CardMan Smart Technology

We smart you up.

FINREAD Whitepaper

Document Title: FINREAD Whitepaper

Document Version: 1.0

Document Type: Whitepaper

Company: OMNIKEY AG

Author: Kurt Schmid & Harald Zeitlhofer

Abstract: This document gives background information on FINREAD and describes the OMNIKEY Trust FINREAD smart card reader.

Disclaimer:

The information in this document may not be changed without express written agreement of OMNIKEY AG and is subject to change without notice.

Contents

1 Overview

In a world, where security is widely a central topic in most different areas, smart cards are increasingly being used for payments, home-banking, access control, internet security, PKI-tokens, healthcare, loyalty, etc. The smart card itself is becoming more and more a device offering high security. To establish this level of security also to the transaction done with interaction by the end-user, a card reader infrastructure is required, that offers security **and** interoperability at the same time.

Securing e-transactions

With this increasing number of smart card based payment and e-commerce transactions on open networks, there is a requirement of suitable solution for providing high security in those environments.

Today we do have the security offered by ATMs in combination with banking smart cards but the smart card reader infrastructure at home lacks this security.

PC/SC, which is currently the most used industry standard in the PC-attached smart card technology, does not provide the needed security for a trusted system

Open architecture

Today each smart card scheme needs a development on each different infrastructure device. This limits the easy and secure usage of smart cards. Therefore an open infrastructure is desirable, where there is only a single developed code that runs in every infrastructure.

2 What is FINREAD?

FINREAD is an architecture to solve these issues: Define a secure **and** interoperable smart card reader infrastructure:

FINREAD is a set of technical specifications for a PC connected secure smart card reader that have been created by a consortium within a EU programme. The specifications (available on www.finread.com) describe a card reader for payment and global financial as well as e-commerce transactions, that guarantees highest end-to-end security in an untrusted environment (e.g. at home, internet). It takes the form of an external peripheral for personal computers and can be compared to the card-reading terminal that consumers are familiar with at retail outlets.

FINREAD adopts and extends the Java applet technology to execute code inside a reader. In a FINREAD environment applets are called **Finlets**. These Finlets perform the security relevant parts inside the reader and communicate to the related FINREAD application running on a PC.

In addition a FINREAD device has to have a small display as well as a PIN-Pad for user interaction.

The PC-application can download Finlets containing **security** functionality into the Card Reader to be executed there. These Finlets perform sensitive transactions with the smart card on the one side and the user on the other hand. Finlets can and shall make use of the added security functionality offered by the FINREAD device:

- Ask the user for the correct PIN on a small PIN-Pad
- Displaying security sensitive information on the LCD-display
- Ask the user to confirm or cancel a transaction by pressing function keys.
- Use cryptography operations like encryption or authentication
- Perform transactions with the smart card
- Communicate with the PC

Interoperability guarantees, that those Finlets developed by or under the responsibility of different application providers (e.g. payment, health or government scheme, etc) can be downloaded into any FINREAD device. For this reason the FINREAD specifications have been adopted as a CWA (CEN Workshop Agreement) by the European Committee for Standardization (CEN).

The specifications are sufficiently open to accommodate transactions also of a non-financial nature (e.g. e-Government, health, access control, and so on).

3 FINREAD Security

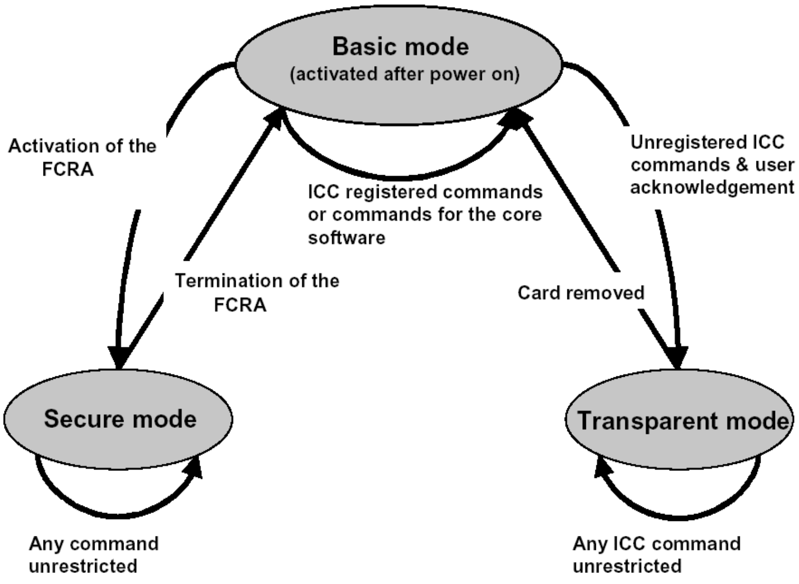
The security within the FINREAD architecture consists of several elements:

A secure display that guarantees the integrity of the information displayed during a transaction (e.g. the purchase amount), while a **secure keypad** prevents PIN capture outside the reader.

An **authentication mechanism** using Public Key Infrastructure within the reader ensures, that the transaction is performed on a trusted device. This authentication using the card reader's certificate ensures that the transaction has been performed on a genuine trusted FINREAD card reader.

Only digitally signed FINREAD-applets (Finlets) are accepted to be downloaded to the reader through a highly **secure download** mechanism. This prevents the execution of malicious software in the device.

In **secure mode** (see figure below) only the Finlet is allowed to communicate with the smart card. Unknown smart cards are used in a transparent access mode of operation only. The transparent mode may be disabled, which means that unknown cards can't be used. This increases the security of the entire system.


Basic mode
(activated after power on)
Activation of the FCRA
ICC registered commands or commands for the core software
Unregistered ICC commands & user acknowledgement
Termination of the FCRA
Card removed
Secure mode
Transparent mode
Any command unrestricted
Any ICC command unrestricted

Finlets are activated by the PC only. It is up to the PC-hosted FINREAD application to activate and terminate the execution of applets in the reader and to send instructions to the card (such as validity control of the PIN, management of the display…).

From a **hardware security** point of view, a FINREAD card reader is tamper evident and the module inside the reader that keeps the private asymmetric keys is tamper resistant. Moreover, only readers which have been approved as compliant with the FINREAD security requirements may be signed by an authorised entity belonging to a PKI.

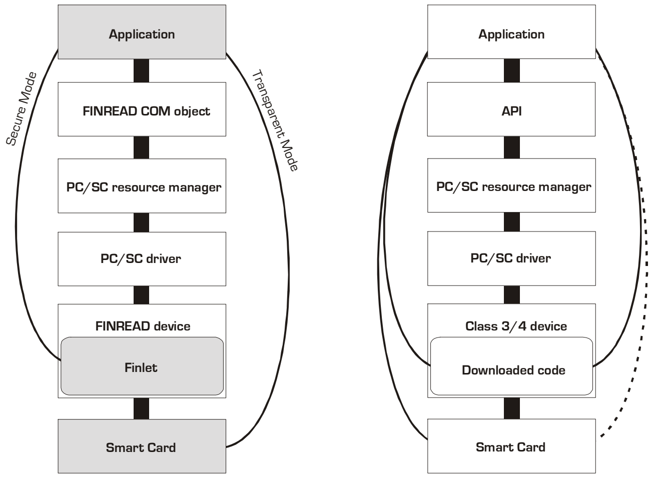
4 FINREAD Interoperability

The interoperability within the FINREAD architecture consists of several elements:

The reader uses the **Java Virtual Machine** technology to execute small application programs (applets) which conform to a standardized set of specifications. A specific applet can therefore be created by different developers in different organizations and be executed on different readers complying to the FINREAD specifications, in a completely interoperable way between a variety of card reader manufacturers. As mentioned these applets are called **Finlets** within the FINREAD terminology.

This interoperability reduces the cost of development and maintenance of applets, since a Finlets needs only to be developed once (e.g. a bank EMV applet), but can run on devices from several different manufacturers, under the control of the party responsible for the applet (e.g. a bank or a payment system, a health authority, etc.). New applications can be created and integrated into existing systems having readers from different manufacturers installed. The readers need not be replaced as the applet may be run on any device.

Following figure shows a basic comparison between the FINREAD and a proprietary class 3/4 architecture. The grey boxes on the left side indicate the "application" parts of the system, that can be developed totally independent of the "infrastructure". In class 3/4 the application code always depends on the used hardware platform within the reader and is not interoperable between different manufacturers.



This concept of interoperability offers the following advantages:

- the cost of development and maintenance of applets is reduced, since a given applet may be executed on any FINREAD compliant device
- the issuance of multi-application smart cards to be executed on FINREAD compliant devices enables several third party providers to share the same reader and so reduce the cost of the equipment needed.
- the FINREAD specifications foresee the ability for the reader to evolve with the future.

5 The CardMan Trust FINREAD device

5.1 General

CardMan® Trust FINREAD is an ISO 7816 and EMV 3.1.1 compliant smart card reader designed to meet the FINREAD specifications.

The internal memory may host different software modules: a permanent core software (Virtual Machine) and one or several Finlets, each dedicated to a given type of smart card application.

CardMan® Trust FINREAD can also be operated in a non-secure transparent mode where it can be used with any type of smart card that does not have an associated FINREAD applet.

FINREAD

Designed for Microsoft® Windows® XP Windows® 2000

EMVCo

5.2 technical details

Smart Card Interface	Smart Card Interface compliant with ISO 7816 and EMV 3.1.1 Support of T=0, T=1 protocols Transmission speed with Smart Card up to 115 KBaud 60 mA max to power the Smart Card Smart Card movement detection with auto power-off Automatic detection of Smart Card type Short circuit and thermal protection
Host Interface	RS 232 (serial COM port) Power Supply from PS/2 keyboard interface Cable length 180 cm USB in preparation
User Interface	Pinpad with 16 keys (4x4) Display 4x20 characters (optional 2x16)
Internal Hardware	32 bit processor with ARM7 core 1 MB flash min. (up to 2 MB, depending on configuration) 256 KB RAM min. (up to 1 MB, depending on configuration)
Cryptographic Functions	Digital signature calculation and verification using RSA Encryption and decryption operations using DES or 3-DES in modes ECB and CBC Hash calculation and verification using SHA-1 (160 bit), MD5 (128 bit), RIPEMD – 160
Compliance	FINREAD 2.0 WHQL (Microsoft) certified EMV 3.1.1 (Europay, Mastercard, Visa) certified ISO 7816
Other Features	SAM (for secret key and RSA operations); Optional without SAM
PC/SC Driver support	Windows 2000 Windows XP others on request
Development Environment	CardMan® Trust FINREAD smart card reader FINREAD COM API JBuilder Plug-In for Finlet Development Administration Tool to • download and manage applications • update firmware • set device features • display device status
OEM	customer specific logo and colors possible b

5.3 Hardware

Processor

The core of the device is an 32 bit ARM 7 microprocessor. A CardMan 3e10 chipset from OMNIKEY is used as the smart card interface.

Memory

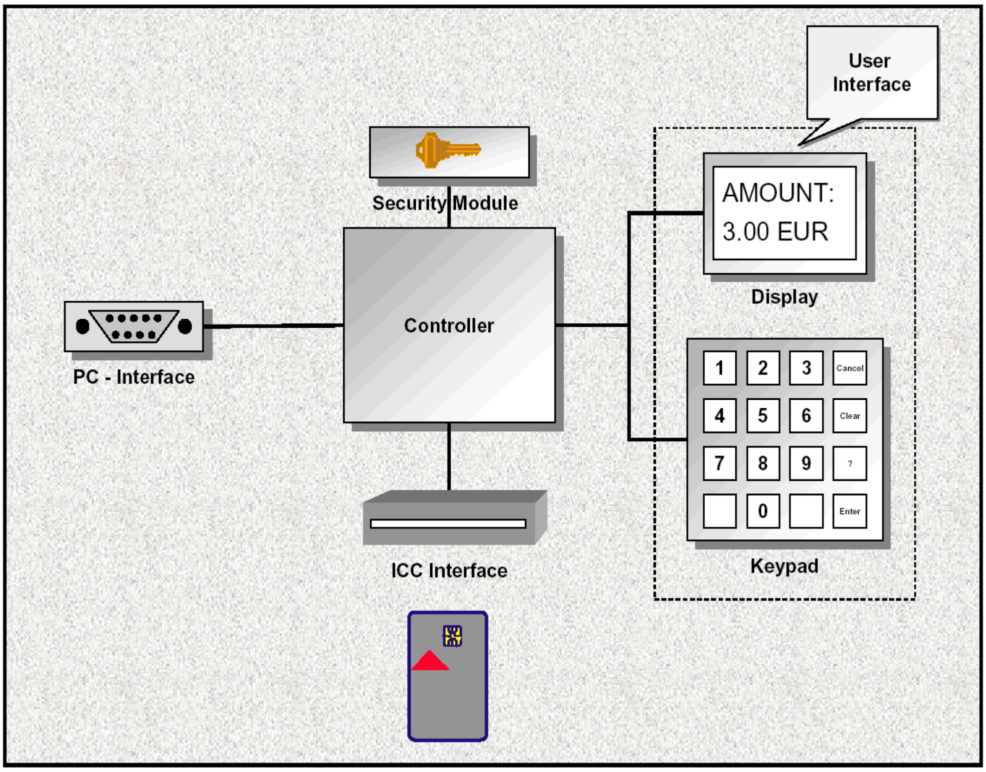
The device is equipped with 1 MB flash for firmware, VM and Finlet storage. This flash memory can be extended up to 2 MB. The used RAM size is 256 KB minimum, extendable up to 1 MB (depending on configuration).

User Interface

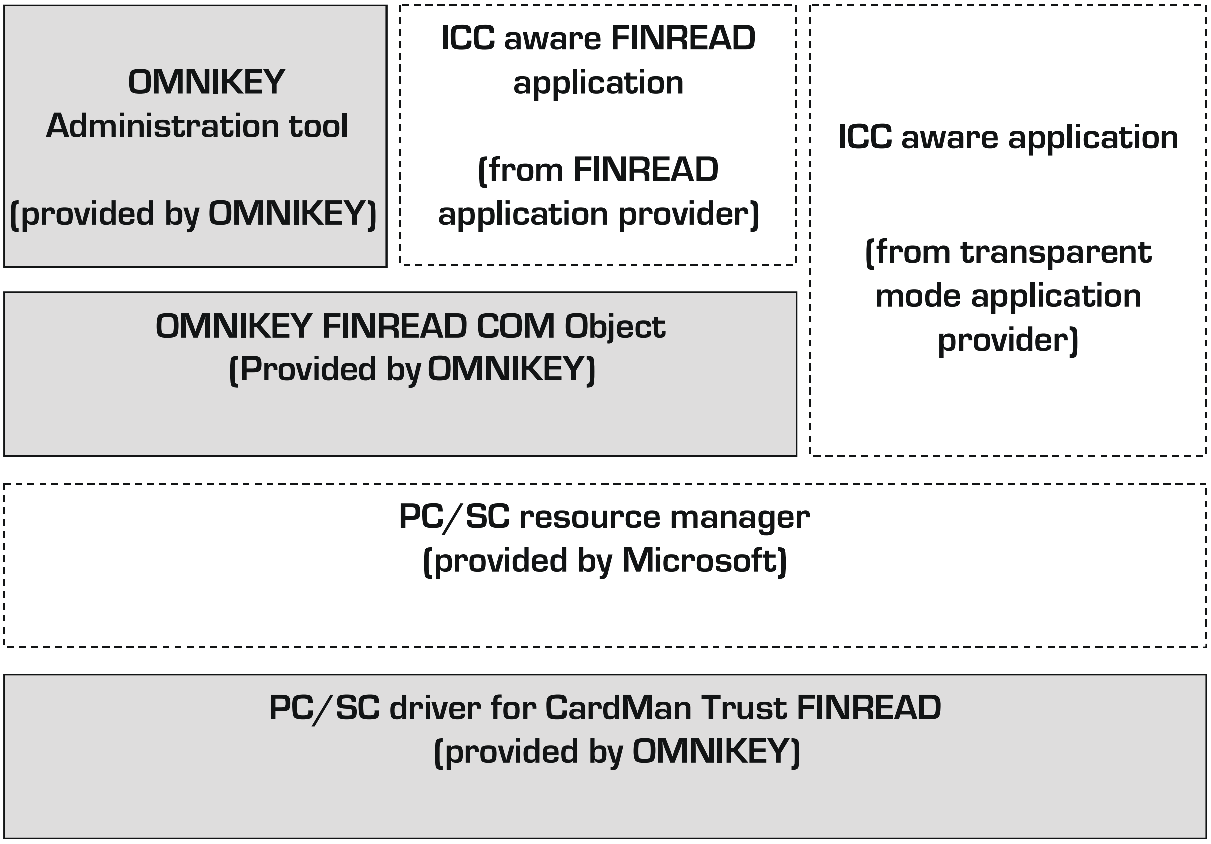
The reader has a keypad with 16 keys and a display with 4x20 characters (optional 2x16).

Security Module

CardMan Trust FINREAD uses an integrated ID-000 smart card as a SAM to guarantee a tamper-proof security solution. This SAM is used for storing the reader's private key as well as for performing RSA operations.



5.4 Software


OMNIKEY
Administration tool
(provided by OMNIKEY)
ICC aware FINREAD application
(from FINREAD application provider)
ICC aware application
(from transparent mode application provider)
OMNIKEY FINREAD COM Object
(Provided by OMNIKEY)
PC/SC resource manager
(provided by Microsoft)
PC/SC driver for CardMan Trust FINREAD
(provided by OMNIKEY)

The grey objects are supplied by OMNIKEY:

PC/SC driver

- for Windows 2000 and Windows XP

COM Object

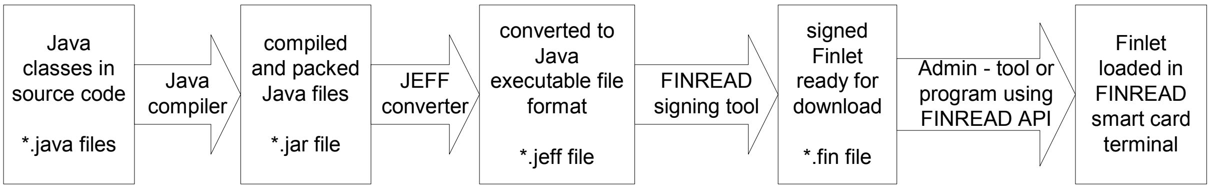
- an API to make the reader's FINREAD functions accessable from the PC

Administration tool

- download applications
- update keys
- manage applications
- set device features
- display device status

6 How to develop a Finlet?

The development of a Finlet is done in several steps:


Java classes in source code
*.java files
Java compiler
compiled and packed Java files
*.jar file
JEFF converter
converted to Java executable file format
*.jeff file
FINREAD signing tool
signed Finlet ready for download
*.fin file
Admin - tool or program using FINREAD API
Finlet loaded in FINREAD smart card terminal

OMNIKEY supplies a SDK for its FINREAD device containing:

The reader

A CardMan Trust FINREAD is delivered with the SDK.

Specifications

This folder contains the STIP (www.stip.org) and FINREAD (www.finread.com) specifications.

ComAPI Setup

The FINREAD COM Object for OMNIKEY FINREAD devices, with an interface as described in part 8 of the FINREAD CWA (CEN-Workshop Agreement)

Driver

The PC/SC device driver for OMNIKEY CardMan Trust FINREAD.

Firmware

The OMNIKEY CardMan FINREAD Trust standard firmware and the firmware with development mode. These firmware versions can be downloaded with the Administration tool.

JEFF converter

This program is provided by the J Consortium and converts class files to JEFF (Java executable file format) files.

BuildPackage

This tool builds a downloadable development package from a JEFF file. This package is not signed according the FINREAD standard and is only downloadable and executable in OMNIKEY FINREAD devices with development mode.

Sample Source Code

Collection of files containing the necessary SDK files, like header and library files, as well as a host and a terminal sample source code.

7 OMNIKEY contact information

For further information please contact:

OMNIKEY AG
Kreuzberger Ring 7
D – 65205 Wiesbaden
Germany

E-Mail: info@omnikey.com
or visit our homepage www.omnikey.com

8 Disclaimer

Information furnished is believed to be accurate and reliable. However, OMNIKEY assumes no responsibility for the consequences of use of such information nor for any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of OMNIKEY. Specifications mentioned in this publication are subject to change without notice. This publication supersedes and replaces all information previously supplied. OMNIKEY products are not authorized for use as critical components in life support devices or systems without the express written approval of OMNIKEY.