

Let's Encrypt / Certificate Authorities

Was ist eine CA?

Eine CA ist eine Organisation oder ein Unternehmen, welche/s berechtigt ist, allgemein anerkannte digitale Zertifikate auszustellen.

Die CAs müssen sehr hohe Sicherheitsstandards erfüllen, um als CA anerkannt zu werden.

Wenn eine CA einmal geprüft und anerkannt wurde, wird ihr Public Key in den Zertifikatstores der Browser eingebunden. Dadurch kann die Integrität der Zertifikate geprüft werden, da die Signatur des Ausstellers, also der CA, geprüft werden kann.

Was ist Let's Encrypt?

Let's Encrypt ist eine CA, unter der Root-CA "ISRG Root X1" und "ISRG Root X2". Die "ISRG" "Internet Security Research Group" ist eine gemeinnützige Organisation, welche durch viele große Tech-Unternehmen wie Google, Mozilla, AWS, EFF, Cisco, SAP und viele mehr finanziert wird.

Let's Encrypt ist eine CA, bei der kostenlos Zertifikate beantragt werden können.

Zertifikate mit Let's Encrypt erstellen:

```
apt install python3-certbot-apache
certbot --apache
```

Revision #1

Created 24 October 2025 21:49:21 by Felix

Updated 24 October 2025 22:08:18 by Felix