MKK
MAIN-KINZIG-KREIS

Main-Kinzig-Kreis

IT-Anbindung der Schulen und Betrieb der IT-Infrastruktur im Schulverwaltungsnetz

Auszüge aus dem Feinkonzept

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Zielsetzung des Dokumentes

Im Rahmen des Konjunkturpakets des Bundes und der Länder wurden dem MKK Mittel unter anderem zur Ausstattung der Schulen im Kreis zugewiesen.

Mit diesen Geldern sollen hauptsächlich „infrastrukturelle Maßnahmen“ angegangen werden. Zu diesen Maßnahmen gehört auch eine Restrukturierung des IT-Schulverwaltungsnetzes des MKK, dem 102 Schulen unterschiedlichster Größen und pädagogischer Zielsetzungen mit ca. 650 Benutzern, 530 Endgeräte und 300 Drucker angeschlossen sind.

Derzeit tragen diese Einrichtungen eine hohe Eigenverantwortung für die Erfüllung der Vorgaben des Schulträgers im EDV-Bereich und werden durch das Amt 65 des MKK planerisch und durch die Bereitstellung dedizierter IT-Services unterstützt. Diese sind jedoch sehr heterogen aufgebaut und folgen keiner klaren technischen wie organisatorischen Strategie.

In Zukunft sollen die IT-Services der Schulen durch das Amt 20, die IT-Abteilung des MKK, geleistet werden. Im Rahmen der gesetzlichen Verordnungen werden somit MKK Mitarbeiter zentral aus Gelnhausen heraus die Infrastruktur betreiben und zentral gesteuerte und homogene Services anbieten. Mit diesem Ziel ist die IT-Abteilung des MKK angetreten, ein technisches Konzept (Aufbau und Beschreibung) zu entwickeln, welches folgende Punkte beinhaltet:

- Netzwerktopologie (WAN/LAN)
- Verzeichnisdienstes (Active Directory)
- Konzeption der Front- und Backendsysteme
- Aufbau der Middleware-Komponenten
- Datenbanksysteme
- Security
- Abgleich mit dem Datenschutzbeauftragten des Landes Hessen
- Hardwarekomponenten
- Pilotierung, Migrations-, Rolloutplanung und Durchführung
- Betriebskonzept

Das Dokument beschreibt das durch die MKK IT-Abteilung erstellte technische Konzept. Es werden 102 Schulen unterschiedlicher Größe angebunden. Dazu wird ein Austausch der gesamten Infrastruktur im Bereich Client, Server, Drucker und Netzwerk (inkl. benötigter Lizenzen) geplant. Es sind weiterhin Wartungsverträge und begleitende Dienstleistungen (z.B. Rollout) berücksichtigt.

1.1 Inhaltliche Angaben

Diesem Konzept liegen folgende Informationen zu Grunde:

- Grobkonzept: „Konzept zur IT-Anbindung der Schulen und zum Betrieb (Support) der IT-Infrastruktur im Schulverwaltungsnetzt,
- Namenskonventionen im Verwaltungsnetz des Main-Kinzig-Kreis, festgelegt im Grobkonzept,
- Beschreibung der Netzwerktopologie,
- Beschreibung der Sicherheitsabgrenzungen im Verwaltungsnetz und
- Bestehendes Sicherungskonzept.

Teile aus dem bestehenden Grobkonzept wurden in dieser Ausführung zu Grunde gelegt und Abschnitte wurden in diesem Dokument verwendet.

1.2 Gültigkeitsbereich

Dieses Dokument ist gültig für das MKK - Netzwerk mit den folgenden Netzwerkbereichen:

- LUSD
- Verwaltungsnetz MKK
- DMZ
- Schulverwaltungsnetz
- Heimarbeitsplätze, angebunden über das Internet

1.3 Zuständigkeiten

Ansprechpartner:

Main Kinzig Kreis:

Sachgebietsleiter Amt 20, EDV
Herr Jens Nebenführ
Tel.: +49 (6051) 85 – 13316
eMail: Jens.Nebenfuehr@MKK.de

acentrix GmbH:

Herr Michael Heyer-Eichstädt
Tel.: +49 (89) 540 545 20
eMail.: m.heyer-eichstaedt@acentrix.de

1.4 Mit geltende Dokumente

- Grobkonzept: „Konzept zur IT-Anbindung der Schulen und zum Betrieb (Support) der IT-Infrastruktur im Schulverwaltungsnetz.
- Netzwerk.vds
- Liste Thin-Clients für Hausmeister 29.05.09.xls
- VLAN-Konzept

2 Netzwerkstruktur

2.1 Beschreibung der Netzwerkstruktur

Das WAN Konzept (Anbindung der Schulverwaltungen an das Rechenzentrum des MKK) ist kein Bestandteil dieser Unterlage und wird in einer separaten Ausschreibung betrachtet.

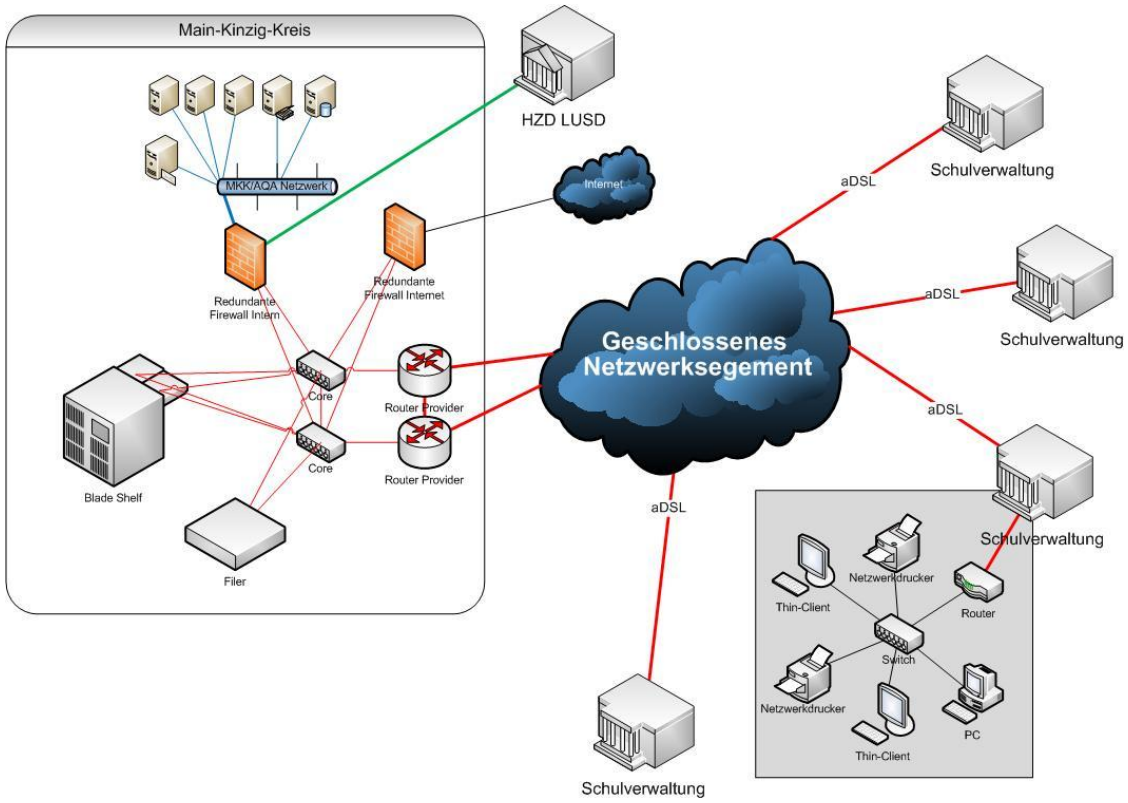

Abbildung 1 Netzwerkstruktur MKK – Schule

2.1.1 Schulverwaltungsnetz des MKK (Rechenzentrum)

Das Schulverwaltungsnetz des MKK (Rechenzentrum) ist ein eigenständiges, auf TCP/IP basierendes Netzwerk. Dieses Netzwerk wird ausschließlich für die Schulverwaltungen benutzt.

Die Netzwerkstruktur des Rechenzentrums (Serverbereich) ist redundant über zwei Core Switches aufgebaut.

Die Core Switches sind mit den Blade-Shelfs über zwei redundante Verbindungen mit je 10Gbit verbunden.

Die Verbindung der zwei Core Switches zu dem NetApp Filer wird über eine 2GBit Leitung realisiert.

Die Router und deren Anbindung an das MPLS-Netz sind redundant ausgelegt.

Es wird „Statisches Routing“ und OSPF zum abgleich der Routen zwischen MKK-Netz und Schulverwaltungsnetz (mit VRRP redundant auf den Core Switches) eingesetzt.

2.1.2 Schulverwaltung

Pro Schule wird ein eigenständiges auf TCP/IP basierendes Netzwerk aufgebaut. In allen Schulen werden Switches vom gleichen Typ eingesetzt.

Das Amt 20 EDV hält entsprechende Netzwerkkomponenten als Reserve (Cold Standby) vor, um bei Ausfall die benötigten Komponenten austauschen zu können.

2.2 Authentifizierung

Die Authentifizierung der Mitarbeiter an das Schulverwaltungsnetz des MKK erfolgt über das Standardprotokoll IEEE 802.1X an einem RADIUS Server. Der RADIUS Server überprüft die Authentifizierung gegen das Microsoft Active Directory. Die Authentifizierung im Active Directory erfolgt über Benutzerkennungen und Computerkonten.

Die Geräte werden über Zertifikate authentifiziert. Die Ausstellung der Zertifikate erfolgt über die interne Stammzertifizierungsstelle, sowie die Zwischenzertifizierungsstelle des MKK. Nähere Informationen sind im Kapitel 4.1 beschrieben. Geräte die eine Zertifikatsbasierte Authentifizierung nicht unterstützen sollten werden mittels MSCHAPv2 authentifiziert werden.

Geräte, die nicht authentifiziert werden können, werden über ein Quarantäne-VLAN verbunden.

2.3 Trennung der Netze gemäß Datenschutzbeauftragten

Das pädagogische Netz ist physikalisch vom Schulverwaltungsnetz getrennt.

Das Schulverwaltungsnetz wird durch eine Firewall mit Paketfilter vom MKK Netzwerk getrennt. Dadurch wird nur ein dedizierter Datenverkehr zwischen den Netzen zugelassen. Die Firewall ist redundant ausgelegt. Die für die Kommunikation der beiden Netzwerke benötigten Protokolle und zu öffnenden Ports werden während der Pilotierung ermittelt und im Rahmen des Betriebsprozesses dokumentiert.

2.4 QoS

QoS wird in dem Schulverwaltungsnetz möglich sein. Es wird als optionaler Bestandteil angeboten und kann nach Bedarf aktiviert werden (Definition im externen WAN-Konzept).

Die höchste Priorität enthält das ICA-Protokoll. In der nächsten Stufe wird der Druckdatenstrom und SNMP bevorzugt behandelt. Alle anderen Protokolle werden nicht priorisiert.

2.5 VLAN

Das Schulverwaltungsnetz wird in VLAN Bereiche aufgeteilt.

Die Zuordnung der VLANs zu den Schulen werden nach der Ausschreibung der WAN Anbindung bestimmt.

Es werden verschiedene VLANs für Endgeräte eingesetzt:

- Endgeräte (Drucker und Clients)
- Telefonanlagen
- Router Provider (Transportnetz), usw.

3 Infrastruktur

3.1 Virtualisierungsplattform

Die Bereitstellung der Server erfolgt auf einem Xen Server 5.5 virtualisiert.

Die XenServer werden über Citrix Storage Link mit dem NetApp Filer verbunden.

Die virtuellen Maschinen werden auf mehrere Storage Repository verteilt. Die Zuteilung zu einem Storage Repository wird in dem Kapitel **Fehler! Verweisquelle konnte nicht gefunden werden.** dargestellt. Als hauptsächliches Kriterium ist hierbei die Sicherung der einzelnen Maschinen zu bewerten.

Alle XenServer der Schulverwaltung werden in einem Pool zusammengefasst. Hierbei besteht unter anderem die Möglichkeit eine Live Migration der Virtuellen Maschinen zu starten, sowie die Verteilung der VMs über alle Virtualisierungshosts zu vereinfachen.

Für jedes eingesetzte Betriebssystem wird ein Template angelegt das als Basis für die Server verwendet wird.

Die Installation und Grundparametrisierung des Xen Virtualisierungs-Servers erfolgt gemäß Best Practice Vorgaben des Herstellers Citrix. Eine Nachjustierung des Xen-Servers mit den passenden Praxiswerten für den MKK wird während der Pilotierung durchgeführt und im Rahmen des Betriebsprozesses dokumentiert.

3.2 Fileservice / Storage

Als zentrales Speichersystem wird ein NetApp System Modell 2050c mit 20 x 450 GB Festplatten eingesetzt.

Das Speichersystem stellt das Storage für die Virtualisierungsplattform mittels ISCSI-Protokoll zur Verfügung. Die Dateiablage der Schulen wird über das CIFS Protokoll zur Verfügung gestellt.

Es wird ein Active/Active-Cluster mit zwei Filerköpfen eingesetzt. Ein Filerkopf wird für ISCSI und der andere für das CIFS genutzt. Für alle Volumes des Filers wird das Deduplication Feature eingeschaltet.

Jeder Kopf erhält ein Raid–DP Aggregat mit einer HotSpare Festplatte.

Von den verbleibenden 14 Festplatten erhält der SAN-Kopf 4 und der NAS-Kopf ebenfalls 4 Festplatten. Die restlichen 6 Festplatten werden vorerst als Ausbaureserve definiert und den Köpfen nicht zugewiesen.

3.2.1 Dateiablage

Auf dem NAS-Aggregat wird ein Flex-Volume mit einer Snapshotreserve von 15 % angelegt.

Für jede Schule wird ein Qtree bereitgestellt. Innerhalb des Qtrees wird ein Ordner und eine Freigabe mit der Ordnungsnummer der Schule angelegt.

In der Testumgebung werden für den jeweiligen Qtree Quotas in der Größe von 150 % des bisherigen Speicherplatzes der Schule angelegt. Die jeweilige Freigabe wird im Profil des Users als Laufwerk „H:“ gemappt.

Auf das Laufwerk „H:“ wird der bisherige Datenbestand der Schule kopiert. Vor der Migration der Daten wird eine Reorganisation der Daten durch die betreffenden Schulen durchgeführt. Die Daten werden redesignt und konsolidiert. Die Rechte- und Gruppenstrukturen der Ablage werden anhand von der im Rahmen des Migrationskonzepts zu erstellenden Checklisten, vor der Migration mit der Schule verbindlich vereinbart.

Die persönliche Freigabe wird als Laufwerk „P:“ dem User zur Verfügung gestellt. Auf diesen persönlichen Ablageort hat nur der User Zugriff.

Weitere Schulübergreifende Projektordner (IT-Lenkungskreis, Sekretariate, Hausmeister…) werden bei Bedarf angelegt und als Laufwerk: „I:“ bereitgestellt.

3.2.2 Laufwerkszuordnungen

Folgende Laufwerke werden für die User verbunden:

Laufwerk	Name	Bemerkung
H:\	Ablage	Pro Schule individuelle Ablage
P:\	Persönliches Laufwerk	Laufwerk das nur dem User zur Verfügung steht
T:\	Transfer	Öffentliches Laufwerk auf das alle Schulen Zugriff haben und als Austausch und Transferlaufwerk benutzt werden kann.

Tabelle 1: verbundene Laufwerke

3.2.3 Storage Repository

Die physikalischen Server arbeiten, nach derzeitigem Stand, nur mit ihrem lokalen Speicher. Ein Zugriff auf den SAN-Bereich des Filers ist nicht notwendig.

Die Server der Virtualisierungsplattform werden per Citrix Storage Link an den SAN-Bereich des Filers angebunden. (Dieses Volume hat eine Größe von 400 GB und eine Fractional Reserve von 100% und die darin befindliche LUN eine max. Größe von 200 GB.)

3.3 Namenskonvention

3.3.1 Organisationseinheiten

Jede Schule wird als Organisation Unit (OU) in der Schuldomäne (Schule.MainKinzig.local) angelegt. Die jeweilige OU wird nach der Ordnungsnummer und dem Kürzel der Schule, sowie des Ortes benannt. Hierbei können die jeweiligen Namen auch gekürzt werden.

3.3.2 Gruppennamen:

Gruppennamen werden wie folgt abgebildet:

- <Art>_<Vorsilbe>_<Kürzel Schule>_Name_<Nachsilbe>

Bedeutung der einzelnen Bereiche:

Kürzel	Bemerkung
GG	Globale Gruppe
LG	Lokale Gruppe

Tabelle 2: Gruppenarten

Kürzel	Bemerkung
ADM	Administrative Gruppen
APP	Applikationsgruppe
RES	Ressourcengruppe
SEC	Berechtigungs- / Securitygruppe
FOL	Filesharezugriff
PRT	Zugriff auf Drucker
PST	Postfachzugriff

Tabelle 3: Gruppenvorsilben

Der Name muss eindeutig sein und dem jeweiligen Zweck zugeordnet werden können.

Die Berechtigungsgruppen sind lokale Gruppen und erhalten eine Nachsilbe, die den jeweiligen Zugriff beschreibt.

3.3.3 Anmeldename (Login)

Der Anmeldename der Benutzer wird aus max. 7 Stellen des Nachnamens plus min. 1 Stelle des Vornamens gebildet. Die Länge des Benutzernamens beträgt 8 Zeichen

3.3.4 Geräte

Geräte werden durch eine Vorsilbe und die Inventarnummer des Gerätes benannt.

Kürzel	**Bemerkung**
SPCxxxxxx	FAT-Client
STCxxxxxx	Thin-Client
SDRxxxxx	Drucker

Tabelle 4: Namenskonventionen Geräte

3.3.5 Server

Die Namensgebung der Server sieht folgende Regel vor:

SVS-<Rolle>-<lfd. Nr.>

Die Server der Schulverwaltung werden mit Kürzel SVS versehen.

3.4 Active Directory

Die Domäne wird unter der vorhandenen Rootdomäne "mainkinzig.local" aufgebaut. Als Basis kommt hier Windows Server 2008 R2 zum Einsatz.

3.4.1 Infrastruktur

Der DNS Service wird als Dienst auf den Domänen Controllern implementiert. Die einzelnen DNS Zonen werden als Active Directory integrierte Zonen eingepflegt.

Die DHCP Services werden ebenfalls als zusätzliche Dienste auf den Domänen Controllern eingepflegt. Bei der Planung der passenden IP-Subnetze wird eine Redundanz berücksichtigt, so dass bei einem Ausfall eines DHCP Server genügend Adressen zur Verfügung stehen.

3.4.2 Struktur

Das Active Directory wird als flache Baumstruktur mit einer Root- und weiteren Subdomänen angelegt. Die Struktur enthält unter der Root-Domäne nur eine weitere Ebene mit der Subdomäne „schule.mainkinzig.local“.

Jede Schule wird als Organisation Unit (OU) in der Schulungsdomäne (schule.mainkinzig.local) angelegt. Innerhalb der OU gibt es weitere OUs für Gruppen, Benutzer und Geräte.

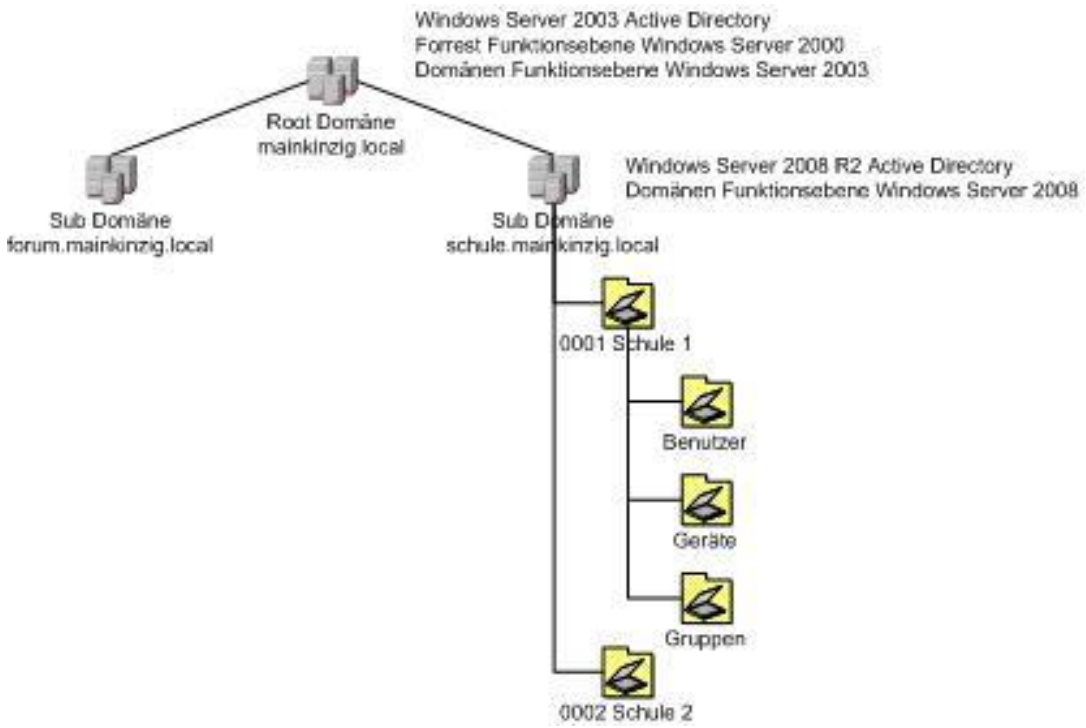

Abbildung 2: Schematische Darstellung der Domänenstruktur

3.4.3 Gruppenrichtlinien

Es werden unterschiedliche Gruppenrichtlinien (GPOs) für Geräte (PC/Server), Domänenbenutzer und Terminalserverbenutzer angewendet.

Die Gruppenrichtlinien der Forum-Domäne bilden die Grundlage der für die Schulen zu erstellenden GPOs.

3.4.4 Erweiterte Benutzerrechte

Die Mitarbeiter des Helpdesks des Main-Kinzig-Kreises erhalten erweiterte Benutzerrechte für die Schuldomäne. Sie haben die Möglichkeit Kennwörter zu vergeben und gesperrte Konten zu entsperren.

3.5 Exchange

Hierzu wird ein separater Exchange-Server analog des vorhandenen Exchange Servers des MKK im Schulverwaltungsnetz aufgebaut.

Für das Schulverwaltungsnetz wird eine Sub-Domäne schule.mkk.de eingerichtet.

Die Anwender aus dem Schulverwaltungsnetz erhalten eine Email Adresse: vorname.name@schule.mkk.de

3.6 Terminalserver

Die Terminalserver werden virtualisiert. Es kommt Citrix XenApp in der Version 5.0 zum Einsatz.

Die Basisfarm wird auf Windows 2008 64-bit aufgebaut. Die Anwendungen werden vorwiegend über das Applikation-Streaming zur Verfügung gestellt. Anwendungen, die nicht unter 64 Bit lauffähig sind, werden auf einer Fallback Terminalserverfarm vorgehalten. Diese wird unter Windows Server 2003 32-bit betrieben.

Die User bekommen einen Desktop veröffentlicht und die weiteren Applikationen werden über den PNAgent in diesen Desktop integriert. Die Anwendungen liegen entweder auf einem XenApp Server der Basisfarm oder auf der Fallbackfarm.

Für die Terminalserver unter Windows 2008 / 64bit wird folgende Konfiguration vorgesehen:

Konfiguration	Einstellung
CPU	4
RAM	8 GB (kann je nach Ressourcenbelastung erweitert werden)
HDD	35 GB Systempartition
Homeserver	Keiner (ermöglicht so die dynamische Zuweisung und die Live Migration)
VCPU priority	Normal
Autoboot	Nein
Advanced Options	Optimiert für Citrix XenApp
Network	Schule_Server VLAN

Tabelle 5: VM Konfiguration der Terminalserver

Der Citrix Datastore liegt auf einem Microsoft SQL Server 2008. Hierfür wird ein dedizierter Server im Schulverwaltungsnetz eingesetzt.

Im Netz des MKK wird ein neuer Lizenzserver installiert, der die Lizenzen für das Forum und der Schulverwaltung vorhält.

Das Webinterface, das nur zur Bereitstellung der config.xml für die Agents und den Data Collector der Farm genutzt wird, befindet sich zentral auf einem Domänencontroller.

Der Zugriff auf die Application Silos wird mit dem Program „Neighborhood Agent“ über den Published Desktop hergestellt. Die Application Silos werden mittels Load Balancing ausfallsicher ausgelegt.

Citrix XenApp bietet die Möglichkeit Sessions der User zu spiegeln um einen effizienteren Support zu gewährleisten. Hierbei muss der Benutzer der Spiegelung explizit zustimmen bevor der Administrator die Session sieht.

3.7 Datenbanken

Der Microsoft SQL Server 2008 (64Bit) wird auf einem virtuellen Windows Server 2008 R2 (64Bit) betrieben.

Der virtuelle Server hat mindestens 4GB Arbeitsspeicher und es stehen mindestens 4 Prozessoren zur Verfügung.

Das Datenverzeichnis liegt auf einem separaten Volume.

Folgende Datenbanken werden angelegt:

- GPUntis
- Citrix Information Store
- Scout Enterprise
- CynapsPro (Endpoint Security)

Auf weitere Datenbanksysteme wird wenn möglich verzichtet, um die Komplexität gering zu halten.

3.8 Drucken

3.8.1 FullService-Druckkonzept

In der Verwaltung des MKK wird seit 2008 ein FullService-Druckkonzept eingesetzt. Dieses wird für den Schulverwaltungsbereich übernommen und sieht folgendes vor:

HP Remote Monitoring ist das HP Supply Chain System, das Verbrauchsmaterialstatus, Wartungsstatus sowie die Anzahl und Art der gedruckten Seiten der Netzwerkdrucker erfasst und regelmäßig an die HP Datenbank berichtet. Dieser Service ermöglicht die proaktive Durchführung von Wartungen und Lieferung von Verbrauchsmaterial frei Verwendungsstelle, ohne dass der Anwender in Aktion treten muss.

Durch die Verwendung der Fernüberwachungssoftware werden durch HP keine personenbezogenen Daten erfasst. Sämtliche erfassten, statistischen und technischen Daten werden ausschließlich zum Zweck der Bereitstellung dieses Überwachungs- und Meldungsservices verwendet. Der MKK hat jederzeit Einblick welche Daten an HP versandt werden.

Die hierfür erforderliche Hardware wird von HP zur Verfügung gestellt und installiert.

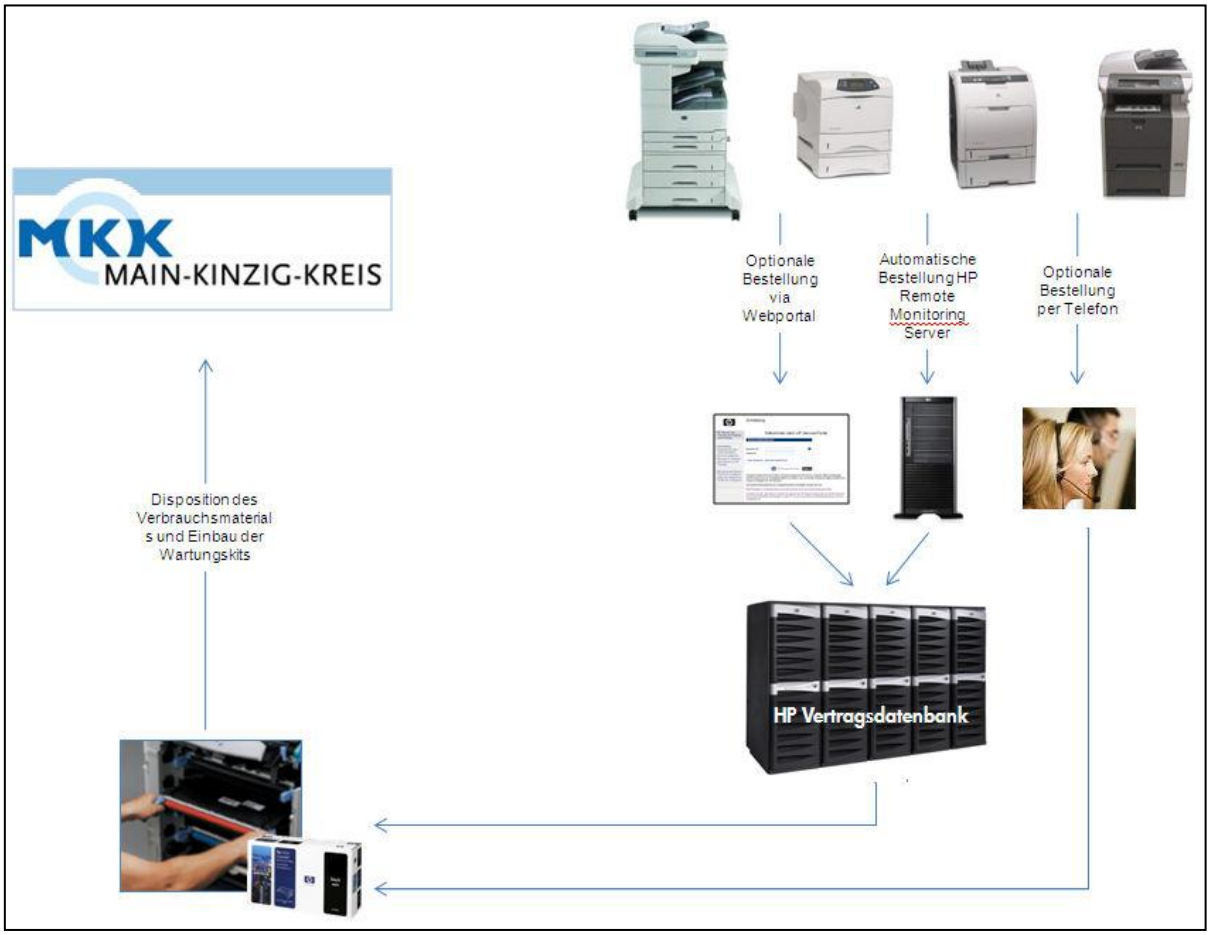

Abbildung 3 Abbildung 4 Schematische Darstellung HP-Remote Monitoring

Verbrauchsmaterialversorgung

HP beliefert den MKK mit den erforderlichen Original Laserdruckkassetten. Die Lieferung erfolgt innerhalb von 48 Stunden an den jeweiligen Standort (Wareneingang) des Gerätes. Der Abruf erfolgt durch HP Remote Monitoring vollautomatisch. Optional kann das Verbrauchsmaterial auch manuell per Telefon oder per Service Portal bestellt werden. Die HP Verbrauchsmaterialien unterliegen den Bestimmungen des Blauen Engels.

Entsorgung Tonerkartuschen:

Die gebrauchten Kassetten werden zur Wiederverwertung an HP zurückgeben. HP stellt auf Wunsch Sammelbehälter zur Verfügung oder die Kartuschen können einzeln zurück versandt werden. Die Versandkosten werden von HP übernommen.

Wartungen:

Um die Leistungsfähigkeit und Druckqualität der Produkte über die Vertragslaufzeit zu erhalten, sind Verschleißteile in bestimmten Wartungsintervallen zu ersetzen. Die Wartungsmaßnahmen umfassen Wartungskomponenten, alle übrigen Verschleißteile und die damit verbundenen Dienstleistungen.

Austausch von Wartungskomponenten: Die Wartungsmaßnahmen werden durch einen autorisierten HP Service Techniker am nächsten Arbeitstag durchgeführt. Die Veranlassung der Wartungseinsätze erfolgt durch HP Remote Monitoring vollautomatisch.

Alle vorhandenen Drucker in der Schule werden automatisch per GPO gemappt. Der Benutzer kann sich aus diesem Pool an Druckern seinen Standarddrucker auswählen Der Zugriff auf Drucker außerhalb der eigenen Schule ist im Standard durch die Berechtigungsstruktur nicht möglich.

Alle Drucker werden über einen zentralen Druckserver mit dem HP Universal Printer Driver PCL6 Version 5.0.1 betrieben. Weitere Druckertreiber werden auf dem Printserver und den angeschlossenen Clientsystemen nicht zum Einsatz kommen.

3.8.2 Secure Printing (über universal Druckertreiber)

Um dem Anwender die Möglichkeit zu geben, seine Ausdrucke zu schützen, ist im HP Universal Druckertreiber die Option, seinen Ausdruck mit einer PIN zu versehen, wählbar. Diese Funktion wird, wenn kritische Informationen ausgedruckt werden sollen, beim Absenden des Druckjobs gewählt. Dadurch wird der Zugriff Unbefugter vermieden. Der Ausdruck wird mit der Eingabe einer PIN-Nummer auf der Festplatte des Druckers gesichert und erst nach der Eingabe der Pin am Drucker ausgedruckt. Hierbei ist zu berücksichtigen, dass diese Option nur bei den Multifunktionsgeräten, die über eine Festplatte zum Speichern des geschützten Druckjobs verfügen, nutzbar ist.

3.8.3 Druckstromkomprimierung / Benötigte Bandbreiten

Hierzu wird parallel ein eigenständiges Druckkonzept bereitgestellt.

3.9 Warenkörbe

Die Warenkörbe definieren die Anwendungen die den Mitarbeitern der Schulverwaltung bereitgestellt werden.

Warenkorb	Anwendungen / Funktionen
Warenkorb Basic	Published Desktop mit Internet Explorer 8, Plugins (Java, Flash, Silverlight), Adobe Reader
Warenkorb Plus	Standard Basis mit Office 2007 und Paint.net
Fachanwendungen	Stundenplansoftware (gpUntis / DaVinci / …), LUSD, Facility Management
Sonderanwendungen	Nero, Corel Draw, Mind Manager, IDV

Tabelle 6: Warenkörbe

3.10 Clients

3.10.1 Beschreibung der Use Cases

Benutzer werden, je nach Aufgaben, zu Gruppen (Rollen) zusammengefasst. Den Benutzergruppen werden standardisierte Arbeitsplätze zugeordnet. Standardisierte Arbeitsplätze werden durch die Hardware, den zugeordneten Softwarepaketen und der netzseitigen Anbindung definiert. Im Folgenden sind die Use Cases (Funktion/Endgeräte, denen Benutzergruppen zugeordnet werden können:

Nr.	Funktion	Endgerät	Zugriff	Anwendung
1	Standardarbeitsplatz	Thin-Client	Intern	Schuldesktop mit Published Application
2	Heimarbeitsplatz	Privat PC	Extern	Homeoffice-Desktop mit Published Application
3	Infoterminal	Thin-Client	Intern	Schuldesktop mit speziellen Gruppenrichtlinien
4	Datenstation	FAT-Client	Intern	FAT Client mit Brennfunktion und USB Anschluss zum Austausch von Daten.

Tabelle 7: Use Cases (Funktion und Endgerät Kombination)

Es kann keine generelle Zuordnung von den Mitarbeitern zu den Use Cases (Funktion/Endgeräte) getroffen werden, d.h. die Mitarbeiter einer Benutzergruppe können auf unterschiedlichen Endgeräten mit unterschiedlichen Funktionen arbeiten.

3.10.2 Clienttypen (Endgeräte)

Dieser Abschnitt beschreibt die standarisierten Hardwarekomponenten, die als Arbeitsplätze eingesetzt werden können.

Typ	Funktion
Thin-Clients (TC)	Als Standardarbeitsplätze werden Thin-Clients eingesetzt. Thin-Clients sind reine Endgeräte (Terminals) der zentralen Terminalserver. Ihr lokales Betriebssystem ist eine Linux-Variante.
Datenaustauschstation (FAT-Client)	Die Datenaustauschstation ist ein PC-Arbeitsplatz und wird genau einmal pro Schulverwaltungen zum Einsatz kommen. Auf diesem PC wird zur Sicherheit die Festplatte mittels Cryption Pro HDD verschlüsselt. Dieser PC ist mit einem DVD und CD - Brenner ausgestattet um der Anforderung des HKM nachzukommen. Dieser wird benötigt um Prüfungsdaten, welche per Download vom HKM zur Verfügung gestellt werden, auf einem externen Medium zu schreiben

Tabelle 8: Auflistung der Clienttypen

3.10.3 Standardisierte Arbeitsplätze (Funktion)

Im Folgenden werden die standardisierten Arbeitsplätze aufgeführt:

3.10.3.1 Standardarbeitsplatz

Der Standardarbeitsplatz ist der typische Schulverwaltungsassistentinnen-, Hausmeister- und Schulleiterarbeitsplatz mit Office, E-Mail, Fachsoftware und Drucken.

3.10.3.2 PC-Arbeitsplatz

Pro Schule wird mindestens ein PC in dem Verwaltungsnetz aufgestellt. Diese PC-Arbeitsplätze werden den Personen zur Verfügung gestellt, die mit externen Datenträgern arbeiten müssen.

3.10.3.3 Heimarbeitsplatz

Der Heimarbeitsplatz ist eine Zugriffsmöglichkeit von Zuhause und wird den Lehrern der Schulverwaltung auf Anforderung durch den Schulleiter zur Verfügung gestellt. Hierzu wird parallel ein Heimarbeitsplatzkonzept mit einer Tokenbasierten Zweifaktor - Authentifizierung erstellt.

3.10.3.4 Infoterminal

An dem Infoterminal können Schüler sich direkt mit der Stundenplansoftware verbinden und Informationen über den aktuellen Stundenplan aufrufen. Dieses Infoterminal wird mit einem anonymisierten Account, der ausschließlich den Zugriff auf den Viewer für das Stundenplan Programm bereitstellt, aufgestellt. Dieses Terminal sollte allerdings in einem „gesicherten“ Bereich stehen, der unter Beaufsichtigung steht. (z. B. Sekretariat)

3.10.3.5 LUSD-Zugriff für die Noteneingabe

Anonymisierter Account für den Zugriff auf die LUSD für die Eingabe der Noten (ein Account pro Schule). Dieser Account soll den Lehrern einen Zugriff auf die LUSD ermöglichen und hat ausschließlich einen Zugriff auf die LUSD und darf sich nur an einem Thin-Client anmelden.

Für die Noteneingabe gibt es zwei Varianten. Hier ist die Variante 1 die bevorzugte Methode, da sie dem aktuellen Stand der LUSD entspricht und erheblich weniger technischen Aufwand in der Bereitstellung durch den Schulträger erfordert.

Variante 1 (Standard).

(Direkteingabe) Bei der Variante 1 geben die Lehrer der Schule die Noten direkt in die LUSD ein. Es existieren 2 Anmeldemöglichkeiten um auf die LUSD zuzugreifen:

Der Lehrer meldet sich mit dem anonymen Account an einem Thin Client des Schulverwaltungsnetzes an.

Der Lehrer meldet sich über die Heimarbeitsplatzlösung von jedem beliebigen Rechner aus dem pädagogischen Netz mit einem Internetzugang an.

Hierfür muss der LUSD-Beauftrage der Schule die Lehrer in der LUSD namentlich anlegen (inklusive den entsprechenden Berechtigungen), damit diese die Noten eingeben können. und die entsprechenden Berechtigungen vergeben

Dies ist die geeignetste Lösung, da die Noten nicht in xml-Dateien zwischengespeichert werden müssen. Mögliche Fehlimporte werden somit ausgeschlossen.

Variante 2 (Der externe Notenclient wird per Citrix zur Verfügung gestellt)

Die Lehrer der Schule können sich mit einem anonymen Account der Schule an einem Thin Client des Schulverwaltungsnetzes anmelden und dort die Noten mit dem externen Notenclient erfassen oder die geplante Heimarbeitsplatzlösung aus dem pädagogischen Netz heraus nutzen. Der externe Noten-Client legt die Daten in dem bereitgestellten Tauschordner ab.

Diese Variante birgt mögliche Fehlerquellen durch den Einsatz des externen Notenclient. So kann eine xml-Datei nur einmal geöffnet und bearbeitet werden. Die Schule sollte auf ein mögliches Fehlverhalten dieser Variante aufmerksam gemacht werden.

3.10.3.6 Benutzergruppen / Rollen

Es kann außer bei den ersten zwei Benutzergruppen keine weitere generelle Zuordnung von Mitarbeitern zu den Use Cases getroffen werden.

Standardarbeitsplatz

(Schulleitung, Sekretariat, Abteilungsleiter, Stufenleiter)

Springer

Benutzer (Hausmeister, Schulleitung, Sekretariat) die für mehrere Schulen tätig sind werden mit einem eigenen Account pro Schule ausgestattet. Dies ist notwendig, um die einwandfreie Zuordnung der Daten zu einer Schule zu gewährleisten.

Personalrat

Für den Personalrat wird nur nach Anforderung ein personenbezogener Account angelegt (muss im Einzelfall geklärt werden.) Mit diesem Account kann der Benutzer sich dann an einem vorhandenen Arbeitsplatz im Verwaltungsbereich anmelden. Separate Thin-Clients werden für den Personalrat nicht aufgestellt.

Hausmeister

Für die insgesamt 100 Hausmeister wird jeweils ein personenbezogener Account angelegt. In einigen definierten Hausmeisterbüros werden Thin-Client (ca. 50 Stück) aufgestellt (max. ein Thin-Client pro Hausmeisterbüro), siehe Liste Thin-Clients für Hausmeister 29.05.09.xls). Für Hausmeister werden keine separaten Drucker vorgesehen. Ausdrucke können auf dem Drucker im Sekretariat vorgenommen werden.

Sonderfall Förderschulen

In den Förderschulen besteht die Anforderung, dass Lehrer, die nicht Teil der Schulverwaltung sind, die Möglichkeit bekommen in der Schulverwaltung personenbezogene Gutachten über ihre Schüler zu erstellen.

Diesen Lehrern werden personenbezogene Accounts in der jeweiligen Schule zur Verfügung gestellt. Diese Accounts besitzen nur Zugriff auf die Applikation Word. Die Anmeldung der Lehrer erfolgt über die Heimarbeitsplatzlösung mittels eines Tokens und nicht über einen ThinClient. Zum Speichern dieser höchst vertraulichen Daten wird jedem Lehrer ein verschlüsseltes Laufwerk zur Verfügung gestellt. Auf dieses Laufwerk bekommt die Rolle des Schulleiters der entsprechenden Schule ebenfalls Zugriff.

3.10.4 Thin-Client (Standardverwaltungsplatz)

Der Standardarbeitsplatz in der Schulverwaltung besteht aus einem Thin Client mit Zugriff auf die zentrale Terminalserverfarm der Schulverwaltung. Über diese Serverfarm können alle benötigten Anwendungen dem Benutzer schnell und performant zur Verfügung gestellt werden.

Ausstattung:

- Thin Client
- Monitor mindestens ein 22 Zoll Widescreen LCD
- Tastatur
- Optische Maus

3.10.5 FAT-Client

Ein PC-Arbeitsplatz ist eine Sonderlösung für die Schulverwaltungen. Der PC wird benötigt um externe Datenträger (USB-Stick, usw.) anzuschließen. Weiterhin ist der PC-Arbeitsplatz mit einem DVD und CD-Brenner ausgestattet, um einer Anforderung des HKM nachzukommen. Dieser wird benötigt, um Prüfungsdaten, die per Download vom HKM zur Verfügung gestellt werden, auf CD oder DVD zu brennen. Auf diesem PC sollten lokal keine Daten abgelegt werden, da diese PC-Systeme nicht in das Datensicherungskonzept integriert sind. Zur Sicherheit gegen Diebstahl wird die Festplatte mittels Cryption Pro HDD verschlüsselt. Da alle für die Schulverwaltung notwendigen Anwendungen zentral zur Verfügung gestellt werden, ist ein PC-Arbeitsplatz (FAT-Client) kein definierter Standardarbeitsplatz des MKK. Der FAT-Client soll so selten wie möglich verwendet werden. Standardmäßig muss allerdings für jede Schule ein PC-Arbeitsplatz eingeplant werden, um der o.g. Brennfunktion für CD und DVD gerecht zu werden.

Ausstattung:

- PC mit Windows XP
- Monitor mindestens ein 22 Zoll Widescreen LCD
- Tastatur
- Optische Maus

Die Rechteverwaltung wird über Gruppenrichtlinien das Active Directory realisiert. Dabei bekommen die Anwender nur „Benutzer“-Rechte ohne administrative Berechtigungen auf das lokale System.

Anwender bekommen zusätzlich die „Nero Burn Rights“, für den Zugriff auf den CD-/DVD-Brenner auf dem lokalen PC-Arbeitsplatz der Schule.

Der Zugriff auf externe Devices wird über Endpointsecurity gesteuert und protokolliert.

Auf FAT-Clients werden keine Server gespeicherten Profile eingesetzt. Hier wird es nur ein lokales Profil geben.

Die Patches für die Microsoft Produkte werden per WSUS eingespielt.

Die Patches und Updates für den Virenscanner TrendMicro OfficeScan werden über die zentrale Managementoberfläche des Virenscanner-Softwarepakets eingespielt.

Software auf dem FAT-Client

- Windows XP SP3
- Nero Burning Rom
- Nero Burn Rights
- Aktueller Citrix Client
- TrendMicro Office Scan
- Device Pro
- Cryption Pro HDD
- Internet Explorer (inkl. Silverlight, Java, Flash)
- .net Framework 2.0 (wegen Vergleichsarbeiten)
- Office-Viewer
- Acrobat Reader

Alle anderen Softwarepakete werden als Published Desktop zur Verfügung gestellt.

3.10.6 Heimarbeitsplätze

Den Usern wird ein Remotezugriff über eine Token basierte Authentifizierungslösung zur Verfügung gestellt. Hierbei wird auf die vorhandene Hardware des Users aufgebaut. Für den Zugriff auf das Verwaltungsnetz wird ein Browser, sowie für die Authentifizierung ein Token, benötigt. Die lokale Hard- und Software wird als Wirtsystem genutzt. Der Zugriff auf das Verwaltungsnetz (Citrix Session) erfolgt dann völlig autark vom Wirtsystem. Lokale Devices (HDD, USB, Printer) werden nicht „gemounted“ (stehen der Citrix-Session nicht zur Verfügung). Damit wird die Kopplung des lokalen Heimarbeitsplatzes mit dem Verwaltungsnetz vermieden und die notwendige Datensicherheit hergestellt. Bis auf die Implementierung eines Plugins (activeX bzw. Java) erfährt der Heimarbeitsplatz keine Systemänderungen. Das Citrix-Plugin wird, wenn nicht schon installiert) während der „Einwahl“ mittels Browser bereitgestellt und kann vom Anwender, ohne große DV-Kenntnisse, selbst installiert werden.

Ein zentraler Service durch den MKK zur Betreuung der Heimarbeitsplätze muss nur in geringem Umfang zur Verfügung gestellt und kann im Normalfall durch den Helpdesk erbracht werden.

Weiterführende Informationen sind im „Konzept Anbindung Heimarbeitsplätze“ zu finden.

3.11 Anwendungen

3.11.1 Frontend

Jedem Benutzer werden Standard-Softwarepakete und die jeweils benötigten Fachsoftwarepakete zur Verfügung gestellt.

Standardsoftware:

- Microsoft Office 2007
- Internet Explorer 7
- Adobe Acrobat Reader
- Paint.NET

Fachsoftware:

- GP Untis
- DaVinci
- LUSD
- Mind Manager
- Microsoft Publisher
- Weitere Software

3.12 Backup

3.12.1 Integration in vorhandenes Backup

Das zentrale Schulverwaltungsnetz der MKK wird durch die vorhandene Backup-Infrastruktur gesichert.

Die Backup-Lösung stellt die Wiederherstellung der Server im Falle von logischen und physikalischen Datenverlusten sicher. Die eingesetzte Backup-Lösung ist kein Ersatz für eine Archivierung der Daten.

Die MKK setzt die Backuplösung Tivoli Storage Manager in der Version 5.5.3 ein.

- Die zu sichernden Daten werden zuerst auf den Festplatten des Datensicherungsservers (Tivoli-Server) gesichert (Backup to Disk).
- Anschließend werden die Daten auf eine virtuelle Tape-Library (NetApp VTL-300) übertragen.
- Die Daten werden dann von der virtuellen Tape-Library auf eine physikalische LTO-4 Tape-Library kopiert/gesichert und in einem Datentresor aufbewahrt

- Die Daten auf den Festplatten des Tivoli-Servers werden nach erfolgreicher Kopie gelöscht.

Auf den zu sichernden Servern (Domänencontroller, Exchange-, SQL-, Print-, spezielle Application-Silo-Server) wird der TSM-Client installiert. Die Sicherung der Systeme wird in den Abend-/Nachtstunden durchgeführt. Bei dem ersten Initialen Sicherungslauf wird der TSM-Client mit gesichert. Ab diesem Zeitpunkt erfolgt täglich eine inkrementelle Sicherung des Clients. Die Sicherung des Schulverwaltungsnetzes wird zwar über das gleiche System wie das des MKK-Netzes, jedoch auf physikalisch getrennten Bändern erstellt.

Zusätzlich wird die Snapshot-Technologie von NetApp genutzt. Es werden pro Tag zwei Snapshots erzeugt, die auf dem Filer verbleiben und zur schnellen Rücksicherung von Ablagedaten genutzt werden.

Die virtuellen Server werden über die NetApp Snapshot-Technologie über NDMP auf den TSM-Server gesichert.

3.13 Hardwaresysteme

3.13.1 Server

Als Serversystem wird die Blade Technologie von Fujitsu eingesetzt.

Als System kommt das Fujitsu Blade Shelf BX900 mit BX920 S1 zum Einsatz.

- Blade Shelf und Server werden mithilfe von Fujitsu Bordmitteln (Managementblade und ServerView) gemanagt
- Die Einbindung in SCOM erfolgt später.

3.13.2 Thin Clients

Standardmäßig soll jeder Arbeitsplatz mit einem Thin-Client ausgestattet werden.

Als Hardware ist aktuelle das Modell S550 des Herstellers FTC vorgesehen.

Das Mengengerüst wird ermittelt nach Abschluss der Inventarisierung.

Alle Thin-Clients werden über die zentrale Administrationsoberfläche „Scout Enterprise“ verwaltet.

Die Datenbank liegt auf dem MS-SQL Server 2008 System der Schulverwaltung.

Diese Software erlaubt es die Thin-Clients zentral zu administrieren, zu konfigurieren, fern zu warten und zu aktualisieren.

Auf den ThinClients besteht die Möglichkeit den Zugriff auf USB Schnittstellen zu ermöglichen. Der Schulleiter entscheidet und haftet dafür, ob die USB-Ports an den ThinClients seiner Schule entweder für den schreibenden und / oder lesenden Zugriff geöffnet werden, oder diese komplett abgeschaltet werden.

3.13.3 FAT-Clients

Pro Schule wird ein Fat-Client als Datenaustauschstation eingesetzt.

3.13.4 Drucker

Folgende Druckertypen werden eingesetzt:

Druckertyp	Modell	Funktion
Multifunktionsgerät DIN A4	HP Laserjet M3035XS MFP	Drucken, Kopieren und Scannen in A4 Schwarzweiß, Faxen in Schwarzweiß, Hefteinrichtung
Multifunktionsgerät DIN A4 Farbe	HP Color LaserJet CM3530	Drucken, Kopieren und Scannen in A4 Farbe und Schwarzweiß, Faxen in Schwarzweiß
Multifunktionsgeräte DinA3 Farbe	HP Color LaserJet CM6030f MFP	Drucken, Kopieren und Scannen in A3 Farbe und Schwarzweiß, Faxen in Schwarzweiß
Laserdrucker DinA4	HP LaserJet P2055dn	Drucken A4 Schwarzweiß
Laserdrucker DinA4 Farbe	HP Color LaserJet CP2025dn	Drucken A4 Schwarzweiß und Farbe

Tabelle 9: Auflistung der Druckertypen

Das Mengengerüst wird nach Abschluss der Inventarisierung in den Schulen ermittelt.

Die Drucker werden über die zentrale Managementoberfläche „HP Web Jet Admin“ und „HP Digital Sending“ Software konfiguriert und administriert.

Für alle Drucker soll der HP Universal PCL6 Druckertreiber zum Einsatz kommen.

4 Security

4.1 Public-Key-Infrastruktur

Um die Funktionalität der Netzwerkauthentifizierung mittels 802.1x sicherzustellen, wird eine Public-Key-Infrastruktur aufgebaut.

Hierfür wird eine neue, eigenständige Stammzertifizierungsstelle für die Umgebung des MKK eingerichtet. Diese wird kein Domänenmitglied sein und im Anschluss an die Konfiguration offline genommen. Zusätzlich wird eine Ausgabe Zertifizierungsstelle in der Domäne der Schulverwaltung eingerichtet. Diese befindet sich im Gegensatz zur Stammzertifizierungsstelle auf einem Domänenmitgliedsserver und wird online gehalten, da hier dynamisch die Zertifikate und Sperrlisten generiert werden.

4.2 Netzwerkauthentifizierung

Um dem Sicherheitsanspruch der Schulverwaltung zu genügen, muss genauestens geprüft werden, wer Zugang zum Netz bekommt. Hierdurch wird ein Missbrauch der Server-Dienste von vornherein ausgeschlossen. Es wird zur Lösung die Netzwerkauthentifizierung 802.1x implementiert. Der IEEE-802.1x-Standard stellt eine wichtige Weiterentwicklung der Netzsicherheit dar, da er es ermöglicht, Benutzer schon an einem Netzzugangs-Port zu identifizieren. Dabei erfolgt die Authentifizierung des Users einmalig an einem zentralen Radius-Server. Der Service ist in RFC 2865 spezifiziert. Der Switch übernimmt hier die Rolle als Client des Radius-Servers.

Die Kommunikation zwischen Radius-Client und -Server wird dadurch gesichert, dass sich beide Kommunikationspartner gegenseitig durch ein "Shared Secret" authentifizieren und den Datentransfer verschlüsseln. Radius unterstützt viele Authentifizierungsmöglichkeiten wie zum Beispiel PAP, CHAP, EAP oder Unix-Login und kann viele erweiterbare Attribute zu einem Benutzer verarbeiten und übermitteln. Es wird im Schulverwaltungsnetz das EAP genutzt.

Das Extensible Authentication Protocol (EAP) wurde ursprünglich für das Point-to-Point Protocol (PPP) entwickelt und ist in den RFCs 2284 und 2716 spezifiziert. Mit Hilfe von EAP können zwei Kommunikationspartner vor der eigentlichen Authentifizierung aushandeln, welche Authentifizierungsmethode angewandt werden soll. EAP beschreibt in einem einfachen Frage-Antwort-Verfahren den Austausch der Authentifizierungsdaten vom Benutzer zum Authentisierungs-Server und dessen Antwort. Dabei können beliebige Authentifizierungsmechanismen wie Kerberos, SecurI oder Zertifikate benutzt werden. EAP wird entweder in Verbindung mit PPP verwendet oder als Protokoll-Framework zum Authentifizierungsdatenaustausch in anderen Protokollen, so etwa auch in IEEE 802.1x.

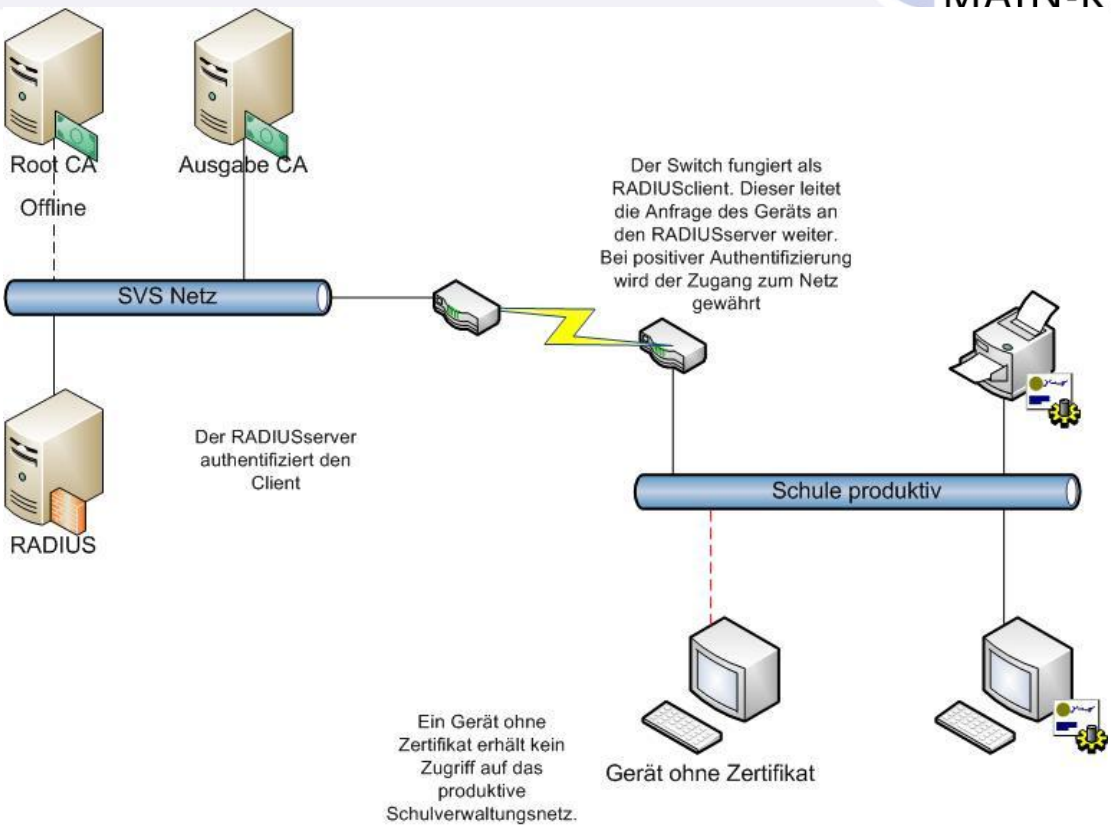

Abbildung 4: Schematische Darstellung der 802.1x Authentifizierung

4.2.1 Funktionsweise Extensible Authentication Protocol

Das Extensible Authentication Protocol (EAP) fordert das Gerät (FatClient, ThinClient oder einen Drucker) auf, sich zu authentifizieren. Seine Authentisierungsinformationen werden zunächst an den Port beziehungsweise den Authenticator weitergeleitet. Sobald dieser die Daten empfangen hat, leitet er sie an den Radius-Server weiter. Dieser identifiziert anhand der hinterlegten Profile das Gerät, das heißt, er entscheidet, ob das Gerät Zugriff auf das Schulverwaltungsnetzt erhält. Der Radius-Server übernimmt die Authentifizierung nicht selbst, sondern leitet die Daten an das Active Directory weiter. Im Falle einer nicht erfolgreichen Authentifizierung bekommt der Authenticator eine entsprechende Information, die dafür sorgt, dass der Port nicht aktiviert wird, also den Modus Authentication on/Port off einnimmt. Hierbei erhält das Gerät keinen Zugriff auf die angefragten Services. Wenn dagegen die Authentifizierung erfolgreich verläuft, wird die entsprechende Meldung, die der Radius-Server an den Switch oder Access Point zurücksendet, mit der Funktionsbezeichnung "Radius/EAP Success" versehen. Der Authenticator schaltet danach sofort den entsprechenden Port für den uneingeschränkten Datentransport frei.

4.2.2 Authentifizierung durch gegenseitige Zertifikate

Das EAP-Transport Layer Security Protocol ist eine Erweiterung und besteht aus einer Kombination von EAP mit SSL. Es verlangt eine gegenseitige zertifikatsbasierende Authentifizierung des Servers und des Clients auf der Transportschicht.

4.2.3 Authentifizierung durch Username/Passwort und Server-Zertifikat

Das EAP-Tunneled Transport Layer Security Protocol erweitert EAP-TLS um eine sehr praktische Funktion. Bevor sich das Gerät gegenüber dem Server authentifizieren muss, wird mit dem Server-Zertifikat ein sicherer TLS-Tunnel zwischen Gerät und Authentisierungs-Server dynamisch aufgebaut. In diesem Tunnel kann sich dann das Gerät beim Authentisierungs-Server mittels Username/Passwort identifizieren.

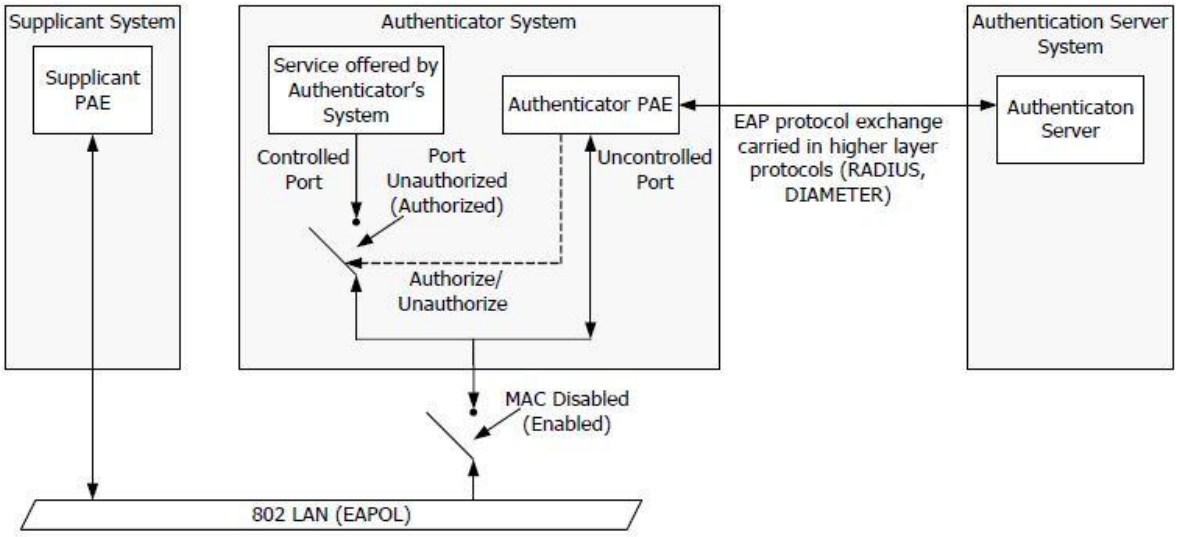

Abbildung 5 Prozessschaubild EAP

4.3 Starke Authentifizierung

Hier wird für die Heimarbeitsplätze ein eigenes Konzept entworfen, welches eine starke Authentifizierung beinhalten wird.

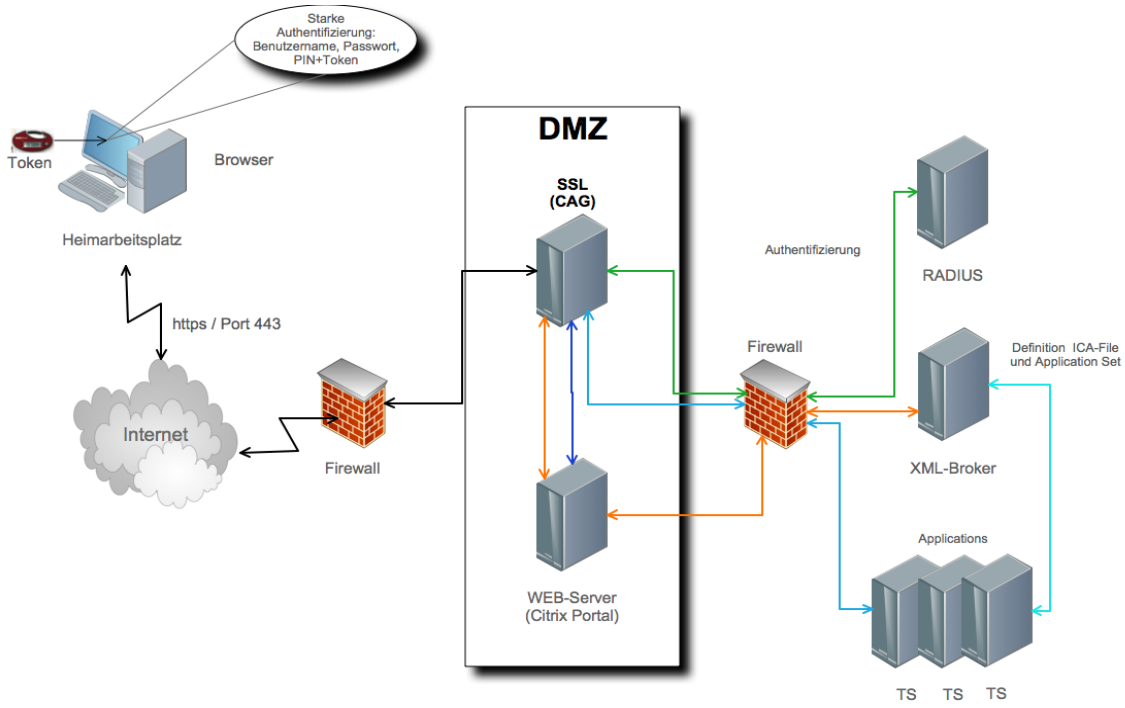

Abbildung 6 Beschreibung der Authentifizierung der Heimarbeitsplätze

4.4 Endpoint Security

Die Endpoint Security soll durch die Software-Suite von CynapsPro realisiert werden. Sie wird den Umgang mit externen Medien (Bspw. CD/DVD/USB Stick) beinhalten. Das Konzept für Aufbau und Integration ist nicht Gegenstand dieses Feinkonzepts, sondern wird separat erstellt.

4.5 Virenschutz / Malware

Das vorhandene Konzept zur Abwehr von Schadsoftware und Viren wird von dem MKK Netz auf das Schulverwaltungsnetz erweitert.

4.5.1 Clients

Der Virenschutz auf den Clients in Schulverwaltungsnetz wird durch den aktuellen TrendMicro-OfficeScan sichergestellt. Dieses Produkt wird durch eine zentrale Managementkonsole verwaltet. Daraus ergeben sich die folgenden Vorteile:

- Der OfficeScan-Client ist ein „Realtime-Scanner“ und bietet somit einen vorbeugenden Virenschutz.
- Das Management und Konfiguration aller OfficeScan-Clients erfolgt zentral.

- Die Benutzer können den OfficeScan-Client nicht um konfigurieren, da diese Option nicht zur Verfügung steht. Es kann allerdings ein manueller Suchlauf angestoßen werden.
- Zentrales stündliches Download der neusten Virenpattern und aktive Verteilung an die OfficeScan Clients.
- Der Versand von Meldungen an die Administratoren, bei der Entdeckung eines Virus erfolgt automatisch.
- Softwareupdates werden zentral von der Managementkonsole auf alle OfficeScan Clients verteilt. Ist ein Computer beim Verteilen des Updates nicht eingeschaltet, so wird dies automatisch nachträglich vorgenommen.
- Das Reporting erfolgt zentral in der Managementkonsole

4.5.2 Exchange

Der Exchange-Server wird durch TrendMicro-Scan-Mail-Exchange (SMEX) geschützt. Der Virenscanner befindet sich auf dem Exchange-Server und scannt den E-Mailverkehr aktiv nach Viren. Zusätzlich werden nachts alle E-Mail Postfächer gescannt.

Zusätzliche Funktionen sind:

- Spamschutz
- Blocken von E-Mail-Anhängen: Sollte ein Dateianhang (.exe usw.) aus der Email entfernt werden, wird dieser in Quarantäne genommen und 10 Tage lang gespeichert. Der Anhang in der Mail wird durch eine Nachricht ersetzt. Der Anwender wird über den Vorgang der Quarantäne informiert und gebeten, sich binnen 10 Tagen bei der IT-Hotline zu melden. Meldet sich der Anwender innerhalb dieser Frist nicht, wird der Anhang unwiderruflich gelöscht.

4.5.3 Server und Terminalserver

Auf den dedizierten Servern und Terminalservern der Schulverwaltung wird der TrendMicro OfficeScan Client installiert. Dieses Produkt wurde inzwischen für Server freigegeben und durch Citrix zertifiziert. Hier bietet es denselben Funktionsumfang wie auf dem Client. Die Ausnahme ist, dass der Benutzer auf dem Terminalserver keinen manuellen Suchlauf anstoßen kann. Hier werden die Server so eingerichtet, dass wöchentlich ein kompletter Suchlauf die Festplatten des Servers untersucht.

4.5.4 Lizenzierung

Diese beiden Produkte von TrendMicro werden im Paket zusammen erworben. Dies hat den Vorteil, das nur einmal alle Benutzer lizenziert werden müssen und nicht für beide Produkte separat.

4.5.5 Virenscanner für NetApp Filer

Der Suchlauf über die Daten auf dem Filer wird einmal täglich in der Nacht durchgeführt. Der Suchlauf wird von einem externen, mit dem Filer verbundenen Server sichergestellt. Hier muss darauf geachtet werden, dass durch den Suchlauf das Feld „Letzter Zugriff“ nicht verändert wird und das eine zweite Scan-Engine eingesetzt wird um einen zweigleisigen Antivirenschutz sicher zu stellen.

4.5.6 Virenschutz in der Firewall

Der Datenfluss über das Firewall-System ins Internet wird mittels VirusBuster (Kaspersky) nach Viren und Malware durchsucht. Der Virenschutz dient der Absicherung der Clients und Server im http / https / ftp Verkehr über den zentralen Proxy

Die Absicherung der Exchangesysteme erfolgt zusätzlich zum bestehen SMEX System

4.6 Gesicherte Kommunikation LAN / WAN

- In der Ausschreibung des WAN ist die Verschlüsselung des Datenverkehrs innerhalb des MPLS Netzes optional mit angefragt.
- Eine mögliche Option ist IPSec.
- Das genutzte Protokoll ICA wird bereits standardmäßig ausreichend verschlüsselt übertragen und bietet hierdurch einen sehr guten Schutz.

4.7 Auditing

Das Auditing wird im Projekt SCOM behandelt.

4.8 Monitoring

Das Monitoring wird im Projekt SCOM behandelt. Die entsprechenden Parameter werden nach der Pilotierung definiert und an das Projekt SCOM übergeben.

4.9 Gesicherter Internetzugriff

4.9.1 Anbindung an die vorhandene dreistufige Firewall

Die Anbindung der Schulnetzwerke erfolgt direkt mittels separaten VLANs (siehe VLAN-Konzept) am inneren Interface der Firewall. Über diesen Zugriff wird sowohl der Web als auch der FTP Zugriff an den bestehenden redundanten Proxy-Servern (Bluecoat Proxy SG) geregelt.

4.9.2 Web-FTP-Read Zugriff über Proxy

Der Zugriff auf FTP / HTTP / HTTPS – Seiten wird über das bestehende Contentfiltering Konzept abgebildet. Hierzu werden die ADS Gruppen (ADMIN, POWERUSER,

STANDARD, FTP-USER) in der Schulverwaltungsdomäne angelegt. Die Authentifizierung auf dem Domaincontroller(-n) wird über den Authentifizierungsdienst „BlueCoat Authentication Agent“ ermöglicht.

Die Freischaltung von blockierten Inhalten wird über die „Blockpage“ des Proxys durchgeführt. Die Liste mit den geblockten Inhalten liegt im Amt 20. Der Browser erlaubt einen lesenden Zugriff auf FTP–Server.

4.9.3 FTP-Write Zugriff über Proxy

Der schreibende FTP-Zugriff wird über zwei weitere AD-Gruppen geregelt, welche eine Citrix Freigabe für einen Filezilla-Client bereit stellen und eine weitere um die Berechtigung im Proxy abzubilden.

Ein separater Filezilla-Client ist notwendig, da der InternetExplorer keine explizite FTP-Proxy Authentifizierung unterstützt.

4.9.4 Protokollierung des Internetverkehrs

Es erfolgt eine Protokollierung im Sinne des §143 TKGS.

Folgende Inhalte werden aufzeichnet und für 6 Monate gespeichert:

- Datum
- Benutzer
- Aufgerufene Webseite
- ADS-Gruppenberechtigung
- Kategorie der Webseite
- URL des aufgerufenen Inhalts

4.9.5 Zugriff auf verschlüsselte FTP (SCP) Verbindungen.

Der Zugriff auf verschlüsselte FTP Verbindungen wird nicht über den Proxy geregelt, sondern explizit auf der Firewall freigegeben.

4.9.6 Virenscanning innerhalb der Firewall

Innerhalb der Firewall wird für folgende Protokolle ein Virenscanning vorgenommen:

- FTP(21)
- HTTP(80)
- SMTP(25)

Der Virenscan für HTTPS-Verbindungen über SSL-Offloading ist in Planung.

4.9.7 Zugriff auf sonstige externe Anwendungen

Ein Zugriff für/auf andere Anwendungen erfolgt nach vorheriger Absprache mit dem Amt 20 und wird über den externen Partner (Change request für Firewall an externe Dienstleister) freigegeben.

5 Glossar

Begriff	Erklärung
Deduplication Feature	**Deduplizierung**, auch **Data-Deduplication, Datendeduplizierung** (engl. Deduplication), ist ein Prozess, der redundante Daten identifiziert und eliminiert. Der Prozess komprimiert wie andere Verfahren auch die Datenmenge, die von einem Sender an einen Empfänger geschickt werden. Hierbei werden nach Herstellerangaben in Abhängigkeit von der Datenstruktur und dem wiederholten Transport ähnlicher Daten Kompressionsfaktoren von 1:500 erreicht.
TS	Terminalserver
TS-Farm	Verbund aus mehreren Terminalservern, die in der Regel im Load-Balancing betrieben werden.
Load-Balancing	Lastausgleich zwischen Servern.
Thin-Client	Systemeinheit (Minicomputer i.d.R.) zum Zugriff auf eine zentrale Verarbeitungseinheit (TS). Programme werden nicht auf der Systemeinheit sondern zentral auf TS ausgeführt.
IDV	Individuelle Daten Verarbeitung. Anwendungen die nur einzelne Schulen einsetzen und diese in Eigenverantwortung betreiben.
MPLS	Multi Protocol Label Switching (MPLS), ermöglicht die verbindungsorientierte Übertragung von Datenpaketen in einem verbindungslosen Netz entlang eines zuvor aufgebauten („signalisierten“) Pfades. Dieses Vermittlungsverfahren wird überwiegend von Betreibern großer Transportnetze eingesetzt, die Sprach- und Datendienste auf Basis von IP anbieten (große Internetprovider).
Cluster	Mindestens zwei Server, die im Cold-Standby oder Hot-Standby eine Hochverfügbarkeit bieten. D.h., fällt ein Server aus, übernimmt je nach Variante der zweite Server alle Aufgaben.
HA	High Availability = Hochverfügbarkeit
FAT-Client	Eigenständiger Computer mit lokal installierter Software.
starke Authentifizierung	Zwei-Faktor Authentifizierung Der Benutzer authentisiert sich über zwei unabhängige Wege an dem entsprechenden System (z.B. physisches Token/Smartcard und Passwort).