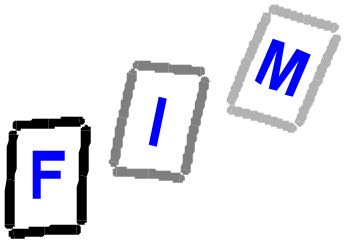


Security Analysis Tool (SAT) 2.0

Heinrich Schmitzberger

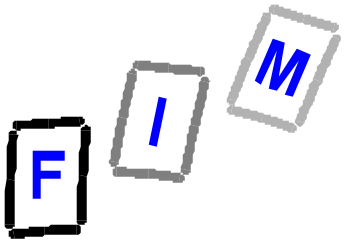
Rudolf Hörmanseder

am 10.12.2002



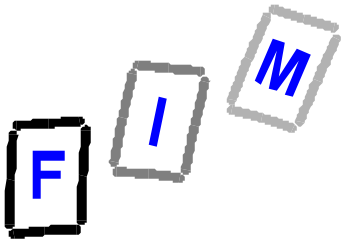
Inhalt

- **Motivation**
- **Geschichte des SAT – Projekts**
- **Architektur**
- **Controller**
- **Projektstatus**
- **Ausblick**



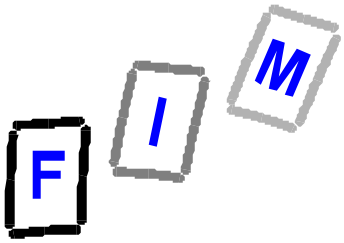
Motivation

- **Sicherheit im Netzwerk gewinnt immer mehr an Bedeutung**
- **Anti-Viren-Programme, Firewalls gegen externe Angriffe**
- **Interne Sicherheit?! → Rechteverwaltung des Betriebssystems**
- **„Sicherheitsgrundstein“ für Technologien wie ADS**
- **Voraussetzung: korrekte Administration**



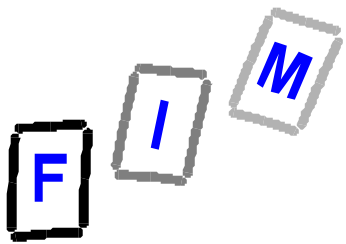
Motivation

- **Typische Administrationsprobleme:**
 - **Firmenstrukturen ändern sich;
Zugriffsberechtigungen müssen angepasst werden**
 - **Verwaltung von Benutzerberechtigungen wird zur komplexen Aufgabe**
 - **nur objekt-zentrierte Sicht**
 - **bei größeren Netzwerken nicht mehr überschaubar**

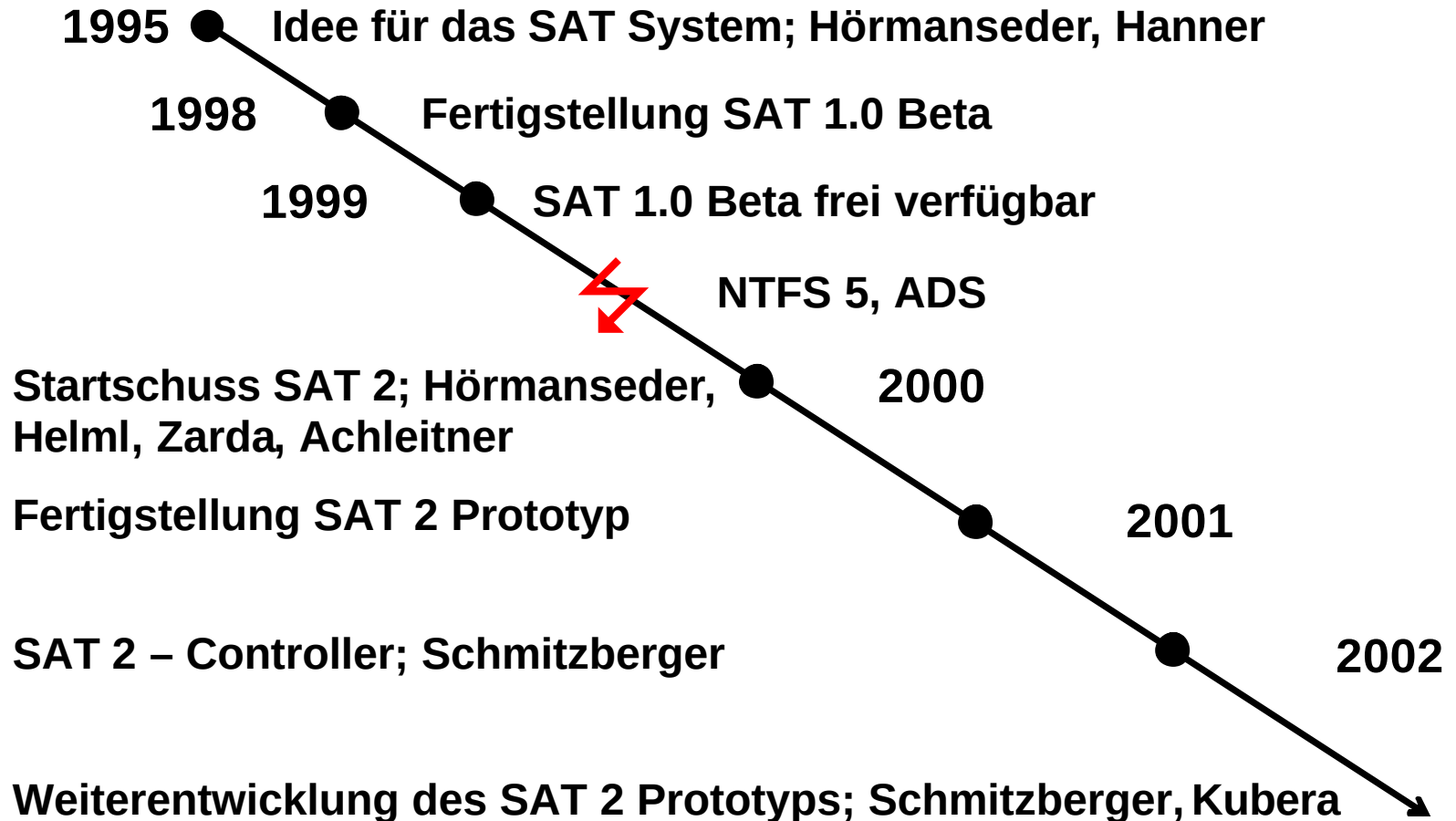


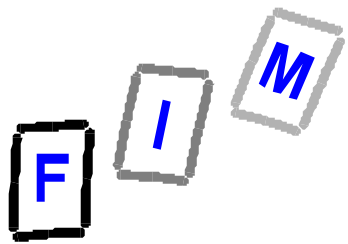
Motivation

- **SAT2 als Lösung**
- **Auflistung aller Objekte, auf die ein bestimmter Benutzer oder eine Gruppe Rechte hat**
- **Benutzer-zentrierte Sicht der Rechte im Netz**
- **Analyse von Active Directory, File System, Registry**
- **MMC als Plattform**

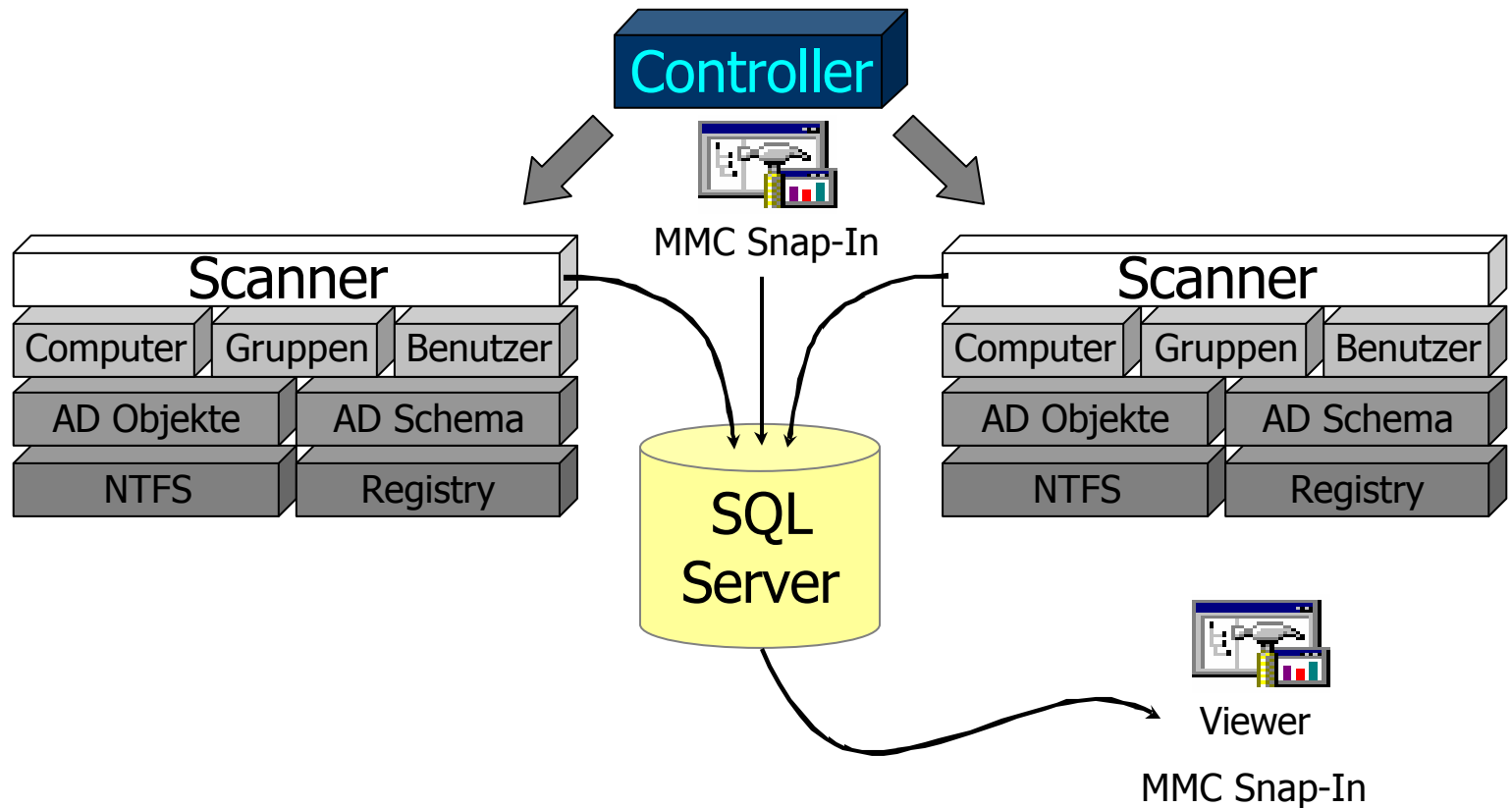


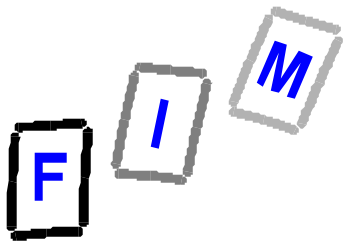
Das SAT Projekt





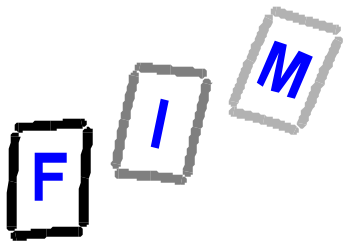
Architektur SAT 2.0





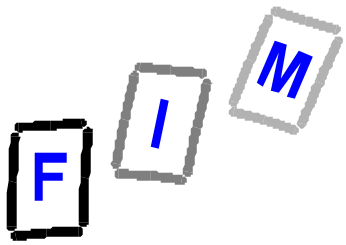
Controller Funktionalität

- **Schaltzentrale des SAT 2**
- **Anwendung als MMC Snap-In**
- **Master – Slave Prinzip**
- **Organisierung der Netzwerk-Rechner in beliebigen Scan-Routinen**
- **Controller von jedem Host im LAN zugreifbar (Authentifizierung vorausgesetzt)**

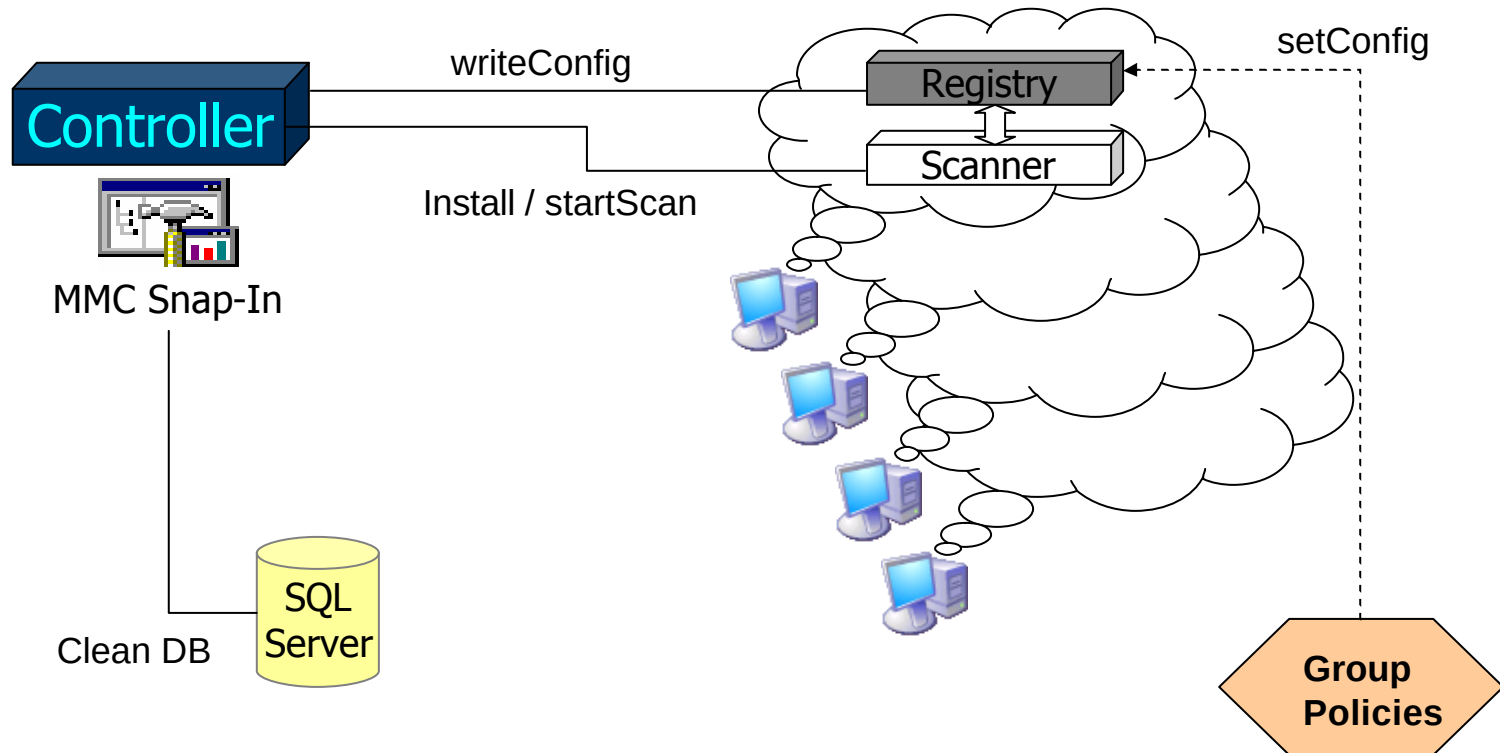


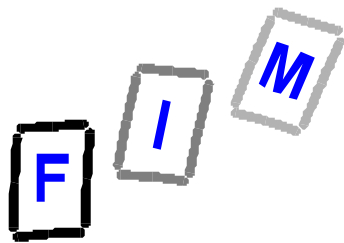
Controller Funktionalität

- **SAT-Scanner auf Remote-Rechner installieren bzw. updaten**
- **Schreiben / Lesen von Registry-Informationen (Konfigurationsdaten des Scanners)**
- **Starten der gewünschten Scanner-Komponenten**
- **Versionierung der Datenbank (noch nicht implementiert)**

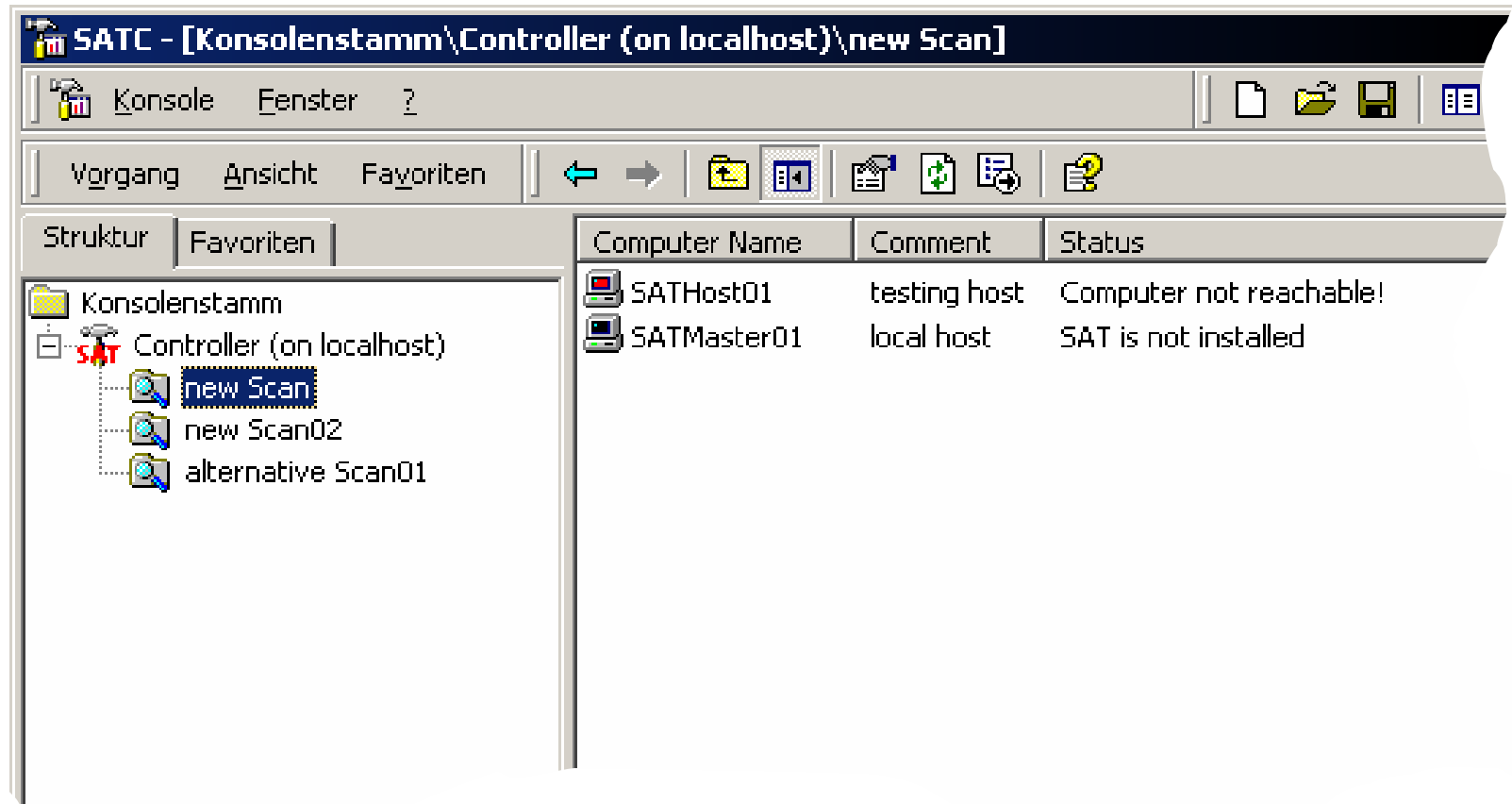


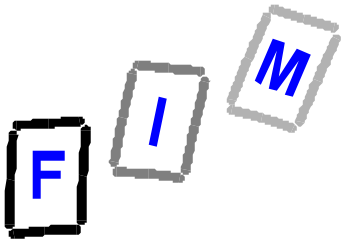
Controller Schema





MMC Snap-In





Features

■ Scanner Check Funktion

➤ Status-Abfrage der einzelnen Rechner im Scan:



Rechner konnte nicht erreicht werden



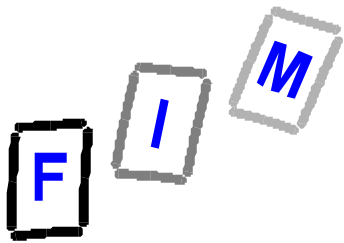
Scanner läuft gegenwärtig auf diesem Rechner



SAT-Scanner ist auf diesem Rechner installiert, aber nicht gestartet

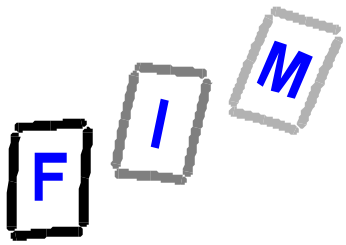


SAT-Scanner ist nicht auf diesem Rechner installiert



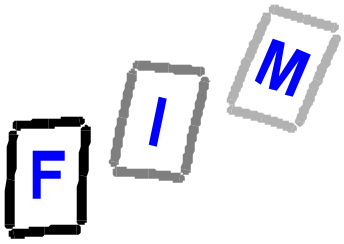
Features

- **Automatische Installation des SAT-Scanners:**
 - Beim Start des Scanners wird überprüft, ob und welche Version des SAT-Scanners vorhanden ist
 - aktuellste Version des Scanners wird auf den Client Rechner kopiert (falls noch nicht vorhanden)
 - alle SAT-Dateien werden ebenfalls kopiert
 - Scanner wird als Service installiert
- **Scannerkonfiguration wahlweise mittels Group Policies**



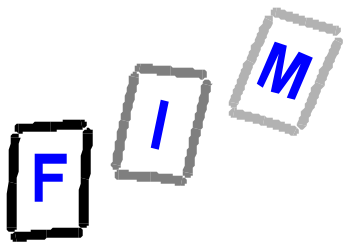
Konfiguration mittels Group Policies

- **Group Policy Object Editor, inkludiert in Windows NT 4 / 2000 / XP ab Server-Version**
- **Administrative Template Dateien *.adm**
 - **Definiert Registry Keys für den Group Policy Object Editor**
 - **Dient als Vorlage für die im GPO Editor dargestellten Eigenschaftsfenster**



Features

- **Philosophie von SAT 2:**
 - Einzelne Installationen auf Netzwerkrechnern nicht mehr nötig
 - System muss lediglich auf zentraler Stelle konfiguriert werden
 - Keine Upgrades (außer auf zentraler Stelle)
- **SAT-Scanner wird automatisch vom Host gelöscht, falls dieser in keiner Scan-Routine mehr vorhanden ist (noch nicht implementiert)**



Scannerkonfiguration

➤ gültig für alle Rechner im Scan:

- ✓ Bezeichnung der Scan-Routine
- ✓ Kommentarzeile
- ✓ Name der Datenbank
- ✓ Versionsnummer
- ✓ Ads Compression
- ✓ File Compression
- ✓ Registry Compression
- ✓ TimeSelect
- ✓ LastScanDate

Eigenschaften von Scan

Scan

 Name: new Scan
Comment: daily scanning routine

Database: myNet_SatDB
Version number: 2

ADS Compression: low compression (1)

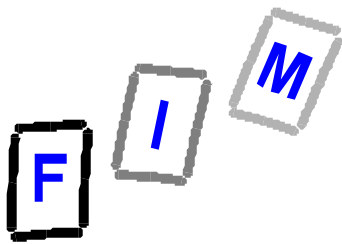
File Compression: high compression (4)

Registry Compression: middle compression (2)

Time Select: ☒ Creation Time
☐ Change Time

Last Scan Date: 00.00.0000, 00:00

OK Abbrechen Übernehmen



Scannerkonfiguration

➤ Für einzelne Rechner:

- ✓ Rechnername
- ✓ Cache Limit
- ✓ scan Ads Domain
- ✓ scan Ads Config
- ✓ scan Ads Schema Rights
- ✓ scan Ads Schema
- ✓ scan Users & Groups
- ✓ scan Registry
- ✓ Scan LastStarted
- ✓ ...

Eigenschaften von Computer

Computer

Name: SATHost01 Browse...

☐ don't change Registry values

Comment: testing host

scan Files: *

scan - stop at:

☐ scan ADS Domain ☐ scan File System

☒ scan ADS Config ☒ scan Users and Groups

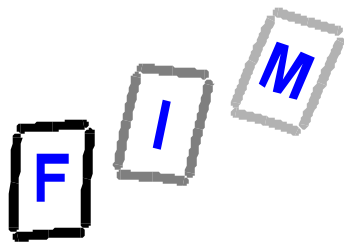
☐ scan ADS Schema Rights ☒ scan - stop at System Dir

☒ scan ADS Schema ☒ scan Registry

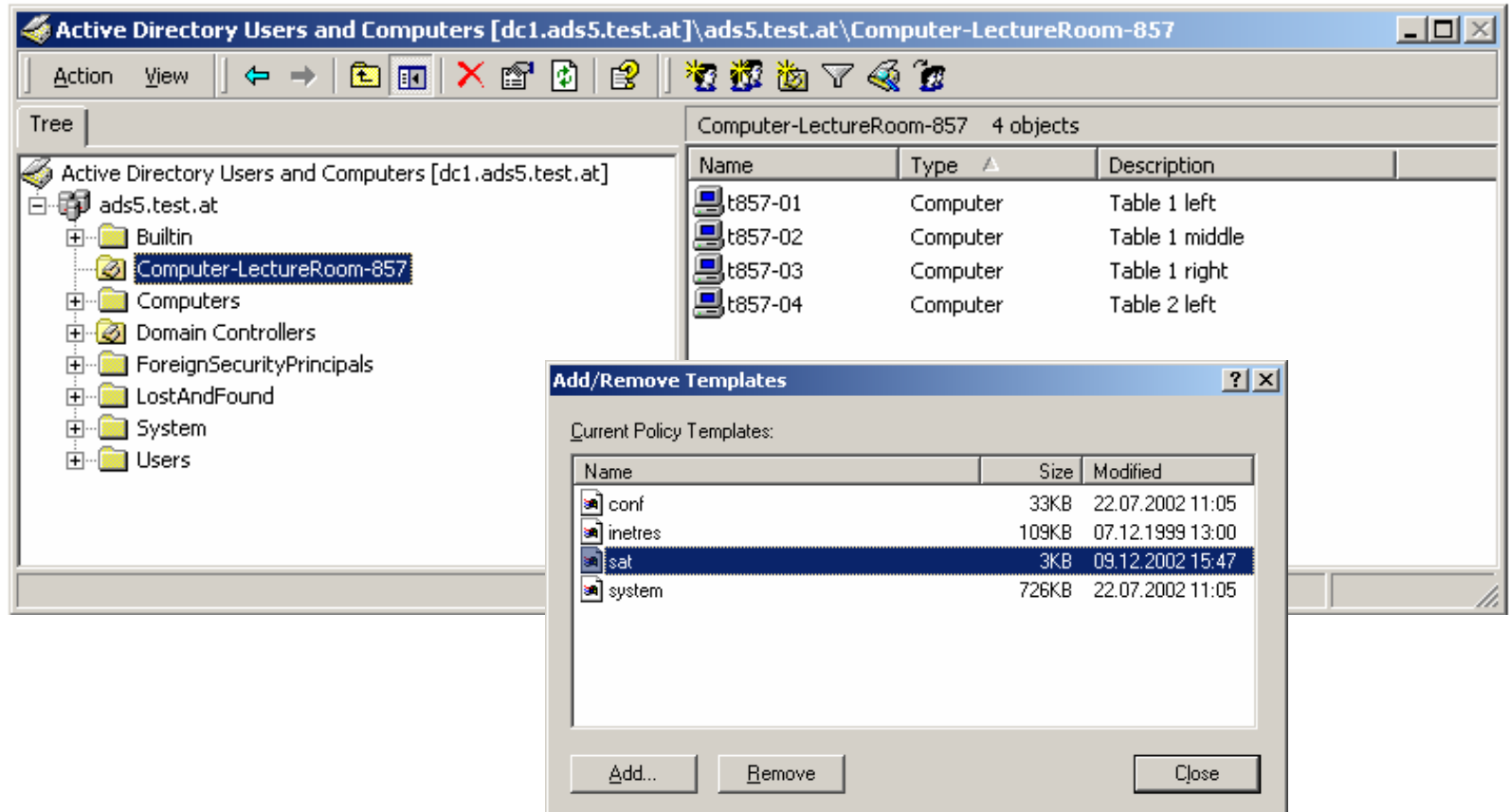
last started scan: 00.00.0000, 00:00

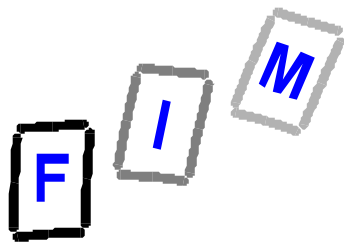
last finished scan: 00.00.0000, 00:00

OK Abbrechen Übernehmen

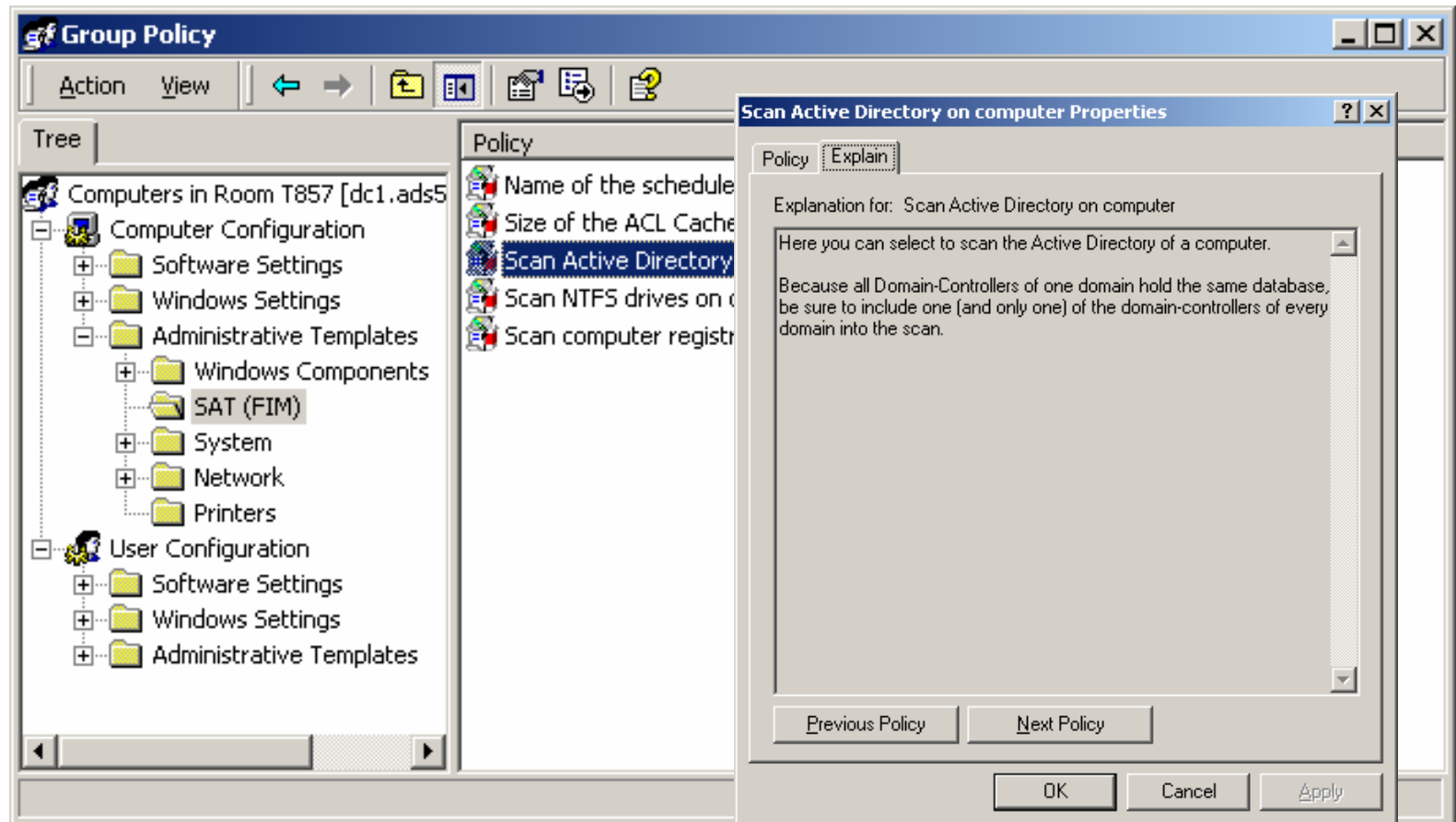


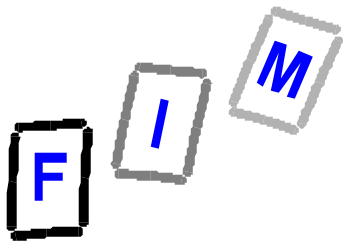
Scannerkonfiguration





Scannerkonfiguration





Scannerkonfiguration

■ SAT.adm:

CLASS MACHINE

CATEGORY !!FIM_SAT

POLICY !!SAT_ScanADS

KEYNAME "Software\FIM\SAT\"

EXPLAIN !!SAT_ScanADS_Help

VALUENAME "ScanADS"

VALUEON NUMERIC 1

VALUEOFF NUMERIC 0

END POLICY

...

END CATEGORY ;SAT

[strings]

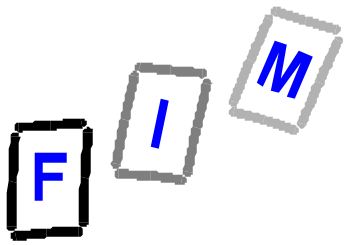
FIM_SAT="SAT (FIM)"

SAT_ScanADS="Scan Active Directory on
computer"

SAT_ScanADS_Help="Here you can select to scan
the Active Directory of a computer. \n\nBecause all
Domain-Controllers of one domain hold the same
database, be sure to include one (and only one) of
the domain-controllers of every domain into the
scan."

...

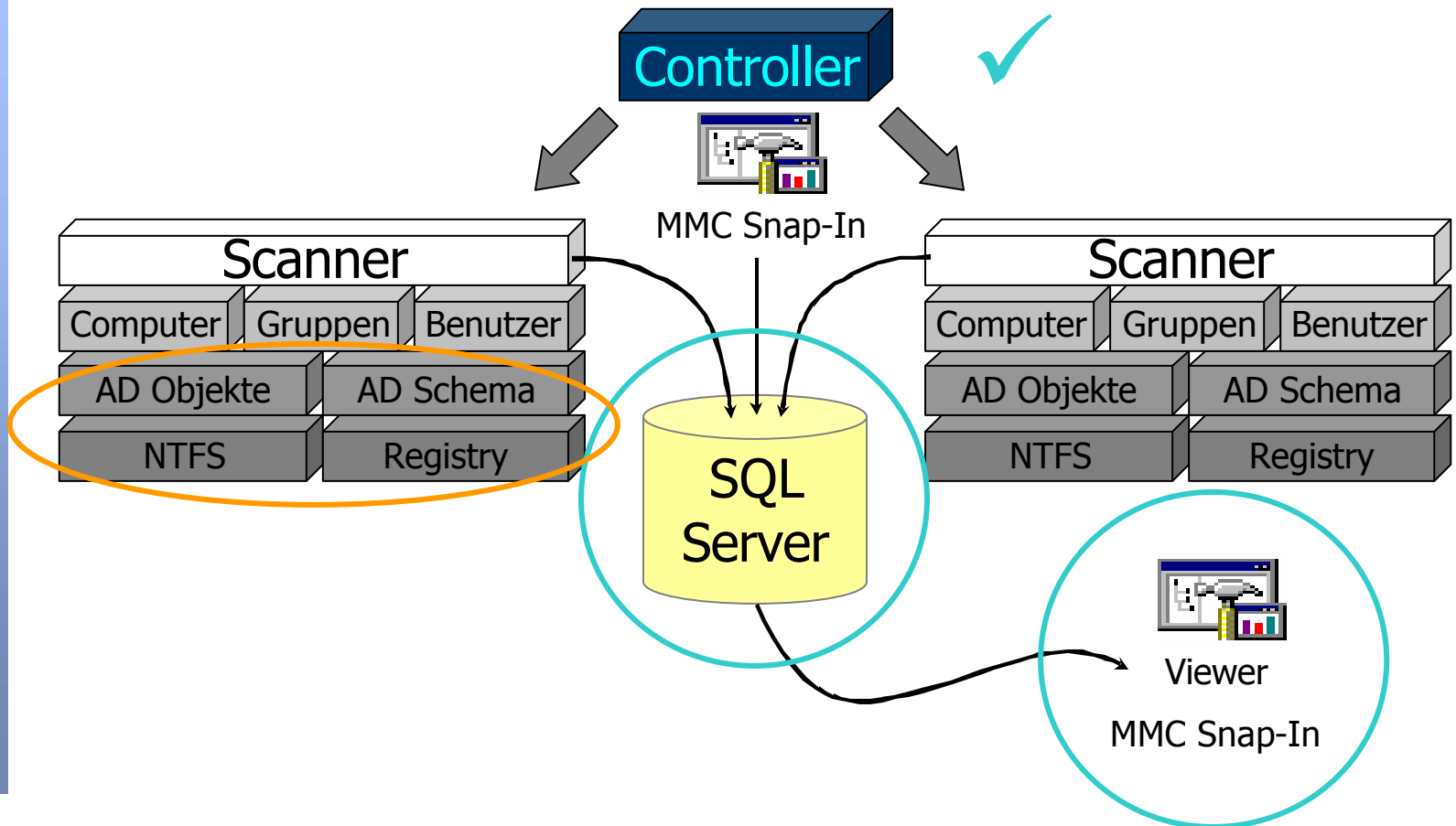
;End of Strings

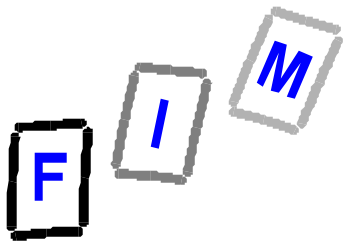


Sicherheitsaspekte

- **Service läuft unter dem Domain-Account SATUser**
- **SATUser gehört zur Gruppe der Domain-Administratoren**
- **Beim Start des Scanners wird das Passwort für SATUser abgefragt, das danach sofort explizit (im Speicher) überschrieben wird**

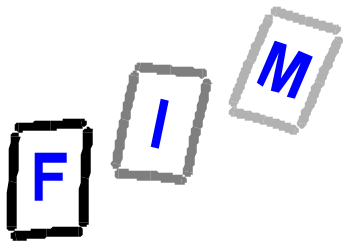
Projektstatus SAT 2.0





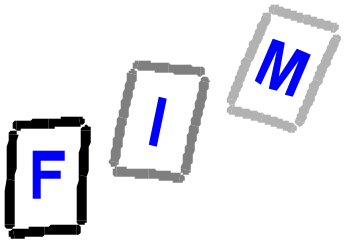
Resumee der bisherigen Projekterfahrungen

- **Bewusste Trennung der einzelnen Komponenten verursachte Komplexität und zusätzliche Performance-Einbußen**
- **Programmierung der MMC (Ver. 1.2) problematisch**
 - **MS Platform SDK schlecht dokumentiert**
 - **Code-Beispiele in der MSDN teilweise fehlerhaft**
 - **Dokumentation behandelt lediglich triviale Themen**
 - **Literatur zum Thema zum Zeitpunkt der Erstellung kaum verfügbar**



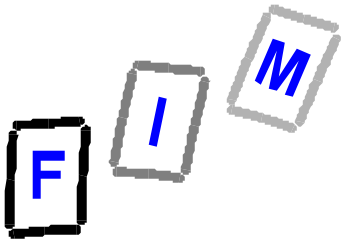
Resumee der bisherigen Projekterfahrungen

- **Visualisierungskomponente überlastet**
 - Dauer der Darstellung von DB-Auswertungen
 - „Flaschenhals“ DB-Zugriffe
 - Abstraktionsgrad der Darstellung der Rechte
- **Datenbank ist auf Größe und nicht auf Performance optimiert**
- **Datenmenge beträchtlich**



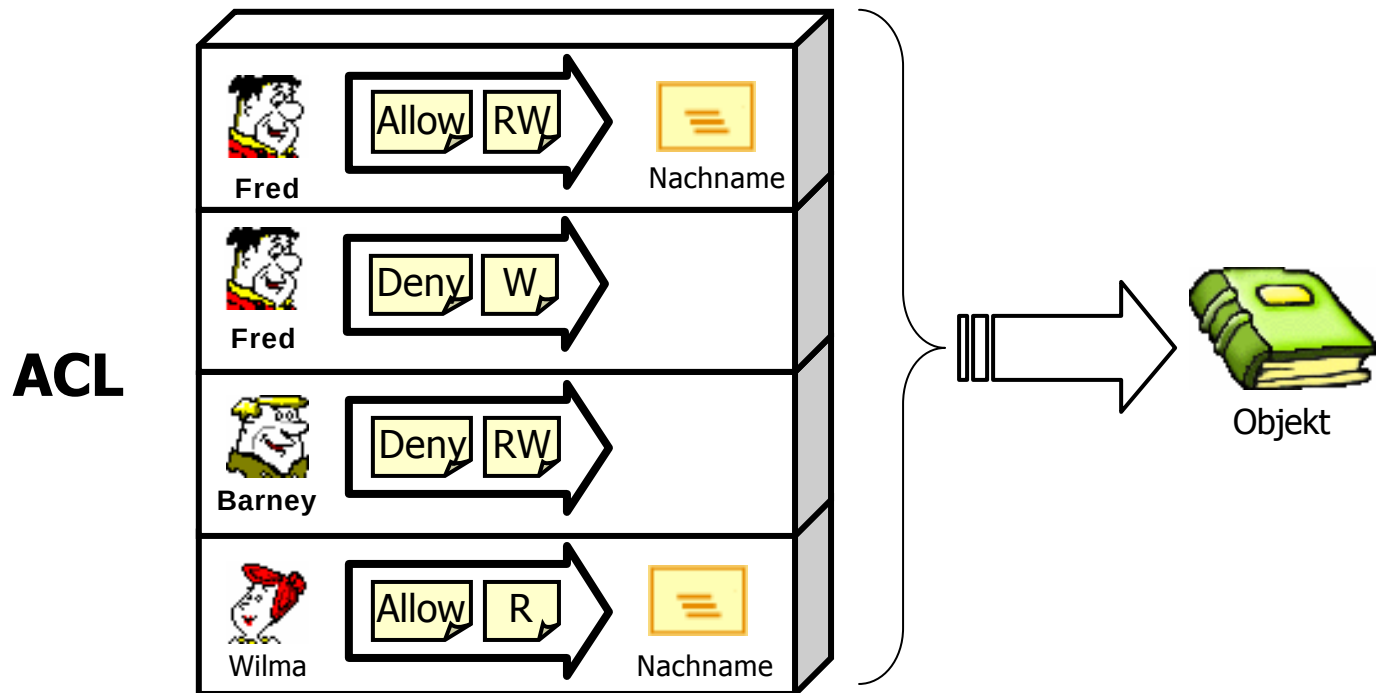
Beispiel: Active Directory

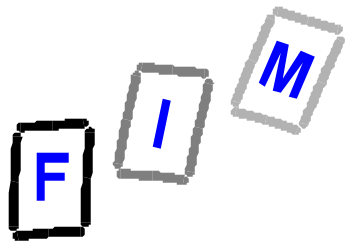
- **Was ist ein Directory?**
 - Ansammlung von Informationen (Objekten), die in einer bestimmten Art gruppiert bzw. aufgelistet werden
 - Vgl. Telefonbuch
- **Was ist ein Directory Service?**
 - Ein spezieller Dienst (Service) für
 - ✓ den Zugriff auf Informationen in einem Verzeichnis
 - ✓ die Speicherung von Informationen in ein Verzeichnis
 - Vgl. Auskunft
- **Active Directory**
 - Verzeichnisdienst von Microsoft
 - Speicherung von Informationen über Firmenstruktur (Firma, Abteilungen, Mitarbeiter, Computer, ...)



Access Control List (ACL)

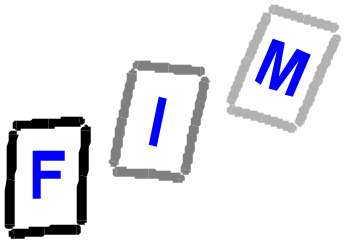
- ACL: Sammlung mehrerer ACE's
 - mehrere User haben Rechte auf EIN Objekt bzw. auf Attribute des Objekts





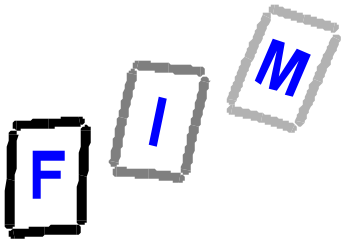
Komprimierung der Rechte

- Einem AD Objekt können 19 verschiedene Standard-Rechte zugewiesen werden (Access Rights)
- Speicherung als Bitmaske (Access Mask)
- Ziel: übersichtliche Darstellung als String
- Abbildung der Access Mask auf einen String
- Form: [R-W-C-D] od. [r-w-c-d]
 - Buchstaben beliebig kombinierbar
 - Unterschied zw. Groß-/Kleinschreibung
 - ✓ Groß: Recht gilt für das „ganze“ Objekt
 - ✓ Klein: Recht gilt für ein Attribut



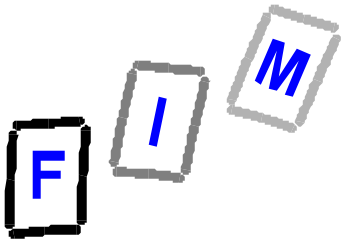
Konsequenzen

- **Überarbeitung des Datenbankschemas**
 - **Anpassung des Datenmodells um Visualisierung zu erleichtern**
 - **Auslagerung der Visualisierungsfunktionalität auf Stored Procedures am DB-Server**
 - **Datenbankinterface für den Controller**



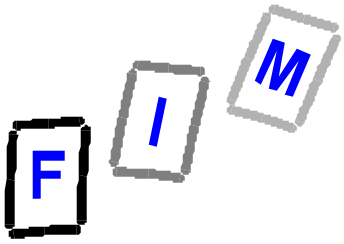
Konsequenzen

- **Neuentwicklung der Visualisierungskomponente**
 - **Programmierung in C#**
 - ✓ Unterstützung der MMC 2.0
 - ✓ Bessere Entwickler - Dokumentation
 - **Erfordert Microsoft .Net Environment**
 - ✓ Enthalten in Windows XP Service Pack 1
 - ✓ auch für ältere Windows Versionen erhältlich



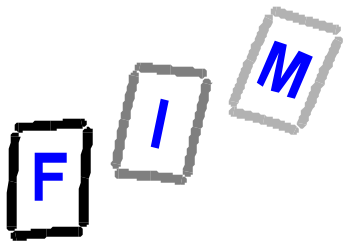
Ziele

- **Bessere Performance der Visualisierungskomponente**
- **Anzeigen von NTFS und Registry Informationen**
- **Eliminierung des Flaschenhalses Datenbank**
- **Komprimierung der Anzeige, Zusammenfassen von Objekten mit gleichen Rechten**
- **SAT 2 als Open Source verfügbar (unter GPL)**



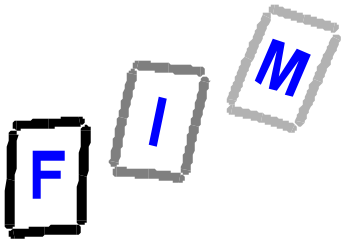
Ausblick

- Erweiterung des Scanners um SELF- und OWNER-Analysen
- Erweiterung der Abfragen
 - „Wo haben alle Mitglieder der Gruppe X Rechte?“
- ALL-IN-ONE Snap-In
 - Steuerung
 - Datensammler
 - Visualisierung



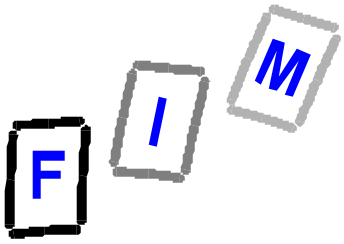
Projektbeteiligung

- Der SAT Controller wurde im Rahmen des 10-stündigen Praktikums realisiert.
- Die Weiterentwicklung des SAT 2 – Prototypen wird im Rahmen der Diplomarbeit „Datenauswertung der Rechtestrukturen unter Windows 2000 und deren Visualisierung“ des Vortragenden verwirklicht.
- Projektleitung: DI Rudolf Hörmanseder
- Finanzielle Unterstützung durch MSR – Microsoft Research, Cambridge (UK)



Verweise

- Developing MMC Snap-Ins using ATL
<http://www.codeproject.com/atl/mmcsnap.asp>
- Microsoft Developer Network
<http://msdn.microsoft.com/>
- Projekt: Security Analysis Tool (SAT),
FIM Institut für Informationsverarbeitung und
Mikroprozessortechnik,
Johannes Kepler Universität Linz
<http://www.fim.uni-linz.ac.at/research/sat>



Danke für Ihre Aufmerksamkeit!