Forschungszentrum Jülich

Zentralinstitut für Angewandte Mathematik
D-52425 Jülich, Tel. (02461) 61-6402
Informationszentrum, Tel. (02461) 61-6658

Technische Kurzinformation

FZJ-ZAM-TKI-0378
J.Meißburger
Update 9.10.2003

Einrichten eines SSL-Zugangs für den Microsoft Internet Information Server IIS

Inhaltsverzeichnis:

1. Einleitung

SSL bietet Schutz gegen Abhören der Kommunikation (Sniffen) und eine Identitätsprüfung des Servers (Masquerading). Zur Aktivierung der SSL-Sicherheit auf einem IIS-Server sind folgende Schritte erforderlich:

1. Erzeugen eines lokalen Schlüsselpaares und einer zugehörigen Anfragedatei zur Erlangung eines Zertifikats.
2. Anfordern des Zertifikats von einer Zertifizierungsstelle, in unserem Falle von der Forschungszentrum Jülich Certification Authority (FZJ-CA).

3. Importieren des erhaltenen Zertifikats und der übergeordneten Zertifikate im Zertifizierungspfad in den Zertifikatsspeicher.
4. Installation des Serverzertifikats im Webserver und Aktivieren der SSL-Sicherheit für einen oder alle Ordner des WWW-Dienstes.
5. Paßwortgeschütztes Sichern des Schlüsselpaares und der Zertifikate auf einem Datenträger. Schlüssel nicht aus dem System entfernen!

Zertifikate und Schlüssel sollten exportiert und an einem sicheren Ort aufbewahrt werden, um sie im Notfall griffbereit zu haben. Es empfiehlt sich, die Dateien auf einer Diskette oder einem USB-Stick gut verschlüsselt abzuspeichern. Beim Export dürfen die Schlüssel nicht aus dem System entfernt werden! Auf keinen Fall sollte man das Passwort vergessen, das beim Export der Schlüsselpaardatei verwendet wurde!

Die hier dargestellte Vorgehensweise mag etwas umständlich erscheinen, hat sich aber vor allem beim Auftreten von Problemen oder bei der Verwaltung mehrerer Serverzertifikate durchaus bewährt. Sie kommt darüber hinaus ohne die Ausführung der vom CA-Server ebenfalls angebotenen Active-X-Funktionalität aus.

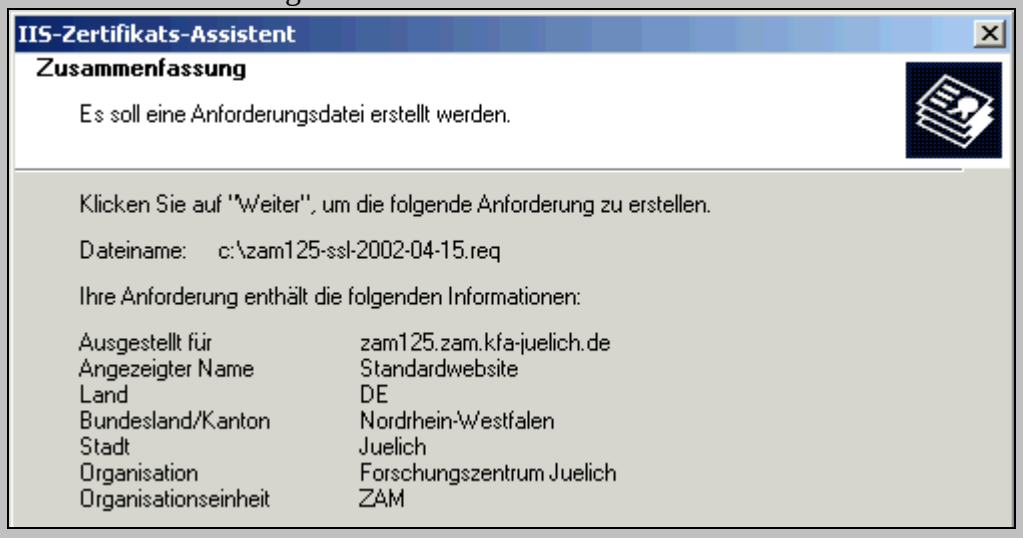
Seite 1

2. Serverzertifikat anfordern

2.1 Schlüsselpaar und Zertifikatsanforderung erstellen

- Als Administrator mit "**Start - Programme - Verwaltung**" den Internetdienste-Manager starten.
- WWW-Server "**Standardwebsite**" im Internetdienste-Manager durch Mausklick auswählen.
- Auf Symbol für Eigenschaften klicken, Lasche "**Verzeichnissicherheit**" auswählen.
- Mit "**Sichere Kommunikation, Serverzertifikat...**" den Assistenten für Serverzertifikate starten
- "**Neues Zertifikat erstellen**" auswählen
- **Anforderung jetzt vorbereiten, aber später senden**
- Namen für die Website (Default ist Standardwebsite) wählen und **Schlüsselstärke auf 1024 Bit** setzen
- Organisationsnamen "**Forschungszentrum Juelich**" und Organisationseinheit eintragen , keine Umlaute verwenden!
- Rechnernamen des Webservers voll qualifiziert angeben (beispielsweise wie zam125.zam.kfa-juelich.de)
- Geographische Informationen wie vorgeschlagen übernehmen oder eingeben (ohne Umlaute!)
- Einen selbsterklärenden Dateinamen für die Zertifikatsanforderung eingeben, etwa **C:\zam125-ssl-2002-04-15.req**

- Die Zusammenfassung



  nochmals prüfen, ggf. mit "Zurück" korrigieren und mit "Weiter" fertigstellen.

Damit wurde eine Zertifikatsanforderung für ein im Hintergrund generiertes Schlüsselpaar (Private/Public Key) erstellt, und die Textdatei mit der Zertifikatsanforderung liegt nun unter **C:\zam125-ssl-2002-04-15.req** bereit. Damit muss als nächstes bei der **C**ertification **A**uthority des Forschungszentrums Jülich ein Zertifikat für die soeben erzeugten Schlüssel angefordert werden.

- Zweckmäßigerweise sichert man sich alle zur Zertifizierung benutzten Informationen wie etwa die gerade erstelle Zertifikatsanforderung zumindest temporär auf einem ZIP-Laufwerk oder auf der Festplatte, etwa als **D:\Install\Zertifikate\zam125-ssl-2002-04-15.req** ab.

Seite 1

2.2 Server-Zertifikat von der FZJ-CA anfordern

Zur Erlangung eines Zertifikats für die zuvor generierten, noch nicht zertifizierten öffentlichen Schlüssel sind zwei Aktionen erforderlich:

1. Eingabe des Textes der gerade generierten Zertifikatsanforderung in ein entsprechendes Web-Formular auf dem CA-Server des Forschungszentrums.
2. Persönliche Identifikation des Antragstellers durch Vorlage einer unterschriebenen Teilnehmererklärung und des Personalausweises des FZJ-Mitarbeiters beim ZAM-Dispatch (Geb. 16.3, ZAM, Tel. 5642).

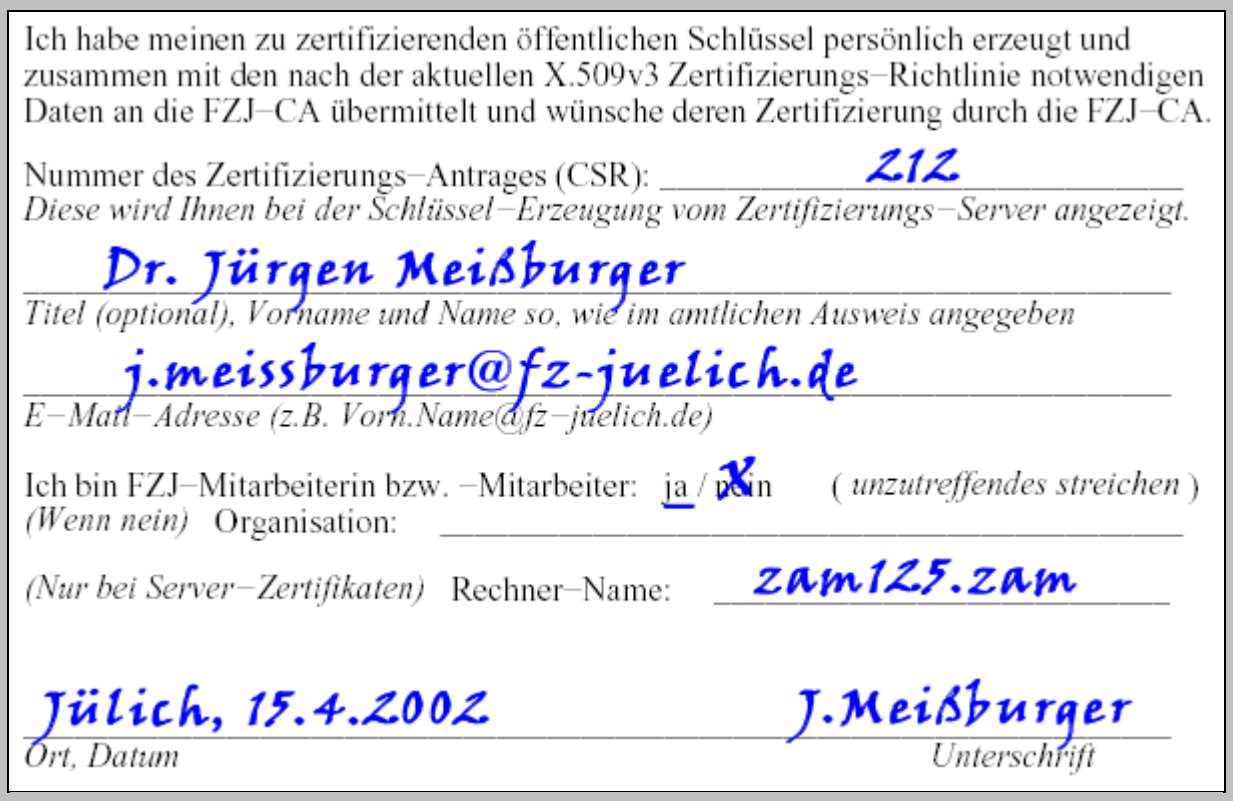
2.2.1 Zertifikatsanforderung absenden

- Das Formular für den elektronischen Zertifikatsantrag findet sich SSL-gesichert (https) unter https://ca.fz-juelich.de/fzj-html/ManServerEnroll.html
- Falls zu diesem Zeitpunkt das Toplevel-Zertifikat des DFN noch nicht im Speicher für vertrauenswürdige Stammzertifizierungsstellen eingetragen ist (er wird später automatisch beim Installieren der Server-Zertifikate installiert), den Sicherheitshinweis mit "Ja" bestätigen.
- Die Datei **C:\zam125-ssl-2002-04-15.req** mit dem Texteditor öffnen, alles auswählen und mit "**Kopieren - Einfügen**" (z.B. mit <Ctrl>-C, <Ctrl>-V) vollständig in das obere Textfeld des Formulars übertragen. Restliche Felder **ohne Verwendung von Umlauten** ausfüllen.

- Mit "**Submit**" abschicken. Der Request erhält vom CA-Server eine Request-ID, die man sich merken muss, da sie später noch benötigt wird. Am besten als Textdatei zusammen mit der Zertifikatsanforderung auf **D:\Install\Zertifikate** sichern.

2.2.2 Teilnehmererklärung erstellen

- Das Formular für die Teilnehmererklärung findet sich in druckbarem PDF-Format unter http://www.fz-juelich.de/CA/docs/teilssla.pdf
- Die Nummer der Request-ID's und die übrigen Daten werden handschriftlich eingetragen und das Formular unterschrieben beim ZAM-Dispatch (G 16.3, R 004, Tel. 5642) eingereicht.



Ich habe meinen zu zertifizierenden öffentlichen Schlüssel persönlich erzeugt und zusammen mit den nach der aktuellen X.509v3 Zertifizierungs–Richtlinie notwendigen Daten an die FZJ–CA übermittelt und wünsche deren Zertifizierung durch die FZJ–CA.

Nummer des Zertifizierungs–Antrages (CSR): 212
Diese wird Ihnen bei der Schlüssel–Erzeugung vom Zertifizierungs–Server angezeigt.

Dr. Jürgen Meißburger
Titel (optional), Vorname und Name so, wie im amtlichen Ausweis angegeben

j.meissburger@fz-juelich.de
E–Mail–Adresse (z.B. Vorn.Name@fz–juelich.de)

Ich bin FZJ–Mitarbeiterin bzw. –Mitarbeiter: ja / nein (X) *(unzutreffendes streichen)*
(Wenn nein) Organisation:

(Nur bei Server–Zertifikaten) Rechner–Name: zam125.zam

Jülich, 15.4.2002 — J.Meißburger
Ort, Datum — *Unterschrift*

Seite 1

3. Zertifikat im Webserver installieren

3.1 Zertifikate lokal sichern

- Als Ergebnis der Zertifikatsanforderung erhält man kurze Zeit später unter der angegebenen offiziellen Email-Adresse eine Email von **ca@fz-juelich.de** mit dem Betreff "Your Certificate Request" mit einem Link auf eine dynamische HTML-Seite des CA-Servers.
- Durch Klick auf dieses Link wird das Zertifikat im Browser (Internet-Explorer) dargestellt. Die verlangten und aus Sicherheitsgründen vielleicht abgeschalteten ActiveX- und Plugin-Funktionen werden zum Import des Zertifikats nicht benötigt. Es genügt der angezeigte Textinhalt des Zertifikats.
- Im Internet-Explorer mit "**Datei - Speichern unter**" als ISO-kodierte Textdatei beispielsweise in dem gleichen Ordner wie die Zertifikatsanforderung etwa als **D:\Install\Zertifikate\zam125-ssl-2002-04-15-Display Certificate.txt** ablegen. Die gerade gespeicherte Textdatei enthält zwei Zertifikate, das für den zuvor generierten eigenen Schlüssel (base 64 encoded) und den Zertifizierungspfad für die FZJ- und DFN-Zertifizierung (pkcs7-Format).

- Datei mit dem Texteditor öffnen, den Text des Base 64-Zertifikats zwischen BEGIN und END in eine neue Textdatei, z.B. **zam125-ssl-2002-04-15.cer** abspeichern.
- ebenso den nachfolgenden Teil des **PKCS7-Zertifikats** zwischen BEGIN und END etwa als **dfn-fzj-chain-2002-04-15.p7b** abspeichern. Damit sind alle für die Zertifizierung benutzten Dateien lokal gesichert.

3.2 Zertifikate installieren

- Auf die Datei **dfn-fzj-chain-2002-04-15.p7b** doppelklicken. Es öffnet sich der Assistent für die Zertifikatsverwaltung und zeigt die drei hierin enthaltenen Zertifikate,
  - neue Server-Zertifikat,
  - das übergeordnete Zertifikat der FZJ-Certification Authority und
  - das DFN-Toplevel-Zertifikat an:
- Das DFN Toplevel-Zertifikat auswählen, Mit "**Vorgang - Alle Tasks - Öffnen**" oder Doppelklick das noch nicht importierte Zertifikat anzeigen und mit Klick auf "**Zertifikat installieren**" den Zertifikats-Importassistenten starten.
- Zertifikatspeicher automatisch auswählen.
- Zertifikatsdaten überprüfen und Hinzufügen des Zertifikats bestätigen.
- Der erfolgreiche Import wird abschließend durch eine PopUp-Meldung bestätigt. Nochmals mit "**OK**" bestätigen. Damit ist das DFN Toplevel-Zertifikat im System installiert.
- Auf die gleiche Weise das **FZJ-CA-Zertifikat** auswählen und mit **"Vorgang - Alle Tasks - Öffnen"** und anschließend mit Klick auf **"Zertifikat installieren"** mit automatischer Auswahl des Zertifikatsspeichers importieren.
- Desgleichen das **Serverzertifikat zam125.zam.kfa-juelich.de** importieren.
- Jetzt kann das Schlüsselzertifikat für den Webserver selbst installiert bzw. diesem bekannt gemacht werden. Wie bereits beim Erstellen der Zertifikatsanforderung **Internetdienste-Manager starten, Standardwebsite auswählen, "Eigenschaften - Verzeichnissicherheit".**
- Mit Klick auf "**Serverzertifikat...**" und "**Weiter**" den IIS-Zertifikats-Assistenten starten, "**Ausstehende Anforderung verarbeiten und Zertifikat installieren**".
- Beim Zertifikatsnamen c:*.cer "**Durchsuchen**" auswählen, die Datei **D:\Install\Zertifikate\zam125-ssl-2002-04-15-zertifikat.cer** angeben und mit "**Öffnen**" übernehmen.
- Mit "**Weiter**" wird nochmals das zu installierende Serverzertifikat angezeigt und mit "**Weiter**" und "**Fertigstellen**" übernommen.

Seite 1

3.3 Importierte Zertifikate überprüfen

- Mit **Start - Einstellungen - Systemsteuerung - Internetoptionen** (oder rechte Maustaste auf Explorer-Symbol - Eigenschaften) **- Inhalt - Zertifikate** können die importierten Zertifikate und ihre Zertifikationspfade im Zertifikatsspeicher überprüft werden.
- Das Serverzertifikat beispielsweise für zam125 mit korrektem Pfad zum FZJ-CA und zum DFN-Toplevel-Zertifikat im Speicher für Zwischenzertifizierungsstellen.
- ebenso das vom DFN zertifizierte FZJ-CA-Zwischenzertifikat im Speicher für Zwischenzertifizierungsstellen.

- Und schließlich das DFN Toplevel-Zertifikat im Speicher für vertrauenswürdige Stammzertifizierungsstellen.

4. Webserver für SSL-Zugriff einrichten

Der SSL-Zugriff kann für einzelne, auch virtuelle Verzeichnisse oder aber für die gesamte Website (Root-Ordner) eingerichtet werden. Letzteres ist, wenn ausschließlich SSL-Zugang gewünscht wird, der einfachste und sicherste Weg. Hierzu:

- **Internet-Informationsdienste-Manager starten, Webserver (Standardwebsite) auswählen und Eigenschaften öffnen**. Lasche "**Website**" auswählen.
- Für **TCP-Anschluß** kann ein beliebiger Port, möglichst ungleich Standardport 80 eingetragen werden. Die Verbindung zum Server kann ohne Verschlüsselung weiter zu diesem Port und gleichzeitig mit Verschlüsselung zum SSL-Port 443 erfolgen. Im allgemeinen ist es jedoch sinnvoll, wie weiter unten beschrieben nur noch die gesicherte Kommunikation über SSL zuzulassen.
- Das "**Basisverzeichnis**" wird mit minimal erforderlichen Zugriffsrechten, d.h. "**Lokaler Pfad Lesen und Besuche protokollieren**" eingerichtet. Damit hat ein Benutzer lesenden Zugriff auf alle Webdokumente dieses Servers. Skripte können nur ausgeführt werden, und das Durchsuchen von Verzeichnissen ist nicht erlaubt.
- Mit "**Verzeichnissicherheit - Sichere Kommunikation - Bearbeiten**" wird schließlich mit "**Sicheren Kanal verlangen**" der sichere SSL-Kanal aktiviert und durch Auswählen von "**128-Bit-Verschlüsselung erforderlich**" die Sicherheit der Datenverschlüsselung erhöht.
- Bei Bedarf kann hier auch eine benutzerbezogene Zugangskontrolle durch Client-Zertifikate aktiviert werden. Diese können lokal auf dem Server vorhandenen Benutzerkonten zugeordnet werden und erlauben einen individuell authentisierten Webzugang zum Server.

Damit ist die SSL-Konfiguration beendet und die Kommunikation vom und zum Server **https://zam125.zam.kfa-juelich.de** ist verschlüsselt und abhörsicher. Sollte sich jetzt ein Benutzer mit dem ungesicherten Port 8765 verbinden wollen, so lehnt der Server dies ab und fordert zur Verwendung der gesicherten SSL-Kommunikation auf. Dies ist besonders wichtig, wenn für den Zugang zum Server unverschlüsselte oder schwach verschlüsseltePasswörter Verwendung finden oder aber (Datenbankanwendungen) sensitive Daten zwischen Browser und Webserver übertragen werden.

Seite 1

3.4 Schlüsselpaar mit Zertifikat sichern

Es empfiehlt sich, das erzeugte und im System abgelegte Schlüsselpaar - darunter den besonders schützenswerten privaten Schlüssel - und die zugehörigen Zertifikate zur Sicherung auf einem speziell geschützten Bereich einer Festplatte oder auf einem beweglichen Datenträger abzuspeichern. Die Schlüssel dürfen hierbei nicht aus dem System entfernt werden, da diese vom Webserver zum Aufbau der SSL-Verbindung benötigt werden!

- Internet-Informationsdienste-Manager starten, Webserver (Standardwebsite) auswählen und Eigenschaften öffnen.
- "**Verzeichnissicherheit - Zertifikat anzeigen**"
- Lasche "**Details**" auswählen, "**In Datei kopieren...**"
- Es öffnet sich der Zertifikatsexport-Assistent - "**Weiter**"
- "**Ja, privaten Schlüssel exportieren - Weiter**"
- Privater Infformationsaustausch - PKCS#12 (.PFX)
  - **Wenn möglich, alle Zertifikate im Zertifizierungspfad einbeziehen**
  - **Verstärkte Sicherheit aktivieren**
  - **Privaten Schlüssel nach erfolgreichem Export löschen nicht aktivieren !**
- Exportdatei auswählen, z.B. **D:\Install\Zertifikate\zam125-ssl-2002-04-15-zertifikatsicherung.pfx**
- Mit "gutem" Kennwort (>8 Zeichen mit Ziffern und Sonderzeichen) schützen
  Anmerkung: **Die für Zertifikate benutzten Kennwörter sollten wegen ihrer besonderen**

Bedeutung für die Sicherheit der eigenen Identität auf jeden Fall gut gewählt und verschieden von allen anderen, für Systemadministration oder Zugangsvalidierung (vor allem auf fremden Servern) benutzten Kennwörter sein!!

- Mit "**Fertigstellen**" alle Zertifikate und Schlüssel in die Datei **zam125-ssl-2002-04-15-zertifikatsicherrung.pfx** schreiben.
- Das gesamte Verzeichnis **D:\Install\Zertifikate** kann und sollte abschließend entweder in einer gut verschlüsselten Container-Datei oder auf einem ebenfalls verschlüsselten Wechselmedium abgelegt werden. Für Windows 2000 bietet sich hier die eingebaute Verschlüsselungsfunktion des **EFS-Dateisystems** an, für andere Systeme die entsprechenden Funktionen wie etwa PGPdisk von PGP oder Utimacos SaveGuard PrivateCrypto. (WinZIP und ähnliche Programme bieten zwar ebenfalls eine Verschlüsselung, diese ist aber nicht besonders sicher).

Seite 1

5. Konfigurationshinweise zur Sicherheit von Webservern

SSL sichert nur die Kommunikation zwischen Browser und Webserver. Um unberechtigten Zugang zu sensitiven Daten des Webservers zu erschweren, sollte man einige grundlegende Richtlinien beachten:

- Aktuelle Sicherheitspatches und Updates einspielen (vor Aktivieren des Netzwerkanschlusses!).
- Webserver auf gängigen Ports, vor allem Port 80, nur aktivieren, wenn unbedingt erforderlich.
- FTP- und ggf. Gopher-Dienste abschalten.
- Funktionen in "Verzeichnissicherheit" wie Benutzerauthentisierung und IP-Filter benutzen, um den Zugang auf das mögliche Mindestmaß zu beschränken.
- Stets mindestens ein Standarddokument definieren und ein solches auch im Zugriffspfad ablegen.
- Durchsuchen von Verzeichnissen nicht zulassen.
- Zugriffe auf übergeordnete Pfade oberhalb der Dokumentpfade überprüfen bzw. verhindern
- Default-Scripte (wie etwa test-cgi) durch Umbenennen des Pfades oder Entfernen auf eine Sicherungsdatei deaktivieren.
- Server-Scripts (cgi, php, asp, servlets etc.) möglichst nur auf dafür bestimmten Alias-Verzeichnissen zulassen.
- Keine Interpreter in Verzeichnissen mit allgemeiner Ausführungsberechtigung (cgi-bin) ablegen.
- Bei Frontpage Server-Extensions (Verzeichnisse _vti_xxx) auf Zugriffsrechte achten.
- Logging für alle Zugriffe aktivieren und regelmäßig überprüfen.

Zur Überprüfung weiterer sicherheitsrelevanter Einstellungen empfiehlt sich auch dringend eine Überprüfung mit Hilfe des Microsoft Baseline Security Analyzers (MBSA) und eine Überarbeitung der Einstellungen mit Hilfe des Lockdown-Tools (siehe auch unter http://www.kfa-juelich.de/zam/net/security/meissbu/2003/pc-windows-xp_html/pc-windows-xp.htm)

Zu guter Letzt bleibt immer ernsthaft zu erwägen, aus welchen Gründen sich der Betrieb eines eigenen Webservers mit all seinen Zusatzinvestitionen (Konfiguration, Systemsicherung, Benutzerverwaltung) und Zusatzrisiken wirklich lohnt. Einfache oder auch den Standards entsprechende dynamische Webseiten lassen sich mit geringerem Aufwand auf dem zentralen Webserver des Forschungszentrums Jülich anbieten und pflegen (S.Höfler-Thierfeldt, Tel. 6765). Der Server www.fz-juelich.de bietet sowohl weltweiten Port 80- als auch gesicherten SSL-Zugang und Untersützung für alle gängigen Verfahren zur Erzeugung dynamischer Webseiten.

Seite 1


J.Meißburger, Forschungszentrum Jülich, FZJ-ZAM, dokumentation.zam@fz-juelich.de