



REF: 2008-9-INF-347 v1
Difusión: Público
Fecha: 15.04.2009

Creado: CERT8
Revisado: TECNICO
Aprobado: JEFEAREA

INFORME DE CERTIFICACIÓN

Expediente: 2008-9 SISTEMA ELEC. DE ID DE CONT. POR RFID
Datos del solicitante: A-25213521 DISTROMEL S.A.

Referencias: EXT-513 Solicitud de Certificación
EXT-581 ETR
CCRA Arrangement on the Recognition of Common Criteria
Certificates in the field of Information Technology Security,
mayo 2000.

Informe de certificación del producto “Sistema electrónico de identificación automática de contenedores por RFID”, versión 1.0, según la solicitud de referencia [EXT-513], de fecha 17 de abril de 2008, y evaluado por el laboratorio Applus, conforme se detalla en el correspondiente informe de evaluación indicado en [EXT-581] de acuerdo a [CCRA], recibido el pasado 4 de junio de 2008.



MINISTERIO DE DEFENSA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN



INDICE

RESUMEN.....	3
RESUMEN DEL TOE	5
REQUISITOS DE GARANTÍA DE SEGURIDAD	5
REQUISITOS FUNCIONALES DE SEGURIDAD	6
IDENTIFICACIÓN	7
PROBLEMA DE SEGURIDAD.....	7
FUNCIONALIDAD DEL ENTORNO.....	7
ARQUITECTURA	8
DOCUMENTOS	8
PRUEBAS DEL PRODUCTO.....	9
CONFIGURACIÓN EVALUADA.....	9
RESULTADOS DE LA EVALUACIÓN.....	9
RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES	9
RECOMENDACIONES DEL CERTIFICADOR.....	9
GLOSARIO DE TÉRMINOS	10
BIBLIOGRAFÍA	11
DECLARACIÓN DE SEGURIDAD	11



Resumen

Este documento constituye el Informe de Certificación para el expediente de la certificación del producto “Sistema electrónico de identificación automática de contenedores por RFID”, versión 1.0.

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.

Fabricante: DISTROMEL S.A.

Patrocinador: DISTROMEL S.A.

Organismo de Certificación: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

Laboratorio de Evaluación: APPLUS

Perfil de Protección: NINGUNO

Nivel de Evaluación: EAL1

Fortaleza de las Funciones: no aplica en CC v3.1

Fecha de término de la evaluación: 4 de junio de 2008

Todos los componentes de garantía requeridos por el nivel de evaluación EAL1 presentan el veredicto de “PASA”. Por consiguiente, el laboratorio APPLUS asigna el VEREDICTO de “PASA” a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL1, definidas por los Criterios Comunes v3.1 [CC-P3] y la Metodología de Evaluación v3.1 [CEM].

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto “Sistema electrónico de identificación automática de contenedores por



MINISTERIO DE DEFENSA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN



RFID” v1.0, se propone la resolución estimatoria de la misma.



Resumen del TOE

- 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

Requisitos de garantía de seguridad

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL1, según la parte 3 de CC v3.1 r2.

ASE_INT.1	ST Introduction
ASE_CCL.1	Conformance claims
ASE_OBJ.1	Security objectives for the operational environment
ASE_ECD.1	Extended components definition
ASE_REQ.1	Stated security requirements
ASE_TSS.1	TOE summary specification
AGD_OPE.1	Operational user guidance
AGD_PRE.1	Preparative procedures
ALC_CMC.1	Labelling of the TOE
ALC_CMS.1	TOE CM coverage
ADV_FSP.2	Basic functional specification
ATE_IND.1	Independent testing - conformance
AVA_VAN.1	Vulnerability survey



Requisitos funcionales de seguridad

La funcionalidad de seguridad del producto satisface los requisitos funcionales, según la parte 2 de CC v3.1 r2, siguientes:

FDP_DAU.1 Basic User Authentication
FDP_ITT.1 Basic internal transfer protection
FDP_SDI.1 Stored data integrity monitoring
FDP_IFC.1 Subset information flow control
FDP_IFF.1 Simple security attributes



Identificación

Producto: “Sistema electrónico de identificación automática de contenedores por RFID” v1.0

Declaración de Seguridad: “Declaración de Seguridad (low assurance) SISTEMA ELECTRÓNICO DE IDENTIFICACIÓN AUTOMÁTICA DE CONTENEDORES POR RFID”, v1.8, de 29/05/2008.

Perfil de Protección: NINGUNO

Nivel de Evaluación: CC v3.1 r2 EAL1

Fortaleza de las Funciones: no aplica en CC v3.1.

Problema de seguridad

Al tratarse de una Declaración de Seguridad de baja garantía (Low Assurance Security Target) no es necesario describir la definición del problema de seguridad. Únicamente se mantiene la descripción de los objetivos del entorno operacional.

Funcionalidad del entorno.

El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

Los objetivos que se deben cubrir por el entorno de uso del producto son los siguientes:

Objetivo entorno 01: OE.Data Center Com_segura

El entorno debe asegurar que el intercambio de datos con el TOE es seguro.

Objetivo entorno 02: OE.Acceso Físico

El entorno debe asegurar que únicamente los usuarios autorizados tienen acceso físico al Lector y al Terminal embarcado.

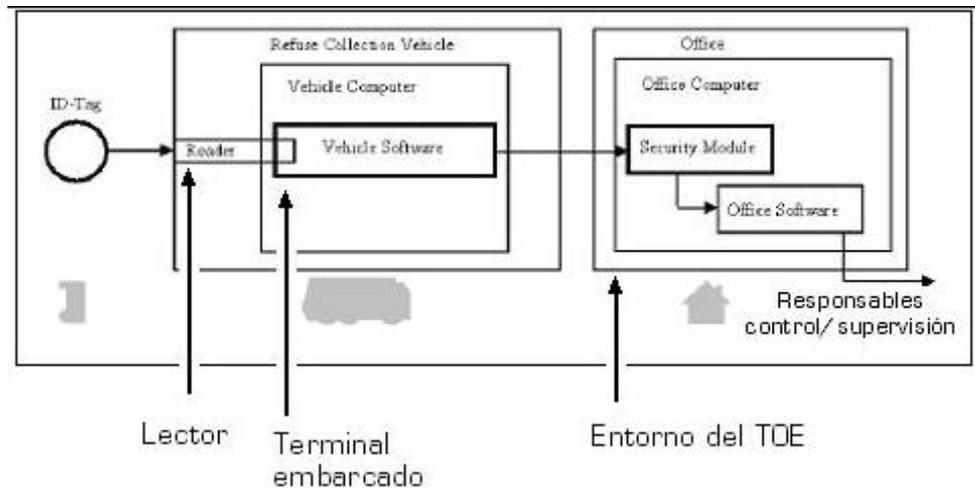
Objetivo entorno 03: OE.Personal

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



Arquitectura

Arquitectura Física:



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.

Documentos

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada.

- Guía Preparativa Sistema electrónico de identificación automática de contenedores por RFID, Edición 3, 29/05/2008
- Manual de Usuario WK NET RSU Carga Trasera/Lateral, Edición 3, Mayo de 2008
- Declaración de Seguridad (low assurance) del Sistema electrónico de identificación automática de contenedores por RFID, v1.8, 29/05/2008



Pruebas del producto

El laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado el evaluador ha constatado que dicha variación no representaba un problema para la seguridad, ni suponía una merma en la capacidad funcional del producto.

Configuración evaluada

Tanto el Lector como el Terminal Embarcado son dispositivos hardware diseñados para cumplir con las especificaciones del producto y programados a bajo nivel con ese propósito.

Resultados de la Evaluación

El producto “Sistema electrónico de identificación automática de contenedores por RFID” v1.0 ha sido evaluado frente a la declaración de seguridad “Declaración de Seguridad (low assurance) SISTEMA ELECTRÓNICO DE IDENTIFICACIÓN AUTOMÁTICA DE CONTENEDORES POR RFID”, v1.8, de 29/05/2008.

Todos los componentes de garantía requeridos por el nivel de evaluación **EAL1** presentan el veredicto de “PASA”. Por consiguiente, el laboratorio APPLUS asigna el **VEREDICTO de “PASA”** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL1, definidas por los Criterios Comunes [CC-P3] y la Metodología de Evaluación [CEM] en su versión 3.1 r2.

Recomendaciones y comentarios de los evaluadores

Aunque se han detectado desviaciones en la documentación del producto éstas han sido corregidas por el desarrollador con gran brevedad. Los evaluadores no han detectado desviaciones en la última versión de cada uno de los documentos que componen las evidencias de evaluación y han comprobado el cumplimiento de la norma Common Criteria versión 3.1. No se han detectado desviaciones en los mecanismo IT del TOE. El TOE evaluado es consistente con la documentación aportada por Distromel.

Recomendaciones del certificador



MINISTERIO DE DEFENSA
CENTRO NACIONAL DE INTELIGENCIA
CENTRO CRIPTOLÓGICO NACIONAL
ORGANISMO DE CERTIFICACIÓN



A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto “Sistema electrónico de identificación automática de contenedores por RFID”, versión 1.0, se propone la resolución estimatoria de la misma.

Glosario de términos

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ETR	Evaluation Technical Report
OC	Organismo de Certificación



Bibliografía

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CC_P1] Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and general model, Version 3.1, r1, September 2007.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 3.1, r1, September 2007.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 3.1, r1, September 2007.

[CEM] Common Evaluation Methodology for Information Technology Security: Introduction and general model, Version 3.1, r1, September 2007.

Declaración de seguridad

Conjuntamente con este informe de certificación, se dispone en el Organismo de Certificación de la declaración de seguridad completa de la evaluación: “**Declaración de Seguridad (low assurance) SISTEMA ELECTRÓNICO DE IDENTIFICACIÓN AUTOMÁTICA DE CONTENEDORES POR RFID**”, v1.8, de 29/05/2008.