

# Sichere PCs und Laptops

Sicherheitstools mit der Bürgerkarte



---

A-SIT Zentrum für Sichere Informationstechnologie  
Dipl.-Ing. Martin Centner

SFG, 9. Februar 2006

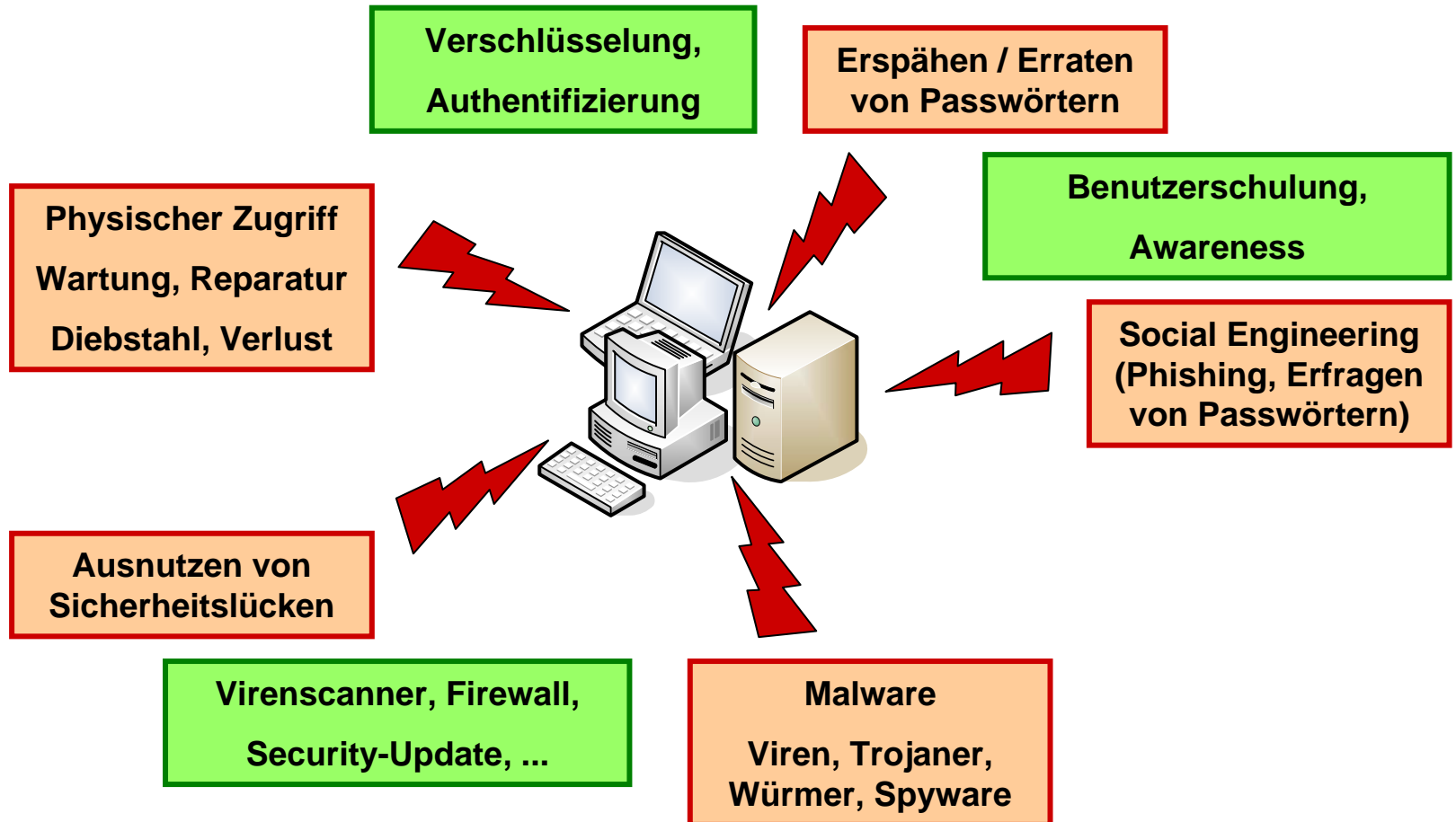
# A-SIT

## Zentrum für Sichere Informationstechnologie – Austria

- Gemeinnütziger Verein, gegründet: 1999
- Mitglieder
  - Bundesministerium für Finanzen (BMF)
  - Österreichische Nationalbank (OeNB)
  - Technische Universität Graz (TU Graz)
- Tätigkeiten
  - Bestätigungsstelle nach §19 Signaturgesetz (SigG)
  - Konzept Bürgerkarte
  - Technologiebeobachtung
  - Zahlungssystemaufsicht
  - E-Government Projekte
  - ...



# Sichere PCs und Laptops



# Sicherheits-Tools mit der Bürgerkarte

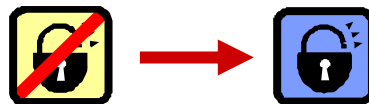
Die Bürgerkarte bietet ...

- elektronischer Ausweis → Identität
- elektronische Signatur → Authentizität
- Ver-/Entschlüsselung → Vertraulichkeit



Tools

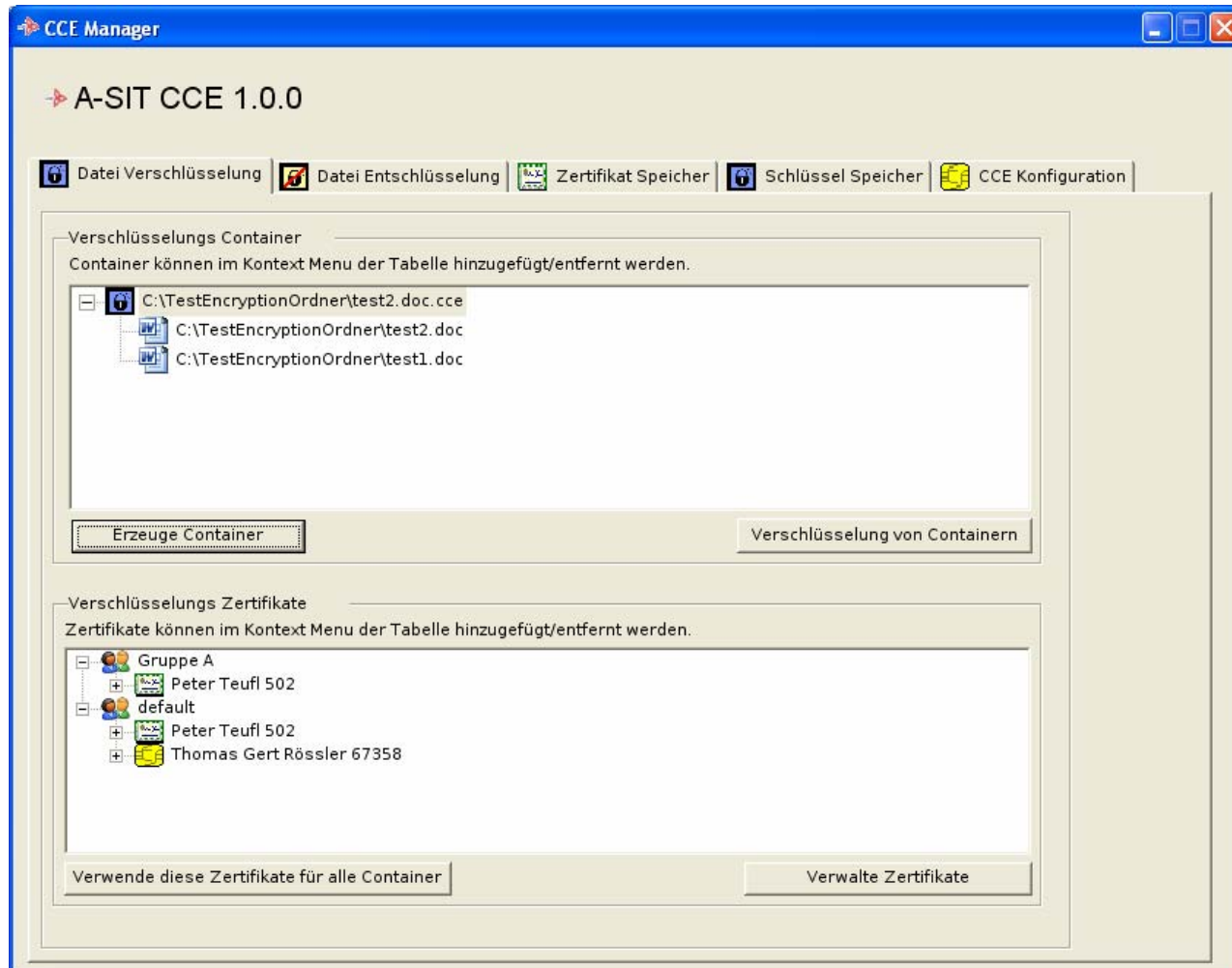
- CCE (Citizen Card Encrypted)
- SecureEFS
- SecurePC



# A-SIT CCE (Citizen Card Encrypted)

- Tool zur Ver-/Entschlüsselung mit der Bürgerkarte
- Erstellt verschlüsselte S/MIME Container
  - kann beliebig viele Dateien enthalten
  - kann mit S/MIME fähigen E-Mailclient geöffnet werden
- Beliebige viele „Empfänger“ pro Container möglich
- Klartext Datei wird nach dem Verschlüsseln *sicher* gelöscht
- Integration ins Kontextmenu des Windows Explorers
- Import von Zertifikaten zur Verschlüsselung
  - LDAP
  - Bürgerkarte
  - Datei

# A-SIT CCE (Citizen Card Encrypted) Demonstration



# EFS (Encrypting File System)

- Microsoft Windows 2000/XP mit NTFS
  - Dateiverschlüsselung (kein *echtes* verschlüsseltes Dateisystem), d.h.
    - Inhalt der Datei wird verschlüsselt
    - Dateinamen, Verzeichnisse bleiben unverschlüsselt
  - Jede Datei wird mit einem eigenen Schlüssel (FEK – File Encryption Key) verschlüsselt
    - DES / 3DES, AES 256 (> WinXP SP1)
  - Der FEK wird mit dem EFS Schlüssel des Benutzers verschlüsselt
    - RSA mit 1024 Bit
  - Der private EFS Schlüssel des Benutzers wird im Windows Crypto Store gespeichert und ist mit dem Passwort des Benutzers verschlüsselt.

# A-SIT SecureEFS

- Der private Schlüssel wird **nicht nur mit dem Passwort** des Benutzers sondern **mit der Bürgerkarte** verschlüsselt
  - Sicherheit hängt nicht vom gewählten Passwort ab
  - Ausspähen des Passworts reicht nicht zum Entschlüsseln
- Private Schlüssel wird mit Bürgerkarte entschlüsselt, dem System zur Verfügung gestellt und anschließend wieder *sicher* gelöscht.
  - Privater Schlüssel liegt nach Systemabsturz nicht unverschlüsselt am System
  - Keine Reste vom privaten Schlüssel auf der Festplatte
- Schlüssel kann für mehrere Personen verschlüsselt werden.
  - Verschlüsselung für Benutzergruppen
  - Vertretungsregelungen möglich



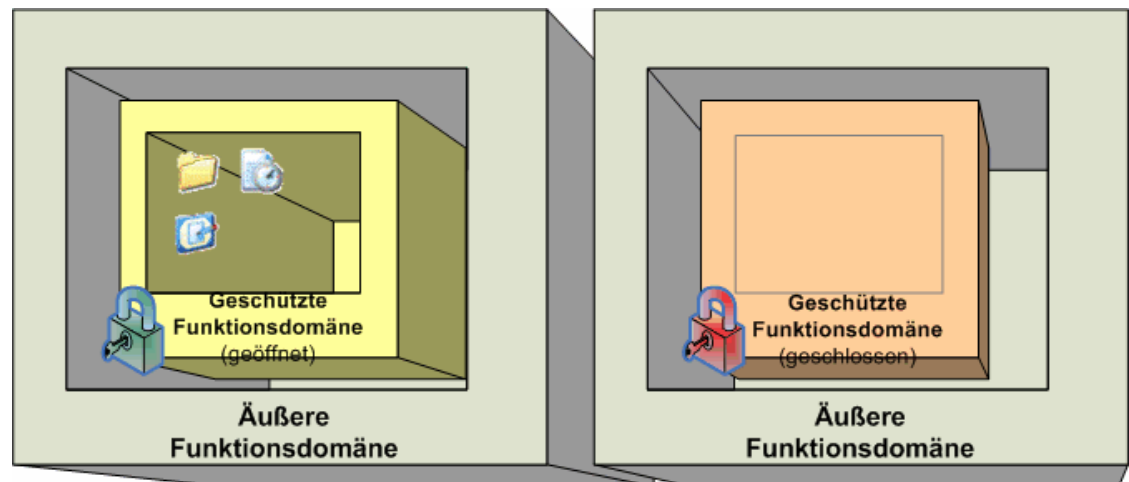
# EFS / A-SIT SecureEFS

## Richtlinien für den sicheren Einsatz

- Immer ganze Verzeichnisse verschlüsseln
  - Programme (z.B. Word) legen beim Bearbeiten von Dateien Kopien an, die sonst unverschlüsselt auf der Festplatte liegen
- Alle Arbeitsverzeichnisse verschlüsseln
  - z.B. auch temporäre Verzeichnisse („Temp“)
- Ruhezustand (Hibernation) / Standby deaktivieren
- Recovery-Agent deaktivieren (erst ab WinXP möglich)
- Backup Schlüssel erzeugen und sicher verwahren
  - z.B. auf USB-Stick / Diskette

# A-SIT SecurePC

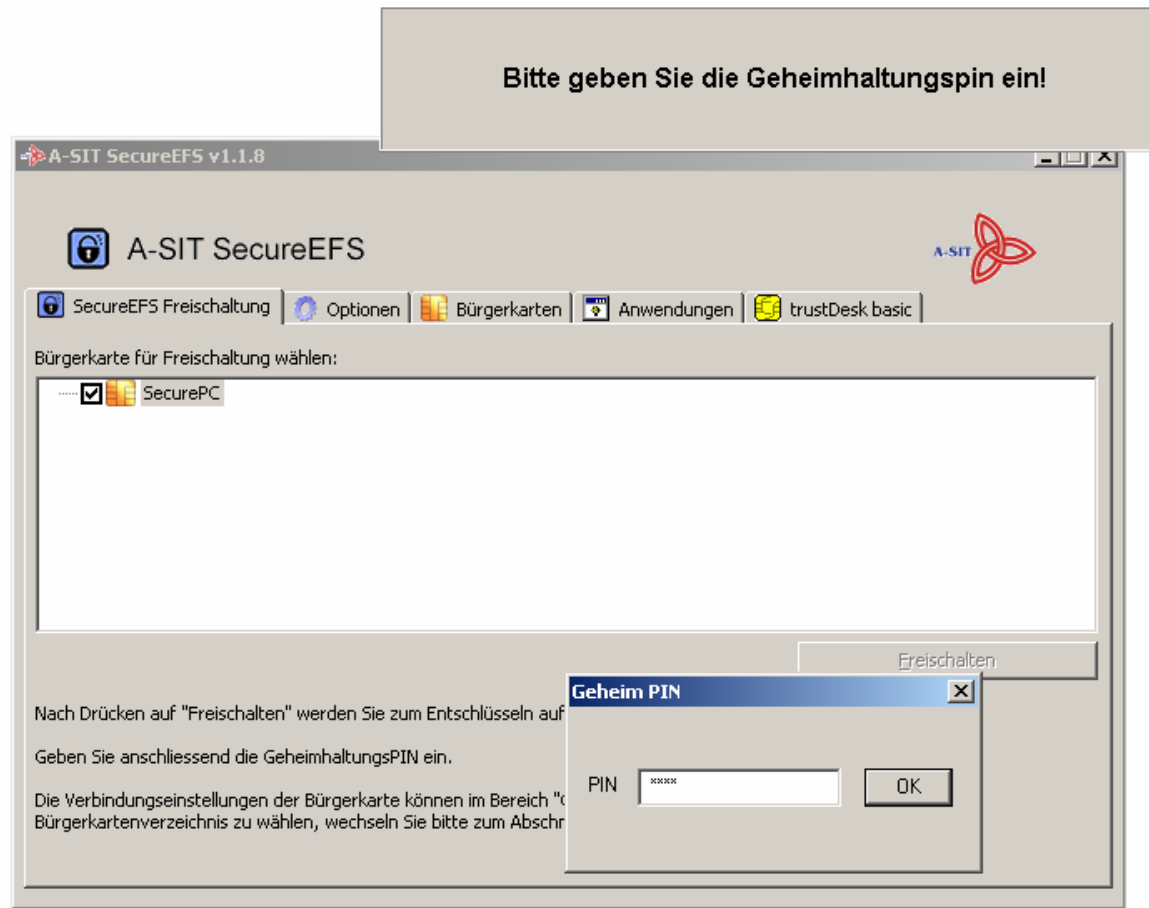
- Segmentierung des Systems in Domänen über Virtuelle Maschinen (VM)
- Äußere Funktionsdomäne stellt nur nicht-sicherheitskritische Funktionen und Daten zur Verfügung
- Geschützte Funktionsdomäne ist in äußere eingebettet und verschlüsselt und kann nur nach starker Authentifizierung mit der Bürgerkate aktiviert werden



# A-SIT SecurePC

- Äußere Funktionsdomäne
  - Firewall und Virenschanner
  - Virtuelle Maschine
  - SecureEFS (zur Verschlüsselung der geschützten Domäne)
  - Bürgerkarten-Umgebung und Tunnel
- Geschützte Funktionsdomäne
  - Firewall und Virenschanner
  - Tunnel
  - geschützte Applikationen und Daten
  - ...

# A-SIT SecurePC Demonstration



[www.a-sit.at](http://www.a-sit.at)

- CCE (Citizen Card Encrypted)
  - SecureEFS
- <https://demo.a-sit.at>

