



CRYPTOSEC-RKL

OVERVIEW

AND

TECHNICAL FEATURES



Table of contents

3. CRYPTOSEC- RKL – OVERVIEW4
 3.1 *Functional description* 4
 3.1.1 *Cryptosec–RKL Set of applications*..... 5
4. System Requirements.....6
 4.1 *Software Requirements*..... 6
 4.2. *HardwareRequirements* 7
5. Assumptions and Premises7
6. References7

1. Introduction

This document is intended to introduce the solution **Cryptosec-RKL** Server from Realsec, a multivendor system for remote loading of the ATMs Initial Keys, using techniques of certificates and electronic signatures with asymmetric key.

In the following chapters we explain the features of **Cryptosec-RKL**, describe its technical architecture and define the system requirements.

2. Executive Summary

With the goal of confidentiality, integrity and ensure non repudiation of electronic transactions, network companies of means of payment and ATM manufacturers have defined a framework of the Security Requirements that clearly specify physical safety requirements, as well as the characteristics that must comply with the introduction of devices and PIN management, indicating in these, the key management techniques and algorithms to be used.

Many of the standards that make up the mechanisms for PIN and key management are reviewed on a regular basis through the X9 committee. This committee is composed mostly of experts from the association of Bankers, and commissioned by the agency ANSI. These revisions are aimed to analyze the emerging technologies and explore new market trends.

In their standard policy, Visa and MasterCard, are also providing special attention to the techniques being used in connection with the transfer of keys to the ATM's, to ensure its integrity in the process. That is why we have implemented the principle of dual control and partial knowledge. This is a traditional procedure that ensures the loading process of keys and ensures that these are not jeopardized (currently the system is designed by key components).

However the complex logistics and inefficiency, typical of all manual processes, makes the manual loading procedure of a relatively large number of ATM's, a tedious burden and very costly for financial institutions, if carried out in compliance with all visa requirements (displace people, hours, travel allowances, registration processes for the subsequent audit, etc).

Taking into account these considerations, and using available technologies for asymmetric cryptography, the huge networks are promoting a revision of standards, in order to include the functionality of key download using public key cryptography. This promotes a new framework for security and global acceptance.

Unfortunately, a parallel review of the standard XFS was not promoted (is a set of specifications for access to financial devices regardless of the hardware elements), and because of this, Cryptosec-RKL does not provide an unique interface for all different ATM's suppliers who interact in the process of loading Initial keys in the ATM's; thus hindering the so much desired basis for interoperability and global acceptance among manufacturers of ATM's and Host Solutions Providers

This scenario poses Financial Institutions the need to implement a solution to download the key for each of its suppliers, taking into account further developments like standards and emerging technologies.

The solution proposed by Realsec is a Remote Key Loader Server, which implements key load schemes for the leading manufacturers of ATM's Service such as Diebold, NCR, Wincor, Fujitsu and others, by providing the following:

- Multivendor Client Architecture -Diebold, NCR, Wincor, Fujitsu ...
- Client Architecture - based on standard XFS
- Server open architecture – based on the NET technology platform

- ❑ Independence of current models of business processes between Hosts and ATMs.

3. CRYPTOSEC- RKL – OVERVIEW

The **Cryptosec-RKL** server is a multivendor system for the remote loading of the ATM's Initial Keys or point of sale terminals (POS's), using certificate techniques and signatures with asymmetric key, as stipulated in Visa and MasterCard security standards.

One of the main objectives of the solution is the fact that it does not require hardware and software changes in the host when it comes to be integrated with the functional Host operation, and there is no need for changes in the ATM applications. This is to ensure that the solution has a complete autonomy and does not require integration with host systems.

3.1 Functional description

This section describes the Cryptosec-RKL system architecture, as well as its functionality.

The Cryptosec-RKL solution module uses a security tamper-resistant and tamper-responsive device, whose memory would store the Transportation Master Key for all the different financial institutions linked to such RKL service.

In each ATM there is a component, which during the start-up of its implementation, would be launched if the operational status of the ATM so determines (for checking if it is initialized with the corresponding hierarchy of keys). Once received by the activation of the application, the component automatically initiates a request for the load of the ATM initial key to the server Cryptosec - RKL.

The server will receive requests from the ATM's Network for the future loading of the initial key. Upon transmission of the Initial key to the related ATM, it will be able to launch operations against the host **in the usual manner** without having to communicate any longer with Cryptosec-RKL server, as long as the ATM is not reinstalled or seized. If so, the process of requesting a new loading key would be relaunched by the ATM application, automatically and transparently for the technical staff.

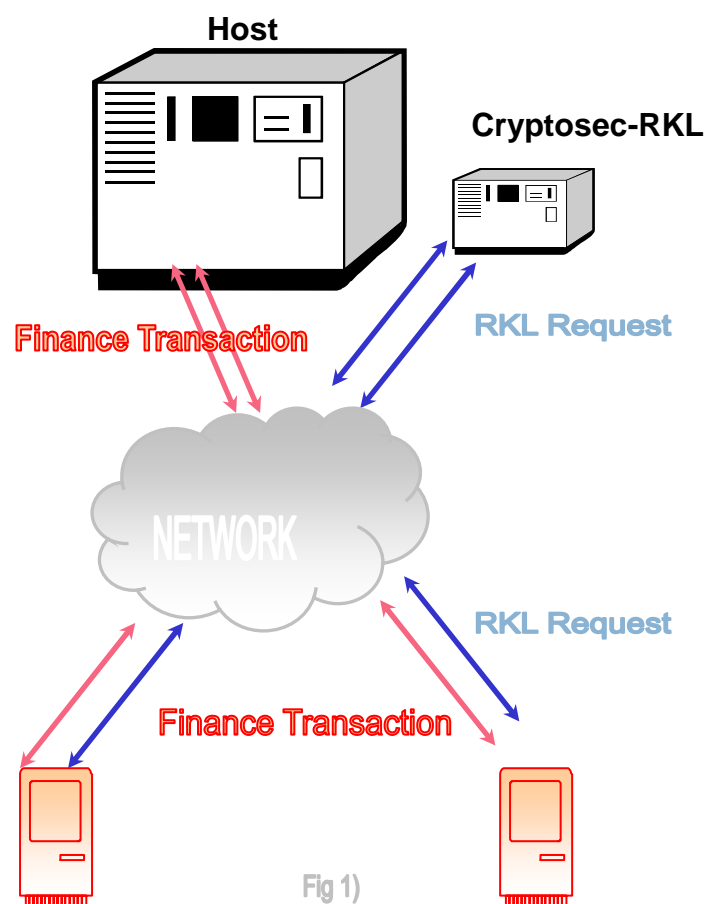


Fig 1)

After completing the loading process of the Initial Key per every ATM-initialization, the implementation of the ATM will communicate the new cashier's condition as "initialized" to the Network Management Solution.

Figure1) shows the operating mode described above.

3.1.1 Cryptosec–RKL Set of applications

The solution includes the following software modules:

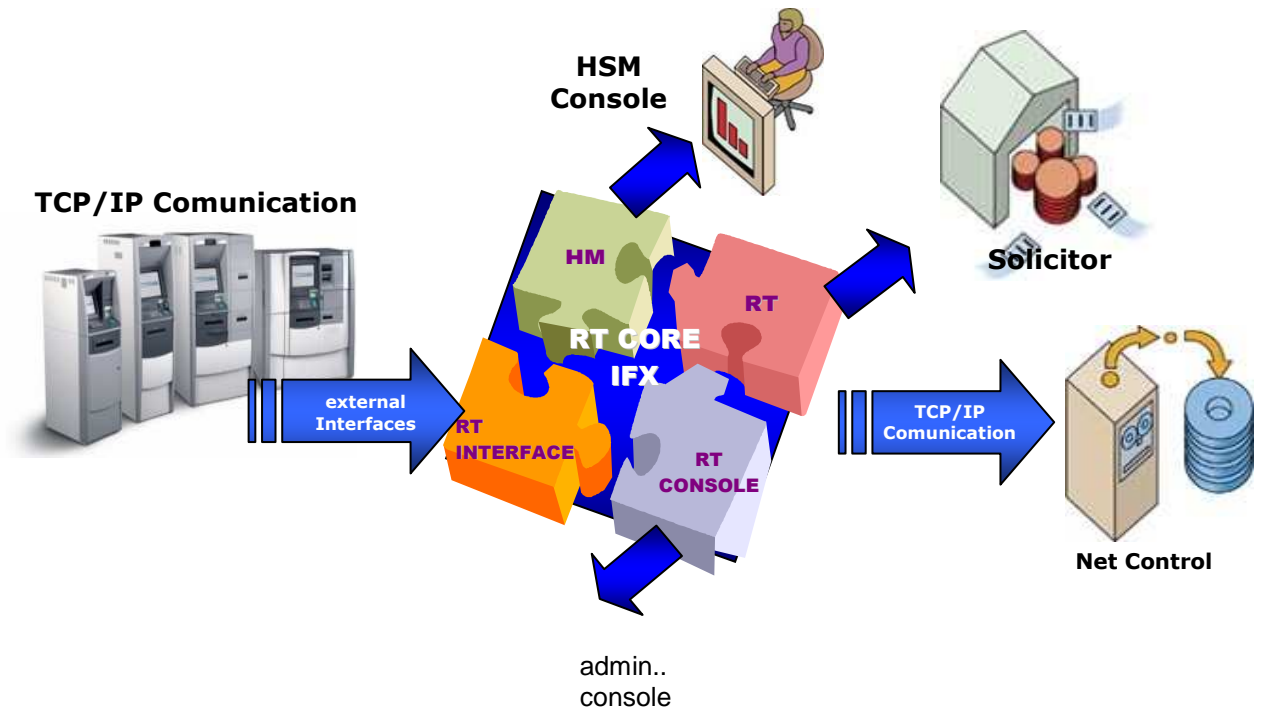
RtCore- This component receives and processes requests from remote key loading coming from the ATMs. It is responsible for the scheduling of the primitive cryptographic security module, to deliver the functionality required under the specific RKL scheme.

RtInterfaces- Cryptosec-RKL communicates with external entities such as ATMs across interfaces. The interfaces carry out **communications** between the system Cryptosec-RKL and the outer world. They are responsible for implementing the protocol for loading specific keys for each of the manufacturers; by initially performing a Bilateral Authentication System and then using the secure established channel to transmit the Initial ATM key. All messages sent between **RtCore** and **RtInterfaces** are formatted according to specific protocol for each manufacturer, using as the standard communications protocol TCP / IP.

RtOffice - Is the component responsible for the management processes of databases, data management necessary for the proper functioning of the system and report generation.

RtAdmin - Is the administration module of the solution Cryptosec-RKL, which allows for Configuration by using a GUI interface to enter the necessary information for optimal functioning of the system and its administration.

RtAgent - Is a component that is stored at the ATM for determining during its start up, whether there is any need to initiate the process request of the Cryptosec-RKL initial key.



4. Systems Requirements

4.1 Software Requirements

Software Requirements of the Server Platform

- There are no requirements, since we are providing a rackable Appliance with basic preinstalled software.

Software Requirements ATM Platform

- Microsoft Windows XP
- EPP XFS Service Provider 3.0

Databases platform

The system will work with all major Databases vendors, like Oracle, SQL Server or DB2, both in local and central operations methods.

The only requirement is that the DBMS shall allow concurrent processes.

Growth estimations of Databases

We estimate that the system would generate between 15 and 20 entries per year per ATM. This should be taken into account when scheduling future growing demands.

4.2. Hardware Requirements***Server Platform***

- There are no requirements. An appliance is provided.

HSM Security Module

The system incorporates the HSM **CryptoSec** of REALSEC which is FIPS 140-2 Level 3 certified.

The HSM model includes all the standard cryptographic functionality needed to manage generation and verification of signatures, by using asymmetric algorithms. The security console provides extensive opportunities for the management of the keys stored in the system and the administration of CriptoOFFICERs users with access rights to the system, the custodians of the Master Key equipment and programming-keeping operations among others.

5. Assumptions and Premises

The solution Cryptosec-RKL is linked to the ATMS under the TCP / IP protocol. Where it is necessary to use another protocol such as X.25, Realsec will provide a communication's conversion protocol card.

6. References

The solution has several clients in the financial market, such as:

No.	Customer	Number of ATMs
1	Caja MADRID	5000 ATMs
2	Caixa Galicia	1000 ATMs
3	CaixaNova	500 ATMs
4	Unicaja	500 ATMs
5	Terrasa	500 ATMs
6	Girona	500 ATMs
7	Manresa	500 ATMs
8	Laietana	500 ATMs