



InteProxy Server Dokumentation

Release 1.0.0

Bjoern Schilberg

19. 03. 2010

Inhaltsverzeichnis

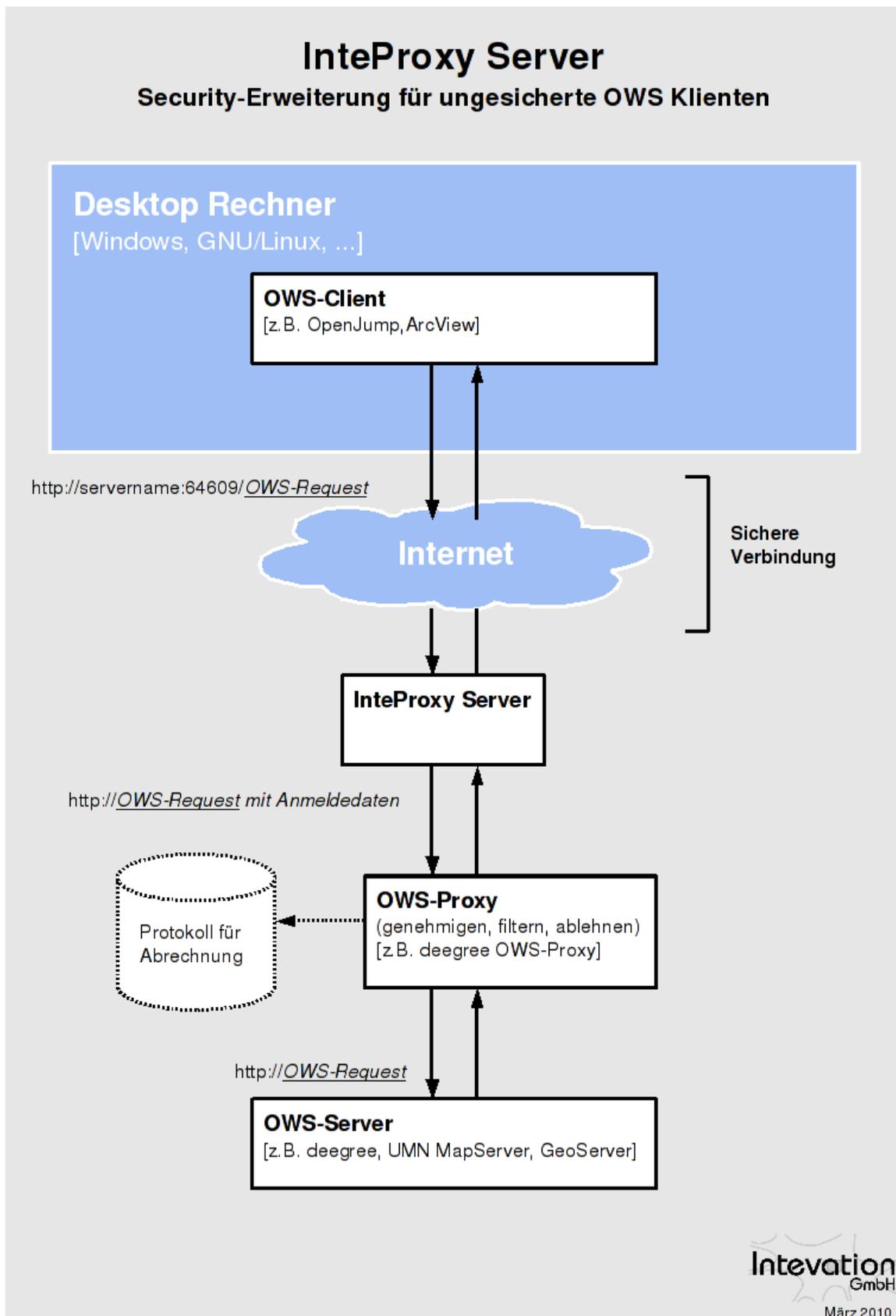
1	Eine kurze Einführung	1
1.1	Unterstützte OWS-Absicherungs-Methoden	1
2	Download	3
3	Anforderungen	5
4	Installation von InteProxy Server für Debian Lenny	7
4.1	Installieren des Apache HTTP Server 2	7
4.2	Herunterladen des InteProxy Servers	7
4.3	Anpassen und Umwandeln der InteProxy Konfigurationsdatei	7
4.4	Einrichten des InteProxy Servers als separaten VirtualHost	8
5	Installation des InteProxy Server für openSuSE 10.3	9
5.1	Installieren des Apache HTTP Server 2	9
5.2	Herunterladen des InteProxy Servers	9
5.3	Anpassen und Umwandeln der InteProxy Konfigurationsdatei	9
5.4	Einrichten des InteProxy Servers als separaten VirtualHost	10
6	VirtualHost Konfigurationsdatei	11
7	Konfigurationsdatei inteproxy.cfg	13
8	Erster Test	17
8.1	Nutzerdaten	17
8.2	Nutzung von InteProxy Server	17
8.3	Einfacher Funktionstest (über Web-Browser)	17
9	Link Liste	19

Eine kurze Einführung

Der InteProxy Server ist eine Zugangshilfe für Klienten-Anwendungen zu einer sicheren Geodateninfrastruktur. Derartigen Anwendungen ermöglicht der InteProxy Server eine sichere Übertragung per Secure Sockets Layer (SSL) sowie eine Benutzeranmeldung am sicheren OGC Web Service (OWS) zu nutzen, sofern die Klienten-Anwendungen dies nicht selbst vermögen.

1.1 Unterstützte OWS-Absicherungs-Methoden

Zur Absicherung des OGC Web Services wird der [deegree OWS-Proxy](#) durch den InteProxy Server unterstützt. Hierbei werden die URL-Parameter `user=` und `password=` gesetzt. In Verbindung mit HTTPS kann jeder OWS Server, der genau diese URL-Parameter verwendet, bedient werden.



Download

Die aktuellsten Versionen des InteProxy Servers befinden sich unter:
<http://inteproxy.wald.intevation.org>.

InteProxy Server ist Freie Software und unter der [GNU GPL \(Version 2\)](#) lizenziert.

Anforderungen

Der InteProxy Server benötigt einen [Apache HTTP Server 2](#) und die folgenden Apache-Module:

- [mod_rewrite](#)
- [mod_authz_host](#)
- [mod_proxy](#)
- [mod_proxy_http](#)
- [mod_ssl](#)

Für die Ausführung des `create-rewrite-rules.py` Skripts werden zusätzlich eine [Python-Umgebung](#) und das [Python-Paket lxml](#) benötigt.

Installation von InteProxy Server für Debian Lenny

Die folgende Beschreibung der Installation des InteProxy Servers bezieht sich auf eine [Debian Lenny GNU/Linux-Distribution](#).

4.1 Installieren des Apache HTTP Server 2

Installieren Sie den Apache HTTP Server 2 mit Hilfe der Anweisung:

```
apt-get install apache2
```

Die benötigten Apache-Module werden hierbei bereits mit installiert.

4.2 Herunterladen des InteProxy Servers

Laden Sie das InteProxy Server Archive herunter (siehe [Download](#)) und entpacken Sie diese in das Verzeichnis /opt.

```
cd /opt
tar zxf InteProxy-SERVER-1.0.0.tar.gz
```

4.3 Anpassen und Umwandeln der InteProxy Konfigurationsdatei

Passen Sie sich die InteProxy Konfigurationdatei `inteproxy.cfg` Ihren Bedürfnissen an. Nach erfolgter Anpassung wandeln Sie die Konfigurationsdatei

tei mit Hilfe des Skripts `create-rewrite-rules.py` aus dem Verzeichnis `/opt/InteProxy-SERVER-1.0.0` in [Apache RewriteRule Direktiven](#) um.

```
./create-rewrite-rules.py --config-file=inteproxy.cfg -o \  
server/conf/inteproxy-rewrite.conf
```

Sie benötigen zur Ausführung des Skripts `create-rewrite-rules.py` noch das Python-Paket `lxml`, gegebenenfalls müssen Sie es nachinstallieren.

```
apt-get install python-lxml
```

4.4 Einrichten des InteProxy Servers als separaten VirtualHost

Um den InterProxy Server als separaten [VirtualHost](#) zu betreiben, kopieren Sie hierfür aus dem Verzeichnis `/opt/InteProxy-SERVER-1.0.0/server/conf` die [Beispiel-Konfigurationsdatei](#) `inteproxy.conf` nach `/etc/apache2/sites-available/`. Sie können die [Beispiel-Konfigurationsdatei](#) auch als Vorlage für Ihre eigene Konfiguration verwenden.

Der Standard-Port des Inteproxy Servers ist `64609`. Ergänzen Sie daher in der Datei `/etc/apache2/ports.conf` noch die folgende Zeile:

```
Listen 64609
```

Aktivieren Sie nun den neu hinzugefügten VirtualHost.

```
a2ensite inteproxy.conf
```

Nach erfolgreicher Aktivierung des VirtualHost `inteproxy` laden Sie den Apache HTTP Server neu.

```
/etc/init.d/apache2 reload
```

Installation des InteProxy Server für openSuSE 10.3

Die folgende Beschreibung der Installation des InteProxy Servers bezieht sich auf eine [openSUSE 10.3](#)-Distribution.

5.1 Installieren des Apache HTTP Server 2

Installieren Sie den Apache HTTP Server 2 mit Hilfe der des Kommandozeilenwerkzeugs `zypper` oder über das graphische Werkzeug `Yast`:

```
zypper install apache2
```

Die benötigten Apache-Module werden hierbei bereits mit installiert.

5.2 Herunterladen des InteProxy Servers

Laden Sie das InteProxy Server Archive herunter (siehe [Download](#)) und entpacken Sie diese in das Verzeichnis `/opt`.

```
cd /opt
tar xzf InteProxy-SERVER-1.0.0.tar.gz
```

5.3 Anpassen und Umwandeln der InteProxy Konfigurationsdatei

Passen Sie sich die InteProxy Konfigurationdatei `inteproxy.cfg` Ihren Bedürfnissen an. Nach erfolgter Anpassung wandeln Sie die Konfigurationsda-

tei mit Hilfe des Skripts `create-rewrite-rules.py` aus dem Verzeichnis `/opt/InteProxy-SERVER-1.0.0/` in **Apache RewriteRule Direktiven** um.

```
./create-rewrite-rules.py --config-file=inteproxy.cfg -o \  
server/conf/inteproxy-rewrite.conf
```

Sie benötigen zur Ausführung des Skripts `create-rewrite-rules.py` noch das Python-Paket `lxml`. Gegebenenfalls müssen Sie es mit `zypper` oder `Yast` nachinstallieren.

```
zypper install python-lxml
```

5.4 Einrichten des InteProxy Servers als separaten VirtualHost

Um den InterProxy Server als separaten **VirtualHost** zu betreiben, kopieren Sie hierfür aus dem Verzeichnis `/opt/InteProxy-SERVER-1.0.0/server/conf` die Beispiel-Konfigurationsdatei `inteproxy.conf` nach `/etc/apache2/vhosts.d`. Sie können die Beispiel-Konfigurationsdatei auch als Vorlage für Ihre eigene Konfiguration verwenden.

Der Standard-Port des Inteproxy Servers ist `64609`. Ergänzen Sie daher in der Datei `/etc/apache2/listen.conf` noch die folgende Zeile:

```
Listen 64609
```

Wenn Sie sich unsicher sind, wie Apache ihre `vhost`-Konfiguration interpretiert, nutzen Sie `httpd2 -S`. Falls SSL im Spiel ist, führen Sie statt dessen `httpd2 -S -DSSL` aus.

Nach erfolgreichem Test des neu eingerichteten **VirtualHost** `inteproxy` starten Sie den Apache HTTP Server neu.

```
rcapache2 restart
```

VirtualHost Konfigurationsdatei

Um den InteProxy Server als Virtuellen Host hinzufügen, kopieren Sie die kommentierte Vorlage `inteproxy.conf` nach `/etc/apache2/sites-available/` für die Debian Distribution und für die openSuSE Distribution nach `/etc/apache2/vhosts.d.` Die VirtualHost Konfigurationsdatei `inteproxy.conf` übernimmt einiges an Automation. So erfolgt das Laden der benötigten Apache-Module plattform-spezifisch durch die Zeile `Include /opt/InteProxy-SERVER-1.0.0/server/conf/platform-debian.conf` für die Debian Distribution **oder** durch die Zeile `Include /opt/InteProxy-SERVER-1.0.0/server/conf/platform-suse.conf` für die openSuSE Distribution. Sollten Sie die Apache-Module bereits geladen haben, können Sie die Zeile einkommentieren.

Die benötigten Apache-Module lassen sich bei Bedarf mit dem Befehl `a2enmod` manuell laden.:

```
a2enmod authz_host proxy proxy_http rewrite ssl
```

Werden die Apache-Module nicht mehr benötigt, können diese manuell mit dem Befehl `a2dismod` entfernt werden.

```
a2dismod authz_host proxy proxy_http rewrite ssl
```

Hinweis: Sollten die oben genannten Apache-Module entfernt werden, läuft der InteProxy Server nicht mehr.

Die VirtualHost Konfigurationsdatei `inteproxy.conf`

```
<VirtualHost *:64609>
ServerAdmin name@domain.de

DocumentRoot /opt/InteProxy-SERVER-1.0.0/server

TransferLog /opt/InteProxy-SERVER-1.0.0/server/logs/access_log

#Include /opt/InteProxy-SERVER-1.0.0/server/conf/platform-suse.conf
```

```
Include /opt/InteProxy-SERVER-1.0.0/server/conf/platform-debian.conf
RewriteEngine On
# RewriteLogLevel 0
RewriteLog /opt/InteProxy-SERVER-1.0.0/server/logs/rewrite.log

# Die Datei conf/inteproxy-rewrite.conf beinhaltet die RewriteRules für die
# aktuelle InteProxy Funktionalität. Sollte die Datei nicht existieren, lesen
# Sie im Kapitel 6 wie Sie eine erstellen können.
Include /opt/InteProxy-SERVER-1.0.0/server/conf/inteproxy-rewrite.conf

# Die Direktive Deny bestimmt, welche Hosts beziehungsweise Netzwerke vom
# Zugriff auf eine Server-Ressource ausgeschlossen sind; die gegensätzliche
# Direktive Allow ermöglicht es, bestimmten Hosts den Zugriff ausdrücklich zu
# gestatten.
# Grundsätzlich darf kein Host auf die Inhalte des InteProxy Servers
# Kontextes zugreifen, in dem die Direktive definiert ist. Niemand darf auf
# URLs zugreifen, die mit / beginnen.
<Directory />
  Order Deny,Allow
  Deny from All
</Directory>

# SSL Konfiguration.
# SSLProxyEngine muss eingeschaltet sein, damit https-Verbindungen zu anderen
# Rechner möglich sind.
SSLProxyEngine on

SSLProtocol all -SSLv2
SSLCipherSuite HIGH:MEDIUM:!ADH

</VirtualHost>
```

Konfigurationsdatei inteproxy.cfg

Die Konfiguration der OWS-Proxydienste erfolgt über eine Konfigurationsdatei. Werden darin keine OWS-Dienste angegeben, verhält sich InteProxy Server wie ein normaler transparenter HTTP-Proxy. Dem Quelltext liegt eine beispielhafte Konfigurationsdatei `inteproxy.cfg` bei. Die Konfigurationsdatei beinhaltet die Services, die als OWS-Proxies fungieren. Bevor der InteProxy Server gestartet wird, muss die Konfigurationsdatei `inteproxy.cfg` mit dem Skript `create-rewrite-rules.py` in [Apache RewriteRule Direktiven](#) umgewandelt werden.

```
./create-rewrite-rules.py --config-file=inteproxy.cfg -o \
server/conf/inteproxy-rewrite.conf
```

Wird beim Starten von InteProxy Server keine Konfigurationsdatei angegeben, wird nach der Datei `inteproxy.cfg` im InteProxy Server-Hauptverzeichnis gesucht. Die Konfigurationsdatei legt darüber hinaus auch fest, ob eine Anmeldung gegen einen Proxy im internen Netzwerk nötig ist, um Dienste zu erreichen. Dazu müssen die Abschnitte `[inteproxy]` und `[http_proxy_authentication]` auskommentiert und angepasst werden. Eine beispielhafte Konfigurationsdatei ist die Datei `inteproxy.cfg`, die den Server `inteproxy-demo.intevation.org` als OWSProxy eingetragen hat.

```
# Demo configuration inteproxy.cfg for InteProxy Desktop.
#
# Diese Datei definiert, wie unterschiedliche entfernte Rechner
# angesprochen werden sollen.
# Alle Server werden über URLs im inteproxy-rules-Abschnitt
# definiert.
#
# Um abwärtskompatibel zu bleiben, wird das alte Format, wo
# jeder Server durch einen eigenen Abschnitt referenziert wurde,
# weiterhin unterstützt.
# Die Benennung der Abschnitte spielt keine Rolle, sie müssen
# nur eindeutig sein.
# Um diese Eindeutigkeit zu bewahren, bietet es sich an,
# den kompletten Domain-Namen auch als Abschnitts-Namen zu
# verwenden.
```

```
# In Zukunft können noch weitere InteProxy-Einstellungen in
# dieser Konfigurationsdatei abgelegt werden.
#
# InteProxy-spezifische Konfigurationseinträge folgen:
# !! WICHTIG:
# !! Sofern ein Intranet-Proxy mit Benutzer/Passwort-
# !! Authentifizierung verwendet wird, kommentieren Sie bitte
# !! die Abschnitte [inteproxy] und
# !! [http_proxy_authentication] aus und passen Sie Ihre
# !! Zugangsdaten entsprechend an.
#
# Anmeldung gegen einen Intranet-Proxy
# [inteproxy]
# https_proxy=http_proxy_authentication
# http_proxy=http_proxy_authentication
#
# [http_proxy_authentication]
# host=upstream.proxy.url.com
# port=8080
# username=john
# password=secret
#
# Haupt-Abschnitt der Absicherungsregeln.
# Der urls-Abschnitt ist eine Liste von URLs. Jede URL muss in
# einer Zeile stehen. Ab der zweiten Zeile müssen die URLs
# eingerückt werden.
#
# Jede URL folgt diesem Schema:
#   SCHEMA://[BENUTZER:PASSWORT@]RECHNERNAME[:PORT]/PFAD
#
# Die Zugangsdaten (BENUTZER und PASSWORT) sowie der Port (PORT)
# sind optional. Wenn kein Port angegeben wird, wird der
# Standardport angenommen.
#
# Das SCHEMA muss eines der folgenden unterstützten Schemen
# sein:
#
#   owsproxy   Der gegenüberliegende Rechner ist ein OWSPProxy,
#               der Authentifizierung und https benötigt.
#
#   basicauth  HTTP Basic Authorization über https
#
# Wenn BENUTZER oder PASSWORT spezielle Zeichen wie '%', ':',
# '@' und Nicht-ASCII Zeichen enthalten, müssen diese mit
# einem "%" gefolgt von 2 hexadezimalen Zeichen maskiert
# werden. Weitere Komplikationen können durch das Prozentzeichen
# entstehen, da es in URLs als Spezialzeichen gilt. Aber auch
# in dieser Konfigurationsdatei muss ein %-Zeichen durch ein
# weiteres Prozentzeichen verdoppelt werden. Ein Prozentzeichen
# müsste wie folgt maskiert werden: "%25" anstatt "%".
```

```
#  
# RECHNERNAME und PFAD-Teile der URL können „*“-Zeichen als  
# Wildcards eingesetzt werden. Diese Wildcards werden auf 0  
# und mehr Zeichen angewandt.  
#  
# Eine Wildcard im RECHNERNAMEN wird nur auf Diesen angewandt,  
# gleiches gilt für den PFAD.  
#  
[inteproxy-rules]  
urls=owsproxy://meier:meier@inteproxy-demo.intevation.org/cgi-bin/frida-wms  
owsproxy://USERNAME:PASSWORT@www.geobasisdaten.niedersachsen.de/mapgate/*
```

Erster Test

Der InteProxy Server bietet die Möglichkeit als normaler HTTP-Web-Proxy zu arbeiten. Im Folgenden wird die Betriebsart als HTTP-Web-Proxy an Beispielen inklusive Konfigurationsschritten vorgestellt.

8.1 Nutzerdaten

Um die Anwendungsbeispiele gegen den hier beschriebenen Demoserver zu nutzen, stehen Ihnen die folgenden Nutzerdaten im OWSPProxy zur Verfügung. Server-URL:

```
http://inteproxy-demo.intevation.org/cgi-bin/frida-wms
```

Zwei Benutzerkonten stehen bereit:

- User/Passwort = meier/meier: Darf alle WMS Ebenen anschauen
- User/Passwort = schmidt/schmidt: Darf alle WMS Ebenen anschauen, außer den Straßen.

8.2 Nutzung von InteProxy Server

Stellen Sie in Ihrer Anwendung der eigentlichen URL für den WMS Dienst den Text `http://servername:64609/` voran, so wird für den WMS explizit der InteProxy Server angesprochen.

8.3 Einfacher Funktionstest (über Web-Browser)

Mit diesem Test wird geprüft, ob InteProxy Server grundsätzlich bei Ihnen funktioniert und auch nicht durch Firewalls blockiert wird. Stellen Sie sicher, dass InteProxy Server gestartet

ist. Um zu testen, ob der InteProxy Server korrekt funktioniert, öffnen Sie einen Web-Browser und geben Sie folgende URL ein:

```
http://servername:64609/inteproxy-demo.intevation.org/cgi-bin/frida-wms?  
Request=GetMap  
&Version=1.1.1&service=WMS  
&layers=strassenall,sehenswuerdigkeiten  
&format=image/png&width=200&height=200  
&srs=epsg:31467&bbox=3427000,5787590,3444000,5800880
```

Der Browser stellt die Anfrage zunächst an InteProxy Server welcher auf Port 64609 auf dem Server auf Anfragen wartet. Nach Eingabe sollte im Browser dann eine Karte der Stadt Osnabrück erscheinen, denn der InteProxy Server führt dann die eigentliche nachfolgende WMS-Anfrage aus:

```
https://inteproxy-demo.intevation.org/cgi-bin/frida-wms?VERSION=1.1.1  
&SERVICE=WMS&REQUEST=GetMap&layers=strassenall,sehenswuerdigkeiten  
&format=image/png&width=200&height=200  
&srs=epsg:31467&bbox=3427000,5787590,3444000,5800880  
&user=meier&password=meier
```

Insbesondere wird natürlich nun über das sichere Protokoll „https“ und nicht mehr über „http“ kommuniziert. Darüber hinaus hängt der InteProxy Server die ihm bekannten Credentials `user=meier&password=meier` an die sichere URL an.

Link Liste

- <http://httpd.apache.org> (Apache HTTP Server)
- <http://httpd.apache.org/docs/2.2/mod/core.html> (Apache Core Features)
- http://httpd.apache.org/docs/2.2/mod/mod_rewrite.html (Apache Module mod_rewrite)
- http://httpd.apache.org/docs/2.2/mod/mod_authz_host.html (Apache Module mod_authz_host)
- http://httpd.apache.org/docs/2.2/mod/mod_proxy.html (Apache Module mod_proxy)
- http://httpd.apache.org/docs/2.2/mod/mod_proxy_http.html (Apache Module mod_proxy_http)
- http://httpd.apache.org/docs/2.2/mod/mod_ssl.html (Apache Module mod_ssl)
- http://httpd.apache.org/docs/2.2/mod/mod_auth_basic.html (Apache Module mod_auth_basic)
- <http://www.python.org/> (Python Programming Language)
- <http://codespeak.net/lxml/>
- <http://inteproxy.wald.intevation.org> (InteProxy - Security extension for unsecure OWS clients to secure spatial data infrastructures)
- <http://www.gnu.org/licenses/old-licenses/gpl-2.0.html> (GNU General Public License, version 2)
- <https://wiki.deegree.org/deegreeWiki/iGeoSecurity> (iGeoSecurity - short description of iGeoSecurity)
- <http://www.debian.org/> (Debian GNU/Linux)