EROAD
SOLUTION

SECURITY TARGET
VERSION 1.3

NTT Com Security (Norway) AS - www.nordics.nttcomsecurity.com

Office address: Havnegaarden – Kystveien 14 – 4841 Arendal
Postal address: Postboks 721 Stoa – 4808 Arendal
T +47 37 01 94 00

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

Abbreviation	Description
AES	Advanced Encryption Standard
CMAC	Cipher-based MAC
AWS	Amazon Web Services
CA	Certificate Authority
COTS	Commercial Off the Shelf
ESP	Ebox to Server Protocol
GPS	Global Positioning System
HOS	Hours of Service
IFTA	International Fuel Tax Agreement
IRP	International Registration Plan
OBU	On-board unit
PKI	Public Key Infrastructure
QMS	Quality Management System
REST	Restful State Transfer
RFID	Radio Frequency Identification
RUAF	Road Use Assessment Fee
RUC	Road User Charges
SaaS	Software as a service
SOAP	Simple Object Access Protocol
WMT	Weight-Mileage Tax

DEFINITIONS

Definition	Description
Basic Authentication	HTTP Basic Authentication uses HTTP headers containing user name and password to authenticate requests. Every request must contain this information.
Environment	For the EROAD Web Portal, the EROAD Depot Application, and the EROAD OBU Gateway the environment refers to infrastructure, platforms, and middleware provided by the cloud provider and/or third party vendors. For the EROAD OBU, the environment refers to the vehicle in which the unit is installed. This is as opposed to EROAD developed components which comprise the TOE.
Geo-fencing	A feature in a software program that uses the GPS or RFID to define geographical boundaries.

1. ST INTRODUCTION (ASE_INT)

1.1. ST AND TOE REFERENCES

The following describes the references for the ST and the TOE:

- ST title: EROAD Solution Security Target.
- CC Version: 3.1 Revision 4.
- Assurance level: EAL2 augmented with ALC_FLR.1.
- PP Identification: None.
- TOE name: EROAD Solution.
- TOE versions of EROAD OBU:
  - Hardware version: 03
  - Firmware version: 1.18.05
- TOE versions of EROAD Application:
  - Software version: 11-11-2014-0239

1.2. TOE OVERVIEW

The TOE is comprised of four major logical components:

1) the EROAD On-Board Unit (OBU endpoint),
2) the EROAD Depot Application,
   … protected by …
3) the EROAD OBU Gateway and
4) the EROAD Web Portal.

Together, these components comprise a solution that enables end users to report on and pay vehicle levies online. These four major components define the scope of the EROAD TOE offered as a SaaS (Software as a Service).

The EROAD OBU is a hardware device that measures distance travelled, tracks location, and transmits data to the EROAD Depot Application via a secure private cellular link. The data (vehicle information) transmitted by the EROAD OBU is processed and made available to end users by the web based EROAD Depot Application. The Depot Application is implemented as a collection of virtualized servers and hosted as a cloud based SaaS. The solution calculates taxes owed, allows for payment, and provides additional value-added services. It is available to end users by means of browser based access via the Internet. See figure 1, System Overview, for a high level view of the solution. See figure 2, System Architecture, for a logical depiction of its major functions.

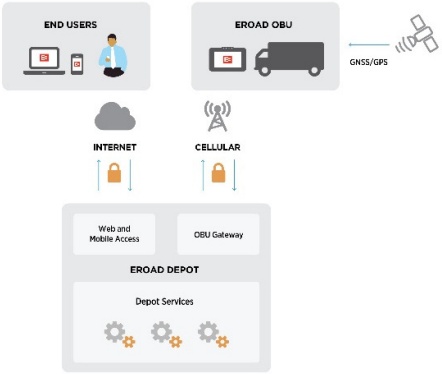

Figure 1: System Overview

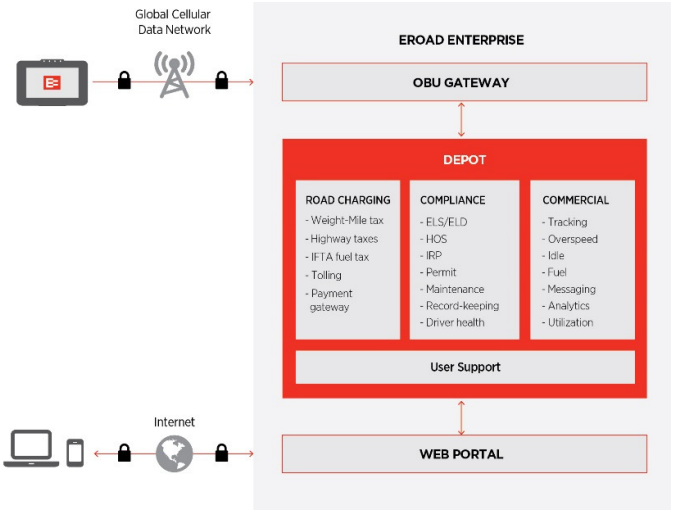

Figure 2: System Architecture

Non-TOE hardware and software required by the TOE:

The following supporting hardware and software are required by the TOE:

- Virtual Hardware: 2 vCPUs (Hosted by High Frequency Intel Xeon E5-2670 (Sandy Bridge) Processors), 7.5 GB Memory, 32 GB SSD Storage.
- Operating System: Linux version 3.2.
- Middleware: Web Server that supports Servlet 3.0, JSP 2.2, and EL 2.2 specifications; Java EE 6 compliant Application Server; ORDBMS that implements SQL:2011 standard and is ACID-compliant; Managed Runtime Environment that supports Java SE 7.

EROAD use their cloud provider to protect all computing infrastructure associated within their production environment. EROAD maintains control over the configuration of the platforms and the software running on them (i.e., OS, middleware, application executables, databases, open ports, TLS/SSL, authentication and authorization, access control, etc.). However that environment is completely private, secure, and not exposed. Therefore, these underlying environmental components are out of scope insofar as the TOE is concerned. Further, EROAD security is stand alone, isolated, self-contained, and presents no exposed surface area that potential threats can exploit except for those presented below.

1.3. TOE DESCRIPTION

The EROAD solution includes four components. These components are:

1) EROAD OBU (physically exposed),
2) EROAD OBU Gateway (access to/from the exposed OBU),
3) EROAD Web Portal (access to/from the Depot Application), and
4) EROAD Depot Application (access via browser based user interface).

The supporting guidance documents are:

1) EROAD Ehubo Installation Guide, 11/2014
2) EROAD Guidance Document, Version 1.0
3) EROAD Guidance Documentation Supplement, 12/2014

As part of the TOE, the EROAD OBU Gateway, EROAD Web Portal, and EROAD Depot Application are protected by environmental devices and elements, supplied by the cloud provider. These devices and elements notify EROAD administrative functions in the event of physical or digital attack. In addition, the EROAD OBU must and does protect itself since it is physically exposed. Internally, the EROAD OBU does so via a permanent metal shield that covers and seals off key circuits and board components. It possesses tamper pills and switches to detect any attempt to open or breach its case. It cross checks its data (results) to assure no fraudulent information has been substituted or injected. Activity within the Depot Application itself is logged for inspection via audit trail, and access (authentication and authorization) is controlled via an authoritative security framework.

TOE scope for the EROAD OBU includes Ehubo hardware/firmware. TOE scope for the EROAD Application includes the EROAD Web Portal, EROAD OBU Gateway, and EROAD Depot Application. Included are the end user interface, exposed web services, and all connected OBU endpoints.

Access by the EROAD OBU is controlled by the EROAD OBU Gateway. Each EROAD OBU is uniquely identified, authenticated, and authorized via user name and password. Only authenticated and authorised units may access the EROAD Depot Application via this interface (entry point). The function is limited to the transfer of messages and events between the EROAD OBU Gateway and EROAD OBU endpoints. Communication to/from the OBU is secured and encrypted via the TLS channel established by the OBU and an environmental device of the EROAD OBU Gateway. All data transmitted from/to the OBU is encrypted/decrypted by the on-board EROAD Cryptographic Module (processor) which uses hardware acceleration in order to maximize performance.

TOE scope for the EROAD Depot Application is that of a typical "N-Tiered" web based application with both telematics devices (EROAD OBU) and browser based end users as secured endpoints. OBU endpoints are authenticated and authorized via a secure gateway (EROAD OBU Gateway). End user browser based access to the EROAD Depot Application is authenticated and authorized via a secure portal (EROAD Web Portal). Communication to/from authenticated and authorized endpoints is protected and secured by environmental infrastructure associated with the hosting of the TOE.

1.3.1. EROAD OBU

The OBU hardware is used to support accurate and trusted reporting of vehicle distance, location and time. This supports the accurate reporting of Road User Charges.

See figure 3, EROAD OBU hardware, as an OBU example.

Figure 3: EROAD OBU hardware

The OBU User Interface consists of a number of status indicators on the EROAD OBU as well as an interactive touch screen on some models:

- LEDs display the current status of the EROAD OBU (normal operation, degraded mode, no external power, faults. etc.).
- A touchscreen shows current status information for the EROAD OBU. Limited driver input to the EROAD OBU is possible. The display allows the driver to change predefined trip configurations via the EROAD OBU as configured in the EROAD Depot Application.

Time, location, and distance information is collected by internal and external sensors. Information gathered from these different sources is compared and cross checked for accuracy. Collected data is processed by the OBU's Event Generation Engine. This includes any and all indications of tampering (tamper sensors and cross checks on data) along with power state. The OBU transmits data via secure cellular. Vehicle and on board unit sensor data is collected continuously. Data is sent as messages and events over a secured Cellular Interface. The EROAD Depot Application receives this data via the EROAD OBU Gateway and processes it further. Any indication of OBU tampering is logged, and the OBU is put into an unauthorized state. When in an unauthorized state, the EROAD OBU can no longer communicate with the OBU Gateway and must be returned to EROAD for reauthorization. See figure 4, EROAD OBU Product.

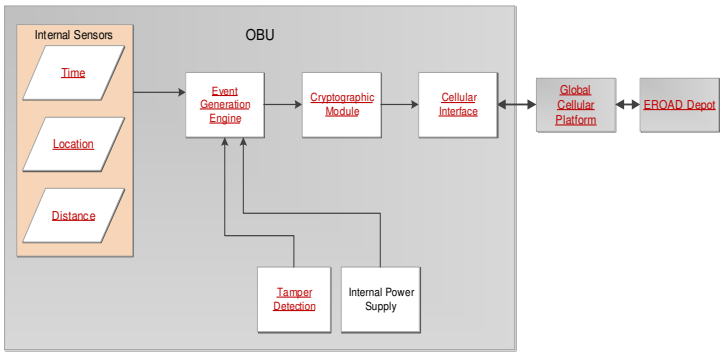

Figure 4: EROAD OBU Product

Time Keeping

The EROAD OBU keeps accurate and auditable time in all operating modes even when external power is removed (via internal battery).

Location

Extremely accurate GPS position data is collected continuously. Location events are created according to vehicle speed and ignition status. The location event interval is never more than 250 metres. Recorded events are stored in the EROAD OBU and periodically sent to the EROAD OBU Gateway. All events bear a timestamp indicating when the event actually took place as opposed to the time it was sent to the EROAD OBU Gateway. The EROAD OBU Gateway transforms this data for use by the EROAD Depot Application, where further processing takes place. Post processing consists of matching the longitude and latitude information sent by the OBU (per event) with centre line road data.

Distance Measurement

The EROAD OBU is designed to be an accurate and auditable electronic vehicle distance recorder that calculates vehicle mileage, location and times of travel.

Event Generation Engine
The Event Generation Engine creates individual events from a variety of inputs. These include both GPS and internal sensors for time, distance, and location. It also generates data based on inputs from the EROAD OBU user interface. Events also come from the vehicle wired interface, tamper detection sensors, and internal power supply.

Tamper Detection
Tampering is monitored continuously by the EROAD OBU hardware. If OBU sensors or cross checks on data reveal attempts at tampering, the Tamper Detection module destroys ("zero's out") the relevant keys on the EROAD OBU. This includes a hardware reset to re-initialise RAM. This disables the EROAD OBU by putting it into an unauthorized state making it unable to communicate further with the OBU Gateway. The EROAD OBU must be physically returned to EROAD to be reauthorized after a tamper event has been detected.

Cryptographic Module
The Cryptographic Module in the OBU takes events generated by the Event Generation Engine and encrypts them according to the FIPS 140-2 security standard. Encrypted events are then transmitted via the Cellular Interface.

Cellular Interface
The Cellular Interface takes the encrypted event data and transmits it via a secure cellular network (i.e. over the Global Cellular Platform) to the EROAD OBU Gateway which transforms events for use by the EROAD Depot Application.

Global Cellular Platform
EROAD uses cellular communications:

- GSM Association (Global System for Mobile communications or Groupe Special Mobile), which sets international standards and protocols for all GSM, GPRS, UMTS (3G) LTE (4G) network operators to ensure interoperability and optimum user experience.
- 3GPP – (3G Partnership Program), which is an evolution of the GSM Association members for development of 3rd Generation technologies, devices, services, applications and roadmaps
- GCF (Global Certification Forum) Mobile Device Compliance Standards
- Complies with ICNIRP Guidelines (International Commission for Non-Ionising Radiation Protection) for SAR (Specific Absorption Rate) compliance - this ensures electromagnetic emissions compliance.
- Contact Centre Standard – the vendor adheres to the Baldridge Quality Framework as adopted by NZ Business Excellence foundation, which has become the de-facto standard for NZ government
- ITIL (Information Technology Infrastructure Library) - Internal IT and Technology processes are aligned to ITIL version 3 principles
- NEBS (network equipment building systems) – standards for specifying resiliency and design guidelines of telecommunications equipment.

1.3.2. EROAD ENTERPRISE

The EROAD Enterprise is comprised of infrastructure, software, and services, all used to deliver solution functionality. The major components of the TOE are:

1) EROAD OBU,
2) EROAD OBU Gateway,
3) EROAD Web Portal and the
4) EROAD Depot Application user interface.

The EROAD OBU Gateway receives data from the EROAD OBU via private cellular network and transforms that data for use by the EROAD Depot Application. The EROAD Web Portal receives and sends data via the Internet to and from end users. This allows for human interaction with the EROAD Depot Application by means of a browser based user interface. Together, data fed to and from the EROAD solution are used to provide a variety of features and functions. These include weight-mileage tax calculation, regulatory compliance, and other value added services. See figure 5, EROAD Enterprise Architecture.

EROAD provides direct protection against physical tampering regarding the OBU via a variety of hard and soft mechanisms built into to the unit itself (described above).

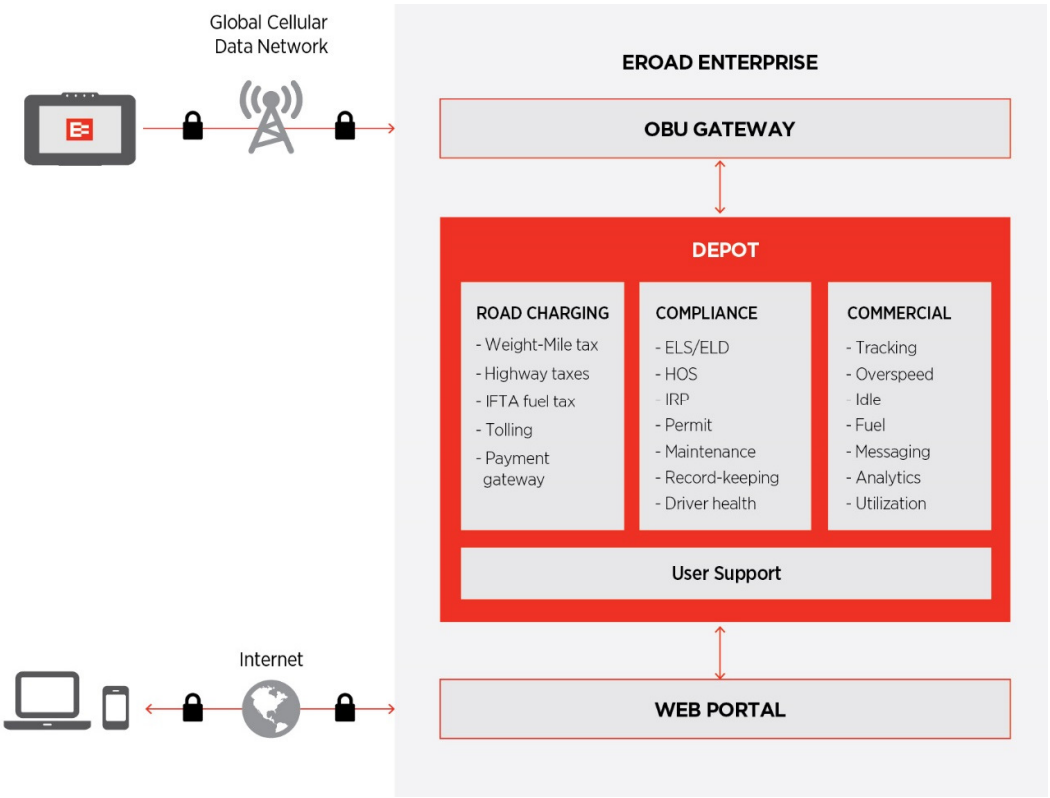

Figure 5: EROAD Enterprise Architecture

1.3.2.1. EROAD OBU GATEWAY

The EROAD OBU Gateway is comprised of software running on the EROAD Server(s). The EROAD OBU Gateway authenticates and authorizes communications to and from EROAD OBU endpoints over a secure private cellular network. The gateway manages and controls the transmission of all messages and events to/from each EROAD OBU secured via signed digital certificate as part of the environment as well as undisclosed user name and password as part of the TOE. Further, the EROAD OBU Gateway transforms all data passed between the EROAD OBUs and the EROAD Depot Application for use by each. All this is done using an authoritative application security framework. See figure 6, EROAD Enterprise – EROAD OBU Gateway.

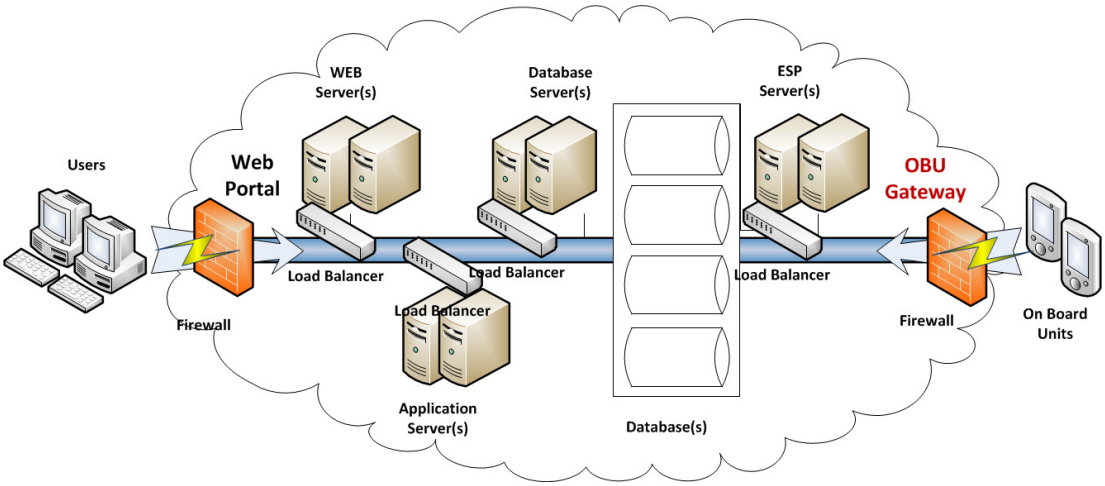

Figure 6: EROAD Enterprise – EROAD OBU Gateway

Additional cloud based infrastructure protects and secures the OBU Gateway and communications with it, but that environment is out of scope insofar as the TOE is concerned.

ESP Server

The ESP server and associated protocol (Ebox to Server Protocol) allow for the transformation and distribution of raw EROAD OBU events and messages. Events and messages are transmitted and transformed into a form that the EROAD Depot Application can use. As such, the ESP server acts as a staging area (database) that receives, transforms, and distributes data for use by the EROAD Depot Application. The only function of this server is to send, receive, and transform messages and events (data) to and from the EROAD OBU's so that system function can be properly realized. As such, the purpose of the Ebox to Server Protocol is to define the format of packet data sent to and from the EROAD OBU by the EROAD Depot Application, and by the EROAD OBU itself, as transformed by the ESP server (EROAD OBU Gateway).

The ESP Server and Protocol are the only means by which EROAD OBU's can be accessed remotely, aside from OTAP which is used to provision and update the firmware image itself. This is also done via the same private cellular network over secure encrypted connections. It is not possible to remotely access the EROAD OBU's or EROAD OBU Gateway by any other means.

1.3.2.2. EROAD Depot

The EROAD Depot Application is the heart of the EROAD solution and is implemented as a SaaS (Software provided as a Service). Communication with it is authenticated and authorized via the EROAD Web Portal and EROAD OBU Gateway. All data are processed and maintained here, regardless of origin. Data can be transmitted by the EROAD OBU (via the EROAD OBU Gateway), or by end users browsers (via the EROAD Web Portal). OBU data and user inputs fed into the EROAD Depot Application form the basis of services like calculating weight-mileage tax or RUC, regulatory compliance, and other value-added amenities. Various features of the EROAD Depot Application are available to end users via browser with authentication and authorization functionality provided by an authoritative application security framework. See figure 7, EROAD Enterprise – EROAD Depot.

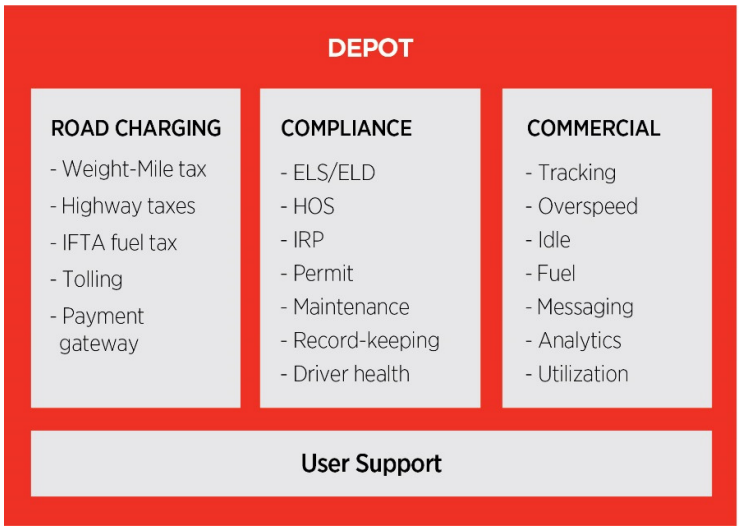

Figure 7: EROAD Enterprise – EROAD Depot

Road User Charging
Road user charging (RUC) is a distance and weight-based user charge for all trucks over 3.5 tons. It also applies to all vehicles that use diesel or other fuel that is not taxed at the source. It is assessed for the use of all public roads in New Zealand.

WMT/RUAF
Weight-mileage tax (WMT) allows carriers to monitor and report taxes owed, as well as road use assessment fees (RUAFs) electronically. It is assessed for the use of all public roads in the state of Oregon (USA).

Tolling
The EROAD solution supports interoperable tolling using conventional toll facilities. By utilizing the location tracking functionality of the EROAD OBU, together with map and geo-fencing tools in the EROAD Depot Application, the EROAD solution accurately and reliably detects toll crossings, and can collect toll payments on behalf of road operators.

Regulatory Services
The EROAD Depot Application features a range of regulatory services for carriers including Hours of Service, Servicing, Permitting, IFTA (International Fuel Tax Agreement), and IRP (International Registration Plan).

The aim of regulatory services is to allow carriers to remain compliant with relevant and applicable rules for the jurisdictions in which they operate. This includes the maintenance of auditable records used to verify compliance.

Commercial Services
The EROAD Depot Application includes various commercial services that complement road charging and regulatory compliance. These services are based on event data (distance and location) reported by the EROAD OBU and include Vehicle Tracking, Over-speed Detection, Idle Time, Fuel Consumption, Insurance Data, and Messaging.

Commercial and Compliance services are available to customers independently. A carrier's decision to use or not use any given commercial service has no impact on the regulatory compliance services like WMT, Hours of Service, or others.

1.3.2.3. EROAD WEB PORTAL

The EROAD Web Portal that allows end user access to the EROAD Depot Application is running on the EROAD Enterprise web server(s). The portal authenticates and authorizes all web based communications to and from the EROAD Depot Application, including:

- Enforcement of access control policies
- Ensuring secure internet connections
- Sending and receiving all data to and from web based end users
- Displaying all information that web based end users request

As part of the TOE, the application protects itself via role based authentication and authorization by means of user ID and password using an authoritative security framework. The application distinguishes between the following hierarchical end user roles (authorizations): Client Administrator, Unit Manager, RUC User, Reporting User, Service User, Basic User, and Super Basic User. In other words, the application establishes access permissions based on role, as part of the TOE. The EROAD Web Portal provides the same functionality for mobile users, within the more limited scope of a dedicated mobile site (subset).

See figure 8, EROAD Enterprise – EROAD Web Portal.

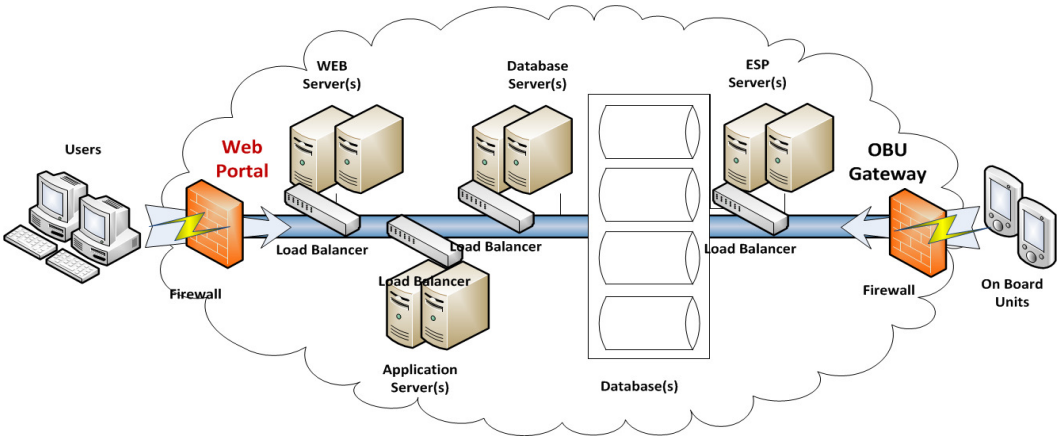

Figure 8: EROAD Enterprise – EROAD Web Portal

1.4. NOTATIONS AND FORMATTING

The notations and formatting used in this ST are consistent with version 3.1 Revision 4 of the Common Criteria (CC).

The **refinement** operation is used to add detail to a requirement, and thus further restricts a requirement. Refinement of security requirements is denoted by **bold text**. Deleted words are denoted by ~~strike-through text~~.

The **selection** operation is used to select one or more options provided by the CC in stating a requirement. Selections are denoted by *italicized* text in square brackets, [*Selection value*].

The **assignment** operation is used to assign a specific value to an unspecified parameter, such as the length of a password. Assignment is indicated by showing the value with bold face in square brackets, [**Assignment_value**].

The **iteration** operation is used when a component is repeated with varying operations. Iteration is denoted by showing the iteration number in parenthesis following the component identifier, (iteration_number).

Assets: Assets to be protected by the TOE are given names beginning with "AS." – e.g. AS.CLASSIFIED_INFO.

Assumptions: TOE security environment assumptions are given names beginning with "A."- e.g., A.Security_Procedures.

Threats: Threat agents are given names beginning with "TA." – e.g., TA.User. Threats to the TOE are given names beginning with "TT." – e.g., TT.Filter_Fails. TOE security environment threats are given names beginning with "TE."-- e.g., TE.Crypto_Fails.

Policies: TOE security environment policies are given names beginning with "P."—e.g., P.Information_AC.

Objectives: Security objectives for the TOE and the TOE environment are given names beginning with "O." and "OE.", respectively, - e.g., O.Filter-msg and OE.Clearance.

2. CC CONFORMANCE CLAIM (ASE_CCL)

This TOE and ST are conformant with the following specifications:

- CC Part 2: Security functional components, September 2012, Version 3.1, Revision 4, extended.
- CC Part 3: Security assurance components, September 2012, Version 3.1, Revision 4, conformant, EAL2 augmented with ALC_FLR.1.
- Assurance level: EAL2 augmented with ALC_FLR.1.
- Protection Profile: none.

3. SECURITY PROBLEM DEFINITION (ASE_SPD)

3.1. THREATS TO SECURITY

3.1.1. ASSETS

Assets	Description
AS.INFO_OBU	Time, Location, and Distance information residing in the EROAD OBU and transmitted as cellular data (messages/events) to EROAD OBU Gateway.
AS.INFO_APPLICATION	RUC, Oregon WMT/RUAF, Tolling, Regulatory and Commercial services residing in the EROAD Depot Application.
AS.FW_OBU	EROAD OBU firmware.
AS.SW_APPLICATION	EROAD Depot Application.

3.1.2. THREAT AGENTS

Threat Agents	Description
TA.FRAUDULENT	A person/company with skills and resources to mislead the system in any way necessary to avoid vehicle levies.
TA.OBU_CLIENT	EROAD OBU clients may unintentionally perform unauthorized actions.
TA.APPLICATION_USER	EROAD Application end users may unintentionally perform unauthorized actions.
TA.SYS_ADMIN	Authorized person/process that performs: • FW installation/updates of OBU • Configuration/set-up of OBU • SW installation/updates of application software • Configuration/set-up of application software in order to ensure that the TOE operates according to end users' needs. This category of personnel/process is an EROAD only system administrative function, performed only by EROAD support and engineering.
TA.MALFUNCTION	TOE malfunction.

3.1.3. IDENTIFICATION OF THREATS

3.1.3.1. THREATS TO THE TOE

Threats to the TOE	**Description**
TT.TAMPERING	The TOE may be subject to physical attack that may compromise information and data processing.
Threat agent:	TA.FRAUDULENT
Assets:	AS.INFO_OBU, AS.INFO_APPLICATION
Attack method:	A person opens and tampers with the OBU to: • Change or remove Time, Location, and Distance information. • Install/Modify SW/FW/HW to change the event generation. A person tampers with the Application to: • Change or remove information about RUC, Oregon WMT/RUAF, Tolling, Regulatory and Commercial services.

TT.MALFUNCTION	A) The TOE may malfunction which may compromise information and data processing. B) The TOE may malfunction which may compromise roles and permissions.
Threat agent:	A) TA.MALFUNCTION together with TA.FRAUDULENT or TA.CLIENT B) TA.MALFUNCTION together with TA.APPLICATION_USER or TA.SYS_ADMIN
Assets:	AS.INFO_OBU, AS.INFO_APPLICATION, AS.FW_OBU and AS.SW_APPLICATION
Attack method:	A) A malfunction in the TOE implies errors with: • Time, Location and Distance information in OBU. • Event generation in OBU. • Regulatory and commercial services in Application. • RUC, WMT/RUAF and Tolling services in Application. B) A malfunction in the TOE implies that a person will gain unauthorized roles and permissions in Application.
TT.SPOOFING	Eavesdropping of the communication between EROAD OBU and EROAD OBU GATEWAY, changing the cellular data and transmitting the changed cellular data.
Threat agent:	TA.FRAUDULENT
Assets:	AS.INFO_OBU
Attack method:	An unauthorized person with no physical access to the radios is eavesdropping on the communication between EROAD OBU and EROAD OBU GATEWAY, changes the cellular data and transmits the changed cellular data in order to achieve error in generated RUC, WMT/RUAF and Tolling.
TT.BYPASSING	Bypassing of a security mechanism may compromise information and data processing in EROAD Application.
Threat agent:	TA.FRAUDULENT
Assets:	AS.INFO_APPLICATION and AS.SW_APPLICATION
Attack method:	A person may bypass a security mechanism in the EROAD Application to: • Change/Remove RUC, WMT/RUAF, Tolling, regulatory and commercial information. • Install/Modify SW to change RUC, WMT/RUAF, Tolling, regulatory and commercial services. • Change configuration data to make the TOE inoperable (DoS - Denial of Service) or to cause fault in operations.
TT.WRONG_SW_FW	Wrong software (EROAD Application) or firmware (EROAD OBU) versions are installed in the TOE, making the TOE inoperable.
Threat agent:	TA.SYS_ADMIN
Assets:	AS. INFO_APPLICATION, AS.SW_APPLICATION, AS. INFO_OBU and AS.FW_OBU
Attack method:	During service or production, the maintenance personnel unintentionally installs wrong SW/FW versions in the TOE, making the TOE inoperable or SW/FW updates concerning security are missed.

Threats to the TOE	Description
TT.GPS_SCRAMBLING	Scrambling the GPS signalling to the EROAD OBU may alter information and data processing. This can be caused by natural causes like tunnel driving, but also by obscure causes that hide the vehicle movement or reduce/change the generated levies.
Threat agent:	TA.FRAUDULENT
Assets:	AS.INFO_OBU
Attack method:	A person is scrambling the GPS signal to the EROAD OBU to alter Time, Location and Distance information, in order to achieve error in the cellular data transmitted from the EROAD OBU to the EROAD OBU Gateway.

3.1.3.2. THREATS TO THE TOE ENVIRONMENT

Threats to the TOE environment	Description
TE.SYS_ADMIN_FAIL	The system administrator fails to perform functions essential to the security.
Threat agent:	TA.SYS_ADMIN
Assets:	AS.INFO_APPLICATION
Attack method:	The system administrator fails to or forgets to update the TOE with security patches.
TE.EXPLOIT_VULN	A person/company tries to exploit vulnerability in the TOE to get unauthorized access to EROAD Application information.
Threat agent:	TA.FRAUDULENT
Assets:	AS.INFO_APPLICATION
Attack method:	A threat agent use hacking methods to exploit weakness in the TOE.
TE.HACK_AC	A person/company gets undetected system access to the TOE due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality or availability.
Threat agent:	TA.FRAUDULENT
Assets:	AS.INFO_APPLICATION and AS.SW_APPLICATION
Attack method:	A threat agent uses hacking methods to exploit missing, weak or incorrectly implemented access control in the TOE.

3.2. ORGANIZATIONAL SECURITY POLICIES

Organizational security Policies	Description
P.CRYPTOGRAPHY	The TOE (EROAD OBU) shall provide cryptographic functions for its own use, including encryption/decryption operations.
P.CRYPTO_VALIDATED	Only FIPS 140-2 compliant cryptography is acceptable for key management and cryptographic services on the OBU.
P.SW_FW	All installations of and changes to EROAD software/firmware shall be done by EROAD, following strict change control and configuration management processes and procedures.
P.PATCH	The patch policy for the TOE environment must be sufficient to stop all known, publicly available vulnerabilities in the TOE environment software.

3.3. ASSUMPTIONS

Assumptions	Description
A.MANAGE	There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains.
A.AREA.PROTECT	The EROAD Depot Application, EROAD OBU Gateway and EROAD Web Portal will be placed in a physically and logically protected area.

4. SECURITY OBJECTIVES (ASE_OBJ)

4.1. TOE SECURITY OBJECTIVES

Security Objectives	Description
O.TAMPER_RESISTANCE	Tampering shall be monitored continuously on the EROAD OBU hardware. If sensors report attempts to tamper, the Tamper Detection module shall erase the access keys on the EROAD OBU. This shall disable the EROAD OBU, and the EROAD OBU must be returned to EROAD to be reactivated. EROAD provides direct protection against physical tampering regarding the OBU via a variety of hard and soft mechanisms built into to the unit itself.
O.ID_AUTH	The different end user roles must identify and authenticate themselves to the TOE (Depot Application via Web Portal) prior to getting access to their functions and data. The different OBU units must identify and authenticate themselves to the TOE (Depot Application via OBU Gateway) prior to communication between OBU and the Depot Application.
O.ACCESS	The TOE must allow authorized end users to access only appropriate TOE functions and data. The TOE must allow only authorized EROAD OBU units to access the system.
O.CRYPTOGRAPHY	The TOE shall provide cryptographic functions to maintain the confidentiality of the data that is transmitted between EROAD OBU and OBU Gateway.
O.CRYPTO_VALIDATED	The TOE shall use FIPS 140-2 compliant crypto modules for cryptographic services implementing approved security functions and services used by cryptographic functions on the EROAD OBU.
O.AUDIT	The TOE shall record security critical errors and messages.
O.PROTECT	The TOE must protect itself from unauthorized modifications and access to its functions and data. The EROAD OBU is physically exposed and must protect itself. The Depot Application user interface must protect itself when exposed. The EROAD Web Portal and the EROAD OBU Gateway are the entry points to the EROAD Depot Application, where identification, authentication and authorization are initiated.
O.INTEGRITY	The TOE must ensure the integrity of all audit and system data.
O.ADMINISTRATION	The TOE must include a set of functions that allow effective administration of its functions and data.

4.2. OPERATIONAL ENVIRONMENT SECURITY OBJECTIVES

Security Objectives	Description
OE.PROTECTION	The EROAD Depot Application, EROAD OBU Gateway and EROAD Web Portal are placed in a physically and logically protected area. Only authorized personnel have admission to the protected area. Only authorized personnel have admission to configure and manage the EROAD Depot Application, EROAD OBU Gateway and EROAD Web Portal and its underlying components.
OE.PERSON	Personnel working as authorized system administrators shall be carefully selected and trained for proper operation of the TOE.

4.3. SECURITY OBJECTIVES RATIONALE

Threats/ Policies/ Assumptions / **Objectives**	TT.TAMPERING	TT.MALFUNCTION	TT.SPOOFING	TT.BYPASSING	TT.WRONG_SW_FW	TT.GPS_SCRAMBLING	TE.SYS_ADMIN_FAIL	TE.EXPLOIT_VULN	TE.HACK_AC	P.CRYPTOGRAPHY	P.CRYPTO_VALIDATED	P.SW_FW	P.PATCH	A.MANAGE	A.AREA.PROTECT
TOE Security Objectives															
O.TAMPER_RESISTANCE	X														
O.ID_AUTH		X		X											
O.ACCESS		X		X											
O.CRYPTOGRAPHY	X	X	X						X	X	X				
O.CRYPTO_VALIDATED											X				
O.AUDIT	X	X				X			X						
O.PROTECT	X	X		X				X	X						
O.INTEGRITY		X		X					X						
O.ADMINISTRATION					X		X	X	X			X			
Operational Environment Security Objectives															
OE.PROTECTION														X	X
OE.PERSON					X		X	X	X			X	X	X	

Table 1: Mapping of Objectives to Threats, Policies and Assumptions.

TT.TAMPERING:
The EROAD OBU is protected by devices and elements that notify administrative functions in the event of physical attack (O.TAMPER_RESISTANCE), and errors are recorded (O.AUDIT). Cryptographic functions shall maintain the confidentiality of the data transmitted between EROAD OBU and EROAD OBU GATEWAY (O.CRYPTOGRAPHY). The EROAD OBU and the Depot Application user interface shall protect themselves (O.PROTECT).

TT.MALFUNCTION:
A TOE malfunction can compromise information and data processing, roles and permissions. Errors are recorded (O.AUDIT), and cryptographic functions shall maintain the confidentiality of the data transmitted between EROAD OBU and EROAD Gateway (O.CRYPTOGRAPHY). End users must identify themselves to the EROAD Depot Application via the EROAD Web Portal and be authenticated and authorized prior to getting access. The OBU units must identify themselves to the EROAD Depot Application via the EROAD OBU Gateway (ESP Server) and be authenticated and authorized prior to communication between OBU and the Depot (O.ID_AUTH). End users and OBU units shall access only appropriate TOE functions and data (O.ACCESS). The TOE must protect itself from

unauthorized modifications and access to its functions and data (O.PROTECT), and ensure the integrity of all audit and system data (O.INTEGRITY).

TT.SPOOFING:
Eavesdropping on the communication between EROAD OBU and EROAD OBU Gateway will change the cellular data and transmit the changed cellular data. Cryptographic functions shall maintain the confidentiality of the data transmitted between EROAD OBU and EROAD OBU Gateway (O.CRYPTOGRAPHY).

TT.BYPASSING:
Bypassing of a security mechanism will compromise information and data processing in EROAD Application. End users must identify and authenticate themselves to the TOE prior to getting access. The different OBU units must identify themselves and be authenticated and authorized via the OBU Gateway prior to gaining access to the Depot Application (O.ID_AUTH). End users shall access only appropriate TOE functions and data, and only OBU units transfer messages and events to and from the ESP server database (O.ACCESS). The TOE (OBU and Depot Application) must protect itself from unauthorized modifications and access to its functions and data (O.PROTECT), and ensure the integrity of all audit and system data (O.INTEGRITY).

TT.GPS_SCRAMBLING
Scrambling the GPS signalling to the EROAD OBU may alter information and data processing. This can be caused by natural causes like tunnel driving, but also by obscure causes that hide vehicle movement or reduce/change the generated levies. Errors are recorded (O.AUDIT).

TT.WRONG_SW_FW:
Wrong software (EROAD Application) or firmware (EROAD OBU) versions can be installed in the TOE, making the TOE inoperable. The TOE must include a set of functions that allow effective administration of its functions and data (O.ADMINISTRATION). Personnel working as authorized system administrators shall be carefully selected and trained for proper operation of the TOE (OE.PERSON).

TE.SYS_ADMIN_FAIL:
The system administrator can fail to perform functions essential to security. The TOE must include a set of functions that allow effective administration of its functions and data (O.ADMINISTRATION). Personnel working as authorized system administrators shall be carefully selected and trained for proper operation of the TOE (OE.PERSON).

TE.EXPLOIT_VULN:
A person or company might try to exploit vulnerability in the TOE environment to get unauthorized access to EROAD Application information. The TOE must protect itself from unauthorized modifications and access to its functions and data (O.PROTECT). Personnel working as authorized system administrators shall be carefully selected and trained for proper operation of the TOE (OE.PERSON), and the TOE must include a set of functions that allow effective administration of its functions and data (O.ADMINISTRATION).

TE.HACK_AC:
A person/company can get undetected system access to TOE due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality or availability. Personnel working as authorized system administrators shall be carefully selected and trained for proper operation of the TOE (OE.PERSON), and the TOE must include a set of functions that allow effective administration of its functions and data (O.ADMINISTRATION). Errors are recorded (O.AUDIT), and the TOE must protect itself from unauthorized modifications and access to its functions and data (O.PROTECT), and ensure the integrity of all audit and system data (O.INTEGRITY).

P.CRYPTOGRAPHY:
The TOE (OBU) shall provide cryptographic functions to maintain the confidentiality of the data that is transmitted between EROAD OBU and OBU Gateway. (O.CRYPTOGRAPHY).

P.CRYPTO_VALIDATED:
Only FIPS 140-2 compliant cryptography is acceptable for credential management and cryptographic services on the OBU. The TOE (OBU) shall use FIPS 140-2 compliant crypto modules for cryptographic services implementing approved security functions and services used by cryptographic functions of the EROAD OBU (O.CRYPTO_VALIDATED), and cryptographic functions shall maintain the confidentiality of EROAD OBU generated data transmitted between EROAD OBU and EROAD OBU Gateway (O.CRYPTOGRAPHY).

P.SW_FW:
All installations of and changes to EROAD software/firmware shall be done by EROAD, following strict change control and configuration management processes and procedures. The TOE must include a set of functions that allow effective administration of its functions and data (O.ADMINISTRATION), and personnel working as authorized system administrators shall be carefully selected and trained for proper operation of the TOE (OE.PERSON).

P.PATCH:
The patch policy for the TOE environment must be sufficient for stopping all known, publicly available vulnerabilities in the TOE environment software. Personnel working as authorized system administrators shall be carefully selected and trained for proper operation of the TOE (OE.PERSON).

A.MANAGE:
There will be one or more competent individuals assigned to manage the TOE and the security of the information it contains. Personnel working as authorized system administrators shall be carefully selected and trained for proper operation of the TOE (OE.PERSON). Only authorized personnel have access to configure and manage the EROAD Depot Application, EROAD OBU Gateway and EROAD Web Portal and its underlying components (OE.PROTECTION).

A.AREA.PROTECT:
The EROAD Depot Application, EROAD OBU Gateway and EROAD Web Portal shall be placed in a physically and logically protected area only accessable by authorized personnel (OE.PROTECTION).

5. EXTENDED COMPONENTS DEFINITION (ASE_ECD)

FPT_ITT_EXP.1 BASIC INTERNAL TSF DATA TRANSFER PROTECTION

Management: There are no management functions.

Audit: There are no auditable events.

Hierarchical to: No other components.

Dependencies: None.

FPT_ITT_EXP.1.1 The TSF shall use its own mechanisms and mechanisms of the Operational environment to protect TSF data from [*selection: disclosure, modification*] when it is transmitted between separate parts of the TOE.

EXTENDED COMPONENTS RATIONALE

The following explicit components have been included in this Security Target because the Common Criteria components were found to be insufficient as stated.

Explicit Component	Identifier	Rationale
FPT_ITT_EXP.1	Basic internal TSF data transfer protection	This explicit component is necessary since it provides for the use of secure communications mechanisms of the Operational Environment.

6. SECURITY REQUIREMENTS (ASE_REQ)

6.1. SECURITY FUNCTIONAL REQUIREMENTS (SFRS)

Functional Class	Functional Class description	Functional Components
FAU	Security audit	FAU_GEN.1, FAU_GEN.2
FCS	Cryptographic support	FCS_CKM.1, FCS_CKM.4, FCS_COP.1
FDP	User data protection	FDP_ACC.1(a), FDP_ACC.1(b), FDP_ACF.1(a), FDP_ACF.1(b), FDP_IFC.1, FDP_IFF.1
FIA	Identification and authentication	FIA_ATD.1, FIA_UAU.1, FIA_UID.1
FMT	Security management	FMT_MOF.1, FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1
FPT	Protection of the TSF	FPT_ITT_EXP.1, FPT_PHP.2, FPT_STM.1

Table 2: Security Functional Requirements

6.1.1. SECURITY AUDIT (FAU)

6.1.1.1. FAU_GEN.1 AUDIT DATA GENERATION

Dependences: FPT_STM.1 Reliable time stamps

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the [*not specified*] level of audit; and
c) [**Auditable events: EROAD OBU and EROAD Depot Application security critical errors and messages**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**None**].

6.1.1.2. FAU_GEN.2 USER IDENTITY ASSOCIATION

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall

be able to associate each auditable event with the identity of the user that caused the event.

6.1.2. CRYPTOGRAPHIC SUPPORT (FCS)

6.1.2.1. FCS_CKM.1 CRYPTOGRAPHIC KEY GENERATION

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or
FCS_COP.1 Cryptographic operation]
FCS_CKM.4 Cryptographic key destruction

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[NIST Special Publication 800-135, NIST Special Publication 800-90]** and specified cryptographic key sizes **[128-bit]** that meet the following: **[FIPS PUB 197, FIPS PUB 198]**.

6.1.2.2. FCS_CKM.4 CRYPTOGRAPHIC KEY DESTRUCTION

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method **[zeroization of keys in OBU]** that meets the following: **[FIPS PUB 140-2]**.

6.1.2.3. FCS_COP.1 CRYPTOGRAPHIC OPERATION

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or
FDP_ITC.2 Import of user data with security attributes, or
FCS_CKM.1 Cryptographic key generation]
FCS_CKM.4 Cryptographic key destruction

FCS_COP.1.1 The TSF shall perform **[listed in Table 3: Cryptographic Operation]** in accordance with a specified cryptographic algorithm **[listed in Table 3: Cryptographic Operation]** and cryptographic key sizes **[listed in Table 3: Cryptographic Operation]** that meet the following: **[listed in Table 3: Cryptographic Operation]**.

Cryptographic operations	Cryptographic algorithm	Key sizes (bits)	Standards
Encryption/decryption	AES	128	FIPS PUB 197
Hashing	SHA-256/SHA-1	N/A	FIPS PUB 180-4
Message Authentication Code	HMAC-SHA256 /HMAC-SHA1	256/160	FIPS PUB 198
TLS Session Keys Generation	DRBG HMAC-SHA256 / TLS KDF	128/160/256	NIST SP800-90 NIST SP800-135
Key Exchange	EC Diffie-Hellman	256	None
Digital Signature	EC DSA	256	FIPS 186-4

Table 3: Cryptographic Operation

6.1.3. User Data Protection (FDP)

6.1.3.1. FDP_ACC.1(a) Subset access control – End User Access Control

Dependences: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [**End User Access Control SFP**] on [subjects: **end users**, objects: **EROAD Depot Application via browser located on the end users client machine via the EROAD Web portal**, operations: **data access**].

6.1.3.2. FDP_ACC.1(b) Subset access control – OBU Unit Access Control

Dependences: FDP_ACF.1 Security attribute based access control

FDP_ACC.1.1 The TSF shall enforce the [**OBU Unit Access Control SFP**] on [subjects: **EROAD OBU units**, objects: **EROAD Depot Application via the EROAD OBU Gateway (ESP Server)**, operations: **send and receive data**].

6.1.3.3. FDP_ACF.1(a) Security attribute based access – End User Access Control

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [**End User Access Control SFP**] to objects based on the following: [subjects: **end users**, subject attributes: **User ID, password,** object: **EROAD Depot Application via browser located on the end users client machine via the EROAD Web portal**, object attributes: **none**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**End-user Privilege Levels**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**no additional rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**no additional rules**].

6.1.3.4. FDP_ACF.1(b) Security attribute based access – OBU Unit Access Control

Dependencies: FDP_ACC.1 Subset access control
FMT_MSA.3 Static attribute initialisation

FDP_ACF.1.1 The TSF shall enforce the [**OBU Unit Access Control SFP**] to objects based on the following: [subjects: **EROAD OBU units**, subject attributes: **user name, password**, object: **EROAD Depot Application via the EROAD OBU Gateway (ESP Server)**, object attributes: **CA Public Key**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**no additional rules**].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**no additional rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**no additional rules**].

6.1.3.5. FDP_IFC.1 SUBSET INFORMATION FLOW CONTROL

Dependences: FDP_IFF.1 Simple security attributes

FDP_IFC.1.1 The TSF shall enforce the **[information flow control SFP]** on [subjects: **end users**, information: **protected application resources**, operations: **access**].

6.1.3.6. FDP_IFF.1 SIMPLE SECURITY ATTRIBUTES

Dependences: FDP_IFC.1 Subset information flow control
FMT_MSA.3 Static attribute initialisation

FDP_IFF.1.1 The TSF shall enforce the **[information flow control SFP]** based on the following types of subject and information security attributes: [subjects: **end users**, subject attributes: **User ID, password**, information: **protected application resources**, information attributes: **URLs of web pages, page objects interfaces, data attributes**].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**the end user has been granted access to the application resource by the EROAD Depot application**].

FDP_IFF.1.3 The TSF shall enforce the [**no additional information flow control SFP rules**].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [**no additional information flow control SFP rules**].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [**no additional information flow control SFP rules**].

6.1.4. IDENTIFICATION AND AUTHENTICATION (FIA)

6.1.4.1. FIA_ATD.1 USER ATTRIBUTE DEFINITION

Dependences: None.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**User ID, password**].

6.1.4.2. FIA_UAU.1 TIMING OF AUTHENTICATION

Dependences: FIA_UID.1 Timing of identification

FIA_UAU.1.1 The TSF shall allow **[identification, connection establishment, non-security relevant functionalities accessible via the OBU's touch screen]** on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.4.3. FIA_UID.1 TIMING OF IDENTIFICATION

Dependences: None.

FIA_UID.1.1 The TSF shall allow **[connection establishment, non-security relevant functionalities accessible via the OBU's touch screen]** on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

6.1.5. SECURITY MANAGEMENT (FMT)

6.1.5.1. FMT_MOF.1 MANAGEMENT OF SECURITY FUNCTIONS BEHAVIOUR

Dependences: FMT_SMF.1 Specification of Management Functions
FMT_SMR.1 Security roles

FMT_MOF.1.1 The TSF shall restrict the ability to [*determine the behaviour of*] the functions **[management of user accounts]** to **[TOE System Administrator and Client Administrator]**.

6.1.5.2. FMT_MSA.1 MANAGEMENT OF SECURITY ATTRIBUTES

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

FMT_MSA.1.1 The TSF shall enforce the [**TOE System Administrator Access Control SFP**] to restrict the ability to [*modify*] the security attributes [**user name, password**] to [**TOE System Administrator and Client Administrator**].

6.1.5.3. FMT_MSA.3 STATIC ATTRIBUTE INITIALISATION

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MSA.3.1 The TSF shall enforce the [**TOE System Administrator Access Control SFP**] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**TOE System Administrator and Client Administrator**] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.4. FMT_SMF.1 SPECIFICATION OF MANAGEMENT FUNCTIONS

Dependencies: None.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [**SW/FW installation/updates and configuration/set-up of the system/system components, management of user accounts, and management of security attributes**].

6.1.5.5. FMT_SMR.1 Security roles

Dependencies: FIA_UID.1 Timing of identification

FMT_SMR.1.1 The TSF shall maintain the roles **[administrators: TOE System Administrator; end users: Client Administrator, Unit Manager, RUC User, Reporting User, Service User, Basic User and Super Basic User]**.

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

6.1.6. Protection of the TSF (FPT)

6.1.6.1. FPT_ITT_EXP.1 Basic internal TSF data transfer protection

Dependencies: None.

FPT_ITT_EXP.1.1 The TSF shall use its own mechanisms and mechanisms of the Operational environment to protect TSF data from [*modification*] when it is transmitted between separate parts of the TOE.

6.1.6.2. FPT_PHP.2 Notification of physical attack

Dependencies: FMT_MOF.1 Management of security functions behaviour

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3 For [**EROAD OBU**], the TSF shall monitor the devices and elements and notify [**TOE System Administrator**] when physical tampering with the TSF's devices or TSF's elements has occurred.

6.1.6.3. FPT_STM.1 Reliable time stamps

Dependencies: None.

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

6.2. Security assurance requirements (SARs)

The assurance level of the TOE is EAL2 augmented with ALC_FLR.1.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.2 Use of a CM system
	ALC_CMS.2 Parts of the TOE CM coverage

Assurance Class	Assurance Components
	ALC_DEL.1 Delivery procedures
	ALC_FLR.1 Basic flaw remediation
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.1 Evidence of coverage
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 4: Assurance requirements

6.3. SECURITY REQUIREMENTS RATIONALE

6.3.1. RELATION BETWEEN SFRS AND SECURITY OBJECTIVES

Requirements / Objectives	FAU_GEN.1	FAU_GEN.2	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FDP_ACC.1(a)	FDP_ACC.1(b)	FDP_ACF.1(a)	FDP_ACF.1(b)	FDP_IFC.1	FDP_IFF.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_ITT_EXP.1	FPT_PHP.2	FPT_STM.1
O.TAMPER_RESISTANCE																					X	
O.ID_AUTH												X	X	X								
O.ACCESS						X	X	X	X	X	X		X	X								
O.CRYPTOGRAPHY			X	X	X																	
O.CRYPTO_VALIDATED			X	X	X																	
O.AUDIT	X	X																				X
O.PROTECT															X	X	X	X				
O.INTEGRITY																		X		X	X	
O.ADMINISTRATION															X	X	X	X	X		X	

Table 5: Tracing of functional requirements to objectives

6.3.1.1. O.TAMPER_RESISTANCE

The EROAD OBU is protected by devices and elements that notify administrative functions in the event of physical attack. **FPT_PHP.2** provides monitoring of TOE and notifies system administrators when physical tampering with the TOE has occurred.

6.3.1.2. O. ID_AUTH

The different end user roles must identify themselves to the TOE and be authenticated and authorized by it via the EROAD Web Portal prior to getting access to their functions and data. The OBU units must identify themselves to the TOE (EROAD Depot Application) and be authenticated and authorized by it via the EROAD OBU Gateway prior to getting access to their functions and data. **FIA_UID.1** only allows connection establishment and non-security relevant functionalities accessible via the OBU's touch screen prior to a user being identified. End users must be identified before they are able to perform any other actions. **FIA_UAU.1** only allows identification, connection establishment and non-

security relevant functionalities accessible via the OBU's touch screen prior to a user being authenticated. End users must be successfully authenticated before they are able to perform any other actions. **FIA_ATD.1** defines security attributes of subjects used to enforce the authentication policy of the TOE.

6.3.1.3. O.ACCESS

The TOE must allow authorized end users to access only appropriate TOE functions and data. The TOE must allow only authorized EROAD OBU units to access the system. **FDP_ACC.1(a) and FDP_ACC.1(b)** requires the TOE to enforce Access Control SFP. **FDP_ACF.1(a)** and **FDP_ACF.1(b)** specifies the attributes used to enforce Access Control SFP. **FDP_IFC.1** requires the TOE to enforce Information Flow Control SFP. **FDP_IFF.1** specifies the attributes used to enforce Information Flow Control SFP. **FIA_UID.1** only allows connection establishment and non-security relevant functionalities accessible via the OBU's touch screen prior to a user being identified. End users must be identified before they are able to perform any other actions. **FIA_UAU.1** only allows identification, connection establishment non-security relevant functionalities accessible via the OBU's touch screen prior to a user being authenticated. End users must be successfully authenticated before they are able to perform any other actions.

6.3.1.4. O.CRYPTOGRAPHY

The TOE (EROAD OBU) shall provide cryptographic functions to maintain the confidentiality of the data that is transmitted between EROAD OBU and OBU Gateway. **FCS_COP.1** requires the TOE to perform encryption in accordance with the specified cryptographic algorithm AES. **FCS_CKM.1** requires the TOE (EROAD OBU) to generate cryptographic keys in accordance with the specified cryptographic key generation algorithm RN generator. **FCS_CKM.4** requires the TOE (EROAD OBU) to destroy cryptographic keys by overwriting previous key with a new key.

6.3.1.5. O.CRYPTO_VALIDATED

The TOE (EROAD OBU) shall use FIPS 140-2 compliant crypto modules for cryptographic services implementing approved security functions services used by cryptographic functions local to the EROAD OBU. **FCS_COP.1** requires the TOE to perform encryption in accordance with the specified cryptographic algorithm AES. **FCS_CKM.1** requires the TOE to generate cryptographic keys in accordance with the specified cryptographic key generation algorithm RN generator. **FCS_CKM.4** requires TOE (EROAD OBU) to destroy cryptographic keys by overwriting previous key with new key.

6.3.1.6. O.AUDIT

The TOE must record EROAD OBU and EROAD Depot Application security critical errors and messages. **FAU_GEN.1** requires that the TOE record EROAD OBU and EROAD Depot Application security critical errors and messages. **FAU_GEN.2** requires that the TOE associate each auditable event with the identity of the user that caused the event. **FPT_STM.1** requires that the TOE provide reliable timestamps for its own use.

6.3.1.7. O.PROTECT

The TOE must protect itself from unauthorized modifications and access to its functions and data. **FMT_MOF.1** requires that the TOE provide the ability to restrict managing functions of the TOE to authorized administrators of the TOE. **FMT_SMF.1** supports this objective by identifying the corresponding management functions. **FMT_MSA.1** specifies which end user roles can access security attributes. **FMT_MSA.3** defines static attribute initialization for the Administrator Access Control SFP.

6.3.1.8. O.INTEGRITY

The TOE must ensure the integrity of all audit and system data. **FPT_PHP.2** provides monitoring of EROAD OBU and notifies system administrators at EROAD when physical tampering with the EROAD OBU has occurred. **FPT_ITT_EXP.1** requires the TOE to protect the collected data and ensure its integrity when the data is transmitted to a separate part of the TOE. **FMT_SMF.1** supports this objective by identifying the corresponding management functions.

6.3.1.9. O.ADMINISTRATION

The TOE must include a set of functions that allow effective administration of its functions and data. **FMT_MSA.3** defines static attribute initialization for the Administrator Access Control SFP. **FPT_PHP.2** provides monitoring of EROAD OBU and notifies system administrators at EROAD Enterprise when physical tampering with the EROAD OBU has occurred. **FMT_MOF.1** requires that the TOE provide the ability to restrict managing functions of the TOE to authorized administrators of the TOE. **FMT_SMF.1** supports this objective by identifying the corresponding management functions. **FMT_SMR.1** requires the TOE to maintain separate end user roles. **FMT_MSA.1** specifies which end user roles can access security attributes.

6.3.2. SFR DEPENDENCIES

The table below shows the dependencies of the security functional requirement of the TOE and gives a rationale for each of them if they are included or not.

Security functional requirement	Dependency	Dependency Rationale
FAU_GEN.1 Audit data generation	FPT_STM.1 Reliable time stamps	Included
FAU_GEN.2 User identity association	FAU_GEN.1 Audit data generation FIA_UID.1 Timing of identification	Included
FCS_CKM.1 Cryptographic key generation	[FCS_CKM.2 Cryptographic key distribution, or FCS_COP.1 Cryptographic operation] FCS_CKM.4 Cryptographic key destruction	Included
FCS_CKM.4 Cryptographic key destruction	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation]	Included
FCS_COP.1 Cryptographic Operation	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	Included

Security functional requirement	Dependency	Dependency Rationale
FDP_ACC.1(a) Subset access control – End User Access Control	FDP_ACF.1(a) Security attribute based access – End User Access Control	Included
FDP_ACC.1(b) Subset access control – OBU Unit Access Control	FDP_ACF.1(b) Security attribute based access – OBU Unit Access Control	Included
FDP_ACF.1(a) Security attribute based access – End User Access Control	FDP_ACC.1(a) Subset access control – End User Access Control FMT_MSA.3 Static attribute initialisation	Included
FDP_ACF.1(b) Security attribute based access – OBU Unit Access Control	FDP_ACC.1(b) Subset access control – OBU Unit Access Control FMT_MSA.3 Static attribute initialisation	Included
FDP_IFC.1 Subset information flow control	FDP_IFF.1 Simple security attributes	Included
FDP_IFF.1 Simple security attributes	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialization	Included
FIA_ATD.1 User attribute definition	None	
FIA_UAU.1 Timing of authentication	FIA_UID.1 Timing of identification	Included
FIA_UID.1 Timing of identification	None	
FMT_MOF.1 Management of security functions behaviour	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles	Included
FMT_MSA.1 Management of security attributes	[FDP_ACC.1(a) Subset access control – End User Access Control, or FDP_IFC.1 Subset information flow control] FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security roles	Included
FMT_MSA.3 Static attribute initialisation	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	Included
FMT_SMF.1 Specification of Management Functions	None	
FMT_SMR.1 Security roles	FIA_UID.1 Timing of identification	Included
FPT_ITT_EXP.1 Basic internal TSF data transfer protection	None	
FPT_PHP.2 Notification of physical attack	FMT_MOF.1 Management of security functions behaviour	Included
FPT_STM.1 Reliable time stamps	None	

Table 6: SFR's dependencies and rationale

6.3.3. SAR RATIONALE

The SARs specified in this ST are according to EAL2 augmented with ALC_FLR.1. The SARs that were chosen are consistent with best industry practices for Common Criteria evaluation of similar products.

7. TOE SUMMARY SPECIFICATION (ASE_TSS)

7.1. TOE SECURITY FUNCTIONS SPECIFICATION

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in section 6.1 Security Functional Requirements (SFRs).

7.1.1. SF.TAMPER

Tampering is continuously monitored on the EROAD OBU hardware. Time, Location, and Distance information is gathered from both GPS satellite data and internal vehicle sensors, and cross checked. This information is processed by the Event Generation Engine along with indications of tampering (tamper sensors and cross checks on data) and power state. If EROAD OBU sensors report attempts to tamper, the Tamper Detection module erases relevant keys on the EROAD OBU. This includes a hardware reset to reinitialise memory. This disables the EROAD OBU, so the unit is no longer able to communicate with the OBU Gateway. The EROAD OBU must be returned to EROAD to be reactivated.

EROAD provides direct protection against physical tampering on the OBU via a variety of hard and soft mechanisms built into to the unit itself (described elsewhere in this document).

EROAD OBU is protected by devices and elements that notify administrative functions in the event of physical attack, and errors are recorded. Cryptographic functions maintain the confidentiality of the data transmitted between EROAD OBU and EROAD OBU GATEWAY. The TOE protects itself from unauthorised modifications and access to its functions and data.

7.1.2. SF.AUTHENTICATION

Authentication based on user ID and password is required for login to the EROAD Depot Web Portal. Immediately thereafter, access controllers determine authorized scope (pages, page objects and data). Authorized scope is determined by organization ID and role. Both are associated with the user ID. Therefore, unauthenticated access and unauthorized scope is not possible. All access violations are logged and identified by user ID, originating IP address and the date/time the violation occurred. In the event of an access violation a user is immediately logged out of the TOE.

The different end user roles identify themselves to the TOE and are authenticated and authorized by it prior to getting access to their functions and data. For end users accessing the EROAD Depot Application via the browser based user interface, access is authenticated and authorized via user ID and password as part of the TOE. Permissions are based on role which is determined by user. As part of the TOE, the Depot Application distinguishes between the following hierarchical end user roles (authorizations): Client Administrator, Unit Manager, RUC User, Reporting User, Service User, Basic User and Super Basic User. All this is done using an authoritative application security framework, which limits access to both pages and data based on role and organization.

The EROAD OBU's are authenticated and authorized by the EROAD Depot Application via the EROAD OBU Gateway and the secure connection established with it. Each EROAD OBU is authenticated using a user ID and password. The OBUs are authenticated and authorized by EROAD Depot Application based web services. The OBU's authorization is extremely limited and is not part of the hierarchical permissions scheme which defines end users roles. All the OBU can do is post raw event data to an isolated staging area.

End users may access non-security relevant functions on the OBU touchscreen without authenticating to the OBU. Access to non-security relevant functions is limited to: Change Vehicle Configuration, Sending a Text Message, Updating a Bill of Lading and Entering Fuel Fill Details. None of these functions impact the security of the TOE in anyway since they are optional services provided for the driver and any such information sent by the OBU may be overridden within the Depot at a later time. While using these functions it is not possible to obtain any sensitive data or manipulate OBU Time, Distance or Location reporting.

7.1.3. SF.ACCESS

The TOE allows authorized end users to access only appropriate TOE functions and data.

The EROAD Web Portal and EROAD Depot Application control all end user access, including:

- Enforcing access control policies.
- Ensuring secure internet connections.
- Receiving input data from all web users and passing EROAD Depot relevant input on to the EROAD Depot.
- Displaying all information that web users request.

Only authenticated and authorised users may access the EROAD Depot Application via the Depot Web Portal interface (entry point). Access to web pages, page objects and data is controlled by an authoritative security framework (controllers) that constrain access based on user ID (authentication). User ID is associated with an organization ID and role. Together, they limit access to TOE information such as pages, page objects, and data (authorization). Permitted scope is determined upon logging into the TOE.

7.1.4. SF.CRYPTOGRAPHY

The EROAD OBU provides cryptographic functions that maintain the confidentiality of the events and messages (data) transmitted between the EROAD OBU and EROAD OBU Gateway. Data from each EROAD OBU is secured by means of TLS transport. The OBU device, as part of the TOE, uses FIPS 140-2 Level 3 compliant crypto modules for cryptographic services that implement approved security functions and services used by cryptographic functions local to the OBU.

7.1.5. SF.AUDIT

The TOE records all security critical errors and messages. The timestamped generated messages from EROAD OBU are used for statistics, diagnostics, critical errors and debug. These are stored at EROAD servers in monthly partitioned tables.

Timestamped user actions are tracked by the EROAD Depot Application logs based on user ID and IP address. Environmental platforms (server logging) also identify transactions by IP address. This provides linkage back to the user via the Depot Application logs. In the case of the OBU's, its identity is its serial number. If a Depot user IP address is a public IP address supporting multiple EROAD Depot user accounts, EROAD can identify server events local to that IP address and correlate them to users who were active at the time.

All local EROAD OBU event data is transmitted to the EROAD Depot Application

Each event bears a local date/time stamp generated by the EROAD OBU and identifies the associated OBU user ID and IP address.

EROAD Depot Application logs include:

Actions: Create, Delete, Update, Exclude Logins, Login and Support.

Each logged item bears a local date/time stamp generated by the EROAD Depot Application and includes the associated user ID and IP address.

7.1.6. SF.PROTECT

The TOE protects itself from unauthorized modifications and access to its functions and data. The EROAD Depot Application is protected from "the wild" by the EROAD Depot Web Portal. The application is also protected from exposed OBU physical endpoints by the OBU Gateway. All communication requests are authenticated and authorised by the TOE (EROAD Depot Application) prior to allowing any further action within an encrypted communications channel provided by the environment.

The way this works is:

1) The EROAD Web Portal and EROAD OBU Gateway present all web users and OBU with a secure login page. This login page requires users to identify themselves by entering their username and password. To enter the EROAD Depot authentic user credentials must be entered.
2) All connections to the EROAD Web Portal are made via secure connections where users are authenticated using Basic Authentication
3) All OBU connections to environmental infrastructure of the EROAD OBU Gateway are HTTPS connections and OBUs are authenticated using Basic Authentication.

Identification, authentication, and authorization are part of the TOE. EROAD OBU hardware protection measures also exist which are described elsewhere in this document.

The TOE is monitored continuously for suspicious activity. Application logs are available for inspection in real time.

Data is protected from modification by using a TLS tunnel. This is performed using mechanisms within the OBU as one end-point of this connection and mechanisms within the load balancer as the other end of the connection.

7.1.7. SF. INTEGRITY

The TOE ensures the integrity of all audit and system data. The TOE is fully redundant (fault tolerant) with at least two of every key TOE component being run in parallel to provide failover capability at every level. Further, the TOE logs all changes made to data in order to show any/all modifications, substitutions, or deletions of data within or between components. Included in these logs are user ID, IP address, and timestamp information which uniquely identifies the origin of the transaction. All such actions are subject to role based access control (permissions). Since all TOE transactions occur via secure web services, and all requests and responses related to such services are authenticated and authorized, it is not possible to make unauthorized changes to TOE system data. Any and all access violations are logged at multiple levels. In the event of an error, access is denied and the offending entity is immediately logged out.

All components of the TOE are implemented in a redundant fashion. EROAD Depot Application and EROAD OBU log items include information related to user ID, originating IP address, and time/date stamps. A variety of data is captured including access violations and tamper events. Authentication and authorization prohibit unauthorized access to pages, page objects, and data. All access violations are logged and can be traced back to individual user, location and date/time. Therefore, it is possible to both verify and validate correct transactions and to detect and identify invalid events (errors).

7.1.8. SF.ADMINISTRATION

The EROAD Depot Application employs a hierarchical role based authorization scheme. As part of this scheme the following hierarchical end user roles exist: Client Administrator, Unit Manager, RUC User, Reporting User, Service User, Basic User, and Super Basic User. The default roles that are assigned to newly created user accounts may be viewed by the TOE System Administrator and Client Administrator when logged into the EROAD Depot Application. The TOE includes a set of functions that allows the creation, deletion and modification of customer end user roles. All TOE specific management functions reside in the EROAD Depot Application and are accessible via the Depot Web Portal. Only the TOE System Administrator may access these functions after being successfully authenticated by the TOE.

Depot end user credentials, including user name and password, may be changed by the TOE System Administrator and Client Administrator. The TOE System Administrator and Client Administrator can modify user credentials via the Depot Web Portal by logging into the Depot and selecting the User Administration area. Only the TOE System Administrator and Client Administrator have access to this area of the Depot.

The TOE is administered by the TOE System Administrator. When logged into the EROAD Depot Application via the Web Portal, the TOE System administrator is able to access the Ebox Admin section where the management of software installation, updates and configuration/set-up of the system and its components may be performed. The management of user accounts and security attributes is managed from the User Administration section.

7.2. SECURITY FUNCTIONS RATIONALE

The table below shows the mapping between the SFRs and the implementing security functions, and a description is given in the following subsections.

Requirements / Functions	FAU_GEN.1	FAU_GEN.2	FCS_CKM.1	FCS_CKM.4	FCS_COP.1	FDP_ACC.1(a)	FDP_ACC.1(b)	FDP_ACF.1(a)	FDP_ACF.1(b)	FDP_IFC.1	FDP_IFF.1	FIA_ATD.1	FIA_UAU.1	FIA_UID.1	FMT_MOF.1	FMT_MSA.1	FMT_MSA.3	FMT_SMF.1	FMT_SMR.1	FPT_ITT_EXP.1	FPT_PHP.2	FPT_STM.1
SF.TAMPER																					X	
SF.AUTHENTICATION												X	X	X								
SF.ACCESS						X	X	X	X	X	X		X	X		X	X					
SF.CRYPTOGRAPHY			X	X	X																	
SF.AUDIT	X	X																				X
SF.PROTECT					X								X							X		
SF.INTEGRITY	X	X																				X
SF.ADMINISTRATION															X			X	X			

Table 7: Mapping SFRs to security functions

7.2.1. SF.TAMPER

The TOE security function SF.TAMPER, "The EROAD OBU is protected by devices and elements that notify administrative functions in the event of physical attack", meets the requirements of "Protection of the TSF" with the requirement **FPT_PHP.2**.

See section 1.3.1, specifically Tamper Detection, for information related to the EROAD OBU.

7.2.2. SF.AUTHENTICATION

The TOE security function SF.AUTHENTICATION, "The different end user roles identify themselves to the TOE (Depot Application) and are authenticated and authorized by it via the EROAD Web Portal prior to getting access to their functions and data.", meets the requirements of "Identification and authentication" with the requirements **FIA_ATD.1**, **FIA_UAU.1** and **FIA_UID.1**.

7.2.3. SF.ACCESS

The TOE security function SF.ACCESS, "The TOE allows authorized end users to access only appropriate TOE functions and data. The TOE allows only authorized EROAD OBU units to access the system.", meets the requirements of "User data protection" with the requirements **FDP_ACC.1(a)**, **FDP_ACC.1(b)**, **FDP_ACF.1(a)**, **FDP_ACF.1(b)**, **FDP_IFC.1** and **FDP_IFF.1**, and the requirements of "Identification and authentication" with the requirements **FIA_UAU.1** and **FIA_UID.1**, and the requirements of "Security management" with the requirements **FMT_MSA.1** and **FMT_MSA.3**.

7.2.4. SF.CRYPTOGRAPHY

The TOE security function SF.CRYPTOGRAPHY, "The TOE provides cryptographic functions to maintain the confidentiality of the data that is transmitted between EROAD OBU and OBU Gateway", meets the requirements of "Cryptographic support" with the requirements **FCS_CKM.1**, **FCS_CKM.4** and **FCS_COP.1**.

7.2.5. SF.AUDIT

The TOE security function SF.AUDIT, "Recording of all security critical errors and messages", meets the requirements of "Security audit" with the requirements **FAU_GEN.1 and FAU_GEN.2,** and the requirements of "Protection of the TSF" with the requirement **FPT_STM.1**.

7.2.6. SF.PROTECT

The TOE security function SF.PROTECT, "Protection from unauthorized modifications and access to its functions and data", meets the requirements of "Cryptographic support" with the requirement **FCS_COP.1**, and the requirements of "Identification and authentication" with the requirement **FIA_UAU.1**, and the requirements of "Protection of the TSF" with the requirement **FPT_ITT_EXP.1**.

7.2.7. SF.INTEGRITY

The TOE security function SF.INTEGRITY, "Integrity of all audit and system data", meets the requirements of "Security audit" with the requirements **FAU_GEN.1 and**

FAU_GEN.2, and the requirements of "Protection of the TSF" with the requirement **FPT_STM.1**.

7.2.8. SF.ADMINISTRATION

The TOE security function SF.ADMINISTRATION, "Functions that allow effective management of its functions and data", meets the requirements of "Security management" with the requirements **FMT_MOF.1**, **FMT_SMF.1** and **FMT_SMR.1**.