
# NEUE SICHERHEITSFUNKTIONEN IN WINDOWS SERVER 2008 R2 UND WINDOWS 7

# Inhalt

- Ueberblick
- Bitlocker, Bitlocker to Go
- Applocker
- Advanced Audit
- Direct Access
- NPS
- PKI Erweiterungen
- UAC
- Neuerungen in der Windows Firewall
- DNSSEC

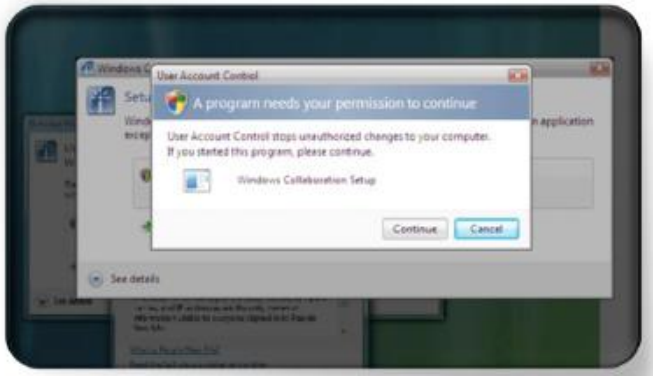
# Referentenvorstellung

- Marc Grote
- Baujahr 1972 – seit 1989 hauptberuflich ITler
  seit 1995 Selbststaendig (bis 2004 Teilzeit Consultant), vorher angestellt als IT-Administrator
- Schwerpunkte: Windows Server seit NT 3.5, Clustering, PKI, Exchange Server seit 5.0, ISA Server (Forefront TMG, FSE, FSC, Stirling)
- E-Mail: grotem@it-training-grote.de
- Web: http://www.it-training-grote.de
- Blog: http://www.it-training-grote.de/blog

# Ueberblick

- Basis Windows Server 2008 und Windows Vista
- Gleiche Codebasis
- Konsequente Weiterentwicklung
- Evolution statt Revolution
- Viele Detailverbesserungen und Neuerungen
- Common Criteria EAL4 – FIPS-140-2

# Windows 7




Die Benutzerkontensteuerung maximiert die Nutzung eines Standardbenutzerkontos, während der entsprechende Zugriff gewährt wird.


Die Firewall bietet eine neue Schnittstelle für erweiterte Sicherheit mit voller Gruppenrichtlinienunterstützung für Konfiguration und Regeln.

Die BitLocker™-Laufwerksverschlüsselung schützt Informationen auf Laptops und Festplatten, um Sicherheitsverletzungen zu verhindern.

# Coffee To Go – aeeh Bitlocker To Go

- Bitlocker Verschluesselung auch fuer Wechselmedien
- Portable Nutzung der Verschluesselung
- Runtime Environment fuer PC, auf welchem der USB Stick eingesetzt werden soll
- Standard 128 Bit AES + Diffuser
  - Aenderung per Group Policy auf AES 256 Bit
  - Computer Configuration, Administrative Templates, Windows Components, and BitLocker Drive Encryption

# Coffee To Go – aeeh Bitlocker To Go

## Situation heute



- Gartner "Forecast: USB Flash Drives, Worldwide, 2001-2011" 24 September 2007, Joseph Unsworth
- Gartner "Dataquest Insight: PC Forecast Analysis, Worldwide, 1H08" 18 April 2008, Mikako Kitagawa, George Shiffler III

## Windows 7 Lösung

### BitLocker To Go™

- Protect data on internal and removable drives
- Mandate the use of encryption with Group Policies
- Store recovery information in Active Directory for manageability
- Simplify BitLocker™ setup and configuration of primary hard drive

# Genug der Worte ….

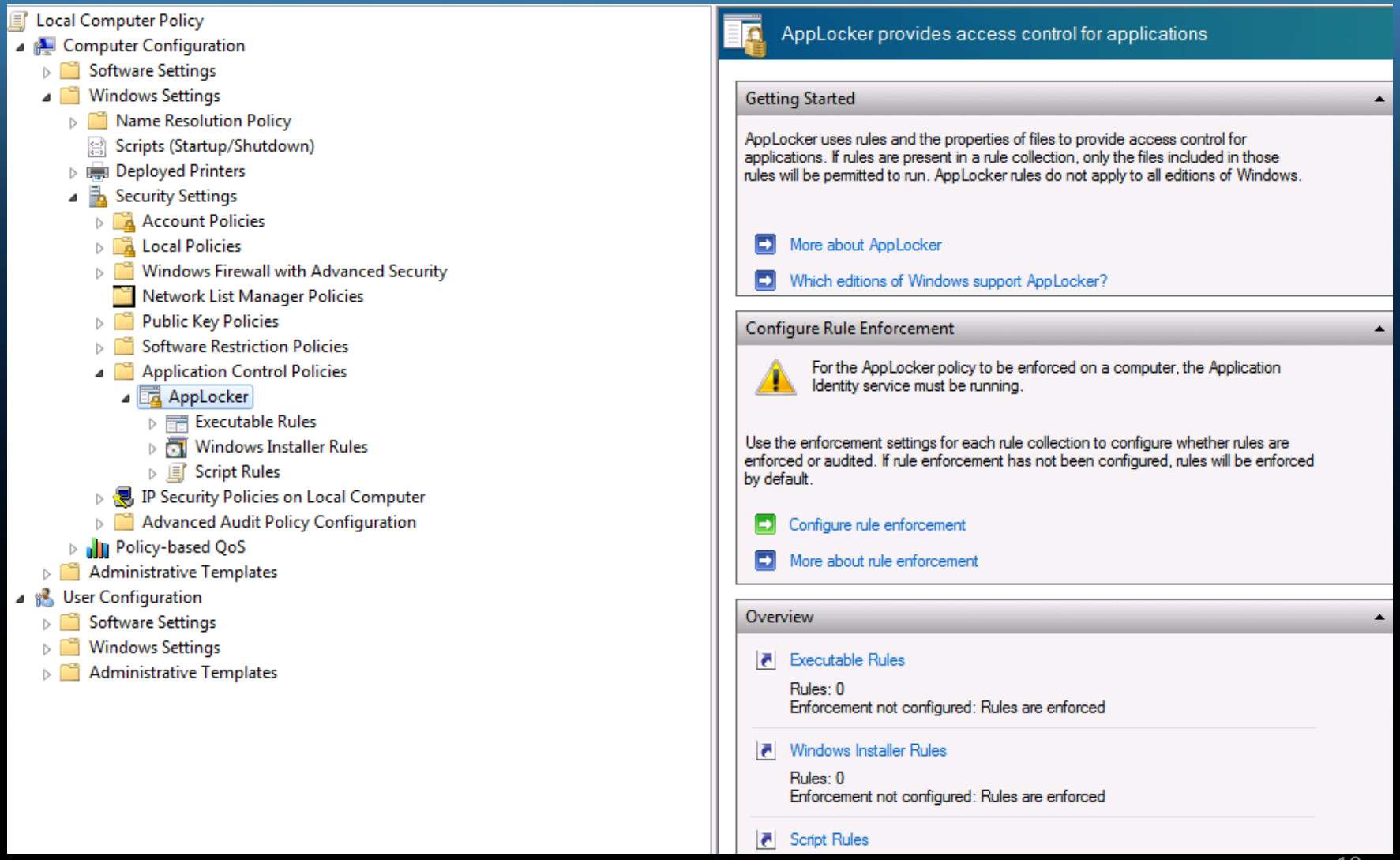
# Demo

Bitlocker in Action

# Applocker

- Weiterentwicklung der Software Restriction Policies
- Verhindert die Ausfuehrung von Anwendungen
- Anwendbar auf bestimmte Benutzer und Gruppen
- Client muss Windows 7 sein
- Applocker Powershell Cmdlets
- Audit Mode

# Applocker


Local Computer Policy
Computer Configuration
Software Settings
Windows Settings
Name Resolution Policy
Scripts (Startup/Shutdown)
Deployed Printers
Security Settings
Account Policies
Local Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
AppLocker
Executable Rules
Windows Installer Rules
Script Rules
IP Security Policies on Local Computer
Advanced Audit Policy Configuration
Policy-based QoS
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
AppLocker provides access control for applications
Getting Started
AppLocker uses rules and the properties of files to provide access control for applications. If rules are present in a rule collection, only the files included in those rules will be permitted to run. AppLocker rules do not apply to all editions of Windows.
More about AppLocker
Which editions of Windows support AppLocker?
Configure Rule Enforcement
For the AppLocker policy to be enforced on a computer, the Application Identity service must be running.
Use the enforcement settings for each rule collection to configure whether rules are enforced or audited. If rule enforcement has not been configured, rules will be enforced by default.
Configure rule enforcement
More about rule enforcement
Overview
Executable Rules
Rules: 0
Enforcement not configured: Rules are enforced
Windows Installer Rules
Rules: 0
Enforcement not configured: Rules are enforced
Script Rules

# Applocker vs. Software Restriction Policies

| Feature | Software Restriction Policies | AppLocker |
|---|---|---|
| Rule scope | All users | Specific user or group |
| Rule conditions provided | File hash, path, certificate, registry path, and Internet zone rules | File hash, path, and publisher rules |
| Rule types provided | Allow and deny | Allow and deny |
| Default rule action | Allow or deny | Deny |
| Audit-only mode | No | Yes |
| Wizard to create multiple rules at one time | No | Yes |
| Policy import or export | No | Yes |
| Rule collection | No | Yes |
| PowerShell support | No | Yes |
| Custom error messages | No | Yes |

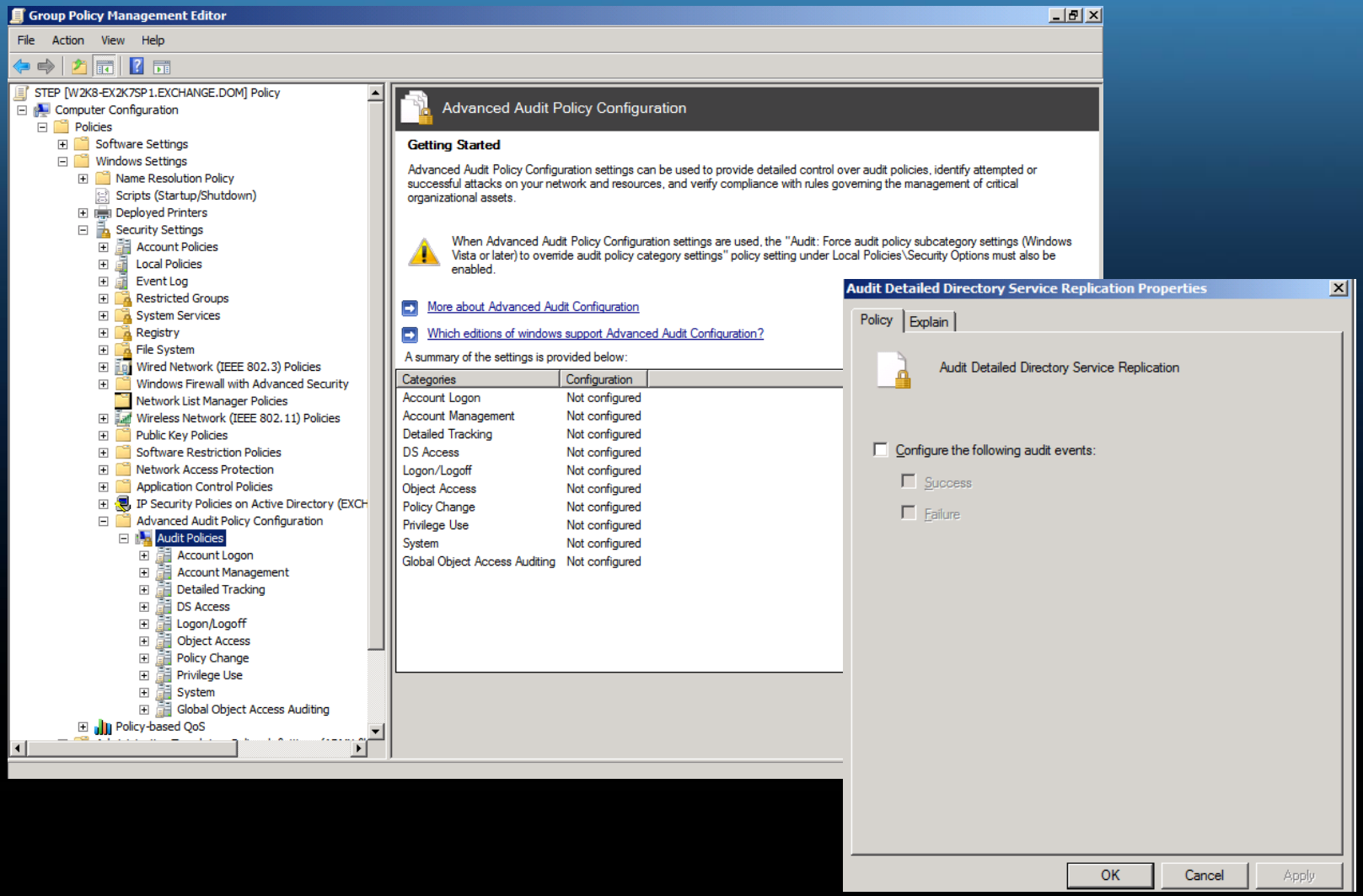
# Genug der Worte ….

# Demo

# Advanced Audit

- Global Object Access Auditing
  - SACL wird automatisch auf Objekte uebertragen
- Erweiterte Audit Einstellungen
  - 53 neue GPO
- Erweiterte Audit Einstellungen und die klassisches Audit Funktion sollten nicht kombiniert werden

# Advanced Audit



# Genug der Worte ….

# Demo

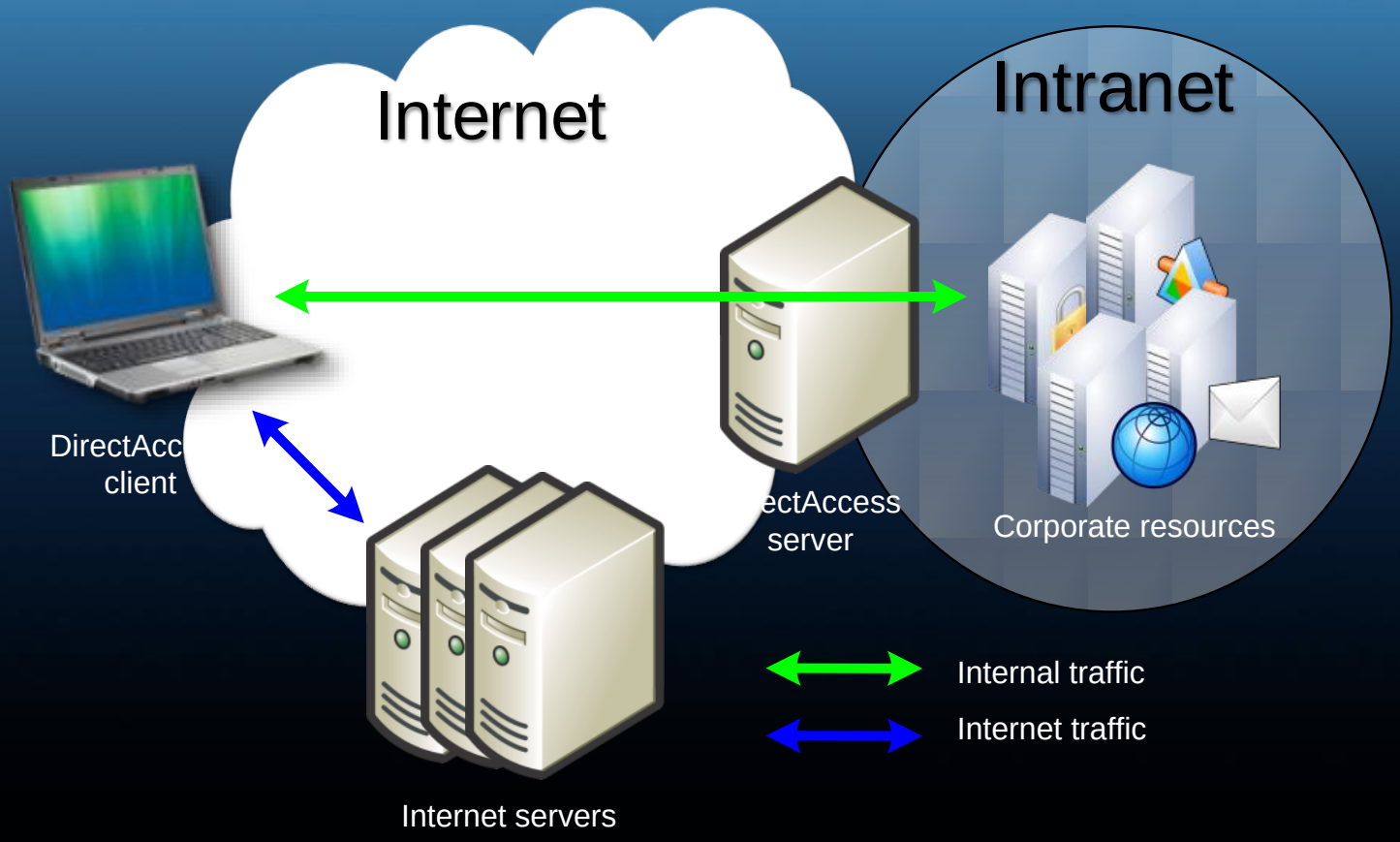
# Direct Access

- VPN Loesung
- Vereinfachte Benutzung durch Enduser
- Always on
- Nahtlose Integration
- Bidirektionaler Zugriff
- Erhoehte Sicherheit
- Integrierte Loesung

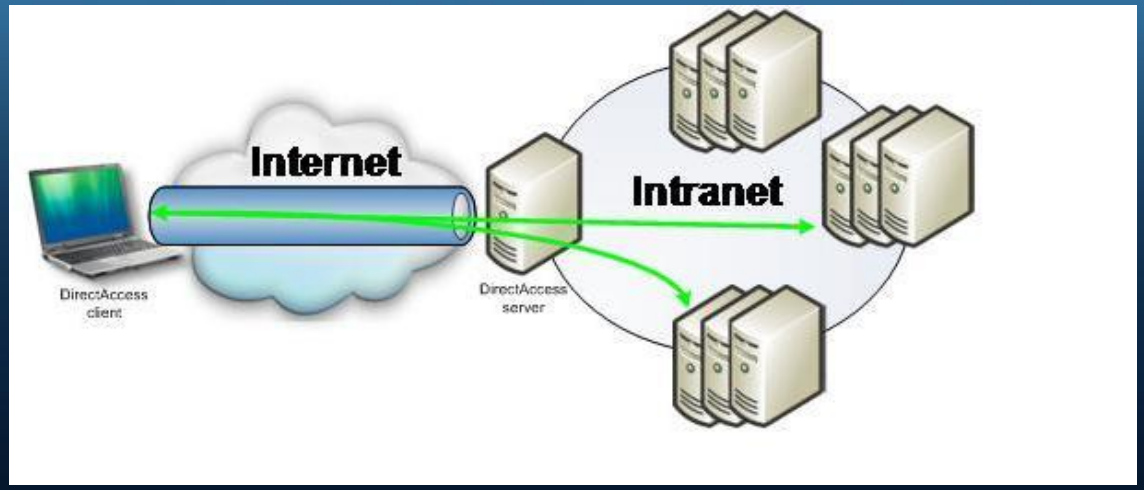
# Direct Access Technik

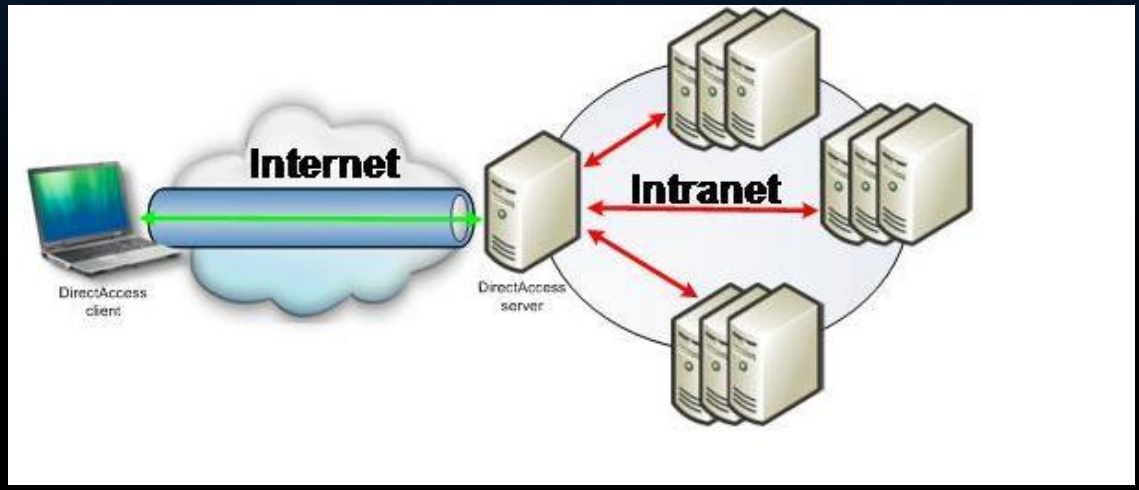
- Permanente IPv6 Verbindung
  - Transitionstechnik integriert (Teredo, 6to4, ISATAP)
- IPSEC Verbindung als Basis
  - Zwei IPSEC Tunnel (Client zu DNS und DC und Client zur Auth. und Intranet Access)
- IP-HTTPS
  - Tunneling von IPv6 Paketen in IPv4 HTTPS
- Split Tunneling ist Grundlage von DA
  - Force Tunneling ist moeglich
  - IP-HTTPS wird verwendet, wenn Split Tunneling aus ist
- DA Client Verwaltung erfordert IPv6
- DA Client Kommunikation untereinander ist moeglich
- Verwaltung ueber DA MMC
- Monitoring ueber DA Monitoring MMC

# Direct Access

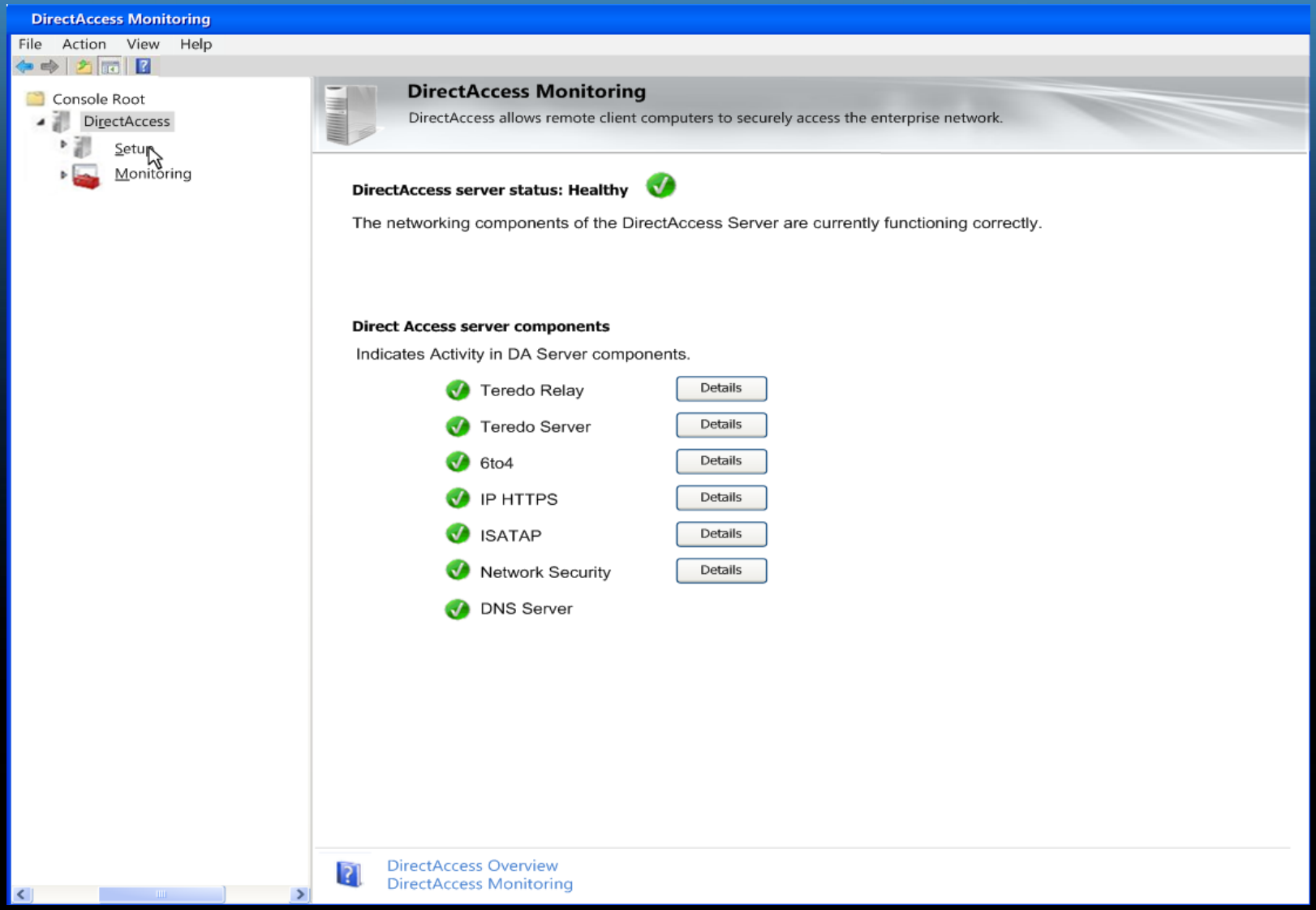


# Direct Access

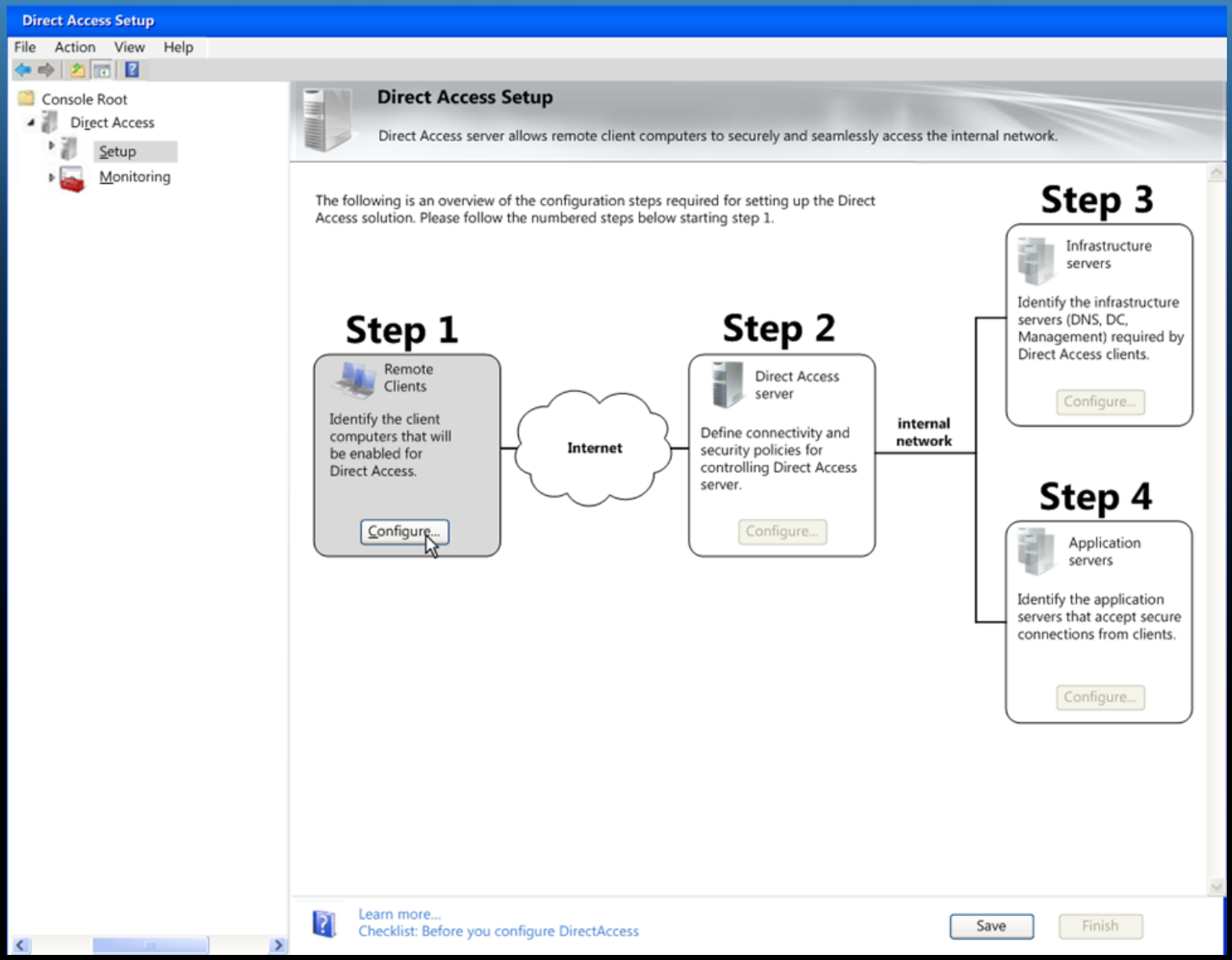


# Direct Access



# Direct Access



# NPS

- Automatisches Setup fuer NPS Protokollierung in MS SQL
- Moeglichkeit zur Protokollierung in eine Textdatei und MS SQL parallel
  - Failover von SQL zu Text Protokollierung
  - Neues Protokollformat aehnlich SQL
- Konfiguration mehrerer SHV (System Health Validator) fuer NAP
  - Unterschiedliche NAP Anforderungen
- NPS Templates
  - Vorlagen fuer unterschiedliche Konfigurationsanforderungen
  - Replikation der Vorlagen zwischen verschiedenen NPS
- Moeglichkeit zur Migration einer IAS Konfiguration zu NPS

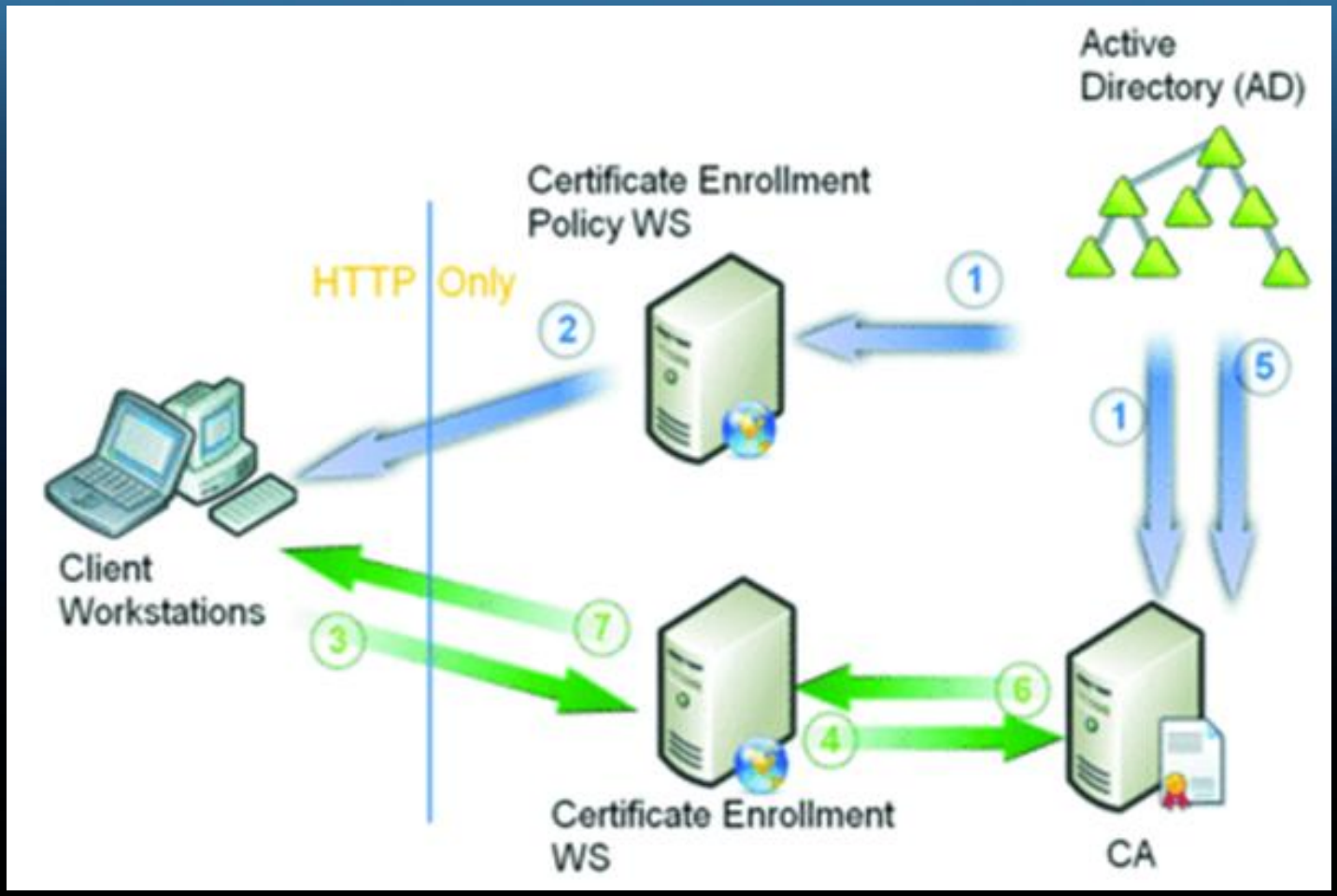
# Genug der Worte ….

# Demo

# PKI Erweiterungen

- Server Konsolidierung
  - Weniger CA im Unternehmen
  - Cross Forest Certificate Enrollment
- Erweiterung / Verbesserung vorhandener Funktionen
  - Best Practice Analyzer
  - SCEP (Simple Certificate Enrollment Protocol) Verbesserung
  - Funktion, ausgestellte Zertifikate/Anforderungen nicht in der CA DB zu speichern
  - HTTP Enrollment mit CEPP (Certificate Enrollment Policy Protocol)
- Verstaerkte Verschluesselungsalgorithmen
  - Verbesserung der Smartcard Integration
  - Windows Biometric Framework
    ECC (Elliptic Curve Cryptography) Smart Card Zertifikate
  - Unterstuetzung fuer NIST SP 800-73-1 fuer PIV (Personal Identity Verfification) ohne Middleware

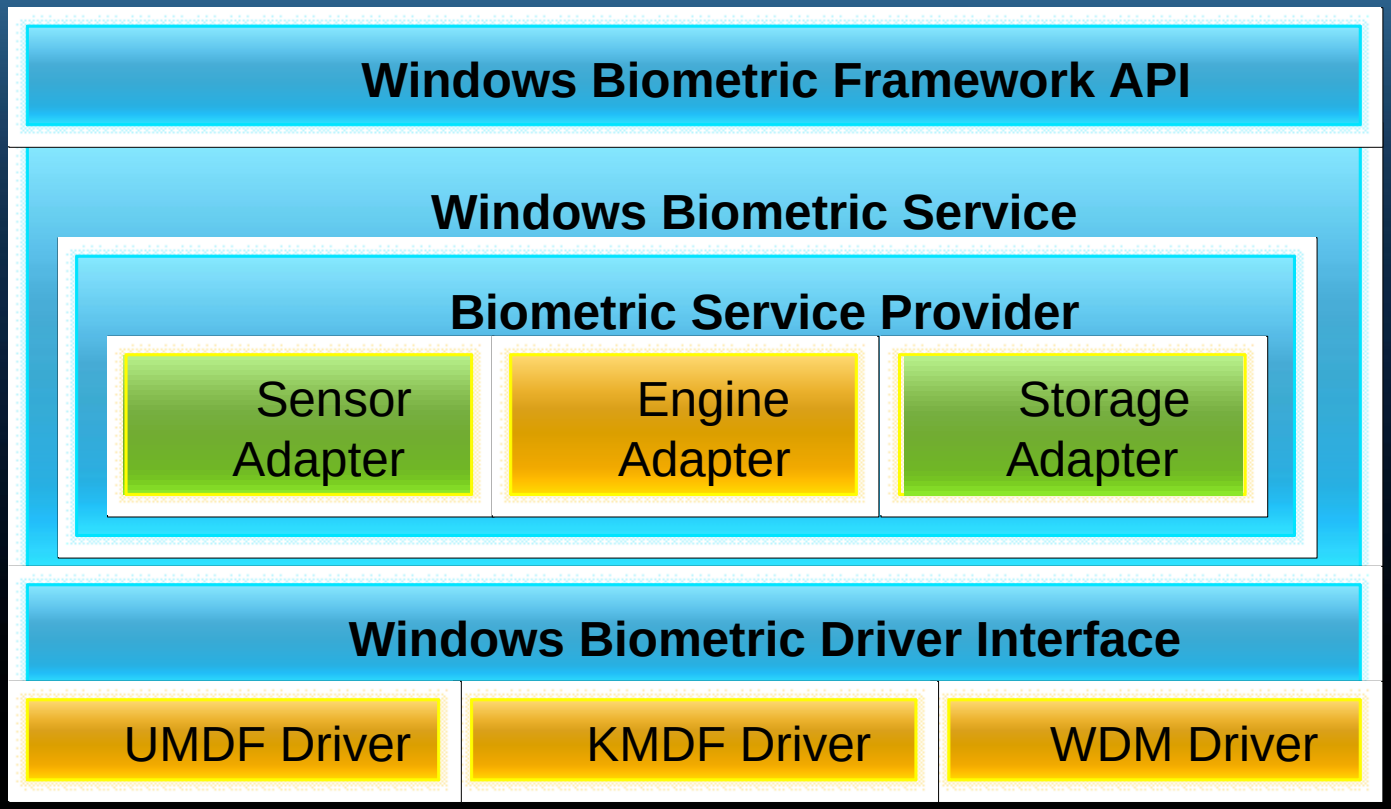
# Certificate Enrollment

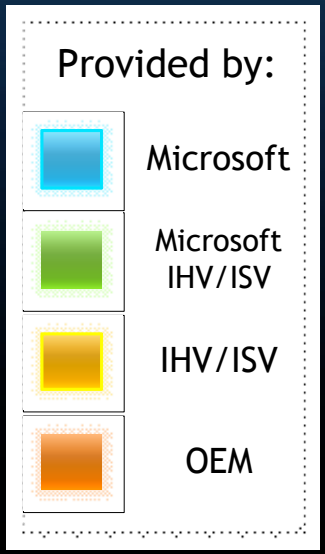


# Windows Biometric Framework

- Schnittstelle zur einfacheren Implementierung von Biometric Geraeten (z. B. Fingerprint Reader)
- Konfigurierbar ueber Windows „Control Panel“
- Device Manager unterstuetzt Verwaltung von BF-Geraeten
- Credential Support Provider (CREDSSP) Integration mit UAC Elevation
- Group Policy Settings zur Konfiguration von BF-Geraeten
- BF Treiber per Windows Update

# Windows Biometric Framework



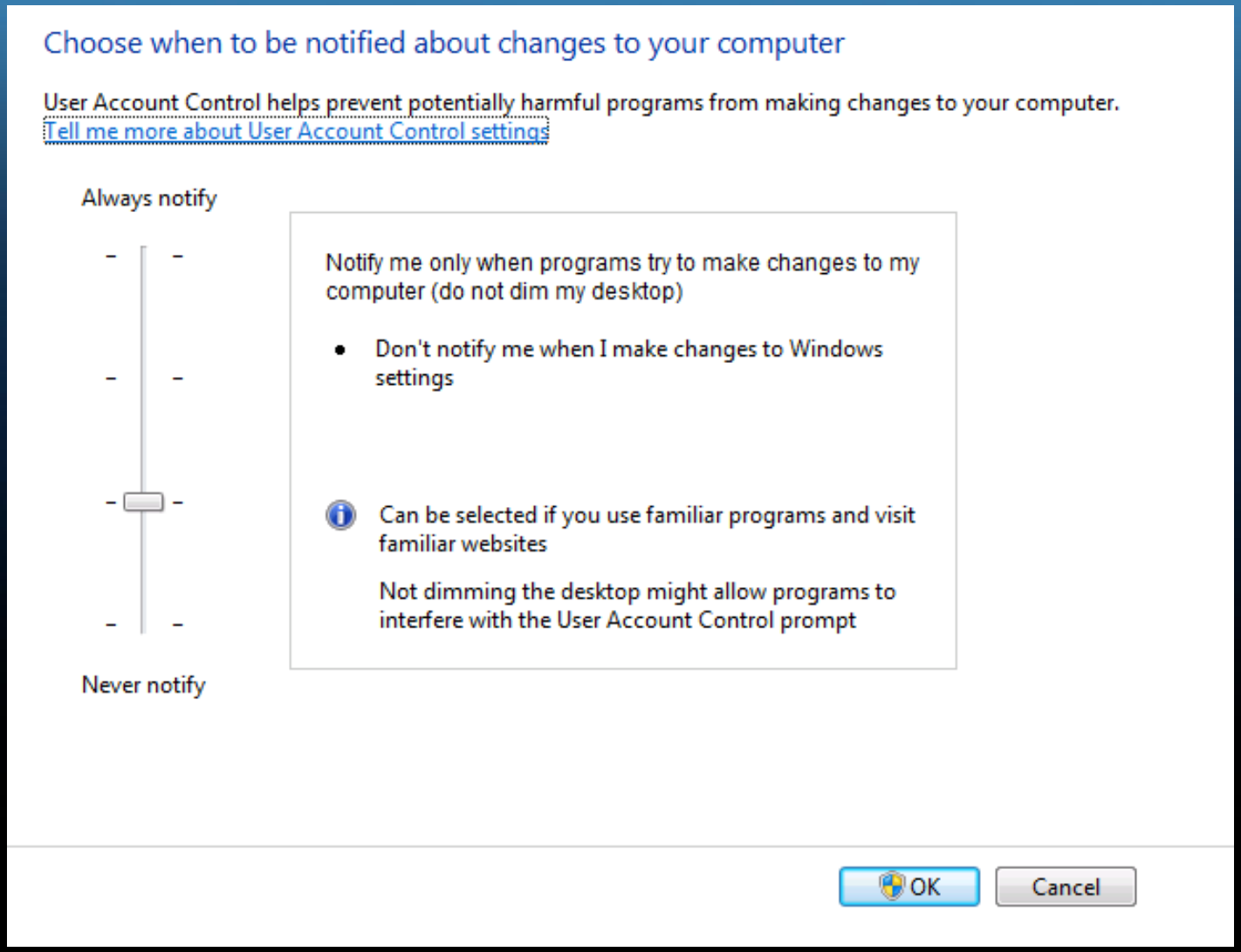
# Genug der Worte ….

# Demo

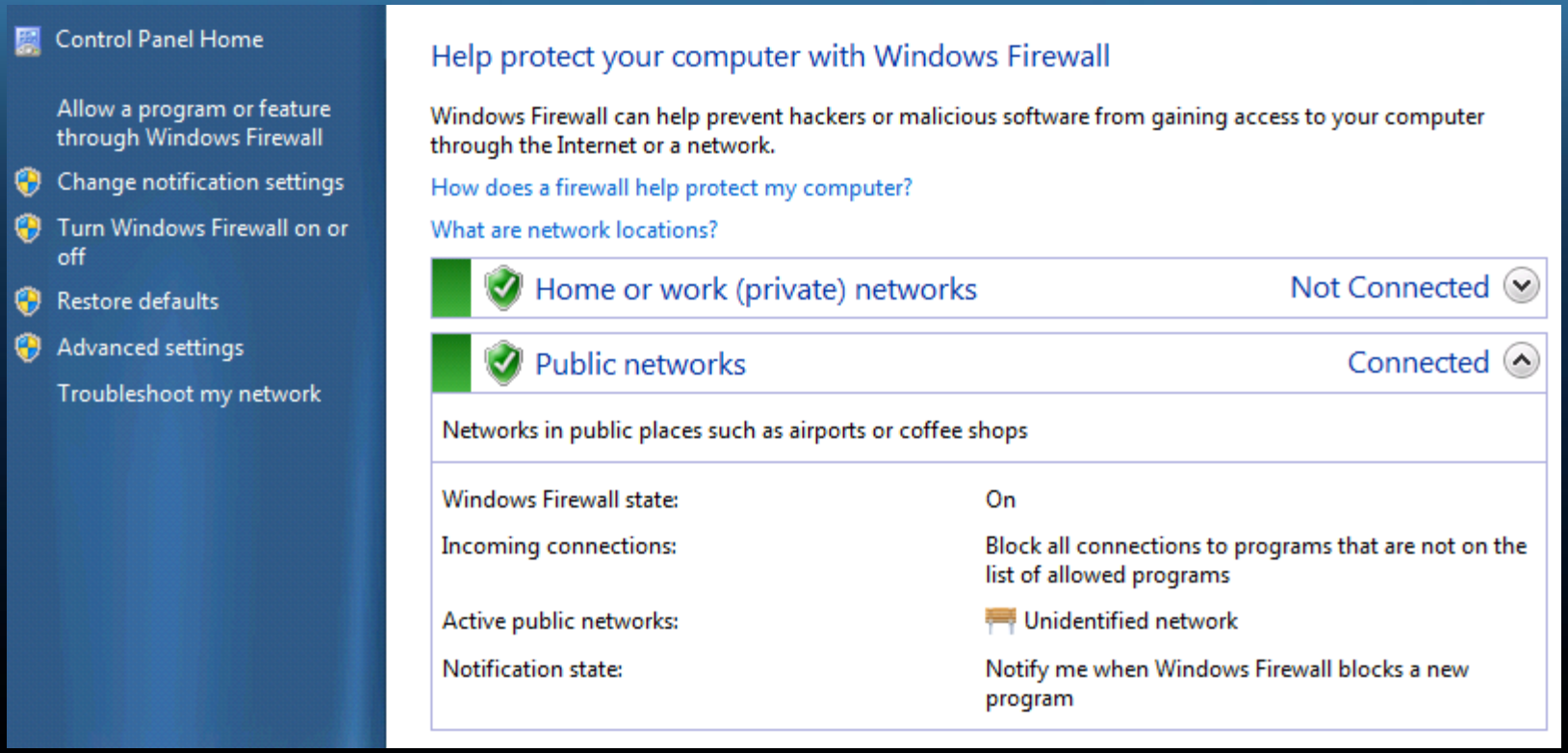
# UAC

- File operation prompts are merged
- Internet Explorer prompts for running application installers are merged
- Internet Explorer prompts for installing ActiveX controls are merged
- The default UAC setting allows a standard user to perform the following tasks without receiving a UAC prompt:
  - Install updates from Windows Update
  - Install drivers that are downloaded from Windows Update
- View Windows settings. (However, a standard user is prompted for elevated privileges when changing Windows settings.)
  - Pair Bluetooth devices to the computer
  - Reset the network adapter and perform other network diagnostic and repair tasks

# UAC


Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Notify me only when programs try to make changes to my computer (do not dim my desktop)
Don't notify me when I make changes to Windows settings
Can be selected if you use familiar programs and visit familiar websites
Not dimming the desktop might allow programs to interfere with the User Account Control prompt
Never notify
OK
Cancel

# Windows Firewall




- Multiple Active Firewall Policies
- Unterschiedliche Firewallregeln pro Netzwerkprofil

# Neue Service Accounts

- Service Accounts laufen als
  - Local System
  - Local Service
  - Network Service
- Zwei neue Service Accounts
  - Managed Service Account
    - Account Isolation fuer z. B. SQL, IIS)
    - SPN und Credentials werden automatisch konfiguriert
  - Virtual Service Account
    - Verwaltete lokale Accounts
    - Verwenden Computer Credentials zum Zugriff auf Netzwerkressourcen

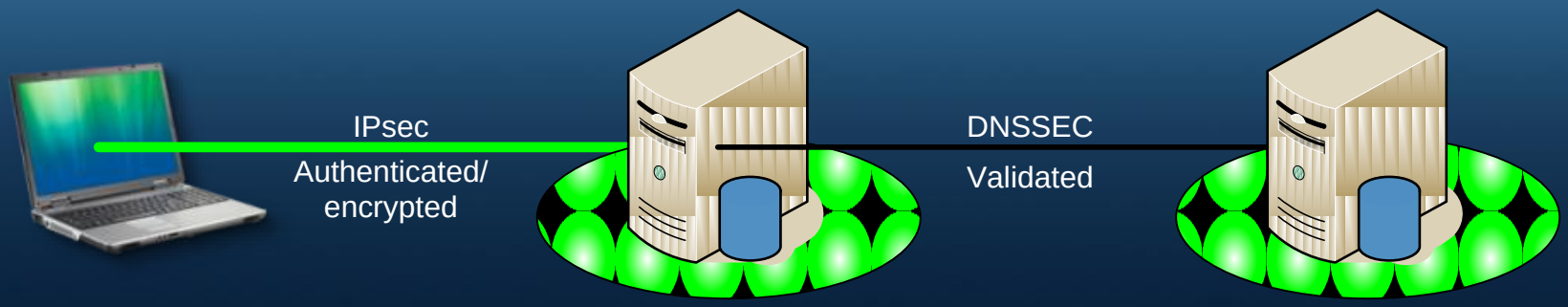
# Genug der Worte ….

# Demo

# DNSSEC

- DNS Security (DNSSEC)
  - Ueberprueft bei der Namensaufloesung, ob diese von einer vertrauten Instanz stammt
  - Ziel: DoS Angriffe verhindern und DNS Antwort-Legitimation pruefen
  - DNSSEC verwendet SSL zur Kommunikation zwischen DNS Client und -Server
  - DNS Zonen koennen digital signiert werden
  - Unterstuetzung fuer DNSKEY, RRSIG, NSEC und DS Eintraege
  - PKI erforderlich

# DNSSEC


IPsec
Authenticated/
encrypted
DNSSEC
Validated
Client
Caching
DNS server
Authoritative
DNS server

# Fragen?

# Das Ende

Vielen Dank fuer Ihre Aufmerksamkeit