FINEID phase 2

Guidelines for Developing Applications using FINEID card

Document version 1.1

30.6.2003

Population Register Centre (VRK)
Certification Authority Services
P.O. Box 70
FIN-00581 Helsinki
Finland
http://www.fineid.fi

Document history

Version	Date	Description	Editor
1.1	30.6.2003	Second edition	AP
1.0	1.10.2002	First edition	MaSi

Contents

1 Overview

The purpose of this document is to offer guidelines for developers who are writing applications using FINEID cards (later referred as FINEID enabled applications).

The FINEID (Finnish Electronic ID) card applies a combination of smart card and Public Key Infrastructure (PKI) technologies. It provides following security services for the electronic community:

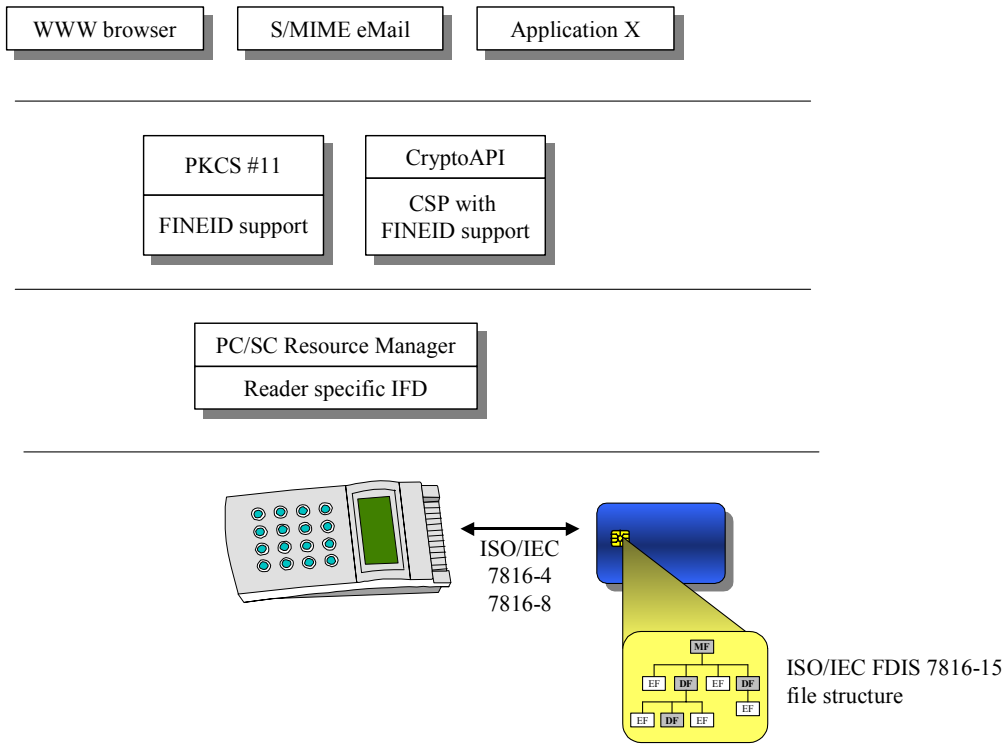
- Strong authentication of communicating entities (used in secure network layer protocols like SSL, SSH and IPSec)
- Encryption key decipherment service for handling of confidential documents (used applications like secure email (S/MIME))
- Non-repudiable electronic signatures (PKCS#7)

Following international standards and open specifications are related to FINEID card:

- Free FINEID specifications are available from http://www.fineid.fi
- ISO/IEC FDIS 7816-15 (draft): standardizing the EID application content (private keys, certificates, PINs) stored into the FINEID card
- ISO/IEC 7816-4, ISO/IEC 7816-8: standardizing smart card commands
- RFC 2459 and RFC 3280: IETF's profile for X.509 certificates and certificate revocation lists

2 Application software architecture

Below is presented an example of a FINEID enabled application architecture:



Open and well-defined upper level APIs (Application Programming Interface) should be used to implement FINEID card support into applications. Such interfaces are PKCS#11 and Microsoft CryptoAPI.

The benefit of that is that the upper level APIs hide lower level technical details of the FINEID card usage like:

- smart card reader interface (typically PC/SC is used),
- smart card command interface,
- data content of the EID application stored into FINEID card.

So, if there comes modifications/upgrades to any of these, then it is not necessary to recode the application, just to upgrade the instance of the upper level API. Remarkable savings in application maintenance can be achieved in comparison to direct access to the card from the application code.

PKCS#11 and CryptoAPI don't offer interfaces to directory (X.500) services (like CRLs (Certificate Revocation List)).

It should be noticed that it is PKCS#11/CryptoAPI vendor specific, how the FINEID card objects (RSA keys, Certificates…) are mapped into the corresponding API objects.

2.1 PKCS #11

PKCS (Public-Key Cryptography Standards) are a set of de-facto standards for public-key cryptography, developed by RSA Laboratories in co-operation with an informal consortium.

PKCS #11 defines a technology-independent programming interface, called Cryptoki, for cryptographic devices such as smart cards. Unlike CryptoAPI, PKCS#11 is not tied into any operating system (also implementations supporting Linux and other operating systems exist).

For example, Netscape and Mozilla based applications (like browser, email…) use PKCS #11 interface for cryptographic devices.

For further information, see http://www.rsasecurity.com/rsalabs/pkcs.

2.2 CryptoAPI

CryptoAPI is Cryptographic Application Programming Interface developed by Microsoft. As PKCS#11, it offers higher-level interface for cryptographic functionalities, but it is tied to Microsoft operating systems.

For example, Microsoft applications (like browser. email) use CryptoAPI interface for cryptographic functionalities.

Also a Microsoft ActiveX control, called CAPICOM, is available from Microsoft. CAPICOM offers COM interface to CryptoAPI.

For further information, see http://www.microsoft.com

3 Security issues

Below are listed security issues to be noticed, when developing FINEID enabled applications:

- When security related data (like PINs) are processed in the application, such data should be wiped from application/workstation memory after it is not needed any more.

4 FINEID specifications

FINEID specifications cover all technical details to implement FINEID compatible software products and (internet) services.

Specifications related to smart cards:

- FINEID S1 - Electronic ID Application, v2.0A
- FINEID S4-1 - FINEID Implementation profile 1 for Finnish Electronic ID Card, v2.0
- FINEID S4-2 - FINEID Implementation profile 2 for Organizational Usage, v2.0

Specifications related to applications and internet services:

- FINEID S2 - VRK (PRC) CA-model and certificate contents, v2.0
- FINEID S5 - Directory Specification, v2.0