EOL: DFN-PKI Generation 1

Am 9. Juli 2019 wird das Wurzelzertifikat *Deutsche Telekom Root CA 2* seine Gültigkeit verlieren. Das Zertifikat wurde im Jahr 1999 ausgestellt und war somit 20 Jahre lang gültig.

Die CA-Zertifikat im Sicherheitsniveau Global Generation 1 der DFN PKI wurde durch eben dieses Wurzelzertifikat ausgestellt und verliert somit ebenfalls seine Gültigkeit. Die DFN PKI im Sicherheitsniveau Global Generation 1 ist somit ab dem 9. Juli 2019 nicht mehr zu verwenden und alle damit ausgestellten Zertifikate verlieren ihre Gültigkeit.

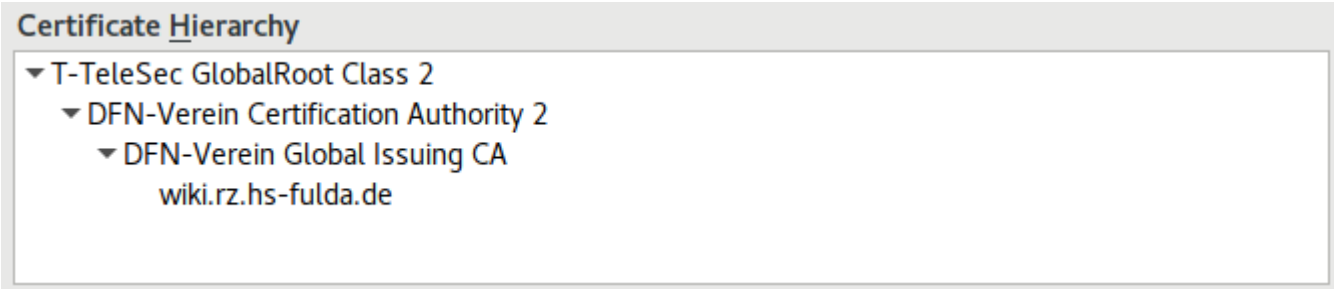
Zertifikate verlieren ihre Vertrauenswürdigkeit am 09.06.2019 auch dann, wenn das im Zertifikat angegebene Gültigkeitsdatum darüber hinaus geht.

In Zukunft ist nur noch die DFN PKI im Sicherheitsniveau Global Generation 2, die mit dem bis 2033 gültigen Wurzelzertifikat *T-Telesec Global Root Class 2* signiert wurde, zu verwenden.

Bitte prüfen Sie alle Zertifikate für die Sie verantwortlich sind auf einen eventuell notwendigen Austausch!

Root-CA-Zertifikat und Zertifikatskette

Die von der Hochschule Fulda aktuell verwendete Zertifikatskette sieht wie folgt aus:



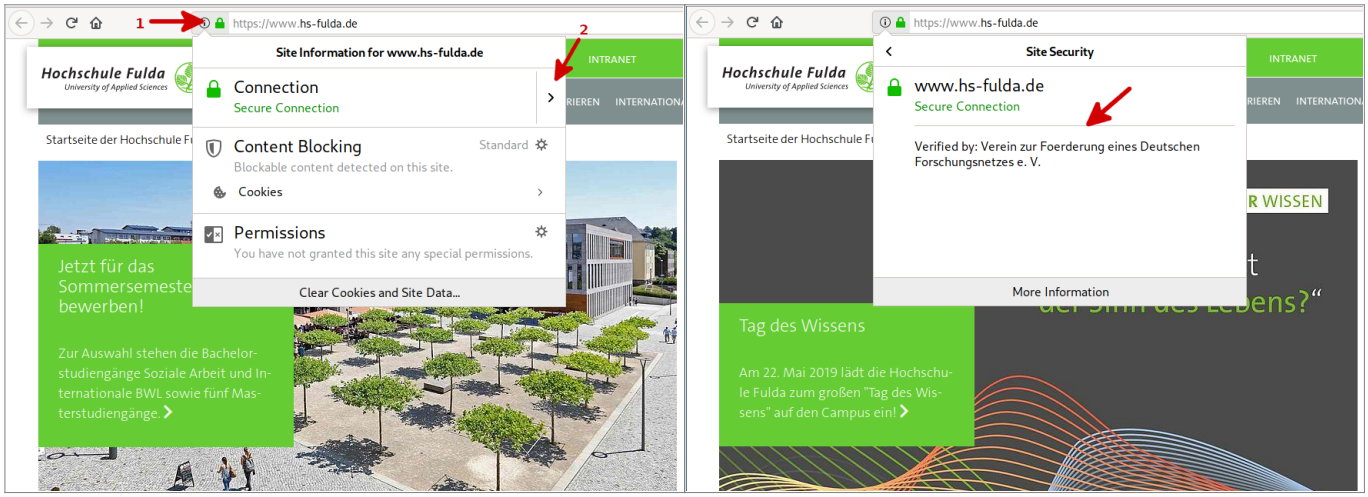
- Das Wurzelzertifikat erhalten Sie hier:
  dfn-ca-g2.pem
- Die Zertifikatskette kann hier heruntergeladen werden:
  dfn-chain-g2.pem

Zertifikat prüfen

Um zu prüfen, ob Sie ein Zertifikat aus der DFN PKI im Sicherheitsniveau Global Generation 1 nutzen, gibt es verschiedene Möglichkeiten.

Im Webbrowser

Falls Sie ein Webserver Zertifikat für Ihre Webseite nutzen, können Sie die Zertifikatkette ganz einfach im Webbrowser prüfen. Öffnen Sie dazu die Webseite die das Zertifikat verwendet in einem Webbrowser (hier beispielhaft mit Firefox dargestellt), klicken Sie auf das grüne Schloß-Symbol und anschließend auf den Pfeil hinter *Connection*.



In der rechten Abbildung sehen Sie, dass die neue PKI verwendet wird. Sollte hier stattdessen *Veryfied by: Hochschule Fulda* stehen, verwenden Sie noch die alte PKI.

Auf der Kommandozeile

Auf der Kommandozeile nutzen Sie das Programm *openssl* im SSL-Client-Modus um ein Zertifikat zu überprüfen.

```
~ $ openssl s_client -connect hs-fulda.de:443

[...]

Certificate chain
 0 s:C = DE, ST = Hessen, L = Fulda, O = Hochschule Fulda, CN =
www.hs-fulda.de
   i:C = DE, O = Verein zur Foerderung eines Deutschen Forschungsnetzes e.
V., OU = DFN-PKI, CN = DFN-Verein Global Issuing CA
 1 s:C = DE, O = Verein zur Foerderung eines Deutschen Forschungsnetzes e.
V., OU = DFN-PKI, CN = DFN-Verein Global Issuing CA
   i:C = DE, O = Verein zur Foerderung eines Deutschen Forschungsnetzes e.
V., OU = DFN-PKI, CN = DFN-Verein Certification Authority 2
 2 s:C = DE, O = Verein zur Foerderung eines Deutschen Forschungsnetzes e.
V., OU = DFN-PKI, CN = DFN-Verein Certification Authority 2
   i:C = DE, O = T-Systems Enterprise Services GmbH, OU = T-Systems Trust
Center, CN = T-TeleSec GlobalRoot Class 2
[...]
```

Das Kommando erzeugt eine Menge an Ausgabe auf der Konsole. Unter anderem finden Sie einen Hinweis auf das Aussehen der Zertifikatskette, die wie in der Abbildung dargestellt strukturiert sein

muss. Beachten Sie vor allem die letzte Zeile, in der mit **CN = T-TeleSec GlobalRoot Class 2** auf das neue Wurzelzertifikat *T-Telesec Global Root Class 2* verwiesen wird. Sollte hier stattdessen *CN = Deutsche Telekom Root CA 2* stehen, verwenden Sie noch die alte Generation der PKI.