

Bechtle-Zertifikat bei Hetzner installieren

Das Bechtle-Zertifikat für Veranstaltungsdomains erneuern: PFX vorbereiten, Schlüssel und Zertifikate prüfen, in Hetzner konsolEH importieren und je Domain aktivieren.

- [Schritt 1: Grundlage](#)
- [Schritt 2: Zertifikate extrahieren](#)
- [Schritt 3: Zertifikat bei Hetzner einrichten und freigeben.](#)

Schritt 1: Grundlage

Worum es geht

Diese Anleitung beschreibt, wie Sie das von Bechtle bereitgestellte TLS-/SSL-Zertifikat für die Veranstaltungsdomains in **Hetzner konsoleH** erneuern. Sie bereiten die Dateien vor, importieren das Zertifikat und aktivieren es anschließend für die betroffenen Domains.

Der Ablauf besteht aus drei Schritten:

1. **Unterlagen und Ziel-Domains prüfen** – diese Seite.
2. [Privaten Schlüssel und Zertifikate extrahieren und prüfen.](#)
3. [Zertifikat bei Hetzner importieren, aktivieren und kontrollieren.](#)

Was Sie benötigen

Im bisherigen Bechtle-Ablauf werden zwei getrennte E-Mails bereitgestellt:

- Eine E-Mail enthält das ZIP-Archiv mit dem Zertifikat.
- Die zweite E-Mail enthält das Passwort. Bisher wurde dasselbe Passwort zum Entpacken des Archivs und zum Öffnen der darin enthaltenen PFX-Datei verwendet. Maßgeblich sind die Angaben zur aktuellen Lieferung.

Zusätzlich benötigen Sie:

- Zugang zum betreffenden Hostingaccount in **konsoleH** mit Berechtigung zur Zertifikatsverwaltung.
- Einen lokalen Rechner mit Terminal, **OpenSSL 3 oder neuer** und einem Texteditor für reine Textdateien.
- Eine Liste der Domains und Subdomains, deren Zertifikat ersetzt werden soll.
- Eine geeignete Domain für den ersten Test, möglichst ohne laufende Online-Registrierung.

Planen Sie die Erneuerung anhand des tatsächlichen Ablaufdatums. Verlassen Sie sich nicht auf einen festen jährlichen Liefertermin.

Dateien vorbereiten

1. Prüfen Sie, ob beide E-Mails zur aktuellen Zertifikatslieferung gehören.
2. Speichern Sie das ZIP-Archiv in einem geschützten lokalen Arbeitsordner außerhalb des Webverzeichnisses und des Projekt-Repositories.
3. Entpacken Sie das Archiv mit dem mitgeteilten Passwort.
4. Prüfen Sie, ob die `.pfx`-**Datei** vorhanden ist. Dieses Dateiformat kann den privaten Schlüssel, das Domainzertifikat und die Zertifikatskette zusammen enthalten.
5. Notieren Sie den tatsächlichen Dateinamen. In den folgenden Beispielen heißt die Datei `bechtle.pfx`.

Die PFX-Datei und das Passwort werden für Schritt 2 benötigt. Bewahren Sie die Originaldatei bis zum erfolgreichen Abschluss geschützt auf.

Ziel und bisherige Zuordnung festhalten

Im bisherigen Ablauf wird in konsoleH das Produkt `dedivirt2627.your-server.de` und darin `bechtle-events.com` verwendet. Prüfen Sie vor jeder Erneuerung, ob diese Zuordnung noch aktuell ist.

Notieren Sie für jede betroffene Domain das bisher zugeordnete Zertifikat und dessen Ablaufdatum. So können Sie bei Problemen auf die vorherige Zuordnung zurückgehen, sofern das alte Zertifikat noch gültig und nicht widerrufen ist.

Das Wildcard-Zertifikat `*.bechtle-events.com` deckt beispielsweise `anmeldung.bechtle-events.com` ab. Die Hauptdomain `bechtle-events.com` oder eine weitere Ebene wie `anmeldung.test.bechtle-events.com` ist dadurch allein nicht abgedeckt. Prüfen Sie die tatsächlich enthaltenen Domainnamen in Schritt 2.

Umgang mit dem privaten Schlüssel

Der private Schlüssel ermöglicht die Nutzung des Zertifikats und muss vertraulich bleiben. Verwenden Sie zum Extrahieren lokale Werkzeuge. Die PFX-Datei, das Passwort und den privaten Schlüssel nicht in Online-Konverter, Tickets, Chats oder diese Dokumentation kopieren.

Ergebnis dieses Schritts: Die aktuelle PFX-Datei, das zugehörige Passwort und die Liste der zu aktualisierenden Domains liegen vor.

Weiter: [Schritt 2: Zertifikate extrahieren.](#)

Schritt 2: Zertifikate extrahieren

Worum es geht

Sie zerlegen die PFX-Datei in drei PEM-Dateien. Dadurch lassen sich Schlüssel, Domainzertifikat und Zertifikatskette beim Import eindeutig zuordnen.

Terminal vorbereiten

Öffnen Sie das Terminal im Arbeitsordner mit der PFX-Datei und prüfen Sie die Version:

```
openssl version
```

Die folgenden Befehle setzen **OpenSSL 3 oder neuer** voraus. Wenn stattdessen LibreSSL oder eine ältere OpenSSL-Version angezeigt wird, verwenden Sie für diesen Ablauf eine aktuelle OpenSSL-Installation.

Unter macOS und Linux beschränken Sie die Rechte neu erzeugter Dateien in dieser Terminal-Sitzung vorab:

```
umask 077
```

Unter Windows schützen Sie den Arbeitsordner über die Dateiberechtigungen Ihres Benutzerkontos.

Drei Dateien erzeugen

Ersetzen Sie `becht1e.pfx` durch den tatsächlichen Dateinamen. Lassen Sie die Anführungszeichen stehen, insbesondere bei Leerzeichen im Namen. Führen Sie jeden Befehl einzeln aus und fahren Sie nur fort, wenn keine Fehlermeldung erscheint.

1. Privaten Schlüssel extrahieren

```
openssl pkcs12 -in "bechtle.pfx" -nocerts -noenc -out priv-key.pem
```

2. Domainzertifikat extrahieren

```
openssl pkcs12 -in "bechtle.pfx" -clcerts -nokeys -out certificate.pem
```

3. Zertifikate der Zertifizierungsstellen extrahieren

```
openssl pkcs12 -in "bechtle.pfx" -cacerts -nokeys -out ca-certificates.pem
```

Geben Sie jeweils bei **Enter Import Password** das Passwort der PFX-Datei ein. Bei der Eingabe werden üblicherweise keine Zeichen angezeigt. Schreiben Sie das Passwort nicht direkt in den Befehl.

`-noenc` erzeugt einen **unverschlüsselten privaten Schlüssel**, wie ihn der Hetzner-Import benötigt. Die bisherige Option `-nodes` ist in OpenSSL 3 veraltet. Die PEM-Datei muss deshalb besonders geschützt bleiben. Die Trennung nach Schlüssel, Domain- und CA-Zertifikaten folgt den [OpenSSL-PKCS#12-Optionen](#).

Datei	Inhalt	Späteres Zielfeld
priv-key.pem	Privater Schlüssel	Privater Schlüssel / Schlüsselblock
certificate.pem	Domainzertifikat	Öffentlicher Schlüssel / Zertifikatsblock
ca-certificates.pem	Mitgelieferte CA-Zertifikate	Zwischenzertifikate / CA Blöcke

Domain und Gültigkeit prüfen

Zeigen Sie die Zertifikatsdaten an:

```
openssl x509 -in certificate.pem -noout -subject -issuer -dates -ext subjectAltName
```

Prüfen Sie die enthaltenen Domainnamen unter **Subject Alternative Name** sowie **notBefore** und **notAfter**. Das Zertifikat muss bereits gültig sein und das erwartete neue Ablaufdatum besitzen. Angaben zu Organisation oder Aussteller können sich gegenüber der vorherigen Lieferung ändern.

Prüfen Sie anschließend jeden vorgesehenen Hostnamen, beispielsweise:

```
openssl x509 -in certificate.pem -noout -checkhost anmeldung.bechtle-events.com
```

Ersetzen Sie den Beispielnamen durch die tatsächliche Domain. Das Ergebnis muss bestätigen, dass der Name passt. Diese Prüfung kontrolliert die Namensabdeckung, nicht die vollständige Vertrauenskette. Die Optionen sind in der [OpenSSL-x509-Dokumentation](#) beschrieben.

Gehören Schlüssel und Zertifikat zusammen?

Erzeugen Sie aus beiden Dateien jeweils den öffentlichen Schlüssel:

```
openssl pkey -in priv-key.pem -pubout -out key-public.pem  
openssl x509 -in certificate.pem -pubkey -noout -out cert-public.pem
```

Beide Befehle müssen ohne Fehler enden. Vergleichen Sie anschließend die Prüfsummen:

```
openssl dgst -sha256 key-public.pem cert-public.pem
```

Die beiden Hashwerte müssen **identisch** sein; die angezeigten Dateinamen unterscheiden sich. Bei Abweichungen nicht importieren, sondern prüfen, ob Dateien aus verschiedenen Lieferungen vermischt wurden. `-pubout` gibt nur den öffentlichen Anteil aus; siehe [OpenSSL pkey](#).

Zertifikatskette kontrollieren

Öffnen Sie `certificate.pem` und `ca-certificates.pem` in einem lokalen Texteditor. Das Domainzertifikat sollte als ein einzelner Zertifikatsblock vorliegen. In der CA-Datei können mehrere Blöcke stehen.

Wenn die CA-Datei leer ist, fehlen im PFX möglicherweise die Zwischenzertifikate. Fordern Sie die passende Kette bei der zuständigen Zertifikatsbetreuung an. Verwenden Sie nicht ungeprüft die Kette einer alten Lieferung. Bei mehreren Domainzertifikaten lassen Sie vor dem Import klären,

welches zum geprüften Schlüssel gehört.

Häufige Fehler

Meldung oder Problem	Nächster Schritt
Datei nicht gefunden	Arbeitsordner, Dateiname und Anführungszeichen prüfen.
<code>Mac verify error</code> / ungültiges Passwort	Passwort der aktuellen PFX-Lieferung prüfen; gegebenenfalls Datei erneut aus dem Originalarchiv entpacken.
<code>unsupported</code> mit Hinweis auf <code>RC2-40-CBC</code>	Bei einer älteren PFX-Verschlüsselung kann OpenSSL 3 die zusätzliche Option <code>-legacy</code> zum Lesen benötigen. Den betroffenen <code>openssl pkcs12</code> -Befehl mit dieser Option wiederholen.
<code>-noenc</code> wird nicht erkannt	Mit <code>openssl version</code> prüfen, ob tatsächlich OpenSSL 3 oder neuer verwendet wird.
Domainprüfung schlägt fehl	Hostnamen und aktuelle Zertifikatslieferung abgleichen; nicht für diese Domain aktivieren.
Unterschiedliche Hashwerte	Schlüssel und Zertifikat stammen nicht aus einem passenden Paar; Dateien erneut zuordnen.

Beispiel für das Lesen einer älteren PFX-Datei:

```
openssl pkcs12 -legacy -in "bechtle.pfx" -nocerts -noenc -out priv-key.pem
```

Nutzen Sie `-legacy` nur bei entsprechendem Lesefehler; die [OpenSSL-Dokumentation](#) beschreibt diesen Fall ausdrücklich.

Ergebnis dieses Schritts: Schlüssel und Zertifikat passen zusammen, die vorgesehenen Domainnamen und Gültigkeitsdaten sind geprüft, die CA-Zertifikate liegen vor.

Weiter: [Schritt 3: Bei Hetzner einrichten und freigeben.](#)

Zurück: [Schritt 1: Grundlage.](#)

Schritt 3: Zertifikat bei Hetzner einrichten und freigeben.

Worum es geht

Sie importieren die vorbereiteten PEM-Inhalte in **konsoleH**. Anschließend aktivieren Sie das Zertifikat zuerst für eine Testdomain und nach erfolgreicher Kontrolle für die weiteren vorgesehenen Domains. **Ein erfolgreicher Import allein schließt die Umstellung noch nicht ab.**

Import öffnen

1. Melden Sie sich bei Hetzner **konsoleH** an.
2. Wählen Sie den zuständigen Hostingaccount und darin **bechtle-events.com**. Gleichen Sie die Zuordnung mit [Schritt 1](#) ab.
3. Öffnen Sie links **Einstellungen** → **SSL Manager**.
4. Klicken Sie auf **Neues Zertifikat** und wählen Sie den Import eines bestehenden Zertifikats. In der bisherigen Oberfläche heißt der Weg **Existierendes Zertifikat** → **Hinzufügen**; die aktuelle Hetzner-Dokumentation nennt **Zertifikat importieren**.

Die drei Felder richtig befüllen

Öffnen Sie die vorbereiteten Dateien in einem lokalen Texteditor und übernehmen Sie nur die vollständigen PEM-Blöcke einschließlich ihrer Anfangs- und Endzeilen. Zusätze wie `Bag Attributes`, `localKeyID`, `friendlyName`, `subject=` und `issuer=` gehören nicht in die Formularfelder.

Feld in der bisherigen Oberfläche	Bezeichnung in der Hetzner-Dokumentation	Inhalt
Privater Schlüssel	Schlüsselblock	Schlüsselblock aus <code>priv-key.pem</code>

Feld in der bisherigen Oberfläche	Bezeichnung in der Hetzner-Dokumentation	Inhalt
Öffentlicher Schlüssel	Zertifikatsblock	Domainzertifikat aus <code>certificate.pem</code>
Zwischenzertifikate	CA Blöcke	CA-Zertifikatsblöcke aus <code>ca-certificates.pem</code>

Privater Schlüssel

Der Schlüssel aus dem beschriebenen Export beginnt und endet normalerweise so:

```
-----BEGIN PRIVATE KEY-----
[Schlüsselinhalt aus priv-key.pem]
-----END PRIVATE KEY-----
```

Bei anderen Schlüsselformaten können die Begrenzungen `BEGIN RSA PRIVATE KEY` oder `BEGIN EC PRIVATE KEY` lauten. Übernehmen Sie die vorhandenen Begrenzungen unverändert. Ein Block mit `BEGIN ENCRYPTED PRIVATE KEY` ist für diesen Import noch verschlüsselt.

Wichtig: In dieses Feld gehört kein `BEGIN CERTIFICATE`-Block. Die frühere Anleitung nannte hier versehentlich die Begrenzung eines Zertifikats.

Domainzertifikat

In **Öffentlicher Schlüssel / Zertifikatsblock** gehört das vollständige Zertifikat:

```
-----BEGIN CERTIFICATE-----
[Zertifikatsinhalt aus certificate.pem]
-----END CERTIFICATE-----
```

Die Bezeichnung „Öffentlicher Schlüssel“ meint hier das Domainzertifikat. Verwenden Sie nicht die in Schritt 2 zur Prüfung erzeugte Datei `cert-public.pem` mit einem `BEGIN PUBLIC KEY`-Block.

CA-Zertifikate

Übernehmen Sie die zur Lieferung gehörenden CA-Blöcke vollständig und untereinander. Beginnen Sie mit dem Zwischenzertifikat, das das Domainzertifikat ausgestellt hat, und folgen Sie der Kette zu den übergeordneten Zertifizierungsstellen. Die Zuordnung erfolgt über Aussteller und Inhaber der Zertifikate, nicht allein über deren Position in der Datei.

Hetzner nennt für **CA Blöcke** ausdrücklich Intermediate- und Root-Zertifikate. Übernehmen Sie eine mitgelieferte passende Root-CA daher ebenfalls entsprechend dieser Importvorgabe. Das

Domainzertifikat selbst gehört ausschließlich in das separate Zertifikatsfeld. Bei unklarer Kette vor dem Import die Zertifikatsbetreuung hinzuziehen.

Klicken Sie anschließend auf **Zertifikat importieren** und kontrollieren Sie die Erfolgsmeldung sowie den neuen Listeneintrag. Die PEM-Anforderungen und aktuellen Feldbezeichnungen stehen in [Hetzner: SSL-Zertifikate](#).

Zuerst eine Domain umstellen

1. Kehren Sie zur Übersicht des **SSL Managers** zurück.
2. Suchen Sie die vorgesehene Testdomain, möglichst ohne laufende Online-Registrierung.
3. Notieren Sie die bisherige Zertifikatszuordnung, falls noch nicht geschehen.
4. Wählen Sie in dieser Domainzeile das neu importierte Zertifikat aus. Achten Sie auf den Zertifikatsnamen und das **neue Ablaufdatum**.
5. Klicken Sie auf das **Aktualisieren-Symbol mit den runden Pfeilen** am Ende der Zeile.
6. Prüfen Sie die Erfolgsmeldung beziehungsweise Statusanzeige.

Die Auswahl und anschließende Aktualisierung aktivieren das Zertifikat für diesen SSL-Account. Siehe [Hetzner: SSL-Guide](#).

Tatsächlich ausgeliefertes Zertifikat prüfen

Öffnen Sie die umgestellte Domain mit `https://` in einer neuen Browser-Verbindung. Prüfen Sie:

- Die Seite öffnet sich ohne Zertifikatswarnung.
- Die Zertifikatsanzeige des Browsers zeigt das erwartete neue Ablaufdatum und den passenden Domainnamen.
- Die Veranstaltungsseite und das benötigte Formular werden korrekt geladen.

Kontrollieren Sie zusätzlich die Zertifikatskette mit dem im bisherigen Ablauf verwendeten [SSL-Check](#). Geben Sie dort ausschließlich den öffentlichen Domainnamen ein. Prüfen Sie Domainabdeckung, Gültigkeit und vollständige Vertrauenskette; vergleichen Sie das angezeigte Ablaufdatum mit der aktuellen Lieferung. Laden Sie keine PFX-Datei und keinen privaten Schlüssel hoch.

Wenn die Domain hinter einem Proxy oder CDN liegt, kann der Browser dessen Zertifikat statt des Zertifikats bei Hetzner anzeigen. Lassen Sie in diesem Fall zusätzlich das Zertifikat am

tatsächlichen Hetzner-Ziel prüfen.

Weitere Domains aktivieren

Erst nach erfolgreicher Kontrolle stellen Sie die weiteren vorgesehenen Domains einzeln um:

1. Domain aus der vorbereiteten Liste auswählen.
2. Neues Zertifikat zuordnen und die Änderung über das Aktualisieren-Symbol anwenden.
3. Domain per HTTPS prüfen und das neue Ablaufdatum bestätigen.
4. Ergebnis in Ihrer Liste vermerken.

Ein Wildcard-Zertifikat erspart diese Zuordnung nicht. Prüfen Sie auch, ob alle umzustellenden Namen tatsächlich vom Zertifikat abgedeckt sind.

Fehler erkennen und beheben

Problem	Was Sie prüfen sollten
Import wird abgelehnt	PEM-Begrenzungen vollständig, Felder richtig zugeordnet, Schlüssel unverschlüsselt und Schlüsselvergleich aus Schritt 2 erfolgreich?
Zertifikat importiert, aber weiterhin altes Ablaufdatum sichtbar	Für die konkrete Domain ausgewählt und Aktualisieren-Symbol betätigt? Neue Verbindung herstellen und gegebenenfalls Proxy/CDN berücksichtigen.
Browser meldet unpassenden Domainnamen	Tatsächliche Domain gegen die Zertifikatsnamen prüfen. Hauptdomain und mehrstufige Subdomains sind nicht automatisch vom Wildcard-Eintrag abgedeckt.
Browser oder SSL-Check meldet eine unvollständige Kette	Passende Zwischenzertifikate und vollständige PEM-Blöcke prüfen. Keine Kette aus einer anderen Lieferung verwenden.
Zertifikat noch nicht oder nicht mehr gültig	<code>notBefore</code> , <code>notAfter</code> , aktuelle Lieferung und Systemzeit prüfen.
Nach der Umstellung treten TLS-Probleme auf	Weitere Domains vorerst nicht umstellen. Für die betroffene Domain gegebenenfalls das zuvor dokumentierte, weiterhin gültige und nicht widerrufen Zertifikat erneut zuordnen und aktivieren. Danach HTTPS prüfen.

Abschluss

- Alle vorgesehenen Domains liefern das neue Zertifikat aus.
- HTTPS und die benötigten Veranstaltungsseiten funktionieren.
- Neues Ablaufdatum und erfolgte Umstellung sind dokumentiert; die nächste Erneuerung ist eingeplant.
- Die Original-PFX-Datei ist nach der internen Ablageregeln geschützt archiviert. Temporäre unverschlüsselte Schlüsselkopien werden nach erfolgreichem Abschluss aus dem Arbeitsordner entfernt; die Zwischenablage wird geleert.

Das alte Zertifikat erst aus der Verwaltung entfernen, wenn keine Domain es mehr benötigt und die Umstellung abgeschlossen ist.

Zurück: [Schritt 2: Zertifikate extrahieren.](#)

Zum Einstieg: [Schritt 1: Grundlage.](#)

Dokumentationsabgleich mit Hetzner und OpenSSL: 18.09.2026. Kontospezifische Produktnamen und Oberflächenbezeichnungen stammen aus dem bisherigen Ablauf und sind vor der Durchführung zu prüfen.