Thomas Denner
Expert Secure Products
Atmel
Parkring 4
85748 Garching b. München
thomas.denner@atmel.com

Warum bin ich hier?

- Verstehen der Marktanforderungen, Trends...
- Vorstellung Atmel Secure Microcontroller Solutions
- Vermitteln, was sichere Hardware für die Systemsicherheit bedeutet
- Haben wir Lösungen für Ihre Probleme?

Vorstellung Atmel SMS (Secure Microcontroller Solutions)

Atmel

- hat mehr als 20 Jahre Erfahrung in Smartcards und Sicherheitscontrollern
- hat CC EAL5+ Zertifikate für alle aktuellen Bankenprodukte
- hat zertifizierte Kryptographiebibliotheken
- hat ca. 30% Marktanteil bei chipbasierten SDA und DDA Kredit- und Debitkarten (Marktzahlen von IMS)
- hat sichere Microcontroller für Embedded Anwendungen in Industriegehäusen
- hat ca. 50% Marktanteil im Bereich Pay-TV (Marktzahlen von IMS)
- hat moderne Cores: AVR, AVR32, ARM (am schnellsten wachsender Microcontrollerhersteller unter den Top 10!)
- ist Marktführer bei ICs für Chipkartenleser

Was ist Sicherheit?

These:

Es gibt keine 100%-ige Sicherheit!
Mit genug Aufwand (=Geld) kann man alles ‚knacken'.
Aber: Lohnt es sich?

Schlußfolgerungen:

1. **Sicherheit ist ein anderes Wort für „Aufwand für Angreifer"**
2. **Sicherheit ist relativ**

Sicherheit ≠ Kryptographie!
(z.B. Angriffe auf EC-Karte)

Welche Fragen sind zu beantworten?

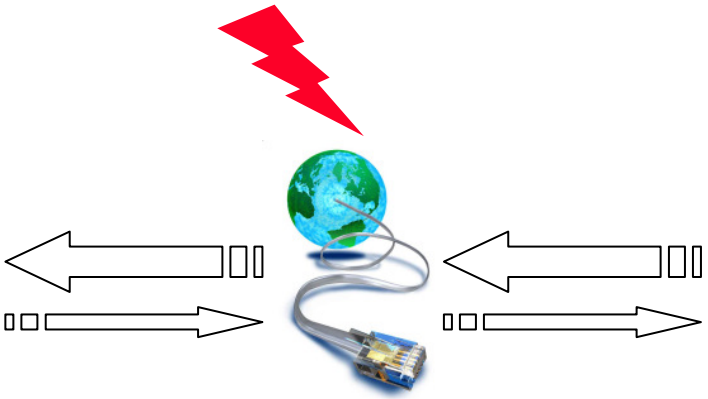
1. Wie hoch ist der Wert, den ich schützen muß?
2. Wie sehen mögliche Angriffe aus?
3. Gibt es einen Rückkanal?
4. Wo finden Angriffe statt (Öffentlichkeit, Privat)?
5. Welche Kryptoalgorithmen werden benötigt?
6. Welche Schlüssellängen sind gefordert?
   (BSI, PTB)
7. Welche Rechenleistung wird dafür benötigt?
8. Wieviel sicherer Speicherplatz wird benötigt?

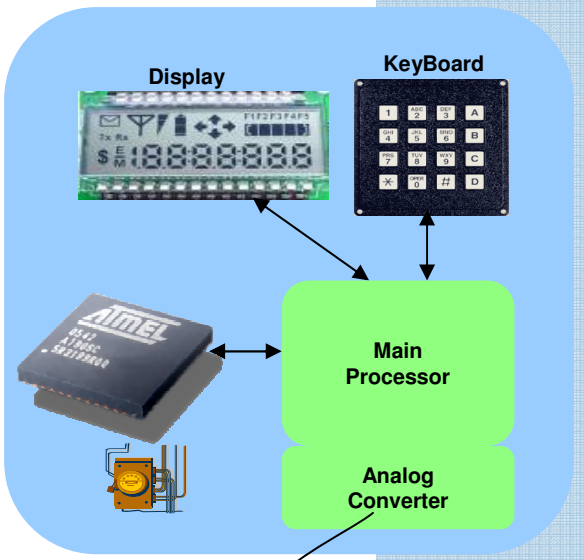
...

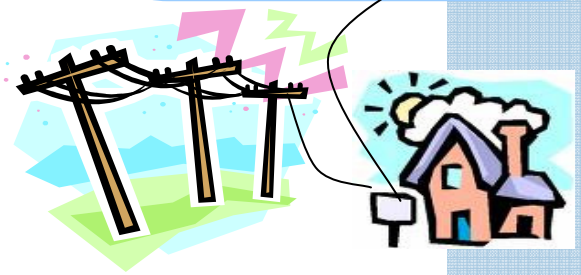
Sichere Authentisierung oder sicheres System?

Authentisierung	Sicheres System
Kombination aus Standard Microcontroller und Sicherheitschip	Sicherer Microcontroller
Geheimnisse (Schlüssel, Daten, Passwörter) sicher gespeichert im Sicherheitschip	Firmware und Daten sind gesichert
Systemfunktionalität angreifbar, veränderbar	Sytemfunktionalität gesichert
System nicht zertifizierbar	Zertifizierung des Gesamtsystems möglich
Geringer Aufwand, um Kryptographie und sichere Datenablage zu ermöglichen durch fertige Firmware im Sicherheitschip	Sehr hoher Softwareaufwand
Hardwaresicherheit nur für Daten/Schlüssel im Sicherheitschip	Hardwaresicherheit für gesamtes Sytem

Sichere Authentisierung







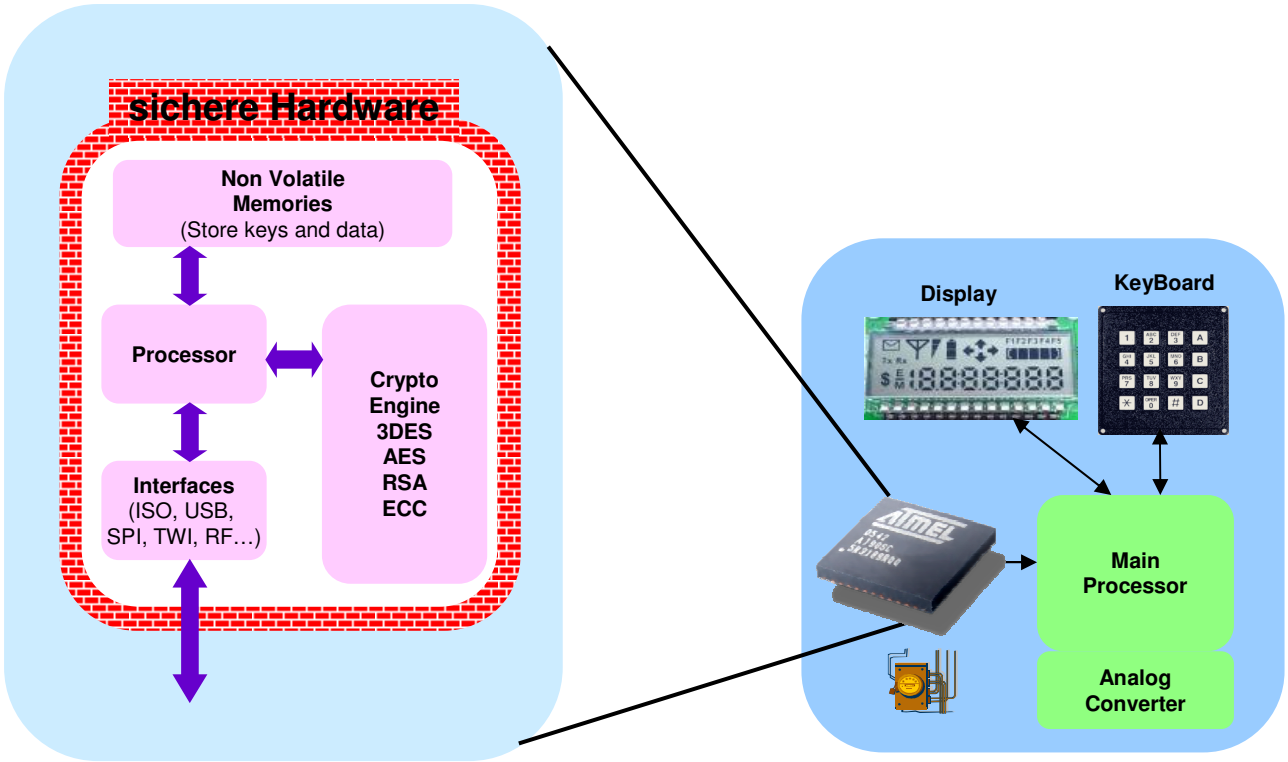
Rechenzentrum (Back-end)
(entschlüsseln und Signaturverifikation)

Datenübertragung über
öffentliches Netz

Zähler
(sammeln, verschlüsseln
und/oder signieren von Daten)

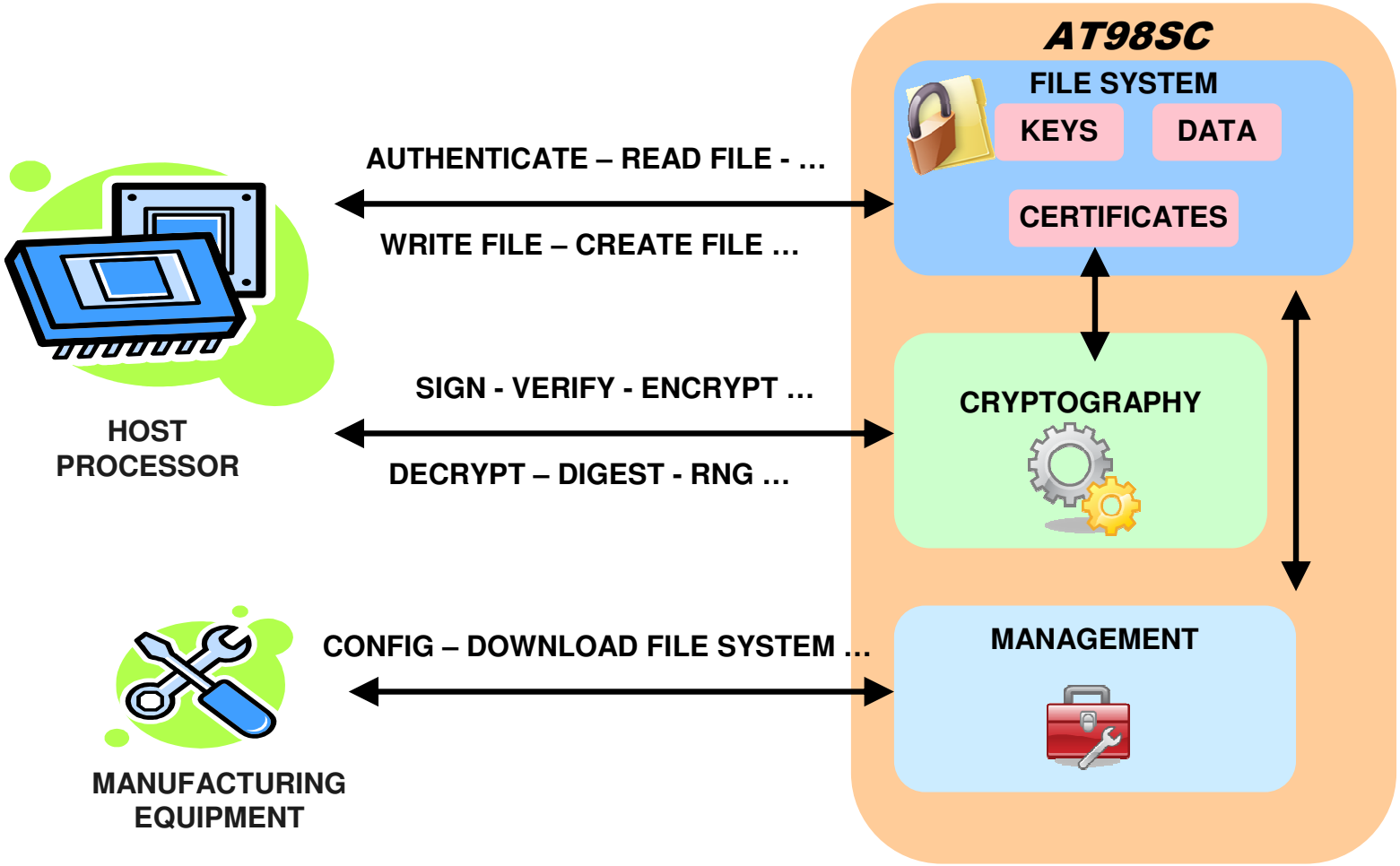
- **Datenauthentizität gesichert durch Asymmetrische Kryptographie (Host und Client authentisieren sich gegenseitig)**
- **Datenintegrität? Wie sind die Messdaten im Hauptcontroller gesichert?**

Sicherheitscontroller AT98SC



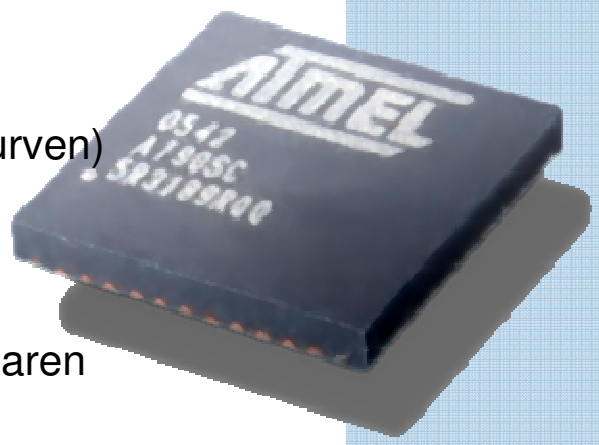
Smartcard Hardware **mit Firmware** im Industriegehäuse

AT98SC auf einen Blick



Was bietet die Firmware?

- Digitale Signaturverfahren (EC-DSA, RSA, DSA, MAC, HMAC)
- Symmetrische Kryptographie (AES, DES/T-DES)
- Asymmetrische Kryptographie (RSA 2048/ 4096, Elliptische Kurven)
- Zufallszahlengenerator
- Sicheres Dateisystem für Schlüssel und Daten mit konfigurierbaren Zugriffsrechten
- RSA und ECC Schlüsselerzeugung auf dem Chip
- Verfügbare Schnittstellen sind SPI, TWI, ISO7816 or USB 2.0-CCID*
- Das **Dateisystem**, sein Inhalt und die **Sicherheitsstrategie** können vollständig vom Anwender **konfiguriert** werden

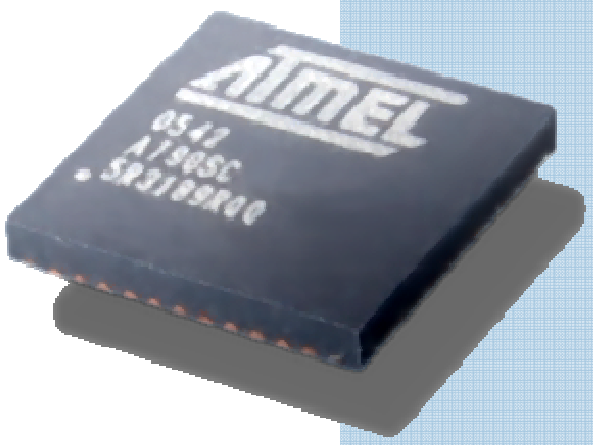


** produktabhängig*

Vorteile / Nachteile

Vorteile:

1. Gehäuse im Industriestandard
2. Kartenleser kann entfallen (Kostensenkung)
3. Keine Kontakte (Korrosion)
4. Kein Entwicklungsaufwand für Kryptographie etc.
5. Entwicklung des Smartcard-OS entfällt (Kostensenkung)
6. Schlüsselerzeugung im Chip möglich
7. Sehr schnell durch Hardwareunterstützung der Kryptographie



Nachteile:

1. Etwas höherer Aufwand für Personalisierung / Initialisierung