# EUCC Certification Report

| CERTIFICATION REPORT INFORMATION | |
|---|---|
| **Certification Report Reference** | FCS506_02 EN EUCC Distromel_WCIS Certification Report v1.0 |
| **Project (TOE) Identification** | Distromel Waste Container Identification System version 1.0.0 |
| **Evaluation Technical Report (ETR) Reference** | Distromel_WCIS-ETR, version 1.1<br>Distromel waste container identification system Evaluation Technical Report |
| **CB identification** | DEKRA Testing and Certification S.A.U. EUCC CB<br>Body Number at ENISA: CB 3095 |
| **Author** | Narcís Pallarés Mulet & Alejandro Muñoz del Rey |
| **Date** | 28/04/2026 |
| **EUCC APPLICANT INFORMATION** | |
| **Applicant identification** | DISTROMEL S.A. |
| **ITSEF INFORMATION** | |
| **ITSEF Identification** | DEKRA Testing and Certification S.A.U<br>Calle Severo Ochoa, 55 (planta 2)<br>Parque Tecnológico de Andalucía<br>29590 Campanillas (Málaga)<br>Body Number at ENISA: ITSEF 3095 |

# CONTENT

# 1. Executive Summary

The TOE is a distributed component of a Waste Bin Identification System (WBIS), comprising an RFID tag attached to each waste container and a software library that implements mechanisms to ensure the integrity of waste collection records. The overall system enables the identification of waste bins through RFID technology in order to determine how often each container is emptied, supporting billing processes based on the number of emptying events and, optionally, on the weight or volume of waste collected.

Within this context, the TOE focuses on providing data integrity assurance functions. It enables the generation and validation of identification data, the creation of emptying records including unique identifiers and timestamps, and the protection of these records through mechanisms such as CRC checks and cryptographic hashing. These security features ensure that collection data remains accurate and verifiable throughout its lifecycle, allowing it to be reliably used for further processing and billing purposes.

This document is the Certification report of the certification of the **Distromel Waste Container Identification System, version 1.0.0** developed on the basis of the Evaluation Technical Report [ETR].

This report is published together with the corresponding TOE EUCC certificate.

A detailed description of the security functionality is included in section **6. SECURITY REQUIREMENTS** of the [ST].

The following provides a summary of the threats addressed by the evaluated ICT product as documented in the [ST][1].

- **Threats:**

  The considered threat agent (S.Attack) is an external actor, either a person or a process acting on their behalf, with limited knowledge, focused on exploiting obvious vulnerabilities through the TOE interfaces, with the objective of compromising security and modifying or corrupting sensitive application data.

  The main identified threats are:

  - Manipulation of identification data (T.Man): random corruption of identification data within the ID-Tag through physical means.
  - Disturbance of data transmission (T.Jam#1): interference with the transfer of identification data from the ID-Tag to the vehicle software, leading to random corruption.
  - Corruption of clearance records (T.Jam#2): alteration of clearance records by the attacker.

[1] The [ST] does not include organisational security policies (OSPs)

The patch management is out of the scope of the evaluation.

The evaluation was conducted by the ITSEF **DEKRA Testing and Certification S.A.U.** and was finished on **January 30th, 2026** with **PASS** verdict.

The evaluation was conducted in accordance with the Common Criteria (CC) standard, version 2022, Revision 1 [CC2022].

The evaluation activities performed during the evaluation correspond to an assurance level of **EAL1**, as specified in [CC2022p3] and [CEM2022].

The certification results apply only to the product version specified in the certificate, subject to the conditions set out in this Certification Report.

Considering that all evaluation activities have been conducted in accordance with the Common Criteria requirements and have resulted in a pass outcome, the Technical Reviewers' Team issues the following recommendation regarding the certification decision:

| **Recommendation on Certification Decision** | | |
|---|---|---|
| **Recommendation of the Technical reviewer's team** | **POSITIVE** | Certificate validity period:<br>5 years |

## 2. Bibliography


[CC2022p1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 2022, Revision 1

[CC2022p2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 2022, Revision 1

[CC2022p3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 2022, Revision 1

[CC2022p4] Common Criteria for Information Technology Security Evaluation. Part 4: Framework for the specification of evaluation methods and activities. Version 2022, Revision 1

[CC2022p5] Common Criteria for Information Technology Security Evaluation. Part 5: Pre-defined packages of security requirements. Version 2022, Revision 1

[CEM2022] Common Methodology for Information Technology Security Evaluation. Version 2022, Revision 1

[CSA] REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[EUCC] COMMISSION IMPLEMENTING REGULATION (EU) 2024/482 of 31 January 2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria-based cybersecurity certification scheme (EUCC)

[SotA] EUCC SCHEME DRAFT STATE-OF-THE-ART DOCUMENT. ACCREDITATION OF ITSEFs FOR THE EUCC SCHEME. Version 1.6c, July 2025

[ST] Security Target - "DISTROMEL WASTE CONTAINER IDENTIFICATION SYSTEM" VERSION 1.8, 27/02/2026

[VUL] DISTROMEL WASTE CONTAINER IDENTIFICATION SYSTEM

| | |
|---|---|
| | Life-Cycle Support. Vulnerability Management and Disclosure (EUCC). Version 1.0<br>Date: 22nd January 2026 |
| [ETR] | Distromel_WCIS-ETR, version 1.1<br>Distromel waste container identification system Evaluation Technical Report |

# 3. Evaluated ICT product

| 3.1. Evaluated ICT product | |
|---|---|
| **Name of the evaluated ICT product** | Distromel Waste Container Identification System Version 1.0.0 |
| **Enumeration of the ICT product's components that are part of the evaluation** | ID-TAG<br>siCORE Security Library |
| **Version number of the ICT product's components** | ID tags (passive transponders that contain a unique ID)<br>siCORE Security Library 1.0.0 |
| **ST reference** | Security Target<br>"DISTROMEL WASTE CONTAINER IDENTIFICATION SYSTEM"<br>VERSION 1.8, 27/02/2026 |
| **CC / CEM Version and Assurance Level** | [CC2022] / [CEM2022]<br>EAL1 (AVA_VAN.1) |
| **Identification of additional requirements to the operating environment of the certified ICT product** | A single configuration is included in the scope of the evaluation. |
| **Name and contact information of the holder of the EUCC certificate** | DISTROMEL, S.A.<br>Address:<br>Carretera A-133 Km. 4,8<br>22512 San Esteban de Litera (Huesca)<br>SPAIN<br>Email: soporte.EUCC@distromel.com |
| **Patch management procedure included into the certificate** | N/A |
| **Vulnerability handling and Disclosure procedures / assurance continuity** | DISTROMEL WASTE CONTAINER IDENTIFICATION SYSTEM |

| | |
|---|---|
| | Life-Cycle Support. Vulnerability Management and Disclosure (EUCC). Version 1.0 Date: 22nd January 2026 |
| **Link to the website of the holder of the EUCC certificate where supplementary cybersecurity information for the certified ICT product in accordance with Article 55 of Regulation (EU) 2019/881 is provided** | https://www.distromel.com/soporte/ and https://www.distromel.com/en/support/ |

| **3.2. TOE Deliverables** | |
|---|---|
| **Component** | **Description** |
| ID-Tag | Hardware<br><br>ID tags are passive transponders that contain a unique ID as well as a check value (CRC).<br><br>The ID tags are attached to waste containers.<br><br>The information stored on the ID tags can be read by a reading device and is used for the identification of the waste container. The tags do not have an explicit version. However, they contain an identifier which is unique (generated at factory) but it cannot be known beforehand delivery.<br><br>The Tags are delivered physically to the clients. |
| SecurityLib v.1.0.0 (siCORE Security Library 1.0.0) | Software<br><br>It is the TOE component of the vehicle software. It is delivered embedded in an Android application (APK format), which is distributed pre-installed in the vehicle computer (tablet). |
| Guidance | Guidance - Distromel waste container identification system v1.0 - version 1.1.pdf<br><br>The operating instructions describe how siCORE is to be operated for secure use. The documentation is provided as a PDF file on an electronic data carrier or by email.<br><br>SHA-256:<br>40ae3a8e95ea60ef94169a4f61bc109ecbef821c4e3766be31191d79eea0598e |

# 4. Security Services

The TOE is composed of the following parts:

- ID-Tag: RFID tag containing the identification data of the waste bin. This is a passive element that allows the emission of stored data in the chip due to the application of an electromagnetic field generated by an external antenna. The data stored in the RFID tag contains a unique identifier (generated at manufacturing time), in accordance with the ISO 11785:1996 format.

  The identification data (AT1) of the waste container is stored in the ID-Tag (Read Only). The identification data together with a CRC check value is sent to the security library as an integrity feature that can be validated.

- SiCore Security Library: checks the integrity of the identification data by forming the CRC over the received identification data of the ID-Tag and comparing it with the also received CRC check value (AT1). If the integrity validation fails, the waste collection register is generated with an error flag. If the integrity check is correct, siCORE Security Library provides the emptying data record (AT) with protection (integrity feature) that acts against alteration of the AT by random manipulation. At the request of the host application, it can validate emptying data records using the integrity mechanisms available before transmission to the office software.

The following Figure shows an overview of the TOE inside the waste bin identification system.

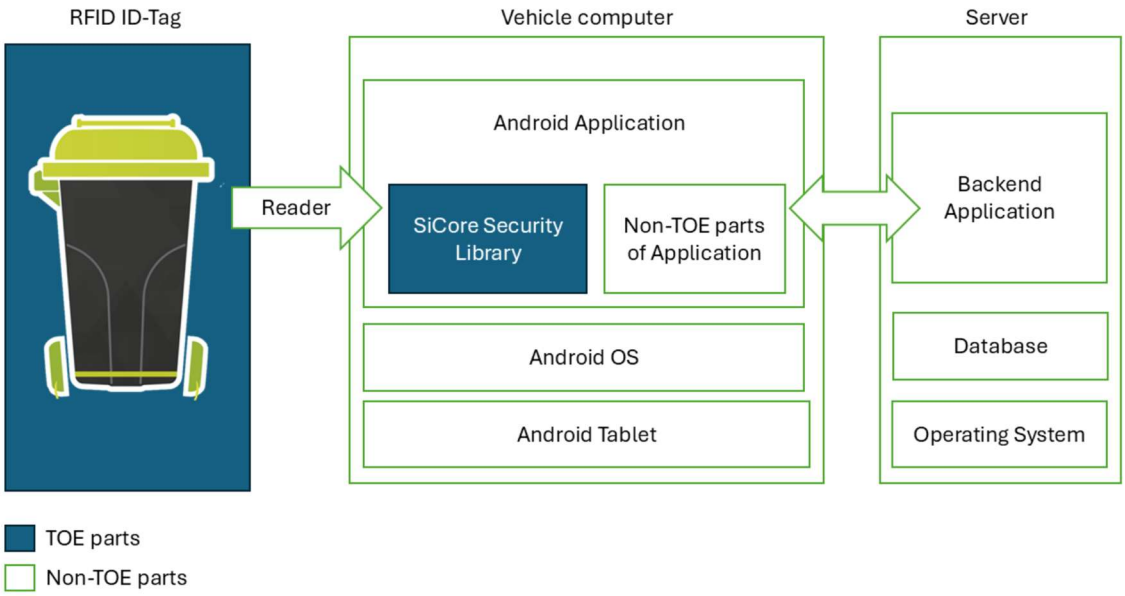



Figure 1: TOE parts inside the Waste Bin Identification System

The TOE aims to provide a secure mechanism to uniquely determine the number of times each waste container is emptied, thereby enabling billing based on emptying events. The product may optionally incorporate a weighing or volume measurement system to support weight- or volume-based billing.

To achieve this, the TOE implements security mechanisms that ensure the integrity and authenticity of identification data and generated records throughout system operation.

The validity of data received from the RFID Tag is ensured through the verification of a checksum (CRC), allowing the detection of potential data corruption during reading and the indication of anomalies when they occur.

Each collection record, including the identifier, timestamp, and other relevant data, is protected through the generation of a cryptographic hash (SHA-256), enabling subsequent verification of data integrity and detection of any unauthorized modifications.

During data transmission between the RFID Tag and the vehicle software, the TOE ensures the integrity of the transferred information through built-in verification mechanisms, preventing alteration during communication.

Finally, the TOE implements integrity monitoring of stored data, allowing the detection of any manipulation affecting both identification data and stored records.

The vulnerability handling policy of the manufacturer is described in [VUL].

The assurance continuity policy will follow [EUCC] regulation.

The patch management is out of the scope of the evaluation.

# 5. Assumptions and Clarification of Scope

The assumptions defined in the Security Target [ST], as well as certain aspects of the identified threats and organisational security policies, are not addressed by the TOE itself. These aspects result in specific security objectives and measures that must be implemented by the operational environment.

The TOE is considered to provide effective security measures in a cooperative, non-hostile environment, provided that it is correctly installed, managed, and used.

The following specific conditions are assumed to exist in the environment in which the TOE operates:

| Asssumption | Description |
|---|---|
| **A.Id**<br>ID-Tag | The ID-Tag is fastened to the waste bin. The identification data (AT1) of the waste bin are saved in the ID-Tag. There are only ID-Tags with unique identification data in use.<br>The correct correspondence of this data to the chargeable person is to be provided by organisational means which are out of the scope of the TOE. |
| **A.Trusted**<br>Trustworthy personnel | The crew of the collection vehicle (S.Trusted) are authorised and trustworthy. All persons who install and maintain the system are authorised and trustworthy (S.Trusted). All persons responsible for the security of the TOE environment (S.Trusted) are authorised and trustworthy. |
| **A.Access**<br>Access protection | The environment ensures by appropriate means (closure, access control by passwords etc.) that only user or service staff (S.Trusted) can directly access the components of the TOE except the ID-Tag. |

# 6. Architectural Information

The TOE is a distributed TOE forming part of a Waste Container Identification System, comprising an RFID tag (hardware ID-Tag) and a software library (siCORE Security Library) that provides mechanisms to monitor the integrity of waste collection records during collection operations.

The ID-Tag and the siCORE Security Library are described in Chapter 1.4 (“TOE Description”) of the Security Target [ST].

# 7. Supplementary Cybersecurity Information

The manufacturer of the certified ICT product makes the following supplementary cybersecurity information publicly available on the website indicated in Section 2.1 Evaluated ICT Product.

a) guidance and recommendations to assist end users with the secure configuration, installation, deployment, operation and maintenance of the ICT products or ICT services;

   The documentation evaluated, as outlined in Section 2.2 TOE Deliverables, is provided to the customer together with the product. This documentation includes the information required for the secure configuration, installation, deployment, operation, and maintenance of the TOE in accordance with the Security Target.

b) the period during which security support will be offered to end users, in particular as regards the availability of cybersecurity-related updates;

c) contact information of the manufacturer or provider and accepted methods for receiving vulnerability information from end users and security researchers;

d) a reference to online repositories listing publicly disclosed vulnerabilities related to the ICT product, ICT service or ICT process and to any relevant cybersecurity advisories.

# 8. ICT Product Testing

The certificate is issued by **DEKRA Testing and Certification S.A.U. EUCC CB (3095)**, under the authority of the Spanish NCCA CCN.

The evaluation was performed by **the ITSEF DEKRA Testing and Certification S.A.U.**

The evaluation activities performed for an assurance level of **EAL1**, as specified in [CC2022p3] and [CEM2022], are summarized in the following table:

| Assurance Class | Assurance Components |
|---|---|
| **ADV: Development** | ADV_FSP.1 Functional specification |
| **AGD: Guidance documents** | AGD_OPE.1 Operational user guidance<br>AGD_PRE.1 Preparative procedures |
| **ALC: Life-cycle support** | ALC_CMC.1 CM capabilities<br>ALC_CMS.1 CM scope |
| **ASE: Security Target evaluation** | ASE_CCL.1 Conformance claims<br>ASE_ECD.1 Extended components definition<br>ASE_INT.1 ST introduction<br>ASE_OBJ.1 Security objectives<br>ASE_REQ.1 Security requirements<br>ASE_TSS.1 TOE summary specification |
| **ATE: Tests** | ATE_IND.1 Independent testing |
| **AVA: Vulnerability assessment** | AVA_VAN.1 Vulnerability Analysis |

No state-of-the-art documents or additional security evaluation criteria were applied in this evaluation.

The [ST] does not claim conformance to any PP.

Independent testing was performed by the evaluator to verify that the TOE operates as specified, following an SFR-oriented approach. All security functional requirements were exercised through the relevant TSFIs and subsystems, using a representative set of test cases based on the Security Target, vendor documentation, and evaluation knowledge. The testing covered all TSFIs, including critical parameters and input variations, confirming that the TOE behaves as expected and that its security functions are correctly implemented.

In addition, a vulnerability analysis was conducted based on publicly available sources, the TOE documentation, and its evaluated configuration. An independent search for potential vulnerabilities did not identify any applicable vulnerabilities or plausible attack paths exploitable with a basic attack potential. As a result, the TOE is considered resistant to vulnerabilities within the defined scope.

# 9. Certificate Holder's Lifecycle Management Processes and Production Facilities

For the assurance level selected for the product certification (EAL1), no additional requirements are imposed beyond ensuring that the TOE has a unique reference. This reference shall ensure that there is no ambiguity regarding the specific instance of the TOE being evaluated. Labelling the TOE with this reference allows users to clearly identify the instance they are using.

The version identifier used by the manufacturer follows a three-number format (X.Y.Z), which enables subsequent product versions to be uniquely identified without ambiguity.

# 10. Evaluation Results

The ITSEF produced and provided the Evaluation Technical Report [ETR] and companion partial reports of each activity (ASE, ADV, ALC, AGD. ATE and AVA) according to the requirements of the [EUCC] and the Common Criteria [CC2022] and the Common Evaluation Methodology [CEM2022].

The evaluation of the ICT product, has confirmed that it meets the requirements for assurance level 'Substantial' as defined in Article 4 of the EUCC Implementing Regulation and Article 52 of Regulation (EU) 2019/881 [EUCC].

The AVA_VAN.1 component indicates that the product was evaluated to resist attacks from attackers with a BASIC attack potential.

Based on the review of the evaluator's analysis and conclusions for the ASE, ALC, AGD, ADV, ATE, and AVA activities, it can be confirmed that the evaluation was conducted in accordance with the Common Criteria [CC2022] requirements and the Common Evaluation Methodology [CEM2022].

## Evaluated Configuration

The evaluated configuration is limited to the ICT product deployed in the environment defined in the [ST]. This configuration is established by strictly following the guidance provided with the TOE and ensuring that all security objectives for the operational environment specified in the [ST] are fulfilled.

The configuration has been verified to align with the intended security posture and functional requirements, ensuring that it operates within the defined environment in a secure and compliant manner.

As detailed in the [ETR] the evaluator tested the TOE in the configuration described in the Security Target [ST].

## Summary of Evaluation Activities

The evaluation resulted in a PASS verdict for all assurance components listed in section 7 of the report and claimed in the Security Target [ST] for the TOE. A summary of the evaluation activities is provided below.

**ASE:**

The Security Target [ST] of the TOE has been developed as a Direct Rationale ST (as defined in [CC2022p1]. In this approach, no explicit security objectives for the TOE are defined. Instead, only the security objectives for the operational environment are specified and justified.

The security requirements are directly derived from and mapped to the elements of the Security Problem Definition (SPD), namely the identified threats and assumptions, as no organisational security policies (OSPs) are defined in the [ST]. This direct rationale establishes the link between the selected security functional requirements (SFRs), the environmental objectives, and the SPD elements.

Furthermore, the rationale ensures that no superfluous SFRs are included and provides justification for any SFR dependencies that are not satisfied, in accordance with the Common Criteria methodology.

The findings of the ASE activity are well-documented and internally consistent, demonstrating a thorough understanding of the [ST] and its components. The identified threats, security objectives for the environment, and security requirements are appropriately addressed, and the TOE description is both accurate and adequate for the evaluation level. Consequently, the ASE activities fulfil the assurance requirements for EAL1. A non-conformity related to the identification of the TOE was addressed and resolved by the manufacturer, with no impact on the assurance of the TOE.

**ALC:**

At EAL1, the life-cycle support requirements include ALC_CMC.1 (TOE configuration management capabilities) and ALC_CMS.1 (TOE configuration management scope), which ensure that the TOE is uniquely identified and that its configuration is defined in a consistent and unambiguous manner. The evaluation confirmed that the TOE identification is correct and unambiguous, and that the list of configuration items is complete, with each item clearly identified. The findings demonstrate that the ALC activities satisfy the assurance requirements for EAL1, with no issues or deviations identified that could compromise the security of the TOE.

**AGD:**

At EAL1, the AGD activities ensure that the TOE is accompanied by basic user and administrator guidance that is clear, complete, and sufficient for secure installation, configuration, and operation. The evaluation has demonstrated that the guidance documentation is clear, complete, and sufficient to support the secure installation, configuration, and operation of the TOE within its intended environment. The evaluation verifies that the documentation allows users to use the TOE securely as intended, without requiring detailed or advanced guidance validation. The guidance effectively helps preventing common misconfigurations and promotes correct usage. Therefore, the AGD activities fulfil the assurance requirements for EAL1, with no issues or deviations identified.

**ADV:**

At EAL1, the ADV (Development) activities are limited to the evaluation of the Functional Specification (ADV_FSP.1). The assessment ensures that the TSF is described in terms of its externally visible interfaces, including their purpose, usage, parameters, and behaviour, providing sufficient understanding of how the TOE security functionality is invoked and operates. During the evaluation, a minor nonconformity related to the completeness of the functional specification was identified. This issue was addressed and resolved by the developer through an update of the Functional Specification. Following this update, the requirements of ADV_FSP.1 were considered to be satisfactorily fulfilled.

**ATE:**

In line with ATE_IND.1 at EAL1, the evaluator performed independent testing to verify that the TOE operates as specified. The testing strategy was SFR-oriented, ensuring that all security functional requirements defined in the Security Target were exercised through the relevant TOE Security Function Interfaces (TSFIs) and subsystems.

The evaluator designed and executed a representative set of test cases based on the Security Target, vendor documentation, and knowledge gained during the evaluation. All TSFIs were covered, with particular attention given to critical parameters and input variations in order to identify potential incorrect behaviour. The results of the independent testing confirm that the evaluated version of the TOE implements the security functionalities as specified by the developer, behaves as expected and that its security functions are correctly implemented.

**AVA:**

Consistent with AVA_VAN.1 at EAL1, the evaluator performed a vulnerability analysis to identify publicly known vulnerabilities and assess whether any could be exploited with a BASIC attack potential. This analysis was based on a review of publicly available vulnerability sources, the TOE documentation, and its evaluated configuration.

The evaluator also conducted an independent search for potential vulnerabilities. No applicable vulnerabilities or plausible attack paths were identified that could be exploited with a BASIC attack potential. Therefore, the TOE is considered resistant to vulnerabilities within the scope of AVA_VAN.1 at EAL1.

## Usage of the TOE

The use of the certified ICT product is recommended, as no exploitable vulnerabilities have been identified within the defined operational environment. The following usage recommendations apply:

- The installation procedures provided in the documentation shall be strictly followed to ensure the correct download and proper installation of the evaluated version of the ICT product.

- The user guidance shall be carefully read and understood to ensure that the product is operated in accordance with the Security Target [ST].
- Compliance with the assumptions specified in Section 4 Assumptions and Clarification of Scope is essential, as these define the evaluated operational environment and imply that certain potential vulnerabilities are considered out of scope.

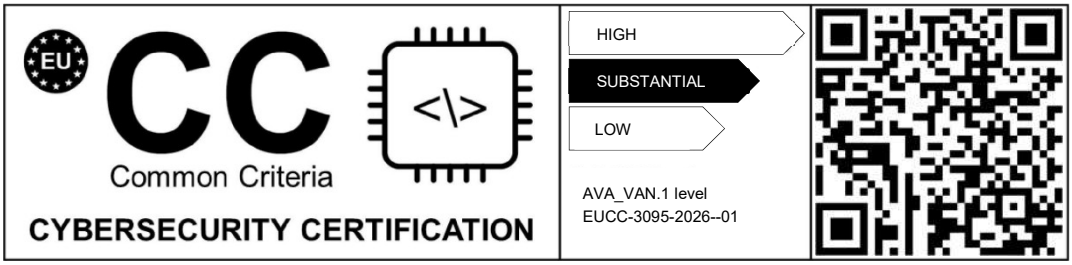
# 11. Information of the Certificate

| | |
|---|---|
| **Date of Issuance** | 28/04/2026 |
| **Period of Validity** | Valid for five years from the date of issuance<br>*The certificate is valid for five (5) years from the date of issuance, inclusive, and remains valid until the end of 27 April 2031, unless suspended or withdrawn earlier* |
| **Unique Identifier of the Certificate** | EUCC-3095-2026-01 |
| **Scheme Name** | (EU) 2024/482 - EUCC |
| **Certification Body Accreditation Reference Number** | DEKRA Testing and Certification S.A.U. EUCC CB<br>ENAC´s Accreditation number **134/C-PR337**<br>ENISA´s Body number: **3095** |

# 12. Summary of the Security Target of the ICT Product

For publication purposes, the Security Target of the TOE [ST] Security Target 'DISTROMEL WASTE CONTAINER IDENTIFICATION SYSTEM', Version 1.8 is provided as a separate document together with this Certification Report.

## 13. Mark and Label



Signature:

**Narcís Pallarés Mulet**

**EUCC CB Technical Reviewer**

DEKRA Testing and Certification S.A.U.

Signature:

**Alejandro Muñoz del Rey**

**EUCC CB Technical Manager**

DEKRA Testing and Certification S.A.U.