Aftek Security Expertise

Aftek Limited

Aftek's key areas for security solutions

- Secure provisioning of third party applications on various embedded devices
- Smartcard / token based systems
- Secure mass storage devices
- PKI enabling of enterprise applications
- Securing mobile handsets and mobile applications
- DRM systems
- Security features provided in hardware for making hardware devices tamper-proof

Applications Security

- PKIX, CMP, OCSP, PKCS #1,
- PKCS #5, PKCS #7 CMS,
- PKCS #11 Cryptoki,
- PKCS #12 PFX, S/MIME

Implementations

- Desktop and web based security,
- Mobile and handheld devices,
- Mass storage devices, Smartcards

Cryptographic Provider

- Desktop, smartcard, Java Card, HSM based key management

Digital Signatures

- MD5, SHA-1,
- RSA signing & verification (RSA private key encryption / decryption)

Confidentiality

- RC2, RC4, 3DES, AES, RSA encryption

Integration with

- MS CAPI, Netscape security services, Entrust SDK, Crypto ++, JCE, JCA, nCipher

Overview

In the world of electronic transactions, exchange of documents and communication, security is a crucial factor. Primary security functions include Authentication, Access control, Privacy, Data integrity and Non-repudiation. Efficient and cost-effective security solutions play an important role in securing various interactions between humans, computers and embedded devices.

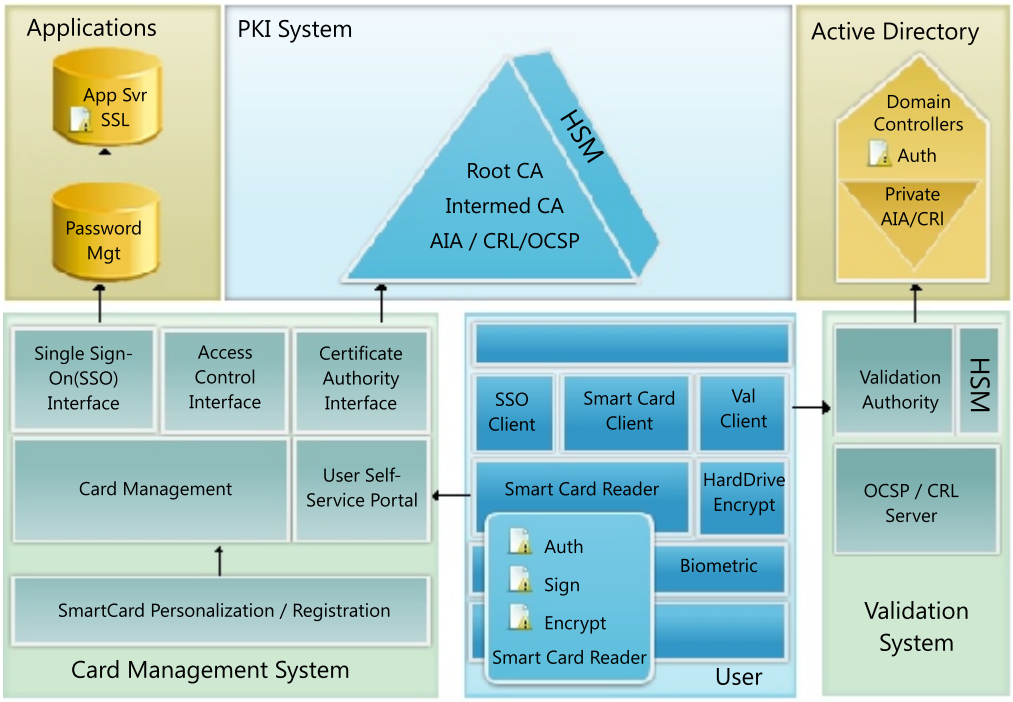
Aftek Expertise

Aftek has been involved in development and delivery of varied solutions involving Cryptography and PKI, from securing embedded devices, communication protocols, mobile transactions to more complex enterprise and system-level solutions for authentication, non-repudiation and confidentiality.

Most of the times the enterprise security framework needs to integrate with existing IT environment containing hardware, software systems, system administrators and users. Aftek anticipates the challenges involved in security deployments on enterprise systems, mobile / handheld devices as well as new generation NFC enabled devices and provides efficient, cost-effective and robust security solutions.

In addition to these soft security mechanisms, Aftek also provides special mechanisms for making hardware devices tamper-proof.

Component diagram showing various aspects where Aftek has provided solutions:



Digital Certificates

- Certificate and RSA key pair generation,
- Certificate trust verification and validation using CRL, OCSP

Frameworks

- Microsoft Active Directory integration,X.509

Authentication

- EAP, PEAP, LEAP, MS-CHAP

Syntax Notations

- ASN.1, XML parsing, encoding and decoding support

BSP

- Creating trusted environment for execution of authorized

Operating Systems

- Windows desktop OS,Windows CE, Linux variants, eCOS®

Hardware

- Tamper-proof embedded devices with piezo-electric sensor, mechanical switches, signal mesh

Security Provisions for Tamper-Proof Hardware

Touch-screen devices, table-top and handheld devices in public places like restaurants, bus terminals which provide consumer functionality for purchase, online transactions etc. are prone to misuse and tampering. Aftek provides special mechanisms for making tamper-proof hardware devices. Client applications store highly sensitive or private data like identification data, encryption keys, which is required for card based transactions. Hence this sensitive data needs to be ultra secured.

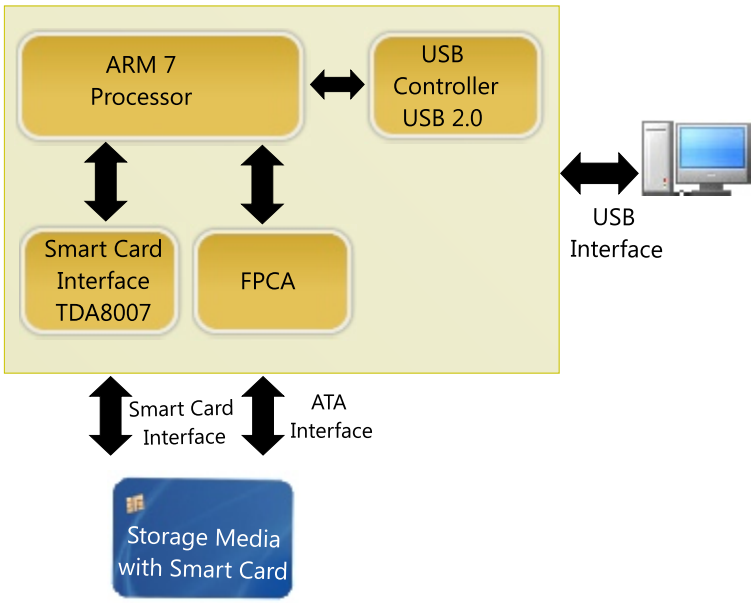
Key Hardware Security Mechanisms

- **Mechanical switch** informs the processor about status of the enclosure open or close /intact.
- **Piezo-electric sensor** gives predefined pulses to inform the processor about any tampering.
- **Signal mesh** designed in PCB layout to protect the PCB from tampering using drilling of enclosure. If the signal is broken, it informs processor about enclosure tampering.
- **Mesh cover over circuits** protects touch-screen signals from tampering, which can't be opened by anyone other than a support person.

Case Studies

Secure Mass Storage Device Reader

The high speed reader device based on eCos platform handles secure communication and data transfer with mass storage device / smartcard based on Java Card technology.
Aftek developed the Java Card application to securely transfer data from card to the host system at high-speeds.



About Aftek

Aftek Limited is a full spectrum technology services company from India. Over last 20 years Aftek has gained significant exposure to variety of technologies. Rich technological capabilities, focused investments in Research & Development and industry exposure enables us to reach beyond the basic IT services to design and deliver projects, products and implement end-to-end solutions to customers in variety of industries. Our service spectrum covers key services as Hardware Development, Firmware Development, Embedded Systems, Application Development, Application Maintenance, and Testing Services.

Aftek developed mass storage reader device which implements a very efficient security engine. This engine has the ability to mutually authenticate the card, card-owner and the reader system with each other. The security engine provides maximum level of security for the card based data transfers with the host.

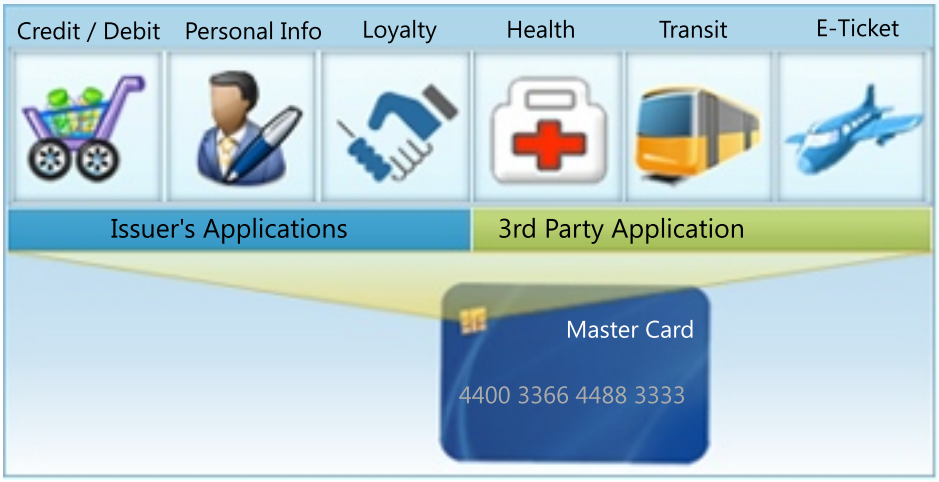
Key security features were:

- Ability to authenticate an individual user (up to 2048 bit PKI)
- 128 / 192 / 256 bits on-board AES encryption of data

Aftek developed the strong security mechanism on the reader device with quick response time and a very minimal footprint.

MULTOS Device Management System

Device management system is based on MULTOS smartcard technology. MULTOS devices are secure embedded devices for online banking transactions, transportation systems, campus / university identification etc. The device is an USB secure device capable of executing applications running on its native OS execution environment.



Key Functionalities Developed by Aftek in this Solution:

- Secure authentication of the device
- Providing secure way of communication between host PC and device
- Packaging the applications and transmitting those packages to the device in a secure way.
- Authentication of the packages
- Disabling the devices when they are stolen or lost
- PKI based authentication, signing and encryption operations
- Entity based mutual authentication protocols

Aftek developed the complete security framework including authentication, end-to-end secure services which act as a backbone to all the transactions done using the MULTOS devices.

Aftek Limited

Visit us at: www.aftek.com
Email: servicesinfo@aftek.com