

# GATE Manual

Thimo Langbehn

4. April 2009

## Inhaltsverzeichnis

<b>1</b>	<b>Kerberos</b>	<b>3</b>
1.1	Voraussetzungen . . . . .	3
1.2	Programme . . . . .	3
1.3	Konfiguration . . . . .	3
1.3.1	Windows XP . . . . .	4
1.3.2	Windows 7 64Bit oder Vista 64Bit . . . . .	4
1.4	Verwendung . . . . .	4
1.4.1	Leash für Windows . . . . .	4
1.4.2	Passwort ändern . . . . .	5
1.5	Fehlerbehebung . . . . .	5
<b>2</b>	<b>SSH Client</b>	<b>6</b>
2.1	Voraussetzungen . . . . .	6
2.2	Konfiguration . . . . .	6
2.3	Test . . . . .	6
2.4	Fehlerbehebung . . . . .	7
2.4.1	Sofortiges Ende bei Verbindungsaufbau . . . . .	7
<b>3</b>	<b>SCP</b>	<b>7</b>
3.1	Voraussetzungen . . . . .	7
3.2	Konfiguration . . . . .	7
3.3	Test . . . . .	7
3.4	Fehlerbehebung . . . . .	8
3.4.1	Authentifizierung schlägt fehl . . . . .	8
<b>4</b>	<b>Maildienste</b>	<b>8</b>
4.1	Mailclient Voraussetzungen . . . . .	8
4.2	Mailclient Programme . . . . .	8
4.3	Mailclient Konfiguration . . . . .	9
4.3.1	Direktes SMTP . . . . .	9
4.3.2	Mozilla Thunderbird für Windows XP . . . . .	9
4.3.3	Mozilla Thunderbird für Windows 7 64Bit oder Vista 64Bit	10
4.3.4	Mozilla Thunderbird für Linux . . . . .	11
4.3.5	Evolution auf Linux . . . . .	12
4.3.6	Mutt auf Linux . . . . .	13
4.3.7	Getunneltes SMTP für Windows . . . . .	13
4.3.8	Getunneltes SMTP für Linux . . . . .	14

4.4	Mailclient Fehlerbehebung . . . . .	14
4.4.1	Mozilla Thunderbird . . . . .	14
4.4.2	Getunneltes SMTP . . . . .	14
4.4.3	Tunnelprobleme unter Windows . . . . .	14
4.4.4	Tunnelprobleme unter Linux . . . . .	15
4.5	Mail Sammeldienst . . . . .	15
4.6	Mail-Aliasadressen . . . . .	16
4.7	Mailverteiler . . . . .	17
4.8	Mailweiterleitung . . . . .	17
<b>5</b>	<b>HTTP / HTTPS</b>	<b>17</b>
5.1	Voraussetzungen . . . . .	17
5.2	Programme . . . . .	17
5.3	Konfiguration . . . . .	17
5.3.1	Allgemein . . . . .	17
5.3.2	Firefox für Windows XP . . . . .	18
5.3.3	Firefox für Windows 7 64Bit oder Vista 64Bit . . . . .	18
5.4	Test . . . . .	18
5.5	Fehlerbehebung . . . . .	19
5.5.1	Access denied . . . . .	19
5.5.2	Zertifikat-Warnung . . . . .	19
<b>6</b>	<b>FTP</b>	<b>19</b>
6.1	Voraussetzungen . . . . .	19
6.2	Programme . . . . .	19
6.3	Konfiguration . . . . .	19
6.3.1	Filezilla . . . . .	20
<b>7</b>	<b>SVN</b>	<b>20</b>
7.1	Voraussetzungen . . . . .	20
7.2	Programme . . . . .	20
7.3	Konfiguration . . . . .	21
7.3.1	Tortoise SVN . . . . .	21
7.4	Verwendung . . . . .	21
7.5	Test . . . . .	21
7.5.1	Windows . . . . .	21
7.6	Migration von Alten Checkouts (Working Copy) . . . . .	21
7.6.1	Windows . . . . .	21
<b>8</b>	<b>Synchronisierung</b>	<b>22</b>
8.1	Voraussetzungen . . . . .	22
8.2	Konfiguration . . . . .	22
8.3	Test . . . . .	24
<b>9</b>	<b>SQL Datenbank</b>	<b>24</b>
9.1	Voraussetzungen . . . . .	24
9.2	Programe . . . . .	24
9.3	Konfiguration . . . . .	24
9.3.1	Konfiguration pgadmin3 . . . . .	24
9.3.2	Konfiguration psql . . . . .	24

<b>10 Andrew File System (AFS)</b>	<b>25</b>
10.1 Voraussetzungen	25
10.2 Programme	25
10.3 Konfiguration	25
10.3.1 OpenAFS für Windows XP	25
10.3.2 OpenAFS auf Windows 7 64Bit oder Vista 64Bit	26
10.4 Test	26
10.5 Fehlerbehebung	26

## 1 Kerberos

Um in den vollen Genuss der Möglichkeiten eines Kerberos-Systems (Single Sign On) zu kommen muss man eine Kerberos-Implementierung installieren. Die Implementierung besteht im wesentlichen aus einer Kerberos Bibliothek und einigen Programmen zur Ticket(cache) Verwaltung.

### 1.1 Voraussetzungen

- Die Namensauflösung für die Domäne „**g4t3.de**“ muss funktionieren.
- Der Host „**auth.g4t3.de**“ muss erreichbar sein (**UDP Port 88**).

### 1.2 Programme

**Windows XP** Hierfür gibt es das MIT Kerberos for Windows (KfW). Es existieren zwei Versionen, eine ältere, Leash, und eine neuere, der Network Identity Manager (NIM). Zweiterer integriert das AFS besser, ist möglicherweise aber noch nicht ganz Fehlerfrei.

- Leash 32Bit: <http://mit.edu/kerberos/dist/kfw/2.6/kfw-2.6.5/MITKerberosForWindows-2.6.5.msi>
- NIM 32Bit: <http://mit.edu/kerberos/dist/kfw/3.2/kfw-3.2.2/kfw-3-2-2.msi>

**Windows 7 64Bit oder Vista 64Bit** Bei diesen Systemen kann man entweder eine 32-Bit Variante installieren (siehe oben) oder aber 64Bit Programme. Wichtig ist, dass alle Programme die Kerberos nutzen sollen ebenfalls in 32Bit bzw. 64Bit installiert werden.

**Hinweis:** Einige Programmen sind unter 64Bit Windows noch nicht mit Kerberos nutzbar, dies betrifft insbesondere SVN (TortoiseSVN) und SSH (PuTTY).

- Leash 64Bit: <http://www.secure-endpoints.com/binaries/mit-kfw-3-2-2/kfw-amd64-3-2-2.msi>
- NIM 64Bit: [http://www.secure-endpoints.com/binaries/kcaplugin-amd64-2\\_2\\_0\\_2.msi](http://www.secure-endpoints.com/binaries/kcaplugin-amd64-2_2_0_2.msi)

## 1.3 Konfiguration

Die Bibliothek muss über eine Konfigurationsdatei eine Liste von sogenannten Realm Spezifikationen erhalten, um einer DNS Adresse einen Realm, und diesem einen KDC-Server zuzuordnen. Sie muss wie folgt abgeändert werden:

```
http://www.g4t3.de/download/krb5.ini
```

```
[libdefaults]
    default_realm = G4T3.DE
    dns_lookup_kdc = true

[realms]
    G4T3.DE = {
        admin_server = auth.g4t3.de
        kdc = auth.g4t3.de
    }

[domain_realm]
    .g4t3.de = G4T3.DE
    g4t3.de = G4T3.DE
```

```
[logging]
```

Die restlichen Realm-Beschreibungen (in der Sektion **[Realms]**) können bestehen bleiben, werden aber für uns nicht benötigt.

Diese Datei ist insofern nicht sicherheitskritisch, als dass sie problemlos gelesen werden darf. Schreibzugriff sollte allerdings nur einem Administrator gestattet sein. Ansonsten könnte durch Manipulation der **kdc** und **admin\_server** Adresse eine Spoofing-Attake eingeleitet werden.

### 1.3.1 Windows XP

Unter Windows heißt diese Datei „**krb5.ini**“, und befindet sich standardmäßig im Windows-Verzeichnis.

Nach den oben beschriebenen Anpassung muss unter Windows Leash bzw. der NIM neu gestartet werden. Um andere Anwendungen mit Kerberos zusammenzubringen, muss noch die „**krb5\_32.dll**“ aus dem Kerberos Programmverzeichnis in das **Windows/System32** Verzeichnis kopiert werden. Nach diesen Einstellungen muss Windows **zwei mal** neu gestartet werden.

### 1.3.2 Windows 7 64Bit oder Vista 64Bit

Unter Windows heißt diese Datei „**krb5.ini**“, und befindet sich standardmäßig im Windows-Verzeichnis.

Nach den oben beschriebenen Anpassung muss unter Windows Leash bzw. der NIM neu gestartet werden. Um andere Anwendungen mit Kerberos zusammenzubringen, muss noch die „**krb5\_64.dll**“ aus dem Kerberos Programmverzeichnis in das **Windows/System32** Verzeichnis kopiert werden. Nach diesen Einstellungen muss Windows **zwei mal** neu gestartet werden.

## 1.4 Verwendung

Voraussetzungen für die Verwendung von Kerberos sind die oben beschriebenen Einstellungen, eine bestehende Netzwerkverbindung (Internet) und Verfügbarkeit des korrekten DNS-Servers. Ein **ping auth.g4t3.de** sollte möglich sein. Weiterhin muss die Uhrzeit des Rechners korrekt eingestellt sein.

### 1.4.1 Leash für Windows

**Zeitsynchronisation** In Windows kann die Zeit Synchronisation bequem per **Action -> Synchronize Time** in Leash erfolgen.

**Einloggen** Nach dem Start von Leash kann in diesem mittels **Action -> Get Ticket(s)** oder CTRL+T kann nun ein Ticket Granting Ticket (TGT) angefordert werden. Name und Passwort müssen die de eigenen Accounts sein, der Realm muss dabei auf **G4T3.DE** stehen. Wenn die Aktion erfolgreich war, so befindet sich nun in dem unteren Bereich des Fensters ein grünes Symbol mit dem Eintrag **user@G4T3.DE**.

### Passwort ändern 1.4.2 Passwort ändern

Das Passwort kann geändert werden, indem man sich per ssh auf z.B. **dev.g4t3.de** einwählt, und dort das Programm **\$> kpasswd** aufruft.

## 1.5 Fehlerbehebung

1. Synchronisiere die Zeit mit einem Internet-Zeitserver. Sollte dies mit einer Fehlermeldung abbrechen, oder die Zeit nicht korrekt synchronisiert werden, so kann eine Ursache dafür in einer dazwischenliegenden Firewall liegen. In diesem Fall kann die Zeit auch manuell gestellt werden. Sie muss nur innerhalb einer Toleranz von 5 Minuten korrekt sein.
2. führe ein **\$> ping 193.34.68.209** aus. Wenn dieser Ping nicht möglich ist, so erlaubt eine zwischen dem Client (dir) und dem Server liegende Firewall diese Operation nicht. Hier kann entweder ein weniger restriktives Netz um testen aufgesucht werden, oder die Einstellungen der Firewall angepasst werden.
3. führe ein **\$> ping auth.g4t3.de** aus, dabei sollte der Name in die korrekte IP (**193.34.68.209**) aufgelöst werden.

Funktioniert dieser Test nicht, der obrige aber schon, dann arbeitet die DNS-Auflösung nicht richtig. Dass kann an einem fehlerhaften Nameserver liegen, oder auch an überschreibenden Einstellungen des Clients bzw. alten Werten in dessen Puffer.

**Eine andere IP (nicht 193.34.68.209) wird angezeigt** Irgendein Nameserver oder Cache liefert die falschen Werte zurück. Überprüfe die hosts Datei. Diese findet sich unter Windows in „**C:\Windows\System32\drivers\etc\hosts**“, und unter Linux in **/etc/hosts**. Suche nach Einträgen der Domain „**g4t3.de**“. Diese sollten entfernt werden, sie sind nur nötig wenn der Nameserver keine korrekten Ergebnisse liefert.

**Es wird gar keine IP angezeigt** Die Domäne wird von dem lokalen Nameserver nicht richtig aufgelöst. Trage die folgenden Einträge in die oben genannte hosts Datei ein:

```
193.34.68.209 auth.g4t3.de
193.34.68.210 info.g4t3.de
193.34.68.211 mail.g4t3.de
193.34.68.212 data.g4t3.de
193.34.68.213 www.g4t3.de
```

4. Überprüfe deine Firewall, ob sie ausgehende Verbindungen zum **Port 88** von **193.34.68.209** zulässt. Ein Test in einer weniger restriktiven Umgebung kann Unklarheiten bezüglich anderer, dazwischen liegender Umgebungen beseitigen).

## 2 SSH Client

Als SSH Client wird eine von „Certified Security Solutions“ modifizierte Version von Putty (v0.55b1, GSSAPI Enhanced) verwendet.

### 2.1 Voraussetzungen

- PuTTY mit GSSAPI für KfW:  
[http://certifiedsecuritysolutions.com/download/putty\\_0-55b1/putty\\_0-55b1\\_installer.zip](http://certifiedsecuritysolutions.com/download/putty_0-55b1/putty_0-55b1_installer.zip)  
[http://www.g4t3.de/download/putty\\_0-55b1\\_installer.zip](http://www.g4t3.de/download/putty_0-55b1_installer.zip)
- Kerberos muss eingerichtet sein (Siehe section1).
- Die Namensauflösung für die Domäne „**g4t3.de**“ muss funktionieren.
- Der Host **dev.g4t3.de** (oder ein anderer kerberisierter Server) muss erreichbar sein.

### 2.2 Konfiguration

In dem Verzeichnis des Modifizierten PuTTY muss die **pluginss.dll** gelöscht werden, die **plugin\_mitgss.dll** kopiert und die Kopie in **pluginss.dll** umbenannt werden.

In dem Konfigurationsmenü unter **Connection -> SSH -> Auth** befinden sich einige weitere Optionen. Für eine loginfreie Anmeldung muss hier „**Attempt GSSAPI/Kerberos 5 authentication**“ aktiviert werden.

„**Allow Kerberos 5 ticket forwarding (SSH 1/2)**“ sollte bei bestimmten Anwendungen ebenfalls gesetzt werden. Mit dieser Option gibt man dem Zielrechner die Möglichkeit, die eigenen Berechtigungen einzufordern, also zum Beispiel auch entsprechende weiterführende ssh Verbindungen zu autorisieren. Generell heißt das, dass ein kompromittierter Zielhost nach einem erfolgreichen login für die Lebensdauer des TGT wie man selbst agieren könnte, insbesondere also auch Dateien löschen, Mails senden und löschen usw. Dieser Zugriff ist aber auf die Lebensdauer des TGTs beschränkt.

Auf der andern Seite ermöglicht dieser Mechanismus einigen Servern nahezu rechtelos zu laufen, da sie die für ihre Dienste erforderlichen Rechte direkt aus diesem übermittelten Ticket ziehen können. Zum einen ist es damit unmöglich, Rechte wahrzunehmen die man selbst nicht hat, und zum anderen kann ein kompromittierter Service so nur sehr begrenzten Schaden anrichten.

## 2.3 Test

Die Authentifizierungsoption GSSAPI setzen und sich mit **dev.g4t3.de** verbinden. Nach eingabe des Benutzernamens sollte der Loginvorgang automatisch abgeschlossen werden (keine weitere Eingabe eines Passwortes).

In der damit gestarteten Shell **\$> ssh www** eingeben. Dies sollte mit einem **Permission denied** vom Server verweigert werden.

Die Authentifizierungsoption **Allow Ticket Forwarding** zusätzlichen zu der GSSAPI-Option setzen und den Vorgang (Einwählen nach **dev.g4t3.de**) wiederholen.

In der damit gestarteten Shell erneut **\$> ssh www** eingeben. Dies sollte jetzt erfolgreich sein.

## 2.4 Fehlerbehebung

### 2.4.1 Sofortiges Ende bei Verbindungsaufbau

Das PuTTY Fenster schließt sich nach dem starten der Verbindung sofort wieder.

1. Lösche eventuell vorhandene Tickets aus Leash (Destroy Tickets). Versuche nun erneut, dich zu verbinden. Fordert Leash nun zur Anmeldung auf? Wenn nein, kopiere die Datei **krb5\_32.dll** aus dem **MIT\Kerberos für Windows\bin** in das **Windows\system32** Verzeichnis und starte den Rechner anschließend **zwei mal** neu.

## 3 SCP

SCP wäre auch mit Putty möglich, allerdings ist mit WinSCP hier ein GSSAPI-fähiges graphische Tool vorhanden, was dem Windows-Nutzer deutlich angenehmer sein dürfte.

### 3.1 Voraussetzungen

- WinSCP  
<http://winscp.net/download/winscp382setup.exe>  
<http://www.g4t3.de/download/winscp382setup.exe>
- Kerberos muss eingerichtet sein (Siehe section1).
- Die Hosts **auth.g4t3.de** und **data.g4t3.de** müssen erreichbar sein.

## 3.2 Konfiguration

Nach dem Start von WinSCP muss links unter **SSH->Authentifizierung** die Option **Kerberos 5 GSSAPI Auth** angewählt werden wenn sich mit den entsprechenden Hosts verbunden werden soll. Als Hostname dann noch **dev.g4t3.de** und den eigenen username angeben, und das unter einem frei wählbaren Namen abspeichern.

## 3.3 Test

Die zuvor angelegte Verbindung laden und öffnen.

## 3.4 Fehlerbehebung

### 3.4.1 Authentifizierung schlägt fehl

Die Authentifizierung kann nicht erfolgreich durchgeführt werden.

1. Lösche eventuell vorhandene Tickets (Leash -> Destroy Tickets). Versuche dich nun erneut zu verbinden. Fordert Leash nun zur Anmeldung auf? Wenn nein, kopiere die Datei **krb5\_32.dll** aus dem **MIT\Kerberos für Windows\bin** in das **Windows\system32** Verzeichnis und starte den Rechner anschließend **zwei mal** neu. Wenn die Date dort schon vorhanden ist, starte den Rechner trotzdem **zwei mal** neu.
2. Log dich per ssh auf **dev.g4t3.de** ein. Wenn irgendwelche Fehlermeldungen auftreten (ein Skript konnte nicht ausgeführt werden, es konnte nicht ins Heimatverzeichniss gewechselt werden usw.), versuche den Grund dafür zu beseitigen. Sobald das erfolgreich durchgeführt wurde, versuche erneut einen SCP transfer.

## 4 Maildienste

Unter g4t3.de wird ein kerberosgesicherter Mailserver betrieben. Dieser bietet den g4t3.de usern unter anderem folgende Features:

- Sehr großes Postfach (momentan im zweistelligen GB Bereich)
- (Nahezu) beliebige Mail Aliasnamen einstellbar
- Automatische Viren- und Spamkennzeichnung (-bewertung)
- Automatischer Mail-Sammeldienst von anderen Konten.
- Standard- und eigene Mailverteiler.
- Shared-Mailboxes nach Bedarf

### 4.1 Mailclient Voraussetzungen

- Ein g4t3.de Mailaccount (im Full-Account enthalten)
- Eine Kerberos-Implementierung
- Die Namensauflösung für die Domäne „**g4t3.de**“ muss funktionieren.

## 4.2 Mailclient Programme

**Windows XP** user müssen derzeit die normale Windows Version von Mozilla Thunderbird verwenden (<http://www.mozilla-europe.org/de/products/thunderbird/>).

**Windows 7 64Bit oder Vista 64Bit** user müssen die 64Bit Version von Thunderbird 3 verwenden, diese findet sich unter <http://wiki.mozilla-x86-64.com/images/Thunderbird-3.0b2.en-US.win64.installer.zip>. Wenn vorhanden sollten neuere Versionen verwendet werden.

**Hinweis:** Der Mailclient muss mit dem **selben user** installiert werden, mit dem auch Kerberos installiert wurde.

## 4.3 Mailclient Konfiguration

Der Mailserver läuft auf **mail.g4t3.de** und ist per **IMAP** und **SMTP** erreichbar. Um auf die jeweiligen Dienste zuzugreifen, wird ein entsprechendes Service-Ticket benötigt. Das heißt in der Regel, dass die Clientanwendung kerberisiert sein muss.

Um auf den IMAP Server zuzugreifen kann normales IMAP oder IMAP über SSL oder TLS verwendet werden (TLS empfohlen)

Der SMTP Server kann über mehrere Ports angesprochen werden, und erfordert eine Authentifizierung um Mails mit einer Zieladresse außerhalb der g4t3.de Domäne zu versenden (Relay). Dies ist nicht nur sinnvoll, sondern auch von der DENIC erwünscht.

### 4.3.1 Direktes SMTP

Hier gibt es derzeit drei verfügbare Ports.

**Port 25** Der Standard SMTP Port, mit optionalem TLS

**Port 465** Der IANA URD Port, verbreitet in der Verwendung als SMTPS Port. Hier ist TLS erforderlich.

**Port 443** Der HTTPS Port, als einer der Ports die in der Regel nicht geblockt werden, stellt eine Möglichkeit dar aus restriktiven Umgebungen Mails zu versenden.

Sollte keiner der drei Ports aufgrund von Firewall-Einstellungen der Umgebung erreichbar sein, kann noch ein SSH Tunnel verwendet werden.

### 4.3.2 Mozilla Thunderbird für Windows XP

in den Konfigurationswerten (Erreichbar über Einstellungen -> Erweitert -> Konfiguration bearbeiten) müssen einige kerberosrelevante Werte angepasst werden:

**network.auth.use-sspi** false

**network.negotiate-auth.allow-proxies** true

**network.negotiate-auth.delegation-uris** – Defaultwert (leer) –

**network.negotiate-auth.gsslib** – Defaultwert (leer) –  
**network.negotiate-auth.trusted-uris** – Defaultwert (leer) –  
**network.negotiate-auth.using-native-gsslib** true

Es sollte ein Konto mit folgenden Daten angelegt werden:

**Name** Frei wählbar

**E-Mail Adresse** user@g4t3.de (Hier kann auch ein beliebiger eingerichteter Alias eingetragen werden).

**Typ** imap

**Imap-Server** mail.g4t3.de

**Port** TLS auf Port 143, oder SSL auf Port 993

**Authentifizierung** Sichere Authentifizierung

Für den Benutzernamen wird der eigene Accountname angegeben.

Weiterhin wird noch der dazugehörige SMTP-Server angelegt. Die Konfiguration erfolgt im Thunderbird unter dem Knoten **Ausgehende Mailserver**. Dort wird ein neuer Eintrag hinzugefügt (der Name kann frei gewählt werden), mit den folgenden Einstellungen:

**SMTP-Server** mail.g4t3.de

**Port** siehe oben, 443 wird empfohlen

**Authentifizierung** Verwende Username und Passwort aktivieren.

**Username** dieses Feld ist leer zu lassen

Direkt in der Hauptkonfiguration z.B. des g4t3 Accounts sollte dann diese SMTP Verbindung für ausgehende Nachrichten gewählt werden. (Rechtsklick auf einen Konteneintrag -> Eigenschaften)

### 4.3.3 Mozilla Thunderbird für Windows 7 64Bit oder Vista 64Bit

Es sollte ein Konto mit folgenden Daten angelegt werden:

**Name** Frei wählbar

**E-Mail Adresse** user@g4t3.de (Hier kann auch ein beliebiger eingerichteter Alias eingetragen werden).

**Typ** imap

**Imap-Server** mail.g4t3.de

**Port** TLS auf Port 143, oder SSL auf Port 993

**Authentifizierung** Sichere Authentifizierung verwenden

Für den Benutzernamen wird der eigene Accountname angegeben.

Weiterhin wird noch der dazugehörige SMTP-Server angelegt. Die Konfiguration erfolgt im Thunderbird unter dem Knoten **Ausgehende Mailserver**. Dort wird ein neuer Eintrag hinzugefügt (der Name kann frei gewählt werden), mit den folgenden Einstellungen:

**SMTP-Server** mail.g4t3.de

**Port** siehe oben, 443 wird empfohlen

**Authentifizierung** Verwende Username und Passwort aktivieren.

**Username** dieses Feld ist leer zu lassen

**Authentifizierung** Sicher Authentifizierung verwenden

Direkt in der Hauptkonfiguration z.B. des g4t3 Accounts sollte dann diese SMTP Verbindung für ausgehende Nachrichten gewählt werden. (Rechtsklick auf einen Konteneintrag -> Eigenschaften)

In den Programm-Konfigurationswerten (Erreichbar über Einstellungen -> Erweitert -> Konfiguration bearbeiten) müssen die folgenden Werte gesetzt werden (dabei wird angenommen das der g4t3 SMTP Server der erste oder einzige ist):

**network.auth.use-sspi** false

**network.negotiate-auth.allow-proxies** true

**network.negotiate-auth.delegation-uris** – Defaultwert (leer) –

**network.negotiate-auth.gsslib** Pfad zur gssapi64.dll Diese liegt im bin Verzeichnis der Kerberos Installation. Beispielsweise: "C:\Program Files\MIT\Kerberos\bin\gssapi64.dll"

**network.negotiate-auth.trusted-uris** – Defaultwert (leer) –

**network.negotiate-auth.using-native-gsslib** false

**mail.smtpserver.default.useSecauth** true

**mail.smtpserver.smtp1.auth\_method** 1

**mail.smtpserver.smtp1.trySecAuth** false

**mail.smtpserver.smtp1.try\_ssl** 2

**mail.smtpserver.smtp1.useSecAuth** true

#### 4.3.4 Mozilla Thunderbird für Linux

in den Konfigurationswerten (Erreichbar über Einstellungen -> Erweitert -> Konfiguration bearbeiten) müssen einige kerberosrelevante Werte angepasst werden:

**network.negotiate-auth.allow-proxies** true

**network.negotiate-auth.delegation-uris** – Defaultwert (leer) –

**network.negotiate-auth.gsslib** – Defaultwert (leer) –  
**network.negotiate-auth.trusted-uris** – Defaultwert (leer) –  
**network.negotiate-auth.using-native-gsslib** true

Es sollte ein Konto mit folgenden Daten angelegt werden:

**Name** Frei wählbar

**E-Mail Adresse** user@g4t3.de (Hier kann auch ein beliebiger eingerichteter Alias eingetragen werden).

**Typ** imap

**Imap-Server** mail.g4t3.de

**Port** TLS auf Port 143, oder SSL auf Port 993

**Authentifizierung** Sichere Authentifizierung

Für den Benutzernamen wird der eigene Accountname angegeben.

Weiterhin wird noch der dazugehörige SMTP-Server angelegt. Die Konfiguration erfolgt im Thunderbird unter dem Knoten **Ausgehende Mailserver**. Dort wird ein neuer Eintrag hinzugefügt (der Name kann frei gewählt werden), mit den folgenden Einstellungen:

**SMTP-Server** mail.g4t3.de

**Port** siehe oben, 443 wird empfohlen

**Authentifizierung** Verwende Username und Passwort aktivieren.

**Username** dieses Feld ist leer zu lassen

Direkt in der Hauptkonfiguration z.B. des g4t3 Accounts sollte dann diese SMTP Verbindung für ausgehende Nachrichten gewählt werden. (Rechtsklick auf einen Konteneintrag -> Eigenschaften)

#### 4.3.5 Evolution auf Linux

Zuerst muss ein neues Konto angelegt werden.

**Voller Name** Frei wählbar

**E-Mail-Adresse** user@g4t3.de (Hier kann auch ein beliebiger Alias eingetragen werden).

Im Fenster "Abrufen von E-Mails" wird dann der IMAP-Server definiert.

**Server-Art** IMAP

**Server** mail.g4t3.de

**Benutzername** der G4T3-Nutzername

**Sichere Verbindung** SSL-Verschlüsselung

### **Legitimationsart** GSSAPI

Im Fenster "Verschicken von E-Mails" wird der SMTP-Server definiert.

### **Server-Art** SMTP

**Server** mail.g4t3.de

**Erfordert Legitimation** Haken setzen

**Sichere Verbindung** TLS-Verschlüsselung

**Legitimationstyp** GSSAPI

**Benutzername** der G4T3-Nutzername

Am Ende kann noch der Name des neuen Kontos eingegeben werden.

### **4.3.6 Mutt auf Linux**

Das textbasierte mailprogramm ist auf dev.g4t3.de bereits installiert. Bei einer eigenen Installation muss darauf geachtet werden, dass SASL und IMAP aktiviert sind.

Zur Konfiguration muss lediglich folgender Inhalt in die .muttrc (im Heimatverzeichnis) eingetragen werden. Dabei muss USERNAME durch den eigenen Accountnamen ersetzt werden:

```
# Automatically log in to this mailbox at startup
set spoolfile='imaps://USERNAME@mail.g4t3.de/INBOX'

# Define the = shortcut, and the entry point for the folder browser (c?)
set folder='imaps://USERNAME@mail.g4t3.de/INBOX'
set record='=Sent'
set postponed='=Drafts'
```

Sollte das G4T3 Master Zertifikat auf dem System nicht installiert sein, fragt Mutt beim erstmaligen Verbindungsaufbau nach der Korrektheit. Nach der manuellen Prüfung kann das Zertifikat permanent (mit a) akzeptiert werden.

### **4.3.7 Getunneltes SMTP für Windows**

Soll statt dem direkten SMTP Zugang ein Tunnel verwendet werden, wird der Mail-Ausgangsserver wie folgt konfiguriert:

**Smtp-Server** localhost

**Port** 10025

**Authentifizierung** keine Authentifizierung

Der Port kann hier natürlich auch anders gewählt werden, muss aber mit dem weitergeleiteten Port des Tunnels übereinstimmen.

Vor dem Versenden von Mails muss dann ein Tunnel zu dem Mailserver aufgebaut werden. Dazu wird in Windows mittels PuTTY eine spezielle Verbindung eingerichtet:

- Der Zielhost ist dev.g4t3.de
- Der Port unverändert 22
- Die Kerberos Authentifizierungsoption muss gesetzt werden (die restlichen Authentifizierungsoptionen sollten nicht gesetzt werden (Forwarding auch nicht)).
- Ein Tunnel mit **Source Port: 10025** und **Destination: mail.g4t3.local:25** muss hinzugefügt werden.
- das Ganze wird unter dem sessionnamen **thunderbird** abgespeichert.

Diese Verbindung kann manuell gestartet werden, oder aber mit einer Verknüpfung auf **putty.exe -load thunderbird**.

#### 4.3.8 Getunneltes SMTP für Linux

Soll statt dem direkten SMTP Zugang ein Tunnel verwendet werden, wird der Mail-Ausgangsserver wie folgt konfiguriert:

**Smtp-Server** localhost

**Port** 10025

**Authentifizierung** keine Authentifizierung

Der Port kann hier natürlich auch anders gewählt werden, muss aber mit dem weitergeleiteten Port des Tunnels übereinstimmen.

Vor dem Versenden von Mails muss dann ein Tunnel zu dem Mailserver aufgebaut werden. Dazu kann das Kommando **ssh -L 10025:mail.g4t3.de:25 -n dev.g4t3.de &** verwendet werden.

## 4.4 Mailclient Fehlerbehebung

### 4.4.1 Mozilla Thunderbird

Wenn die Mails nach dem Versand nicht in das Gesendet (oder Sent) Verzeichnis kopiert werden, so kann man versuchen in den entsprechenden Konteneinstellungen unter Kopien und Ordner die Einstellung "Anderer Ordner" auswählen und dann über die eigene IMAP-Inbox auf Gesendet navigieren.

### 4.4.2 Getunneltes SMTP

Wenn keiner der SMTP Ports angesprochen werden kann, oder der Mailclient keine Kerberos-Authentifizierung unterstützt, kann auch ein ssh Tunnel auf einen der g4t3-server verwendet werden um eine ausreichende Autorisierung zum Mailversand zu gewährleisten.

Bei diesem Zugang wird die Authentifizierung über den vorhandenen Tunnel hergestellt, genauer genommen durch die Tatsache dass der Mailursprung aus einem privaten Server-Adressbereich stammt. Das heißt, bevor Mails versendet werden können muss stets ein spezielle Verbindung mit dem Server hergestellt werden. Als Tunnelendpunkt wird hier dev.g4t3.de empfohlen, wobei der lokale Port auf **mail.g4t3.de:25** gemappt werden muss. Wenn einer der anderen Ports

verwendet wird, wird ein guter Client aufgrund der unpassenden Zertifikate zumindest eine Warnung ausgeben, evtl. sogar die Verbindung verweigern.

Ein Mailabruf ist damit jedoch nicht direkt möglich, da hier nicht nur das Vorhandensein eines Accounts, sondern auch der spezifische Account geprüft werden müssen (Jeder soll ja nur auf seine eigenen Mails zugreifen).

#### 4.4.3 Tunnelprobleme unter Windows

Wenn der Server nicht erreichbar sein sollte (aus dem Mailclient heraus), überprüfe ob der Tunnel korrekt eingerichtet ist. Ein **netstat -abnp tcp** sollte folgende Zeile enthalten:

```
TCP    127.0.0.1:10025    0.0.0.0:0    ABHÖREN    720    [putty.exe]
```

#### 4.4.4 Tunnelprobleme unter Linux

Wenn der Server nicht erreichbar sein sollte (aus dem Mailclient heraus), überprüfe ob der Tunnel korrekt eingerichtet ist. Ein **netstat -anp tcp -inet** sollte folgende Zeile enthalten:

```
TCP 0 127.0.0.1:10025    0.0.0.0:0    ABHÖREN    xxxx/ssh
```

### 4.5 Mail Sammeldienst

Auf dem Mailserver läuft ein Subsystem, welches für jeden Mailuser eine beliebige Anzahl von Mailkonten auf anderen Servern abrufen und in ein beliebiges Mailkonto übertragen kann. Die abzurufenden Mailkonten werden über LDAP Verzeichniseinträge eingerichtet, somit kann jeder Nutzer seine eigenen Einträge verwalten. Alle eingerichteten Konten werden alle 5 Minuten auf neue Mails überprüft (polling). Demzufolge ist diese Methode der Mail-Aggregation etwas schlechter als eine vom Quellserver vorgenommene direkte Weiterleitung. Solch eine Weiterleitungs-Option wird allerdings nicht von jedem Mailserver angeboten, und bei jenen die es nicht tun, bietet sich der Sammeldienst an.

Da der Sammeldienst das Passwort des abzurufenden Mailkontos benötigt, muss dieses ebenfalls in dem entsprechenden LDAP Eintrag hinterlegt werden (im Klartext). Die Einträge sind zwar geschützt, denn nur der User und der Sammeldienst haben vollen (lesenden) Zugriff auf die Einträge, LDAP Administratoren haben Zugriff auf die Einträge, nicht aber die Passwort-Attribute. Aber, ein Programm mit root Rechten auf dem LDAP Server oder dem Root-Server kann natürlich ebenfalls Zugriff auf die Daten erlangen. Insbesondere kann der Server-Administrator also auf diese Einträge zugreifen, auch auf die Passwörter.

Demzufolge sollte, so ein Konto mit diesem Mechanismus automatisch abgerufen werden soll, das Zugangspasswort vorher auf ein neues, langes (es muss ja nicht mehr manuell eingegeben werden) und möglichst zufällig generiertes, gesetzt werden. Zum einen erhöht das die Widerstandskraft gegen Brute-Force Angriffe, und zum anderen kann mit diesem Passwort dann weder in ein anderes System eingebrochen werden, noch auf Teile anderer Passwörter geschlossen werden. Das Programm **pwgen** ist ein tool, mit dem man solche Passwörter erzeugen kann. Es findet sich z.B. auf **dev.g4t3.de**.

Weiterhin sollte, so möglich, eine SSL gesicherte Verbindung verwendet werden. Andernfalls wäre es für einen Angreifer aufgrund der starken Regelmäßigkeit

und damit Vorhersagbarkeit der Zugriffe recht leicht, ein im Klartext übertragenes Passwort mitzulesen (so er irgendwie an die Route dazwischen kommt).

Die LDAP Einträge sind in dem Pfad **ou=fetch,ou=mail,dc=g4t3,dc=de** untergebracht. Die Klasse ist **fetchmailAccount** und erlaubt die folgenden Attribute:

**mailAddress** Der Schlüsselname, die vollständige Mailadresse, welche abgerufen werden soll.

**mailDrop** Eien beliebige Mailadresse, an die die abgerufenen Mails weitergeleitet werden sollen.

**mailServerProtocol** (IMAP | POP) Dies spezifiziert das Zugriffsprotokoll, welches verwendet werden soll.

**mailServerName** Der voll-Qualifizierte DNS Name des Servers, auf welchem der entsprechende Zugansserver für das Mailkonto gehostet wird.

**mailServerLoginName** Der username mit welchem sich authentifiziert werden soll.

**mailServerLoginPasswd** Das Authentifizierungspasswort. Dies sollte frisch generiert sein. LDAP Administratoren haben keinen Zugriff auf dieses Attribut.

**owner** Der user, welcher administrative Rechte für diesen Eintrag erhalten soll (das ist in der Regel der anlegende user).

**enabled** (TRUE | FALSE) Wenn dieses Attribut auf FALSE gesetzt ist, wird das Mailkonto nicht durch den Sammeldienst abgefragt. Dies ermöglicht es, ein Konto zu deaktivieren ohne es löschen und später wieder neu hinzufügen zu müssen.

**useSSL** (TRUE | FALSE) Spezifiziert, ob die SSL Version des Zugangsprotokolls genutzt werden soll oder nicht.

**fetchReadMail** (TRUE | FALSE) Wenn dies auf TRUE gesetzt ist, werden auch bereits als gelesen markierte Mails von dem Mailserver abgerufen. Dies ist nützlich falls man separat noch per Mailclient auf das Konto zugreift.

**keepMailOnServer** (TRUE | FALSE) Hier verhindert TRUE, dass abgerufene Mails gelöscht werden. In Kombination mit der **fetchReadMail** Option wird dies zu einem höheren Download Aufwand führen.

**mailServerPort** Sollte der Mailserver auf einem nichtstandart-Port hören (oder muss z.B. ein Tunnel verwendet werden), so kann der entsprechende Port hier eingetragen werden. Wenn dieses Attribute nicht spezifiziert ist, wird der passende (je nach SSL oder nicht) Standard-Port verwendet.

## 4.6 Mail-Aliasadressen

Jeder Mailuser kann beliebige Aliasnamen auf sein Mailkonto einrichten, d.h. beliebige Adressen der Form **name@g4t3.de**. Auch diese Mail-Aliasnamen werden über LDAP Einträge spezifiziert. Sie befinden sich in **ou=alias,ou=mail,dc=g4t3,dc=de** und sollten die Klasse **mailTranslationTable** enthalten. Diese Klasse enthält folgende Attribute:

**owner** Derjenige user, welche administrative Rechte an diesem Alias hat.

**enabled** (TRUE | FALSE) Mit FALSE kann dieser Alias (vorübergehend) deaktiviert werden.

**localMailAlias** Der aliasname, welcher umgesetzt werden soll (ist schlüsselattribut).

**mailDrop** Die Mailadresse auf welche die unter dem alias eingehenden Mails weitergeleitet werden.

**description** Eine optionale kurze Beschreibung des Aliasnamens.

## 4.7 Mailverteiler

Alle vorhanden Gruppen sind automatisch als Mailverteiler verwendbar. Um neue statische Verteiler einzurichten wird eine neue Gruppe benötigt. Derzeit können solche Gruppen nur von einem Administrator angelegt werden, dies sollte allgerind nur ein kleines Hindernis darstellen.

## 4.8 Mailweiterleitung

Sollte jemand seinen Mail-Account auf g4t3.de nicht direkt abrufen ist es ratsam, die dort ankommenden Mails an eine andere Adresse weiterzuleiten.

Dazu reicht es aus, die eigene Mail-Adresse (Attribut **mail** im LDAP) auf die gewünschte Zieladresse zu setzen. Wenn die Mails zugleich noch an das Mailkonto auf g4t3.de gleitet werden sollen, kann auch ein doppelter **mail** Eintrag verwendet werden.

# 5 HTTP / HTTPS

Seiten, welche auf dem Server liegen können mit einem Zugriffsschutz versehen werden der gegen Kerberos authentifiziert und somit keine weitere Anmeldung erfordert. Um diese Möglichkeit zu nutzen muss ein Browser verwendet werden welcher mit Kerberos zusammenarbeiten kann. Ein Beispiel dafür ist **Mozilla Firefox**

## 5.1 Voraussetzungen

- Kerberos muss eingerichtet sein
- [www.g4t3.de](http://www.g4t3.de) muss erreichbar sein.
- Das G4T3 Masterzertifikat  
<http://www.g4t3.de/download/g4t3-ca-master.crt>

## 5.2 Programme

**Windows XP** user benötigen Mozilla Firefox ab der Version 1.5

<http://getfirefox.com>

**Windows 7 64Bit oder Vista 64Bit** user müssen (durch das 64Bit Kerberos) den Mozilla Firefox der Version 3 als 64Bit Variante installieren.

<http://wiki.mozilla-x86-64.com/images/Firefox-3.0.7.en-US.win64.installer.zip> (stable)

**Hinweis:** Der Browser muss mit dem **selben user** installiert werden, mit dem auch Kerberos installiert wurde.

## 5.3 Konfiguration

### 5.3.1 Allgemein

Nach der Installation des Firefox sollte das Zertifikat eingestellt werden. Das kann im Firefox einfach durch den Klick auf den entsprechenden Link im Download-Bereich <http://g4t3.de/download/g4t3-ca-master.crt> geschehen. Das Zertifikat sollte für alle drei möglichen Anwendungszwecke abgesegnet werden.

### 5.3.2 Firefox für Windows XP

Im Firefox in der Adresszeile **about:config** eingeben. Dort als Filter **sspi** eingeben und den Wert von **network.auth.use-sspi** auf **false** ändern (durch Doppelklick).

Diese Einstellung stellt den Firefox bei der Verwendung von Kerberos von dem Windows-Active-Directory auf natives (standardkonformes) Kerberos um.

Mit dem Filter **nego** sind diese Einstellungen zu setzen:

```
network.negotiate-auth.allow-proxies true
```

```
network.negotiate-auth.delegation-uris https://
```

```
network.negotiate-auth.gsslib -LEER-
```

```
network.negotiate-auth.trusted-uris https://
```

```
network.negotiate-auth.using-native-gsslib true
```

### 5.3.3 Firefox für Windows 7 64Bit oder Vista 64Bit

Im Firefox in der Adresszeile **about:config** eingeben. Dort als Filter **sspi** eingeben und den Wert von **network.auth.use-sspi** auf **false** ändern (durch Doppelklick).

Diese Einstellung stellt den Firefox bei der Verwendung von Kerberos von dem Windows-Active-Directory auf natives (standardkonformes) Kerberos um.

Mit dem Filter **nego** sind diese Einstellungen zu setzen:

```
network.negotiate-auth.allow-proxies true
```

```
network.negotiate-auth.delegation-uris https://
```

**network.negotiate-auth.gsslib** Pfad zur gssapi64.dll

Diese liegt im bin Verzeichnis der Kerberos Installation.

Beispielsweise: "C:\Program Files \MIT \Kerberos \bin \gssapi64.dll"

**network.negotiate-auth.trusted-uris** https://

**network.negotiate-auth.using-native-gsslib** false

## 5.4 Test

Firefox starten und in die Adresszeile `https://g4t3.de` eingeben. Die Seite sollte, eventuell nach einer Anmeldeaufforderung des installierten Kerberos-Frontends, geladen werden könne. Dabei sollten keine Fehlermeldung (weder Zertifikat-Frage, noch Autorisierung) auftreten.

## 5.5 Fehlerbehebung

### 5.5.1 Access denied

Wenn die Webseite wegen eines **Access denied** nicht geladen werden konnte, überprüfe folgendes:

1. Ist ein Ticket vorhanden (je nach Kerbero Frontend)?
2. Sind die oben angegebenen `about:config` Einstellungen richtig gesetzt?  
Bei Abweichenden Einstellungen sind diese zu korrigieren.
3. Überprüfe die Rechner Uhr. Am besten gleiche sie direkt mit einem Internet Zeitserver ab (`pool.ntp.org`)
4. Lösche eventuell vorhandene Tickets. Wähle nun die oben angegebene Webseite nochmals an.  
Dies sollte fehlschlagen oder eine Anmeldeaufforderung des Kerberos-Frontends nach sich ziehen.

### 5.5.2 Zertifikat-Warnung

Wenn der Browser die Gültigkeit des Zertifikates von `https://www.g4t3.de` abfragt, stelle sicher dass das G4T3-Master-Zertifikat korrekt in den Browser importiert wurde.

## 6 FTP

Auch der Datentransfer per FTP ist über Kerberos abgesichert und erfordert (nach der initialen Anmeldung per Kerberos) keine Passworteingabe.

### 6.1 Voraussetzungen

- FTP Zugangsberechtigung (im full-account enthalten)
- Kerberos muss eingerichtet sein.
- `data.g4t3.de` muss erreichbar sein.

## 6.2 Programme

- Filezilla  
[http://downloads.sourceforge.net/filezilla/FileZilla\\_2\\_2\\_32\\_setup.exe](http://downloads.sourceforge.net/filezilla/FileZilla_2_2_32_setup.exe)  
[http://g4t3.de/download/FileZilla\\_2\\_2\\_32\\_setup.exe](http://g4t3.de/download/FileZilla_2_2_32_setup.exe)

## 6.3 Konfiguration

Der FTP Server läuft auf **data.g4t3.de** und horcht dort auf dem Standard Port **21**. Um eine Verbindung herzustellen, muss eine Client das passende Service-Session Ticket besitzen (das heißt der Client muss Kerberos unterstützen, und es muss ein TGT vorhanden sein). In der Regel wird der passive Modus für den Datentransfer verwendet werden.

### 6.3.1 Filezilla

Unter **Bearbeiten->Einstellungen** auf der linken Seite in **Verbindungen->GSS-Unterstützung** das Häkchen bei Kerberos-GSS Unterstützung aktivieren. Anschließend **g4t3.de** in der darunterbefindlichen Liste einfügen.

In **Datei->Server Verwaltung** auf **Neuen Server**, als Namen ist data oder data.g4t3.de recht passend, kann aber frei gewählt werden. Auf der Rechten Seite folgende Einstellungen vornehmen:

**Host** data.g4t3.de

**Port** 21

**Servertyp** FTP

**Logontyp** Normal

**Benutzer** euer Username

**Passwort** -LEER-

Diese Einstellungen mit **Speichern** übernehmen.

Ihr könnt eine Verknüpfung auf FileZilla einrichten, welche automaisch die eben eingerichtete Verbindung aufbaut, indem ihr als Parameter den Namen der Verbindung angebt.

Kopiere eine Verknüpfung auf Filezilla, wähle im **Kontextmenü Eigenschaften** und für im Feld **Ziel** hinter dem Pfad zur File-Zilla.exe den Namen der Verbindung an (mit Leerzeichen zwischen der .exe und derm Namen).

**Test** In **Datei->Server Verwaltung** den eben eingerichteten Server auswählen und auf **Verbinden**, oder direkt die Verknüpfung verwenden (so eingerichtet).

## 7 SVN

Auf dem Server können eine beliebige Anzahl von SVN Repositories betrieben werden, sei es für den ausschließlich eigenen Gebrauch, oder für eine Gruppe.

Zugriff auf die SVN Repositories erfolgt direkt über das svn Protokoll:

## 7.1 Voraussetzungen

- Kerberos muss eingerichtet sein.
- **data.g4t3.de** muss erreichbar sein.

## 7.2 Programme

**Windows XP** hat den TortoiseSVN Client zur Verfügung, hier muss mindestens die Version 1.5 verwendet werden.

<http://downloads.sourceforge.net/tortoisesvn/TortoiseSVN-1.5.4.14259-win32-svn-1.5.3.msi?download> (32-Bit) Weiterhin muss die `saslGSSAPI.dll` installiert werden. Hierbei handelt es sich um ein GSSAPI (Kerberos5) Plugin für eine Authentifizierungsschicht (Cyrus SASL)  
<http://g4t3.de/download/saslGSSAPI.dll> (32-Bit)

**Windows 7 64Bit oder Vista 64Bit** Hierfür existiert zwar bereits eine TortoiseSVN 64Bit Version:

<http://downloads.sourceforge.net/tortoisesvn/TortoiseSVN-1.5.4.14259-x64-svn-1.5.3.msi?download> (64-Bit)

Allerdings fehlt derzeit (März 2009) noch das die benötigte `saslGSSAPI.dll` in einer 64Bit Version. Somit kann SVN als 64Bit Lösung derzeit nicht unter Windows verwendet werden. Als Workaround könnten Repositories über `dev.g4t3.de` in das AFS Home ausgecheckt (und später eingechekkt) werden um anschließend von Windows aus über AFS editiert zu werden.

## 7.3 Konfiguration

### 7.3.1 Tortoise SVN

Die Heruntergeladenen `saslGSSAPI.dll` muss in das `bin` Verzeichnis des installierten TortoiseSVN kopiert werden (normalerweise `C:\Programme\TortoiseSVN\bin`).

Danach muss der Rechner einmal neu gestartet werden.

## 7.4 Verwendung

Vor dem Zugriff auf Kerberos-basierte SVN Repositories muss ein Ticket angefordert werden. Je Nach Anmeldeclient wird, sollte dieses zum Zugriffszeitpunkt nicht vorhanden sein, die Eingabe der User-Credentials gefordert. Dies ist jedoch nur einmalsig im Gültigkeitszeitraum des Tickets notwendig.

Wenn ein Ticket vorhanden ist, können vorhandenen Repositories unter der URL `svn://data.g4t3.de/REPOSITORY` angesprochen werden. **REPOSITORY** muss hierbei natürlich durch einen gültigen namen ersetzt werden.

## 7.5 Test

Als Beispiel kann das Repository dieser Dokumentation augecheckt werden, die dazugehörige URL lautet `svn://data.g4t3.de/g4t3-doc/trunk`.

Dazu bedarf es folgender Schritte:

### 7.5.1 Windows

Mit der Rechten Maustaste auf ein neu angelegtes, leeres Verzeichnis (oder auf eine freie Fläche in einem geöffneten Ordner) klicken, und SVNCheckout aus dem dann aufklappenden Kontextmenü auswählen.

In der oberen Zeile des Checkout-Dialogs nun die gewünschte URL angeben und mit OK bestätigen.

Der checkout sollte erfolgreich durchgeführt werden können, in dem ausgewählten (oder neu erstellten) Ordner sollten nun einige .tex Dateien zu finden sein.

## 7.6 Migration von Alten Checkouts (Working Copy)

### 7.6.1 Windows

Mit der Rechten Maustaste auf das Wurzelverzeichniss des Checkouts klicken. In dem daraufhin erscheinenden Kontextmenü **relocate** auswählen und die neue URL eintragen (z.B. `svn://data.g4t3.de/g4t3-doc/trunk`).

Die neue URL kann nun durch Ersetzen des ersten Teils (bis zum Repository-Namen mit `svn://data.g4t3.de/` gebildet werden.

## 8 Synchronisierung

Hier geht es um ein Tool, um den Inhalt von lokalen Verzeichnissen mit dem Inhalt von Verzeichnissen auf dem Server abzugleichen. Unison wurde an der Universität von Pensilvania entwickelt, und stellt eine Synchronisierungslösung dar, welche sowohl unter Windows als auch Linux verfügbar ist.

Mittlerweile wurde die Weiterentwicklung offiziell zwar eingestellt, das Programm liegt aber in einer stabilen Version vor. Desweiteren ist eine kleine Community dabei immer wieder neue Versionen zu entwickeln. Unison basiert auf dem unter Unix üblichen rsync Protokoll.

### 8.1 Voraussetzungen

- Unison 2.13.16  
`https://svn.cis.upenn.edu/svnroot/unison-contributed-binaries/windows/unison-2.13.16-win-gtk2.exe`  
`http://g4t3.de/download/unison-2.13.16-win-gtk2.exe`
- SSH mit GSSAPI muss eingerichtet sein.
- `dev.g4t3.de` muss per ssh erreichbar sein (mit Kerberos)

### 8.2 Konfiguration

Es muss sehr genau auf die korrekte Version geachtet werden (Version 2.13.16-2).

Weiterhin müssen vor der Verwendung noch einige Umgebungsvariablen eingerichtet und ein wenig mit den Einstellungen getrickst werden. Dazu wählt man **Start -> Einstellungen -> Systemsteuerung** und dort **System -> Erweitert -> Umgebungsvariablen**.

Hier gibt es zwei Vorgehensmöglichkeiten, Es können alle Variablen Lokal, das heist nur für den gerade angemeldeten User gesetzt werden, oder ein Teil (der Userunabhängige Teil) wird allgemein für alle User auf dem System gesetzt. Auf euren Rechnern könnt ihr die Variablen besser für alle User setzen.

Je nach dem müssen die entsprechenden Variablen im oberen (user) oder unteren (system) Teil gesetzt werden, für Systemweite Variablendefinition benötigt man Administratorrechte.

**PATH** hier sollte der Pfad zu dem modifizierten Putty-Verzeichniss angehängt werden. Wichtig, dieser Pfad darf keine Leerzeichen enthalten (Leerzeichen in anderen Pfaden machen aber keinerlei Probleme).

**UNISON** (optional) gibt den Namen (und Pfad) des Verzeichnisses an, welches von Unison für interne Daten und Profile verwendet wird. Ist dies nicht gesetzt wird \$HOME/.unison verwendet.

**HOME** (optional) gibt den von einigen Programmen verwendeten Pfad zu dem Heimatverzeichnis an. Dies wird von Windows nicht standardmäßig gesetzt, und sollte rpo Konto manuell gesetzt werden. Wenn dieser Pfad definiert ist, werden die Unison dateien und Profile in dem unterverzeichnis .unison in eben diesem Pfad abgelegt (empfohlene Variante). Ist diese Variable auch nicht definiert, so wird C:\.unison verwendet.

Unison benötigt einen SSH Client um eine abgesicherte Verbindung zum Zielhost herzustellen. Eine Cygwin-Installation oder eine gewisse unfreie SSH Implementierung sind vorgesehen, um die Vorzüge von Kerberos auch hier nutzen zu können muss aber das modifizierte Putty verwendet werden. Da dies nicht mit allen standard-ssh Kommandozeilenoptionen zurechtkommt muss ein wenig getrickst werden. Es sollte in dem unison Verzeichnis eine Profildatei mit dem Namen **connection** (ohne Endung, einfache Textdatei) mit folgendem Inhalt angelegt werden:

```
http://g4t3.de/download/connection  
  
rshcmd = C:/Programme/PuTTY_GSSAPI/plink.exe  
rshargs = -load unison -batch
```

Dabei ist der Pfad bei **rshcmd** natürlich durch den entsprechend gültigen Pfad auf die **modifizierte plink.exe** zu ersetzen.

Weiterhin muss in dem modifizierten Putty noch eine Session für den Zielhost, **dev.g4t3.de** und den in section2 beschriebenen Kerberos Optionen (beide) angelegt werden. Die Option „**Attempt Keyboard-interactive auth**“ (gleiches Submenü) sollte deaktiviert werden. Das ganze muss unter dem sessionnamen **unison** abgespeichert werden.

Es sollten Profildateien für die tatsächliche Synchronisierung eingerichtet werden. Informationen dazu findet man im Unison Handbuch (<http://www.g4t3.de/download/unison-2.13.16-manual.pdf>) als Beispiel sei hier folgende gegeben

```
(http://www.g4t3.de/download/home-sync-win.prf): root = C:\home\torian\sync  
root = rsh://dev.g4t3.de//home/torian/sync/win-home include connection
```

```
ignore = Name *.aux
```

```
ignore = Name *.bbl
ignore = Name *.blg
ignore = Name *.log
ignore = Name *.toc
ignore = Name {,}*{.aux}
ignore = Path {,}*.bash_history}
```

Wichtig dabei ist, dass die Serveradresse mit dem **rsh://** Präfix versehen wird (ja, nicht mit ssh) und nach dem Rechnernamen ein doppelter Slash eingefügt wird.

Zu guter Letzt kann noch eine Verknüpfung angelegt werden, welches die Synchronisierung direkt anstößt (und somit auch für die regelmäßige, automatische Ausführung geeignet ist). Dazu sollte folgender Aufruf verwendet werden: `P:\fad\zur\unison-2.13.16-win-gtk2.exe -ui text -contactquietly -auto -batch home-sync`

### 8.3 Test

Die Synchronisierung kann entweder per GUI angestoßen werden (da passende Profil auswählen), mit der oben angelegten Verknüpfung, oder mit der Kommandozeile.

## 9 SQL Datenbank

Als Datenbank wird PostgreSQL verwendet, welches eine ausgereifte Kerberos-Anbindung ermöglicht, und mit pgAdmin steht auch ein Administrationswerkzeug zur Verfügung, welches kerberosfähig ist.

### 9.1 Voraussetzungen

- Es muss eine Datenbankberechtigung existieren (im full-account enthalten)
- **data.g4t3.de** muss erreichbar sein
- Kerberos muss eingerichtet sein

### 9.2 Programme

- pgAdmin 3  
<http://www.pgadmin.org>  
<http://g4t3.de/download/pgadmin3-1.6.3.zip>

### 9.3 Konfiguration

Der Datenbankserver läuft auf **data.g4t3.de** auf dem standard PostgreSQL Port **5432**. Die Wartungs-DB ist **template1**.

### 9.3.1 Konfiguration pgadmin3

**Datei-> neuen Server hinzufügen.** Der Name kann frei Gewählt werden, z.B. „G4T3 Main“, Server und Port wie oben aufgeführt. Unter Username gebt ihr euren User an, das Passwort-Feld bleibt leer und das Häcken bei Passwort speichern kann gesetzt werden. Der Rest kann auf den Standardwerten verbleiben.

**Test** Wenn ihr euch mit dem Server verbindet, sollte (nach dem Anklicken des Servers) dieser geladen und „Aufklappbar sein“.

### 9.3.2 Konfiguration psql

Es ist keinerlei weitere Konfiguration für psql erforderlich (neben der Kerberos installation). Es muss allerdings stets der Datenbankserver mittels der **-h** Option mitgeliefert werden, auch wenn man sich auf **data.g4t3.de** eingeloggt hat.

## 10 Andrew File System (AFS)

### 10.1 Voraussetzungen

- Kerberos muss eingerichtet sein.
- Ein entsprechender Account muss eingerichtet sein.
- **data.g4t3.de** muss erreichbar sein.

### 10.2 Programme

**Windows XP** user müssen sich einen der OpenAFS (<http://www.openafs.org/>) installer herunterladen.  
<http://dl.openafs.org/dl/openafs/1.5.54/winxp/OpenAFSforWindows-1-5-54.exe> (32-Bit)

**Windows 7 64Bit oder Vista 64Bit** können die 64Bit Variante verwenden, so sie ein 64Bit Kerberos installiert haben.  
[http://dl.openafs.org/dl/openafs/1.5.54/winxp/openafs-en\\_US-64bit-1-5-54.msi](http://dl.openafs.org/dl/openafs/1.5.54/winxp/openafs-en_US-64bit-1-5-54.msi) (64-Bit)

### 10.3 Konfiguration

#### 10.3.1 OpenAFS für Windows XP

OpenAFS liegt für Windows in zwei Varianten zur Installation vor. Einmal als .exe für die manuelle Installation und einmal als .msi für eine gemanagete Installation mit Hilfe eines Wizards. Es wird empfohlen, die manuelle Installation zu wählen. Diese wird hier detailliert beschrieben. Für die Installation und Konfiguration muss der Nutzer Admin-Rechte besitzen.

Nachdem den Lizenzbedingungen zugestimmt wurde, kann zwischen verschiedenen Arten der Installation gewählt werden. Hier sollte die Wahl auf *AFS Client* fallen. Nachdem ein Installationsverzeichnis gewählt wurde wird

die Frage nach der *CellServDB* gestellt. Hier sollte die Option „download from“ gewählt und folgende Adresse eingetragen werden: <http://g4t3.de/download/CellServDB>

Im nächsten Schritt wird nach dem Zellennamen der AFS Zelle gefragt. Der Name für G4T3 lautet *g4t3.de*. Die restlichen Optionen können so gelassen werden, wie sie vorgegeben sind. Nach der Installation muss das System neu gestartet werden.

Nach dem Neustart versucht AFS eventuell ein Ticket zu bekommen. Das sollte erst einmal abgebrochen werden, da noch einige Konfigurationen fehlen.

Wenn als Kerberos Client der Network Identity Manager (NIM) anstelle von Leash verwendet wird, sollte dort unter Options→AFS die Option „Prevent AFSCreds.exe from starting automatically when you log in to Windows.“ aktiviert werden.

Danach sollte das *OpenAFS Control Panel* geöffnet und dort sichergestellt werden, dass die Option „AFS-Token beim Anmelden bei Windows erhalten“ deaktiviert ist.

Zusätzlich können in dem Tab *Laufwerksbuchstaben* beliebige Laufwerksbuchstaben Pfaden im AFS zugeordnet werden. Der Grundpfad für G4T3 ist dabei immer `\afs\g4t3.de`. Weitere Verzeichnisse können nach belieben angehängt werden. Um zum Beispiel das eigene Home-Verzeichnis an den Buchstaben „Z“ zu binden, muss nur der Buchstabe ausgewählt werden und der Pfad `„\afs\g4t3.de\user\USER“` benutzt werden, wobei USER natürlich durch den eigenen Username ersetzt werden muss.

### 10.3.2 OpenAFS auf Windows 7 64Bit oder Vista 64Bit

Die Installation kann genau so vorgenommen werden wie bei Windows XP, jedoch muss die richtige Version (32Bit oder 64Bit) verwendet werden.

## 10.4 Test

## 10.5 Fehlerbehebung

- Die Systemzeit des eigenen Rechners muss korrekt sein. Eine Differenz von mehr als drei Minuten wird das Anfordern von Kerberos-Tickets oder AFS-Tokens verhindern.
- Die Rechner **auth.g4t3.de** und **data.g4t3.de** müssen erreichbar sein (**ping**).