
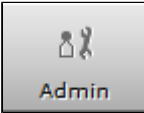



Webserver auf der STARFACE konfigurieren

Weboberfläche der STARFACE	Menüpunkt "Admin"	Menüpunkt "Server"	Reiter "Webserver"
	 Admin	 Server	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. Werden diese Standardports verändert hat dies weitreichende Auswirkungen und muss auch bei Firewallfreigaben beachtet werden (z.B. Zugriff der STARFACE Desktop App auf STARFACE NEON oder das Adressbuch).

Alle Cloudinstanzen, die nach dem 01.06.2018 erstellt worden sind, verfügen über ein offizielles Zertifikat.



Hinweis: Eine Anpassung des Webserver auf den Cloudinstanzen der Firma Starface ist möglich, es sollen aber keine eigenen Zertifikate eingespielt werden!

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



Hinweis: Bei Cloudinstanzen ohne dedizierte IPv4-Adresse darf der Port für HTTPS (443) nicht geändert werden.

HTTP-Dienst	
<input checked="" type="checkbox"/> Aktiv	Port: <input type="text" value="80"/>
HTTPS-Dienst	
<input checked="" type="checkbox"/> Aktiv	Port: <input type="text" value="443"/>
<input type="checkbox"/> Umleitung auf HTTPS erzwingen	
Gültige Zertifikate	
Schlüssel	Wert
Gültig	true
Aussteller	CN=GeoTrust RSA CA 2018,OU=www.digicert.com,O=DigiCert Inc,C=US
Inhabername	CN=*.starface-cloud.com,O=STARFACE GmbH,L=Karlsruhe,ST=Baden-Württemberg,C=DE
Alternative Inhaberbe...	*.starface-cloud.com,starface-cloud.com
Nicht vor	December 7, 2022 1:00:00 AM CET
Nicht nach	December 7, 2023 12:59:59 AM CET
Signatur	SHA-256 - f6:4f:df:37:7c:b3:da:c2:2c:08:b3:92:2b:9a:df:10:e1:47:b7:c3:2f:a9:d7:23:1d:de:5...
<div>Certificate Response importierenCertificate RequestNeues ZertifikatZertifikat mit privatem Schlüssel importieren</div>	

Sollte das provisorische Zertifikat abgelaufen sein, kann es neu erstellt werden über die Schaltfläche **Neues Zertifikat**. Dabei öffnet sich die folgende Eingabemaske:

Neues Zertifikat erstellen	
Servername:*	<input type="text"/>
SAN:*	<input type="text"/>
Organisationseinheit:	<input type="text"/>
Organisation:	<input type="text"/>
Stadt:	<input type="text"/>
Bundesland:	<input type="text"/>
Ländercode:	<input type="text"/>
Gültigkeitstage:*	<input type="text"/>
Schlüsselalgorithmus:*	<input type="text" value="RSA 4096"/> <input type="button" value="v"/>
<input type="button" value="Speichern"/> <input type="button" value="Abbrechen"/>	

In dieser Maske sind folgende 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.
Schlüsselalgorithmus	In diesem Drop-Down-Menü wird der Algorithmus konfiguriert, der für das neue Zertifikat genutzt werden 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. Es sind auch die Anforderungen und die Bedingungen der jeweiligen Zertifizierungsstellen für diesen Prozess zu berücksichtigen.

Über die Schaltfläche **Certificate Request** wird eine verschlüsselte Version des Zertifikats erzeugt, wobei auch die Stärke des Schlüsselalgorithmus via Drop-Down-Feld ausgewählt werden kann. 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.



Hinweis: Ein neuer Request sollte erst ausgelöst werden, wenn die vorherige Anfrage vollständig bearbeitet worden ist. Bei jedem neuen Request wird ein neuer privater interner Schlüssel generiert.

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 dem folgenden X.509 Format zusammen zu kopieren:

```
-----BEGIN CERTIFICATE-----
      Server Zertifikat (Eigenes 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 in der Form:

```
-----BEGIN CERTIFICATE-----  
    Root Zertifikat  
-----END CERTIFICATE-----
```

Über die Schaltfläche:


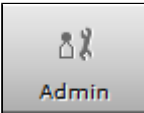

Zertifikat mit privatem Schlüssel importieren

kann ein Zertifikat mit privatem Schlüssel importiert werden. Dabei müssen die verschiedenen Teile der Zertifikatskette zwingend in der folgenden Reihenfolge eingegeben werden:

1. privater Schlüssel ohne Passwort
2. Serverzertifikat
3. Intermediate CA-Zertifikate
4. Root-CA-Zertifikat



Hinweis: Der private Schlüssel darf nicht verschlüsselt sein!

Weboberfläche der STARFACE	Menüpunkt "Admin"	Menüpunkt "Server"	Reiter "Webserver"
	 Admin	 Server	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. Werden diese Standardports verändert hat dies weitreichende Auswirkungen und muss auch bei Firewallfreigaben beachtet werden (z.B. Zugriff der STARFACE Desktop App auf STARFACE NEON oder das Adressbuch).

Alle Cloudinstanzen, die nach dem 01.06.2018 erstellt worden sind, verfügen über ein offizielles Zertifikat.



Hinweis: Eine Anpassung des Webserver auf den Cloudinstanzen der Firma Starface ist möglich, es sollen aber keine eigenen Zertifikate eingespielt werden!

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



Hinweis: Bei Cloudinstanzen ohne dedizierte IPv4-Adresse darf der Port für HTTPS (443) nicht geändert werden.

HTTP-Dienst

☒ Aktiv

Port:

HTTPS-Dienst

☒ Aktiv

Port:

☐ Umleitung auf HTTPS erzwingen

Gültige Zertifikate

Schlüssel	Wert
Valid	false
Issuer	CN=localhost,OU=IT,O=empty,L=empty,ST=empty,C=DE
Issued to	CN=localhost,OU=IT,O=empty,L=empty,ST=empty,C=DE
Not before	Jun 1, 2015
Not after	May 31, 2017
Serial number	556c4246
Sig. alg.	SHA1withRSA

Certificate Response importieren

Certificate Request

Neues Zertifikat

Sollte das provisorische Zertifikat abgelaufen sein, kann es neu erstellt werden über die Schaltfläche **Neues Zertifikat**. Dabei öffnet sich die folgende Eingabemaske:

Neues Zertifikat erstellen

Servername:*

SAN:*

Organisationseinheit:

Organisation:

Stadt:

Bundesland:

Ländercode:

Gültigkeitstage:*

Speichern

Abbrechen

In dieser Maske sind folgende 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. Es sind auch die Anforderungen und die Bedingungen der jeweiligen Zertifizierungsstellen für diesen Prozess zu berücksichtigen.



Hinweis: Bitte beachten Sie, dass über die Weboberfläche keine Private Keys importiert werden können.

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 dem folgenden X.509 Format 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.

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. Werden diese Standardports verändert hat dies weitreichende Auswirkungen und muss auch bei Firewallfreigaben beachtet werden (z.B. Zugriff der STARFACE Desktop App auf STARFACE NEON oder das Adressbuch).

Alle Cloudinstanzen, die nach dem 01.06.2018 erstellt worden sind, verfügen über ein offizielles Zertifikat.



Hinweis: Eine Anpassung des Webserver auf den Cloudinstanzen der Firma Starface ist möglich, es sollen aber keine eigenen Zertifikate eingespielt werden!

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



Hinweis: Bei Cloudinstanzen ohne dedizierte IPv4-Adresse darf der Port für HTTPS (443) nicht geändert werden.

HTTP-Dienst

☒ Aktiv

Port:

HTTPS-Dienst

☒ Aktiv

Port:

☐ Umleitung auf HTTPS erzwingen

Gültige Zertifikate

Schlüssel	Wert
Valid	false
Issuer	CN=localhost,OU=IT,O=empty,L=empty,ST=empty,C=DE
Issued to	CN=localhost,OU=IT,O=empty,L=empty,ST=empty,C=DE
Not before	Jun 1, 2015
Not after	May 31, 2017
Serial number	556c4246
Sig. alg.	SHA1withRSA

Certificate Response importieren

Certificate Request

Neues Zertifikat

Sollte das provisorische Zertifikat abgelaufen sein, kann es neu erstellt werden über die Schaltfläche **Neues Zertifikat**. Dabei öffnet sich die folgende Eingabemaske:

Neues Zertifikat erstellen

Servername:*

SAN:*

Organisationseinheit:

Organisation:

Stadt:

Bundesland:

Ländercode:

Gültigkeitstage:*

Speichern

Abbrechen

In dieser Maske sind folgende 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. Es sind auch die Anforderungen und die Bedingungen der jeweiligen Zertifizierungsstellen für diesen Prozess zu berücksichtigen.



Hinweis: Bitte beachten Sie, dass über die Weboberfläche keine Private Keys importiert werden können.

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 dem folgenden X.509 Format 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.

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. Werden diese Standardports verändert hat dies weitreichende Auswirkungen und muss auch bei Firewallfreigaben beachtet werden (z.B. Zugriff der STARFACE Desktop App auf STARFACE NEON oder das Adressbuch).

Alle Cloudinstanzen, die nach dem 01.06.2018 erstellt worden sind, verfügen über ein offizielles Zertifikat.



Hinweis: Eine Anpassung des Webserver auf den Cloudinstanzen der Firma Starface ist möglich, es sollen aber keine eigenen Zertifikate eingespielt werden!

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



Hinweis: Bei Cloudinstanzen ohne dedizierte IPv4-Adresse darf der Port für HTTPS (443) nicht geändert werden.

HTTP-Dienst

☒ Aktiv
 Port:

HTTPS-Dienst

☒ Aktiv
 Port:

☐ Umleitung auf HTTPS erzwingen

Gültige Zertifikate

Schlüssel	Wert
Valid	false
Issuer	CN=localhost,OU=IT,O=empty,L=empty,ST=empty,C=DE
Issued to	CN=localhost,OU=IT,O=empty,L=empty,ST=empty,C=DE
Not before	Jun 1, 2015
Not after	May 31, 2017
Serial number	556c4246
Sig. alg.	SHA1withRSA

Certificate Response importieren

Certificate Request

Neues Zertifikat

Sollte das provisorische Zertifikat abgelaufen sein, kann es neu erstellt werden über die Schaltfläche **Neues Zertifikat**. Dabei öffnet sich die folgende Eingabemaske:

Neues Zertifikat erstellen

Servername:*

SAN:*

Organisationseinheit:

Organisation:

Stadt:

Bundesland:

Ländercode:

Gültigkeitstage:*

Speichern

Abbrechen

In dieser Maske sind folgende 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. Es sind auch die Anforderungen und die Bedingungen der jeweiligen Zertifizierungsstellen für diesen Prozess zu berücksichtigen.



Hinweis: Bitte beachten Sie, dass über die Weboberfläche keine Private Keys importiert werden können.

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 dem folgenden X.509 Format 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.

Die Dokumentation für die abgekündigten Versionen der STARFACE finden sich in unserem Archiv:

[Link zum Archiv](#)