

CertesGUI 1.0

diub - Dipl.-Ing. Uwe Barth

18.05.2020

Inhaltsverzeichnis

1	Allgemeine Nutzungsbedingungen	2
2	Einleitung	3
3	Grundlagen	4
3.1	Hoster im Vergleich	4
3.2	Zertifikat und Berechtigung	4
3.3	Arbeitsschritte	5
3.4	Beispiel: HostEurope	6
4	Zertifikat anfordern und aktivieren	8
4.1	Einstellungen	8
4.2	Zertifikat abrufen	9
4.3	Zertifikat beim Hoster einrichten	10
5	Wichtige Hinweise	11
5.1	Kopierschutz	11

PRÄAMBEL

Hinweis: Dieses Dokument wurde mit *Documenter* erstellt und steht daher mit gleichem Inhalt als

- Webseite
- PDF-Datei
- Windows-Hilfe und
- ePub

zur Verfügung!

Documenter ist eine Entwicklung von diub zur Erstellung von Dokumentationen aus einer Quelle mit unterschiedlichen Zielformaten.

Empfohlene ePub-Reader

ePub-Reader gibt es massenhaft. Nur leider sind die meisten davon schlicht unbrauchbar; falsche Schriften, kaputte Formatierungen usw. sind die Tagesordnung. Am schlimmsten ist jedoch die Unfähigkeit zur Skalierung, für Normalanwender die Änderung der 'Schriftgröße'.

Nachstehend die von mir bevorzugten Reader mit korrekter Darstellung.

- **Browser**
Firefox → Addon EPUBReader (<https://addons.mozilla.org/de/firefox/addon/epubreader>)
- **Android**
GitdenReader (angenehm schlicht und einfach, positioniert Bilder und Tabellen immer links)
Bluefire Reader
- **Windows**
Digital Editions (Adobe), leider - wie alle anderen auch - keine Skalierung der Bilder

1 Allgemeine Nutzungsbedingungen

HAFTUNG

diub bemüht sich im Rahmen des Zumutbaren, richtige und vollständige Informationen zur Verfügung zu stellen. In diesem Sinne ist *diub* bemüht, nach bekannt werden von Fehlern diese zu beseitigen. Forderungen irgendwelcher Art an *diub* können daraus nicht abgeleitet werden.

diub behält sich das Recht vor, ohne vorherige oder nachherige Ankündigung Änderungen oder Ergänzungen an den bereitgestellten Informationen oder Programmen vorzunehmen.

diub haftet nicht für direkte oder indirekte Schäden, die aufgrund von oder sonst wie in Verbindung mit Informationen oder Programmen oder durch die Nutzung dieser Informationen oder Programme entstehen.

Alle Informationen oder Programme sind gemäß Ihrer Bestimmung zu gebrauchen. Unsachgemäßer Gebrauch schließt automatisch alle Forderungen gegenüber *diub* aus. Gleiches gilt für Folgen die durch Mängel, die durch eine Abänderung der Software, durch Beschädigung der Datenträger, durch Missbrauch oder zweckwidrige Nutzung entstehen. Ebenso ausgeschlossen sind Forderungen aus Schäden die durch eine Datensicherung (Backup) oder vergleichbare Maßnahmen vermeidbar sind.

LIZENZ

Eine Lizenz besteht aus der Überlassung eines Lizenz-Codes. Jedem Lizenz-Code ist eine bestimmte Anzahl von Aktivierungen zugeordnet. Die Aktivierung erfolgt Online. Die Software enthält Mechanismen zur Sicherstellung, das die vorgesehene Anzahl an Aktivierungen nicht überschritten wird (Kopierschutz).

RECHTE

Sie sind berechtigt, das Programm je erworbener einzelner Lizenz auf genau einem Rechner zu installieren und zu betreiben. Bei Installation auf einem Rechner mit Zugriffsmöglichkeiten über Netzwerk (zum Beispiel Server) ist je auf das Programm zugriffsberechtigtem Rechner oder je Rechner auf den zugegriffen wird eine Lizenz zu erwerben.

Kopien zum Zwecke der Sicherung und des Erhaltes für die Zukunft sind gestattet.

Sie sind nicht berechtigt, Kopien gegen Entgelt oder sonstige Gegenleistungen oder auch ohne Gegenleistung weiter zu vertreiben oder zu verbreiten.

BESCHRÄNKUNGEN

Es ist Ihnen untersagt, die Software zu dekompileieren, sie einer Rückentwicklung zu unterziehen, sie zu zerlegen oder die Software in anderer Form zu entschlüsseln.

Es ist Ihnen untersagt, die Software zu verkaufen, zu mieten, zu vermieten oder eine Unterlizenz dafür zu vergeben.

Sie dürfen die Software nicht abändern oder Derivate davon anfertigen.

UPDATES

Updates werden soweit möglich kostenfrei zur Verfügung gestellt.

Updates ersetzen die ursprüngliche Version. Updates sind keine neuen Lizenzen und unterliegen den gleichen Beschränkungen wie die erste von Ihnen erworbene Version.

2 Einleitung

CertesGUI ist

- eine einfache Möglichkeit *Let's Encrypt* Zertifikate mit Hostern zu nutzen, die *Let's Encrypt* nicht direkt unterstützen,
- eine Benutzeroberfläche für das Kommandozeilen-Programm *certes CLI* (wird mit installiert),
- kostenfrei für jeden (Freeware).

Damit steht der Nutzung von *Let's Encrypt* Zertifikaten zum Beispiel auch bei *Hosteurope* nichts mehr im Wege.

Fortgeschrittene und erfahrene Benutzer können gleich unter (4) *Zertifikat anfordern und aktivieren* (Seite 8) weiterlesen.

3 Grundlagen

Die Darstellung erfolgt hier am Beispiel von *Hosteurope*.

Hosteurope findet sich auf der *Let's Encrypt* Webseite in der Liste der nicht unterstützenden Hosters. Das bedeutet aber letztlich nur, dass *Hosteurope* keinen Automatismus für *Let's Encrypt* anbietet. Die von *Let's Encrypt* erzeugten Zertifikate lassen sich jedoch problemlos nutzen.

Schwierigkeiten bereitet daher nur die Erstellung der Zertifikate. Das hat mit *CertesGUI* auch für Windows-Anwender ein Ende.

3.1 Hoster im Vergleich

Heute, also am 18.05.2020, sieht es bei 3 bekannten Hostern für vergleichbare Leistungen so aus:

1 UND 1

Kosten: 8,- € / Monat.

Let's Encrypt: inklusive; es wird als kostenfrei beworben, aber alles ist relativ...

(nicht getestet)

HOSTEUROPE

Kosten: 5,- € / Monat.

Let's Encrypt: keine Automation

Integrierte gewerbliche Zertifikaterstellung: 3,-€ / Monat je Domäne.

- Bei nur einer Domäne macht das keinen Unterschied zu dem Angebot von 1&1.
- Bei weiteren Sub-Domänen wird es aber teuer.
- Mit *Let's Encrypt* via *CertesGUI/certes CLI* ist das Angebot aber besser als das von 1&1.

MANITU

Kosten: 2,50 € / Monat.

Let's Encrypt: inklusive.

(nicht getestet)

Das Preis/Leistung-Verhältnis ist einfach ungeschlagen.

3.2 Zertifikat und Berechtigung

Damit *Let's Encrypt* überhaupt ein Zertifikat ausstellen kann, muss *Let's Encrypt* vorher prüfen, ob die Anfrage rechters ist.

Das Prinzip dabei ist ganz einfach: der Antragsteller muss eine Datei

- mit einem durch *Let's Encrypt* bestimmten Namen und

- mit einem durch *Let's Encrypt* bestimmten Inhalt

auf dem Webserver anlegen und dafür Sorge tragen, das *Let's Encrypt* diese Datei via HTTP-Zugriff lesen und prüfen kann.

Man geht dabei von der (durchaus berechtigten) Annahme aus, das jemand, der ohnehin vollen Zugriff auf die Webseite besitzt, auch jemand ist, der die Berechtigung dazu hat.

3.3 Arbeitsschritte

Folgende Schritte sind automatisiert:

- Ftp-Zugriff sicherstellen
- *Let's Encrypt*-Konto prüfen
- Zertifikat für Domänen anfordern
- für jeden Domänen-Namen einzeln validieren
- Dateien für Zertifikat und Schlüssel herunterladen

Manuell ist nur noch ein Schritt zu erledigen:

- Dateien für Zertifikat und Schlüssel in der Verwaltungs-Oberfläche des Hosters aktivieren.

VORBEREITUNGEN

Den schwierigen Teil erledigt die Kombination *CertesGUI* / *certes CLI* für Sie.

Sie benötigen lediglich einige Angaben, damit die Anforderung des Zertifikats automatisch abläuft:

- eine langfristig erreichbare Email-Adresse
- die Namen der Domänen
- einen Ftp-Zugang zum Server der Webseite (Server-Name, Benutzername, Passwort)
- den Verzeichnis-Pfad, unter dem die Dateien (index.html, ...) für die Webseite zu finden sind.

Bei *Hosteurope* (und auch bei jedem anderen Anbieter) finden Sie in der Verwaltungsoberfläche bzw. der Online-Hilfe alle Angaben die Sie brauchen.

Wundern Sie sich nicht, wenn die Benutzernamen **keine Email-Adressen** sind. *Email-Adressen* als Benutzer-/Kontennamen zu verwenden ist eine Unsitte.

DOMÄNENNAMEN

Auch wenn es oft behauptet wird, das WWW ist nicht das Internet. (WWW ist die Abkürzung für Werner Will's Wissen.)

Beispiel: www.diub.de

- de → Top-Level-Domain, hier *de* für Deutschland

- diub → First-Level-Domain, kurz Domain, eben der Name, den der Inhaber sich hat reservieren lassen und über den nur er Verfügungsgewalt hat
- www → Sub-Level- Domain, kurz Sub-Domain, also eine Unter-Domäne, die ein Teilbereich der Domäne ist, jedoch nicht zwingend die selbe Webseite bezeichnet

Der Begriff Domäne bezeichnet (hier) also einen (Wirkungs-)bereich.

Bei *Hosteurope* (siehe (3.4) *Beispiel: HostEurope* (Seite 6) ; bei anderen bitte nachlesen) richten sich die anzugebenden Domänen-Namen nach dem Verzeichnis, für welches das Zertifikat erstellt werden soll.

Die Sub-Level-Domäne *www* wird dabei automatisch fest der eigentlichen First-Domäne zugeschlagen. Das bedeutet, das *diub.de* und *www.diub.de* immer zusammen aufgeführt sein müssen und zusammen nur ein Zertifikat benötigen.

Selbst definierte Sub-Level-Domänen können anderen, eigenen Verzeichnissen zugeordnet sein, oder auch dem Verzeichnis der First-Level-Domäne.

In meinem Beispiel gehört die Sub-Level-Domäne *kodierecke* zum Verzeichnis der First-Level-Domäne, daher sieht die Liste dort so aus:

diub.de www.diub.de kodierecke.diub.de

Auch wenn dabei nur eine Zertifikats-Datei entsteht, muss dennoch für jede First-Level-Domäne und Sub-Level-Domäne die Validierung einzeln durchgeführt werden. Im Umkehrschluss bedeutet dies, das eventuell vorhandene weitere Domänen nicht in dieses Zertifikat einfließen dürfen, sondern für sich selbst bearbeitet werden müssen.

Das bedeutet 3 Durchläufe für die Validierung der Zugriffsrechte:

- Validierung anfordern
- Daten zur Validierung auf Server hochladen
- eigentliche Validierung anstoßen
- Ergebnis abfragen

3.4 Beispiel: HostEurope

In der Verwaltung Menü → Sicherheit & SSL → SSL administrieren



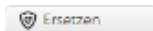
Nach unten rollen.



- Verzeichnis: /www
- Domäne: diub.de (schließt www.diub.de mit ein!)
- weitere: kodierecke.diub.de

ZERTIFIKAT AKTUALISIEREN

Nach dem Erhalt des Zertifikats (Dateien *---cert.pem und *---key.pem) auf klicken.



ÜBERTRAGEN SIE IHRE ZERTIFIKAT-DATEI:

Zertifikat:	<input type="button" value="Datei auswählen"/>	Keine ausgewählt
Key:	<input type="button" value="Datei auswählen"/>	Keine ausgewählt
📘 Passwort:*	<input type="text"/>	
📘 CA:*	<input type="button" value="Datei auswählen"/>	Keine ausgewählt

- Unter *Zertifikat* die Datei *---cert.pem angeben.
- Unter *Key* die Datei *---key.pem angeben.
- *Passwort* bleibt leer.
- *CA* bleibt leer.
- *Absenden* anklicken.

4 Zertifikat anfordern und aktivieren

Geben Sie die passenden Angaben ein oder laden Sie einfach eine bestehende Konfiguration: (4.1) *Einstellungen* (Seite 8)

Klicken Sie auf Start: (4.2) *Zertifikat abrufen* (Seite 9)

Aktivieren Sie das neue Zertifikat: (4.3) *Zertifikat beim Host er einrichten* (Seite 10)

4.1 Einstellungen

Das Beispiel zeigt die Einstellungen für eine Hauptdomäne mit 2 Sub-Level-Domänen.

Der Host er ist hierbei *Hosteurope*.

The screenshot shows the CertesGUI application window with the following fields filled in:

- Anforderung**
 - Email-Adresse: diub@diub.de
 - Domain-Name(n): diub.de www.diub.de kodierecke.diub.de
 - Loakler Zertifikat-Pfad: C:\Daten\WebSeiten\diub.de\well-known\acme-challenge\
- Etp**
 - Benutzername: ftpxxxxxxxx-Master
 - Server-Name: diub.de
 - Passwort: [masked]
 - Wuzelverzeichnis: /www/

At the bottom, there is a table with columns: Index, Zeitpunkt, and Meldung.

EMAIL-ADRESSE

Wird von *Let's Encrypt* dazu verwendet, vor Ablauf eines Zertifikats eine entsprechende Mitteilung zu senden.

DOMAIN-NAME(N)

Alle von dem Zertifikat betroffenen Domänen müssen mit Namen hier aufgeführt werden.

Trennzeichen ist einfach ein Leerzeichen.

LOKALER ZERTIFIKAT-PFAD

CertesGUI bzw. *certes CLI* kopiert

- die Datei mit dem Zertifikat (Domänenname---cert.pem) und
- die Schlüsseldatei (Domänenname---key.pem)

bei Erfolg in dieses Verzeichnis.

FTP - WURZELVERZEICHNIS

Die Angaben für den Ftp-Zugriff sind im Grunde selbsterklärend.

- Benutzername
- Passwort
- Server-Name

Das Wurzelverzeichnis ist der Pfad zu eben jenem Verzeichnis auf dem Server des Hosters, welches die Webseite als *Root* ansieht.

4.2 Zertifikat abrufen

Nach einem Klick auf werden die nachstehen Schritte abgearbeitet. Bei einem Fehler ist dies in der Log-Anzeige deutlich zu erkennen.

FTP-ZUGRIFF PRÜFEN

Vorab erfolgt ein Verbindungstest zum Ftp-Server.

ACCOUNT PRÜFEN

Dazu wird die Email-Adresse genutzt.

ANFORDERUNG SENDEN

Mit der Anforderung wird ein einzelnes Zertifikat für alle angegebenen Domänen-Namen bestellt.

Mehrere Domänen-Namen die (bei *Hosteurope*) zu demselben Verzeichnis gehören, müssen alle in einem Zertifikat bestätigt werden.

PRÜFUNG DER AUTHENTIZITÄT

Die Prüfung der Authentizität muss für jeden Domänen-Namen einzeln initiiert und bestätigt werden. Die Prüfung erfolgt dabei in mehreren Teil-Schritten, so das mehrfach ähnliche Aufrufe zu sehen sind:

- Anforderung der Prüfung via HTTP → Prüfdaten und Dateiname werden zurück geliefert
- die Daten werden in eine Datei auf dem Server geschrieben
- Anforderung der Verifikation der Zugriffsrechte auf die Domäne

Die Verifikation dauert öfter länger als 60 Sekunden. Daher wird nur alle 30 Sekunden der Status erneut abgefragt.

ZERTIFIKAT UND SCHLÜSSEL SPEICHERN

Die Dateien mit dem endgültigen Zertifikat und dem dazugehörigen Schlüssel werden unter *Lokaler Zertifikat-Pfad* gespeichert.

4.3 Zertifikat beim Hoster einrichten

Bei *Hosteurope* geht man dazu einfach in die Verwaltung zum Punkt *SSL administrieren*.

Mit Klick auf die zum Verzeichnis / den Domänen-Namen gehörende Schaltfläche *Ersetzen / Aktualisieren* gelangt man in einen Dialog zum Hochladen der beiden Dateien.

Achten Sie beim Hochladen auf die Angaben *cert* (Zertifikat) und *key* (Schlüssel) im Dialog und den Dateinamen.

Die optionale dritte Datei (CA) bleibt leer.

Das war es auch schon. Bleibt noch der Aufruf jedes einzelnen Domänen-Namens zum Test.

5 Wichtige Hinweise

5.1 Kopierschutz

Die Programme von *diub* sind in der Regel durch einen Kopierschutz gegen unrechtmäßige Weiterverbreitung gesichert.

Die Umgehung und auch der Versuch einer Umgehung dieses Kopierschutzes werden rechtlich verfolgt.

CertesGUI wird als **Freeware lizenziert** (Lizenz-Code: FreewareLicense) und ist kostenfrei erhältlich und weiterzugeben. Es sind keine weitergehenden Rechte damit verbunden.

Die Aktivierung erfolgt anonym.

Die eingeblendete Werbung (Werbebanner) stammt ausschließlich von *diub*.

KOPIERSCHUTZ TYP II

- Online-Kopierschutz
- Die Aktivierung erfolgt je PC einmalig via Internet.
- Ein weiterer Zugang zum Internet ist notwendig; die Aktivierung wird automatisch verlängert.
- Eine Portierung der Lizenz auf einen anderen PC ist einfach möglich.
- Für eine Portierung auf einen anderen PC ist in der Regel **keine Kontaktaufnahme zu *diub*** notwendig.

Typ: Lizenz für Rechner mit regelmäßigen Zugang zum Internet