Eigene CA und lokales Zertifikat erstellen

Für Tests ist es sinnvoll, Serveranwendungen auch unter https zu testen. Um das auf dem Entwicklungsrechner zu tun, benötigt man ein lokales Zertifikat und möglichst auch eine eigene CA, damit das Zertifikat auch ohne die lästigen Warnungen akzeptiert wird.

Auf einem Mac oder jedem anderen System mit Homebrew kann das mit brew erledigt werden. Zuerst aktualisiert man brew:

```
brew update && brew upgrade
```

Danach installiert man das Tool mkcert:

```
brew install mkcert
```

Damit mkcert das neu erstellte Zertifikat bzw. die CA in Firefox installieren kann, benötigt mkcert noch das Tool certutil aus dem Cask nss. Wird also auch mit Firefox getestet, ist nss noch zu installieren:

```
brew install nss
```

Nun kann eine CA und ein Zertifikat für localhost erstellt werden:

```
mkcert -install
mkcert localhost 127.0.0.1 ::1
```

Der Befehl `mkcert -install` kann übrigens beliebig oft wiederholt werden.

Um die erzeugten <name>.pem- und <name-key>.pem Dateien in <name>.crt und <name>.key Dateien umzuwandeln, wird openssl genutzt.

```
openssl x509 -in localhost.pem -out localhost.crt
openssl pkey -in localhost-key.pem -out localhost.key
```

Einsatz z. B. in einer Go-Anwendung mit dem Echo Framework:

```
func main() {
	e := echo.New()
	// add middleware and routes
	// ...

	sc := echo.StartConfig{Address: ":1323"}
	if err := sc.StartTLS(context.Background(), e, "localhost.crt", "localhost.key"); err != nil {
		e.Logger.Error("failed to start server", "error", err)
	}
}
```

Revision #1
Created 2026-09-26 13:20:52 UTC by ralf
Updated 2026-09-26 13:20:52 UTC by ralf