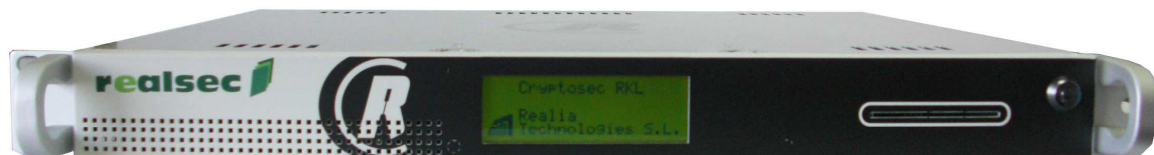




VISION DE CONJUNTO Y CARACTERISTICAS TÉCNICAS DE CRYPTOSEC-RKL



Cryptose-RKL



15 de Febrero de 2010

Lista de distribución: Director General Comercial Realsec : JESUS RODRIGUEZ CABRERO

Director Departamento Técnico Realsec : JOSE ALBERTO GORDO

Tabla de contenidos

1. Introducción	3
2. Resumen ejecutivo	3
3. Servidor RKL – VISION DE CONJUNTO	4
3.1. Descripción funcional	4
3.1.1. <i>RtServer – conjunto de aplicaciones</i>	5
4. Requerimientos sistema	6
4.1. Requerimientos Software	6
4.2. Requerimientos Hardware	6
5. Suposiciones y Dependencias	6
6. Referencias	7

1. Introducción

En este documento presentamos la oferta del Servidor **Cryptosec-RKL** de Realsec, un **sistema multivendor** para automatizar el proceso de la carga remota de las Claves Iniciales del parque de cajeros, sirviéndose de técnicas de certificados y firmas con claves asimétricas.

En los capítulos siguientes se explican las funcionalidades de **Cryptosec-RKL** y se describe la arquitectura técnica del mismo, además de realizar una definición de los requerimientos del sistema.

2. Resumen ejecutivo

Con el objetivo de lograr confidencialidad, integridad y evitar el repudio de las transacciones electrónicas, las grandes marcas y redes definen un marco de Requerimientos de Seguridad en el cual precisan no solo las exigencias de seguridad física, que deberían cumplir los dispositivos de introducción y manejo de PIN, sino además indican las técnicas de Gestión de Claves y los Algoritmos a emplear.

Algunos de los estándares que gobiernan las políticas de seguridad lógica en lo que respecta a la gestión de PIN y claves son los publicados y revisados por el comité X9, participado por expertos de la Asociación de la Banca, y encargado por el organismo ANSI, quien esta a cargo de la revisión de estas especificaciones cada 5 años para acomodar las tecnologías emergentes y el impacto de las nuevas tendencias del mercado.

En sus estándares Visa y MasterCard prestan también una especial atención a las técnicas a utilizar para transferir las claves en el cajero con el fin de preservar su integridad. En el caso de carga de claves en claro, que es el sistema tradicional, para asegurar que en el proceso de carga, estas no sean comprometidas, se exige el cumplimiento del principio de control dual y conocimiento parcial (que actualmente es el sistema diseñado de claves en componentes).

Sin embargo la compleja logística y la ineficiencia, propia de todos los procesos manuales, hace que el procedimiento de carga manual de un numero relativamente grande de cajeros, si se realiza cumpliendo todos los requisitos de VISA (desplazar a personas, horas, viajes dietas, el registro de los procesos para la auditoria posterior, etc.) se traduce en una carga tediosa y con un coste elevado para las entidades financieras.

Coincidiendo estas inquietudes de la industria, con la tecnología disponible de criptografía asimétrica, las grandes Redes promueven una revisión de los estándares para incluir la funcionalidad de carga remota de claves utilizando criptografía de clave pública, definiendo un nuevo marco de seguridad y aceptación global. Desafortunadamente, no se promovió una revisión en paralelo del estándar XFS (el conjunto de especificaciones para el acceso a los dispositivos financieros con independencia de los elementos hardware), para incluir en él la funcionalidad de carga remota de claves, permitiendo aproximarse al objetivo de un interfaz único para los diferentes proveedores para el proceso de carga de las claves iniciales en los cajeros, definiendo así la deseada base para la interoperabilidad y aceptación global entre Fabricantes de Autoservicio y Proveedores de Soluciones Host.

Este escenario plantea a las Entidades Financieras la necesidad de implementar una solución de carga remota de claves por cada uno de sus proveedores, teniendo en cuenta además la evolución según los estándares y tecnologías emergentes.

La solución que propone Realsec es un Servidor de Carga Remota de Claves, que implementa los esquemas de carga de los principales fabricantes de Autoservicio DIEBOLD, NCR, Wincor, Fujitsu etc. y que ofrece:

- Arquitectura Cliente multivendor – NCR, WINCOR, DIEBOLD etc.
- Arquitectura Cliente - basada en estándar XFS
- Arquitectura Servidor abierta - basada en la plataforma tecnológica .NET
- Independencia de los modelos actuales de los procesos operativos del Host y Autoservicios.

3. CRYPTOSEC- RKL – VISION DE CONJUNTO

El Servidor **Cryptosec-RKL** es un sistema multivendor para la carga remota de las Claves Iniciales del parque de cajeros o terminales de punto de venta, sirviéndose de técnicas de certificados y firmas con claves asimétricas, como establece los estándares de Visa y MasterCard.

Uno de los principales objetivos de la solución es que ésta no requiera cambios hardware y software en el Host a la hora de integrar este proyecto con la operativa funcional del Host, y además no plantear la necesidad de cambios en la Aplicación que se ejecuta actualmente en los Autoservicios. Se trata por tanto de lograr que la Solución tenga una autonomía completa y no requiera integración con los sistemas Host.

3.1. Descripción funcional

Este apartado describe la arquitectura del sistema Cryptosec-RKL, así como su funcionalidad.

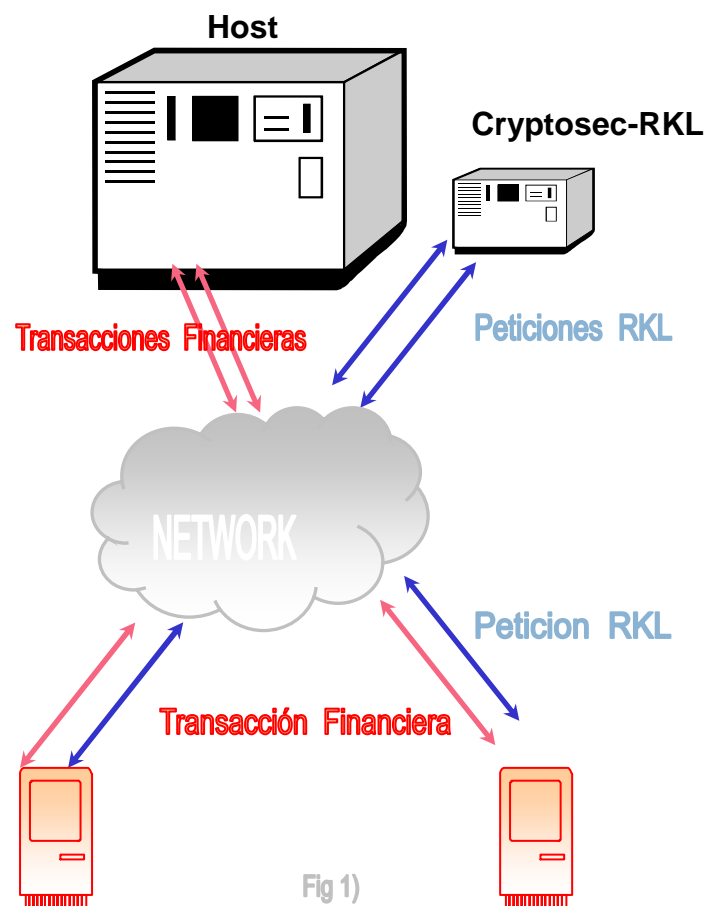
La solución **Cryptosec-RKL** utiliza un modulo de seguridad tamper-resistant y tamper-responsive, en cuya memoria residirían las Claves Master de Transporte para las distintas entidades financieras adheridas al servicio de RKL.

En cada uno de los Autoservicios residiría un componente, que durante el arranque de la aplicación de Autoservicio, sería lanzado por ella, si la condición de operatividad del cajero así lo determina (comprobando para ello si está inicializado con la jerarquía de claves correspondiente). Una vez recibida la activación por parte de la aplicación, el componente automáticamente iniciará una petición de carga de la clave inicial del Autoservicio hacia el Servidor Cryptosec-RKL.

El Servidor recibirá peticiones procedentes del parque de cajeros para la carga de la clave inicial de los diferentes cajeros. Finalizada la sesión de transmisión de la clave Inicial para el Autoservicio en cuestión, éste estará en condiciones para iniciar operaciones contra el Host **de la manera habitual** sin necesidad de dialogar nunca mas con el Servidor Cryptosec-RKL, mientras el equipo en cuestión no sea reinstalado o decomisionado. En estos dos últimos supuestos, el proceso de petición de carga de claves será lanzado de nuevo por la aplicación de Autoservicio, de forma automática y transparentemente para el personal técnico o de la oficina.

Una vez completado el proceso de carga de la Clave Inicial por cada Autoservicio Inicializado, la Aplicación de Autoservicio comunicaría la nueva condición del cajero como "inicializado" a la Solución de Gestión de Red.

La figura 1) muestra el modelo de operaciones descrito mas arriba.



3.1.1. Cryptosec-RKL Conjunto de aplicaciones

La solución cuenta los siguientes módulos software:

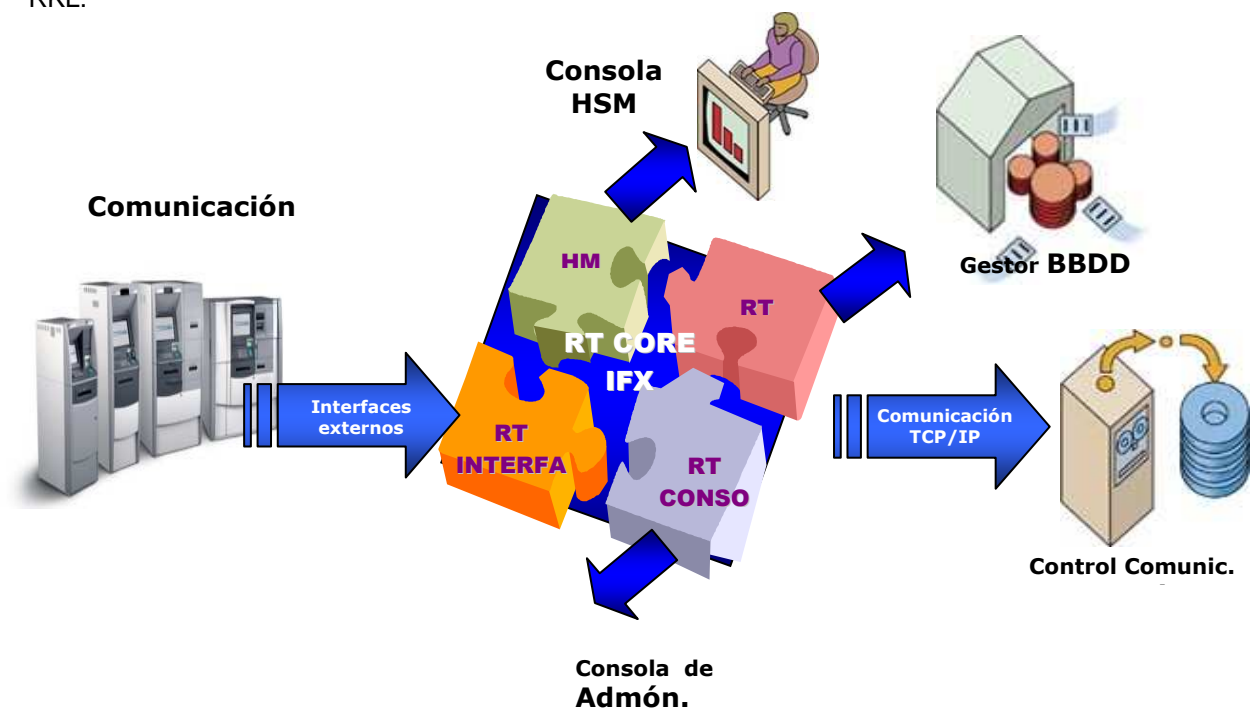
RtCore– este componente recibe y procesa las peticiones de carga remota de claves que recibe procedentes del parque de Cajeros. Se responsabiliza de la programación de las primitivas criptográficas del modulo de seguridad, para brindar la funcionalidad requerida según el esquema específico RKL.

RtInterfaces– Cryptosec-RKL se comunica con entidades externas tales como el parque de Cajeros a través de interfaces. Las interfaces llevan a cabo las **comunicaciones** entre el sistema Cryptosec-RKL y el mundo exterior. Son los responsables de ejecutar el protocolo de carga de claves específico para cada uno de los fabricantes, llevando primero la Autenticación Bilateral y posteriormente utilizando el canal seguro establecido transmiten la clave Inicial del Autoservicio. Todos los mensajes enviados entre el **RtCore** y los **RtInterfaces**, son formateados de acuerdo con protocolo específico por cada fabricante, usando como protocolo de comunicaciones el estándar TCP/IP.

RtOffice – es el componente encargado de los procesos de gestión de las bases de Datos, el manejo de los datos necesario para el correcto funcionamiento del sistema y de la generación de informes.

RtAdmin – Es el modulo de administración de la solución Cryptosec-RKL, que a través del GUI permite la configuración de la Solución con los datos necesario para el optimo funcionamiento del sistema y su gestión administrativa.

RtAgent – se trata de un componente que reside en el Cajero y que durante el arranque del Autoservicio determinara la necesidad de iniciar el proceso de petición de la clave inicial a Cryptosec-RKL.



4. Requerimientos sistema

4.1. Requerimientos Software

Requerimientos Software de la Plataforma Servidor

- No existen requerimientos al tratarse de un “Appliance” enracable con software basico incorporado.

Requerimientos Software Plataforma Autoservicio

- Microsoft Windows XP
- EPP XFS Service Provider 3.0

Plataforma Bases de Datos

Por parte de Realsec no existe ninguna preferencia técnica por la Base de Datos a utilizar – podría ser tanto Oracle como SQL Server, como DB2, ni sobre el modelo de instalación de ésta – si en local o central.

El único requerimiento aplicable a ésta es que la SGBD permita la concurrencia de procesos. La elección que haga la Entidad Financiera podría basarse a los acuerdos de licencias corporativas vigentes.

Estimación de Crecimiento del tamaño de las Bases de Datos.

Calculamos que se generarían entre 15 y 20 registros por cajero al año que sería necesario a tener en cuenta en la estimación del orden de crecimiento de las Bases de Datos.

4.2. Requerimientos Hardware

Plataforma Servidor

- No existen requerimientos al tratarse de un “Appliance” enracable .

Modulo de Seguridad HSM

El sistema incorpora el HSM **CryptoSec 2048** de REALSEC con Certificación FIPS 140-2 Level 3 por el NIST.

El modelo HSM cubre el conjunto de primitivas criptográficas necesarias para la gestión de generación y verificación de firmas utilizando algoritmos asimétricos. La consola de seguridad ofrece extensas posibilidades de gestión de las claves que residen en el sistema y de la administración de la los usuarios CriptoOFFICERs con derechos de acceso al sistema, de los custodios de la Clave Master del equipo y la programación de las operaciones de mantenimiento entre otros.

5. Suposiciones y Dependencias

La solución Cryptosec-RKL se enlaza con el parque de ATMS bajo el protocolo TCP/IP. Donde sea necesario utilizar otro protocolo como el X.25, Realsec proporcionará una tarjeta convertidora de protocolos de comunicaciones.

En el alcance de este proyecto no esta incluida la gestión, ni el coste de obtener una certificación externa por parte de Entidades Independientes. Si le es requerido Realsec presentara una oferta económica, cuyo objeto será la definición de la gestión a llevar a cabo para obtener una certificación externa en el marco de referencia indicado por la Entidad Financiera.

6. Referencias

La solución cuenta, entre otros, con los siguientes clientes en el sector financiero.

Instalación /Cliente
Caja MADRID
Caixa GALICIA
CAIXANOVA
UNICAJA
Caixa TERRASA
Caixa GIRONA
Caixa MANRESA
Caixa LAIETANA
Caixa PENEDES
Caixa MANLLEU
Caja CANTABRIA
Caja SOL
Banco Nacional di Laboro (Italia)
Banco SABADEL
Grupo BBVA
HSBC (Mexico)
ERST BANK (Rumanía)
Etc