Protonet Server mit DynDNS-Adresse/Subdomain konfigurieren

Du möchtest, dass Dein Protonet Server unter einer eigenen Adresse erreichbar ist?

In diesem Dokument wird im ersten Teil beschrieben, wie der Server via DynDNS-Adresse erreichbar gemacht werden kann.

Der zweite Teil behandelt das Einrichten eines eigenen Zertifikates unter Nutzung einer eigenen Subdomain. Diese ist nur nötig, wenn der Meldung, dass das Zertifikat des Servers ungültig ist, vorgebeugt werden soll.

In dieser Anleitung spielen wir das Szenario exemplarisch durch und nutzen dabei einige Dienste anderer Hersteller und Anbieter:

DynDNS:	selfHOST.de	https://secure.selfhost.de
Internet-Router:	FRITZ!Box 7490	http://avm.de/produkte/fritzbox/fritzbox-7490
Webhoster:	Prosite	https://www.prosite.de
SSL-Zertifizierungsstelle:	StartSSL	https://www.startssl.com

Diese dienen nur als praktisches Beispiel und können durch andere Hersteller und Geräte ersetzt werden. Die Handhabung sollte dann jeweils ähnlich sein.

Jegliche Modifikationen an der Protonet-Lösung geschehen auf eigenes Risiko und sind nicht durch den Standard-Support abgedeckt!

Stellst Du nach Änderungen, dem Implementieren eigener Konfigurationen oder Skripte Beeinträchtigungen an der Protonet-Lösung fest, mach diese bitte rückgängig und teste, ob das Deaktivieren der eigenen Anpassungen die Probleme behebt. Hierfür kann das aktuelle Wartungspasswort, ein HDMI-fähiger Monitor sowie eine USB-Tastatur - beides direkt an der Box angeschlossen - nötig werden.

Gerne leiten wir Anfragen nach professioneller Unterstützung bei den folgenden Schritten an unseren externen Dienstleister und Spezialisten für kundenspezifische Anpassungen - Onlinehelp24 - weiter.

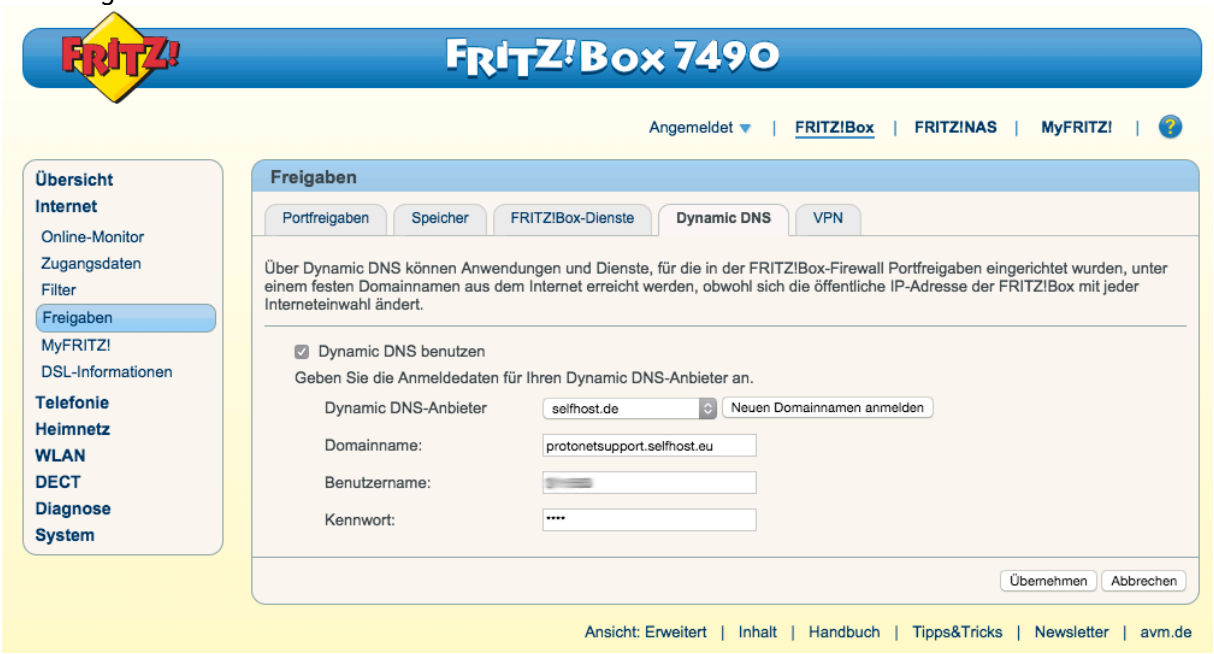
Teil 1: DynDNS Einrichtung

1. Bei einem DynDNS Dienstleister anmelden und Adresse registrieren

In dieser Anleitung nutzen wir: https://secure.selfhost.de und haben die Adresse protonetsupport.selfhost.eu dort angelegt.

2. Router mit der DynDNS Adresse konfigurieren

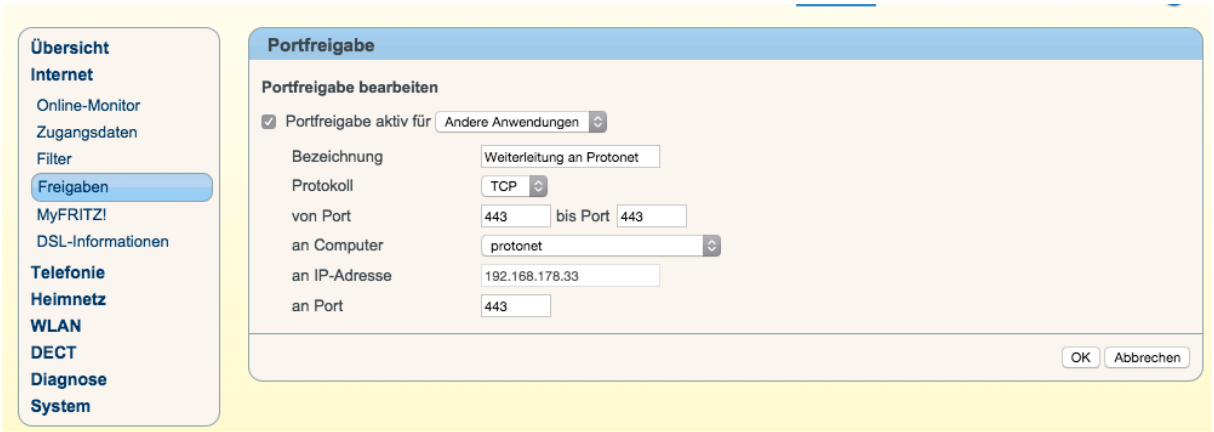
Der Router wird so eingerichtet, dass er regelmäßig seine aktuelle IP-Adresse an den DynDNS-Dienst meldet. In der Regel stellen sowohl die DynDNS Anbieter als auch die Routerhersteller hierfür Anleitungen bereit.



Achtung: Bei selfHOST.de werden im Router nicht die zuerst zugesandten Zugangsdaten eingegeben, sondern die unter „DynDNS Accounte“ gelisteten (Zugangsdaten Updateclient)!

3. Portfreigabe einrichten

Der Router soll alle Anfragen, die er an Port 443 erhält, an den Protonet Server an Port 443 weiterleiten. Bei „Computer“ ist hier der Hostname des Protonet Servers auszuwählen.



4. Änderung der Links in Protonet SOUL auf die neue Server-Adresse

Mit Benutzer „protonet“ und Wartungskennwort via ssh auf dem Protonet Servers einloggen und folgendes Kommando ausführen:

`custom_nodename` *`DynDNS-Adresse`*

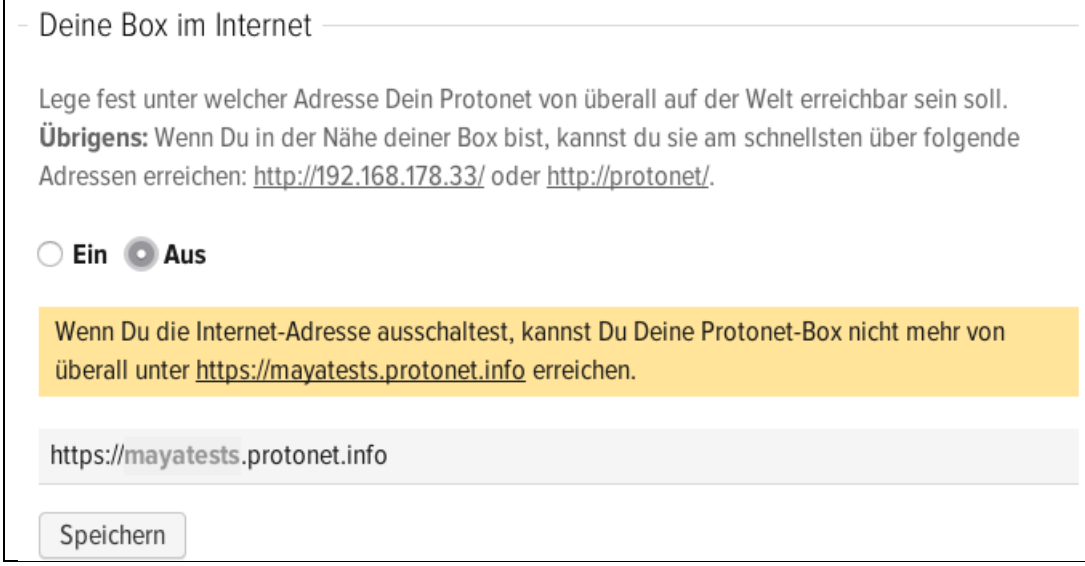
Beispiel:

```
protonet@mayatests.protonet.info soul2 (stable/57)
 ~ $ custom_nodename protonetsupport.selfhost.eu
protonetsupport.selfhost.eu
```

An dieser Stelle bitte das Wartungskennwort sicher zur Seite legen!

5. Internet-Adresse *.protonet.info in den Systemeinstellungen abschalten

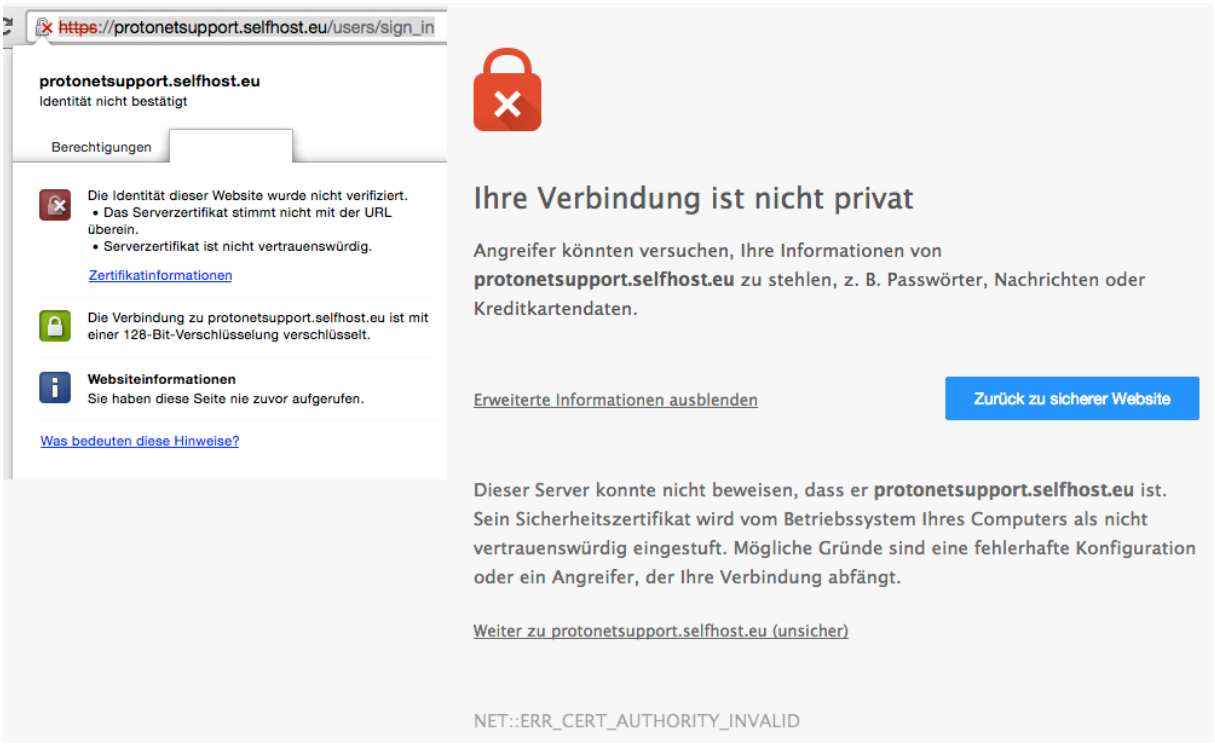
Ohne Abschaltung werden die Anpassungen in SOUL nicht aktiv!



Teil 2: Nutzung eines eigenen Zertifikates

6. Zertifikatsfehler (Serverzertifikat ist nicht vertrauenswürdig)

Nach Einrichtung der DynDNS-Adresse auf Router und Protonet Server wie im ersten Teil beschrieben, kann zwar via Browser und verschlüsselter Verbindung https://... auf Protonet SOUL zugegriffen werden, allerdings wird vorab eine Sicherheitswarnung angezeigt:



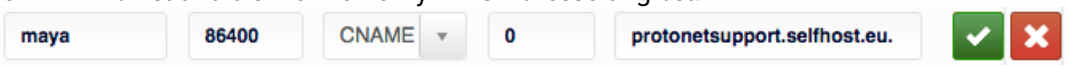
Diese besagt, dass die Verbindung zwar 128-Bit verschlüsselt ist, jedoch die Identität des Servers nicht bestätigt werden kann. Das ist Folge davon, dass das standardmäßig auf einem Protonet Server hinterlegte Zertifikat nur lokal gilt (protonet.local).

Möchtest Du diese Warnmeldung vermeiden, brauchst Du ein eigenes SSL-Serverzertifikat welches auf dem Protonet Server hinterlegt werden muss. Die folgenden Schritte helfen Dir dabei!

7. Eigene (Sub)domain auf DynDNS Adresse weiterleiten

Es scheint derzeit keinen Anbieter zu geben, bei dem es möglich ist für eine DynDNS Adresse ein Zertifikat zu erhalten. Die Domain-Inhaberschaft ist hier Voraussetzung und wird auch während der ersten Zertifikaterstellung gegen die Emailadresse des zuständigen Postmasters verifiziert.

Daher brauchst Du nun als erstes eine Domain, Subdomain oder jemanden, der eine hat, wo Du wie z.B. hier beim Websiteanbieter Prosite eine Subdomain unterhalb „DNS ändern“ anlegst, den Typ CNAME wählst und als Ziel Deine DynDNS-Adresse angibst.



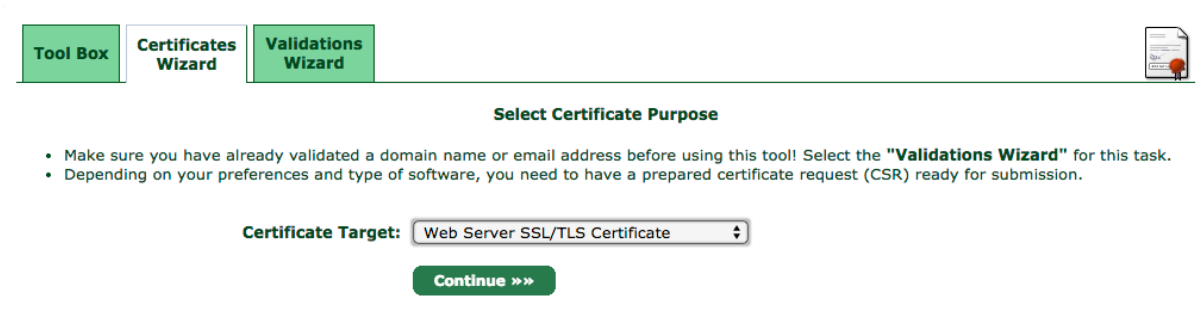
Kurz danach sollte über maya.*deinedomain.de* Dein Protonet Server bereits erreichbar sein.

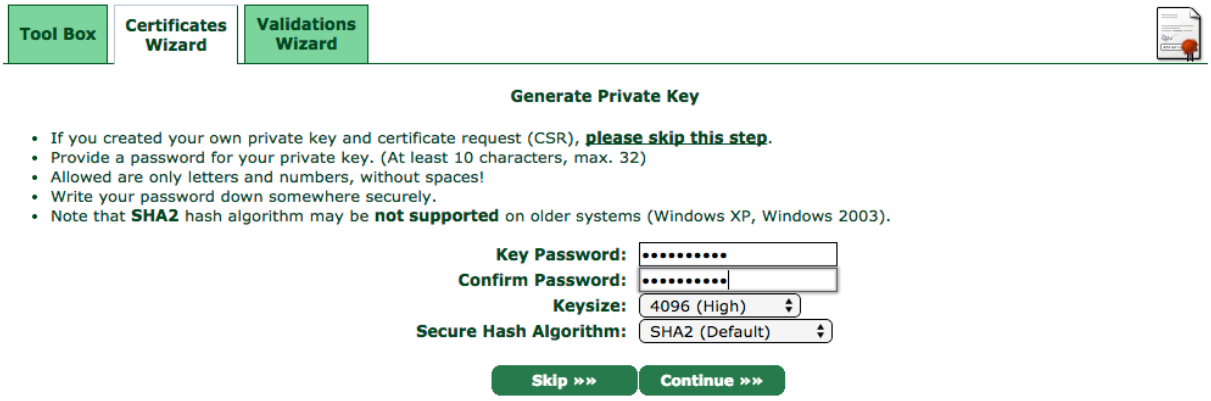
Da Du nun eine neue Adresse verwenden wirst, führe Schritt 4. „Änderung der Links in Protonet SOUL auf die neue Server-Adresse“ erneut aus, um die neue Adresse maya.deinedomain.de auf dem Server zu hinterlegen.

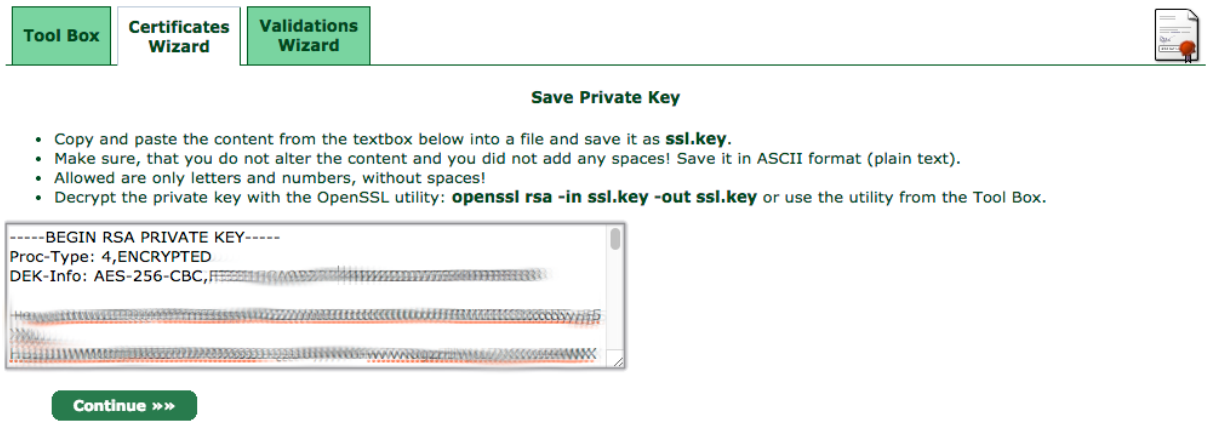
8. SSL Zertifikat erstellen, z.B. bei StartSSL im „Kontrollbereich“

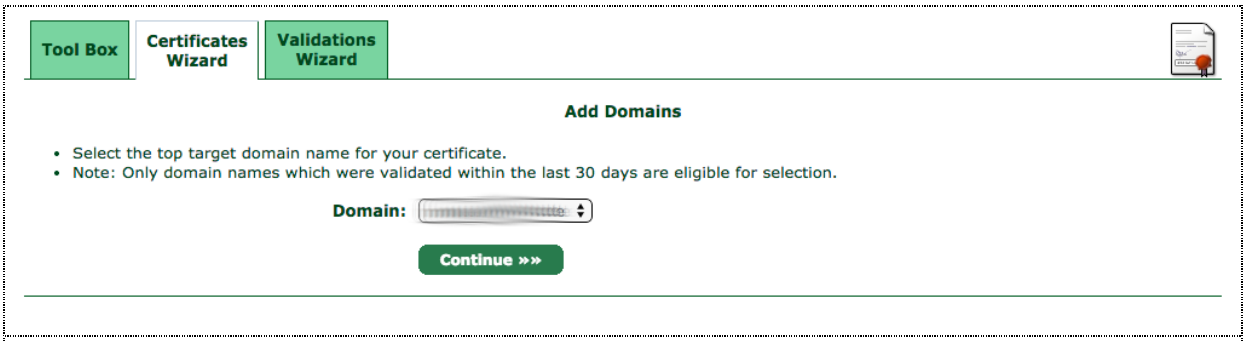
Was jetzt noch fehlt ist das SSL Serverzertifikat. Dieses erhälst Du z.B. bei Deinem Websiteanbieter oder weiteren Diensten, wie in unserem Beispiel StartSSL https://www.startssl.com.

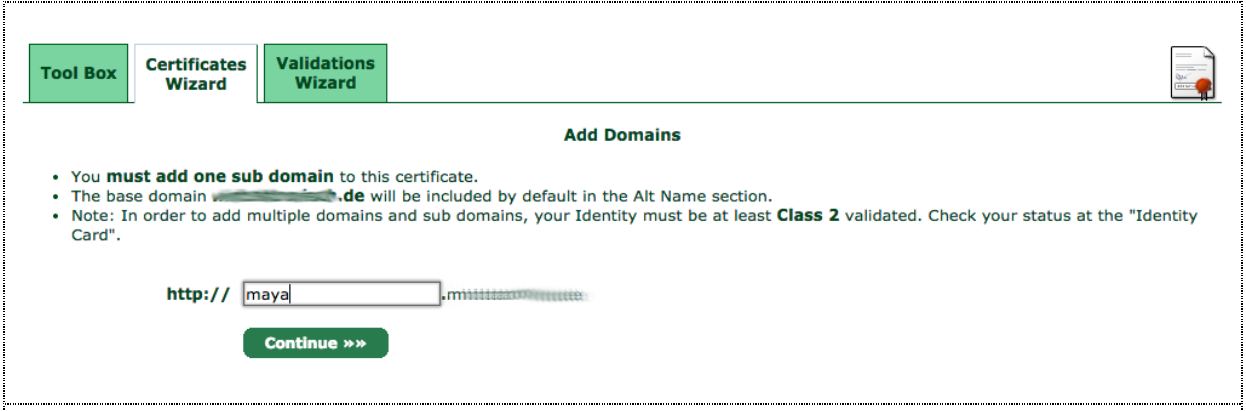
Nach erfolgreicher Registrierung kann über den Kontrollbereich der „Certificates Wizard“ ausgeführt werden, der die nötigen Zertfikate/Schlüssel bereitstellt. Folgende Screenshots zeigen die einzelnen Schritte. Diese werden sich nicht großartig von denen bei anderen Anbietern unterscheiden.

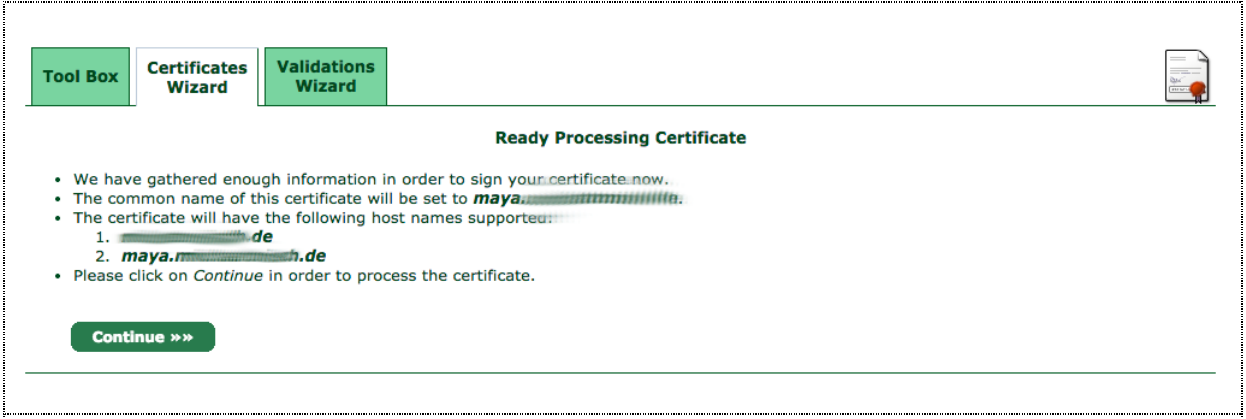


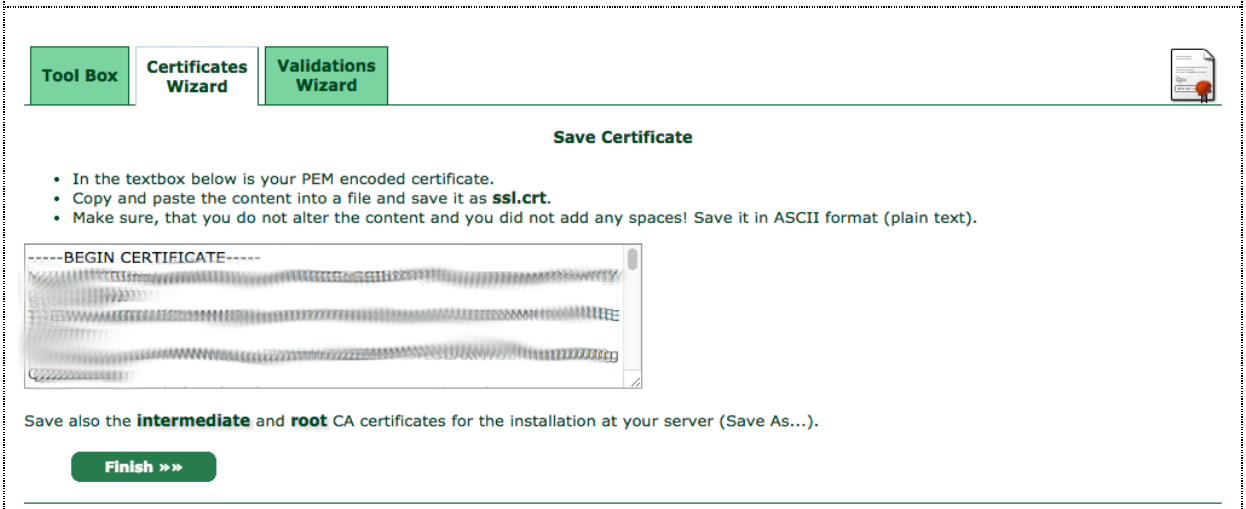












Der Prozess ist nun abgeschlossen. Die soeben erhaltenen Dateien liegen für die nächsten Schritte optimalerweise im gleichen Verzeichnis.

9. Zertfikat bearbeiten

Die während des Generierungsprozesses gespeicherten Dateien ssl.crt und ssl.key müssen nun noch bearbeitet werden.

a) Entschlüsseln des privaten Schlüssels, Benennung httpd_ssl.key
Über die StartSSL Toolbox oder den openssl-Befehl in der Linux oder MacOS-Konsole erstellst Du eine neue Datei „httpd_ssl.key“:

```
openssl rsa -in ssl.key -out httpd_ssl.key
```

b) Download der Dateien ca.pem und sub.class1.server.ca.pem
http://www.startssl.com/certs/ca.pem
http://www.startssl.com/certs/sub.class1.server.ca.pem
Optimalerweise speicherst Du diese in den gleichen Ordner wie die key und crt-Dateien.

c) Zusammenfassung der Dateien ssl.crt, sub.class1.server.ca.pem, ca.pem zu neuer Datei httpd_ssl.crt
Unter Linux oder MacOS geschieht das einfach über die Konsole:

```
cat ssl.crt sub.class1.server.ca.pem ca.pem > httpd_ssl.crt
```

Unter Windows würde man eine neue Datei httpd_ssl.crt erstellen und darin den Inhalt der einzelnen Dateien hintereinander kopieren.

Wichtig: Dateiinhalt konrollieren!

FALSCH:
Wenn ihr eine lange Zeile seht, diese zur Korrektur nach 5 - (Bindestrichen/Minuszeichen) umbrechen.
-----END CERTIFICATE----------BEGIN CERTIFICATE-----

RICHTIG:
Die einzelnen Segmente sind durch Zeilenumbrüche voneinander getrennt:
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

Vor und nach END bzw. BEGIN CERTIFICATE müssen jeweils 5 „-“ stehen!

10. Zertifikate auf dem Protonet Server bereitstellen

Die entstandenen Dateien httpd_ssl.key und httpd_ssl.crt müssen auf dem Protonet Server unter /**etc/protonet** hinterlegt werden.

Achtung: Hast Du das **Wartungskennwort** zum jetzigen Zeitpunkt noch nicht notiert und zur Seite gelegt, **solltest Du das jetzt tun!**
Das Bereitstellen inkorrekter Zertifkate kann dazu führen, dass Protonet SOUL nicht mehr geladen werden kann. In diesem Fall brauchst Du Konsolenzugriff um das Problem zu lösen!

11. Server neustarten

12. Nach Neustart und 5 Minuten warten SOUL nicht erreichbar?

a) Via SSH einloggen
b) Log auf Fehlermeldungen überprüfen:
```
tail -f /home/protonet/dashboard/shared/log/services/nginx/current
```
c) Ggf. die eigenen Zertifikate erstmal wieder löschen (neue werden automatisch generiert)

Bei Fragen oder Problemen, findest Du Unterstützung in der Support Community.