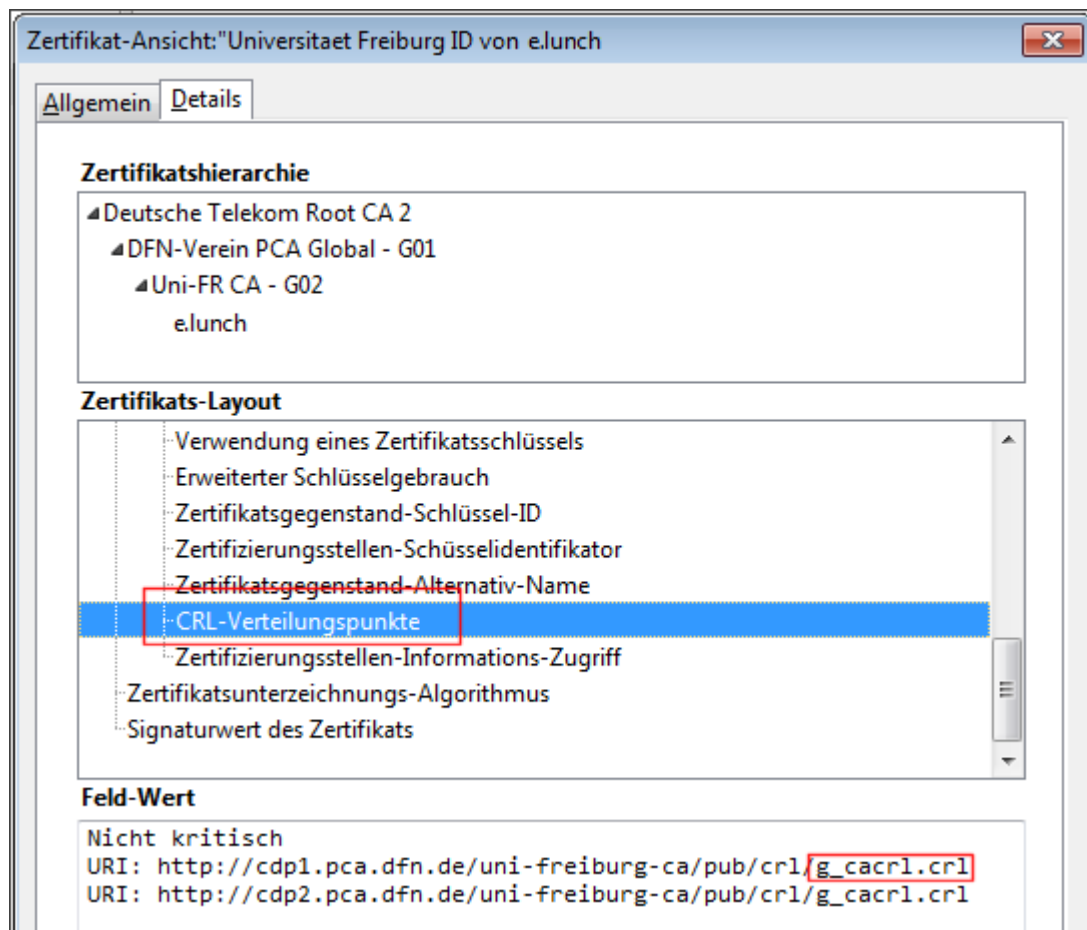


# Thunderbird - Zertifikats-Sperrlisten

Wenn ein Zertifikat für ungültig erklärt wird, weil z.B. durch eine Neuinstallation der private Schlüssel verloren gegangen ist, wird der **Rückruf** von der Zertifizierungsstelle in einer Sperrliste veröffentlicht. Leider werden solche Listen von vielen Zertifikate-Nutzern sehr stiefmütterlich behandelt. Deshalb möchten wir hier etwas genauer darauf eingehen.

Die Zertifikate sind in der Lage, die Quelle für die Rückrufliste der eigenen Zertifizierungsstelle mit zu liefern (im vorliegenden Beispiel **g\_cacrl.crl**):

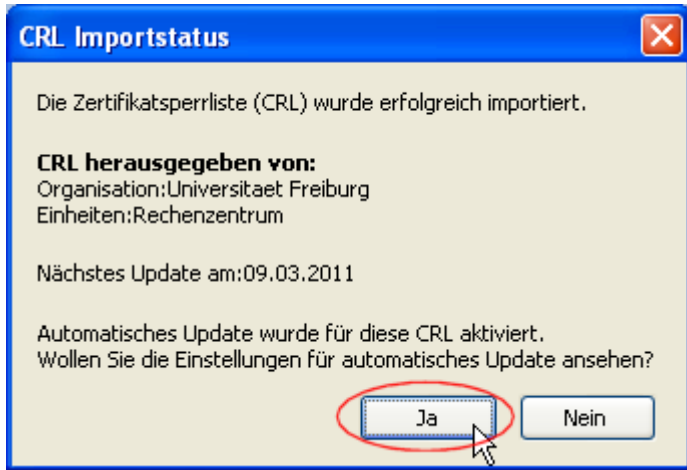


Um die Sperrliste zu importieren, rufen Sie die **Sperrlistenseite** der Uni-FR CA auf.

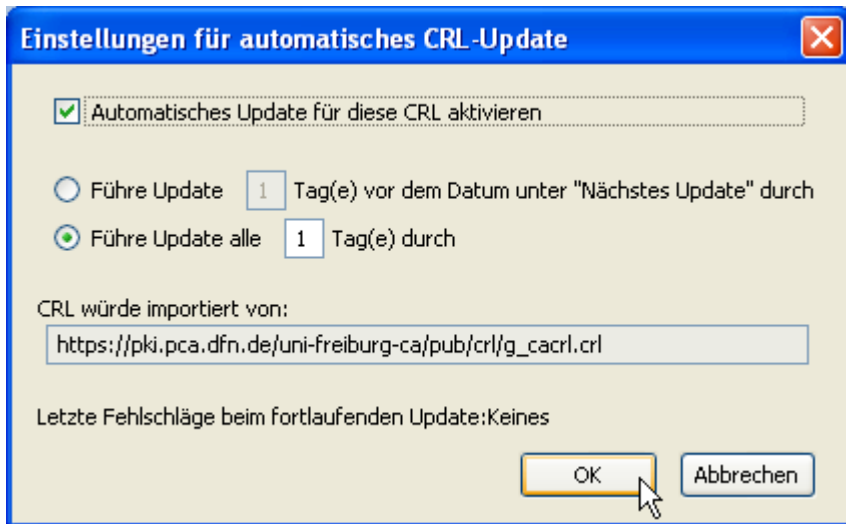


Klicken Sie dann mit der linken Maustaste auf den Menüpunkt **Zertifikatsperrliste installieren**.

Es erscheint folgendes Fenster:



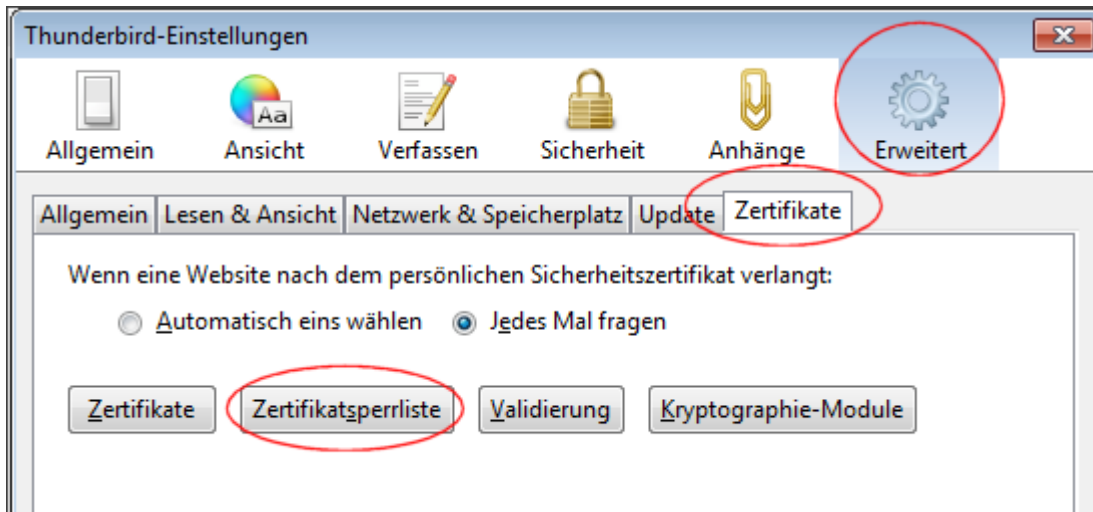
Klicken Sie auf jeden Fall auf die Schaltfläche Ja, damit Sie die Gelegenheit bekommen, das automatische Verfahren zum regelmäßigen Import der Sperrliste zu konfigurieren. Das geschieht dann im nachfolgenden Fenster. Wählen Sie die Optionen wie vorgeschlagen:



Das von der Sperrliste selbst festgelegte und meist recht großzügig bemessene Update-Intervall kann man durchaus kürzer einstellen.

Auf diese Weise kann man von diversen Zertifizierungsstellen die Sperrlisten importieren und das Update-Verhalten festlegen.

Sie finden die Liste der importierten Sperrlisten in den Thunderbird-Einstellungen:

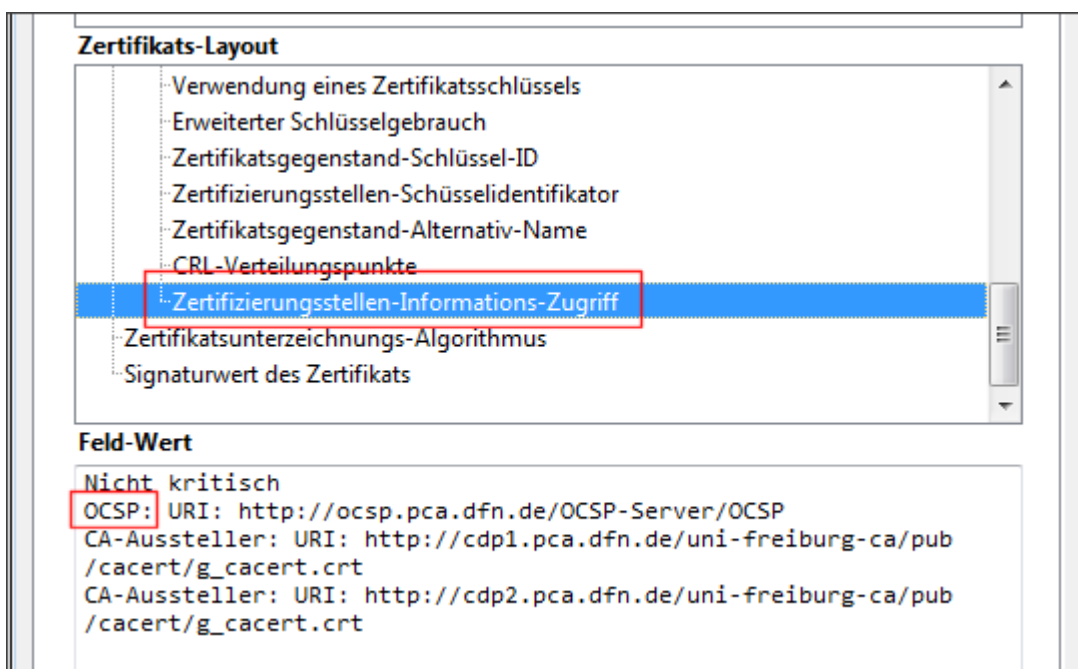


Dort können Sie auch nachträglich die Update-Einstellungen verändern.

## Der OCSP-Server

Von vielen Zertifizierungsstellen wird neben den Rückruflisten auch ein Server bereit gestellt, bei dem die Client-Programme (wie z.B. Thunderbird) beim Eintreffen eines Zertifikates unmittelbar nachfragen können, ob das Zertifikat z.Zt. noch (oder schon) gültig ist. Das geschieht über ein spezielles Protokoll mit dem Namen **OCSP (Online Certificate Status Protocol)**. Die Uni-FR CA kann persönliche und Webserver-Zertifikate mit der Option OCSP ausliefern. Man muss allerdings dabei berücksichtigen, das eventuell vorhandene Firewalls die OCSP-Kommunikation verhindern könnten und deshalb dafür freigeschaltet werden müssen.

Auch die Adresse des OCSP-Servers wird von einem OCSP-fähigen Zertifikat mitgeliefert:



Um die Verwendung des OCSP-Protokolles müssen Sie sich nicht bemühen; Thunderbird setzt es wenn möglich selbständig ein.

[Zertifikate - Artikelübersicht](#), [Sicherheit - Artikelübersicht](#), [Software - Adobe Connect](#)

From:

<https://wiki.uni-freiburg.de/rz/> - **RZ**

Permanent link:

<https://wiki.uni-freiburg.de/rz/doku.php?id=thundercrt>



Last update: **2011/02/14 12:25**