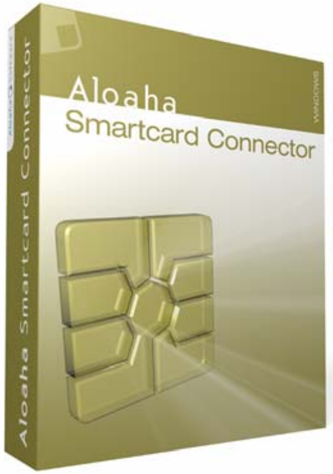
Aloaha Software



Aloaha
Smart Card Connector

Native, plug & play security
enhancement to Microsoft Windows
Operation Systems and Applications

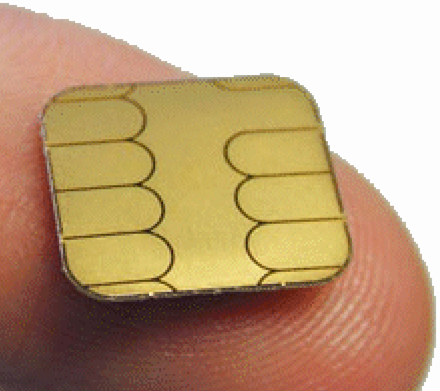
Aloaha Software

Presentation Outline

- What are Smart Cards?
- The Advantages
- Encryption Technologies
- Usage
- What is the Aloaha Smart Card Connector?
- Why Aloaha?
- Supported Cards
- Corporate Overview

What are Smart Cards?

- Microprocessor cards, or smart cards, contain an entire computer with a processor, RAM, ROM, EEPROM and operating system.
- The embedded microcontroller transforms a credit card-sized piece of plastic into a portable, tamperresistant computer with a calculating power of the original IBM PC.
- Cards have a higher processing power than the mainframe computer which brought Apollo to the moon.



The Advantages

- Flexibility
- Secure – unlike magnetic cards smart cards cannot be duplicated
- Secret Key cannot leave the card.
- They provide tamper-proof storage of user and account identity.
- Smart cards can have information written to them in real time.
- Chip Operating Systems support multiple applications on one card

Encryption Technologies

- Smart Cards use public/private key encryption.
- The Private Key on the card can only be accessed by the micro processor for a cryptographic operation.
- The Public Key is known to everyone (PKI).
- Data which has been encrypted with either the Private Key or the Public Key can only be decrypted with the other key.

Usage

- **Digital Signature**

  The card processor encrypts the digest of a document with the private key saved on the card. The recipient decrypts the hash and compares it with a self calculated hash. If they match this means that the data has not been modified.

- **Authentication**

  The card encrypts a secret exchanged by two parties with the private key of the card. The other party decrypts that data with the public key and confirms the identity.

- **Decryption**

  The card decrypts the public key encrypted secret of a confidential document with its private key.

Aloaha Smart Card Connector

- Responsible for the communication between PC/Software and Smart Card.
- Could be called Smart Card Device Driver.
- Offers Applications access via MS Cryptographic Service Provider, PKCS #11 Interface or Aloaha native APIs.
- For example signing of emails, invoices, PDF or Office documents.
- Decryption of PDF documents or NTFS files.
- Authentication via SSL/HTTPS.

Technical Details

Hash Algorithm

- SHA1 & SHA2
- MD4 & MD5 on request (not considered as save anymore)

Interfaces

- Microsoft Cryptographic API (CSP)
  (Aloaha CSP is Microsoft approved)
- PKCS #11
- Aloaha native Interface

Encryption Algorithm

- RC2/RC4
- DES & Triple DES
- RSA

Why Aloaha?

- Microsoft approved and signed.
- Automation support with secure PIN caching. Called also comfort signature or batch signature.
- Access to card via MS Crypto API, PKCS #11 and automation compatible API.
- Supports a broad range of different cards.
- Only one Card Driver has to be rolled out company wide.
- Zero Administration.
- SHA2 and 2048 Bit support.
- Supports secure PIN Pad via PC/SC.
- Card PINs cannot be logged by keyloggers since they never leave the card reader itself.
- Adobe 6/7/8 and NTFS encryption supported.

Some supported cards

Corporate Overview

- Wrocklage GmbH founded in 1991.
- Wrocklage Intermedia GmbH founded in 1998. (www.wrocklage.de)
- Aloaha Software founded in 2003. (www.aloaha.com)
- Offices in Germany and Malta.
- A channel focused company with partners throughout the world.

- **Aloaha Software is worldwide used:**

by siav, ILOXX AG, LBS Nord AG, ABN Amro,

OB 10, ECS, PriceWaterhouseCoopers, Ingram Micro, Pitney Bowes, LG Electronics, German Federal Chamber of Physicians, Chamber of Physicians North Rhine, Captaris, Nordwest Lotto und Toto, WesternUnion, Woodforest National Bank, Accenture, various local councils, Banks, integrated in software for lawyers, health professionals, document management systems, call center applications …