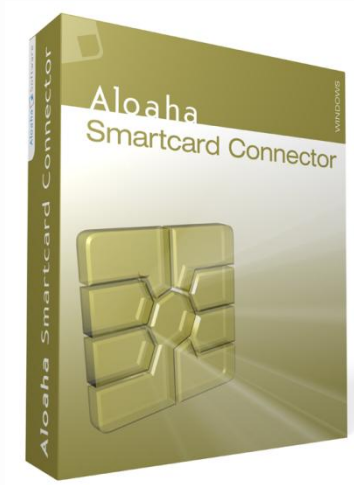
Aloaha Software



Aloaha
Smart Card Connector

plug & play Zugriff auf Smartkarten
von Windows Betriebssystemen und
Anwendungen

Aloaha Software

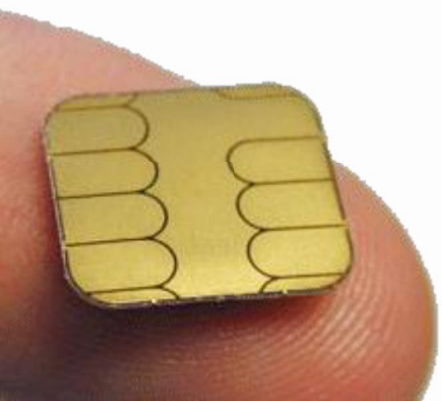
Präsentationsübersicht

- Was sind Smartkarten/Chipkarten?
- Die Vorteile
- Verschlüsselungstechnologie
- Anwendung
- Was ist der Aloaha Smart Card Connector?
- Warum Aloaha?
- Unterstützte Smartkarten
- Firmenübersicht

Aloaha Software

Was sind Smartkarten/Chipkarten?

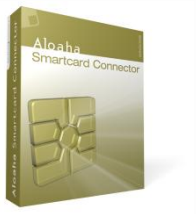
- Mikroprozessorkarten oder Smartcards beinhalten einen Minicomputer mit Prozessor, RAM, ROM, EEPROM und ein Betriebssystem
- Der integrierte Mikroprozessor verwandelt die kreditkartengroße Plastikkarte in einen kleinen, transportierbaren und manipulationssicheren Computer mit der Rechenleistung der ersten IBM-PCs
- heutige Karten haben mehr Rechenleistung als die früheren Supercomputer, die z.B. die Apollo-Raumfähren zum Mond gebracht haben



Aloaha Software

Die Vorteile

- Flexibel
- Sicher – im Gegensatz zu Scheckkarten können diese Karten nicht dupliziert werden
- Der private Schlüssel kann nicht ausspioniert werden
- Benutzerdaten sind manipulationssicher auf der Karte untergebracht.
- Smartcards können in Echtzeit mit Informationen beschrieben werden
- Die Kartenbetriebssysteme unterstützen mehrere Anwendungen auf einem Chip



Aloaha Software

Verschlüsselungstechnologie

- Smartkarten benutzen die public/private key Verschlüsselung
- Der private Schlüssel kann nur von dem integrierten Mikroprozessor benutzt werden
- Der Öffentliche Schlüssel wird veröffentlicht
- Daten, die mit dem privaten oder öffentlichen Schlüssel verschlüsselt werden, können nur mit dem jeweils anderen Schlüssel entschlüsselt werden

Aloaha Software

Anwendung

- **Elektronische Signatur**

  Der Prozessor auf der Chipkarte verschlüsselt einen Auszug eines Dokumentes mit dem Privaten Schlüssel der Karte. Ein Empfänger entschlüsselt den Hash und vergleicht diesen mit einem selbst errechneten Schnipsel des Dokumentes. Wenn beide Teile identisch sind, ist das Dokument mit Sicherheit nicht manipuliert.

- **Authentifizierung**

  Die Chipkarte verschlüsselt ein Passwort, welches beide Seiten kennen, mit dem Privaten Schlüssel der Karte. Das verschlüsselte Passwort wird versandt und der Empfänger entschlüsselt mit dem Öffentlichen Schlüssel des Zertifikates und kann so die Identität beweisen.

- **Entschlüsselung**

  Die Chipkarte entschlüsselt den mit einem Öffentlichen Schlüssel verschlüsselten Code eines vertraulichen Dokumentes mit dem Privaten Schlüssel.

Aloaha Software

Aloaha Smart Card Connector

- Schnittstelle zwischen Chipkartenprozessor und PC-Betriebssystem bzw. der PC-Anwendungen
- Könnte man Smart Card-Treiber nennen
- Stellt Anwendungen via MS Cryptographic Service Provider, PKCS #11 Interface oder Aloaha native APIs Verbindung zur Chipkarte her
- z.B. Zum elektronischen Unterzeichnen von E-Mails, Rechnungen, PDF-Dateien oder Office-Dokumenten
- Ver/Entschlüsseln von PDF-Dokumenten oder NTFS Dateien
- Authentifizierung/Anmeldung via SSL/HTTPS.

Aloaha Software

Technische Einzelheiten

Hash Algorithmen

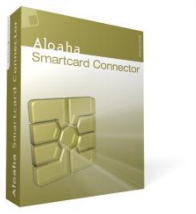
- SHA1 & SHA2
- MD4 & MD5 auf Anfrage (mittlerweile als unsicher eingestuft)

Schnittstellen

- Microsoft Cryptographic API (CSP)
  (Aloaha CSP ist abgenommen von Microsoft)
- PKCS #11
- Aloaha native Interface (von anderen Aloaha Produkten)

Verschlüsselungsalgorithmen

- RC2/RC4
- DES & Triple DES
- RSA



Aloaha Software

Warum Aloaha?

- von Microsoft abgenommen und signiert
- Automatisierung möglich mittels Secure PIN Caching. Das wird auch Batchsignatur, Stapelsignatur oder Komfortsignatur genannt
- Chipkartenzugriff via MS Crypto API, PKCS #11 und automation compatible API
- Unterstützt eine breite Palette von Chipkarten
- Nur ein Treiber muss innerhalb eines Unternehmens ausgerollt werden
- Keine Administration
- SHA2 und 2048 Bit Unterstützung
- Unterstützung der sicheren PIN-Eingabe via PC/SC
- Karten-PINs können nicht von Schnüffelsoftware erspäht werden, da diese die Karte nie verlassen
- Adobe 6/7/8 und NTFS-Verschlüsselung werden unterstützt

Aloaha Software

Eine Auswahl unterstützter Karten

Firmenüberblick

- Wrocklage GmbH gegründet 1991
- Wrocklage Intermedia GmbH gegründet in 2003 (www.wrocklage.de)
- Geschäftsbereich Aloaha Software gegründet 2003 (www.aloaha.com)
- Büros in Deutschland und Malta
- Vertrieb über Reseller in der ganzen Welt

- **Aloaha Software wird weltweit genutzt:**

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

OB 10, ECS, PriceWaterhouseCoopers, Ingram Micro, Pitney Bowes, LG Electronics, Bundesärztekammer, Ärztekammer Nordrhein, Captaris, Nordwest Lotto und Toto, WesternUnion, Woodforest National Bank, Accenture, Städte und Gemeinden, Banken, integriert in Anwaltssoftware, in Dokumenten Management Systeme und Call Center Software …