



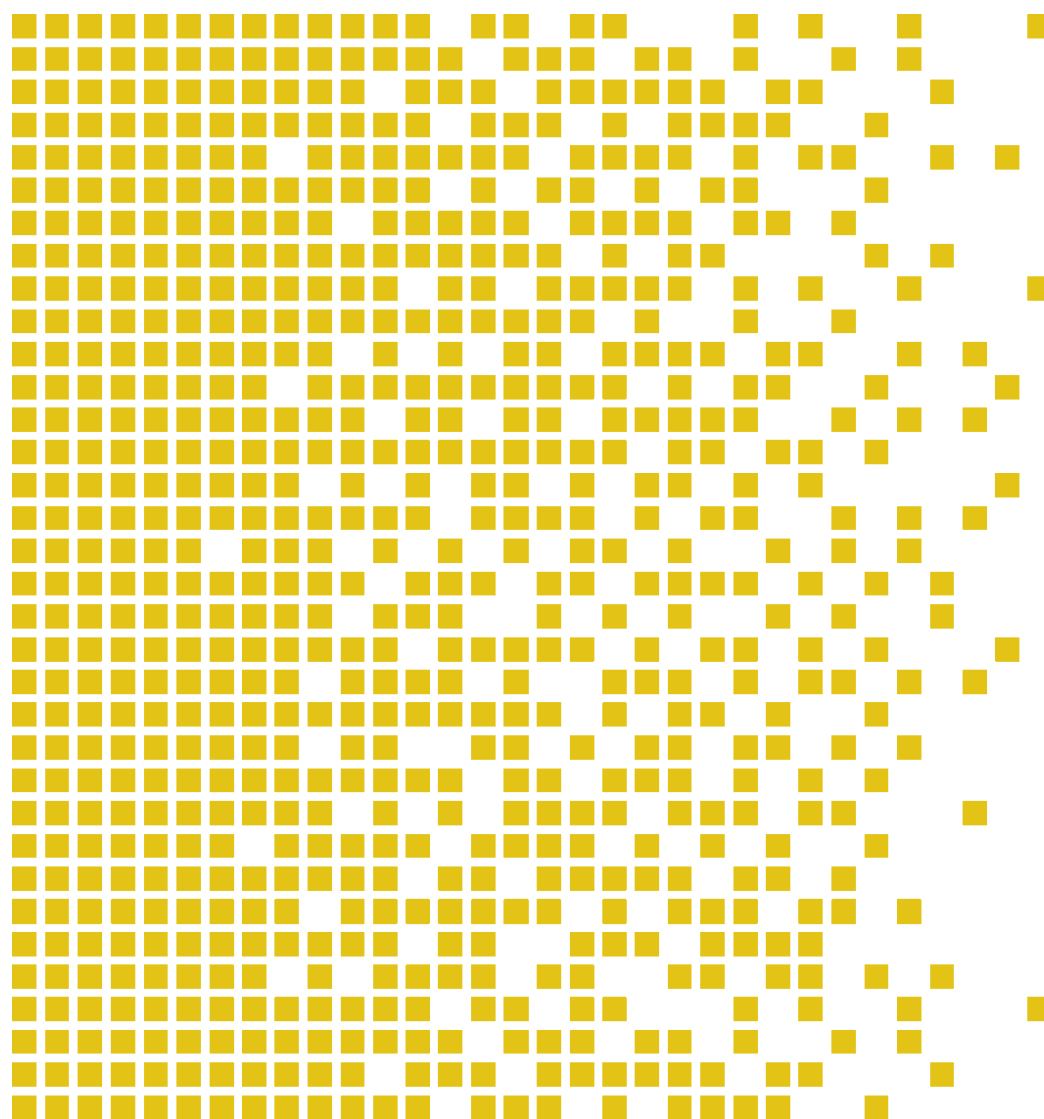
**SERTIT**

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

# SERTIT-059 CR Certification Report

Issue 1.0 25 June 2015

## EROAD Solution



CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009E VERSION 2.2 16.12.2013

**ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN  
THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of the CCRA May 23rd 2000. The recognition under CCRA is limited EAL 4 and ALC\_FLR CC part 3 components.



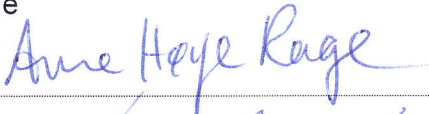
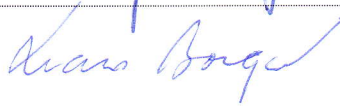



## Contents

Certification Statement	4
1 Abbreviations	5
2 References	6
3 Executive Summary	7
3.1 Introduction	7
3.2 Evaluated Product	7
3.3 TOE scope	7
3.4 Protection Profile Conformance	7
3.5 Assurance Level	7
3.6 Security Policys	8
3.7 Security Claims	8
3.8 Threats Countered by the TOE	8
3.9 Threats Countered by the TOE's environment	8
3.10 Threats and Attacks not Countered	9
3.11 Environmental Assumptions and Dependencies	9
3.12 Security Objectives for the TOE	9
3.13 Security Objectives for the operational environment	10
3.14 Security Functional Components	10
3.15 Evaluation Conduct	10
3.16 General Points	11
4 Evaluation Findings	11
4.1 Introduction	11
4.2 Delivery	12
4.3 Installation and Guidance Documentation	12
4.4 Misuse	12
4.5 Vulnerability Analysis	12
4.6 Developer's Tests	12
4.7 Evaluators' Tests	13
5 Evaluation Outcome	13
5.1 Certification Result	13
5.2 Recommendations	13
Annex A: Evaluated Configuration	14
TOE Identification	14
TOE Documentation	15
TOE Configuration	15

## Certification Statement

EROAD Solution (Version stated in 3.2) has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and has met the Common Criteria Part 3 (ISO/IEC 15408) conformant components of Evaluation Assurance Level EAL 2 augmented with ALC\_FLR.1 for the specified Common Criteria Part 2 (ISO/IEC 15408) extended functionality (see Security Target chapter 5) in the specified environment when running on the platforms specified in Annex A

Author	Rage, Arne Høye Certifier 
Quality Assurance	Lars Borgos Quality Assurance 
Approved	Øystein Hole Head of SERTIT 
Date approved	25 June 2015



## 1 Abbreviations

CC	Common Criteria for Information Technology Security Evaluation(ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
ISO/IEC 15408	Information technology -- Security techniques -- Evaluation criteria for IT security
POC	Point of Contact
PP	Protection Profile
QP	Qualified Participant
SERTIT	Norwegian Certification Authority for IT Security
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
OBU	On Board Unit



## 2 References

- [1] EROAD Solution Security Target Version 1.3. 15.06.2015.
- [2] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2012-09-001, Version 3.1 R4, September 2012.
- [3] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, CCMB-2012-09-002, Version 3.1 R4, September 2012.
- [4] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, CCMB-2012-09-003, Version 3.1 R4, September 2012.
- [5] The Norwegian Certification Scheme, SD001E, Version 9.0, 02 April 2013.
- [6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1 R4, September 2012.
- [7] ETR for the evaluation project SERTIT-059, Common Criteria EAL2 Augmented with ALC\_FLR.1 Evaluation of EROAD Solution. v1.1, 17.06.2015.
- [8] EROAD Ehubo Installation Guide, 11/2014
- [9] EROAD Guidance Document, Version 1.0
- [10] EROAD Guidance Documentation Supplement, 12/2014



## 3 Executive Summary

### 3.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of EROAD Solution to the developer, EROAD, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation components.

### 3.2 Evaluated Product

TOE versions of EROAD OBU:

Hardware version: 03

Firmware version: 1.18.05

TOE versions of EROAD Application:

Software version: 11-11-2014-0239

This product is also described in this report as the Target of Evaluation (TOE). The developer was EROAD Limited.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

### 3.3 TOE scope

The Scope is described in the ST [1], chapter 1.3.

### 3.4 Protection Profile Conformance

The Security Target [1] did not claim conformance to any protection profile.

### 3.5 Assurance Level

The Security Target [1] specified the assurance components for the evaluation. Predefined evaluation assurance level EAL 2 augmented with ALC\_FLR.1 was used. Common Criteria Part 3 [4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [2].



### 3.6 Security Policies

The TOE security policies are specified in the ST [1] in chapter 3.

### 3.7 Security Claims

The Security Target [1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional components and security functions to elaborate the objectives. The SFR's are taken from CC Part 2 [3]; use of this standard facilitates comparison with other evaluated products. There is however one extended functional component. The rationale for this component can be found in the Security Target [1] chapter 5.

### 3.8 Threats Countered by the TOE

- **TT.TAMPERING** The TOE may be subject to physical attack that may compromise information and data processing.
- **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.
- **TT.SPOOFING** Eavesdropping of the communication between EROAD OBU and EROAD OBU GATEWAY, changing the cellular data and transmitting the changed cellular data.
- **TT.BYPASSING** Bypassing of a security mechanism may compromise information and data processing in EROAD Application.
- **TT.WRONG\_SW\_FW** Wrong software (EROAD Application) or firmware (EROAD OBU) versions are installed in the TOE, making the TOE inoperable.
- **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.

### 3.9 Threats Countered by the TOE's environment

- **TE.SYS\_ADMIN\_FAIL** The system administrator fails to perform functions essential to the security
- **TE.EXPLOIT\_VULN** A person/company tries to exploit vulnerability in the TOE to get unauthorized access to EROAD Application information.
- **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.



### 3.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

### 3.11 Environmental Assumptions and Dependencies

- **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.

### 3.12 Security Objectives for the TOE

- **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.

### 3.13 Security Objectives for the operational environment

- **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.

### 3.14 Security Functional Components

- 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

### 3.15 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E [5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information

Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [1], which prospective consumers are advised to read. To ensure that the Security Target [1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3 [4] and the Common Evaluation Methodology (CEM) [6].

SERTIT monitored the evaluation which was carried out by the Advanced Data Security Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the Evaluation Technical Report (ETR) [7] to SERTIT in 17 June 2015. SERTIT then produced this Certification Report.

### 3.16 General Points

The evaluation addressed the security functionality claimed in the Security Target [1] with reference to the assumed operating environment specified by the Security Target [1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

## 4 Evaluation Findings

### 4.1 Introduction

The evaluation addressed the requirements specified in the Security Target [1]. The results of this work were reported in the ETR [7] under the CC Part 3 [4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.



## 4.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.

OBU devices are shipped to customers using only approved carriers. On receipt of the OBU the customer shall check that the screw covers are in place on the OBU and have not been tampered with or removed. The customer will then power up the OBU and check the version number displayed on the bottom right of the OBU screen.

At this point, the customer shall confirm that power is correctly applied to the OBU and that the screen illuminates when touched. This confirms that the OBU is in the Operating Mode. If the FIPS power-up self-tests fail then the OBU will not boot and the screen will not be illuminated when touched.

## 4.3 Installation and Guidance Documentation

Installation procedures and user guidance is described in detail in the supporting documents [8], [9] and [10].

## 4.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. Developers should follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

## 4.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process. The evaluators have searched for potential vulnerabilities and penetration tests have been devised and performed. The evaluators have not found any exploitable vulnerabilities or residual vulnerabilities in the TOE.

## 4.6 Developer's Tests

The evaluators have examined the developers test plan and determined that it describes the scenarios for performing each test, including any ordering dependencies on results of other tests. The test plan provides information about the test configuration being used: both on the configuration of the TOE

and on any test equipment being used, as well as information about how to execute the tests.

#### 4.7 Evaluators' Tests

The evaluators have employed a combination of a random sampling method and a method based on the intent to cover the TSFI, Security Functions, and subsystems to the maximum extent possible both for the sampling of the developer's tests and for the independent testing.

### 5 Evaluation Outcome

#### 5.1 Certification Result

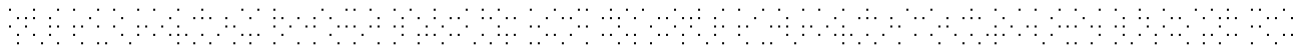
After due consideration of the ETR [7], produced by the evaluators, and the conduct of the evaluation, as witnessed by the certifier, SERTIT has determined that EROAD Solution meets the Common Criteria Part 3 conformant components of Evaluation Assurance Level EAL 2 augmented with ALC\_FLR.1 for the specified Common Criteria Part 2 extended functionality, in the specified environment, when running on platforms specified in Annex A.

#### 5.2 Recommendations

Prospective consumers of EROAD Solution should understand the specific scope of the certification by reading this report in conjunction with the Security Target [1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 3.3 "TOE Scope" and Section 4 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.



## Annex A: Evaluated Configuration

### TOE Identification

TOE versions of EROAD OBU:

Hardware version: 03

Firmware version: 1.18.05

TOE versions of EROAD Application:

Software version: 11-11-2014-0239

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 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.

### TOE Documentation

The supporting guidance documents evaluated in addition to the Security Target [1] were:

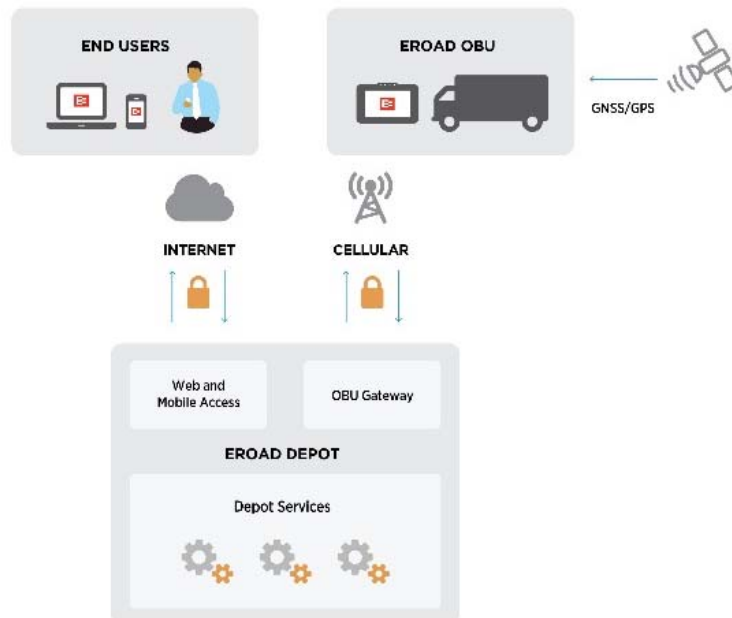
- [a] EROAD Ehubo Installation Guide, 11/2014
- [b] EROAD Guidance Document, Version 1.0
- [c] EROAD Guidance Documentation Supplement, 12/2014

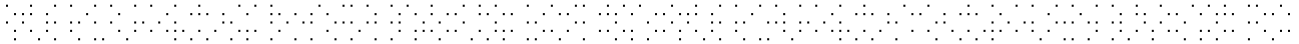
Further discussion of the supporting guidance material is given in Section 4.3 “Installation and Guidance Documentation”.

### TOE Configuration

The following configuration was used for testing:

System overview:





System architecture:

