Knowledge Base

Importieren von Zertifikaten

Boll Engineering AG
Jurastrasse 58
CH-5430 Wettingen

Telefon +41 56 437 60 60
Fax +41 56 427 29 29
info@boll.ch • www.boll.ch

Datum	25.02.10 14:50
Hersteller	Fortinet, Seppmail, Watchguard, Mailfoundry
Modell Type(n)	n/a
Firmware	
Copyright	Boll Engineering AG, Wettingen
Autor	Tech-Abteilung
Dokument-Version	1.1

Situation:

In diesem Dokument wird beschrieben, wie Zertifikate, welche von einer Zertifizierungsstelle ausgestellt wurden, in verschiedenen Geräte wie Fortigate, FortiMail, Seppmail etc. importiert werden können und auf welche Besonderheiten der Geräte geachtet werden muss.

In den Beispielen wurde mit einem Wildcard-Zertifikat gearbeitet, welches von der SwissSign ausgestellt wurde (www.swisssign.ch).

Lösung:

Umwandeln des Zertifikateformats

Zertifikate werden von Signaturstellen typischerweise im PKCS#12 Format ausgeliefert. Dieses Format beinhaltet sowohl das öffentliche Zertifikateteil als auch den privaten Schlüssel aus dem das gesamte Zertifikat besteht.

Unter Umständen wird zum Importieren des Zertifikates von den jeweiligen Systemen andere Formate verlangt. Das Umwandeln von einem Format in ein anderes ist am Einfachsten mit OpenSSL (www.openssl.org) zu bewerkstelligen.

Verschiedene Formate:

-	.CER	CER-kodiertes Zertifikat oder Zertifikatsfolgen
-	.CRT	DER- oder Base64-kodiertes Zertifikat
-	.DER	DER-kodiertes Zertifikat
-	.P12	oder
	.PFX	PKCS#12, kann öffentliche Zertifikate und private Schlüssel (Kennwort-geschützt) enthalten.
-	.P7C	oder
	.P7B	PKCS#7-signierte Datenstruktur ohne Dateninhalt, nur mit Zertifikat(en) oder Zertifikatsperrliste(n)
-	.PEM	Base64-kodiertes Zertifikat, umschlossen von „-----BEGIN CERTIFICATE-----“ und „-----END CERTIFICATE-----“

Boll Engineering AG
Jurastrasse 58
CH-5430 Wettingen
Telefon +41 56 437 60 60
Fax +41 56 427 29 29
info@boll.ch • www.boll.ch

Die Installation und Nutzung von OpenSSL ist kostenfrei. Unter www.openssl.org können die Software Packages herunter geladen werden. Ein Link für ein Windows-Binary findet sich unter www.openssl.org/related/binaries.

Nach der Installation unter Windows kann OpenSSL im DOS Prompt im Installationsverzeichnis\bin gestartet werden.

A) Extrahieren des öffentlichen Zertifikats aus einem PKCS#12 File

```
openssl pkcs12 -in <filename>.p12 -nokeys -out <neuer_filename>.crt
```

B) Extrahieren des privaten Schlüssels aus einem PKCS#12 File
(Der private Schlüssel wird verschlüsselt abgelegt)

```
openssl pkcs12 -in <filename>.p12 -nocerts -out <neuer_filename>.key
```

C) Extrahieren des privaten Schlüssels aus einem PKCS#12 File
(Der private Schlüssel wird unverschlüsselt abgelegt)

```
openssl pkcs12 -in <filename>.p12 -nocerts -out <neuer_filename>.key -nodes
```

D) Konvertieren des privaten Schlüssels aus einem PKCS#12 File in ein PKCS#8 File

```
openssl pkcs12 -in <filename>.p12 -nocerts -out <neuer_filename>.key -nodes
openssl pkcs8 -in <filename>.key -topk8 -out <neuer_filename>.pk8
```

> Achtung: Achten Sie darauf, dass kein Unberechtigter in Besitz des privaten Keyfiles kommt. Schon gar nicht, wenn dieses unverschlüsselt ist. Sonst wäre es möglich, dass ein Fremder sich mit der Identität Ihres Zertifikates ausgibt oder Ihren über das Zertifikat verschlüsselten Datenstrom ohne Probleme wieder entschlüsseln kann.

Importieren des Zertifikats in eine FortiGate

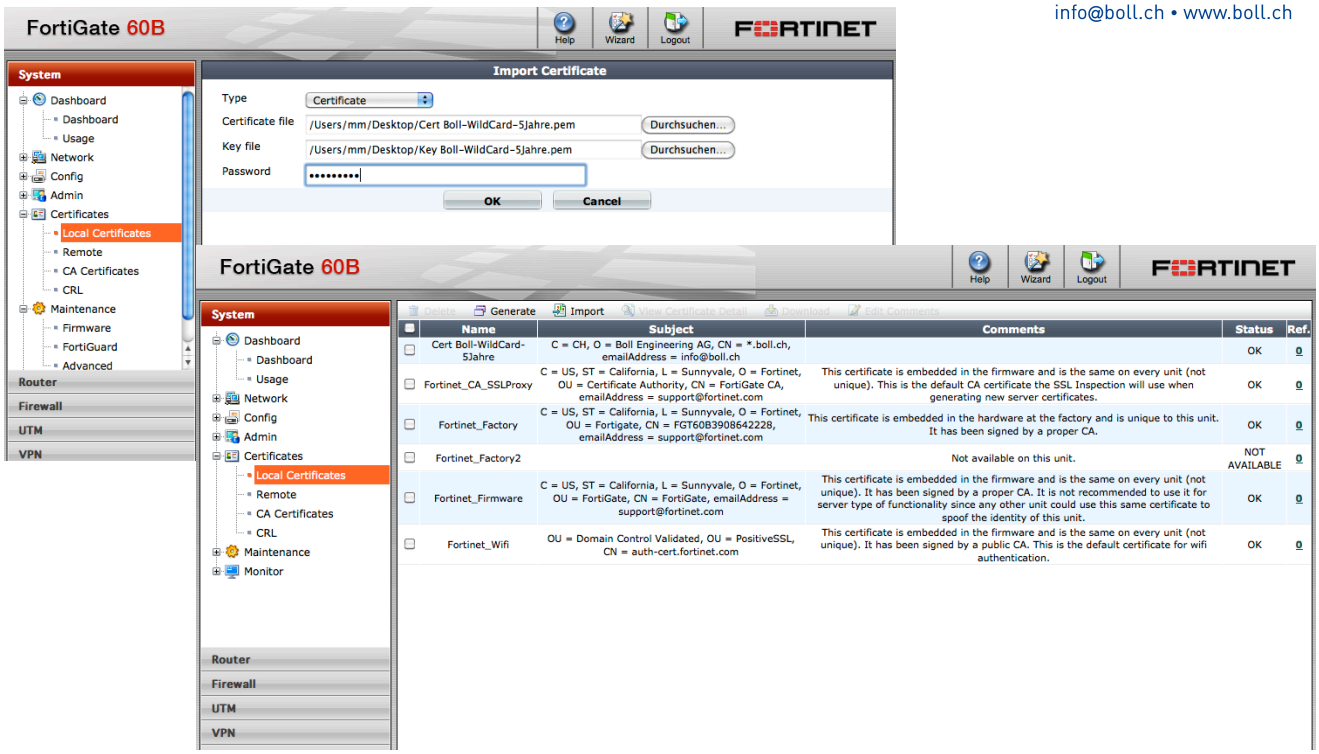
Auf der Fortigate haben sie die Möglichkeit ein Zertifikate Request direkt auf dem Gerät zu generieren (System → Certificates → Local Certificates → Button: Generate). Diesen Zertifikate Request können Sie dann von einer CA signieren lassen und über den dazu gehörigen Import-Button das signierte Zertifikat dann einlesen.

Allerdings ist es auch möglich, ein Zertifikat zu importieren, welches nicht auf der Fortigate generiert wurde (dies ist insbesondere für Wildcard-Zertifikate wichtig). Dieser Import kann entweder über das PKCS#12 File erfolgen oder über die getrennten Files (.crt-file, .key-file).

Für die Fortigate Geräte scheint es sinnvoll zu sein, das Zertifikat wie oben beschrieben zuerst aufzuteilen.

Danach können die beiden Dateien dann im Menu „System → Certificates → Local Certificates“ über den Button „Import“ → Type: Certificate eingelesen werden.

Boll Engineering AG
Jurastrasse 58
CH-5430 Wettingen
Telefon +41 56 437 60 60
Fax +41 56 427 29 29
info@boll.ch • www.boll.ch



Nun muss noch konfiguriert werden, wofür das Zertifikat überhaupt verwendet werden soll. Typischerweise kann das Zertifikate im WebGUI über eine Dropdown-Liste ausgewählt werden (z.B. für IPSec oder SSL VPN, SSL Offloading).

Für eine Einstellung wird jedoch das CLI gebraucht:

- Zum Aufruf des Fortigate WebGUI mit https:
  (FortiOS v3.0/v4.0)

```
config system global
  set admin-server-cert <cert-name>
end
```

Besonderheiten:
Ist das Zertifikat nicht direkt von einem CA Zertifikat, sondern von einem Intermediate Zertifikat signiert worden, so wird es zumindest bei Nutzung von Firefox eine Fehlermeldung geben, das dem Aussteller des Zertifikates nicht vertraut wird. Eine Variante wäre dann, dieses Intermediate Zertifikat im Browser zu installieren, die elegantere Variante ist aber, die Fortigate dazu zu bringen, dieses Intermediate Zertifikat gerade mitzuliefern.

Dieses geschieht recht einfach, indem man das Intermediate Zertifikat auf der Fortigate als „CA Certificate“ importiert. Das Intermediate Zertifikat kann dafür direkt auf den Webseiten der CA herunter geladen werden. Meist ist es aber auch im .crt-file des eigenen Zertifikats enthalten. Die .crt-Datei kann einfach mit dem Wordpad geöffnet werden. Nun muss lediglich der entsprechende Abschnitt (beginnend mit „-----BEGIN CERTIFICATE-----“ und endend mit „-----END CERTIFICATE-----“ in ein eigenes .crt-File gespeichert werden.

Boll Engineering AG
Jurastrasse 58
CH-5430 Wettingen
Telefon +41 56 437 60 60
Fax +41 56 427 29 29
info@boll.ch • www.boll.ch

Beispiel (Abschnitte wurden der Übersichtlichkeit wegen gekürzt):

```
Bag Attributes
    localKeyID: …
    friendlyName: Boll Engineering AG
subject=/C=CH/O=Boll Engineering AG/CN=*.boll.ch/emailAddress=info@boll.ch
issuer=/C=CH/O=SwissSign AG/CN=SwissSign Server Gold CA 2008 - G2
-----BEGIN CERTIFICATE-----
MII…
…
…xmQ=
-----END CERTIFICATE-----
Bag Attributes
    localKeyID: …
subject=/C=CH/O=SwissSign AG/CN=SwissSign Server Gold CA 2008 - G2
issuer=/C=CH/O=SwissSign AG/CN=SwissSign Gold CA - G2
-----BEGIN CERTIFICATE-----
MII…
…
…0qo=
-----END CERTIFICATE-----
Bag Attributes
    localKeyID: …
subject=/C=CH/O=SwissSign AG/CN=SwissSign Gold CA - G2
issuer=/C=CH/O=SwissSign AG/CN=SwissSign Gold CA - G2
-----BEGIN CERTIFICATE-----
MII…
…
…ZfJ
-----END CERTIFICATE-----
```

In diesem .crt-File ist ein Zertifikat für `CN=*.boll.ch` zu sehen (erster Abschnitt). Dieses ist signiert worden vom Intermediate Zertifikat `CN=SwissSign Server Gold CA 2008 - G2`. Der dazugehörige (im Beispiel gelbmarkierte) Abschnitt muss für unserem Fall in ein .crt-File gespeichert werden, welches dann als CA-Certificate in der Fortigate importiert werden kann.

Als letztes ist in diesem Beispiel das CA Zertifikat `CN=SwissSign Gold CA - G2` hinterlegt. Dieses Zertifikat ist bei den meisten aktuellen Browsern bereits als vertrauenswürdiges CA Zertifikat gespeichert.

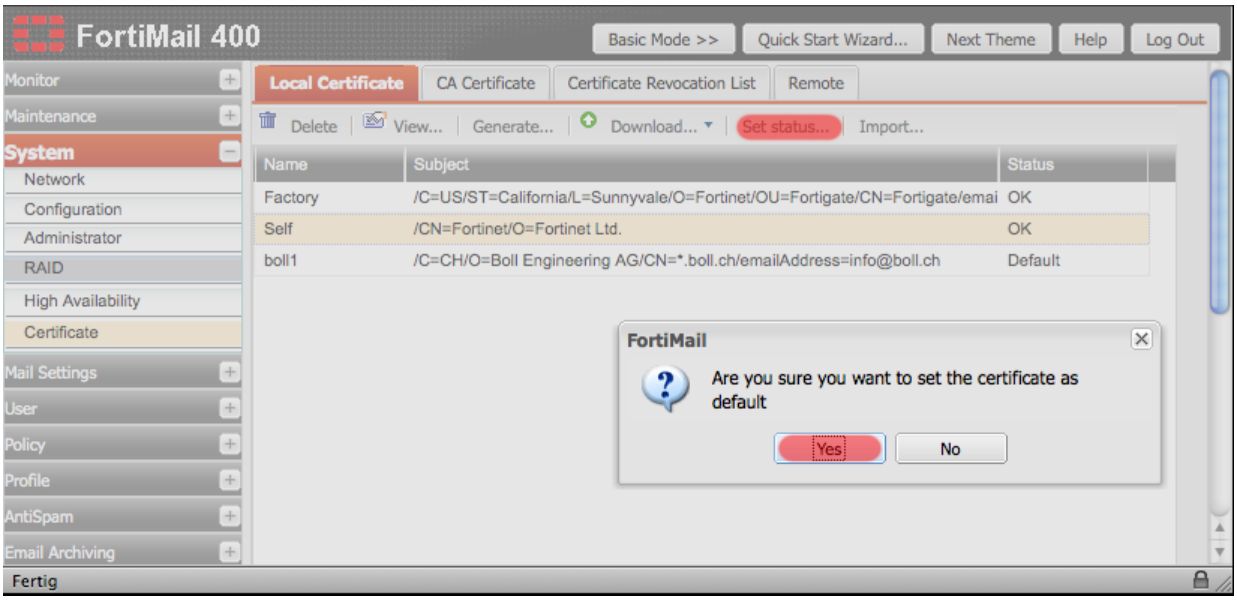
Zu beachten ist hierbei, dass zumindest bis zu FortiOS v4.1 die Fortigate rebootet werden muss, damit das importierte CA Zertifikate auch verwendet werden. Die Notwendigkeit des Reboots ist ein „known issue“ und sollte zumindest seit v4.2 gefixt sein.

Boll Engineering AG
Jurastrasse 58
CH-5430 Wettingen
Telefon +41 56 437 60 60
Fax +41 56 427 29 29
info@boll.ch • www.boll.ch

Importieren des Zertifikats in eine FortiMail

Für den Import des Zertifikats auf der FortiMail gelten prinzipiell die gleichen Regeln wie für die Fortigate. Auch hier erscheint es erfolgsversprechender, nicht das PKCS#12-File einzulesen, sondern die beiden getrennten Files (einmal das öffentliche Zertifikat, einmal den private Key).

Um dieses Zertifikat als Default-Zertifikat zu setzen, muss dieses über das Web-GUI mit dem Button „Set status“ definiert werden:



Unter FortiMail v3.0 passiert dies mit einem Klick auf den Haken hinter dem jeweiligen Zertifikate:

Oder man kann ebenfalls ins CLI wechseln und die Zertifikate dort als „default“ setzen:

FortiMail v3.0:

```
set system certificate local defaultcertificate '<certname>'
```

FortiMail v4.0:

```
config system global
  set default-certificate '<certname>'
end
```

Besonderheiten:
Für den Fall, dass das eigene Zertifikat von einem Intermediate Zertifikat signiert wurde, so gibt es hier eine Unterscheidung zur Fortigate.

Auf der FortiMail muss das Intermediate Zertifikat nicht als CA Zertifikat eingelesen werden. Sofern das .crt-File nicht nur das öffentliche Zertifikat selbst, sondern zusätzlich die gesamte Zertifikate-Kette enthält (wie im Beispiel auf Seite 4), so reicht die FortiMail automatisch die gesamte Zertifikate-Kette weiter.

BOLL
IT Security Distribution

Boll Engineering AG
Jurastrasse 58
CH-5430 Wettingen

Telefon +41 56 437 60 60
Fax +41 56 427 29 29
info@boll.ch • www.boll.ch

Importieren des Zertifikats in eine Watchguard SSL 100

Importieren des CA Certificates
Das CA Certificate wird benutzt, falls Sie Benutzerauthentifizierung mittels Zertifikaten machen möchten.

1. Gehen Sie dazu im Administration Web UI unter „Manage System“ → „Certificates“ → „Add Certificate Authority...”
2. Geben Sie im Feld „CA Certificate „das CA Zertifikat von Ihrem Zertifikatsanbieter an.
3. Falls der Zertifikatsanbieter „Certificate Revokation Lists“ anbieten, können Sie dies ebenfalls in diesem Menü konfigurieren.

Importieren des Server Certificates
Das Server Zertifikat kann für den Zugriff auf das SSL Portal und das Administration UI genutzt werden.

1. Gehen Sie dazu im Administration Web UI unter „Manage System“ → „Certificates“ → „Add Server Certificate...
2. Geben Sie im Feld „Certificate „das Zertifikat von Ihrem Zertifikatsanbieter an. Konvertieren Sie dieses gemäss Anleitung „Extrahieren des öffentlichen Zertifikats aus einem PKCS#12 File“ in ein .crt File.
3. Geben Sie im Feld Key das Keyfile an. Dieses erhalten Sie gemäss Anleitung „Konvertieren des privaten Schlüssels aus einem PKCS#12 File in ein PKCS#8 File“
4. Geben Sie im Password Feld das gesetzte Passwort aus der Konvertierung des PKCS#8 Files ein.
5. Falls Sie das Root CA Certificate hocheladen haben, können Sie dieses dem Server Certificate zurodnen. Wählen Sie dazu das erstellte CA Zertifikat aus.

Setzen des Server Zertifikates für das SSL Portal

1. Gehen Sie dazu im Administration Web UI unter „Manage System“ → „Device Settings“ → und wählen Sie das erstellte „Server Certificate“ aus.
2. Speichern und Publishen Sie die Konfiguration.

Setzen des Server Zertifikates für das Administration UI

3. Gehen Sie dazu im Administration Web UI unter „Manage System“ → „Administration Service“ → und wählen Sie das erstellte „Server Certificate“ aus.
4. Speichern und Publishen Sie die Konfiguration.

Boll Engineering AG
Jurastrasse 58
CH-5430 Wettingen
Telefon +41 56 437 60 60
Fax +41 56 427 29 29
info@boll.ch • www.boll.ch

Importieren des Zertifikats in eine Mailfoundry

Zertifikate einlesen
Auf der Mailfoundry werden Zertifikate unter folgendem Menü eingelesen:
„System Settings“ → „SSL Certificates“ → „SSL Certificate Uploads”

Geben Sie im Feld „Upload SSL Certificate File“ das Zertifikat an. Dieses generieren Sie gemäss Anleitung „Extrahieren des öffentlichen Zertifikats aus einem PKCS#12 File“.

Den Key generieren Sie gemäss Anleitung „Extrahieren des privaten Schlüssels aus einem PKCS#12 File (der private Schlüssel wird unverschlüsselt abgelegt)“ und geben diese Datei im Feld „Upload SSL Key File“ an.

Das CA Zertifikat für das Feld „Upload SSL CA Cert File” erhalten Sie von Ihrem Zertifikatsanbieter.

SSL Zugang aktivieren
Den HTTPS Zugang auf die Mailfoundry aktivieren Sie im Menü:
„System Settings“ → „SSL Settings → Enable SSL and non-SSL Web User Interface oder Enable SSL for Web User Interface only (für Zugang nur auf Port 443).

Boll Engineering AG
Jurastrasse 58
CH-5430 Wettingen
Telefon +41 56 437 60 60
Fax +41 56 427 29 29
info@boll.ch • www.boll.ch

Importieren des Zertifikats in eine SeppMail

Menüpunkt "SSL"
Dient der Verwaltung des Secure Sockets Layer (SSL) Zertifikats der Appliance.

Folgende SSL Einstellungen können auf der SeppMail vorgenommen werden:

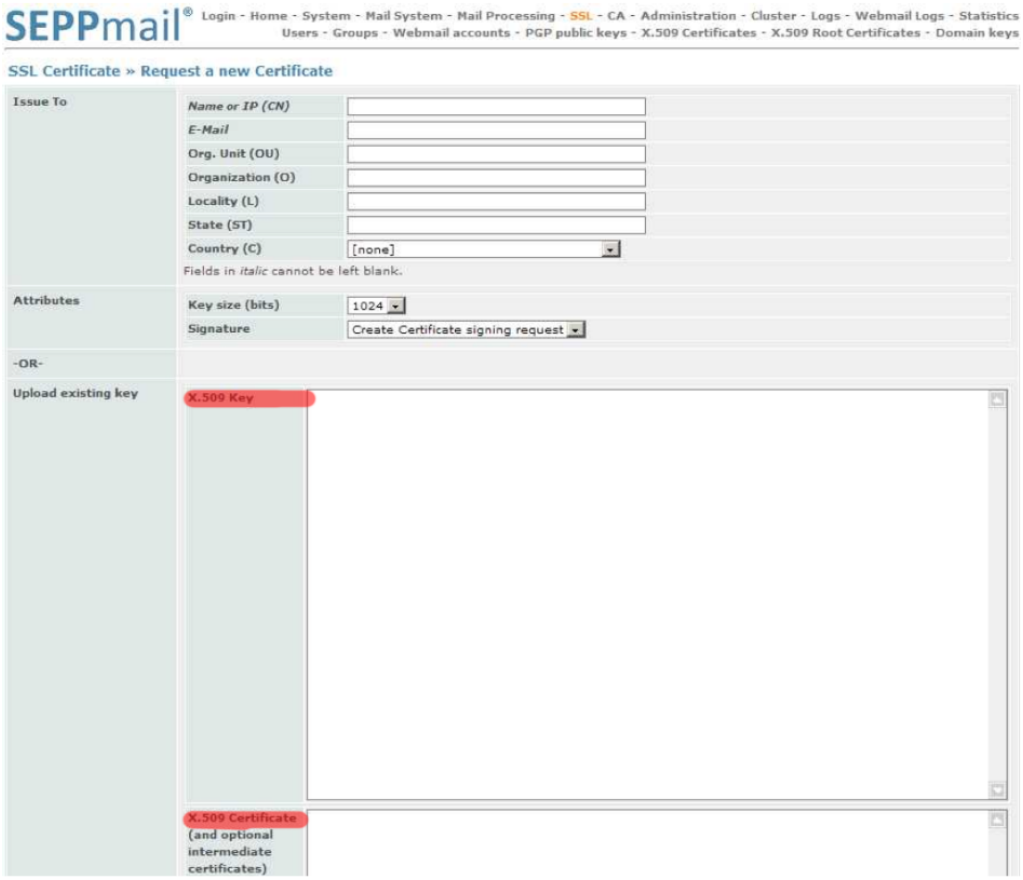
- SSL-Zertifikat selbst erstellen
- SSL-Zertifikat von einer Zertifizierungsstelle anfordern
- Bestehendes SSL-Zertifikat verwenden
- SSL-Zertifikat sichern

Um für Ihre Appliance ein eigenes, bereits bestehendes SSL-Zertifikat zu verwenden, klicken Sie im Web-Administrationsportal auf den Menüpunkt `SSL`. Klicken Sie anschliessend auf die Schaltfläche "Request a new Certificate...".

Verwenden Sie eines der folgende Felder in der Rubrik `Upload existing key`:

- `X.509 Key:` Fügen Sie hier Ihr SSL-Zertifikat in Textform ein.
- `X.509 Certificate (and optional intermediate certificates):` Benutzen Sie dieses Feld, falls Sie ein Zertifikat inkl. Zertifikate übergeordneter Zertifizierungsstellen verwenden wollen.

Schliessen Sie den Vorgang in beiden Fällen ab, indem Sie auf die Schaltfläche "Create Request" klicken.



Felder "X.509 Key" und "X.509 Certificate (and optional intermediate certificates)"