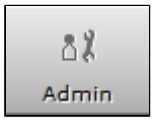
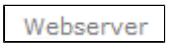
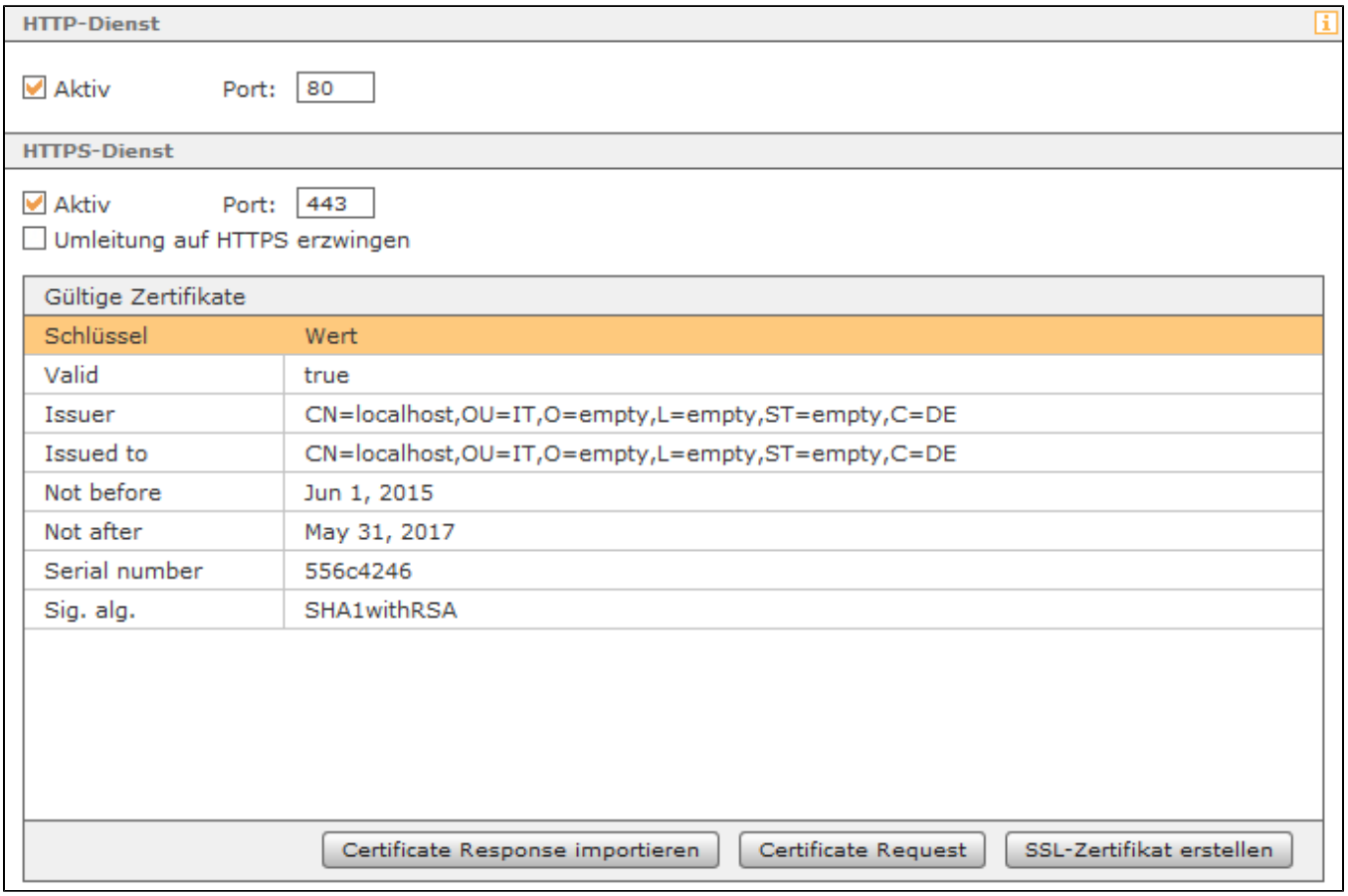
Webserver auf der STARFACE konfigurieren

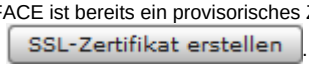
Weboberfläche der STARFACE	Menüpunkt "Admin"	Menüpunkt "Server"	Reiter "Webserver"
			

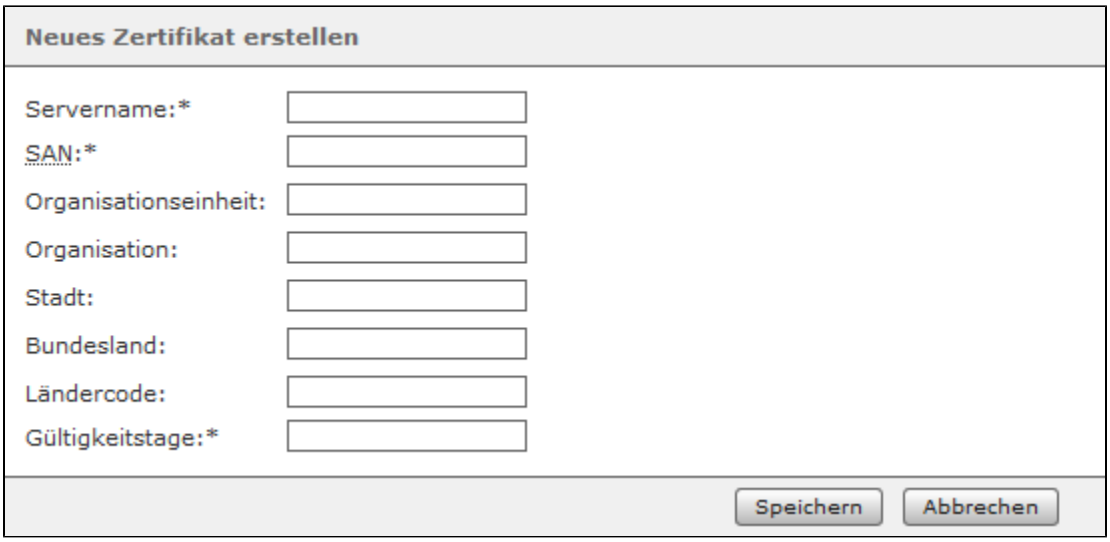
Standardmäßig ist für den Webserver der STARFACE neben dem HTTP-Dienst auch der HTTPS-Dienst aktiviert. Beide Dienste sind auf den Standardports (80 und 443) erreichbar und diese können durch die Auswahl der jeweiligen Checkbox aktiviert bzw. deaktiviert werden.



Die "Checkbox Umleitung auf HTTPS erzwingen" ermöglicht den Zugriff auf die Weboberfläche der STARFACE nur noch über HTTPS.

> **Hinweis:** Wenn der HTTP-Dienst deaktiviert oder der Standardport 80 geändert wird, kann es zu Problemen mit einigen Anbindungen kommen wie z.B. dem Adressbuch auf SIP-Telefonen.

Um HTTPS zu verwenden, wird ein Zertifikat für den Webserver benötigt. In der STARFACE ist bereits ein provisorisches Zertifikat hinterlegt. Sollte dieses provisorische Zertifikat ablaufen sein, kann es neu erstellt werden über die Schaltfläche  . Dabei öffnet sich die folgende Eingabemaske:



In dieser Maske sind zwei Angaben zwingend erforderlich:

Feldname	Beschreibung
Servername	Diese Angabe bezeichnet die Domain für die das Zertifikat gültig sein soll.
SAN	Diese Angabe bezeichnet den Alternativnamen, welcher im Zertifikat angegeben ist und die Gültigkeit um weitere Domainnamen erweitert. Dieser Name muss nicht mit der Grunddomain zusammenhängen (Common name).
Gültigkeitstag	Diese Angabe bezeichnet wie lange das Zertifikat in Tagen gültig sein soll.

Der Domainname muss vollständig und korrekt sein, z.B. firmenname.net (ohne https://). Ein Zertifikat besitzt in der Regel keine Gültigkeit für etwaige Subdomains, wobei sogenannte Wildcard-Zertifikate eine Ausnahme bilden. Um dem Sinn eines echten Serverzertifikats gerecht zu werden, muss das Zertifikat von einer externen Zertifizierungsstelle (Certificate Authority oder CA) signiert werden. Eine Auswahl anerkannter Zertifizierungsstellen findet sich in den Einstellungen des verwendeten Webbrowsers. Eine externe Zertifizierung ist allerdings nicht zwingend notwendig, wenn z.B. die STARFACE nur intern erreichbar ist.

> ⚠ **Hinweis:** Bitte beachten Sie auch die Anforderungen und Bedingungen der jeweiligen Zertifizierungsstellen für diesen Prozess.

Über die Schaltfläche Certificate Request wird eine verschlüsselte Datei des Zertifikats erzeugt. Der Inhalt des Fensters muss kopiert werden und per E-Mail an die ausgewählte Zertifizierungsstelle gesendet werden. Die Zertifizierungsstelle prüft den Antrag und sendet, in der Regel per E-Mail, das signierte Zertifikat zurück.

Das Importieren des signierten Zertifikats erfolgt über die Schaltfläche Certificate Response importieren, dabei öffnet sich ein neues Fenster mit zwei Textfeldern. Das signierte Zertifikat der Zertifizierungsstelle wird dabei in das obere Textfeld eingetragen. Da der Aufbau der Rückmeldungen der verschiedenen Zertifizierungsstellen sehr unterschiedlich ausfallen können, wird empfohlen alle erhaltenen Zertifikate (mit Ausnahme des Root-Certificate der Zertifizierungsstelle) in der folgenden Form zusammen zu kopieren:

```
-----BEGIN CERTIFICATE-----
        CA Zertifikat
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
        Intermediate Zertifikat 1
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
        Intermediate Zertifikat 2
-----END CERTIFICATE-----
```

und in dieser Form in das obere Textfeld einzutragen. Dabei ist zu beachten, dass es nicht immer ein Intermediate Zertifikat gibt bzw. es auch mehr als 2 Intermediate Zertifikate geben kann.

> ⚠ **Hinweis:** Es muss beachtet werden, dass beim Kopiervorgang keine überschüssigen Leerzeilen und Leerzeichen eingefügt werden.

Das Root-Certificate der Zertifizierungsstelle wird in das untere Textfeld kopiert.