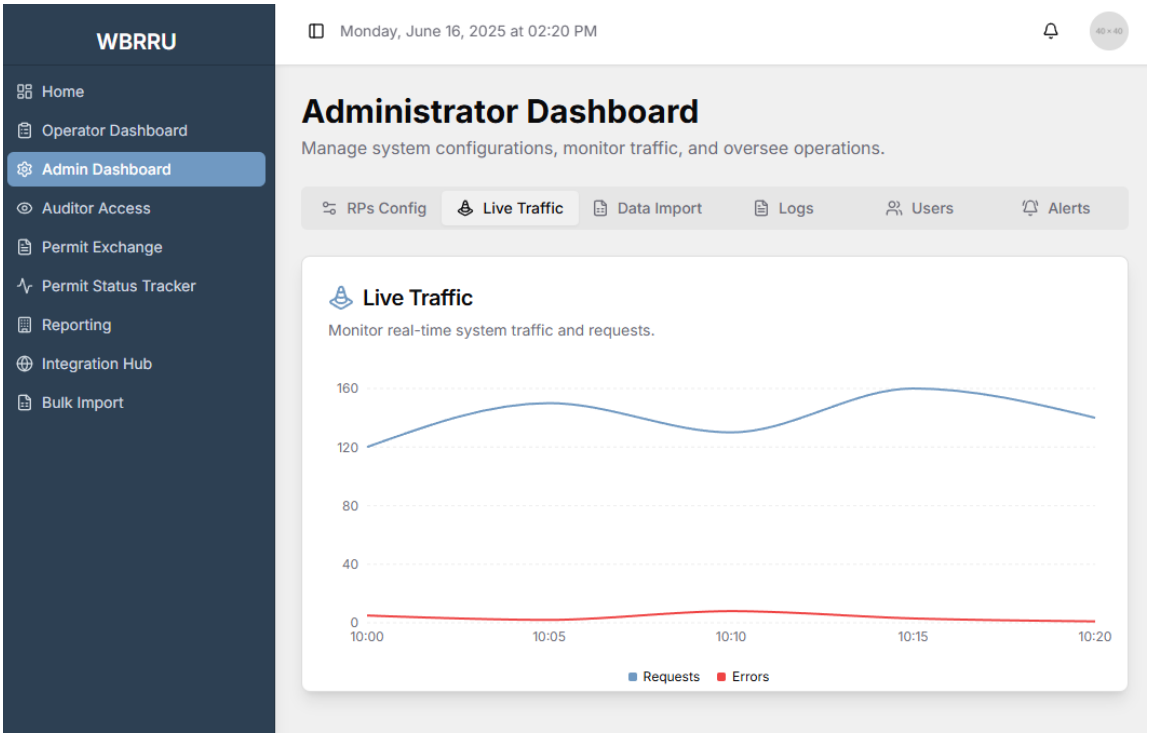


Figure 5: Administrator Dashboard - Live View

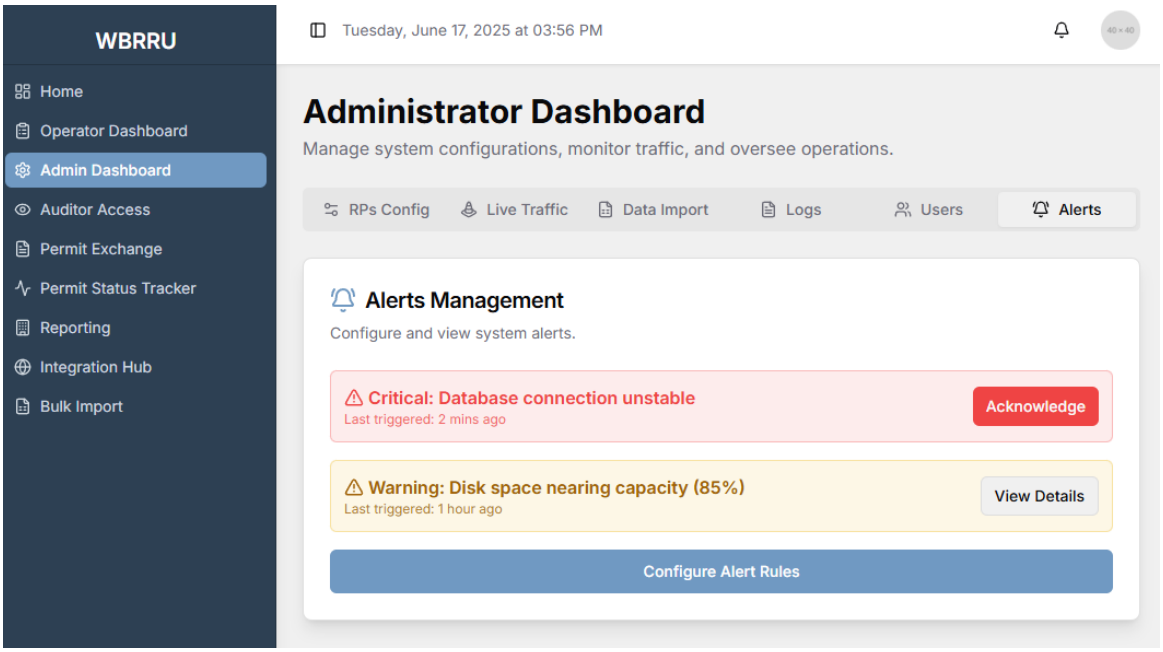


Figure 6: Administrator Dashboard (Alerts)

Auditor View (Read-only):

- Access to operator records, configuration snapshots, message archives, and audit logs.
- Export functions for compliance and audit review (CSV/XML format).

Auditor View has the following additional operational and functional requirements:

Category	Requirement ID	Description
AV GEN (General)	**FR-AV-GEN-01**	The page shall present five areas: Operators, Config Snapshots, Audit Logs, System Alerts, and DLQ Messages.
	FR-AV-GEN-02	All areas shall be read-only; no actions shall mutate underlying data.
	FR-AV-GEN-03	The page shall display consistent timestamps and identifiers to support traceability.
	FR-AV-GEN-04	Each table/list shall support scrolling for long datasets.
	FR-AV-GEN-05	Filters shall apply client-side to visible data and be reflected in exports.
AV OPS (Operators – Activity Logs)	**FR-AV-OPS-01**	The system shall provide filters for Operator and Action with an Apply Filters control.
	FR-AV-OPS-02	The system shall display a table with columns Log ID, Timestamp, Operator, Action, Entity ID, and Details.
	FR-AV-OPS-03	The system shall render the Action as a badge for quick visual scanning.
	FR-AV-OPS-04	The system shall provide Export CSV and Export XML actions for the filtered dataset.
AV CS (Configuration Snapshots)	**FR-AV-CS-01**	The system shall provide a Snapshot Date picker and a Snapshot Time selector.
	FR-AV-CS-02	The system shall provide a Load Snapshot action to display results for the selected time.
	FR-AV-CS-03	The system shall display a table with columns Snapshot ID, Timestamp, Changed By, Module, and Change Description.
	FR-AV-CS-04	The system shall provide Export CSV and Export XML actions for the current snapshot list.
AV AUD (Audit Logs Trail)	**FR-AV-AUD-01**	The system shall provide filters for Operator, Action, and Entity ID with an Apply Filters control.
	FR-AV-AUD-02	The system shall display a table with columns Log ID, Timestamp, Operator, Action, Entity ID, and Details.

Category	Requirement ID	Description
	FR-AV-AUD-03	The system shall display an empty-state message when no records match the current filters.
	FR-AV-AUD-04	The system shall provide Export CSV and Export XML actions for the filtered dataset.
AV ALT (System Alerts)	**FR-AV-ALT-01**	The system shall provide filters for keyword and level (Critical/Warning) with an Apply control.
	FR-AV-ALT-02	The system shall display alert cards including message, timestamp, level, and details with level-specific styling.
AV DLQ (Dead-Letter Queue)	**FR-AV-DLQ-01**	The system shall provide filters for partner and error message with an Apply Filters control.
	FR-AV-DLQ-02	The system shall display a table with columns Message ID, Partner, Error, Timestamp, and Action.
	FR-AV-DLQ-03	The system shall provide a View Payload dialog showing the raw message payload in a read-only scrollable area.
	FR-AV-DLQ-04	The system shall not expose Retry or Delete actions in the Auditor View.
AV EXP (Export & Evidence)	**FR-AV-EXP-01**	The system shall provide Export CSV and Export XML for Operators, Config Snapshots, and Audit Logs.
	FR-AV-EXP-02	Exports shall reflect the currently applied filters.
	FR-AV-EXP-03	Exports shall include a generated timestamp and, where feasible, the filter summary in file metadata or filename.
AV ACC (Accessibility & Usability)	**FR-AV-ACC-01**	All inputs and buttons shall have accessible labels and keyboard focus order.
	FR-AV-ACC-02	Dialogs and scroll areas shall be keyboard navigable; focus shall return to the triggering control on close.
	FR-AV-ACC-03	Status and level indicators (e.g., badges, alert colors) shall be accompanied by text labels.

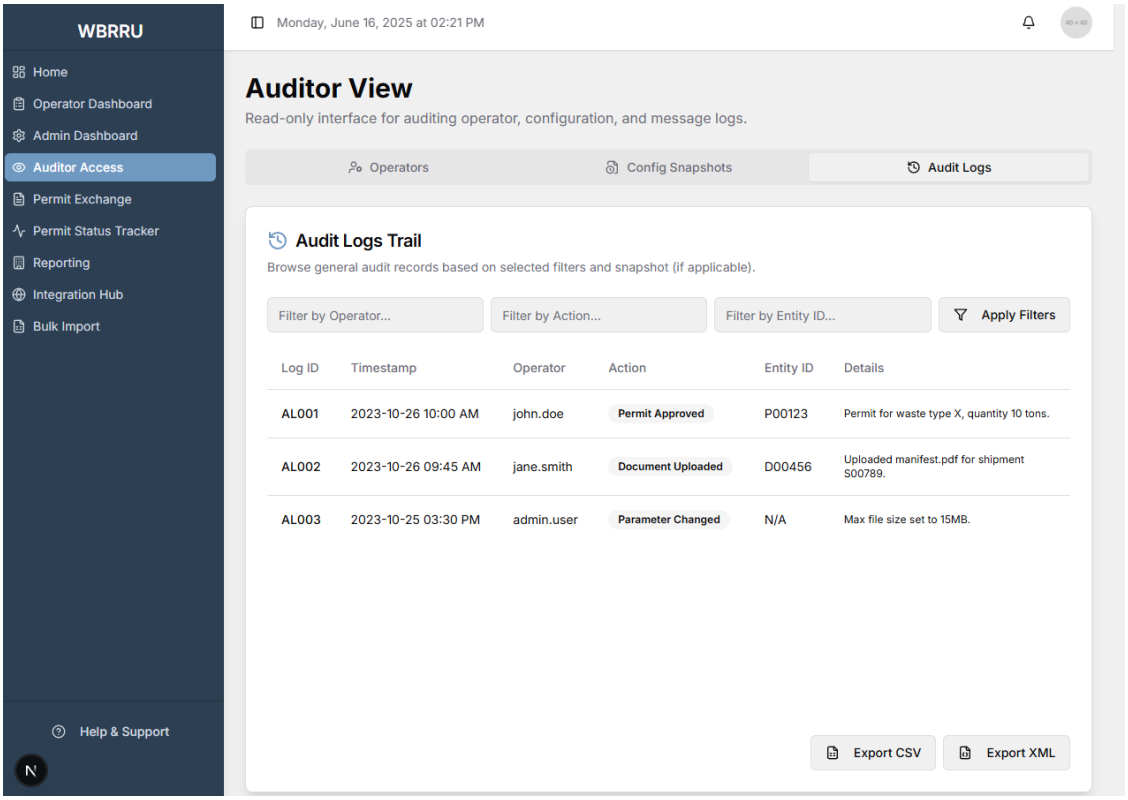


Figure 7: Auditor (read only) View

Technical Features:

- Responsive UI design for both desktop and tablet environments.
- Multilingual interface options (EN default, with regional language packs).
- Secure session management and automatic timeout for inactive users.
- Accessibility compliance with WCAG 2.1 standards where applicable.

These UIs ensure the WBRRU system can be used efficiently by a wide range of stakeholders and reduce reliance on technical personnel for operational workflows.

16 Performance Metrics (KPIs)

Performance metrics are established to ensure the WBRRU system meets operational benchmarks and EU interoperability standards under both normal and peak workloads. These metrics serve as key performance indicators (KPIs) for infrastructure reliability, service efficiency, and user responsiveness.

System-Level KPIs:

Availability	Minimum 99.9% system uptime measured monthly, with automatic failover capabilities for core services.
Message Throughput	Support for 5000+ ERRU-compliant messages per day per RP with burst capacity of 500 messages/minute.
Latency	Average response time for dashboard interactions below 1 second; message dispatch confirmation within 500 milliseconds

Error Rate	Less than 0.5% failure rate for message submissions, with retry queue logic covering transient faults.
Scalability Margin	Platform supports scaling for 2x data volume without downtime or performance degradation.

User-Level KPIs:

UI Load Time	Web portal pages should load in < 2 seconds over standard broadband.
Search & Retrieval	Records should return in < 1.5 seconds when filtered by license, name, or status.
Export Speed	Permit and operator record exports (PDF/XML) complete within 10 seconds for files <50MB.

Monitoring of these metrics is achieved using real-time dashboards, with alert thresholds configured to inform system administrators of deviations from service-level objectives (SLOs). Periodic performance testing and SLA audits ensure continued adherence to these benchmarks.

17 Quality Assurance

The WBRRU system shall undergo continuous validation through structured testing protocols that cover functional, technical, and compliance domains. Quality assurance (QA) processes are embedded into the development lifecycle and maintained throughout operational deployment.

Testing Types and Practices:

Unit Testing	All microservices undergo automated unit tests that validate core business logic, message parsing, normalization, and schema compliance
Integration Testing	Simulated end-to-end flows test message transformation, queuing, delivery, and receipt. Integration tests also validate interactions between normalization logic and partner-specific APIs
Compliance Testing	Messages are validated against latest ERRU XML schemas and WSDL, with test suites ensuring full message compatibility. Conformance tests are aligned with EU MOVEHUB certification requirements
User Acceptance Testing (UAT)	Conducted by representatives from each RP to verify functionality, workflows, and multilingual interface handling under realistic conditions

Regression Testing	Performed before deployment of any new version, ensuring previously validated functionality remains unaffected.

Test Environments and Tools:

- Dedicated staging environment simulating the EU interoperability layer and multiple RP adapters.
- Use of CI/CD pipelines to automate build, test, and deployment workflows.
- Application of QA tools such as Postman, SoapUI, Jest, Cypress, or equivalent.

Documentation and Reporting:

- QA reports are generated per release cycle, identifying passed/failed test cases, code coverage, and incident logs.
- Bug tracking and resolution metrics are maintained to measure time-to-fix and release velocity.

The above QA framework ensures the WBRRU system remains robust, user-friendly, and compliant across evolving regulatory and operational needs.

18 Infrastructure Requirements

The WBRRU system requires both capital and operational investments to ensure successful deployment, secure operation, and sustainable maintenance. This section outlines infrastructure components, licensing needs, cloud services, and cost estimation models for each Regional Partner (RP).

17.1 Infrastructure Components:

Cloud Hosting	Multi-tenant or RP-specific virtualized environments with Kubernetes clusters and persistent volume storage.
Database Services	Firestore (NoSQL) with optional Postgres for relational operations.
Container Registry	Storage for versioned microservice containers with controlled access.
Logging/Monitoring Stack	Tools like Prometheus, Grafana, Stackdriver, or DataDog for observability.

17.2 Software and Services Licensing

- Open-source components will be used where possible. Enterprise licenses (e.g., VPN, TLS certs, API gateways) will be budgeted separately.
- Middleware to connect national registers may require additional license fees based on existing vendor agreements.

19 Training and Documentation

Successful adoption of WBRRU by all WB6 regional participants requires structured onboarding, training, and user support. Training and documentation activities are critical to promote system understanding, facilitate adoption, and build local capacity.

Training Strategy

Training Strategy	
Task	**Description**
Initial Training Workshops	In-person or online training events tailored to each RP with technical sessions for IT staff and administrative sessions for authority users
User Role Orientation	Split-track training materials based on user roles (Authority Admin, WBRRU Admin, Auditor).
Onboarding Playbooks	Per-RP manuals describing connection steps, schema validation, message templates, and normalization configuration.

Documentation Deliverables:

- User Manuals: Detailed manuals per role, translated into local languages, with annotated screenshots.
- Quick Reference Guides: 2-page visual cheat sheets for frequent tasks (message dispatch, operator registration, etc.).
- Video Tutorials: Pre-recorded step-by-step video walkthroughs embedded in the help section of the platform.
- API Integration Docs: Swagger/OpenAPI-based guides and Postman collections for developers.

Support and Helpdesk:

- Centralized ticketing system for issue logging and escalation (e.g., Jira Service Desk or Freshdesk).
- First-line email support available in English with local contact points designated per RP.
- Knowledge base articles and FAQs searchable within the admin interface.

Training and documentation ensures WBRRU is not only technically implemented, but functionally adopted and sustained across the regional partners.

20 Annexes

The annexes section below provides reference material that complements the main specification, including regulatory excerpts, technical samples, and source links for further context and traceability.

Annex I – Minimum Requirements for XML messages

Minimum requirements for the content of the XML messages

Common Header		Mandatory
Version	The official version of the XML specifications will be specified through the namespace defined in the message XSD and in the *version* attribute of the Header element of any XML message. The version number ('n.m') will be defined as fixed value in every release of the XML Schema Definition file (xsd).	Yes
Test Identifier	Optional id for testing. The originator of the test will populate the id and all participants in the workflow will forward/return the same id. In production it should be ignored and will not be used if it is supplied.	No
Technical Identifier	A UUID uniquely identifying each individual message. The sender generates a UUID and populates this attribute. This data is not used in any business capacity.	Yes
Workflow Identifier	The workflowId is a UUID and should be generated by the requesting Member State. This id is then used in all messages to correlate the workflow.	Yes
Sent At	The date and time (UTC) that the message was sent.	Yes
Timeout	This is an optional date and time (in UTC format) attribute. This value will be set only by the central hub for forwarded requests and is calculated based on the date/time the initial request has been received by the central hub. This will inform the responding Member State of the time when the request will be timed out. This value is not required in initial requests sent to the central hub and all response messages.	No
From	The ISO 3166-1 Alpha 2 code of the Member State sending the message or 'EU'.	Yes
To	The ISO 3166-1 Alpha 2 code of the Member State to which the message is being sent or 'EU'.	Yes

Check Good Repute

Check Good Repute Request		**Mandatory**
Business Case Identifier	A serial or reference number identifying each individual request.	Yes
Requesting Competent Authority	The competent authority that has issued the search request.	Yes
Transport Manager Details		*Yes, if no CPC details*
Family Name	Transport manager's family name(s) as indicated on the CPC.	Yes
First Name	Transport manager's complete given name as indicated on the certificate of professional competence.	Yes
Date of Birth	Transport manager's birth date in ISO 8601 format (YYYY-MM-DD).	Yes
Place of Birth	Transport manager's place of birth.	No
Address	The address, city, postcode and country of the transport manager.	No
CPC Details		*Yes, if no transport manager details*
CPC Number	Number of certificate of professional competence	Yes
CPC Issue Date	Date of issuance of the CPC, in ISO 8601 format (YYYY-MM-DD).	Yes
CPC Issue Country	Issuing country of the CPC in ISO 3166-1 alpha 2 format.	Yes

Check Good Repute Response		**Mandatory**
Business Case Identifier	A serial or reference number matching the business case identifier of the request.	Yes
Requesting Competent Authority	The competent authority that has issued the search request.	Yes
Responding Competent Authority	The competent authority that has responded to the search request.	Yes
Status Code	The status code of the search (e.g. found, not found, error, etc.).	Yes
Status Message	An explanatory status description (if necessary).	No
Found Transport Manager Details		*Yes if Status Code is Found*
Family Name	Transport manager's family name(s) as recorded in the register.	Yes
First Name	Transport manager's complete given name as recorded in the register.	Yes
Date of Birth	Transport manager's birth date in ISO 8601 format (YYYY-MM-DD) as recorded in the register.	Yes
Place of Birth	Transport manager's place of birth as recorded in the register.	No
CPC Number	Number of certificate of professional competence as recorded in the register.	Yes
CPC Issue Date	Date of issuance of the CPC, in ISO 8601 format (YYYY-MM-DD) as recorded in the register.	Yes
CPC Issue Country	Issuing country of the CPC in ISO 3166-1 alpha 2 format as recorded in the register.	Yes
CPC Validity	Declaration of either 'Valid' or 'Invalid'	Yes
Total Managed Undertakings	The number of transport undertakings with which the transport manager is associated.	Yes

Check Good Repute Response		**Mandatory**
Total Managed Vehicles	The total number of vehicles with which the transport manager is associated.	Yes
Fitness	Declaration of either 'Fit' or 'Unfit'.	Yes
Start Date of Unfitness	Start date of unfitness of the transport manager in ISO 8601 format (YYYY-MM-DD).	Yes if 'Fitness' is 'Unfit'.
End Date of Unfitness	End date of unfitness of the transport manager in ISO 8601 format (YYYY-MM-DD).	Yes if 'Fitness' is 'Unfit'.
Search Method	The method used to find the transport manager: NYSIIS, CPC, Custom.	Yes
Transport Undertaking (for each found Transport Manager)		*Yes if Managed Undertakings > 0*
Transport Undertaking Name	The name of the transport undertaking (name and legal form) as recorded in the register.	Yes
Transport Undertaking Address	The address of the transport undertaking (address, postal code, city, country) as recorded in the register.	Yes
Licence Number	The serial number of the licence of the transport undertaking (free text alphanumeric field with length 1 to 20).	Yes
Licence Status	The status of the licence of the transport undertaking as recorded in the register.	Yes
Managed Vehicles	The number of vehicles managed as recorded in the register.	Yes

Notification of Check Result

Notification of Check Result		**Mandatory**
Business Case Identifier	A serial or reference number identifying each individual notification.	Yes
Notifying Competent Authority	The competent authority that issues the notification.	Yes
Transport Undertaking		Yes
Transport Undertaking Name	The name of the transport undertaking being object of the check.	Yes
Licence Number	The serial number of the licence or of the certified true copy of the transport undertaking (free text alphanumeric field with length 1 to 20).	Yes
Vehicle Registration Number	The vehicle registration number of the vehicle checked	Yes
Vehicle Registration Country	The country in which the vehicle checked is registered	Yes
General information about the check		
Date of check	Date of check in ISO 8601 format (YYYY-MM-DD)	Yes
Clean check	Yes/No	Yes
Minor infringements		Yes, if minor infringement(s) detected during the check
Date of minor infringement	Date of the infringement in ISO 8601 format (YYYY-MM-DD)	Yes
Number of minor infringements	The number of minor infringements detected.	Yes

Notification of Check Result		**Mandatory**
Serious infringement		Yes, if serious infringement detected during the check
Date of Infringement	Date of the infringement in ISO 8601 format (YYYY-MM-DD)	Yes
Category	The category of the infringement: — MSI: Most serious infringement — VSI: Very serious infringement — SI: Serious infringement	Yes
Infringement Type	In accordance with the classification provided in Annex IV to Regulation (EC) No 1071/2009 and Annex I to Commission Regulation No (EU) 2016/403 [(1)]	Yes
Appeal Possible	If an appeal against the infringement is still possible at the time of notification. Yes/No	Yes
Penalty Imposed (for each serious infringement)		Yes, if relevant
Penalty Imposed Identifier	The serial number of the individual penalty imposed.	Yes
Final Decision Date	The final decision date of the penalty imposed in ISO 8601 format (YYYY-MM-DD).	Yes
Penalty Type Imposed	Declaration of either: — 101: ‘Warning’ — 201: ‘Temporary ban on cabotage operations’ — 202: ‘Fine’ — 203: ‘Prohibition’ — 204: ‘Immobilisation’ — 102: ‘Other’	Yes

Notification of Check Result		Mandatory
Start Date	The start date of the penalty imposed in ISO 8601 format (YYYY-MM-DD)	No
End Date	The end date of the penalty imposed in ISO 8601 format (YYYY-MM-DD)	No
Executed	Yes/No	Yes
Penalty Requested (for each Serious Infringement)		No
Penalty Requested Identifier	The serial number of the individual penalty requested.	Yes
Penalty Type Requested	Declaration of either: — 101: 'Warning' — 301: 'Temporary withdrawal of some or all of the certified true copies of the licence' — 302: 'Permanent withdrawal of some or all of the certified true copies of the licence' — 303: 'Temporary withdrawal of the licence' — 304: 'Permanent withdrawal of the licence' — 305: 'Suspension of the issue of driver attestations' — 306: 'Withdrawal of driver attestations' — 307: 'Issue of driver attestations subject to additional conditions in order to prevent misuse'	Yes
Duration	The duration of the requested penalty (calendar days).	No

([1])

Commission Regulation (EU) 2016/403 of 18 March 2016 supplementing Regulation (EC) No 1071/2009 of the European Parliament and of the Council with regard to the classification of serious infringements of the Union rules, which may lead to the loss of good repute by the road transport operator, and amending Annex III to Directive 2006/22/EC of the European Parliament and of the Council (OJ L 74, 19.3.2016, p. 8).

Notification of Check Result Response		**Mandatory, if infringement(s) detected during the check**
Business Case Identifier	A serial or reference number matching the business case identifier of the notification.	Yes
Originating Competent Authority	The competent authority that issued the original infringement notification.	Yes
Licensing Competent Authority	The competent authority responding to the infringement notification.	Yes
Status Code	The status code of the infringement response (e.g. found, not found, error, etc.).	Yes
Status Message	An explanatory status description (if necessary).	No
Transport Undertaking		*Yes*
Transport Undertaking Name	The name of the transport undertaking as recorded in the register.	Yes
Transport Undertaking Address	The address of the transport undertaking (address, postal code, city, country) as recorded in the register.	Yes
Licence Number	The serial number of the licence of the transport undertaking as recorded in the register (free text alphanumeric field with length 1 to 20).	Yes
Licence Status	The status of the licence of the transport undertaking as recorded in the register.	Yes
Penalty Imposed		*No*
Penalty Imposed Identifier	The serial number of the individual penalty imposed (given in the Penalty Requested Identifier of the Notification of Check Result).	Yes
Competent Authority Imposing Penalty	The name of the competent authority imposing the penalty.	Yes
Is Imposed	Yes/No	Yes

Notification of Check Result Response		Mandatory, if infringement(s) detected during the check
Penalty Type Imposed	Declaration of either: — 101: 'Warning' — 301: 'Temporary withdrawal of some or all of the certified true copies of the licence' — 302: 'Permanent withdrawal of some or all of the certified true copies of the licence' — 303: 'Temporary withdrawal of the licence' — 304: 'Permanent withdrawal of the licence' — 305: 'Suspension of the issue of driver attestations' — 306: 'Withdrawal of driver attestations' — 307: 'Issue of driver attestations subject to additional conditions in order to prevent misuse' — 102: 'Other'	Yes
Start Date	The start date of the penalty imposed in ISO 8601 format (YYYY-MM-DD).	No
End Date	The end date of the penalty imposed in ISO 8601 format (YYYY-MM-DD).	No
Reason	Reason if penalty is not imposed.	No

Notification of Check Result Acknowledgement		Mandatory
Business Case Identifier	A serial or reference number matching the business case identifier of the notification or the response.	Yes
Status Code	Status code of the acknowledgement.	Yes
Status Message	Status Message String	No

Originating Competent Authority	For a NCRN_Ack: in the legislation this field is represented as 'Destination Competent Authority Identifier'. For a NCRR_Ack: in the legislation this field is represented as 'Acknowledging Competent Authority Identifier'.	Yes
Licensing Competent Authority	For a NCRN_Ack: in the legislation this field is represented as 'Acknowledging Competent Authority Identifier'. For a NCRR_Ack: in the legislation this field is represented as 'Destination Competent Authority Identifier'.	Yes
Acknowledgement Type	Defining Acknowledgement Type Possible Values: — 'NCRN_Ack' — 'NCRR_Ack'	Yes

Check Transport Undertaking Data

Check Transport Undertaking Data Request		**Mandatory**
Business Case Identifier	A serial or reference number identifying each individual request.	Yes
Originating Competent Authority	The competent authority issuing the search request.	Yes
Transport Undertaking Identification		Yes
Transport Undertaking Name	The name of the transport undertaking.	At least two of the search fields are required.
Licence Number	The serial number of the licence or of the certified true copy (free text alphanumeric field with length 1 to 20).	
Vehicle Registration Number	The registration number of one of the vehicles of the transport undertaking.	
Vehicle Registration Country	The country of registration of the vehicle.	Yes, if vehicle registration number provided.
Request All Vehicles	To request the registration numbers of all vehicles managed by the undertaking. Yes/No	Yes

Check Transport Undertaking Data Response		**Mandatory**
Business Case Identifier	A serial or reference number identifying each individual request	Yes
Originating Competent Authority	The competent authority issuing the search request.	Yes
Responding Competent Authority	The competent authority providing the response.	Yes
Status Code	The status code of the response (e.g. found, not found, error, etc.).	Yes
Status Message	An explanatory status description (if necessary).	No
General Information about the Transport Undertaking		*Yes, if status code is found*
Transport Undertaking Name	The name of the transport undertaking (name and legal form).	Yes
Transport Undertaking Address	The address of the transport undertaking (address, postal code, city, country) as recorded in the register	Yes
Number of Managed Vehicles	The number of vehicles managed as recorded in the register.	Yes
Number of People Employed	The number of people employed in the undertaking on last 31 December.	Yes
Risk Rating	The risk rating of the undertaking.	Yes
Risk Rating Band	The risk rating band of the undertaking (green, amber, red, grey).	Yes
Licence Details		*Yes, if status code is found*
Licencing Competent Authority	The competent authority that issued the licence to the transport undertaking	Yes

Check Transport Undertaking Data Response		**Mandatory**
Licence Number	The serial number of the licence of the transport undertaking as recorded in the register (free text alphanumeric field with length 1 to 20)	Yes
Licence Status	The status of the licence of the transport undertaking as recorded in the register	Yes
Licence Type	The type of the licence as recorded in the register. A declaration of: — 'International licence for passenger transport' — 'National licence for passenger transport' — 'International licence for goods transport' — 'International licence for goods transport, exclusively ≤ 3,5 t' — 'National licence for goods transport'	Yes
Start Date	The start date of the licence	Yes
Expiry Date	The expiry date of the licence	Yes
Withdrawal Date	The withdrawal date of the licence	Yes, if found
Suspension Date	The suspension date of the licence	Yes, if found
Suspension Expiry Date	The date on which the licence suspension expires	Yes, if found
Certified True Copy Details		*Yes*
Certified True Copy Number	The serial number of each certified true copy of the licence of the transport undertaking as recorded in the register (free text alphanumeric field with length 1 to 20)	Yes
Start Date	The start date of each certified true copy of the licence.	Yes
Expiry Date	The expiry date of each certified true copy of the licence.	Yes
Withdrawal Date	The withdrawal date of each certified true copy of the licence.	Yes, if found

Check Transport Undertaking Data Response		**Mandatory**
Suspension Date	The suspension date of the certified true copy of the licence.	Yes, if found
Suspension Expiry Date	The date on which each certified true copy of the licence suspension expires.	Yes, if found
Vehicle Details		Yes, if value of 'Request All Vehicles' in CTUD Request is 'Yes'.
Vehicle Registration Number	The registration number of each of the vehicles of the transport undertaking	Yes
Vehicle registration country	The registration country of each of the vehicles of the transport undertaking.	Yes

Notification of Unfitness

Notification of Unfitness		**Mandatory**
Business Case Identifier	A serial or reference number identifying each individual notification.	Yes
Notifying Competent Authority	The competent authority that issues the notification.	Yes
Transport Manager Details		*Yes, if no CPC details*
Family Name	Transport manager's family name(s) as indicated on the CPC.	Yes
First Name	Transport manager's complete given name as indicated on the certificate of professional competence.	Yes
Date of Birth	Transport manager's birth date in ISO 8601 format (YYYY-MM-DD).	Yes
Place of Birth	Transport manager's place of birth.	No
CPC Details		*Yes, if no transport manager details*
CPC Number	Number of certificate of professional competence	Yes
CPC Issue Date	Date of issuance of the CPC, in ISO 8601 format (YYYY-MM-DD).	Yes
CPC Issue Country	Issuing country of the CPC in ISO 3166-1 alpha 2 format.	Yes
Declaration of Unfitness		Yes
Start Date of Unfitness	Start date of unfitness, in ISO 8601 format (YYYY-MM-DD).	Yes

Notification of Unfitness Acknowledgement		Mandatory
Business Case Identifier	A serial or reference number matching the business case identifier of the notification.	Yes
Originating Competent Authority	The competent authority issuing the notification.	Yes
Responding Competent Authority	The competent authority providing the acknowledgement.	Yes
Status Code	Status code of the acknowledgement.	Yes
Status Message	Status Message String	No

Check Bilateral Permit Data

Check Bilateral Permit Data Request		**Mandatory**
Business Case Identifier	A serial or reference number identifying each individual request.	Yes
Originating Competent Authority	The competent authority issuing the search request.	Yes
Transport Undertaking Identification		Yes
Transport Undertaking Name	The name of the transport undertaking.	At least two of the search fields are required.
Licence Number	The serial number of the licence or of the certified true copy (free text alphanumeric field with length 1 to 20).	
Vehicle Registration Number	The registration number of one of the vehicles of the transport undertaking.	
Vehicle Registration Country	The country of registration of the vehicle.	Yes, if vehicle registration number provided.
Request All Vehicles	To request the registration numbers of all vehicles managed by the undertaking. Yes/No	Yes

Check Bilateral Permit Data Response		**Mandatory**
Business Case Identifier	A serial or reference number identifying each individual request	Yes
Originating Competent Authority	The competent authority issuing the search request.	Yes
Responding Competent Authority	The competent authority providing the response.	Yes
Status Code	The status code of the response (e.g. found, not found, error, etc.).	Yes
Status Message	An explanatory status description (if necessary).	No
General Information about the Transport Undertaking		*Yes, if status code is found*
Transport Undertaking Name	The name of the transport undertaking (name and legal form).	Yes
Transport Undertaking Address	The address of the transport undertaking (address, postal code, city, country) as recorded in the register	Yes
Number of Managed Vehicles	The number of vehicles managed as recorded in the register.	Yes
Number of People Employed	The number of people employed in the undertaking on last 31 December.	Yes
Risk Rating Band	The risk rating band of the undertaking (green, amber, red, grey).	Yes
Permit Details		*Yes, if status code is found*
Licencing Competent Authority	The competent authority that issued the permit to the transport undertaking	Yes

Check Bilateral Permit Data Response		**Mandatory**
Permit Number	The serial number of the permit of the transport undertaking as recorded in the register (free text alphanumeric field with length 1 to 20)	Yes
Permit Status	The status of the permit of the transport undertaking as recorded in the register	Yes
Permit Type	The type of permit as recorded in the register. A declaration of: — 'Bilateral Permit for passenger transport' — 'Bilateral Permit for goods transport' — 'Bilateral Permit for goods transport, exclusively ≤ 3,5 t' — 'Permit for dangerous goods transport'	Yes
Start Date	The start date of the permit	Yes
Expiry Date	The expiry date of the permit	Yes
Withdrawal Date	The withdrawal date of the permit	Yes, if found
Suspension Date	The suspension date of the permit	Yes, if found
Suspension Expiry Date	The date on which the permit suspension expires	Yes, if found
Certified True Copy Details		*Yes*
Certified True Copy Number	The serial number of each certified true copy of the permit of the transport undertaking as recorded in the register (free text alphanumeric field with length 1 to 20)	Yes
Start Date	The start date of each certified true copy of the permit.	Yes
Expiry Date	The expiry date of each certified true copy of the permit.	Yes
Withdrawal Date	The withdrawal date of each certified true copy of the permit.	Yes, if found
Suspension Date	The suspension date of the certified true copy of the permit.	Yes, if found

Check Bilateral Permit Data Response		Mandatory
Suspension Expiry Date	The date on which each certified true copy of the permit suspension expires.	Yes, if found
Vehicle Details		Yes, if value of 'Request All Vehicles' in CTUD Request is 'Yes'.
Vehicle Registration Number	The registration number of each of the vehicles of the transport undertaking	Yes
Vehicle registration country	The registration country of each of the vehicles of the transport undertaking.	Yes