

**Anthony Thorn**

AT Systems & Services GmbH

Unabhängiger Berater

Seit 15 Jahren im Sicherheitsbusiness tätig

Seit 9 Jahren selbstständig

Schwergewicht    technisch, konzeptuell  
                          vorallem Finanzindustrie

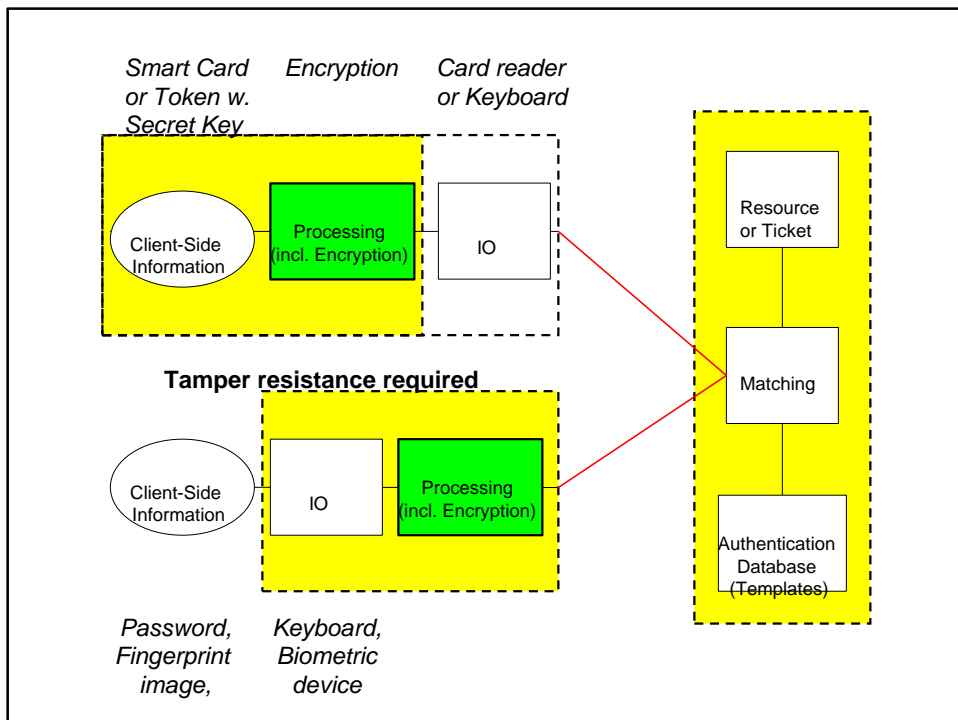
Projekte:

Sicherheits-Politik, Standards, Sicherheits-Dokumentation  
für Finanzdienstleister, sowie einen CA (Zertifizierungsdienstleister)  
Sicherheits Konzepte für CA, Multi-Channel Bank, Internet Banking,  
WAP Broker, ...

Technische Schwerpunkte

PKI, Netzwerk, Client-Server

*Beim Lesen von Artikeln über IT Sicherheit, stelle ich immer wieder fest,  
dass ich das Thema ganz anders angegangen wäre...*



## Evaluation Criteria for Authentication Solutions

### Management: Effort & Culture

- User enrolment
- Reorganisation
- Recovery from compromise of "key"
- Recovery from loss of "key"
- Policy and/or Control: Central /hierarchical / local
- Audit

### Feasibility & Acceptability

- Roaming users
- Cost including Integration with IT environment
- Computing resources required
- Scalability
- Performance (speed)
- User acceptance
- False Positives and False negatives

### Vulnerability

- Disaster or malfunction
- Internal attack
- External attack
- Administrators - segregation of duties
- Vendors

## Vulnerabilities *oldies but goodies !*

- replay attack** (network sniffing or other)
- guessing the user input (or key, or template)
- active attack – e.g. spoofing “oracle-style” authentication
- physical tampering
- copying of password or "key"
- theft / **undiscovered theft** (*hence token*)
- offline** dictionary / exhaustive search attack (cracking)
- manipulation of template database – exchanging fields
- miserable cryptography
  - lack of entropy
  - global keys
- Single Sign On disguises differences in security levels

### **Loss of availability !**

## **Biometrische Verfahren**

*Fingerprint, Iris, Retina (Nethaut), Handprint, Voice, DNA ?*

- + Fast kein Vergessen/Verlust der User Daten
- + Für die Meisten Users recht Bequem
  
- Teuer, nicht nur Hardware auch Enrollment
- Technologie noch in Entwicklung (nicht Reif)
- Zukunfftige Migrationskosten Keine Standards
- Nicht immer schnell
  
- Inhärent FAR / FRR Tradeoff
  - Hersteller Optimismus + Birthday Paradox
  - Kein Begrenzung der Anzahl Logon-Versuche
  
- Einzelne Problem-Users
  - Kein Universalsensor: Finger mit mehr oder weniger Minutiae, Brillen/Linsenträger bei Iris Erkennung usw.
  
- Recoveryproblem bei kompromittierte User-Daten
- Privatsphäre tangiert

**Eher PIN- als Passwort Ersatz**