

Migration der Monopolkommission auf Open Source Software (OSS)

beauftragt durch das
Bundesamt für Sicherheit in der Informationstechnik (BSI)

ausgeführt von
natural computing GmbH
SFI Technology Service AG
Quelltext AG

Dokumentiert durch
natural computing GmbH, Oktober 2002

Migration der Monopolkommission auf Open Source Software (OSS)

Projektleitung

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Christel Marquardt

eMail: christel.marquardt@bsi.bund.de

Monopolkommission

Peter Göbel

eMail: peter.goebel@bundeskartellamt.bund.de

natural computing GmbH

Thomas Sprickmann Kerkerinck

eMail: thomas.sprickmann@natural-computing.de

Das Projekt

- Ausgangssituation
- Das Konzept für die Monopolkommission
- Der Umstellungsprozess
- Nach der Migration
- Fazit

Ausgangssituation

- Aufgaben der Monopolkommission als Determinante für die IT-Struktur
 - Erstellung von Gutachten für die Bundesregierung
 - Datenzusammenstellung und Auswertung
 - Datenaufbereitung zur Präsentation und Drucklegung
 - Allgemeine Aufgaben zur eigenen Organisation
 - Bibliotheksverwaltung
 - Sekretariat
 - Geschäftsstelle der Monopolkommission

Die Rahmenbedingungen

- Migration im Produktionsbetrieb
- Nutzung der vorhandenen Hardware
- Ersetzung der „Windows-Applikationen“ durch
 - Geeignete Open-Source-Software (OSS)
 - mit OSS-Betriebssystem (GNU/Linux) lauffähige Applikationen
- Mitarbeiterschulung zeitnah zur Umstellung
- Zeitrahmen 1.8.2002 – 31.10.2002
- Aufgabe definiert im „*Kurztext der Ausschreibung*“
- Testumgebung steht zur Verfügung

Hardware

Server

Dell Poweredge 2500

Dualprozessor 2x 1 GHZ P III
1 GB RAM

Raid-Controller, Scsi-Controller, 1x Raid 1 – 18 GB, 1x Raid
1 – 36 GB (noch leer), 1x SCSI 36 GB,
interner Dat-Streamer DDS-4 (HP 20-40 GB)

Netzwerk

LWL Netzwerkarte

SMC-9432 FTX eingebaut

Clients

Handelsübliche PC

Celeron 400 bzw. 500 Mhz,
Asus oder Gigabyte-Hauptplatine,
256 MB RAM,
IDE Platte 6,4 GB
Soundblaster 128 PCI,
ATI-Grafikkarte,
CD-ROM, Floppy-Disc

Peripherie

Drucker als Netzwerkdrucker

2 x Kyocera FS-1800
2 x Kyocera FS 1200
1 x Minolta QMS Magiccolor 6100 (DIN A3+)

Scanner

1 x Epson-Expression 1640 XL mit USB und SCSI-Anschluß (DIN A3+)

Webcam

2x Modell Hyper Vcam Aiptek (OV511 Chipsatz)

CD-Brenner

Das Konzept für die Monopolkommission

- Der Client
- Der Server
- Zentraler Ansatz
- Das „Einheitlicher Client“-Konzept
- Einfache Installation und Sicherung
- Integration besonderer Sicherheitsmerkmale
- Digitale Signatur

Der Client

- natural.DESKTOP.client als Ausgangspunkt der Entwicklung
- vollwertiger PC mit lokalen Applikationen
- optisch und funktional für die intuitive Nutzung durch die Anwender gestaltet
- Verwendung vorhandener Hardware

Die Client-Funktionen

| <i>Applikationen unter Windows2000</i> | <i>Applikationen unter GNU/Linux</i> |
|--|--------------------------------------|
| MS Windows Desktop | IceWM |
| MS Office | StarOffice 6.0 |
| MS Outlook | Sylpheed |
| MS Internet Explorer | Galeon |
| Windows Explorer | GNOME Midnight Commander (GMC) |
| Scannersoftware | Xsane |
| Netmeeting | GNOMEmeeting |
| Nero, WinOnCD | CD-Roast |
| | KTeXMaker2 |
| Adobe Photoshop, Gimp | GIMP |
| Netobject Fusion | AMAYA |
| Adobe Acrobat | StarOffice 6.0 |
| Adobe Acrobat Reader | Adobe Acrobat Reader |
| WinZIP | Fileroller |
| MS Access | PostgreSQL, Perl |
| Hoppenstedt Applikation | Hoppenstedt unter WINE |



Die Server-Produkte

- *INFRAppliance* Administration Console
- *INFRAppliance* Fileserver mit Backup
- plus CUPS Printserver-Modul
- *INFRAppliance* Webserver mit Backup
- plus PHP-Groupwaremodul

Die Server-Funktionen

Produktbeschreibung

INFRAppliance Fileserver mit Backup

INFRAppliance Webserver mit Backup

INFRAppliance CUPS-Printserver-Modul
für den Fileserver mit Backup

**INFRAppliance PHP-Groupware und
Webfilespace Modul** für den Webserver mit
Backup

INFRAppliance Administration Console
inkl. Agenten für Fileserver und Webserver

Funktionalität

Er dient als zentraler Fileserver, auf dem die Benutzer ihre „home“-Verzeichnisse erhalten. Die Backup-Funktion sichert die Benutzerdaten nach verschiedenen Sicherungsarten

Basis für die zentralen Web-Applikationen, Softwareverteilung, Datenbanken (mySQL, PostgreSQL),

Printserver zur Druckaufbereitung für die Netzwerkdrucker

Dieses Modul ergänzt den Webserver um die PHP-Groupware und Webfilespace, damit die Benutzer über das Groupware-Modul die Kalenderfunktion nutzen können und über den Webfilespace leicht und wie in bisher gewohnter Form Dokumente austauschen können.

Die Admin Console ist der zentrale Ort, von dem sich die gesamte Client- und Server- Umgebung administrieren lässt. Hier wird definiert, welche Benutzer es gibt, welche Rechte die Benutzer haben, welche Applikationen den Benutzern zur Verfügung stehen und welche Einstellungen für die Applikationen getätigt werden können.

Zentraler Ansatz

- Administration der Arbeitsplätze
- Zentrale Datenhaltung
- Zentrale Softwareverteilung
- Roaming
- Zentrale Funktionalitäten

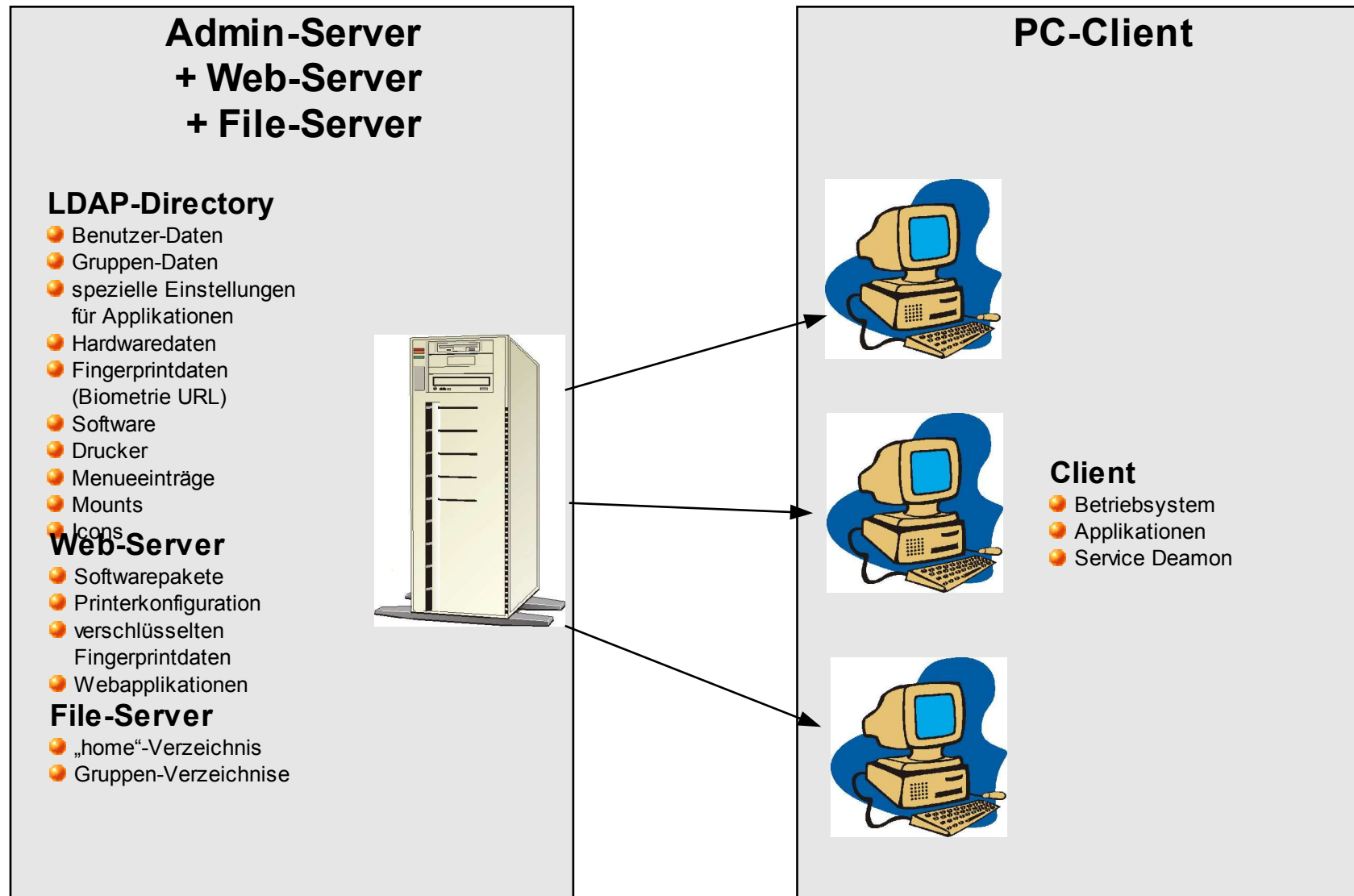
Administration der Arbeitsplätze

- Benutzerdaten
 - Name, User ID, Group IDs
- Benutzereinstellungen für Applikationen
- Die Zuweisung von im Netzwerk befindlichen Druckern
- Hardware-Konfiguration der Clients
 - MAC-Adresse der Netzwerkkarten als Client ID-Merkmal
 - automatische Hardwareerkennung
 - Grafikkarte, Grafikkartentreiber, Monitoreinstellungen

Administration der Arbeitsplätze

- Installation und Verwaltung der Client-Softwarepakete
 - Patches
 - Updates oder
 - Applikationen
- Administration ausschließlich über die INFRAppliance Administration-Console („Webmin“-Oberfläche)
- Ablage der Konfigurationsparameter im LDAP-Tree und auf dem INFR*Appliance* Fileserver in den jeweiligen Homeverzeichnissen

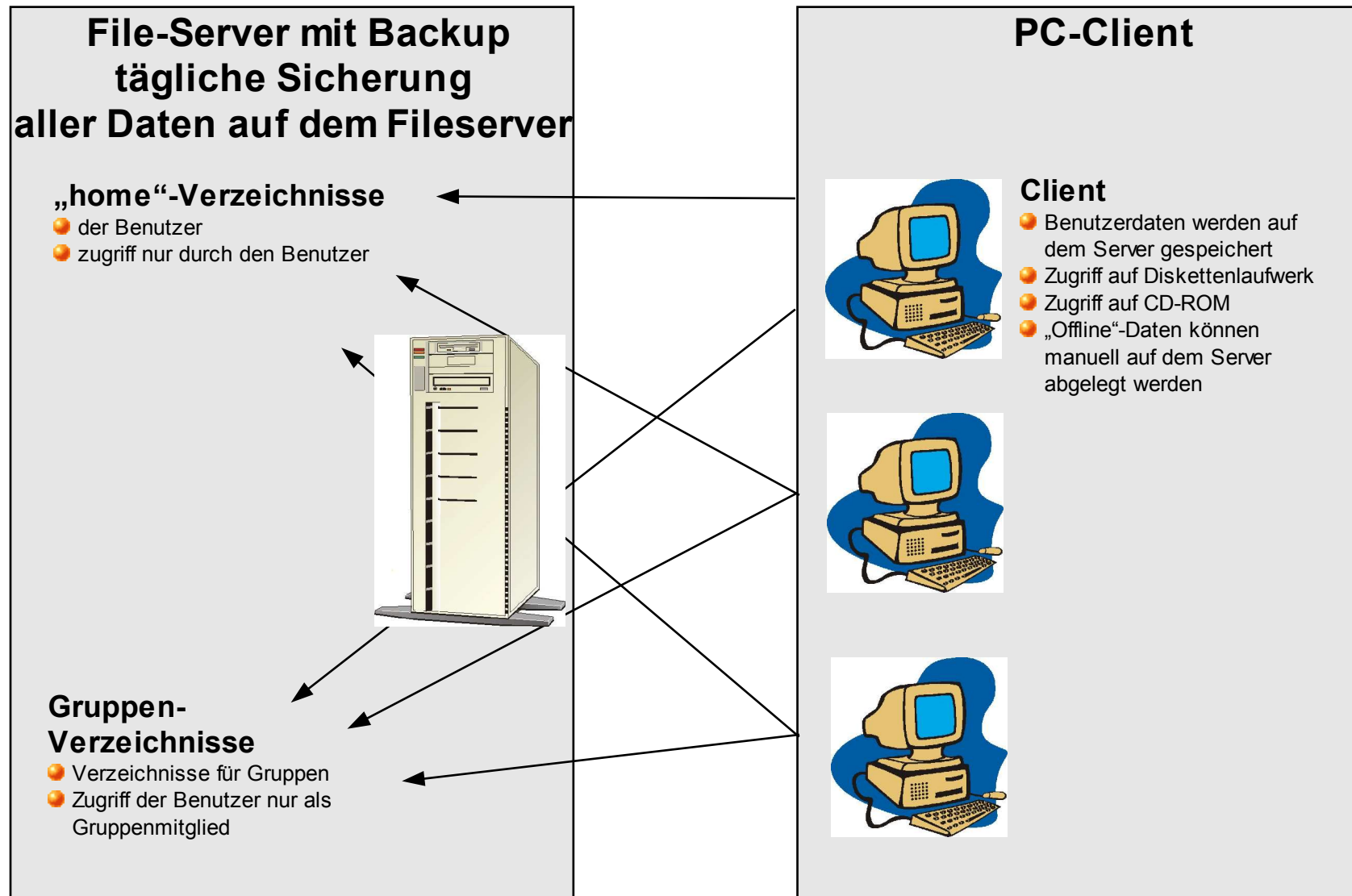
Administration der Arbeitsplätze



Zentrale Datenhaltung

- Benutzerdaten werden zentral auf dem INFR*Appliance* Fileserver mit Backup gehalten.
- Die Daten sind jederzeit wiederherstellbar.
- Der Zugriff auf die Daten auf dem Server ist durch User- und Gruppenrechte gesteuert.
- Die im Offline-Betrieb erstellten Daten können manuell durch den Benutzer in sein „home“-Verzeichnis kopiert werden.

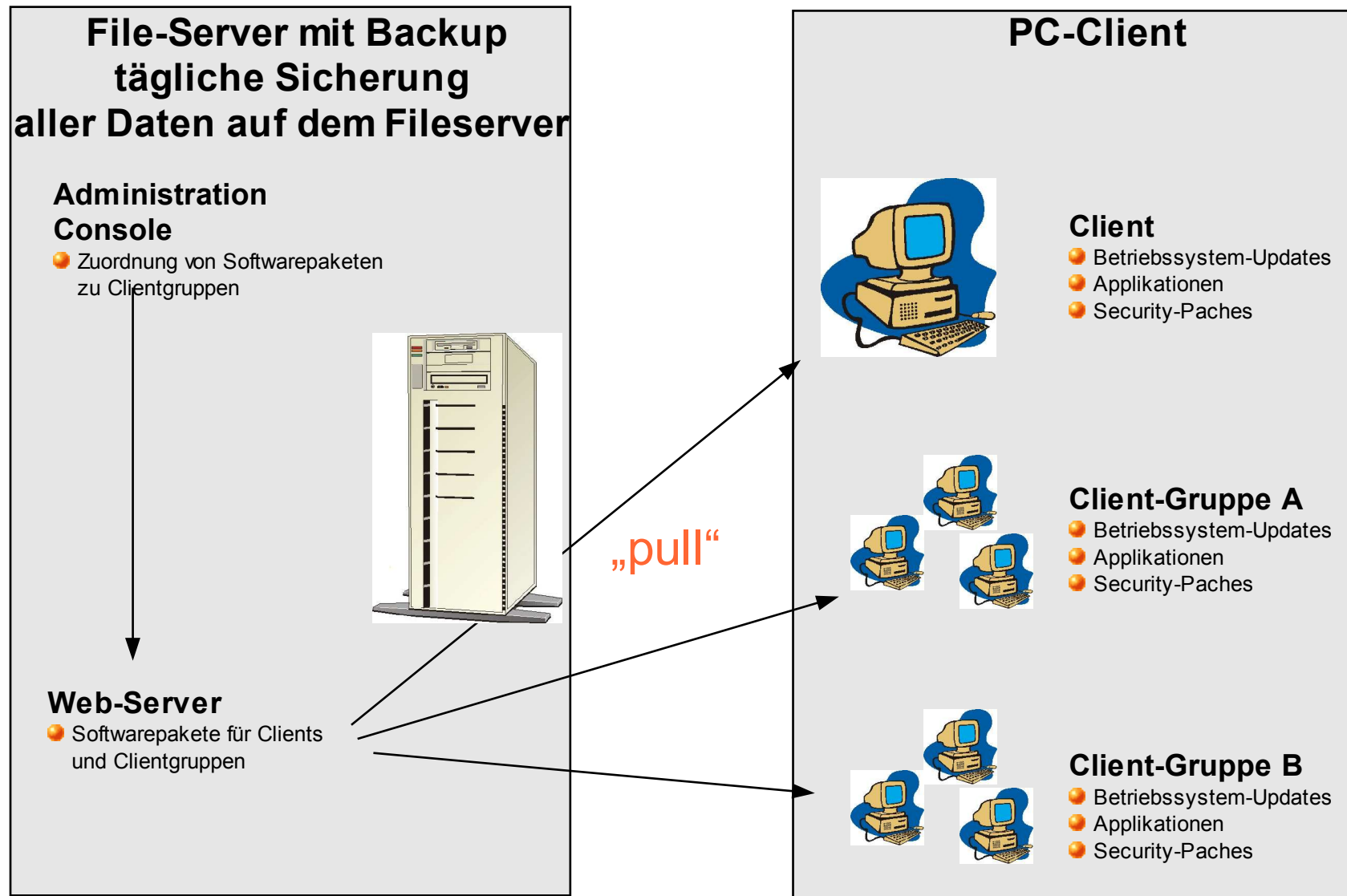
Zentrale Datenhaltung



Zentrale Softwareverteilung

- apt-get Schnittstelle der Debian Distribution
 - Betriebssystem-Updates
 - Applikationen
 - Security-Patches
- Softwareverteilung für einzelne Clients über Clientklassen

Zentrale Softwareverteilung



Roaming

- Grundsätzlich einheitlicher Softwarestand
- Benutzerabhängige Einstellungen liegen im „home“-Verzeichnis auf dem File-Server
- Laden der Daten beim Anmelden
- Anmelden an jedem Arbeitsplatz möglich
 - Individuelle Arbeitsumgebung mit
 - allen Einstellungen
 - Zugang zu allen Daten
- Roaming kann durch Zuordnung von Applikationen oder Devices zu einzelnen Arbeitsplatzrechnern stark eingeschränkt oder sogar verhindert werden

Zentrale Funktionalitäten

- Bibliotheksverwaltung
- CD-Archivierung
- Kalender
- Adressbuch

Das „Einheitlicher Client“-Konzept

- Möglichst gleiche Installation auf allen Geräten
 - Vereinfachung der Administration
 - Unterstützt Roaming
- Bildung von Gruppen gleichartiger Geräte (Clientgruppen)
 - einfache Administration von Gruppen von Geräten
 - Realisierung von differenten Client-Konfigurationen
- Einfache Anpassung an spezielle Umgebung

Einfache Installation und Sicherung

- Server
 - INFRAppliance Produkte per CD installiert
 - Wiederherstellung der jeweiligen Server-Komponenten (INFRAppliance) durch Recovery-CDs
 - Übernahme bzw. die Wiederherstellung der Benutzerdaten über die in den INFRAppliances integrierten Backup-Module.

Einfache Installation und Sicherung

- Client
 - Installation eines Clients über Installations-CD
 - Automatische Hardwareerkennung
 - manuelle Client-Installation
 - Sicherung der Daten auf einem Client nur manuell durch den Benutzer, da nur im „Offline“ Zustand Daten auf der lokalen Festplatte abgelegt werden

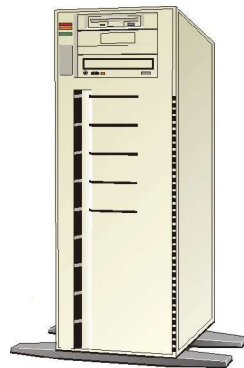
Integration besonderer Sicherheitsmerkmale

- Chipkarte
 - „Online“-Umgebung
 - „Offline“-Umgebung
- Biometrie

- Die Kombination der zwei Sicherheitsmerkmale ergibt eine besonders komfortable und sichere Anmeldung (Zutritt zu den Daten)

Funktionsdarstellung „Online“

Admin-Server + Web-Server



LDAP-Directory

- Verweis auf die Fingerprint-Daten

[2]

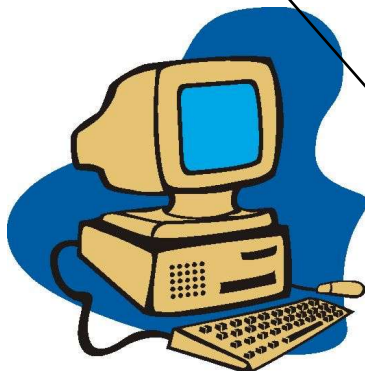
Web-Server

- verschlüsselte Fingerprintdaten

[3]

Client

- Siemens SDK für das „matching“
- PAM-Modul



[4] Schlüssel für die Fingerprintdaten

[5]

[6]

[7]

Zugriff auf

- „home“-Verzeichnis auf dem Fileserver
- „home“-Verzeichnis auf dem Client
- Gruppenverzeichnisse
- Applikationen
- digitale Signatur

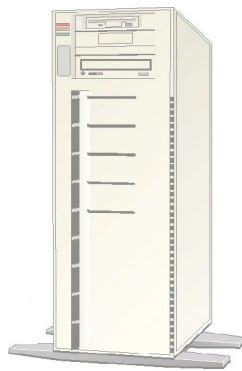
[1] Benutzername, UID



- Name (Klartext)
- UID (Klartext)
- Schlüssel für Entschlüsselung der Fingerprint-Daten
- Verschlüsseltes Passwort
- Digitale Signatur (GNUpg Schlüssel)

Funktionsdarstellung „Offline“

Admin-Server +
Web-Server



LDAP-Directory

- Verweis auf die Fingerprint-Daten

Web-Server

- verschlüsselte Fingerprintdaten



[1] Benutzername, UID

Client

- Siemens SDK für das „matching“
- PAM-Modul



[2]

Zugriff auf

- „home“-Verzeichnis auf dem Fileserver
- „home“-Verzeichnis auf dem Client
- Gruppenverzeichnisse
- StarOffice und Sylpheed
- digitale Signatur



- Name (Klartext)
- UID (Klartext)
- Schlüssel für Entschlüsselung der Fingerprint-Daten
- Verschlüsseltes Passwort
- Digitale Signatur (GNUpg Schlüssel)

Digitale Signatur

- Signierung des eMail-Verkehrs mit dem eMail-Client Sylpheed
 - Einsatz von GNUPG
 - Schlüssel befindet sich auf der Chipkarte
 - Signatur und Unterschrift erfolgt mit der Bestätigung durch den Fingerprint
- vorbereitet für SPHINX-Ägypten des BSI seitens der Chipkartenerstellung

Der Umstellungsprozess

- Qualitätsplan
- Meilensteine
- Testumgebung
- Mitarbeiterereinbindung

Die Migration

- 1. Schritt
 - Aufbau von INFRAppliance Fileserver und Webserver mit den Modulen für die Administration Console
- 2.Schritt
 - Enrollment der Mitarbeiter und Ausgabe der Chipkarten
 - Installation der Client-CD (Migration der Clients)
- 3.Schritt
 - Installation der INFRAppliance Server und Servermodule auf dem zentralen Server (Migration des Servers)

Fazit

- Unter schwierigen Rahmenbedingungen konnte eine geeignete Arbeitsumgebung für die Monopolkommission geschaffen werden
- Erhaltung der bisherigen Funktionalität
- Realisierung zusätzliche Sicherheitsfeatures
- Akzeptanz der Mitarbeiter für
 - neue Arbeitsumgebung
 - die Sicherheitsfeatures
- Die Arbeitsumgebung* ist Open Source Software (General Public License- GPL)

* bis auf das Biometrie SDK der Firma Siemens

Ausführende Unternehmen

natural  COMPUTING



Quelltext AG
Professionelle Software-Dienstleistungen

natural computing GmbH
Martener Str. 535
D-44379 Dortmund
Tel.: +49 231 6104850
Fax: +49 231 6104840
Ansprechpartner : Thomas Sprickmann Kerkerinck

SFI Technology Services AG
Stettbacher Str. 10
CH-8600 Dübendorf
Tel.: +41 1 8244900
Fax: +41 1 8244901
Ansprechpartner : Peter Stevens

Quelltext AG
Ostenhellweg 51
D-44135 Dortmund
Tel.: +49 231 9503750
Fax: +49 231 9503751
Ansprechpartner : Hans-Peter Wiedau