INHALTSVERZEICHNIS

1 Einführung Zertifikat 1

2 Verlängerung des SSL-Zertifikats 2

3 Fazit 6

1 EINFÜHRUNG ZERTIFIKAT

Was ist ein Zertifikat

Beim einem Zertifikat handelt es sich um ein digitales Schlüsselpaar für eine sogenannte asymmetrische Verschlüsselung. Im Gegensatz zur symmetrischen Verschlüsselung wird bei der asymmetrischen Verschlüsselung das Zertifikat mit seinen beiden Schlüsseln benötigt. Dabei ist der ein Schlüssel für die Verschlüsselung zuständig und muss öffentlich zugänglich sein (Public-Key). Die zu schützenden Daten werden mit einem speziellen Verschlüsselungsverfahren und diesem Public-Key verschlüsselt. Nur mit dem zweiten Schlüssel des Schlüsselpaars lassen sich die Daten wieder entschlüsseln. Dieser zweite Schlüssel muss geheim bleiben (Private-Key).
In vielen Anwendungsgebieten wird die asymmetrische Verschlüsselung verwendet, ohne dass der Anwender dies mitbekommt und mit dem Schlüsselpaar (Zertifikat) hantieren muss.

Wofür wird ein Zertifikat benötigt

In der Zwischenzeit werden digitale Zertifikate in einer Vielzahl von Anwendungsbereichen eingesetzt. In der Regel handelt es sich dabei um den Schutz von Daten und die Glaubwürdigkeit von Angaben.

- **Signatur**: Durch die Signatur wird die Echtheit und Unverfälschtheit von Daten garantiert. Zertifikate zur Signatur werden beispielsweise bei folgenden Anwendungen Verwendet:
  - Geschäftlichen Dokumenten
  - E-Mail-Kommunikation
  - Softwareprogrammen
- **Verschlüsselung**: Der Vorteil von Zertifikaten wird in der heutigen Zeit häufig beim Schutz von Daten durch die asymmetrische Verschlüsselung verwendet. Als Beispiele zur Verschlüsselung mit öffentlichen und privaten Schlüssel gegen unerlaubten Zugriff gelten:
  - Netzwerkkommunikation: IPsec
  - Verschlüsselung im Internet: SSL (HTTPs)
  - Virtual Private Netzwerk: VPN
  - Email-Verschlüsselung: PGP, S/MIME
  - Datei-Verschlüsselung: z. B. abylon BASIC oder abylon CRYPTDRIVE
  - Messenger: Signal, WhatsApp und viele mehr
  - Und vieles mehr…

Welche Vorteile hat eine SSL-Verschlüsselung

© Blueflexx -Webdesign (www.blueflexx.com) – Ohne Befugnis durch den Autor ist die Vervielfältigung, Verwendung oder Weitergabe dieses Dokuments und dessen Inhaltes nicht gestattet!

Bei der Verschlüsselung von Webseiten wird der Inhalt der Internetseite auf dem Server verschlüsselt und erst auf dem Computer oder Handy wieder entschlüsselt. Die Verschlüsselung verhindert beispielsweise, dass der Internetanbieter (ISP, z. B. Telekom) oder sonstige Parteien mitbekommen, welchen Inhalt die besuchten Seiten haben. Dies hat auch den Vorteil, dass beispielsweise persönliche Daten aus einem Kontaktformular nicht in die falschen Hände gelangen. Eine Verschlüsselung wird im Browser durch HTTPs angezeigt.

Weiter Informationen zu Zertifikaten (extern)

Bei den folgenden Links handelt es sich um Informationen rund um das Thema Zertifikat und Verschlüsselung. Die Liste ist nur eine Auswahl, ohne Anspruch auf Vollständigkeit.

- Kostenlose Zertifikate zur SSL-Verschlüsselung: Lets Encrypt (https://letsencrypt.org/)
- Wizard zur Verwendung und Verlängerung von kostenlosen Zertifikaten: Zero SSL (https://zerossl.com)
- Tool zum Erstellen von selbstsignierten Zertifikaten: abylon SELFCERT (https://www.abylonsoft.de/selfcert/index.htm)
- Allgemeine Informationen zu Zertifikaten: LogoSec (https://www.logosec.de/certificates.html)
- Installation eines Zertifikats in der Windows Zertifikatsdatenbank: Withepaper von abylonsoft (https://www.abylonsoft.de/tutorial/installation-eines-zertifikates-in-der-windows-zertifikatsdatenbank.htm)

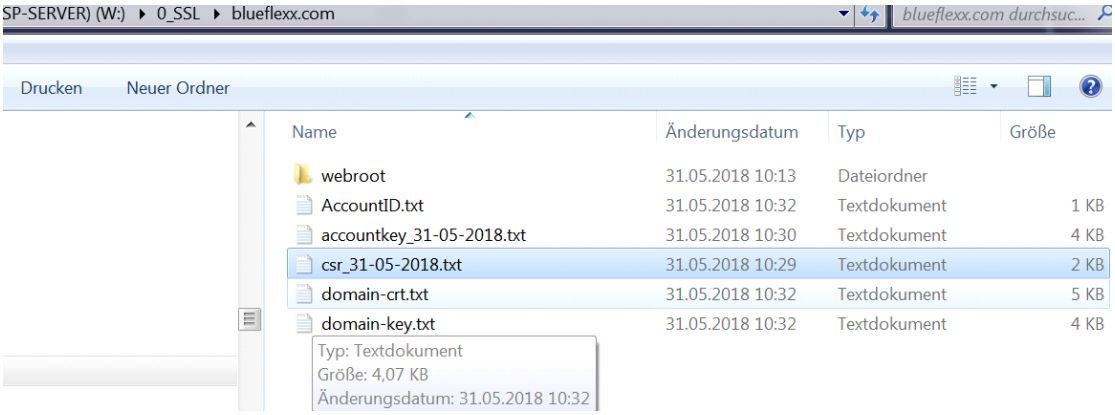
2 VERLÄNGERUNG DES SSL-ZERTIFIKATS

Die Verschlüsselung von Webseiten dient zum Schutz der übertragenden Daten und dem Anbieter für ein höherwertiges Such-Ranking bei Suchmaschinen (z. B. Google). Leider bieten manche Internet-Provider nur die Verwendung von kostenpflichtigen SSL-Zertifikaten an. Unser Provider Hosteurope ermöglicht die Verwendung von kostenlosen Lets Encrypt Zertifikaten. Da diese jedoch nur eine Gültigkeit von 3 Monaten besitzen, müssen diese regelmäßig manuell erneuert werden. Im Folgenden finden Sie unsere Anleitung dazu:

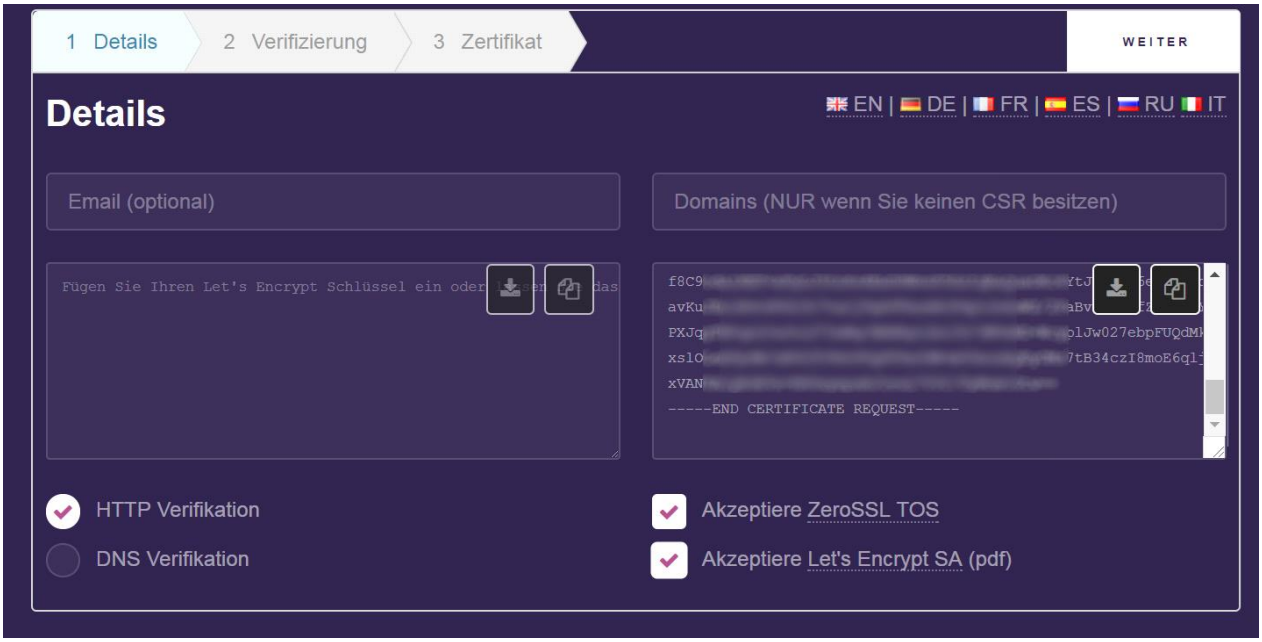
Anleitung zum Update des SSL-Zertifikats bei Hosteurope:

1. Die Seite von SeroSSL wird im Browser geöffnet (https://zerossl.com/free-ssl/#crt)
2. Die vorhandene CSR-Datei öffnen und den Inhalt in die Zwischenablage kopieren.

© Blueflexx -Webdesign (www.blueflexx.com) – Ohne Befugnis durch den Autor ist die Vervielfältigung, Verwendung oder Weitergabe dieses Dokuments und dessen Inhaltes nicht gestattet!

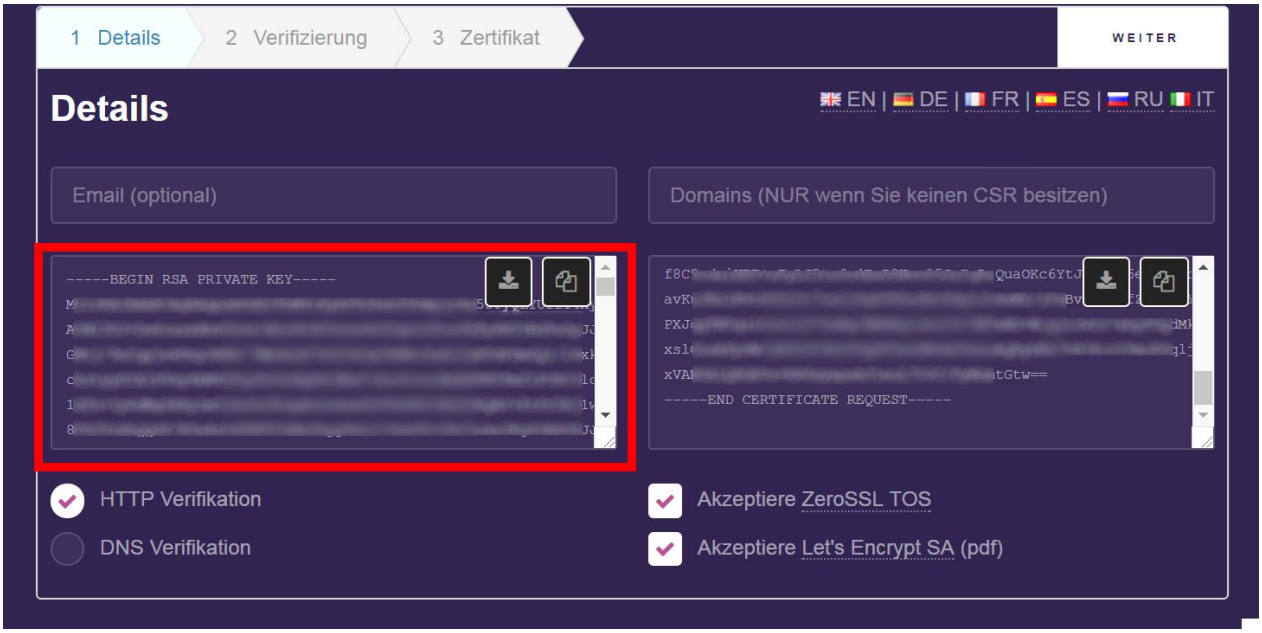


3. Den Inhalt aus der Zwischenanlage in das rechte Feld kopieren und oben rechts auf weiter klicken.



4. Dabei wird der Account-Key erstellt und links angezeigt.

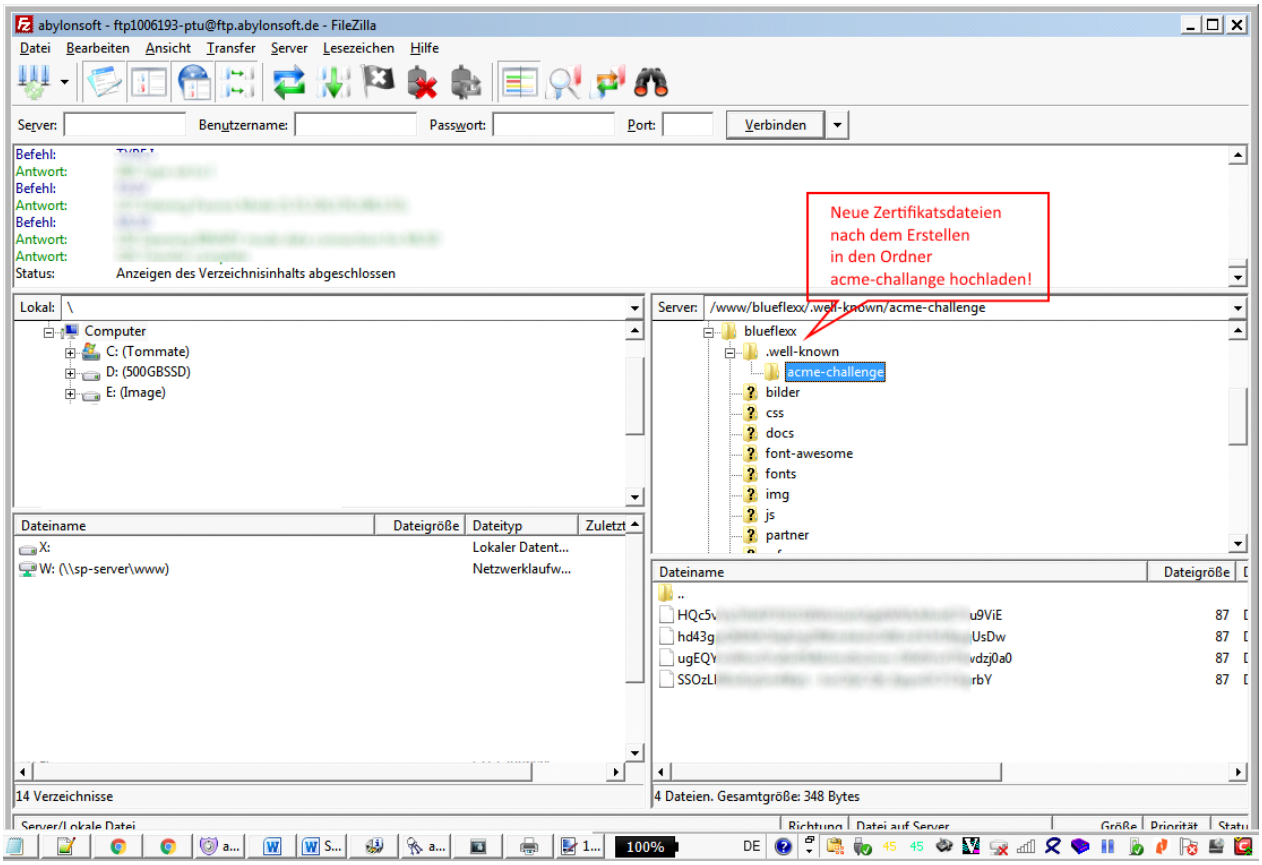
© Blueflexx -Webdesign (www.blueflexx.com) – Ohne Befugnis durch den Autor ist die Vervielfältigung, Verwendung oder Weitergabe dieses Dokuments und dessen Inhaltes nicht gestattet!



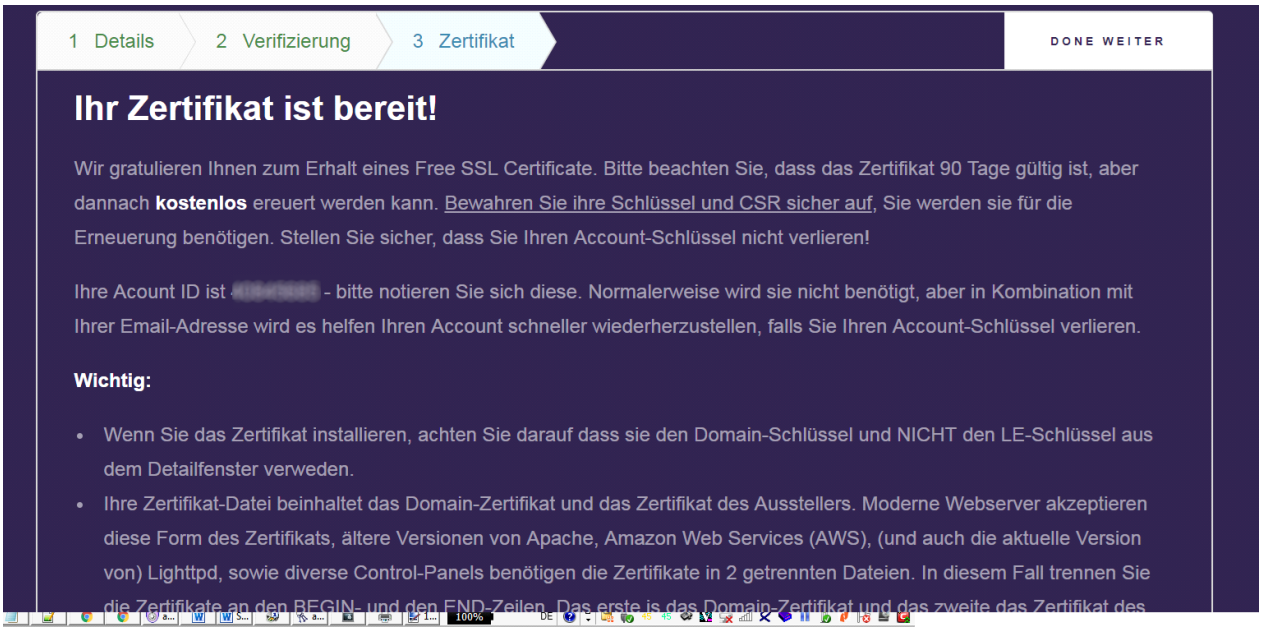
5. Die zwei Dateien herunterladen.

6. Vor dem fortfahren die beiden Dateien per FTP ins WEBROOT der Domain hochladen. Dabei die alten Dateien NICHT löschen.

© Blueflexx -Webdesign (www.blueflexx.com) – Ohne Befugnis durch den Autor ist die Vervielfältigung, Verwendung oder Weitergabe dieses Dokuments und dessen Inhaltes nicht gestattet!

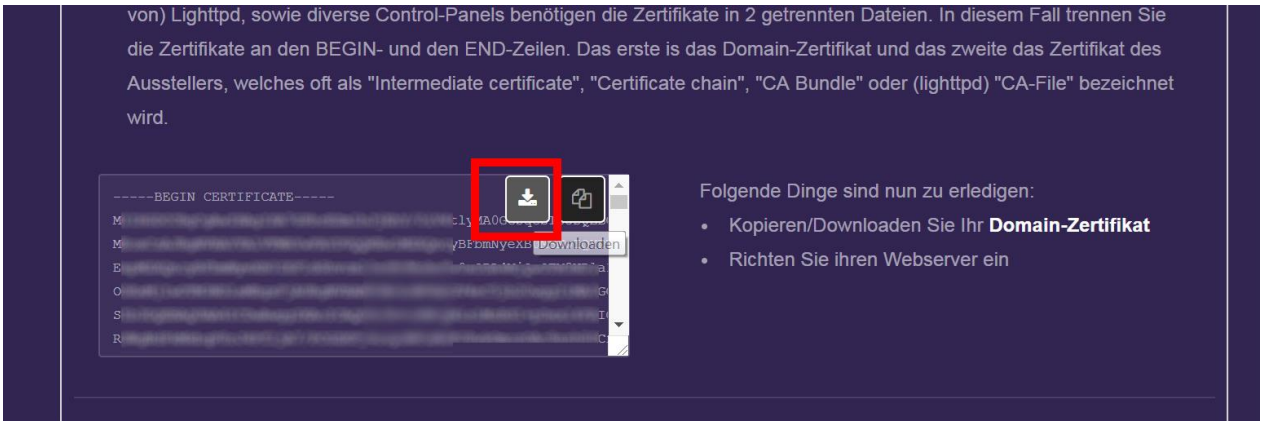


7. Bei ZeroSSL auf weiter klicken. Dabei werden die beiden hochgeladenen Dateien verifiziert und das Zertifikat erstellt.

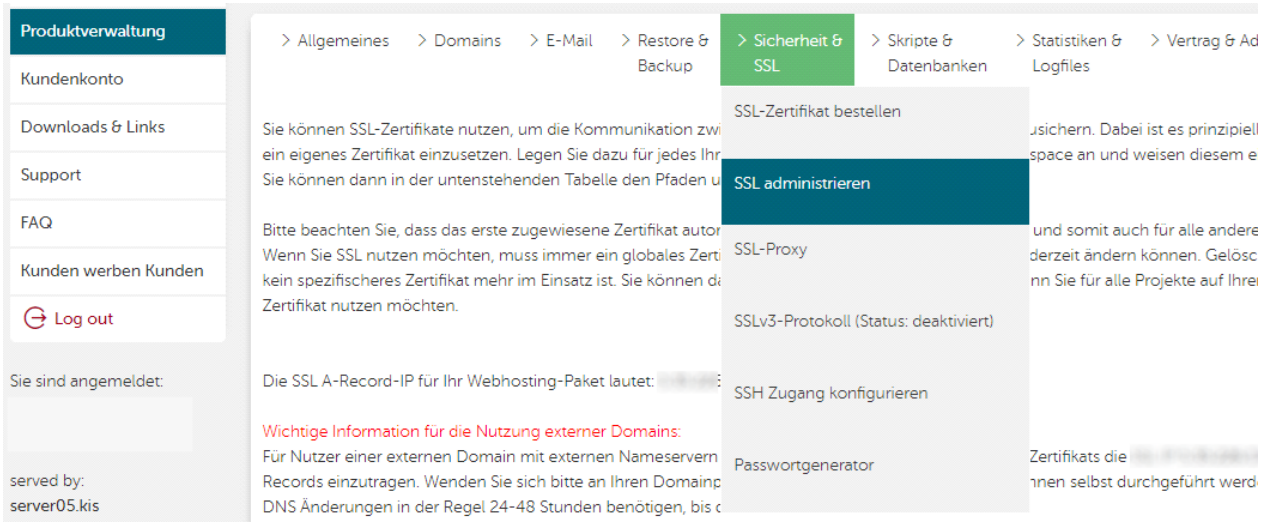


8. Das erstellte Zertifikat (domain-crt.txt) kann nun heruntergeladen werden.

© Blueflexx -Webdesign (www.blueflexx.com) – Ohne Befugnis durch den Autor ist die Vervielfältigung, Verwendung oder Weitergabe dieses Dokuments und dessen Inhaltes nicht gestattet!



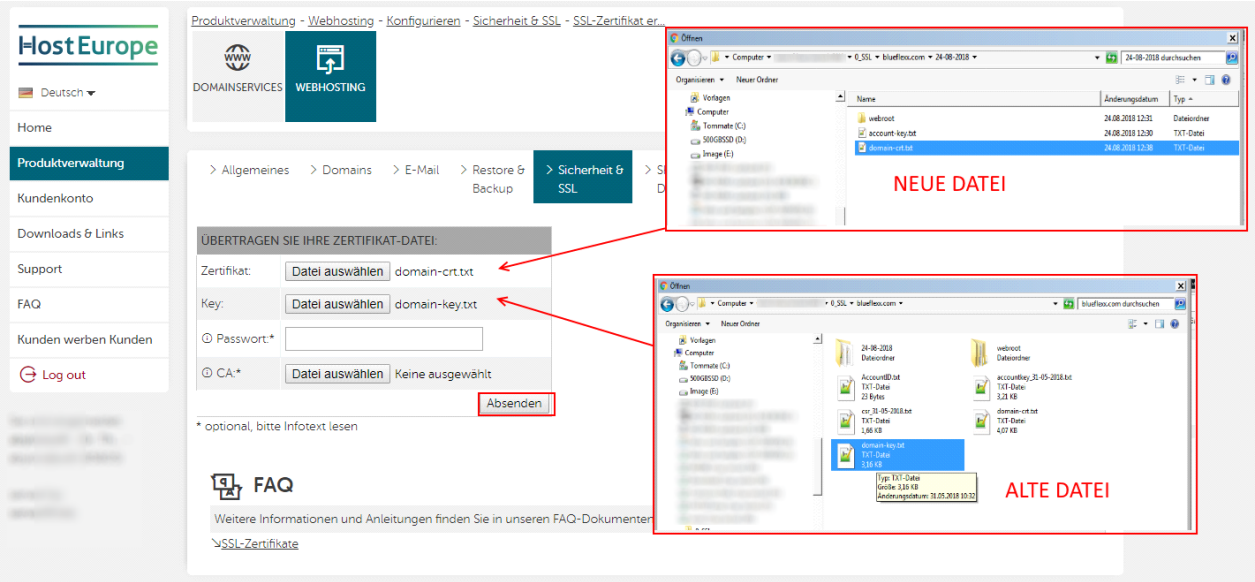
9. Melden Sie sich bei Hosteurope an und wechseln auf die Seite „Sicherheit & SSL -> SSL administrieren“.



10. Wählen Sie bei der entsprechenden Domain den Schalter „Ersetzen“.

11. Zum Schluss muss noch das neue Zertifikat und der Key hochgeladen und über den Schalter „Absenden“ eingetragen werden. ACHTUNG: Als Keydatei wird jetzt bei Hosteurope NICHT die ACCOUNT-KEY.TXT-Datei, sondern die DOMAIN-KEY.TXT-Datei (besteht seit Einrichtung) hochgeladen.

© Blueflexx -Webdesign (www.blueflexx.com) – Ohne Befugnis durch den Autor ist die Vervielfältigung, Verwendung oder Weitergabe dieses Dokuments und dessen Inhaltes nicht gestattet!



12. Jetzt noch 48h warten und hoffen, dass es klappt :)

3 FAZIT

Die kostenlosen Zertifikate von Lets Encrypt sind ein tolles Angebot um den Besucher eine verschlüsselte Datenübertragung zu bieten und dabei noch die Datenschutzvorschriften der DSGVO zu erfüllen. Durch die kurze Gültigkeitsdauer ist jedoch mehrmals im Jahr eine manuelle Verlängerung erforderlich. Einige Internetprovider bieten schon eine automatische Verlängerung der Lets Encrypt Zertifikat an. Hosteurope gehört leider bisher (06.09.2018) noch NICHT dazu.

ÄNDERUNGSCHRONIK

Version	Datum	Autor	Kommentar
1.0	06.09.2018	Thomas Klabunde	Dokument mit allgemeinen Informationen zu Zertifikaten ergänzt
0.9	02.09.2018	Uwe Velten	Dokument neu erstellt

© Blueflexx -Webdesign (www.blueflexx.com) – Ohne Befugnis durch den Autor ist die Vervielfältigung, Verwendung oder Weitergabe dieses Dokuments und dessen Inhaltes nicht gestattet!