Security Target

“DISTROMEL WASTE CONTAINER IDENTIFICATION SYSTEM”

VERSION 1.8, 27/02/2026

DISTROMEL, S.A.

Table Of Contents

1. ST INTRODUCTION

This section specifies the Security Target (ST) and the Target of Evaluation (TOE) and provides a short description of the TOE and its security properties.

1.1 ST-Identification

TITLE:	Security Target Distromel waste container identification system
AUTHOR:	DISTROMEL, S.A.
ST VERSION:	1.8
DATE:	27/02/2026

1.2 TOE-Reference

NAME:	Distromel waste container identification system
VERSION:	1.0.0

1.3 TOE overview

The intent of this Security Target is to specify functional and assurance requirements for Distromel waste container identification system v1.0.0 which is the target of evaluation (TOE). The Security Target defines the security requirements of Distromel waste container identification system v1.0.0 for the acquisition and storage of records of clearance data.

Waste Bin Identification Systems (WBIS) in the sense of this document are systems, which allow to identify waste bins by an ID-tag (e.g. an electronic chip which is referred to as transponder) in order to determine how often a specific waste bin has been cleared. Note that these systems do not identify the waste directly but the waste bin, which contains the waste for disposal.

The purpose of the product is to count, how often the waste bins have been cleared in order to allow an originator-related billing of waste fees.

Frequently, such systems are combined with e.g. a weighing or volume measurement system in order to allow billing according to the frequency of clearance and the weight or volume of the waste disposed of.
After a collection vehicle has finished a clearance tour, the collected data are transmitted to the office of the maintenance and storage facility (either of the community or the private waste management enterprise) by means of possibly different media (data media, wire connection, wireless). In the office these data are stored in a central database. From there the data can be transmitted on a regular basis to authorities or regional computer centres for the billing process.

The description of the Waste Bin Identification System is provided so that the reader understands the role of the TOE (a subset of functionality) inside the system.

The TOE provides data integrity assurance functions within the siCORE system (the product, whose complete functionality was described in the paragraphs above) and includes the associated RFID tag hardware component (which is tied to each of the waste bins to be cleared) that stores the unique identification code and its CRC according to ISO 11784, and the software library implementing the integrity assurance mechanisms that are calculated at the moment of the waste collection of a bin for the generation of a verifiable proof of collection and the validation functions to be executed prior to data extraction from the vehicle.

1.3.1 TOE usage and major security features

The objective of the TOE is to provide a secure mechanism that makes it possible to uniquely determine the number of times each waste container is emptied, thereby enabling potential billing based on the number of times the container is emptied.

Identification data is generated when a waste collection vehicle empties a container. As a result of this operation, an emptying record is created that includes the container's identification data (unique identifier of the RFID tag according to ISO/IEC 11785:1996), a timestamp, and other optional fields related to the collection operation.

The TOE major security functionalities are:

1. CRC generation according to an input representing a RFID tag identifier.
2. CRC validation of the input representing a RFID tag identifier based, enabling the detection of errors in the identifier data.
3. Generation of emptying records: A data structure that contains the RFID tag identifier, a timestamp (and other optional data) for which a hash is calculated for future integrity validation.
4. Integrity validation of emptying records whenever it is requested by the host application (prior to the transfer of data to the office backend)

1.3.2 TOE type

This is a distributed TOE.

The TOE is part of a Waste Container Identification System, which includes the RFID tag (hardware) and a software library provides the mechanisms to monitor the integrity of the waste collection records during the waste collection tours.

1.3.3 Non-TOE Hardware/Software/Firmware required by the TOE

Component	Requirements
Reader	ISO 11784 reader Compatible to the vehicle computer using CAN BUS interface
Vehicle computer	Hardware requirements: - DISTROMEL Touch Pro or compatible (min. OS Android 9). - Internet connection. - Interface for communication with the other vehicle-side components (e.g.,

Component	Requirements
	CAN, Bluetooth, WLAN).
Software	- SiCORE Android Application (which embeds the Security Library) - Backend Server Application

1.4 TOE Description

The TOE is composed by 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.
- **SiCore Security Library:** A software library embedded in the SiCORE Android application to be run on the vehicle computer (tablet). This library is in charge of the generation and validation of the integrity proofs of the waste collection.

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

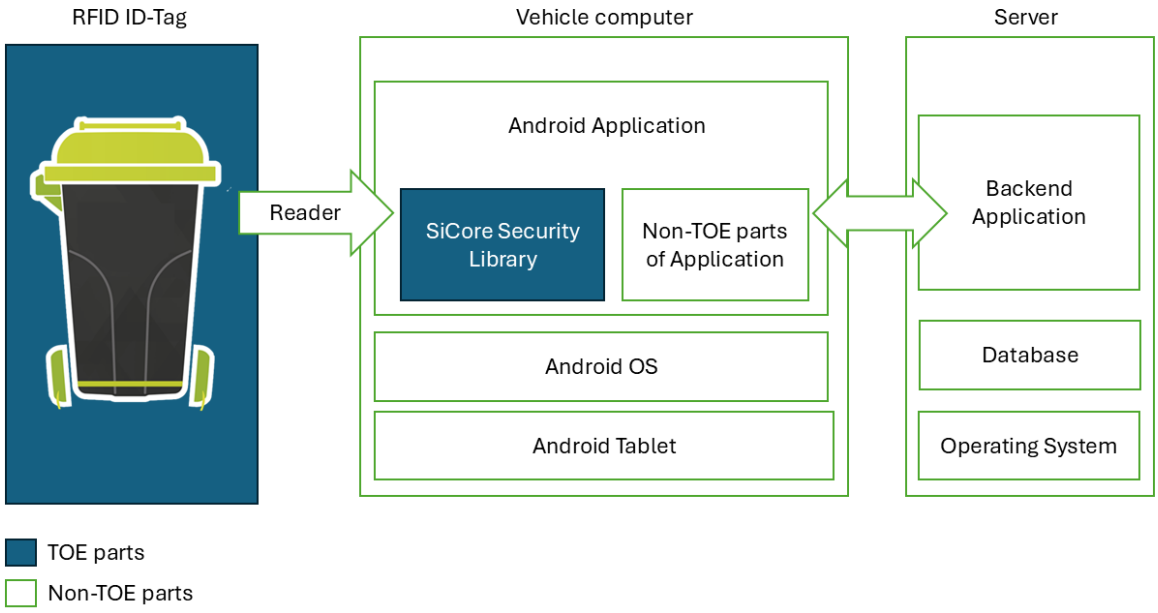

Figure 1: TOE parts inside the Waste Bin Identification System

The objective of the TOE is to provide a secure mechanism that makes it possible to uniquely determine the number of times each waste container is emptied, thereby enabling potential billing based on the number of times the container is emptied. The product can optionally comprise e.g. a weighing or volume measurement system for a weight-based billing.

The waste bins are equipped with a data carrier (ID-Tag). The ID-Tag stores identification data,

which are used for the identification of the waste bin. These data are unique and not confidential. Usually there is a one-to-one correspondence between a set of identification data and the person who is subject to charge. The identification data are read during (or before/after) clearance of the waste bin by the reader. Possible malfunctions during transfer and manipulations are detected using the CRC included in the tag identifier and validated by the software library. The identification data is then transmitted to the vehicle software. Optionally the weight of the waste or the filling height of the waste bin are determined by a dedicated sensors in the vehicle and are transmitted in parallel to the identification data to the vehicle software. The vehicle software supplements these data by adding a date and time information and then forms a record of clearance from all these data.

1.4.1 Physical Scope

Component	Description
ID-Tag	Hardware ID tags are passive transponders that contain a unique ID as well as a check value (CRC). The ID tags are attached to waste containers. 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. The Tags are delivered physically to the clients.
SecurityLib v.1.0.0 (siCORE Security Library 1.0.0)	Software 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 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. SHA-256: 40ae3a8e95ea60ef94169a4f61bc109ecbef821c4e3766be31191d79eea0598e

The TOE does not provide the possibility of different configuration options. Therefore, only one configuration is included in the scope of the evaluation.

1.4.2 Logical Scope

The TOE is a product in the sense of the EUCC.

The TOE consists of an ID-Tag and software library, which is a part of the vehicle software. All other components (see also Fig. 1) are not part of the TOE but of the TOE environment.

The TOE has an external interface to the memories of the vehicle computer, a logical internal interface between the ID-Tag and the vehicle software. The physical channel from the ID-Tag to the vehicle software are not part of the TOE. Only the internal interfaces are considered in this ST. Additional interfaces, especially to the accounting centres of the town councils, are not part of the evaluation. The security module and the office software are also not part of the TOE.

To give the reader of the security requirements a general understanding of the security features of the TOE, the logical security features offered for each TOE part are presented below:

ID-Tag
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
The 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.

2. CONFORMANCE CLAIMS

2.1 Conformance Claim

The Security Target claims conformance to the following Common Criteria documents:

- Common Criteria for Information Technology Security Evaluation (CC:2022) Part 1 Revision 1
- Common Criteria for Information Technology Security Evaluation (CC:2022) Part 2 Revision 1
- Common Criteria for Information Technology Security Evaluation (CC:2022) Part 3 Revision 1
- Common Criteria for Information Technology Security Evaluation (CC:2022) Part 4 Revision 1
- Common Criteria for Information Technology Security Evaluation (CC:2022) Part 5 Revision 1

The security functional requirements in this ST claim extended conformance to CC Part 2.

The security assurance requirements in this ST claim conformant conformance to CC Part 3.

2.2 Protection Profile Conformance claim

This Security Target does not claim conformance to any Protection Profile.

2.3 Package claim

This Security Target is package-conformant with an Evaluation Assurance Level 1 (EAL1), as defined in CC Part 5.

2.4 Conformance rationale

The evaluation assurance level is EAL1. This level provides a significant increase in assurance to unevaluated products. The EAL1 level provides independent assurance that satisfies the assertion of applying measures to protect information related to the identification of waste containers and the timestamp of collection.
The ID-Tag and the data transfer between the ID-Tag and the vehicle software, the data stored in the vehicle are subject to potential attacks. When considering the attack potential, one must take into account the potential value of the data to be protected. This value can be regarded as low. Therefore, low attack potential can be assumed. Only authorised personnel have access to the vehicle software due to suitable physical and organisational measures. This protection is implemented by the vehicle with its components.

Since the assets to be protected are not particularly critical, an EAL1 assurance level is sufficient to meet the needs of Distromel S.A.'s customers.

3. SECURITY PROBLEM DEFINITION

The purpose of this section is to define the nature and scope of the “security needs” to be addressed by the TOE. Therefore, this section will involve (i) any assumptions that are made regarding the TOE environment, (ii) the assets requiring protection, the identified threat agents and the threats they pose to the assets which the TOE must address by fulfilling the security needs.

3.1 **Assets**

AT: A record of clearance AT corresponding to a clearance of a waste bin is an asset **of the TOE**. The record of clearance AT consists of the following data fields:

- **AT1**: Identification data of the waste bin
- **AT2**: Time stamp (date and time) of the clearance.
- Other optional data: Weighing data, GPS position, incident codes.

Application Note:
The identification data AT1 is stored in the ID-Tag and it is the asset itself until the creation of the record of clearance AT. The record of clearance AT can as an option consist of further data fields like for example information about the weight of the collected waste or such as diagnostic data, additional inputs, and others, which, however, do not constitute protected assets.

3.2 Subjects

S.Trusted_personnel: (Trustworthy User) The crew of the collection vehicle and the users of the office computer. Personnel for installation and maintenance of the system. Furthermore, personnel responsible for the security of the environment.

S.Trusted_application: (Trustworthy application) The application that embeds the Security Library which enforces the Security Functions is considered as trustworthy in the sense that is not expected to have hostile activity against the security library with whom it shares application memory space. Given the attack potential for this evaluation and the considered Objectives for the environment, this consideration is feasible.

3.3 Threat agents

S.Attack *Attacker*
A human or a process acting on his behalf located outside the TOE. The main goal of the S.Attack attacker is to modify or corrupt application sensitive information. The attacker has at most a knowledge of obvious vulnerabilities.

Application Note:
The data of the record of clearance (AT) can be corrupted during transfer by purely random effects. Such corruptions are not considered as threats here since no attacker can be identified. The

effectiveness of eventually implemented functionality can be verified by functional tests (homologation testing).

3.4 Assumptions

A.Id *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. 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 *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 *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.

3.5 Threats

An attacker interacts with the TOE interfaces to exploit vulnerabilities, resulting in arbitrary security compromises. The threats address all assets.

T.Man *Manipulated identification data*
An attacker (S.Attack) manipulates the identification data (AT1) within an ID-Tag by means of e.g. mechanical impact, which corrupts the identification data (AT1) only in a purely random way.

T.Jam#1 *Disturbed identification data*
An attacker (S.Attack) disturbs the transfer of the identification data (AT1) from the ID-Tag to the vehicle software by means of e.g. electromagnetic radiation, which corrupts the identification data (AT1) only in a purely random way.

T.Jam#2 *Corrupted record of clearance*
An attacker (S.Attack) corrupts records of clearance (AT) during processing and storage within the vehicle by means of e.g. electromagnetic radiation.

4. SECURITY OBJETIVES

This section identifies and defines the security objectives for the TOE operational environment.

4.1 Security Objectives for the Environment

OE.Id *ID-Tag*
The ID-Tag is fastened to the waste bin. The identification data of the waste bin are saved in the ID-Tag. There shall be only ID-Tags with unique identification data in use. 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.

OE.Trusted *Trustworthy personnel*
It shall be ensured by organisational means that the crew of the collection vehicle (S.Trusted_personnel) are authorised and trustworthy. All persons which install and maintain the system shall be authorised and trustworthy (S.Trusted_personnel). All persons responsible for the security of the TOE environment (S.Trusted_personnel) shall be authorised and trustworthy.

OE.Access *Access protection*
The environment shall ensure by appropriate means (closure, access control by passwords etc.) that only user or service staff (S.Trusted_personnel) can directly access the components of the TOE except the ID-Tag.

4.2 Security Objectives rationale

Assumptions / Objectives for the environment	**OE.Id**	**OE.Trusted**	**OE.Access**
A.Id	X		
A.Trusted		X	
A.Access			X

A.Id (Identification unit) ensures that the identification unit is fastened to the waste bin which it identifies and the data of installed identification units is unique. The correspondence between the identification data and the chargeable customer is established by organisational means. Since the objective OE.Id states exactly the same, it is sufficient for A.Id to be upheld by the objective.

A.Trusted (Trustworthy personnel) ensures that all subjects (except the attacker) are trustworthy. The objective OE.Trusted states exactly the same, so it is sufficient for A.Trusted to be upheld by the objective.

A.Access (Access protection) ensures that the access to the TOE, except for the identification unit, is limited to trustworthy personnel only. The objective OE.Access states exactly the same, so it is sufficient for A.Access to be upheld by the objective.

5. EXTENDED COMPONENTS DEFINITION

The extended component used is the one defined in the [WBISPP104] Protection Profile (not claimed in this Security Target). It was chosen to define FDP_ITT.5 explicitly, because Part 2 of the Common Criteria does not contain a generic security functional requirement for integrity protection of user data when it is transmitted between physically separated parts of the TOE without linking it to access controls or information flow policies. Furthermore FDP_ITT.5 has a more narrowed approach than FDP_ITT.1, as it does not necessarily require that the TOE implements access control SFP and/or information flow control SFP, and it addresses only manipulations of data.

FDP_ITT.5 Internal transfer integrity protection
Hierarchical to: No other components.
Dependencies: No dependencies

FDP_ITT.5.1: The TSF shall enforce the [assignment: *integrity SFP*] to prevent the modification of user data when it is transmitted between physically-separated parts of the TOE.

6. SECURITY REQUIREMENTS

This chapter gives the security functional requirements for the TOE.

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

Assignment: The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bold text and are surrounded by square brackets as follows **[assignment]**.

6.1 TOE Security Functional Requirements

6.1.1 Data authentication (FDP_DAU)

6.1.1.1 Basic data authentication (FDP_DAU.1)

FDP_DAU.1.1	The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **[AT1 and AT clearance records]**
FDP_DAU.1.2	The TSF shall provide **[subject S.Trusted_application]** with the ability to verify evidence of the validity of the indicated information.

Application note:

It is considered that the above requirements can be fulfilled at the targeted assurance level of the evaluation without usage of secrets.

6.1.2 Internal TOE transfer (FDP_ITT)

6.1.2.1 Internal transfer integrity protection (FDP_ITT.5)

FDP_ITT.5.1	The TSF shall enforce the **[Data Integrity Policy]** to prevent the modification of user data when it is transmitted between physically-separated parts of the TOE.

Application note:
The following Security Function Policy (SFP) Data Integrity Policy is defined for the requirement “Internal transfer integrity protection (FDP_ITT.5)”: The User Data (AT1) shall be protected in order to maintain its integrity.

6.1.3 Stored data integrity (FDP_SDI)

6.1.3.1 Stored data integrity monitoring (FDP_SDI.1)

FDP_SDI.1.1 The TSF shall monitor user data stored in containers controlled by the TSF for **[random character integrity error]** on all objects, based on the following attributes: **[identification data AT1 within identification unit and records of clearance AT during storage within the vehicle]**.

6.2 TOE Security Assurance Requirements

Table Assurance Requirements: EAL1

Assurance Class	Assurance Components
ADV	ADV_FSP.1
AGD	AGD_PRE.1 and AGD_OPE.1
ALC	ALC_CMC.1 and ALC_CMS.1
ASE	ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.1, ASE_REQ.1 and ASE_TSS.1
ATE	ATE_IND.1
AVA	AVA_VAN.1

6.3 Security Requirements rationale

6.3.1 Security Functional Requirements dependencies

SFR	CC Dependencies	Satisfied dependencies
FDP_DAU.1	No dependencies	N/A
FDP_ITT.5	No dependencies	N/A
FDP_SDI.1	No dependencies	N/A

6.3.2 Security Functional Requirements rationale

The demonstration that each threat is countered by the SFRs and that at least each SFR is traced back to one threat is as follows:

- **FDP_DAU.1**: Counters threat T.Man. The identification data of the ID Tag embeds a CRC code that makes it possible the detection of a basic manipulation due to a very basic attack (e.g. mechanical impact or misreading of the identifier). The CRC protection is considered sufficient as the attack potential considered is basic.
- **FDP_ITT.5**: Counters threat T.man and T.Jam#1. T.man is countered as the identification data is sent from the ID Tag to the software part with the embedded CRC code, making it possible for the software part to assess if the identifier has suffered any kind of random manipulation. T.Jam#1 is countered as the policy, enforced by the software mandates that all AT1 assets to be checked prior to continue performing any other operations.
- **FDP_SDI**.1: Counters threat T.Jam#2. T.Jam#2 is countered because the software stores a SHA-256 hash value based on the stored record that contains the AT1 and AT records. Therefore, the TSF is able to detect any corruption of such data.

7. TOE SUMMARY SPECIFICATION

FDP_DAU.1 Basic data authentication

This SFR requires the TOE to generate evidence that guarantees the validity of stored records. The TOE satisfies this requirement through the following secure mechanisms:

- The RFID Tag identifier contains a CRC code that is transmitted from the tag to the software part of the TOE to be checked before generating a collection record. If the CRC validation passes the collection record is generated normally and stored. If it the validation fails, the collection record is generated with the addition of a corruption error flag. The host application of the software library is able to obtain such validation results and display them to the operator of the vehicle.
- Each collection record, which contains the RFID Tag Identifier, a timestamp and other optional information (depending on the capabilities of the vehicle) is processed by the security library and a SHA-256 hash of the data structure related to that particular collection is generated and stored. The host application of the software library is able to obtain such validation results and display them to the operator of the vehicle.

FDP_ITT.5 Internal transfer integrity protection

This SFR requires the TOE to protect the integrity of AT1 during transmission between physically separated components of the TOE (the RFID Tag and the software security library). The implementation addresses the following transmission path:

Protection of AT1 integrity during transmission from the ID Tag to the vehicle software: AT1 includes an embedded checksum that the vehicle software verifies upon receipt.

FDP_SDI.1 Stored data integrity monitoring

FDP_SDI.1 requires the TSF to monitor the data stored for random manipulation. This requirement also has two different parts: Monitoring of AT1 integrity within identification unit: as stated in the summary specification of FDP_ITT.5 this is achieved with the verification of the checksum in AT1 performed by the vehicle software. Monitoring of AT integrity during storage within the vehicle: when a record is created it is automatically saved along with its SHA-256 hash. When the record is recovered, this hash is also recovered and verified before further processing the data.

8. APPENDIX A – ACRONYMS

CC Common Criteria

EAL Evaluation Assurance Level

IT Information Technology

ST Security Target

TSF TOE Security Functionality

SFP Security Function Policy

TOE Target of Evaluation

TSF TOE Security Functionality

References

[1] International Organization for Standardization, ISO 11785:1996 Radio frequency identification of animals -- Technical concept

[2] BSI (Bundesamt für Sicherheit in der Infromationstechnik), Protection Profile Waste Bin Identification Systems WBIS-PP Version 1.04