
# Projektdokumentation

## Migration einer NIS Umgebung nach LDAP mit Integration der Accounts in einen Samba DC

12. Mai 2003

Christian Wenke
Beentweg 20
26 135 Oldenburg

Kuratorium OFFIS e. V.
Escherweg 2
26 121 Oldenburg

# Inhaltsverzeichnis

# Tabellenverzeichnis



# Abbildungsverzeichnis

# 1 Planung

## 1.1 Ausgangssituation

Der OFFIS FuE[1]-Bereich „Eingebettete Hardware-/Software-Systeme“ hat ca. 35 Mitarbeiter (MA) und 15 Wissenschaftliche Hilfskräfte (WiHi). Der Bereich hat 3 Administratoren, davon zwei nur halbtags beschäftigt und einen Auszubildenden.

Die Forschungsaktivitäten des Bereichs gliedern sich in drei Arbeitsgruppen:

- **System Design Methodik (SDM)**

  Diese Gruppe beschäftigt sich mit Methoden und Werkzeugen für den objektorientierten Entwurf eingebetteter Systeme.

- **Systemanalyse und -optimierung (SAO)**

  Die Arbeitsgruppe Systemanalyse und -optimierung beschäftigt sich mit der Verlustleistungsabschätzung und -optimierung von Eingebetteten Systemen schon im Entwurfsstadium. Das dazu entwickelte Toolset ORINOCO wird hierbei sehr erfolgreich eingesetzt.

- **Design Center (DES)**

  Das Design Center entwickelt unter Einbeziehung von Forschungsergebnissen und Werkzeugen der angegliederten Forschungsgruppen in enger Zusammenarbeit mit Partnern aus der Wirtschaft konkrete eingebettete Systeme.

Alle drei Gruppen sind auf Werkzeuge aus dem EDA[2]-Bereich angewiesen. Die Produkte der Marktführer (Synopsys, Cadence und Mentor) laufen (noch) hauptsächlich nur auf Solaris.

Neben Solaris kommen auch noch MS Windows 2000 und NT 4 sowie Linux als Betriebssystem zum Einsatz: Windows wird hauptsächlich für die üblichen Büroanwendungen (MS Office, Lotus Notes, etc.) aber auch zur Software-Entwicklung genutzt, Linux hingegen als extrem flexible UNIX-Entwicklungsplattform für eigene Software. Strategische Plattform für die hier entwickelten EDA-Tools ist derzeit noch Solaris, die Entwicklung selbst läuft aber größtenteils unter Linux und Windows.

## 1.2 Ist-Analyse

Zentraler Server ist eine SUN Enterprise 250 mit Samba als Fileserver in einer einfachen Konfiguration (kein Domain-Controller), hat lprng als Drucksystem und ist konfiguriert als NIS-Server für die Solaris-Systeme.

Das zentrale Usermanagement der Solaris-Systeme ist per NIS realisiert. Hier existieren einheitliche Accounts für Mitarbeiter und WiHis.

Die Mitarbeiter haben je einen eigenen eigenständigen PC mit Linux und/oder Windows. Hier sind für die Mitarbeiter jeweils lokale Accounts eingerichtet.

Ein Teil der WiHis teilt sich einen kleinen Pool mit Linux-Rechnern. Das Verteilen der Accounts auf diesen PCs wird zur Zeit über ein einfaches Shellscript realisiert, dass die /etc/passwd, /etc/shadow und die /etc/group auf die Clients kopiert.

[1] FuE → Forschung und Entwicklung

[2] EDA → Electronic Design Automation, Computergestützte Entwurfsautomatisierung bei der Entwicklung von Mikrochips, siehe z.B. auch c’t 7/2003 S.86-91

## 1.3 Problemstellung

Auf den Arbeitsplatzrechnern existiert – vom WiHi-Pool abgesehen – kein zentrales Accountmanagement. Dies ist sehr unübersichtlich und verursacht vermeidbaren administrativen Aufwand bei regelmäßigen Aufgaben wie dem Neuaufsetzen eines Systems, beim Tausch von Rechnern zw. Mitarbeitern o.ä. Vor allem beim Klonen von Rechnern ist noch recht viel Nacharbeit nötig, bis das System für den Mitarbeiter fertig ist.

Dazu ist das bestehende NIS-System alt und relativ unsicher im Vergleich zu neueren Systemen, wie z.B. LDAP oder Microsofts „Active Directory“, was bei den vertraulichen Daten (u.a. Chip-Prototypen von Projektpartnern wie Bosch, Siemens/Infineon, ARM, etc.) auf dem Fileserver eine wichtige Rolle spielt.

## 1.4 Anforderungskatalog

Aus den vorhin erwähnten Problemen mit dem aktuellen Zustand ergeben sich folgende Anforderungen an das neue System:

- Zentrale Benutzerverwaltung
- Unterstüzung von Solaris, Linux und Windows auf Client-Seite
- Verwaltung nach Möglichkeit auch von allen drei Client-Betriebssystemen aus
- Sicherheit der Passwörter bei der Übertragung und gegenüber angemeldeten Benutzern

## 1.5 Alternativen

Für die Realisierung einer zentralen Benutzerverwaltung kommen prinzipiell folgende Lösungen in Frage:

- Microsoft Active Directory
- Sun ONE Directory Server
- NIS
- OpenLDAP
- Samba als Domain-Controller

Microsofts **„Active Directory“** basiert auf einer Kombination aus LDAP als Verzeichnisdienst, Kerberos zur Authentifikation und DNS zur Namensauflösung und ist nur für reine Windows-Umgebungen geeignet. Aus sicherheitstechnischer Sicht ist die Verwendung von Kerberos als sehr gut zu bewerten.

Der **„Sun ONE Directory Server“** ist der zentrale LDAP-Verzeichnisdienst von Suns neuer Schlüsseltechnologie „Sun ONE[3]“. Der Sun ONE Directory Server kann zur Datenübertragung SSL/TLS verwenden, daher auch hier keine Sicherheitsbedenken.

[3] Sun ONE → „Sun Open Net Environment“

**NIS** („Network Information System“) ist ein mittlerweile schon recht altes System zur zentralen Verwaltung von Benutzern Rechnernamen, Netgroups und anderen Dingen für UNIX-artige Systeme. NIS ist auf den RPC-Portmapper angewiesen; dadurch und durch die Tatsache, dass hierbei keine wirkliche Verschlüsselung bei der Übertragung von Informationen verwendet wird, ist dieses System als sicherheitstechnisch bedenklich einzustufen.

**OpenLDAP** ist eine freie Implementation des LDAP-Protokolls inklusive LDAP-Server und vielen anderen nützlichen Tools, ebenfalls für UNIX-artige Systeme. Auch OpenLDAP beherrscht die verschlüsselte Kommunikation via SSL/TLS, daher auch hier keine Bedenken.

**Samba** ist eine freie Implementation des SMB Protokolls, das Microsoft für eigene Netzwerkdienste wie die Freigabe von Dateisystemen und Druckern in seinen Windows Betriebssystemen verwendet. Samba kann im Netz einen Domain-Controller, wie man ihn von Windows NT 4 her kennt, darstellen und damit zentral die Accounts der Windows-Benutzer verwalten. Samba überträgt die eigentlichen Daten unverschlüsselt, die Passwörter werden aber verschlüsselt übertragen, was soweit noch im Rahmen des akzeptablen liegt.

Da Samba seine Benutzer und ihre Passwörter auch aus einem LDAP-Verzeichnis beziehen kann, eignen sich aus rein technischer Sicht die beiden Kombinationen „Samba – OpenLDAP“ und „Samba – Sun ONE Directory Server“ für die Realisierung der zukünftigen Benutzerverwaltung im OFFIS Bereich HS.

## 1.6 Kosten-Nutzen-Analyse

Auch wenn das Active Directory von Microsoft mit ca. 475 €, etwa 150 € für Windows 2000 Server und 50 Client-Access-Lizenzen (CAL) zu je 6,50 € zu F&L[4]-Konditionen mit einem Microsoft-SELECT Rahmen-Vertrag, noch innerhalb akzeptabler Preise liegt und die Administration des Systems recht einfach, sowie die Authentifizierung dank Kerberos-Integration sehr sicher ist, deckt es nicht alle erforderlichen Plattformen ab, was diese Lösung recht früh disqualifiziert. Die 50 CALs rechne ich hierbei pro Mitarbeiter mit „eigenem“ Rechner, egal ob regulärer Mitarbeiter oder WiHi.

Der Sun ONE Directory Server ist eine sehr interessante Lösung, es stellt einen LDAP-Server zur Verfügung und kostet für F&L bei ca. 400 Einträgen und einem Preis von 2,12 € pro Eintrag (Die Software selbst ist kostenlos, die Lizensierung erfolgt pro Verzeichnis-Eintrag), sowie einem F&L-Rabatt von 75% nur 212 €. Sollte der Bereich HS bei den Sun-Rechnern von Solaris 8 auf Solaris 9 umsteigen, dann ist diese Lösung noch günstiger, denn Solaris 9 enthält bereits den Directory Server inklusive einer Gratislizenz für 200.000 Einträge. Der Sun ONE Directory Server konnte leider nicht weiter evaluiert werden, aber es ist dennoch anzunehmen, dass hierbei die Administration der Account über mitgelieferte Tools im Gegensatz zu OpenLDAP relativ einfach zu erledigen ist. Die 400 zu lizensierenden Einträge rechnen sich aus den bereits im NIS existierenden Accounts (ca. 200, davon viele Projekt-bezogen oder Studenten-Accounts für Übungen zu bestimmten Vorlesungen, etc.) und zusätzlichen Host-, Netzwerk- und Netgroup-Einträgen (ca. 150) plus einer Reserve von 50 Einträgen.

NIS kommt für das neue System eigentlich nicht mehr in Frage, da es ja schon eingesetzt wird und zu unsicher ist. Der Vollständigkeit halber sei es hier trotzdem aufgeführt. NIS ist in der Anschaffung kostenlos, da es bei Solaris bereits enthalten und auch sonst im Internet frei verfügbar ist. Man könnte das System (das derzeit nur die Solaris-Systeme bedient) auch auf die Linux-Systeme ausweiten, um den Nutzen zu steigern, doch kommt dies aus sicherheitstechnischen Gründen nicht weiter in Frage.

[4] F&L → Forschung & Lehre

OpenLDAP ist dank GPL-Lizensierung frei erhältlich und ist in der Anschaffung kostenlos. Jedoch ist hier der Aufwand für die Einrichtung relativ hoch. Es gibt zwar viele frei verfügbare LDAP-Administrations-Tools, wie z.B. gq[5], jedoch ist keines davon für alle anfallenden Aufgaben gleichzeitig geeignet. Am einfachsten bei der Administration ist das Erstellen von LDIF-Dateien per Hand bzw. mit Hilfe von Vorlagen, die dann nur noch importiert werden müssen. OpenLDAP ist aber eine recht ausgereifte und stabile Software, die bereits seit einigen Jahren in vielen Bereichen in Universitäten und Instituten, aber auch in größeren Firmen eingesetzt wird. Will man OpenLDAP für eine volle NIS-Funktionalität benutzen, kann man für die Migration von NIS nach LDAP die sog. „MigrationTools“ von PADL Software[6] verwenden, die ebenfalls unter der GPL stehen und leicht anpassbar sind, so dass hierbei die Kosten für den Zeitaufwand fast vernachlässigbar sind.

Auch Samba ist „Freie Software“ unter der GPL und ist in der Anschaffung erst einmal kostenlos. Die Kosten bei der Einrichtung halten sich in Grenzen, da diese Software auch sehr ausgereift und sehr gut dokumentiert ist, so dass man schnell zu einem lauffähigen System kommt. Die Kombination von Samba und OpenLDAP deckt alle technischen Anforderungen ab und ist dank der MigrationTools und der guten Dokumentation der Software recht einfach und schnell zu realisieren.

Zur übersichtlicheren Bewertung der Alternativen im Hinblick auf Kosten und Nutzen der einzelnen Lösungen verwende ich hier eine einfache Entscheidungstabelle, in der für die wichtigsten Kriterien Punkte vergeben und die nach der angegebenen Gewichtung addiert werden.

Die Kriterien hinsichtlich der zu erwartenden Kosten sind aufgegliedert in Kosten für die Anschaffung der Software, die Einführung (Installation, Integration, Migration) und den laufenden Betrieb. Da die Realisierung der verschiedenen Lösungen dank des bereits vorhandenen Know-Hows jeweils relativ schnell zu erledigen sein dürfte, ist die Gewichtung eher niedrig anzusetzen. Wichtiger sind hier die Kosten der Anschaffung und vor allem die laufenden Betriebskosten.

Der Nutzen der verschiedenen Lösungen wird anhand der Kriterien Sicherheit, Flexibilität (im Sinne von „Was ist mit dieser Lösung zukünftig sonst noch möglich?“), Plattformunabhängigkeit (Server- und Client-seitig), Herstellerunabhängigkeit, und der Abdeckung der Clients bewertet und ergibt sich hauptsächlich aus dem Anforderungskatalog. Am wichtigsten bei der Einordnung des Nutzens der einzelnen Lösungen sind Sicherheit und die Abdeckung alle drei Arten von Clients (Solaris, Linux, Windows), gefolgt von Plattform- und Herstellerunabhängigkeit. Das Schlusslicht bildet hier das Kriterium Flexibilität, da es hier in erster Linie darum geht die Benutzerverwaltung zu zentralisieren. Mögliche andere Anwendungen der zu realisierenden Lösung spielen ersteinmal eine stark untergeordnete Rollle.

| **Kriterium** | **Gewichtung** | **Max. erreichb. Punkte** | **Microsoft Active Directory** | **NIS** | **Sun ONE Directory Server** | **OpenLDAP mit Samba DC** | **alter Zustand** |
|---|---|---|---|---|---|---|---|
| Kosten Anschaffung (SW) | 7 | 10 | 4 | 10 | 6 | 10 | 10 |
| Kosten Einführung | 4 | 10 | 8 | 6 | 6 | 4 | 10 |
| Kosten Betrieb | 10 | 10 | 8 | 7 | 8 | 8 | 2 |
| Sicherheit | 10 | 10 | 10 | 3 | 10 | 10 | 3 |
| Flexibilität | 5 | 10 | 2 | 4 | 4 | 8 | 2 |
| Plattformunabhängigkeit | 6 | 10 | 2 | 6 | 4 | 8 | 8 |
| Herstellerunabhängigkeit | 6 | 10 | 2 | 8 | 2 | 8 | 6 |
| Client-Abdeckung | 10 | 9 | 3 | 6 | 9 | 9 | 3 |
| **Summe** | | 570 | 304 | 358 | 392 | **492** | *284* |

Tabelle 1: Bewertung der Alternativen

[5] `http://biot.com/gq/` [Stand: 2003-05-08]
[6] `http://www.padl.com/OSS/MigrationTools.html` [Stand: 2003-05-01]

## 1.7 Entscheidung

Die Anforderung, alle im OFFIS-Bereich HS eingesetzten Client-Systeme zu unterstützen, erfüllen nur die LDAP-Basierten Lösungen mit dem „Sun ONE Directory Server“ sowie „OpenLDAP“. Bei beiden funktioniert die Verbindung zum Client im Prinzip gleich (PAM/NSS auf Solaris und Linux, der Umweg über einen Samba-Domain-Controller für die Windows-Systeme). So stellt sich die Entscheidung nur noch zwischen der Lizenzfreien und der kommerziellen Lösung auf der Server-Seite.

Beim „Sun ONE Directory Server“ fehlt die Erfahrung, außerdem ist die Software noch relativ jung, während Kenntnisse mit dem OpenLDAP-Server „slapd“ schon vorhanden sind und das System – wie schon erwähnt – sehr ausgereift ist und bereits in einer breiten Basis eingesetzt wird.

Das System zur zentralen Benutzerverwaltung wird also mit OpenLDAP und Samba realisiert.

## 1.8 Konkretes Soll-Konzept

Ziel des Projekts ist es, einheitliche Benutzer-Accounts für alle Plattformen (Solaris, Linux, Windows) zu haben. Dies soll mit LDAP (Backend), PAM[7]/NSS[8] (Client für Linux, Solaris) und Samba (als Domain-Controller für Windows) realisiert werden.

Um die zu erwartende Last bezüglich der Reaktionszeiten auf Anfragen an den LDAP-Server etwas aufzuteilen, sollen zwei LDAP-Server eingerichtet werden. Der Hauptserver soll auf einer neu anzuschaffenden Maschine laufen, der zweite auf dem Fileserver, auf dem auch Samba läuft. Das Verzeichnis auf dem Haupt-LDAP-Server soll regelmäßig auf den anderen repliziert werden. Dies sorgt auch gleich für die nötige Redundanz im Falle des Ausfalls einer Maschine.

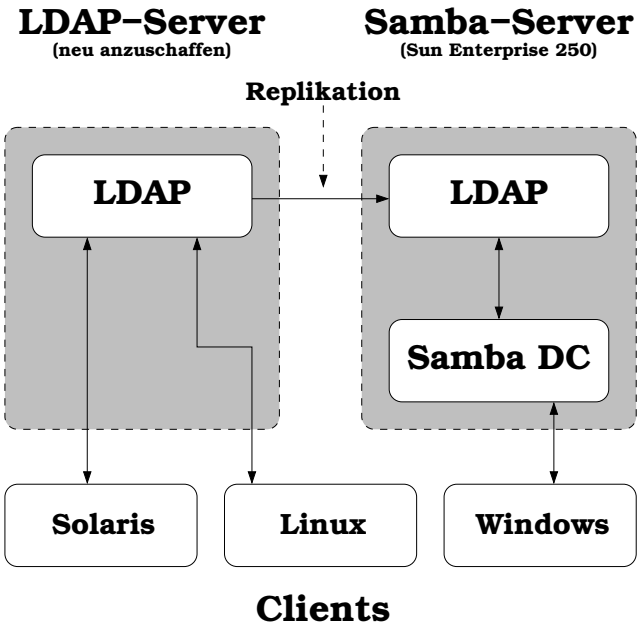



Abbildung 1: Schema des Authentifikationssystems

[7] PAM → Pluggable Authentication Modules, Authentifizierungsframework für Linux, Solaris und einige andere UNIX-Derivate

[8] NSS → Name Service Switch, Framework zur Namensauflösung verschiedenster Dienste unter Linux, Solaris und einigen anderen UNIX-Derivaten

Aus Sicherheits- und Verfügbarkeitsgründen soll der LDAP-Server auf einer anderen Maschine laufen, als der Fileserver. Da der Fileserver bereits mit Samba unter Solaris auf einem „Sun Enterprise 250“-Rechner realisiert ist, der einfach umkonfiguriert werden müsste, ist lediglich neue Hardware für den LDAP-Server zu beschaffen.

# 2 Hardwarebeschaffung für den LDAP-Server

## 2.1 Produktauswahl

Bei dem zu realisierenden System sind viele Anfragen an das LDAP-Verzeichnis zu erwarten, die jeweils aber recht wenig Daten beinhalten. Um möglichst kurze Zugriffszeiten zu erreichen, soll das Server-System eine schnelle (10.000 oder 15.000 Umdrehungen/Min.) SCSI-Festplatte bekommen. Die Kapazität ist nicht ganz so wichtig, 9 GB reichen vorerst, mit 18 GB wäre genug Reserve für mögliche weitere Anwendungen in den nächsten Jahren da. Der Server soll mit 512 MB RAM ausgestattet sein, nicht nur damit die Datenbank des LDAP-Servers (die nur ca. 1 MB auf der Festplatte beansprucht) und die notwendigen Suchindexe komplett hineingeladen werden können, sondern auch die ganzen anderen benötigten Standard-Dienste unter Solaris 8. Ziel ist, dass die Maschine im normalen Betrieb auch bei erhöhter Last und vielen Prozessen für die Beantwortung der Client-Anfragen nicht den Auslagerungsspeicher benutzen muss.

Das Serversystem sollte von Sun sein, da der bestehende Haupt-Server („Enterprise 250“) wie auch der Abteilungs-Webserver („Ultra 5“) und fast[9] alle anderen permanent laufenden Rechner schon Sun-Hardware sind.

Der neue Rechner sollte außerdem ein 19-Zoll Gehäuse haben, da sonst kein Platz mehr für weitere Rechner im Serverraum vorhanden ist. Ich entscheide mich deshalb für ein Sun-System aus der Netra-Reihe. Aus Kostengründen werden allerdings auch Angebote über ältere, bzw. gebrauchte Rechner angefragt[10].

Auch bei den Computern von Sun geht der Trend immer weiter in Richtung IDE statt SCSI, weshalb in von den insgesamt drei angebotenen Rechnern nur eines mit einer SCSI-Platte auftaucht, trotz expliziter Anfrage nach einem SCSI-System.

Hier die wichtigsten Daten des angebotenen SCSI-Systems:

- Sun Netra X1
- 500 MHz UltraSPARC IIe Prozessor
- 512 MB Arbeitsspeicher
- 9,1 GB SCSI Festplatte mit 7200 U/Min
- 2 Ethernet Ports 10/100BASE-T
- 19 Zoll Rack-Mount Kit

## 2.2 Lieferantenauswahl

Angebote wurden bei zwei Lieferanten angefragt, ISS und IPS, beide mit Sitz in Bremen. Gerade bei Sun Hardware ist eigentlich IPS der erfahrenere Händler (zertifizierter Sun-, sgi-, HP- und Compaq-Vertragshändler), aber ISS bietet auch solche Systeme an. ISS und IPS gehören außerdem

[9] Ausnahmen sind nur ein Dual-Athlon System mit Linux als Kompilier-Maschine und ein Linux-System, das als „WiHi-Server“ gemeinsame Homes für die WiHi-PCs exportiert.

[10] Angebote im Anhang, ab Seite 15.

anscheinend zusammen, beide haben die gleiche Adresse und verwenden das gleiche System für die Angebotserstellung (siehe Angebote im Anhang).

Da es bei Hardware von/für Sun eine bei weitem geringere Geräte-Bandbreite als bei Intel-basierten Systemen gibt, halten sich auch die Qualitätsunterschiede in engen Grenzen. Es kann eigentlich immer davon ausgegangen werden, dass man hier gute Qualität angeboten bekommt, besonders da fast alle Anbieter für Sun Hardware zertifizierte Vertragshändler sind.

Weil die beiden Firmen der Angebote kooperieren, ist es für das OFFIS nicht entscheidungsrelevant, welcher Anbieter liefert. Daher wird das günstigste Angebot ausgewählt, bzw. hier in diesem Fall das einzige angebotene SCSI-System.

## 2.3 Entscheidung

Da die Anschaffung neuer Server-Hardware doch nicht genehmigt wurde, muss nun eine Alternativ-Lösung gefunden werden. Die Rechner im Sun-Pool werden in der letzten Zeit weniger benutzt als z.B. noch vor einem Jahr. Hier könnte man eine Maschine herausnehmen, ohne dass sie dort fehlen würde. Allerdings sind dies eigentlich nur IDE-basierte Desktop-Computer, die nicht für den Servereinsatz konzipiert wurden. Ich weise noch einmal ausdrücklich darauf hin, dass hier ein richtiges Serversystem die bessere und zuverlässigere Entscheidung ist. Da aber eben keine neue Maschine angeschafft werden kann und der Haupt-LDAP-Server aus Last- und Redundanzgründen nicht mit auf dem Fileserver laufen darf, muss auf eine der schon vorhandenen Desktop-Suns zurückgegriffen werden. Hier stehen die Modelle „Sun Ultra 10“, „Sun Blade 100“ und einige mit der Ultra 10 vergleichbare Clones zur Verfügung. Ich entscheide mich hierbei für eine Ultra 10, da sie etwas besser als die Blade 100 ist und ich keinem Clone die zu erfüllenden Aufgabe anvertrauen möchte. Sollten sich im laufenden Betrieb Probleme mit der Performance zeigen, wird der Rechner je nach Bedarf mit einer schnelleren (dann SCSI-) Festplatte und/oder mehr RAM ausgestattet.

# 3 Realisierung

## 3.1 LDAP-Server

Als Software für den LDAP-Server kommt OpenLDAP in einer aktuellen Version zum Einsatz. OpenLDAP ist recht ausgereift und läuft stabil und zuverlässig auf nahezu allen UNIX-Plattformen.

Wegen Schwierigkeiten mit der Installation des OpenLDAP Servers unter Solaris 8 wurde das LDAP-Server-Testsystem zur Zeitersparnis zunächst unter Debian GNU/Linux 3.0 („Woody“ oder „stable“) aufgesetzt. Für die Funktionsweise im Netzwerk ist das unter der Serversoftware liegende Betriebssystem nicht weiter relevant. Die Schwierigkeiten bei der Installation von OpenLDAP unter Solaris zeigten sich dadurch, dass beim Kompilieren der Software via make der Linker ld die vorhandenen Bibliotheken unter /usr/local/lib nicht gefunden hat.

## 3.2 Migration der NIS-Daten nach LDAP

Basis für die Migration der NIS-Daten in das LDAP-Verzeichnis sind die „MigrationTools“ von PADL Software[11]. Da diese Tools nur die LDAP-Einträge für die NIS-Funktionalität erzeugen, mussten sie noch entsprechend umgeschrieben werden, um auch noch die Objektklasse „sambaAccount“ mit einigen dazugehörigen Einträgen zur Verfügung zu stellen, was jedoch recht einfach und problemlos vonstatten ging.

## 3.3 Linux und Solaris als Clients

Damit Solaris und Linux die Accounts im LDAP-Verzeichnis nutzen können sind PAM und NSS entsprechend zu konfigurieren. Dies setzt natürlich vorraus, das die hierfür benötigten LDAP-Module jeweils installiert sind. Solaris 8 beinhaltet diese, jedoch ohne SSL/TLS-Support. Die gängigen Linux-Distributionen wie Debian und SuSE stellen entsprechzende Pakete zur Verfügung.

NSS steht für „Name Service Switch“ und stellt ein einheitliches System für die Auflösung von Namen aller Art (Benutzer, Hosts, Netzwerke, IP-Services, etc.) zur Verfügung.

PAM („Pluggable Authentication Modules“) ist ein System für die Authentifizierung von Benutzern.

Während PAM z.B. beim Login auf der Konsole, unter X, via FTP, ssh oder anderen Diensten benötigt wird kommt NSS schon bei einfachsten Befehlen, wir z.B. ls zur Namensauflösung der Benutzer-IDs in die entsprechenden Namen zum Einsatz.

Näheres zur Konfiguration von PAM/NSS in der Systemdokumentation im Anhang ab Seite 23.

## 3.4 Samba Domain-Controller mit LDAP-Backend

Auf dem Samba-Testserver wird ein aktueller Samba-Server aus dem 2.2er Versionszweig installiert und als Domain-Controller konfiguriert. Außerdem werden die entsprechenden Einträge für den LDAP-Server, der als Backend für die Samba-eigene Benutzerdatenbank dient, hinzugefügt.

Näheres zur Samba-Konfiguration in der Systemdokumentation im Anhang, ab Seite 20

[11] `http://www.padl.com/OSS/MigrationTools.html` [Stand: 2003-05-01]

## 3.5 Windows 2000 als Client-System

Windows 2000 muss als Client-System der zentralen Benutzerverwaltung über Samba und LDAP einfach wie auch in einem reinen Windowsnetzwerk mit einem Domain-Controller zur Domain hinzugefügt werden. Vorraussetzung dazu ist lediglich, dass zuvor ein Maschinen-Account für den jeweiligen Client-Rechner im LDAP-Verzeichnis angelegt wird.

## 3.6 Systemtest

Für den Systemtest wurden mehrere Login-Versuche von den verschiedenen Client-Systemen aus durchgeführt. Sie verliefen allesamt erfolgreich. lediglich das Ändern der Passwörter durch den jeweiligen Benutzer selbst funktioniert noch nicht. Dieses Problem sollte aber in kurzer Zeit lösbar sein, da es mit diesem System definitiv funktionieren soll und bei anderen Realisierungen so bereits im Einsatz ist. An der Lösung dieses Problem kann hier nicht weiter gearbeitet werden, da dies sonst den zeitlichen Rahmen der Projektarbeit sprengen würde. Als Übergangslösung ist aber auch das Ändern der Passwörter durch die Administratoren denkbar.

## 3.7 Migration der Produktivumgebung

Die Migration der Produktivumgebung kann zeitlich nicht mehr innerhalb dieses Projektes stattfinden (Da der Fileserver unter anderem wegen eines neuen RAID-Systems von Solaris 2.6 auf Solaris 8 umgestellt werden soll und dabei eine komplette Umstrukturierung erforderlich ist, wird der Einsatz der zentralen Benutzerverwaltung mit der Umstellung zusammengelegt.).

# 4 Resumée und weitere Entwicklung

Rückblickkend auf diese Projektarbeit ist festzustellen, dass einige Dinge nicht ganz so gelaufen sind, wie ich mir das Ganze vorgestellt hatte:

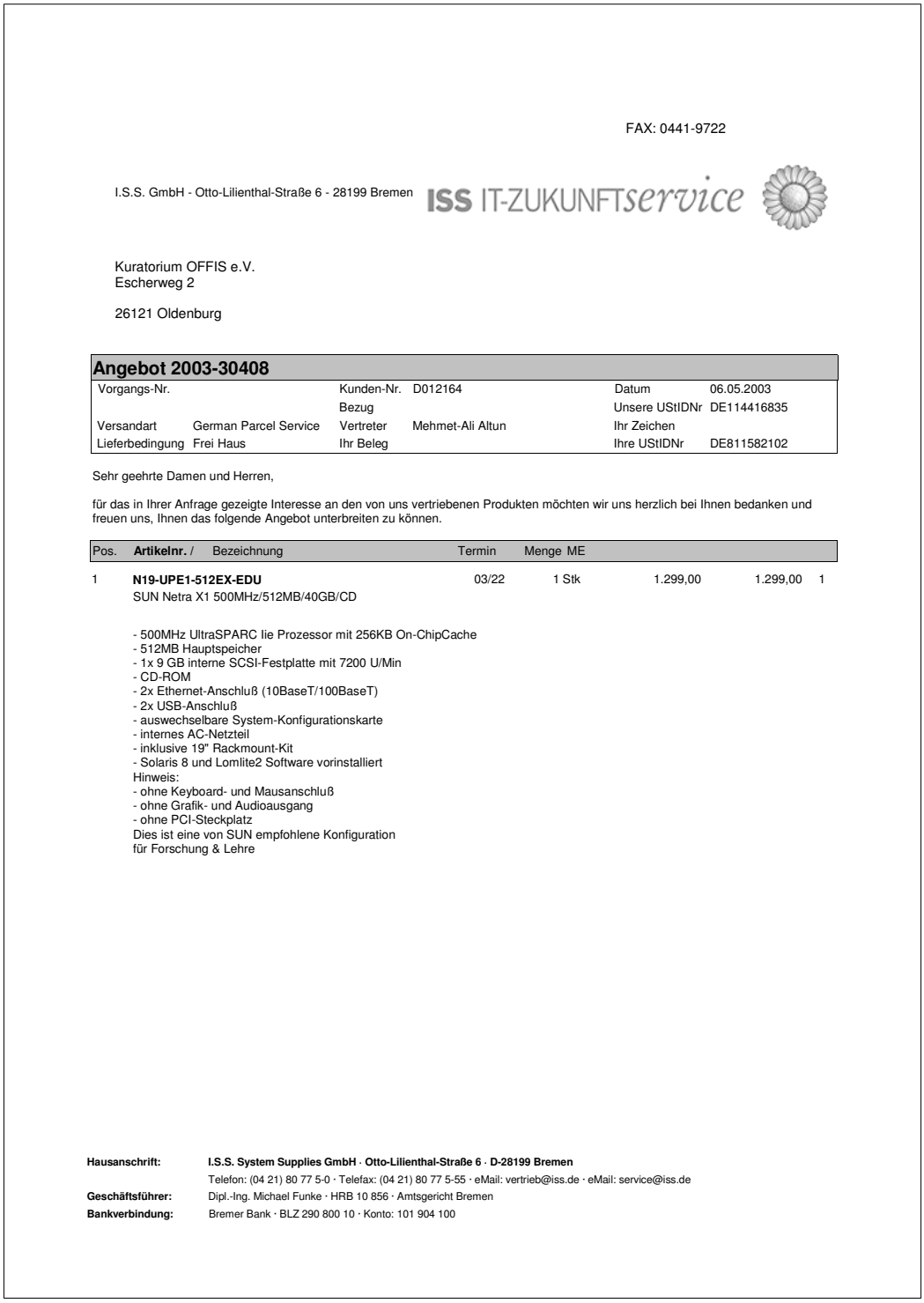
- Die 35 Stunden waren etwas zu knapp angesetzt, um die auftauchenden Probleme und die endgültige Umstellung in den Produktionsbetrieb mit berücksichtigen zu können.
- Gerade als das Testsystem fertig war und bis auf einige kleine und unwesentlichen Probleme (z.B. das Ändern der Passwörter durch den Benutzer selbst) funktionierte, gab es I/O-Errors auf allen Partitionen der Platte, so dass ein weiterer Betrieb des Test-Servers nicht mehr möglich war. Die Festplatte wurde nicht einmal mehr vom BIOS erkannt. Es war eine Platte von IBM, die bekannterweise in letzter Zeit sehr häufig defekte aufweisen. Das System musste neu aufgesetzt werden, was die Zeitplanung negativ beeinflusste. Dies sehe ich als eine Bestätigung meiner Aussage bei der Entscheidung für ein Serversystem, dass hier besser gute, aber teurere Hardware verbaut werden sollte.
- Unter Solaris gestaltete sich die Installation von Software generell als schwierig. OpenLDAP und die PAM- und NSS-Module lassen sich zwar prinzipiell unter Solaris kompilieren und laufen dann auch, doch liefert Sun mit Solaris keinen Compiler aus und der gcc von `http://www.sunfreeware.com/` lief leider nicht ohne weiteres „out-of-the-box“. Es gab oft Probleme mit den Include- und Library-Pfaden für den Linker. Aber auch die ./configure-Scripte vieler Software-Projekte ist viel zu oft auf reine GNU/Linux-Systeme ausgelegt, auch wenn die eigentliche Software auf so gut wie allen UNIX-Systemen sauber kompilierbar und lauffähig ist.

Obwohl das System noch nicht in den Produktiveinsatz gelangen konnte, wird dieses Projekt weiter verfolgt werden. Es kommen dann auch noch etliche Erweiterungen hinzu. Langfristiges Ziel ist eine komplette Single-Sign-On Lösung mit Kerberos und der Integration von weiteren Diensten, wie z.B. dem bereichsinternen Instant Messaging über Jabber. Eventuell ist auch eine Anbindung an das LDAP-Verzeichnis des OFFIS-weit eingesetzten Lotus Domino denkbar.

# A Ergänzungen zur Hardwarebeschaffung

## A.1 Angebote

### A.1.1 Angebot 1 (von ISS)



FAX: 0441-9722

I.S.S. GmbH - Otto-Lilienthal-Straße 6 - 28199 Bremen ISS IT-ZUKUNFTservice

Kuratorium OFFIS e.V.
Escherweg 2

26121 Oldenburg

**Angebot 2003-30408**

| | | | | | |
|---|---|---|---|---|---|
| Vorgangs-Nr. | | Kunden-Nr. | D012164 | Datum | 06.05.2003 |
| | | Bezug | | Unsere UStIDNr | DE114416835 |
| Versandart | German Parcel Service | Vertreter | Mehmet-Ali Altun | Ihr Zeichen | |
| Lieferbedingung | Frei Haus | Ihr Beleg | | Ihre UStIDNr | DE811582102 |

Sehr geehrte Damen und Herren,

für das in Ihrer Anfrage gezeigte Interesse an den von uns vertriebenen Produkten möchten wir uns herzlich bei Ihnen bedanken und freuen uns, Ihnen das folgende Angebot unterbreiten zu können.

| Pos. | **Artikelnr.** / | Bezeichnung | Termin | Menge | ME | | |
|---|---|---|---|---|---|---|---|
| 1 | **N19-UPE1-512EX-EDU** | SUN Netra X1 500MHz/512MB/40GB/CD | 03/22 | 1 | Stk | 1.299,00 | 1.299,00 1 |

- 500MHz UltraSPARC Iie Prozessor mit 256KB On-ChipCache
- 512MB Hauptspeicher
- 1x 9 GB interne SCSI-Festplatte mit 7200 U/Min
- CD-ROM
- 2x Ethernet-Anschluß (10BaseT/100BaseT)
- 2x USB-Anschluß
- auswechselbare System-Konfigurationskarte
- internes AC-Netzteil
- inklusive 19" Rackmount-Kit
- Solaris 8 und Lomlite2 Software vorinstalliert

Hinweis:
- ohne Keyboard- und Mausanschluß
- ohne Grafik- und Audioausgang
- ohne PCI-Steckplatz

Dies ist eine von SUN empfohlene Konfiguration
für Forschung & Lehre

**Hausanschrift:** **I.S.S. System Supplies GmbH · Otto-Lilienthal-Straße 6 · D-28199 Bremen**
Telefon: (04 21) 80 77 5-0 · Telefax: (04 21) 80 77 5-55 · eMail: vertrieb@iss.de · eMail: service@iss.de
**Geschäftsführer:** Dipl.-Ing. Michael Funke · HRB 10 856 · Amtsgericht Bremen
**Bankverbindung:** Bremer Bank · BLZ 290 800 10 · Konto: 101 904 100

Abbildung 2: Angebot von ISS (Seite 1)

ISS IT-ZUKUNFTservice



| Pos. | Artikelnr. / Bezeichnung | Termin | Menge | ME | Einzelpreis | Gesamtpreis | |
|---|---|---|---|---|---|---|---|
| ***Alternativ :*** | | | | | | | |
| 2 | **RN19-UJE1-9S-256TW**<br>SUN Netra X1<br>400MHz, 256MB, 40.8 GB die<br>****gebraucht****<br>***remanufactured***<br>SUN Netra X1<br>One pack - Web Only<br>- 1x 400MHz UltraSPARC-II Prozessor 256KB eCache<br>- 256MB Hauptspeicher<br>- 40,8GB IDE Interne Festplatte/5400 rpm<br>- 2 Ethernet 10/100 ports<br>- 2 USB Ports<br>- removable configuration card<br>- Internes AC Netzteil<br>- kein Tastatur und Maus Anschluß<br>- keine Grafikkarte und Sound möglich<br>- ohne PCI Slots<br>- inkl. 19" Einbaukit<br>- Solaris 8 & Lomlite2 vorinstalliert | 03/22 | 1 | Stk | 749,00 | 749,00 | 1 |

| | | | |
|---|---|---|---|
| Zwischensumme | | EUR | 1.299,00 |
| zzgl. MwSt. mit Steuercode | 1 | | |
| 16,00 % von | 1.299,00 | | 207,84 |
| | **Endsumme** | **EUR** | **1.506,84** |
| | **entspricht** | **DM** | **2.947,12** |

Wir liefern alle Artikel nur zu unseren derzeit gültigen AGB´s. Diese sind über das Internet abrufbar. URL: ftp://ftp.ips-gruppe.de/pub/docs/agb/iss.pdf

Unsere Produkte sind nach dem deutschen Außenwirtschaftsrecht für den Export teilweise genehmigungspflichtig. Produkte mit US Ursprung unterliegen grundsätzlich den „US-Export-Regulations“. Dieses gilt für einzelne als auch in ein System integrierte Produkte

***Zahlungsvereinbarungen:***

14 Tage ohne Abzug 1.506,84 EUR entspricht 2.947,12 DM

**Hausanschrift:** **I.S.S. System Supplies GmbH · Otto-Lilienthal-Straße 6 · D-28199 Bremen**
Telefon: (04 21) 80 77 5-0 · Telefax: (04 21) 80 77 5-55 · eMail: vertrieb@iss.de · eMail: service@iss.de
**Geschäftsführer:** Dipl.-Ing. Michael Funke · HRB 10 856 · Amtsgericht Bremen
**Bankverbindung:** Bremer Bank · BLZ 290 800 10 · Konto: 101 904 100

Abbildung 3: Angebot von ISS (Seite 2)

## A.1.2 Angebot 2 (von IPS)

(Angebotsanfragen laufen im OFFIS ebenso wie die Bestellungen nur über den zentralen Einkauf bz. technischen Einkauf der technischen Verwaltung (TV), weswegen hier auch nicht mein Name auftaucht, sondern der eines Kollegen von der TV.)

FAX:

IPS-GmbH Bremen - Otto-Lilienthal-Straße 6 - 28199 Bremen

Firma
OFFIS e.V.
Escherweg 2

26121 Oldenburg

***Lieferanschrift:***

Firma
OFFIS e.V.
-R&D Division Embedded Systems-
Escherweg 2

26121 Oldenburg

Vertriebsgesellschaft für innovative
EDV-Produkte und -Systeme mbH

Otto-Lilienthal-Straße 6
D-28199 Bremen
Telefon: (0421) 536 88-0
Telefax: (0421) 536 88-66
EMail: info@ips-bremen.de
support@ips-bremen.de
URL: http://www.ips-bremen.de

**Angebot 2003-31066**

| | | | | |
|---|---|---|---|---|
| Vorgangs-Nr. | Kunden-Nr. | D103895 | Datum | 07.05.2003 |
| | Bezug | | Unsere UStIDNr | DE 114417104 |
| Versandart | Vertreter | Askim Kaya | Ihr Zeichen | |
| Lieferbedingung Frei Haus | Ihr Beleg | | Ihre UStIDNr | |

Sehr geehrter Herr Goerdes,

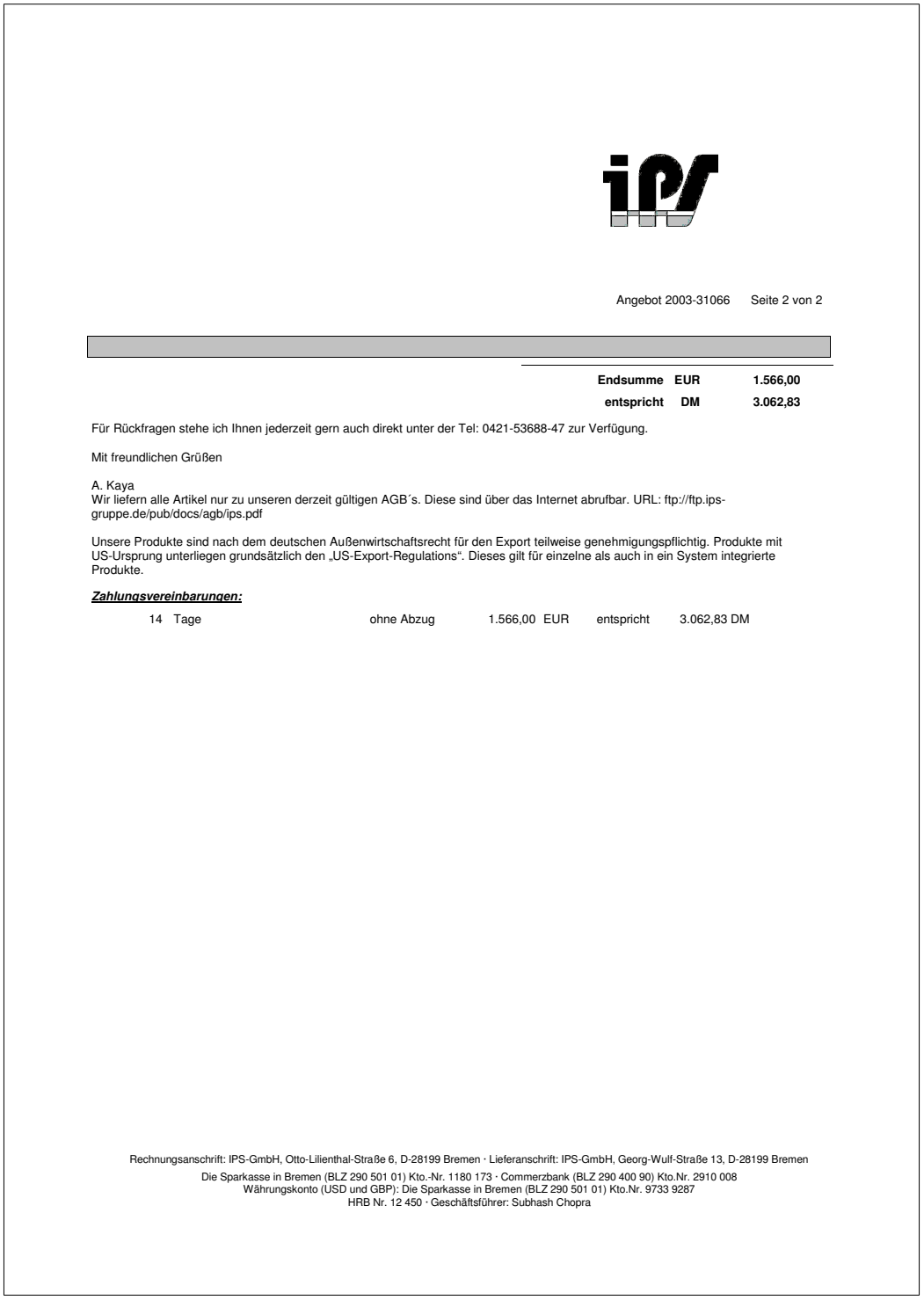
für das in Ihrer Anfrage gezeigte Interesse an den von uns vertriebenen Produkten möchten wir uns herzlich bei Ihnen bedanken und freuen uns, Ihnen das folgende Angebot unterbreiten zu können.

| Pos. | **Artikelnr.** / Bezeichnung | Termin | Menge | ME | | | |
|---|---|---|---|---|---|---|---|
| 1 | **N19-UPE1-512EX-EDU**<br>SUN Netra X1 500MHz/512MB/40GB/CD<br>***Gebraucht***<br>- 500MHz UltraSPARC lie Prozessor mit 256KB On-ChipCache<br>- 512MB Hauptspeicher<br>- 1x 40GB interne IDE-Festplatte mit 7200 U/Min<br>- CD-ROM<br>- 2x Ethernet-Anschluß (10BaseT/100BaseT)<br>- 2x USB-Anschluß<br>- auswechselbare System-Konfigurationskarte<br>- internes AC-Netzteil<br>- inklusive 19" Rackmount-Kit<br>- Solaris 8 und Lomlite2 Software vorinstalliert<br>Hinweis:<br>- ohne Keyboard- und Mausanschluß<br>- ohne Grafik- und Audioausgang<br>- ohne PCI-Steckplatz<br>Dies ist eine von SUN empfohlene Konfiguration<br>für Forschung & Lehre | 03/19 | 1 | Stk | 1.350,00 | 1.350,00 | 1 |

| | | | |
|---|---|---|---|
| Zwischensumme | | EUR | 1.350,00 |
| zzgl. MwSt. mit Steuercode | 1 | | |
| 16,00 % von | 1.350,00 | | 216,00 |

Rechnungsanschrift: IPS-GmbH, Otto-Lilienthal-Straße 6, D-28199 Bremen · Lieferanschrift: IPS-GmbH, Georg-Wulf-Straße 13, D-28199 Bremen
Die Sparkasse in Bremen (BLZ 290 501 01) Kto.-Nr. 1180 173 · Commerzbank (BLZ 290 400 90) Kto.Nr. 2910 008
Währungskonto (USD und GBP): Die Sparkasse in Bremen (BLZ 290 501 01) Kto.Nr. 9733 9287
HRB Nr. 12 450 · Geschäftsführer: Subhash Chopra

Abbildung 4: Angebot von IPS (Seite 1)



Angebot 2003-31066 Seite 2 von 2

| | | |
|---|---|---|
| **Endsumme** | **EUR** | **1.566,00** |
| **entspricht** | **DM** | **3.062,83** |

Für Rückfragen stehe ich Ihnen jederzeit gern auch direkt unter der Tel: 0421-53688-47 zur Verfügung.

Mit freundlichen Grüßen

A. Kaya
Wir liefern alle Artikel nur zu unseren derzeit gültigen AGB´s. Diese sind über das Internet abrufbar. URL: ftp://ftp.ips-gruppe.de/pub/docs/agb/ips.pdf

Unsere Produkte sind nach dem deutschen Außenwirtschaftsrecht für den Export teilweise genehmigungspflichtig. Produkte mit US-Ursprung unterliegen grundsätzlich den „US-Export-Regulations". Dieses gilt für einzelne als auch in ein System integrierte Produkte.

***Zahlungsvereinbarungen:***

| | | | | | | |
|---|---|---|---|---|---|---|
| 14 | Tage | ohne Abzug | 1.566,00 | EUR | entspricht | 3.062,83 DM |

Rechnungsanschrift: IPS-GmbH, Otto-Lilienthal-Straße 6, D-28199 Bremen · Lieferanschrift: IPS-GmbH, Georg-Wulf-Straße 13, D-28199 Bremen
Die Sparkasse in Bremen (BLZ 290 501 01) Kto.-Nr. 1180 173 · Commerzbank (BLZ 290 400 90) Kto.Nr. 2910 008
Währungskonto (USD und GBP): Die Sparkasse in Bremen (BLZ 290 501 01) Kto.Nr. 9733 9287
HRB Nr. 12 450 · Geschäftsführer: Subhash Chopra

Abbildung 5: Angebot von IPS (Seite 2)

# B Systemdokumentation

## B.1 LDAP-Server

Das Testsystem für den LDAP-Server ist ein einfacher PC.

| | | |
|---|---|---|
| Hostname | : | doto |
| IP | : | 134.106.53.72 |
| MAC | : | 00:04:76:17:39:60 |

### B.1.1 Software

- OpenLDAP[12], Version 2.0.23
- MigrationTools[13], Version 44
- smbldap-tools[14], Version 0.7

### B.1.2 Konfigurationsdateien

#### slapd.conf

```
##############################################################################
#                                                                            #
#  slapd.conf (2003-05-03 by Christian Wenke, OFFIS/HS)                      #
#                                                                            #
##############################################################################
#                                                                            #
#  This is the main ldapd configuration file. See slapd.conf(5) for          #
#  more info on the configuration options. This file is based on the         #
#  default configuration file from Debian GNU/Linux                          #
#                                                                            #
##############################################################################

# Schema and objectClass definitions
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/samba.schema

# Schema check allows for forcing entries to
# match schemas for their objectClasses's
schemacheck     on

# Where the pid file is put. The init.d script
# will not stop the server if you change this.
pidfile         /var/run/slapd.pid

# List of arguments that were passed to the server
argsfile        /var/run/slapd.args

# Where to store the replica logs
replogfile      /var/lib/ldap/replog

# Loglevel, read slapd.conf(5) for possible values
loglevel 0
```

[12] http://www.openldap.org/ [Stand: 2003-05-01]
[13] http://www.padl.com/OSS/MigrationTools.html [Stand: 2003-05-01]
[14] http://samba.idealx.org/index.en.html [Stand: 2003-05-01]

```
#######################################################################
# ldbm database definitions
#######################################################################

# The backend type, ldbm, is the default standard
database        ldbm

# The base of your directory
suffix          "ou=HS,o=OFFIS,c=DE"

# Where the database file are physically stored
directory       "/var/lib/ldap"

# Indexing options
index objectClass,rid,uid,uidNumber,gidNumber,memberUid eq
index cn,mail,surname,givenname eq,subinitial

# Save the time that the entry gets modified
lastmod on

#######################################################################
# TLS stuff
#######################################################################

TLSCipherSuite HIGH:MEDIUM:+SSLv2
TLSCertificateFile /etc/ldap/sslcert.pem
TLSCertificateKeyFile /etc/ldap/sslcert.pem
TLSCACertificateFile /etc/ldap/sslcert.pem

#######################################################################
# Access Control Lists
#######################################################################

# The userPassword by default can be changed
# by the entry owning it if they are authenticated.
# Others should not be able to see it, except the
# admin entry below
access to attribute=userPassword
        by dn="cn=ldap-admin,ou=HS,o=OFFIS,c=DE" write
        by anonymous auth
        by self write
        by * none

access to attribute=lmPassword
        by dn="cn=ldap-admin,ou=HS,o=OFFIS,c=DE" write
        by self write
        by * none

access to attribute=ntPassword
        by dn="cn=ldap-admin,ou=HS,o=OFFIS,c=DE" write
        by self write
        by * none

# The admin dn has full write access
access to *
        by dn="cn=ldap-admin,ou=HS,o=OFFIS,c=DE" write
        by * read

# For Netscape Roaming support, each user gets a roaming
# profile for which they have write access to
access to dn=".*,ou=Roaming,o=morsnet"
        by dn="cn=ldap-admin,o=OFFIS,c=DE" write
        by dnattr=owner write
```

## B.2 Samba-Server

Der Samba-Testserver läuft auf derselben Maschine, wie der LDAP-Server.

### B.2.1 Software

- Samba, Version 2.2.8a
- Solaris 8

### B.2.2 Konfigurationsdateien

### smb.conf

```
#######################################################################
#                                                                     #
#  smb.conf (2003-05-03 by Christian Wenke, OFFIS/HS)                 #
#                                                                     #
#######################################################################
#                                                                     #
#  This file contains the configuration data for the Samba server.    #
#                                                                     #
#######################################################################


[global]

# basic settings

        workgroup      = OFFIS-HS
        netbios name   = DOTO
        server string  = %h server (Samba %v)
        security       = user
        os level       = 255

        domain admin group  = @admin
        admin users         = admin
        invalid users       = root
        guest account       = nobody


# interfaces and ip based settings

        interfaces            = 134.106.53.72/24 127.0.0.1/8
        bind interfaces only  = yes
        socket options        = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        hosts allow           = 134.106.53. 127.


# log settings

        ;log file      = /var/log/samba/log.%m
        log level     = 2
        max log size  = 1024
        syslog        = 1


# samba server behaviour

        domain master       = yes
        local master        = yes
        preferred master    = yes
        domain logons       = yes
        wins support        = yes
        dns proxy           = yes
        name resolve order  = lmhosts host wins bcast
        time server         = yes


# password settings

        encrypt passwords   = yes
        unix password sync  = yes
```

```
        passwd program      = /usr/local/bin/smbldap-passwd.pl -o %u
        passwd chat         = *new*password* %n\n *new*password:* %n\n \
                              *successfully*


# logon settings

        logon path    = \\%L\profiles\%u
        logon drive   = H:
        logon home    = \\%L\%u
        logon script  = logon.bat


# LDAP settings

        ldap suffix      = ou=HS,o=OFFIS,c=DE
        ldap admin dn    = cn=ldap-admin,ou=HS,o=OFFIS,c=DE
        ldap port        = 389
        ldap server      = localhost
        ldap ssl         = no
        add user script  = /usr/local/bin/smbldap-useradd.pl -m \
                              -d /dev/null -g 1000 -s /bin/false


# misc settings

        character set        = iso8859-1
        preserve case        = yes
        short preserve case  = yes


[homes]

        comment         = Home Directories
        browseable      = no
        writeable       = yes
        create mask     = 0600
        directory mask  = 0700
force user      = %U
force group     = %G
hide dot files  = no


[netlogon]

        comment     = Network Logon Service
        path        = /home/samba/netlogon
        public      = no
        read only   = yes
        browseable  = no


[profiles]

        path            = /home/samba/profiles
        read only       = no
        browseable      = no
        create mode     = 0600
        directory mode  = 0700


[printers]

        comment     = All Printers
        browseable  = yes
        path        = /var/spool/lpd/samba
        printable   = yes
        public      = yes
        guest ok    = yes


[public]

        comment              = Public Stuff
```

```
        path                    = /home/samba/public
        writeable               = yes
        guest ok                = yes
        public                  = yes
        browseable              = yes
force create mode     = 0777
force directory mode  = 0777
force user            = nobody
force group           = nogroup
```

## B.3 Linux- und Solaris-Client

### B.3.1 Software

Folgene Linux-Distributionen werden als Client-System verwendet:

- Debian GNU/Linux: 3.0 (stable, „Woody“), testing („Sarge“) und unstable („Sid“)
- SuSE Linux: 8.2

Solaris kommt in Version 8 zum Einsatz.

Die benötigten LDAP-Module für PAM und NSS sind jeweils im Lieferumfang von Debian GNU/Linux und SuSE Linux 8.2 enthalten.

Für Solaris müssen die Module von padl.com selber kompiliert werden:

`http://www.padl.com/OSS/nss_ldap.html`
`http://www.padl.com/OSS/pam_ldap.html`

### B.3.2 Konfiguration

Die Konfiguration unter Solaris ist die selbe wie auch unter Linux.

#### nsswitch.conf

```
# /etc/nsswitch.conf
#

passwd:         files ldap
group:          files ldap
shadow:         files ldap

hosts:          files dns
networks:       files

protocols:      db files
services:       db files
ethers:         db files
rpc:            db files

netgroup:       files
```

## libnss-ldap.conf

```
# /etc/libnss-ldap.conf
#

# LDAP Server.
uri ldaps://doto.offis.uni-oldenburg.de/

# The distinguished name of the search base.
base dc=bbs-haarentor,dc=de

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3
```

## pam_ldap.conf

```
# /etc/pam_ldap.conf
#

# LDAP server
uri ldaps://doto.offis.uni-oldenburg.de/

# The distinguished name of the search base.
base dc=bbs-haarentor,dc=de

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
rootbinddn cn=admin,dc=bbs-haarentor,dc=de

# Check the 'host' attribute for access control
# Default is no; if set to yes, and user has no
# value for the host attribute, and pam_ldap is
# configured for account management (authorization)
# then the user will not be allowed to login.
pam_check_host_attr yes


# Password hashes are MD5
pam_password md5
```

## pam.d/login

```
#%PAM-1.0
auth       required     /lib/security/pam_securetty.so
auth       required     /lib/security/pam_nologin.so
auth       sufficient   /lib/security/pam_ldap.so
auth       required     /lib/security/pam_unix_auth.so try_first_pass
account    sufficient   /lib/security/pam_ldap.so
account    required     /lib/security/pam_unix_acct.so
password   required     /lib/security/pam_ldap.so
session    required     /lib/security/pam_unix_session.so
```

## pam.d/su

```
#%PAM-1.0
auth       sufficient   /lib/security/pam_rootok.so
auth       sufficient   /lib/security/pam_ldap.so
auth       required     /lib/security/pam_unix_auth.so try_first_pass
account    sufficient   /lib/security/pam_ldap.so
account    required     /lib/security/pam_unix_acct.so
password   required     /lib/security/pam_ldap.so
session    required     /lib/security/pam_unix_session.so
```

### pam.d/ssh

```
#%PAM-1.0
auth       required     /lib/security/pam_nologin.so
auth       sufficient   /lib/security/pam_ldap.so
auth       required     /lib/security/pam_unix_auth.so try_first_pass
account    sufficient   /lib/security/pam_ldap.so
account    required     /lib/security/pam_unix_acct.so
password   required     /lib/security/pam_ldap.so
session    required     /lib/security/pam_unix_session.so
```

### pam.d/kde

```
#%PAM-1.0
auth       required     pam_nologin.so
auth       sufficient   pam_ldap.so
auth       required     pam_unix_auth.so shadow nullok
auth       required     pam_env.so
account    sufficient   pam_ldap.so
account    required     pam_unix_acct.so
account    required     pam_unix.so
password   required     pam_ldap.so
session    required     pam_unix_session.so
session    required     pam_unix.so
session    required     pam_limits.so
```

## B.4 Windows-Client

### B.4.1 Einrichtung

Windows als Client einzurichten geht sehr einfach vonstatten: Man muss nur den Rechner wie auch bei einem Domain-Controller in einem reinen Windows-Netzwerk mittels der Systemsteuerung (Systemeigenschaften → Netzwerkidentifikation → Eigenschaften) zur Domäne hinzufügen. Nach Eingabe von Benutzername und Passwort eines Administrators (Adm. auf dem Server) und einem Neustart des Systems ist der Windows-Rechner in der Domäne und bezieht die Accounts über den Server.

### B.4.2 Mögliche Probleme

Beim Hinzufügen des Windows-Clients zur Domäne kann nach dem Eingeben des Administrator-Accounts für den Server eine Fehlermeldung erscheinen, wenn die Arbeitsgruppe, in der sich der Rechner vorher zuvor befand den selben Namen wie die Domäne hat, der man beitreten will.

# C Administrationsdokumentation

## C.1 Überblick

Die Benutzeraccounts werden im LDAP-Verzeichnis unter dem Zweig `ou=People,ou=HS,o=OFFIS,c=DE` mit einem dn nach dem Schema `uid=<loginname>,ou=People,ou=HS,o=OFFIS,c=DE` gespeichert.

## C.2 Neue Benutzer anlegen

Als Grundlage für einen neuen Benutzer dient folgendes LDIF-Template:

```
dn: uid=<loginname>,ou=People,ou=HS,o=OFFIS,c=DE
uid: <loginnname>
cn: <Firstname Lastname>
givenName: <Firstname>
sn: <Lastname>
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: sambaAccount
userPassword: {MD5}0cmp2W7BskW9l2kwvmuasw==
loginShell: /bin/tcsh
uidNumber: 10030
gidNumber: 10000
homeDirectory: /home/<loginname>
gecos: <same as cn:>
rid: <uidNumber * 2 + 1000>
lmPassword: 193130B61A7F81C0AAD3B435B51404EE
ntPassword: FA4942AF3BB92B0C5DDAA88F0C2A95A2
pwdLastSet: 0
logonTime: 0
logoffTime: 0
kickoffTime: 0
pwdCanChange: 1
pwdMustChange: 0
primaryGroupID: <gidNumber * 2 + 1001>
acctFlags: [U          ]
```

Nach den entsprechenden Modifikationen kann man die LDIF-Datei mit folgendem Befehl in das LDAP-Verzeichnis importieren:

```
ldapadd -vcx -D "cn=ldap-admin,ou=HS,o=OFFIS,c=DE" \
        -H "ldap://localhost:389/" -W <new-user.ldif
```

## C.3 Benutzerdaten ändern

Zum Ändern von einzelnen Benutzerdaten unter Linux oder Solaris eignet sich am besten das Tool „gq“ von `http://biot.com/gq/`. Für Windows gibts es z.B. den auf Java basierten „LDAP Browser/Editor“ von `http://www.iit.edu/~gawojar/ldap/`. Diesen kann man dann auf allen Systemen mit einer Java Runtime Umgebung verwenden.

Das Anlegen von neuen Benutzern funktioniert mit diesen Tools nicht ganz so gut, weil sie meist kein Template-Management beinhalten, mit einigen Tools kann man aber sehr einfach fertige LDIF-Dateien in das Verzeichnis importieren.

## C.4 Benutzer löschen

Das Löschen von Benutzern geht am besten wie das Ändern von einzelnen Attributen mit einem der LDAP Browser/Editoren: Einfach den entsprechenden „distinguished name“ selektieren und löschen.

# Literatur


[1] Heinz Johner, Larry Brown, Franz-Stefan Hinner, Wolfgang Reis, Johan Westman: „Understanding LDAP“, IBM, Juni 1998, http://www.redbooks.ibm.com/pubs/pdfs/redbooks/sg244986.pdf [Stand: 2003-05-01]]

[2] http://de.samba.org/samba/docs/Samba-HOWTO-Collection.pdf [Stand: 2003-05-01]

[3] http://samba.idealx.org/samba-ldap-howto.pdf [Stand: 2003-05-01]

[4] „Zentrale Meldestelle“, Linux Magazin, Ausgabe 04/2002, Linux New Media AG

[5] http://doc.daasi.de/DaasiWiki/SambaLdapAuthentifikation [Stand: 2003-05-02]

[6] http://www.mitlinx.de/ldap/ [Stand: 2003-05-01]