midpoints
purify it

lotus notes | traveler | apple ios
we mobilize notes
deployment, security, monitoring

AdminCamp 09.2011

Lotus Mobile Connect
als Auth. Reverse Proxy für iNotes & Traveler

Detlev Pöttgen
midpoints GmbH

midpoints
purify it

lotus notes | traveler | apple ios
we mobilize notes
deployment, security, monitoring

Detlev Pöttgen

Solutions Architekt & Consultant
Gesellschafter |Geschäftsführer

midpoints GmbH
http://www.midpoints.de

IBM Advanced Business Partner
IBM Design Partner for Domino Next
IBM Mobile Design Partner
Apple Enterprise Developer Program

Schwerpunkte:
- Notes / Domino Consulting
- E-Mail Management
- Notes / Domino & mobile App Entwicklung

- we mobilize Notes
  Lotus Traveler Planung & Implementierung
  Domino basiertes Mobile Device Management

Blog: http://www.netzgoetter.net

midpoints purify it

Agenda

Lotus Mobile Connect
als Auth. Reverse Proxy für iNotes & Traveler

- Warum benötige ich einen Reverse Proxy?

- Lotus Mobile Connect als Auth. Reverse Proxy

- Funktionsweise & Konfiguration

- Lotus Traveler & Lotus Mobile Connect

midpoints purify it

Warum benötige ich einen Reverse Proxy?

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Wat issen Proxy?

- Proxy heisst auf Englisch Stellvertreter, Bevollmächtigter.
- Im Internet-Umfeld ist ein Proxy generell ein System, welches stellvertretend für einen Benutzer eine Aktion durchführt und das Resultat zurückmeldet.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Wat issen Proxy?

- Das bekannteste Beispiel ist der "normale" HTTP Proxy, der im Browser konfiguriert werden kann.
- Der Browser schickt dann alle Requests an diesen Proxy statt direkt ans Zielsystem.
- Ein solcher Proxy erfüllt vor allem die Funktion eines Filters, meist kombiniert mit Caching Funktionalität.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Wat issen Reverse Proxy?

- Im Gegensatz zum "normalen" oder "Forward" Proxy dient der HTTP Reverse Proxy nicht als Stellvertreter des Benutzers bzw. seines Browsers, sondern als Stellvertreter des Webservers, welcher den Request abarbeiten soll.
- Der HTTP Reverse Proxy leitet den Request des Browsers an einen Webserver weiter und gibt die Antwort an den Browser des Benutzers zurück.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Wie funktioniert ein Reverse Proxy?

Die Grundfunktionalität des Reverse Proxy liegt darin, Requests für eine URL entgegenzunehmen,

daraus anhand eines vorkonfigurierten Mappings einen Request an einen der angeschlossenen Webserver zu generieren

und anschließend das Ergebnis dieses Requests an den Client zurückzugeben.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Wieso wird ein Reverse Proxy verwendet?

1. Ein HTTP Reverse Proxy bietet sich als Lösung an, wenn gewisse Funktionalitäten (z.B. **Authentisierung**, **Autorisierung** und **Verschlüsselung**) zentral gelöst werden sollen.

   Diese müssen dann nicht mehr von jedem Webserver einzeln übernommen werden. Dies kann die Konfiguration und Administration der Webserver vereinfachen und vereinheitlichen.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Wieso wird ein Reverse Proxy verwendet?

2. Der HTTP Reverse Proxy ermöglicht es auch, heterogene Infrastruktur

   (mehrere Webserver, ev. mit unterschiedlichen Technologien für verschiedene Services)

   für den Benutzer als ein logisches System zusammenzufassen und zu präsentieren.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Wieso wird ein Reverse Proxy verwendet?

3. Ein weiterer Grund für den Einsatz eines Reverse Proxy sind dessen Sicherheits-Features.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Welche Feature bietet ein Secure Reverse Proxy?

- Minimale Funktionalität und daher potenziell weniger Sicherheitslücken als ein "voller" Webserver.
- "Verstecken" des eigentlichen Webservers, der vom Internet her nicht mehr direkt zugreifbar ist.
- Untersuchung des HTTP Requests und Filtern von ungültigen oder potenziell gefährlichen Requests.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Welche Feature bietet ein Secure Reverse Proxy?

- Endpunkt für die Verschlüsselung zwischen Browser und interner Infrastruktur. Die Konfiguration der Verschlüsselung kann zentral vorgenommen werden.
- Zentrale Authentisierung und Single-Sign-On über alle angeschlossenen Webserver.
- Autorisierung der Zugriffe auf die angeschlossenen Webserver.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Lässt sich mit Open Source ein Secure Reverse Proxy umsetzen?

- Das Apache Modul *mod_proxy* bietet die volle Funktionalität eines Reverse Proxies.
- Die Authentisierung lässt sich mittels "Basic Authentication" realisieren. Die User-Credentials werden dabei vom Browser mit jedem Request an den Reverse Proxy mit geschickt.
- Über LDAP für die Benutzerverwaltung haben Sie schnell einmal eine recht ansehnliche Lösung.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Lässt sich mit Open Source ein Secure Reverse Proxy umsetzen?

- Probleme macht hierbei in der Regel aber das Single Sign On zwischen dem Apache Proxy und Domino
- Der User meldet sich in der Regel am Secure Reverse Proxy an, dieser müßte die Session an den Domino Server weitergeben.
- Es gibt kein fertiges Modul das ein SSO mit Domino ermöglicht!

midpoints purify it

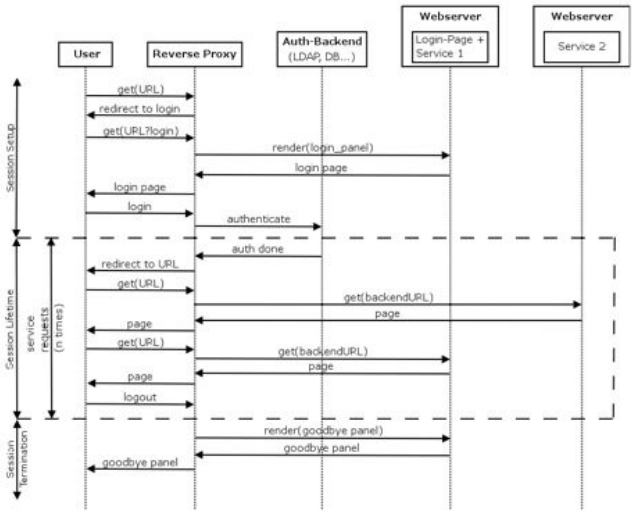
Warum benötige ich einen Reverse Proxy?

Wie läuft das Login ab?

- Jeder Request auf einen geschützten Bereich auf dem Reverse Proxy, der mit einem unbekannten (noch nicht authentifizieren) Benutzer erfolgt, wird vom Reverse Proxy abgefangen. Anstatt der angeforderten Seite wird dem Benutzer eine Login-Seite des Proxy präsentiert.
- Die User-Credentials werden wiederum vom Reverse Proxy abgefangen und damit eine Authentifizierung gegen ein Backend System (LDAP, Datenbank...) durchgeführt.
- Das Login ist damit abgeschlossen und es erfolgt ein Redirect auf die ursprünglich angefragte URL, umgesetzt durch das im Reverse Proxy definierte Mapping.

midpoints purify it

Warum benötige ich einen Reverse Proxy?



midpoints purify it

Warum benötige ich einen Reverse Proxy?

Wie läuft das Login ab?

Bei Verwendung eines authentisierenden Reverse Proxy besitzt ein Benutzer in der Regel jedoch zwei Sessions:

- Eine mit dem Reverse Proxy und eine mit dem Webserver.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Wie wird die Proxy Anmeldung an den Webserver weitergegeben ?

sehr sehr sehr spannend
insbesondere mit Domino

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Die Lösung für ein Single Sign On zwischen mehreren IBM Server-Systemen (Domino, Sametime, Websphere)

ist eine Multi Session Authentifizierung per **LTPA Token** zu verwenden.

Bedeutet: Damit die Proxy Anmeldung auch für Lotus Traveler verwendet werden kann, muß mein Proxy in der Lage sein nach erfolgreicher Anmeldung ein LTPA-Token auszustellen.

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Lightweight Third-Party Authentication *(LTPA, „leichtgewichtige Authentifizierung durch Dritte“) ist eine Authentifizierungstechnik, die in den Software-Produkten IBM Websphere und Lotus Domino verwendet wird.*

Beim Zugriff auf Webserver, die LTPA verwenden, ist es für einen Anwender möglich, seine Benutzeranmeldung serverübergreifend zu verwenden, was auch als Single Sign-on bezeichnet wird.

Quelle: Wikipedia

midpoints purify it

Warum benötige ich einen Reverse Proxy?

Für einen Apache Reverse Proxy müßte ein Plugin existieren, das ein gültiges LTPA-Token generieren kann.

Hab ich dies nicht, muß sich der Anwender zweimal anmelden:

Erst am Reverse Proxy und dann nochmals am Domino Server.

Für den Zugriff auf iNotes evt. noch zumutbar, leider unterstützt Traveler nicht diese doppelte Anmeldung.

Warum benötige ich einen Reverse Proxy?

Falls bereits ein Reverse Proxy vorhanden ist und eine Anmeldung am Reverse Proxy benötigt wird, muß dieser LTPA unterstützen.
Für Apache gibt es meines Wissens kein fertiges LTPA-Plugin.

Ansätze hierzu sind auf OpenNTF zu finden:
SSO zwischen Domino & Apache Tomcat
http://www.openntf.org/Projects/pmt.nsf/ProjectLookup/DominoTomcatSSO

oder Blog Per Henrik Lausten:
How to create your own LTPA session cookie
http://per.lausten.dk/blog/2009/04/how-to-create-your-own-ltpa-session-cookie.html

Warum benötige ich einen Reverse Proxy?

IBM bietet selbst zwei Lösungen an, die als Secure Reverse Proxy mitverwendet werden können bzw. neben anderen Dingen ähnliche Funktionen zur Verfügung stellen:

1. Tivoli Access Manager = TAM
2. Lotus Mobile Connect = LMC

Beide unterstützen LTPA und bieten ein Single Sign On über die IBM-Welt.

midpoints purify it

Lotus Mobile Connect

midpoints purify it

Lotus Mobile Connect

Überblick und online kaufen | Produktmerkmale und Vorteile (auf Englisch)

Ermöglicht es Unternehmen, Anwendungen über viele verschiedene drahtlose und drahtgebundene Netze effizient auf mobile Mitarbeiter auszudehnen

IBM Lotus Mobile Connect ist eine dezentrale, skalierbare, vielseitig einsetzbare Kommunikationsplattform. Sie wurde dafür konzipiert, die Bandbreite zu optimieren, die Kosten zu senken und die Sicherheit zu erhöhen. Sie erstellt ein mobiles virtuelles privates Netz (VPN), das Daten bei potenziell angreifbaren drahtlosen LAN- und drahtlosen WAN-Verbindungen verschlüsselt. Sie integriert viele gebräuchliche drahtlose Trägernetze (mit und ohne IP), Server-Hardware, Gerätebetriebssysteme und Sicherheitsprotokolle für Mobilbetrieb. Unterstützte Clients sind Windows Mobile V5 sowie Windows Vista-Workstations und die Geräte Nokia E50, E60, E61, E62, E70 und E90 (neu in den letzten Releases).

Lotus Mobile Connect (das Nachfolgerelease von IBM WebSphere Everyplace Connection Manager) kann mit IBM WebSphere Portal, IBM Lotus Expeditor, IBM Lotus Sametime, IBM Lotus Notes und IBM Workplace Forms verwendet werden, um Geschäftsanwendungen zu verschlüsseln und auf mobile Benutzer auszudehnen. Es handelt sich um eine wesentliche Komponente in der Infrastrukturlösung der Benutzerplattform und in vielen Branchenlösungen von IBM.

Lotus Mobile Connect

Services für mobilen Zugriff (VPN)
Ein optimierter und gesicherter IP-Tunnel wird für die Kommunikation mit der Mobility Client-Software auf dem PC / Device erstellt.
VPN-Zugang mit optimierter Bandbreitennutzung für mobile Netze.

HTTP-Kommunikation (Secure HTTP Reverse Proxy)
Bietet gesicherte HTTP-Kommunikation im Tunnelungsverfahren für HTTP-Clients.

Nachrichtenübertragungsservices (Pager / SMS Gateway)
Ermöglicht einer Anwendung, Nachrichten über mobile Netze an Nachrichtenübertragungs-Clients wie Pager oder Telefone zu senden.

Lotus Mobile Connect

Lotus Mobile Connect LMC
aktuelle Version 6.1.4

Server:
Windows - 2003/2008 Server (32 & 64 Bit)
Linux – Red Hat Enterprise & SuSE Enterprise Server
AIX

Mobility (VPN) Clients:
Microsoft Windows 2000, XP, Vista, 7
Mac
Linux (Red hat, SuSE, Novell)

Windows Mobile inkl. 6.5, Symbian (ausgewählte Devices), ~~Palm~~

Browser:
IE, Firefox, Safari, Chrome

midpoints purify it

Lotus Mobile Connect

Soll LMC lediglich als Reverse Proxy für iNotes oder Lotus Traveler verwendet werden, werden auf den Endgeräten keine speziellen Clients benötigt.

LMC stellt dann lediglich für HTTP einen sicheren zentralen Zugangspunkt zur Verfügung.

LMC ist dann verantwortlich für die Anmeldung & Verschlüsselung.

midpoints purify it

Lotus Mobile Connect

Kosten: LMC wird pro Server und CAL lizenziert.

Das schöne in der Lotus Notes Lizenz ist seit 8.5.1, die LMC CAL Lizenz enthalten. Somit muß lediglich „nur“ der Server lizenziert werden:

Detaillierte Preisliste

Auswahl	Artikelbeschreibung	'IBM Preis ohne Steuern	'IBM Preis mit Steuern
☐	IBM Lotus Mobile Connect Authorized User License + SW Subscription & Support 12 Months (D59QLLL)	92.33	110.80
☐	IBM Lotus Mobile Connect Processor Value Unit (PVU) License + SW Subscription & Support 12 Months (D59QKLL)	54.22	65.06

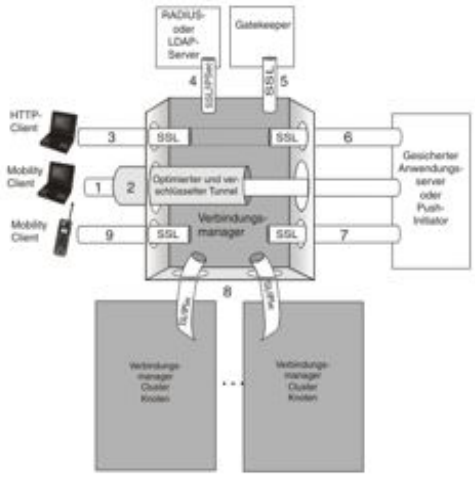
http://www.edbrill.com/ebrill/edbrill.nsf/dx/announcing-notesdomino-8.5.1-part-3-lotus-mobile-connect

midpoints purify it

Funktionsweise & Konfiguration

midpoints purify it

Funktionsweise & Konfiguration



LMC Connection Manager
LMC Gatekeeper
LMC Access Manager

Datenspeicher
LDAP Verzeichnis

Browser / LMC Mobile Client

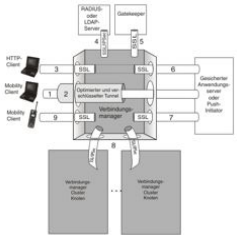
midpoints purify it

Funktionsweise & Konfiguration

LMC Connection Manager

Der Verbindungsmanager ist die Hauptkomponente.

Auf den Verbindungsmanager greifen die Clients zu. Der Verbindungsserver verwaltet die Clientzugriffe und leitet diese an die internen Ressourcen weiter.



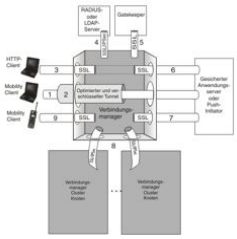
midpoints purify it

Funktionsweise & Konfiguration

LMC Gatekeeper

Der Gatekeeper ist der Java basierte Administrationsclient von Lotus Mobile Connect.

Der Gatekeeper kann auf dem LMC mitinstalliert oder auf einem getrennten System installiert werden.

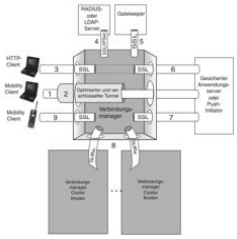


midpoints purify it

Funktionsweise & Konfiguration

Datenspeicher

Der Verbindungsmanager ließt seine Konfiguration aus einem persistenten Datenspeicher aus und legt Session-informationen und Zugriffsdaten dort ab.



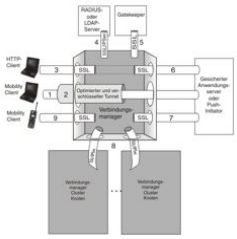
Als Datenspeicher kann für Pilotinstallationen eine mit
dem Connection Manager mitinstallierte Cloudscape Datenbank verwendet werden. Für den produktiven Einsatz wird eine DB2 Datenbank empfohlen.

midpoints purify it

Funktionsweise & Konfiguration

LMC Access Manager

Der Access Manager wird mit dem Verbindungs-manager auf dem LMC Server installiert.



Beim Access Manager handelt es sich um einen getrennten Service, welcher vom Verwaltungsclient (Gatekeeper) verwendet wird.

Der Access Manager ist dafür verantwortlich Konfigurationsänderungen in die Datenbank zu übernehmen und den Verbindungs-manager dynamisch zu aktualisieren.

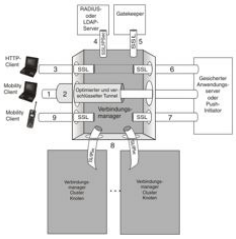
midpoints purify it

Funktionsweise & Konfiguration

LDAP / Radius

LMC unterstütz zur Authentifizierung der Benutzer LDAP oder Radius.

Auf diesen Weg kann ein Domino Directory oder ein Active Directory integriert werden.

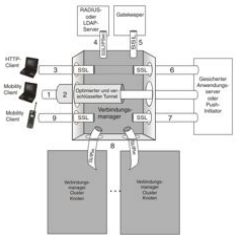


midpoints purify it

Funktionsweise & Konfiguration

7 - Installationsschritte

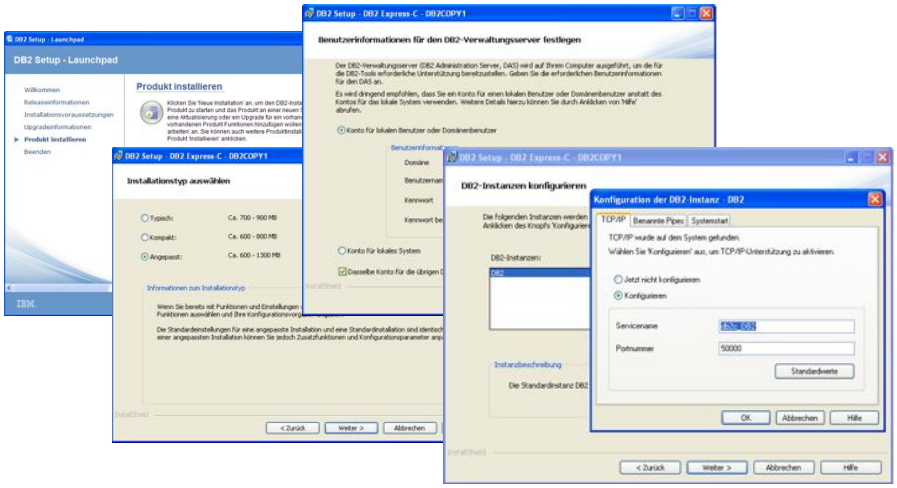
1. Basisbetriebssystem & Härtung
2. Installation & Konfiguration DB2|DB2 Express
3. Installation Connection Manager
4. Installation Gatekeeper
5. Einrichtung LDAP Server
   (Konfiguration Domino LDAP-Task)
6. Erstkonfiguration per Gatekeeper



midpoints purify it

Funktionsweise & Konfiguration

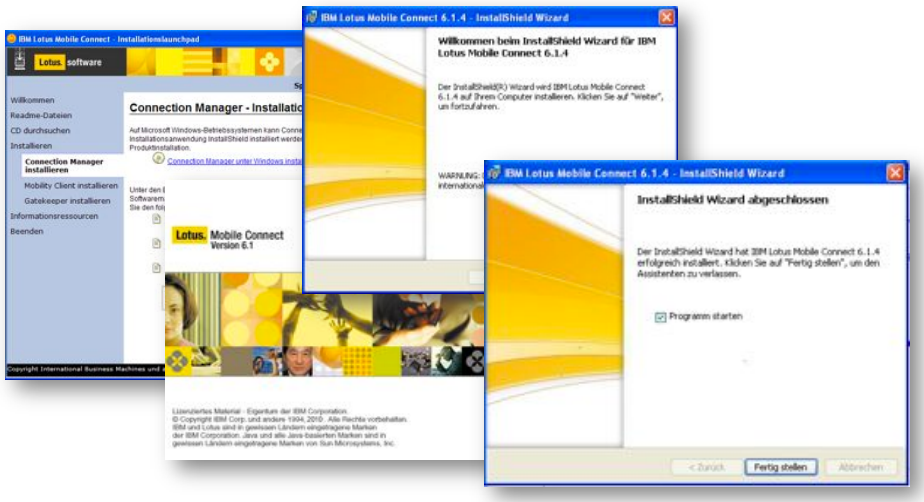
2. Installation & Konfiguration DB2 Express 9.7.2



midpoints purify it

Funktionsweise & Konfiguration

3. Installation Connection Manager 6.1.4 (CZDI2ML)

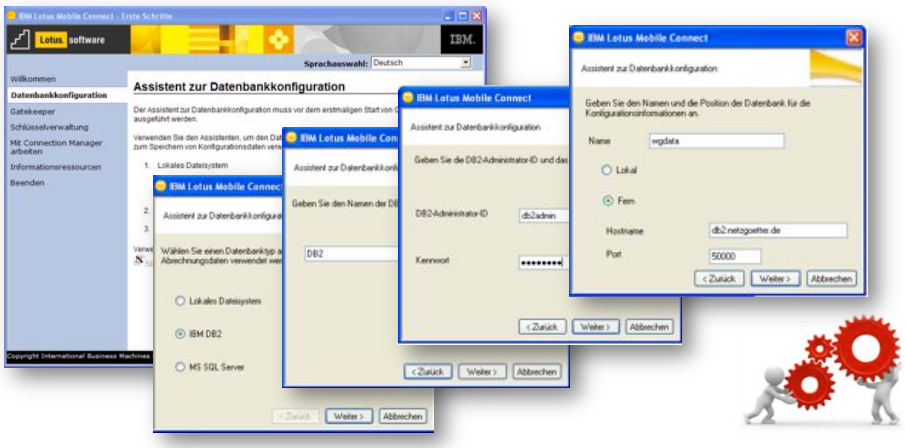


midpoints purify it

Funktionsweise & Konfiguration

3. **Installation Connection Manager 6.1.4 (CZDI2ML)**

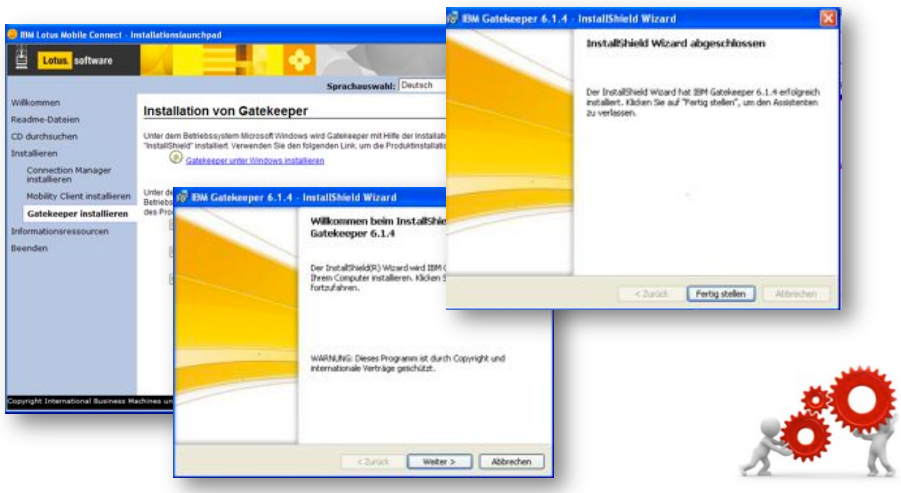
Unter Windows startet automatisch der Konfigurationsassistent



midpoints purify it

Funktionsweise & Konfiguration

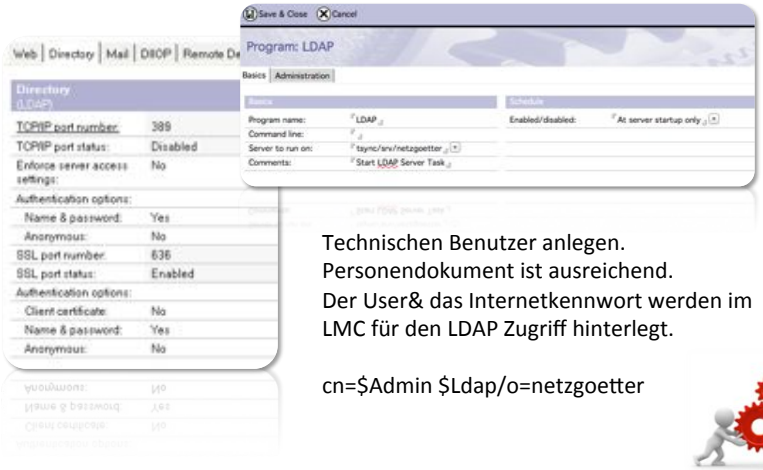
4. **Installation LMC Gatekeeper 6.1.4**



midpoints purify it

Funktionsweise & Konfiguration

5. **Einrichtung LDAP – Domino LDAP-Task**



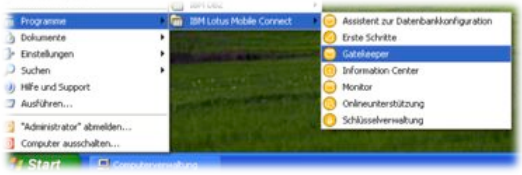
Technischen Benutzer anlegen.
Personendokument ist ausreichend.
Der User& das Internetkennwort werden im LMC für den LDAP Zugriff hinterlegt.

cn=$Admin $Ldap/o=netzgoetter

midpoints purify it

Funktionsweise & Konfiguration

6. **Erstkonfiguration per Gatekeeper** (vorher das System einmal booten)



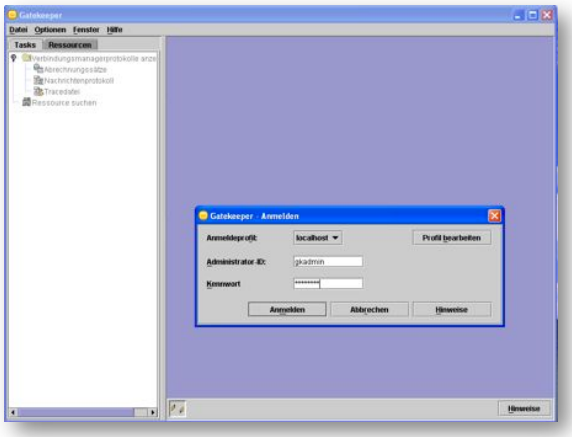
Der Gatekeeper verbindet sich über den TCP Port 9555 mit dem Access Manager

Administrator-ID: gkadmin
Kennwort: gk4admin

midpoints purify it

Funktionsweise & Konfiguration

6. **Erstkonfiguration per Gatekeeper**



Der Gatekeeper verbindet sich über den TCP Port 9555 mit dem Access Manager

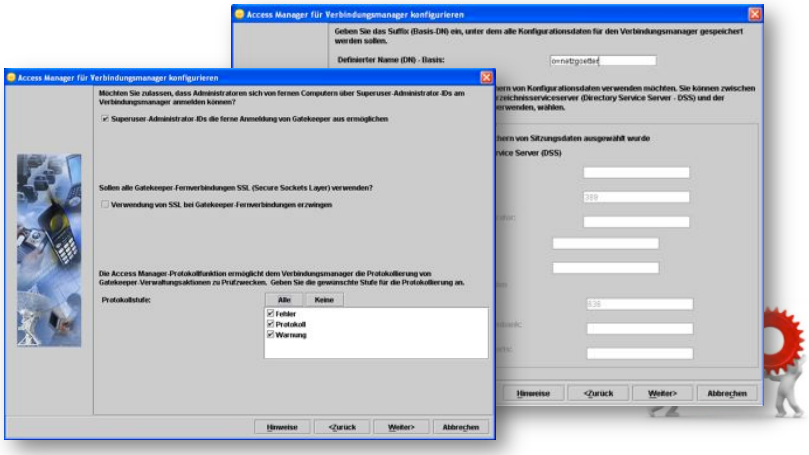
Administrator-ID: gkadmin
Kennwort: gk4admin

midpoints purify it

Funktionsweise & Konfiguration

6. **Erstkonfiguration per Gatekeeper**

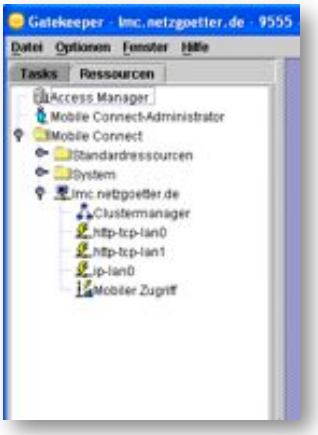
Beim ersten Start des Gatekeepers startet ein Einrichtungsassistent der eine Initialkonfiguration durchführt, die später angepasst wird.



midpoints purify it

Funktionsweise & Konfiguration

Ergebnis der Erstkonfiguration



midpoints purify it

Lotus Traveler & Lotus Mobile Connect

midpoints purify it

Lotus Traveler & Lotus Mobile Connect

midpoints purify it

Lotus Traveler & Lotus Mobile Connect

Um Lotus Traveler über Lotus Mobile Connect zur Verfügung zu stellen, wird folgendes benötigt:

1. Einen installierten Lotus Traveler Server in der DMZ-Zone 2
   Hostname: travint.netzgoetter.de
2. Das LDAP Verzeichnis welches der LMC zur Authentifizierung verwendet. (Domino-LDAP des travint.netzgoetter.de)
3. Externer DNS Name des LMC: lmc.netzgoetter.de

midpoints purify it

Lotus Traveler & Lotus Mobile Connect

4. Firewall-Regeln:

Internet	→DMZ1:	Port 80/443 auf lmc.netzgoetter.de
DMZ1	→DMZ2:	Port 80/443 auf travint.netzgoetter.de
DMZ1	→DMZ2:	Port 636 auf travint.netzgoetter.de (LDAP)
DMZ2	→Intern:	Port 1352 auf Domino Mail-Server

midpoints purify it

Lotus Traveler & Lotus Mobile Connect

5. SSL-Keys:

Die Kommunikation zwischen Endgerät und LMC sollte auf jeden Fall verschlüsselt werden.
Hierfür wird ein SSL Zertifikat (lmc.netzgoetter.de) benötigt.

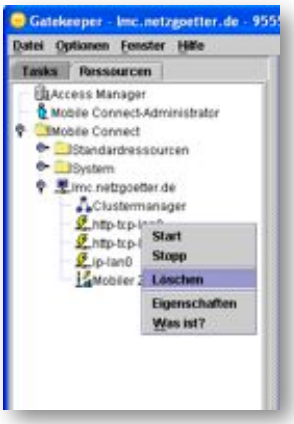
Ratsam insbesondere für Traveler ein off. Zertifikat zu erwerben. Ein Thawte Zertifikat kostet für drei Jahre nur ca. 200€.

Die Verbindung zwischen LMC und Traveler sollte auch per SSL verschlüsselt werden, hierfür kann ein selbstgeneriertes Zertifikat verwendet werden.

midpoints purify it

Lotus Traveler & Lotus Mobile Connect

6. LMC-Konfiguration – Bereinigung der Default-Config



midpoints purify it

Lotus Traveler & Lotus Mobile Connect

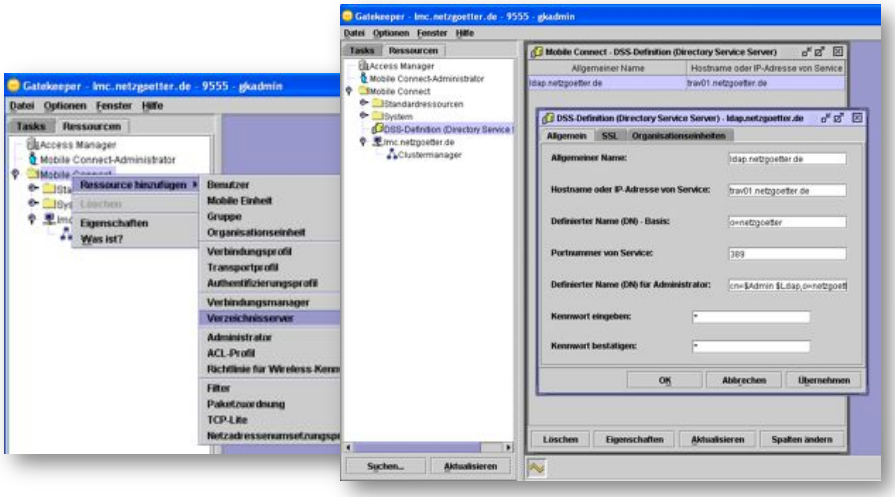
7. **LMC-Konfiguration – 3 Schritte**

a. LDAP Verzeichnis definieren
b. Authentifizierungsprofil erstellen
c. HTTP Zugriffsprofil anlegen

midpoints purify it

Lotus Traveler & Lotus Mobile Connect

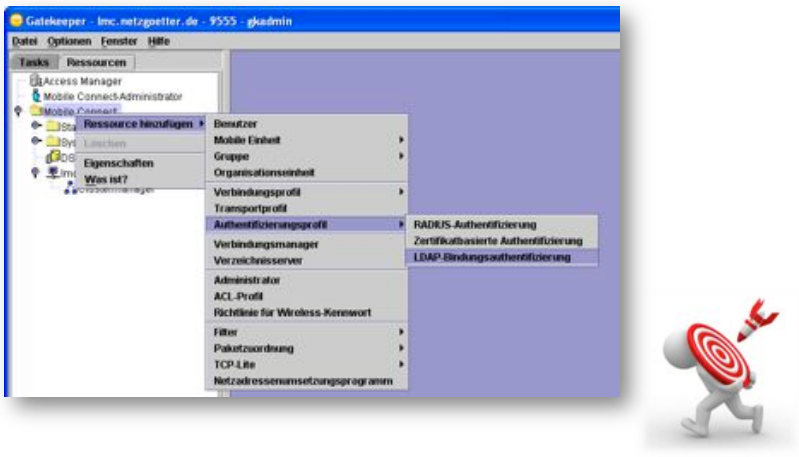
7. LMC-Konfiguration – LDAP Verzeichnis definieren



midpoints purify it

Lotus Traveler & Lotus Mobile Connect

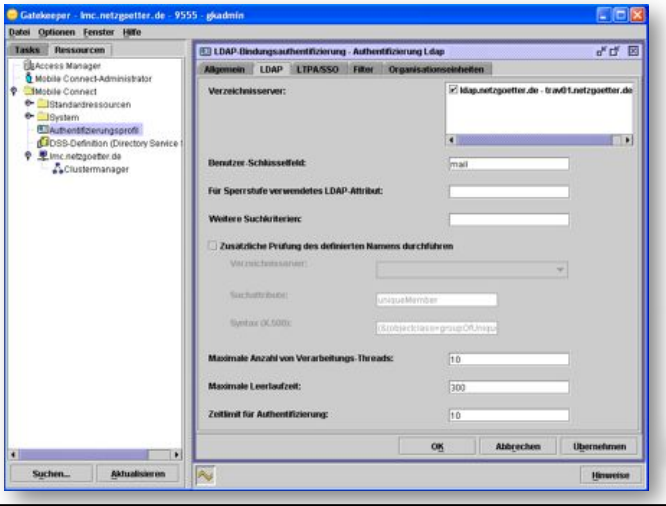
7. LMC-Konfiguration – Authentifizierungsprofil erstellen



midpoints purify it

Lotus Traveler & Lotus Mobile Connect

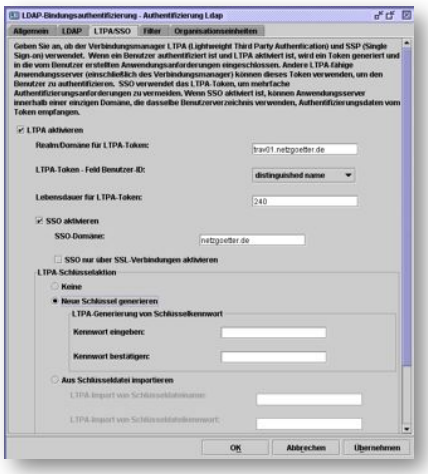
7. LMC-Konfiguration – Authentifizierungsprofil erstellen



midpoints purify it

Lotus Traveler & Lotus Mobile Connect

Im Authentifizierungsprofil erfolgt die LTPA / SSO Konfiguration



Es wird ein neues Token erzeugt.

Die Realm Domain ist der Name des verwendeten LDAP Servers: trav01.netzgoetter.de

Das Token ist 240 min gültig und wird für die Domain netzgoetter.de ausgestellt.

Das erzeugte Token wird anschließend In eine Datei exportiert: netzgoetter-ltpa.token

midpoints purify it

Lotus Traveler & Lotus Mobile Connect

8. LMC-Konfiguration – HTTP Zugriffsprofil anlegen

midpoints purify it

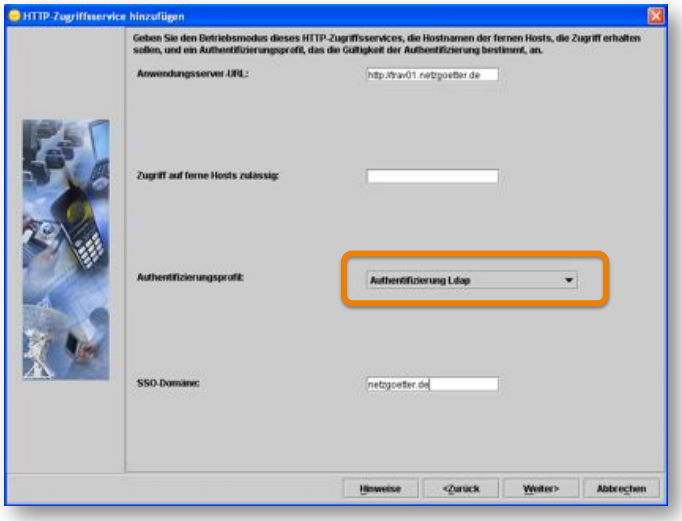
Lotus Traveler & Lotus Mobile Connect

8. LMC-Konfiguration – HTTP Zugriffsprofil anlegen

midpoints purify it

Lotus Traveler & Lotus Mobile Connect

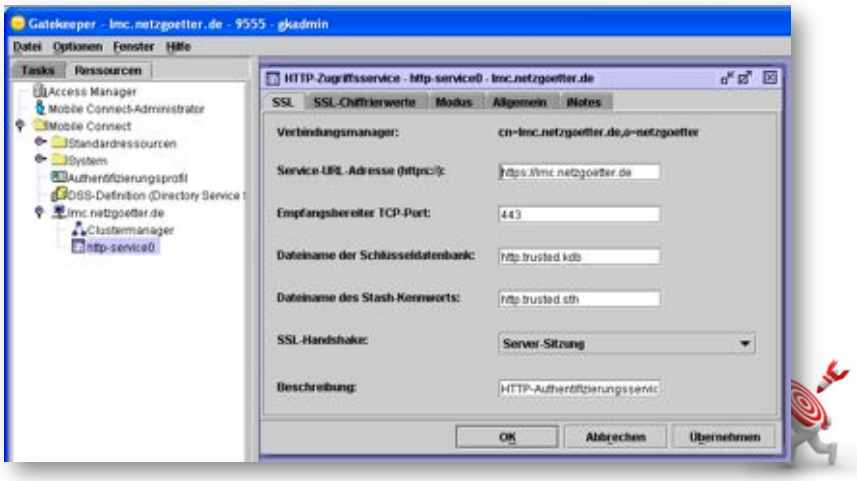
8. LMC-Konfiguration – HTTP Zugriffsprofil anlegen



midpoints purify it

Lotus Traveler & Lotus Mobile Connect

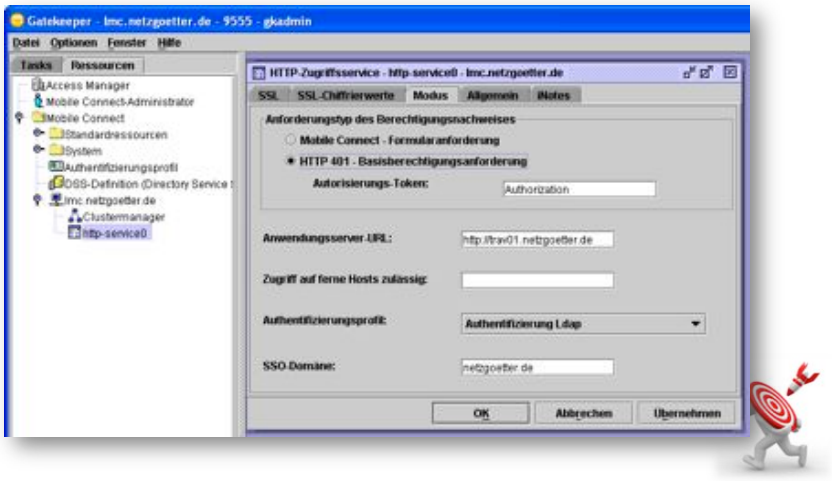
8. LMC-Konfiguration – HTTP Zugriffsprofil anpassen



midpoints purify it

Lotus Traveler & Lotus Mobile Connect

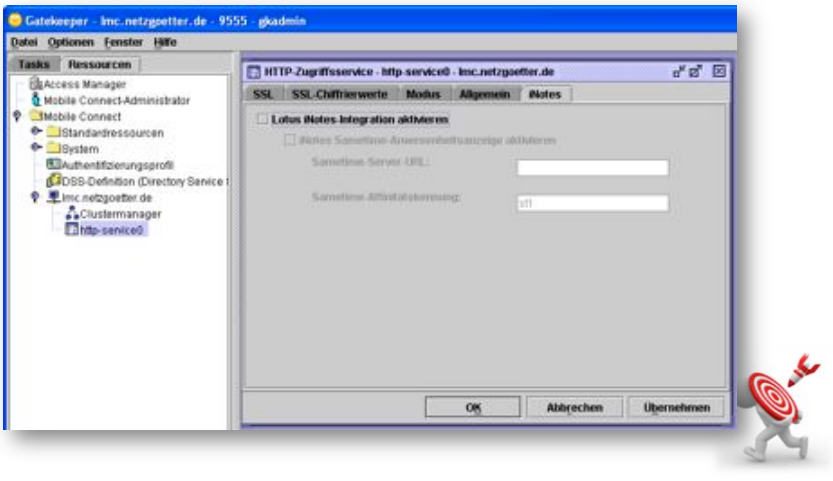
8. LMC-Konfiguration – HTTP Zugriffsprofil anpassen



midpoints purify it

Lotus Traveler & Lotus Mobile Connect

8. LMC-Konfiguration – HTTP Zugriffsprofil anpassen



midpoints purify it

Lotus Traveler & Lotus Mobile Connect

9. LMC-Konfiguration – SSL Konfigurieren

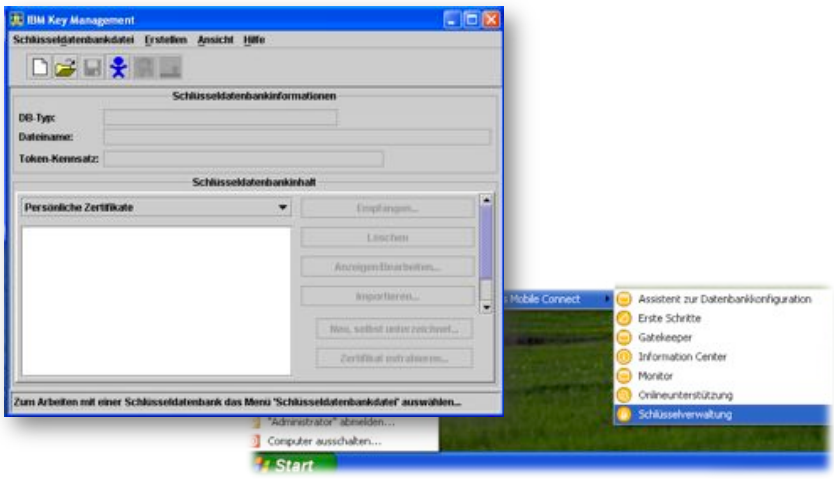
LMC erwartet, das die SSL-Zertifikate in einer Schlüsseldatenbank (Key-Store) liegen. Benötigte SSL Keys müssen somit in einem eigenen Keystore bereitgestellt werden.

Zur Anlage eines Keystores und der Verwaltung der Keys wird mit dem Connection Manager der allseits „beliebte“ IBM Key Manager (Schlüsselverwaltung) mitinstalliert.

midpoints purify it

Lotus Traveler & Lotus Mobile Connect

9. LMC-Konfiguration – SSL Konfigurieren

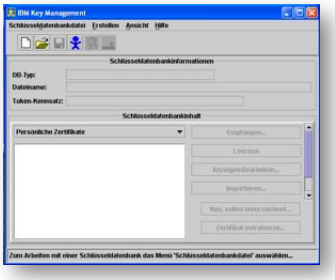


midpoints purify it

Lotus Traveler & Lotus Mobile Connect

9. LMC-Konfiguration – SSL Konfigurieren

- Neue Schlüsseldatenbank anlegen
  Format: CMS
  Option: Kennwort in Stash
  Datei speichern aktivieren
- Import evt. benötigter Root-Zertifikate inkl. Zertifikatskette
- Import des eigentlichen Server-zertifikats im PKCS12 Format

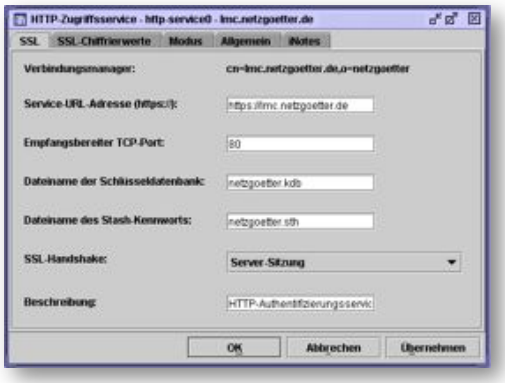


midpoints purify it

Lotus Traveler & Lotus Mobile Connect

9. LMC-Konfiguration – SSL Konfigurieren

Die neu erzeugte Schlüsseldatenbank wird im HTTP-Service hinterlegt:



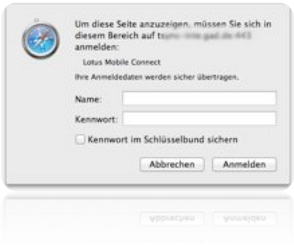
midpoints purify it

Lotus Traveler & Lotus Mobile Connect

LMC-Konfiguration - DONE

Die eigentliche LMC Einrichtung ist nun abgeschlossen.

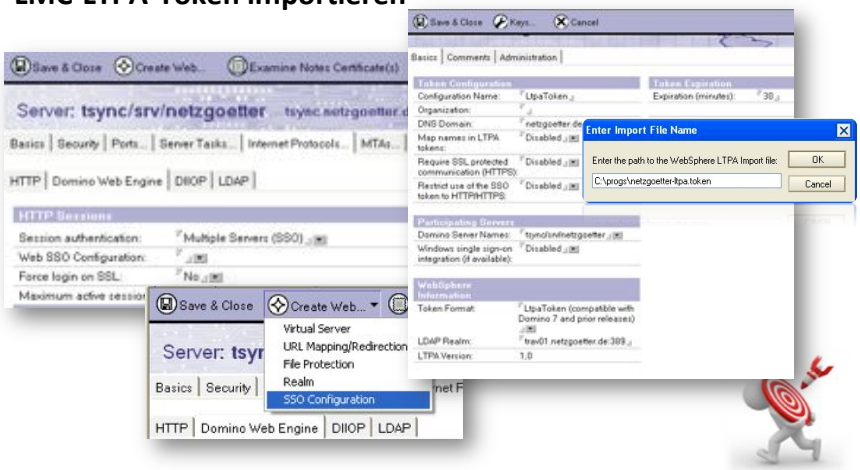
Wenn alle Firewall-Port und DNS Einträge korrekt sind, wird nun beim Zugriff auf https://lmc.netzgoetter.de das LMC Login angezeigt:



midpoints purify it

Lotus Traveler & Lotus Mobile Connect

Domino Multi Server SSO Authentifizierung aktivieren & LMC-LTPA-Token importieren



midpoints purify it

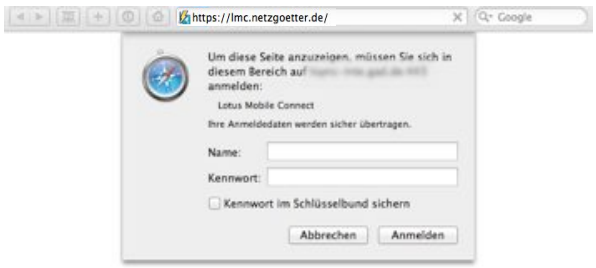
Lotus Traveler & Lotus Mobile Connect

Traveler External URL anpassen

midpoints purify it

Lotus Traveler & Lotus Mobile Connect

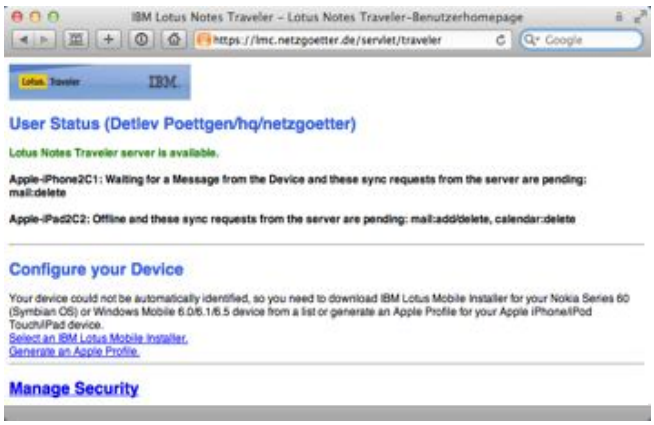
That's it – Anmeldung am LMC



midpoints purify it

Lotus Traveler & Lotus Mobile Connect

That's it – Nach Anmeldung am LMC – SSO mit Domino



midpoints purify it

Vielen Dank!

Mein Blog
(Präsentation + Links):

http://www.netzgoetter.net