Declaración de Seguridad (low assurance)

"SISTEMA ELECTRÓNICO DE IDENTIFICACIÓN AUTOMÁTICA DE CONTENEDORES POR RFID"

VERSION 1.8, 29/05/2008

DISTROMEL, S.A.

TABLA DE CONTENIDOS

1. INTRODUCCIÓN

1.1 REFERENCIA ST

TITULO:	Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID
AUTOR:	Virginia Pirla en representación de DISTROMEL, S.A.
VERSIÓN ST:	1.8
FECHA:	29/05/2008

1.2 REFERENCIA TOE

NOMBRE:	Sistema electrónico de identificación automática de contenedores por RFID
VERSIÓN TOE:	1.0

1.3 RESUMEN

El “Sistema electrónico de identificación automática de contenedores por RFID” es un sistema que permite identificar contenedores de residuos mediante un tag identificador RFID

El objetivo del TOE es proporcionar un mecanismo seguro que posibilite determinar unívocamente el número de veces que se vacía cada contenedor de residuos, y de esta manera posibilitar una posible facturación en función del número de veces que se realice el vaciado.

Los datos de identificación se generan cuando un vehículo de recogida de residuos vacía un contenedor. Como resultado de esta operación, se crea un registro de vaciado que incluye los datos de identificación del contenedor (identificador unívoco del tag RFID conforme a ISO/IEC 11785:1996), un fechado de tiempo y otros campos relativos a la operativa de recogida.

El TOE abarca las siguientes funcionalidades:

1. Toma de datos (captura de la señal emitida por el TAG RFID conforme a la norma ISO/IEC 11785:1996),
2. Transferencia integra de los datos de identificación entre la antena y el lector
3. Procesado de los datos de identificación (verificación de integridad y concatenación fechado de tiempo)
4. Transferencia integra de los registros de vaciado (que incluyen los datos de identificación del TAG RFID) al Terminal embarcado
5. Almacenamiento seguro en el Terminal embarcado.

.

2. DESCRIPCIÓN TOE

El TOE consiste de:

- Tag RFID, elemento pasivo que permite emitir unos datos almacenados en el chip debido a la aplicación de un campo electromagnético generado por una antena externa. Los datos almacenados en el TAG RFID contienen un identificador unívoco, conforme al formato ISO 11785:1996

- Lector de tags ID, elemento activo compuesto de una antena y un transceptor/decodificador (firmware versionado a 3.18). El lector emite constantemente un campo de electromagnético que permite activar los TAG's RFID y recibir datos íntegros de los TAGS modulados conforme al estándar definido en la ISO 11785:1996. Una vez recibidos los datos de identificación el lector asegura la integridad mediante la verificación del CRC. Y retransmite los registros al Terminal incluyendo en cada registro (el identificador unívoco, un sellado de tiempo, otros campos relativos a la operativa de recogida y el atributo de integridad CRC)

- Terminal embarcado, componente embarcado en el vehículo que almacena persistentemente los datos de vaciado recibidos desde el lector una vez verificada la integridad de éstos.(software versionado a 4.64)

Los componentes del entorno del TOE son:

- Terminal de oficina. Servidor instalado en las oficinas de Distromel S.A. o del cliente que ha adquirido el producto, que permiten recibir a través de una red de telecomunicaciones externa los datos de vaciado de contenedores

La figura siguiente muestra una descripción del sistema.

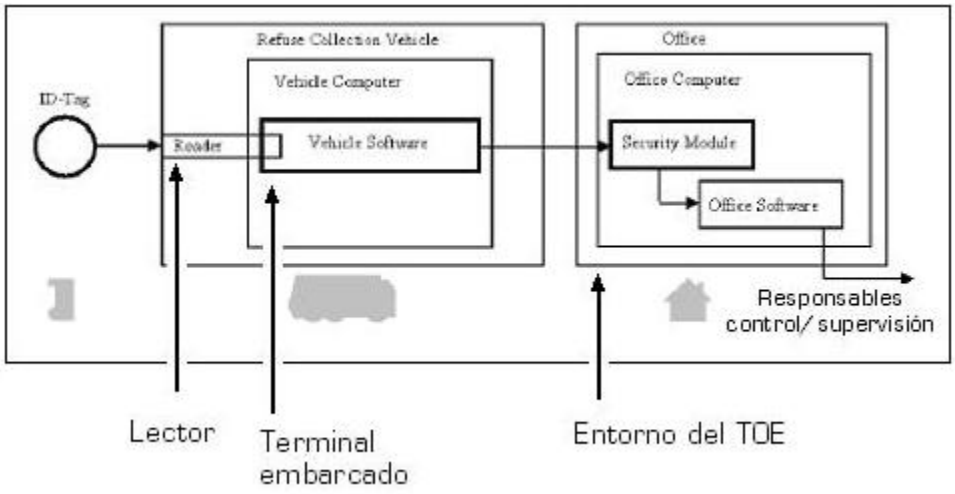

Figura 1: Sistema electrónico de identificación automática de contenedores por RFID

El objetivo del TOE es proporcionar un mecanismo seguro que posibilite determinar unívocamente el número de veces que se vacía cada contenedor de residuos, y de esta manera posibilitar una posible facturación en función del número de veces que se realice el vaciado.

Los contenedores están equipados con TAGS mediante remaches.

El tag-ID guarda datos de identificación y CRC para el control de integridad que se utilizan para la identificación del contenedor de residuos. Estos datos son unívocos y no son confidenciales pero se debe asegurar la integridad. Los datos de identificación se leen durante el vaciado del contenedor por el lector.

El lector verifica la integridad de estos datos y los complementa añadiendo la hora y fecha del proceso y forma un registro de vaciado con todos esos datos. Los posibles fallos de funcionamiento durante la transmisión y manipulación son detectados gracias a la verificación del CRC. Después, los datos del registro de vaciado son transmitidos al Terminal embarcado.

El tag-ID y la transferencia de datos de identificación entre el tag-ID y el lector y los datos de vaciado entre el lector y el Terminal embarcado son objeto de posibles ataques. Se deber tener en cuenta el valor de los datos a proteger (el atributo a proteger es la integridad del dato, no la confidencialidad), ya que el TAG RFID es un elemento físico remachado en los contenedores de residuos y accesibles. Y únicamente personal autorizado tiene acceso al Lector y al Terminal embarcado.

Límites del TOE
El TOE consiste en un tag-ID, el lector de tags ID y el Terminal embarcado. Los otros componentes (ver Figura 1) no son parte del TOE sino del entorno del TOE.

3. CONFORMANCE CLAIMS

3.1 CONFORMANCE CLAIM

Esta Declaración de Seguridad es conforme a:

- Common Criteria versión 3.1 R1 Parte 1
- Common Criteria versión 3.1 R2 Parte 2
- Common Criteria versión 3.1 R2 Parte 3

3.2 Protection Profile claim

No aplica

3.3 Package claim

Esta Declaración de Seguridad tiene una conformidad EAL1. El package EAL1 no contiene operaciones no completadas. No se han añadido SARs extras al nivel EAL1 y los SARs en la ST son consistentes con el nivel EAL1.

3.4 Conformance rationale

El nivel de garantía de evaluación es EAL1. Este nivel proporciona un incremento de garantía significativo respecto a productos no evaluados. El nivel EAL1 proporciona una garantía independiente que satisface la aseveración de aplicar medidas para proteger la información relativa a la identificación de contenedores de residuos y al sellado de tiempo de recogida.

Debido a que los activos a proteger no son especialmente críticos, un nivel de garantía EAL1 es suficiente para cubrir las necesidades de los clientes de Distromel S.A.

4. DEFINICIÓN DE TÉRMINOS

A continuación presentamos una definición de términos

Objetos:

Didentificación:	Registro que incluye datos de identificación del contenedor, asociados al TAG Did, y de vaciado del contenedor, establecidos por Dhora-fecha
Did:	Datos de identificación del contenedor
Dhora-fecha:	Hora y fecha de identificación de vaciado del contenedor

Sujetos:

TAG:	Dispositivo pasivo que almacena internamente un código numérico único
LECTOR:	Dispositivo que lee los datos del tag de manera inalámbrica gracias a su antena lectora
TERMINAL EMBARCADO:	Dispositivo con display incorporado que muestra la lectura de los datos leídos por el dispositivo lector
OFICINA:	Servidor instalado en las oficinas de Distromel S.A. o del cliente que ha adquirido el producto, que permiten recibir a través de una red de telecomunicaciones externa los datos de vaciado de contenedores de residuos

Users:

Usuarios Autorizados:	Personal de cabina del vehículo y personal de mantenimiento e instalación del TOE

Operaciones:

TRASPASO DE DATOS TAG: Transferencia de los datos de identificación del tag hasta el lector

TRASPASO DE DATOS LECTOR: Transferencia de los datos de identificación más registro de vaciado (incluye fecha y hora) del lector al terminal

Atributos de seguridad:

CRCId:	CRC polinomial (CRC-CCITT inverso) empotrado a Did
CRCIdentificación:	CRC polinomial (CRC-CCITT inverso) asociado a Didentificación
ChecksumIdentificación:	XOR de los datos Didenticación

5. SECURITY OBJETIVES

Esta sección identifica y define los objetivos de seguridad para el entorno IT.

5.1 Security Objectives for the Environment

OE.Data Center Com_segura
El entorno debe asegurar que el intercambio de datos con el TOE es seguro.

OE.Acceso Físico
El entorno debe asegurar que únicamente los usuarios autorizados tiene acceso físico al Lector y al Terminal embarcado.

OE.Personal
El entorno debe asegurar que los usuarios autorizados serán confiables y deben conocer y aplicar las guías de uso seguro del TOE.

6. IT SECURITY REQUIREMENTS

Este capítulo proporciona los requisitos de seguridad funcionales y de garantía para el TOE y su entorno.

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 [*los registros* de *Didentificación y de Did]*

FDP_DAU.1.2 The TSF shall provide *user [los usuarios autorizados]* with the ability to verify evidence of the validity of the indicated information.

6.1.2. Internal TOE transfer (FDP_ITT)

6.1.2.1. Basic Internal transfer protection (FDP_ITT.1)

FDP_ITT.1.1 The TSF shall enforce the *[Política de integridad de datos]* to prevent the *[modification]* of user data when it is transmitted between physically-separated parts of the TOE.

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 within the TSC for [*errores de integridad de carácter aleatório]* on all objects, based on the following attributes: *[ChecksumIdentificación de los registros de evidencia de identificación Didentificacion durante el almacenaje dentro del vehiculo]*

6.1.4. Information flow control policy (FDP_IFC)

6.1.4.1. Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the *[Política de integridad de datos]* on *[las operaciones que se detallan a continuación:*

Sujeto	Objeto	Operación
Lector	Did	TRASPASO DE DATOS TAG
Terminal	Didentificación	TRASPASO DE DATOS LECTOR

]

6.1.5. Information flow control functions (FDP_IFF)

6.1.5.1. Simple Security attributes (FDP_IFF.1)

FDP_IFF.1.1 The TSF shall enforce the *[Política de integridad de datos]* based on the following types of subject and information security attributes: *[*

Sujeto	Objeto	Atributo de seguridad
Lector	Did	CRC_{id} de control Did
Terminal	Didentificación	$CRC_{identificación}$ de control Didentificación

]

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: *[Valor correcto de CRC_{id} y $CRC_{identificación}$]*.

FDP_IFF.1.3 The TSF shall enforce the [*Política de integridad de datos*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [*ningún otro caso*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [*todos los otros tipos expectos los marcados en la política de integridad de datos*].

6.2 TOE Security Assurance Requirements

Tabla Assurance Requirements: EAL1

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

6.2.1. Development (ADV)

6.2.1.1. Basic functional specification (ADV_FSP.1)

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorisation of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

6.2.2. Guidance documents (AGD)

6.2.2.1. Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1D The developer shall provide operational user guidance.

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

6.2.2.2. Preparative guidance (AGD_PRE.1)

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

AGD_PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

6.2.3. Life-cycle support (ALC)

6.2.3.1. Labelling of the TOE (ALC_CMC.1)

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

ALC_CMC.1.1C The TOE shall be labelled with its unique reference.

6.2.3.2. TOE CM Coverage (ALC_CMS.1)

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

6.2.4. Security Target (ASE)

6.2.4.1. Conformance claims (ASE_CCL.1)

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the

security problem definition in the PPs for which conformance is being claimed.

ASE_CCL.1.9C The conformance claim rationale shall demonstrate that the statement of security objectives is consistent with the statement of security objectives in the PPs for which conformance is being claimed.

ASE_CCL.1.10C The conformance claim rationale shall demonstrate that the statement of security requirements is consistent with the statement of security requirements in the PPs for which conformance is being claimed.

6.2.4.2. Extended Components definition (ASE_ECD.1)

ASE_ECD.1.1D The developer shall provide a statement of security requirements.
ASE_ECD.1.2D The developer shall provide an extended components definition.

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

6.2.4.3. ST Introduction (ASE_INT.1)

ASE_INT.1.1D The developer shall provide an ST introduction.
ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST. ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarise the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE. ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

6.2.4.4. Security objectives for the operational environment (ASE_OBJ.1)

ASE_OBJ.1.1D The developer shall provide a statement of security objectives.

ASE_OBJ.1.1C The statement of security objectives shall describe the security objectives for the operational environment.

6.2.4.5. Stated security requirements (ASE_REQ.1)

ASE_REQ.1.1D The developer shall provide a statement of security requirements. ASE_REQ.1.2D The developer shall provide a security requirements rationale.

ASE_REQ.1.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.1.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.1.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.1.4C All operations shall be performed correctly.

ASE_REQ.1.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

6.2.4.6. TOE summary specification (ASE_TSS.1)

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

6.2.5. Tests (ATE)

6.2.5.1. Independent testing- conformance (ATE_IND.1)

ATE_IND.1.1D The developer shall provide the TOE for testing.

ATE_IND.1.1C The TOE shall be suitable for testing.

6.2.6. Vulnerability assessment (AVA)

6.2.6.1. Vulnerability survey (AVA_VAN.1)

AVA_VAN.1.1D The developer shall provide the TOE for testing.

AVA_VAN.1.1C The TOE shall be suitable for testing.

6.3 Security Requirements Rationale

A continuación se presentan las dependencias entre SFR y la justificación por la cual no se incluyen todas las dependencias

Componente	Dependencia	Justificación de dependencia
FDP_DAU.1	Ninguna	No aplica
FDP_ITT.1	FDP_ACC.1 o FDP_IFC.1	Se ha incluido el componente FDP_IFC.1
FDP_SDI.1	Ninguna	No aplica
FDP_IFC.1	FDP_IFF.1	Se ha incluido el componente
FDP_IFF.1	FMT_MSA.3	No se ha incluido el componente ya que los atributos de seguridad (CRCid y CRCidentificación) son dinámicos, o sea calculados/verificados en tiempo de recepción y por tanto no existen valores por defecto que hagan aplicar una política en base a estos valores. Además tampoco se pueden asignar valores iniciales que modifiquen los valores por defecto.
FDP_IFF.1	FDP_IFC.1	Se ha incluido el componente

A continuación se detalla la justificación de cobertura entre los SAR y los requisitos de garantía

Componente	Evidencia
ADV_FSP.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008 • Especificación funcional de “Sistema electrónico de identificación automática de contenedores por RFID”, 1.4 19/05/2008 • Manual de Usuario WK NET RSU Carga Trasera/Lateral, Edición 3, Mayo de 2008 • Guía Preparativa Sistema electrónico de identificación automática de contenedores por RFID, Edición 3, 29/05/2008
AGD_PRE.1	• Declaración de Seguridad (low assurance) del Sistema

	electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008 • Guía Preparativa Sistema electrónico de identificación automática de contenedores por RFID, Edición 3, 29/05/2008
AGD_OPE.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008 • Manual de Usuario WK NET RSU Carga Trasera/Lateral, Edición 3, Mayo de 2008 • Especificación funcional de "Sistema electrónico de identificación automática de contenedores por RFID", 1.4 19/05/2008
ALC_CMC.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008 • Listado de configuración, v1.4, 29/05/2008
ALC_CMS.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008 • Listado de configuración, v1.4, 29/05/2008
ASE_CCL.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008
ASE_ECD.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008
ASE_INT.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008
ASE_OBJ.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008
ASE_REQ.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008
ASE_TSS.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008
ATE_IND.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008 • Sistema electrónico de identificación automática de contenedores por RFID v1.0 • Manual de Usuario WK NET RSU Carga Trasera/Lateral, Edición 3, Mayo de 2008 • Especificación funcional de "Sistema electrónico de identificación automática de contenedores por RFID", 1.4

	19/05/2008 • Guía Preparativa Sistema electrónico de identificación automática de contenedores por RFID, Edición 3, 29/05/2008
AVA_VAN.1	• Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, 1.8, 29/05/2008 • Sistema electrónico de identificación automática de contenedores por RFID v1.0 • Especificación funcional de "Sistema electrónico de identificación automática de contenedores por RFID", 1.4 19/05/2008 • Guía Preparativa Sistema electrónico de identificación automática de contenedores por RFID, Edición 3, 29/05/2008

7. TOE SUMMARY SPECIFICATION

7.1 TOE Summary specification

A continuación se presenta un resumen de las funcionalidades de seguridad implementadas en el TOE. También se presenta un mapeado y justificación de cobertura entre requisitos funcionales de seguridad y funcionalidades de seguridad.

1. COMUNICACIÓN INTEGRA TAG-LECTOR

Requisitos que implementa: FDP_DAU.1, FDP_ITT.1, FDP_IFC.1, FDP_IFF.1

Esta funcionalidad de seguridad se encarga de permitir la transferencia de datos protegiendo la integridad de los datos transferidos desde el Tag hasta el Lector. Toda esta funcionalidad de seguridad está basada en el algoritmo CRC de 16 bits en su versión especificada en la norma ISO 11785.

Justificación de cobertura de requisitos:

- FDP_DAU.1: Los datos se consideran auténticos si el valor del CRC computado sobre el código identificador de Tag concatenado con el CRC es igual a cero (CRCId válido).
- FDP_ITT.1: Los datos se consideran válidos (sin errores de integridad) si el atributo de seguridad CRCId es válido.
- FDP_IFC.1: Los datos de Did a proteger son el código de identificación de Tag.
- FDP_IFF.1: Se considerará que Did es válido CRCId lo es.

2. COMUNICACIÓN INTEGRA LECTOR-TERMINAL EMBARCADO

Requisitos que implementa: FDP_DAU.1, FDP_ITT.1, FDP_IFC.1, FDP_IFF.1

Esta funcionalidad de seguridad se encarga de permitir la transferencia de datos protegiendo la integridad de los datos transferidos desde el Lector hasta el Terminal embarcado.

Toda la funcionalidad de seguridad está basada en el algoritmo CRC de 16 bits en su versión especificada en la norma ISO 11785.

Justificación de cobertura de requisitos:

- FDP_DAU.1: Los datos se consideran auténticos si el valor del CRC computado sobre la trama completa (incluyendo el CRC final) es igual a cero (CRCIdentificación válido).
- FDP_ITT.1: Los datos se consideran válidos (sin errores de integridad) si el atributo de seguridad CRCIdentificación es válido.
- FDP_IFC.1: Los datos a proteger son todos los elementos de Didentificacion (Header, Día, Mes, Año, Hora, Minuto, Segundo, Nº Identificación TAG, Extensión Identificación TAG, Peso, Tiempo de Maniobra, Grupo de Incidencia).
- FDP_IFF.1: Se considerará que Didentificación es válido si el CRC es correcto.

3. ALMACENAMIENTO SEGURO TERMINAL EMBARCADO

Requisitos que implementa: FDP_DAU.1, FDP_SDI.1

Esta funcionalidad de seguridad se encarga de asegurar el almacenamiento de datos protegiendo su integridad. Toda la funcionalidad de seguridad está basada en un algoritmo de suma de comprobación que consiste en un XOR de todos los bytes a comprobar.

Justificación de cobertura de requisitos:

- FDP_DAU.1: Los datos se consideran auténticos si el valor de la suma de comprobación sobre la trama completa (incluyendo el valor de la suma de comprobación) es igual a cero.
- FDP_SDI.1: Se comprobará la integridad de los datos Didentificación almacenados en el Terminal embarcado cada vez que se realiza un acceso, mediante la comprobación XOR de los datos almacenados (ChecksumIdentificación)

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