

Leitfaden für die Deinstallation des Zscaler-Root-Zertifikats



Beratungsstelle Digitale Medien in Schule und Unterricht – imedias
SAI-Koordinationsstelle Kanton Solothurn
Ronny Standtke, Daniel Stüber

Solothurn, 19.09.2018

Inhaltsverzeichnis

1 Einleitung.....	3
2 Deinstallation aus Internet Explorer / Edge.....	4
3 Deinstallation aus Firefox.....	7
4 Deinstallation aus Safari.....	9
4.1 Mac OS X.....	9
4.2 iOS (iPhone / iPad).....	13
5 Deinstallation aus Android.....	16
6 Deinstallation aus Chrome/Chromium.....	19

1 Einleitung

Internetinhalte an Solothurner Schulen werden im Auftrag des Volksschulamtes seit dem 1. Juli 2007 zentral gefiltert. Dieser Service gilt ausschliesslich für Volksschulen, die über die Bildungsinitiative «Schulen ans Netz» von Swisscom ans Internet angeschlossen sind.

Wenn Webseiten mit HTTP aufgerufen werden, ist die Verbindung leicht abhör- und auch manipulierbar. Wenn im Gegensatz dazu der Aufruf mit HTTPS erfolgt und der Webserver ein gültiges Zertifikat verwendet, ist die Verbindung zwischen Browser und Webserver vertraulich und gegen Manipulation geschützt. Auf diese Art und Weise ist jedoch keine Überwachung und damit auch keine Filterung der Daten durch Dritte, an dieser Stelle die Swisscom, mehr möglich.

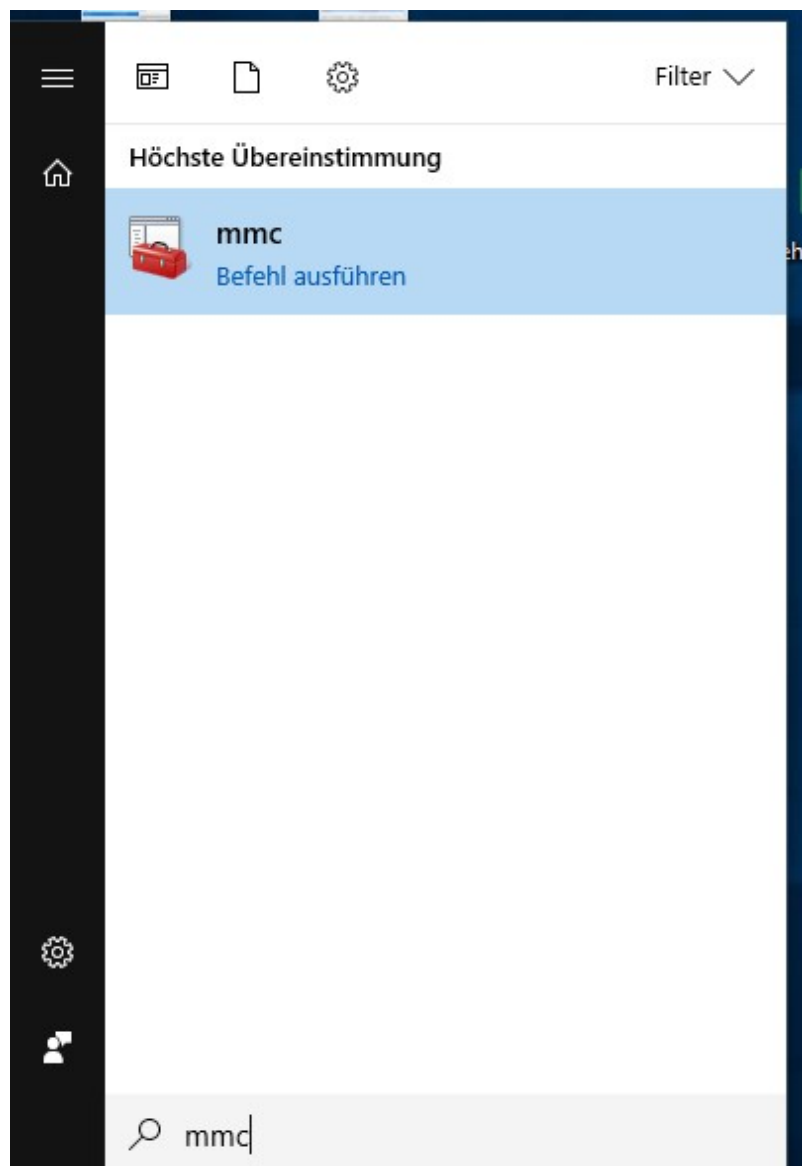
Um HTTPS-Verbindungen dennoch überwachen zu können, benutzt die Swisscom das klassische Man-in-the-middle-Verfahren (siehe Wikipedia-Artikel¹). Allerdings führt dieses Verfahren zu einer Warnmeldung in den üblichen Webbrowsern, da die verwendeten Zertifikate in diesem Verfahren gefälscht werden müssen. Um diese Warnmeldung auszuschalten, müssen zusätzliche Zertifikate (Zscaler-Zertifikate) auf den Computern der Anwender installiert werden, was dazu führt, dass die von der Swisscom gefälschten Zertifikate ohne Warnmeldung als korrekt akzeptiert werden.

Wenn von einer Schule der Schulen-ans-Internet-Anschluss der Swisscom später jedoch nicht mehr verwendet werden würde, so sollten diese zusätzlichen Zertifikate wieder entfernt werden. Dieser Leitfaden beschreibt daher für die wichtigsten Browser die notwendigen Schritte zur Deinstallation des Zertifikats.

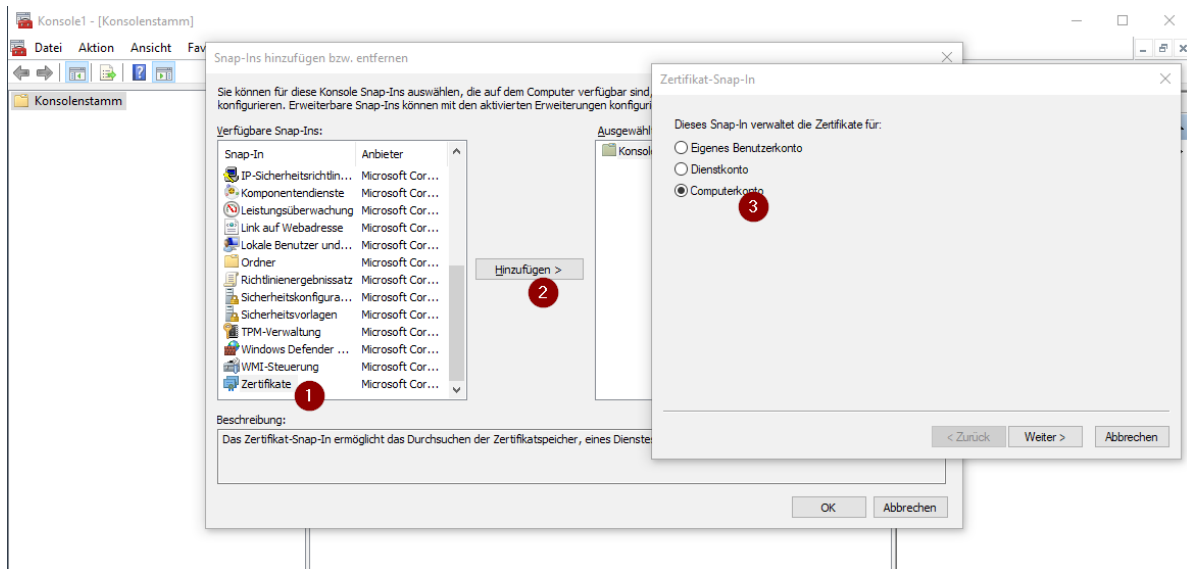
¹ <https://de.wikipedia.org/wiki/Man-in-the-Middle-Angriff>

2 Deinstallation aus Internet Explorer / Edge

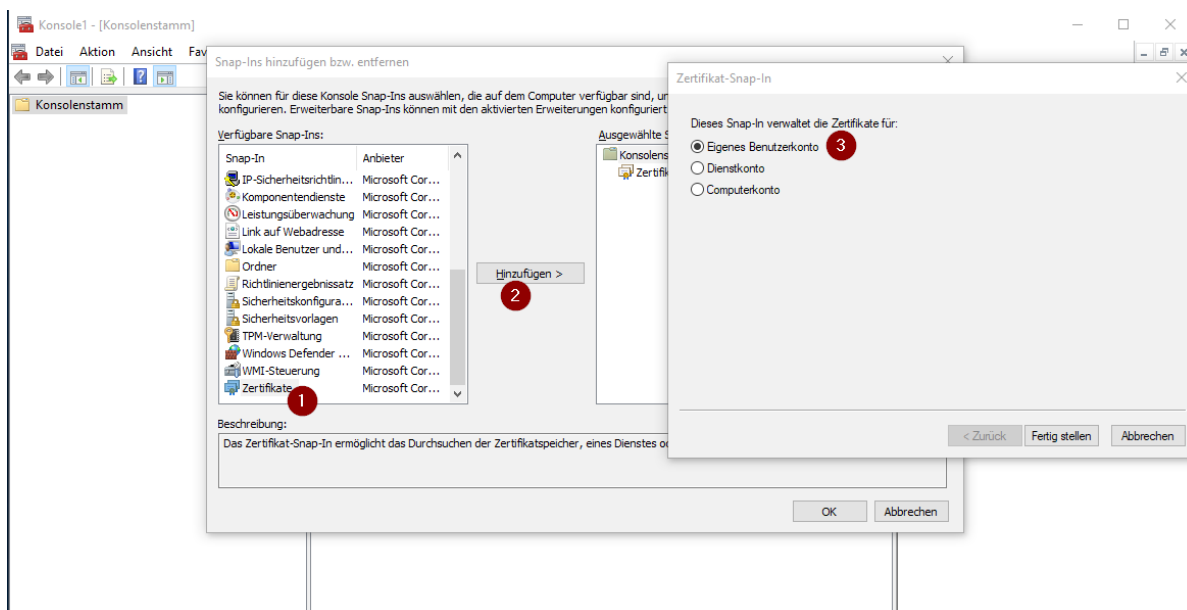
- in Windows links unten auf Start klicken und die Buchstaben «mmc» eintippen
- den Eintrag «mmc» anklicken



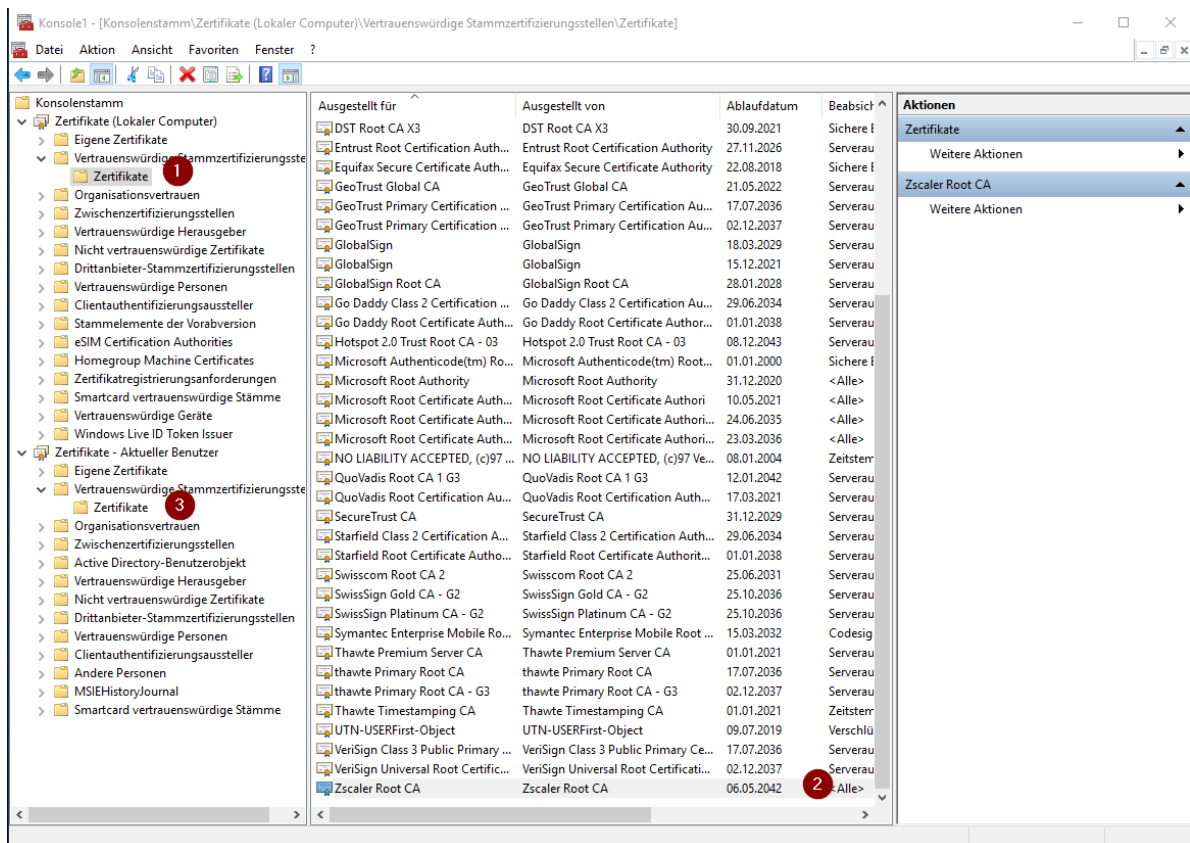
- die Tastenkombination «CTRL+M» drücken
- in der Liste auf der linken Seite den Eintrag «Zertifikate» (1) anwählen
- auf «Hinzufügen» (2) klicken
- im nun geöffnete Dialog-Fenster den Eintrag «Computerkonto» (3) wählen
- auf «Weiter» klicken.



- nochmals die Tastenkombination «CTRL+M» drücken
- in der Liste auf der linken Seite den Eintrag «Zertifikate» (1) anwählen
- auf «Hinzufügen» (2) klicken
- im nun geöffnete Dialog-Fenster den Eintrag «Eigenes Benutzerkonto» (3) wählen
- auf «Weiter» klicken

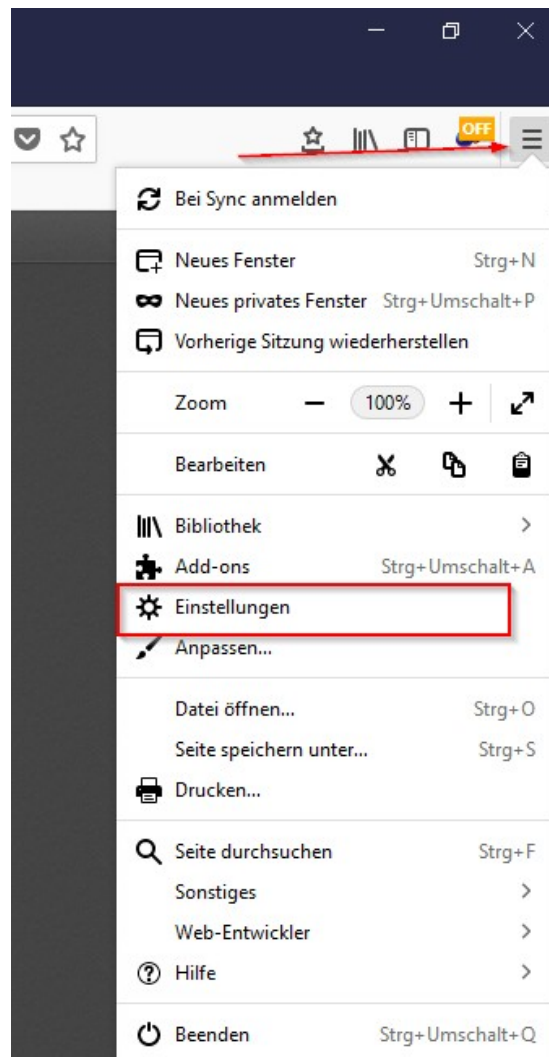


- in der aktuellen Anzeige «Zertifikate (lokaler Computer)» und dann «Vertrauenswürdige Stammzertifizierungsstellen» (1) aufklappen
- in der angezeigten Liste die Zscaler-Einträge mit Rechtsklick und dann «Löschen» entfernen (2)
- in der aktuellen Anzeige «Zertifikate – aktueller Benutzer» und dann «Vertrauenswürdige Stammzertifizierungsstellen» (3) aufklappen
- in der angezeigten Liste überprüfen, ob die Zscaler-Einträge vorhanden sind und gegebenenfalls mit Rechtsklick und dann «Löschen» entfernen (2)

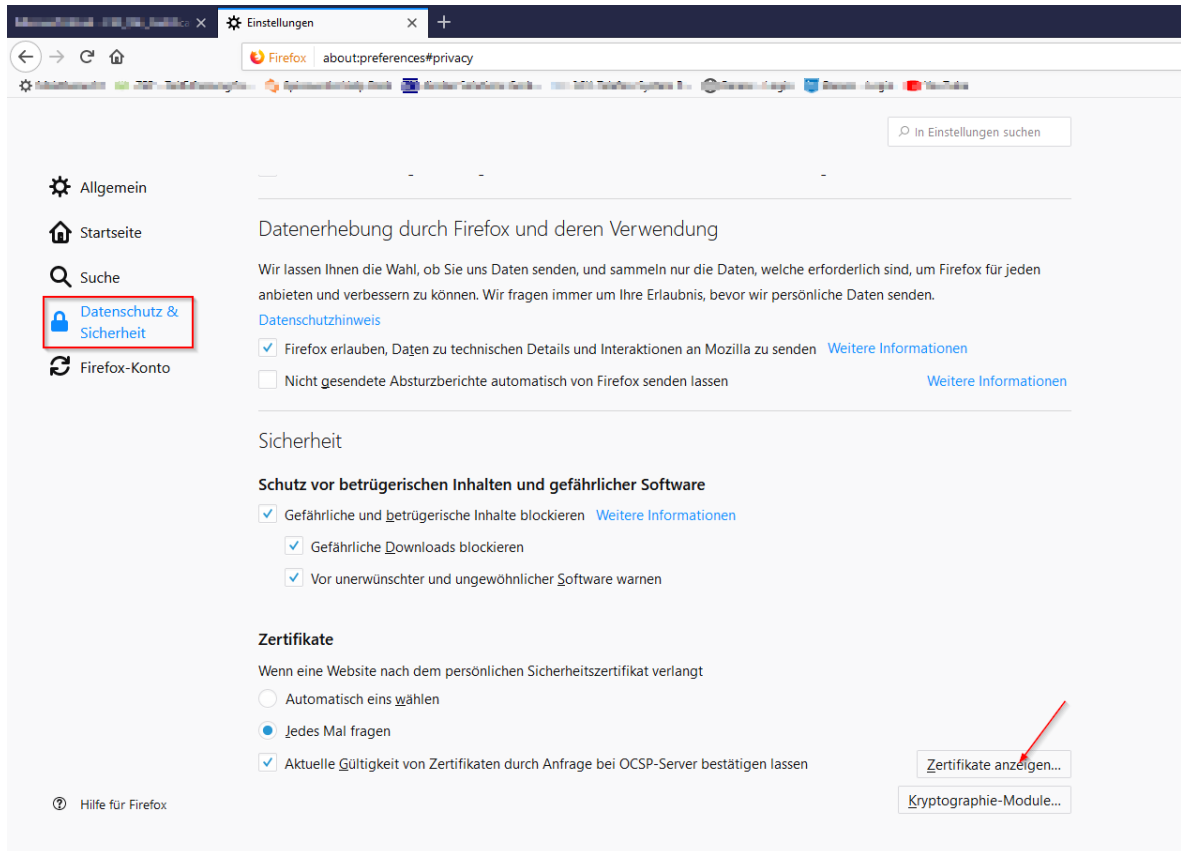


3 Deinstallation aus Firefox

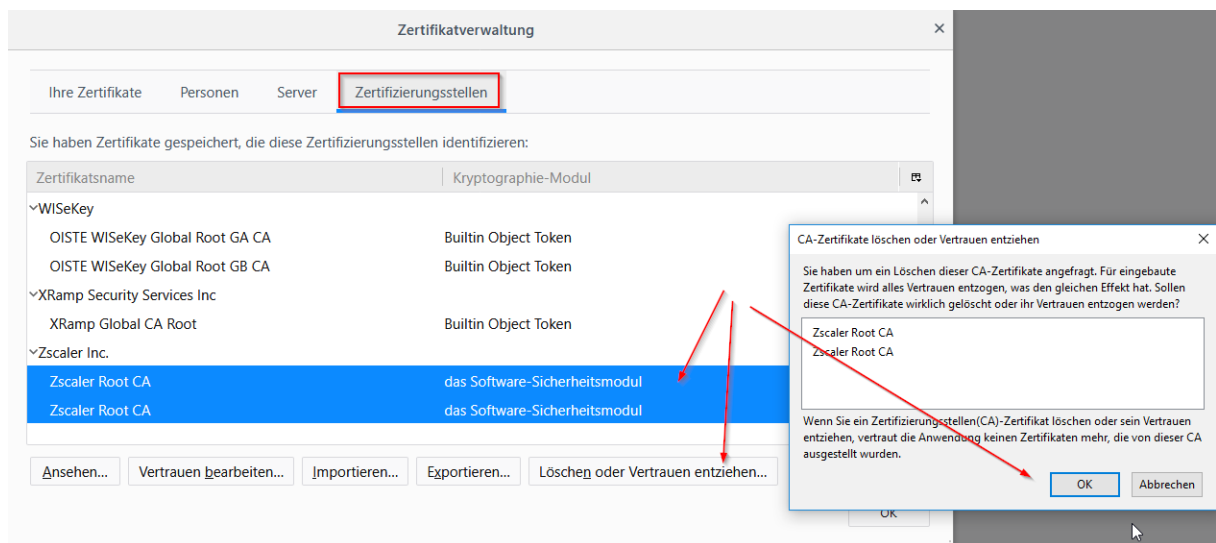
- im geöffneten Firefox rechts oben auf das «Hamburger-Menü» klicken
- den Menüpunkt «Einstellungen» auswählen



- auf der linken Seite «Datenschutz & Sicherheit» anwählen
- ganz nach unten scrollen
- auf «Zertifikate anzeigen» klicken



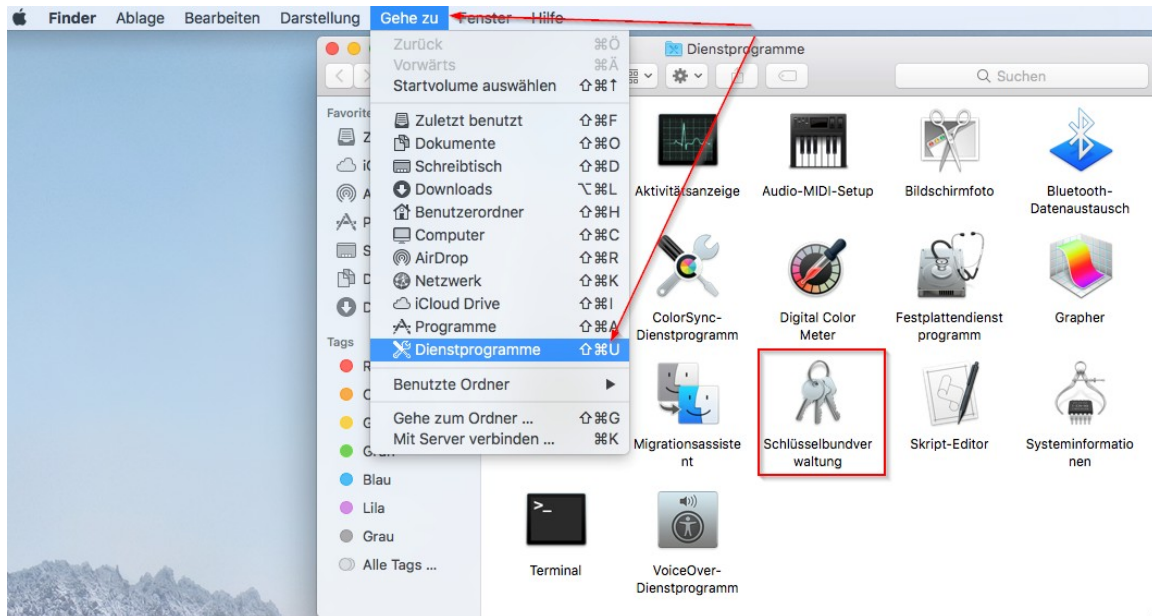
- «Zertifizierungstellen» anwählen
- in der Liste nach ganz nach unten scrollen
- die Zscaler-Zertifikate anwählen
- auf «Löschen oder Vertrauen entziehen» klicken



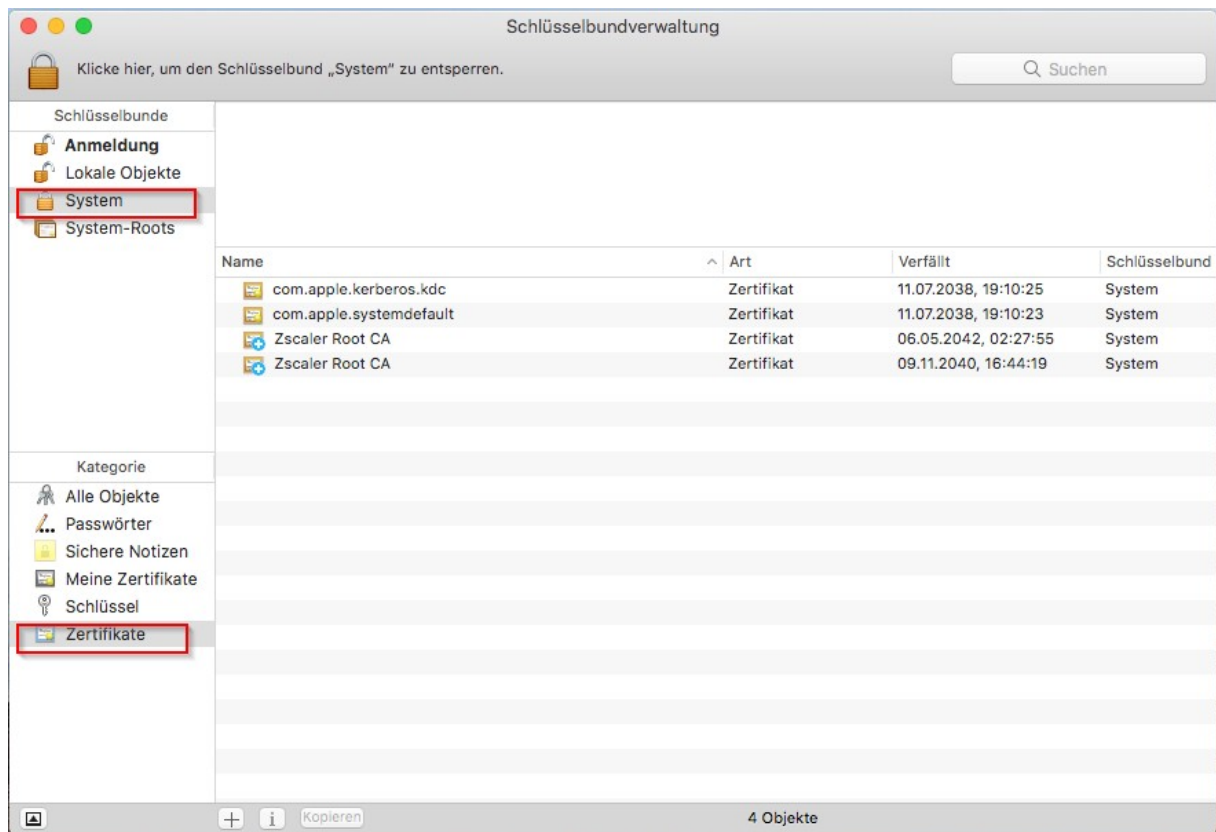
4 Deinstallation aus Safari

4.1 Mac OS X

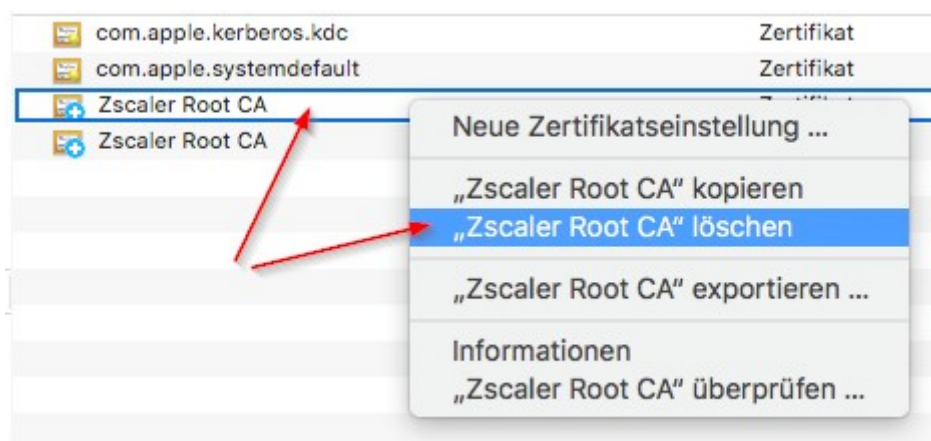
- im Finder auf «Gehe zu» und dann auf «Dienstprogramme» klicken
- in diesem Fenster den «Schlüsselbund» öffnen



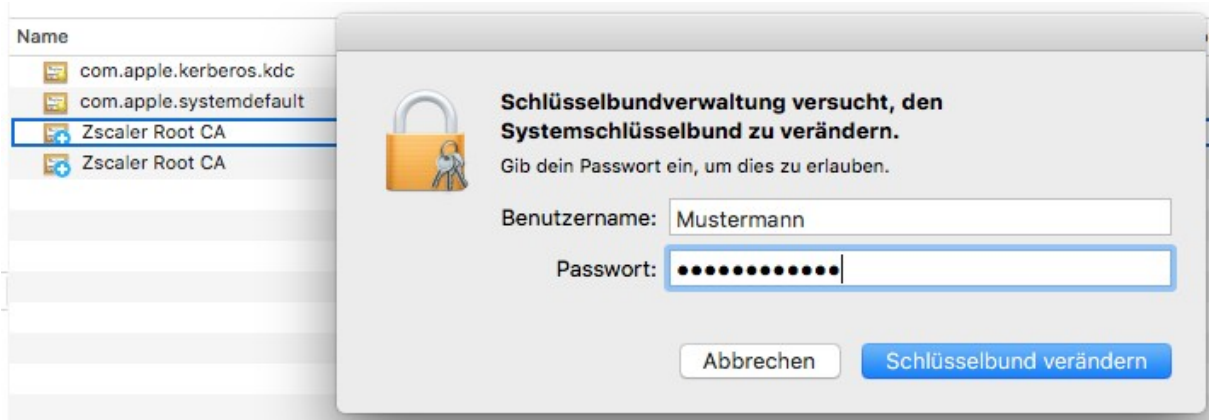
- im Schlüsselbund links oben auf «System» und links unten auf «Zertifikate» klicken
- es werden die installierten Zertifikate angezeigt



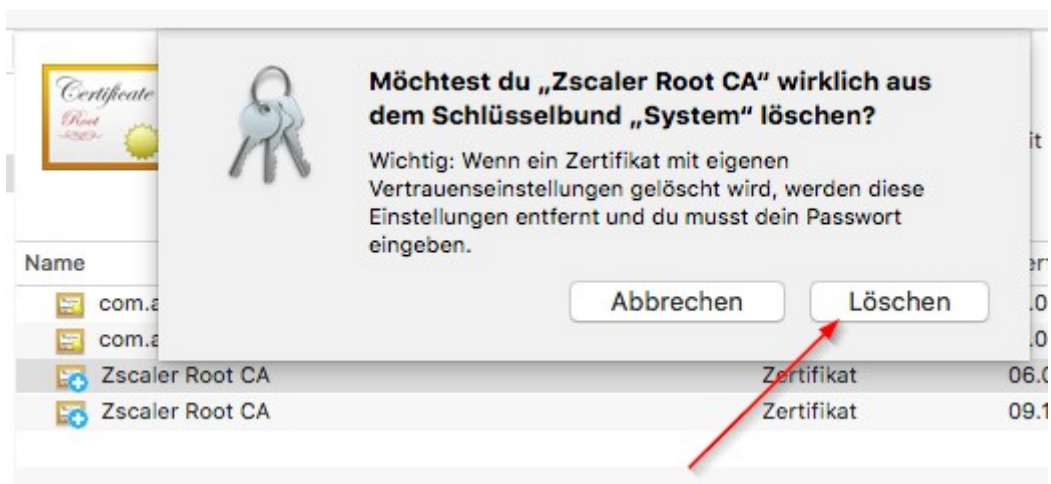
- mit Rechtsklick oder Taste «CTRL» + Mausklick auf das Zertifikat das Kontextmenu öffnen
- den Eintrag «Zscaler Root CA löschen» wählen



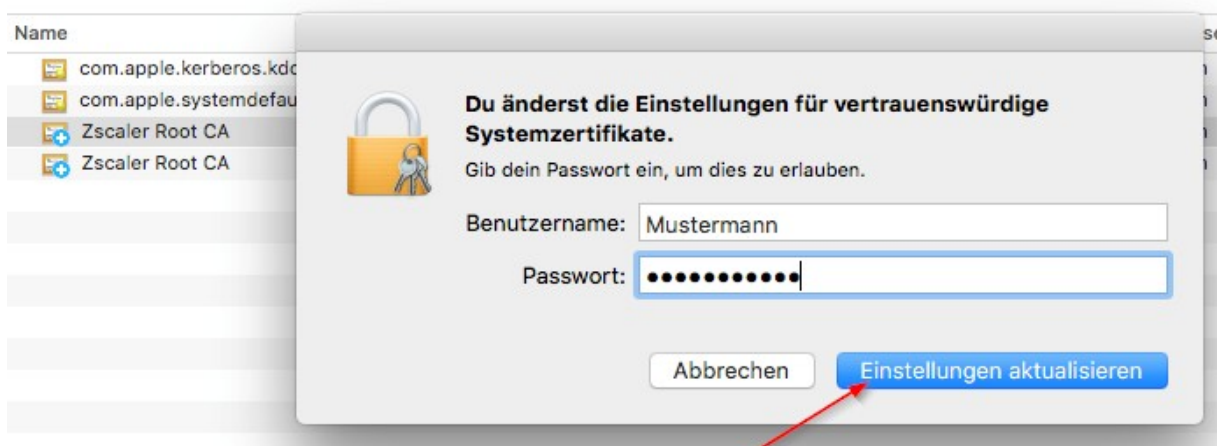
Es folgt eine Passwort-Abfrage um den Schlüsselbund zu entsperren. Ein Administrator-Login ist notwendig:



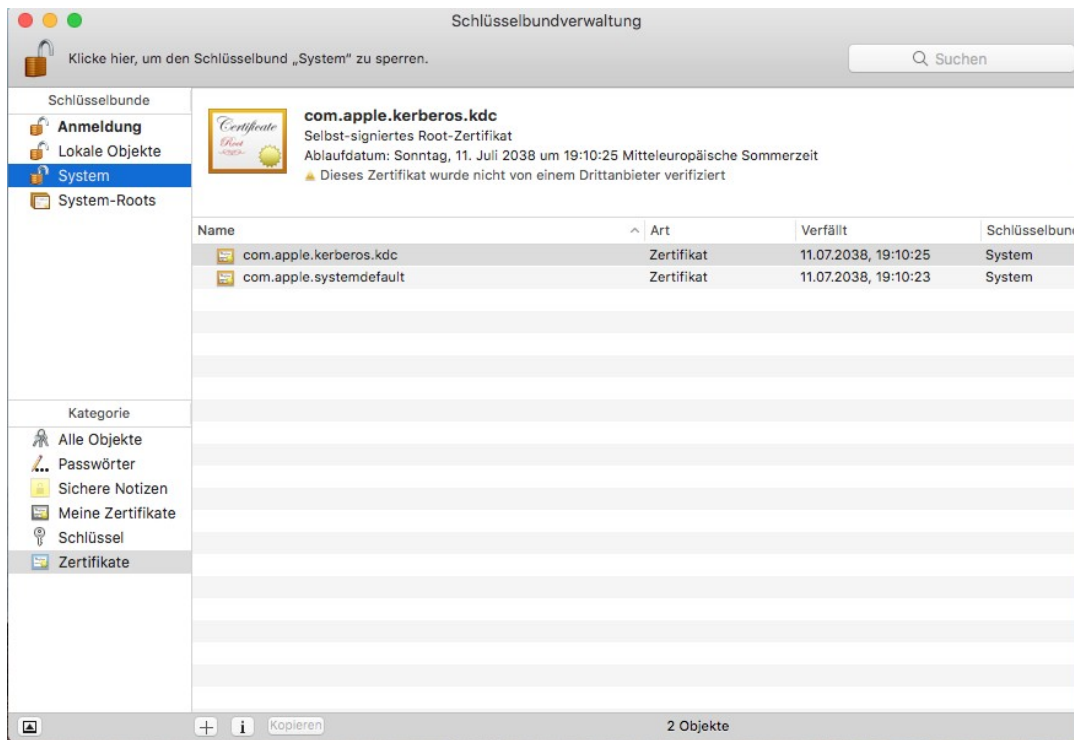
Das Löschen muss im folgenden Dialog-Fenster bestätigt werden:



Die Aktion muss noch einmal mit dem Administrator-Login bestätigt werden:

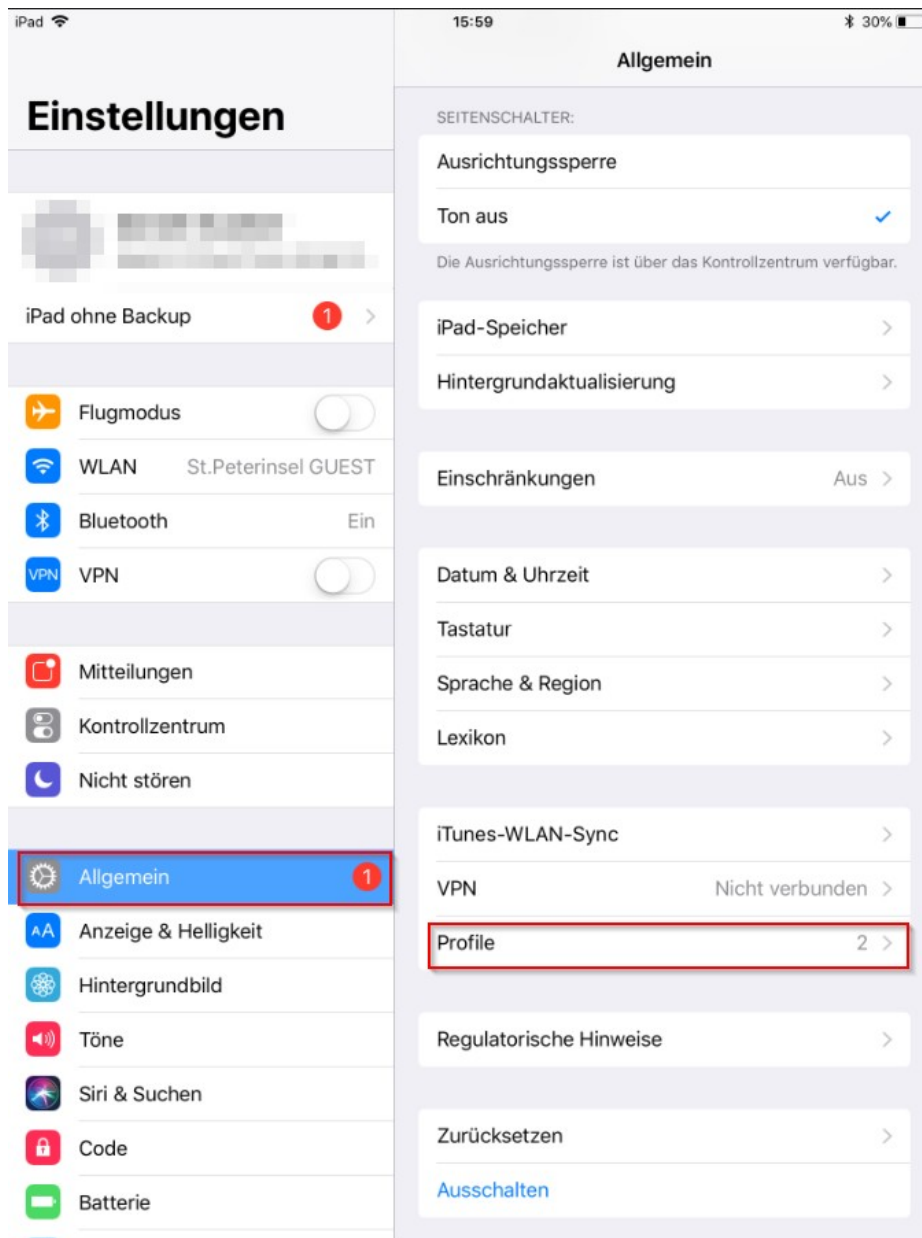


Die Zscaler-Zertifikate sind nun dauerhaft vom MacOS X entfernt:

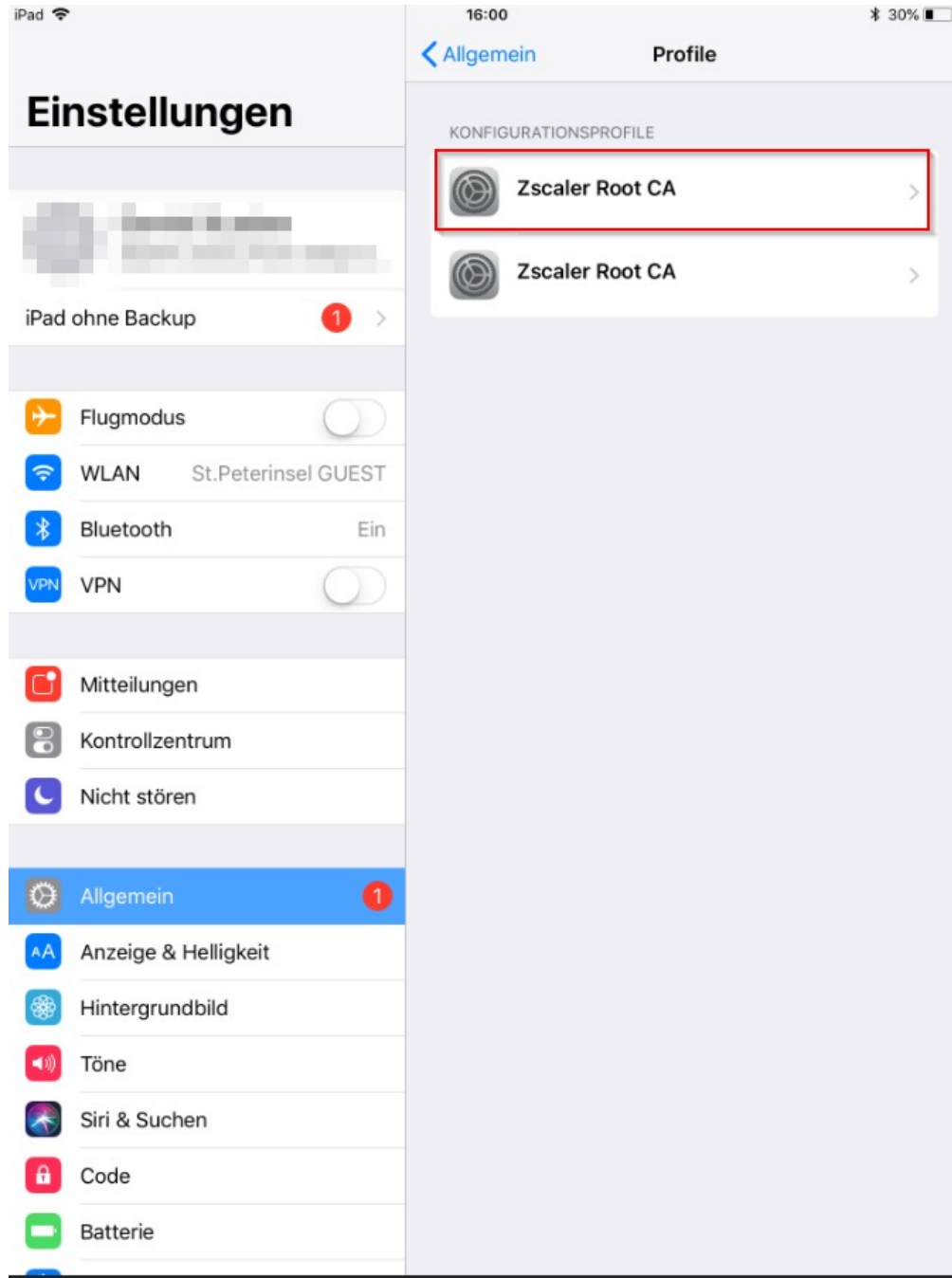


4.2 iOS (iPhone / iPad)

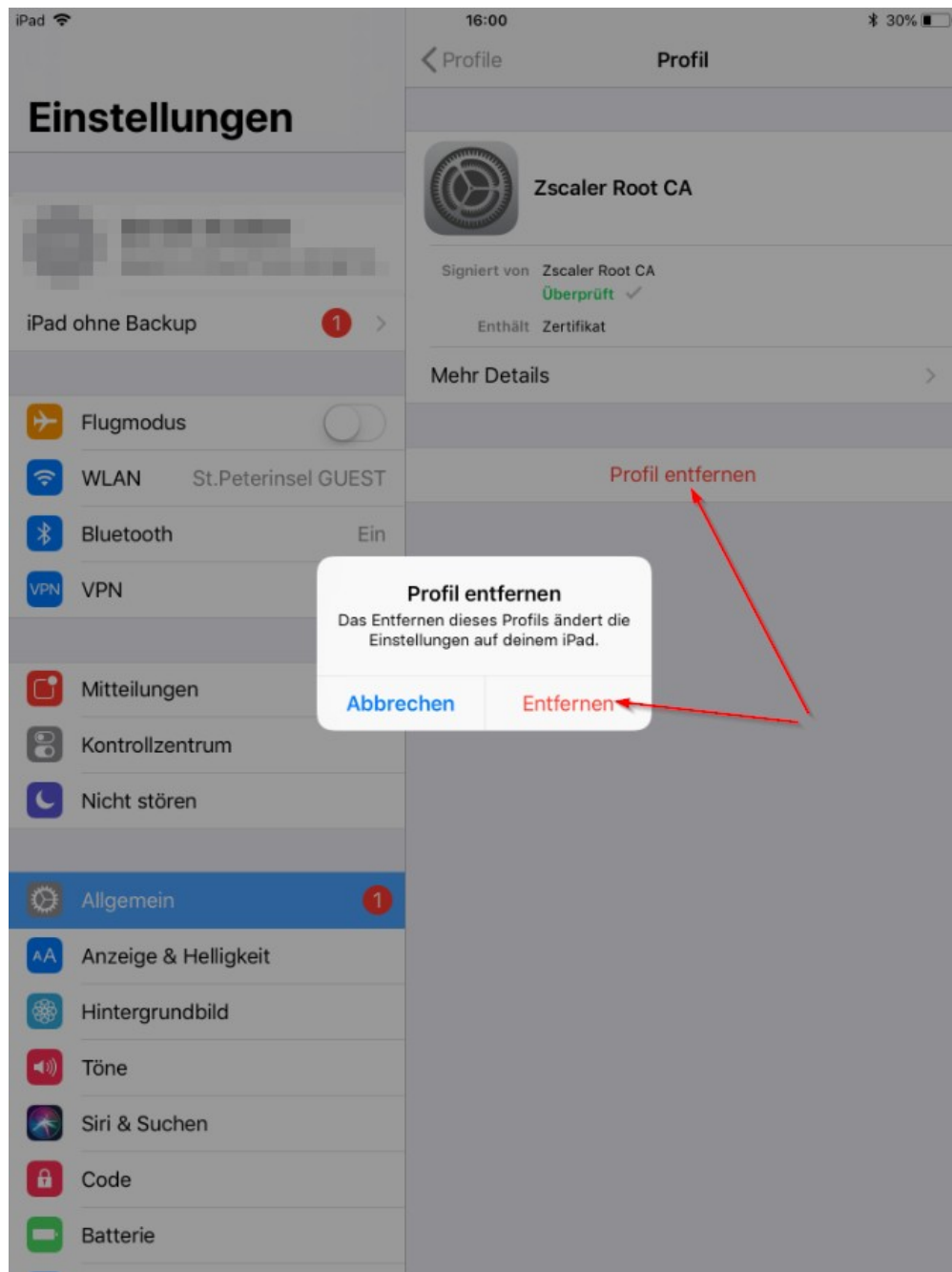
- auf dem iPad/iPhone die «Einstellungen» öffnen
- unter «Allgemein» «Profile» antippen



- die «Profile» (Zertifikate) antippen

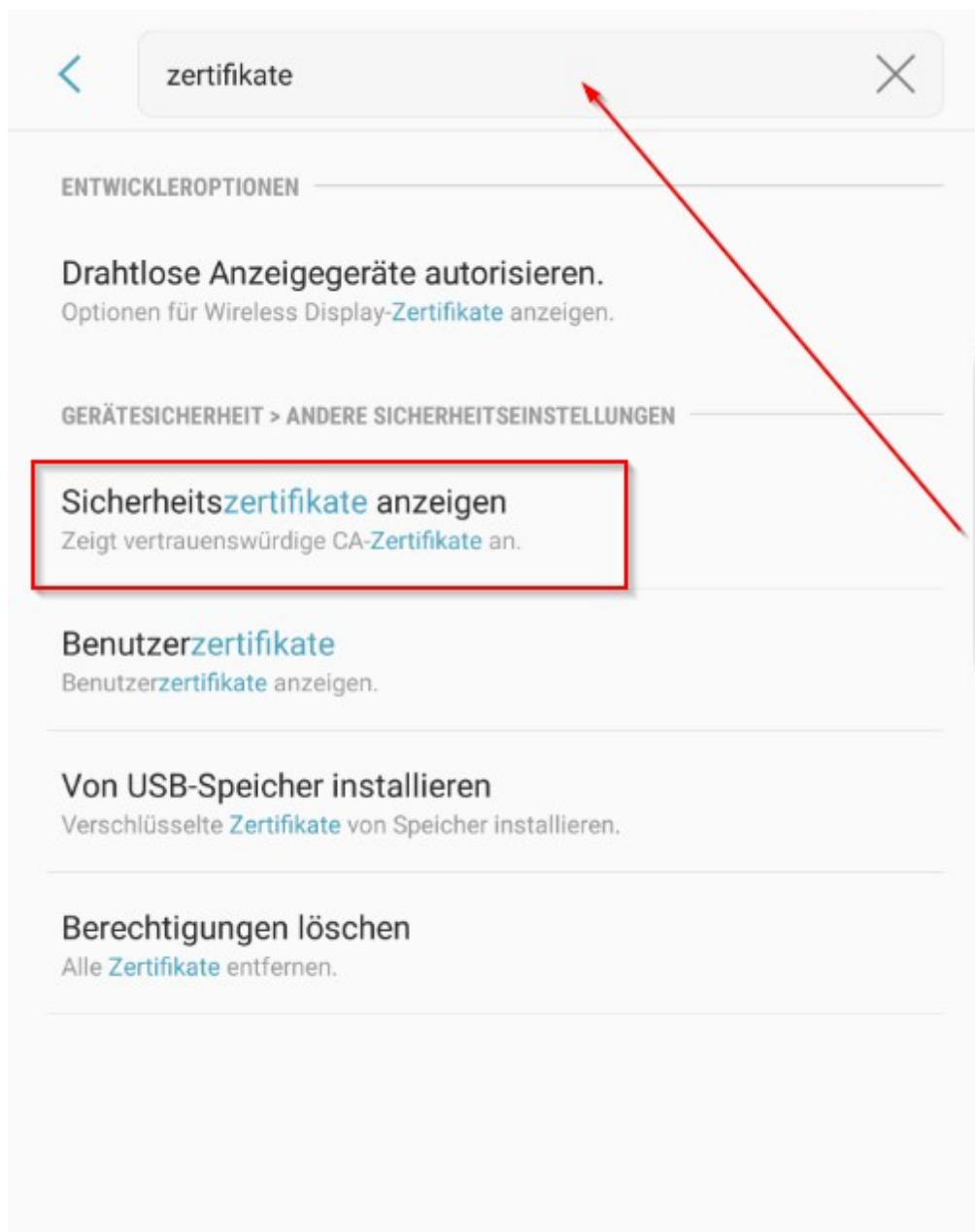


- «Profil entfernen» antippen
- den Sicherheits-Dialog bestätigen

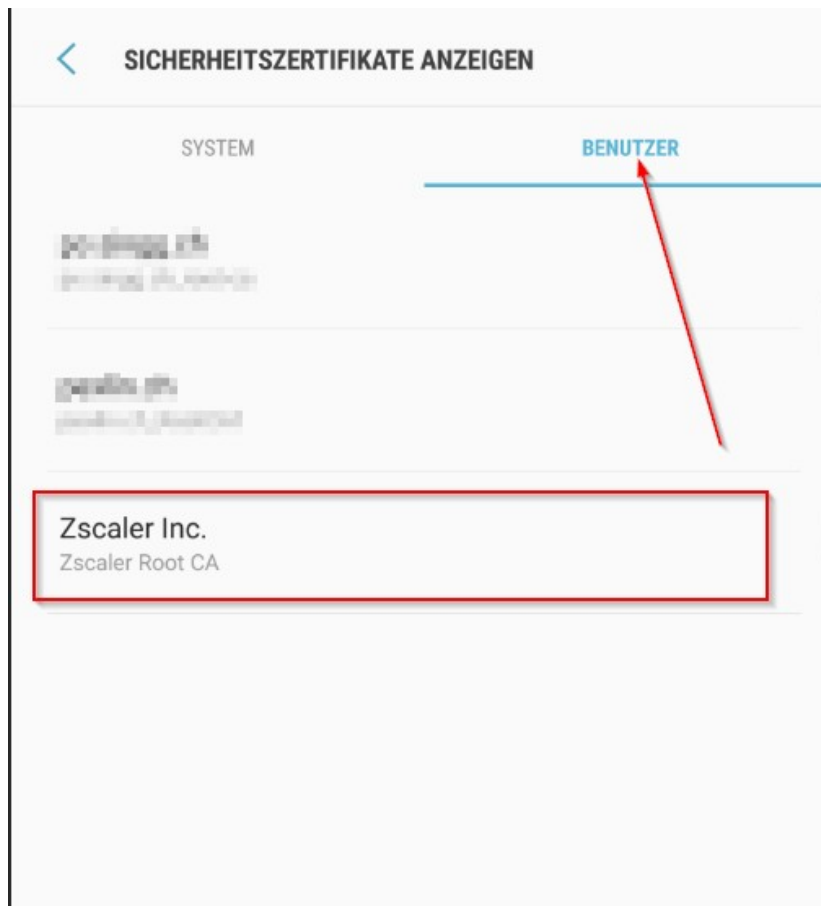


5 Deinstallation aus Android

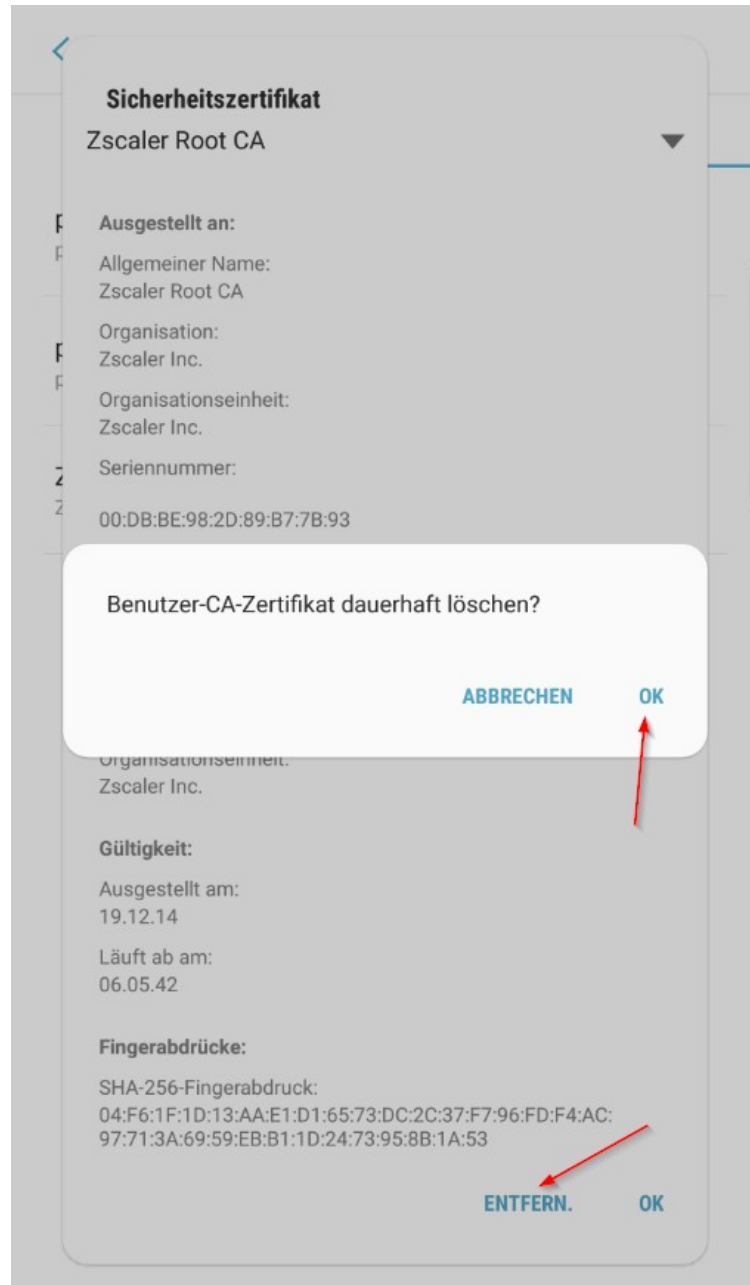
- die Einstellungen auf dem Android-System öffnen
- oben rechts in die Suchfunktion klicken und «Zertifikate» eintippen
- die Option «Sicherheitszertifikate anzeigen» antippen



- auf «Benutzer» tippen und die Einträge «Zscaler» antippen



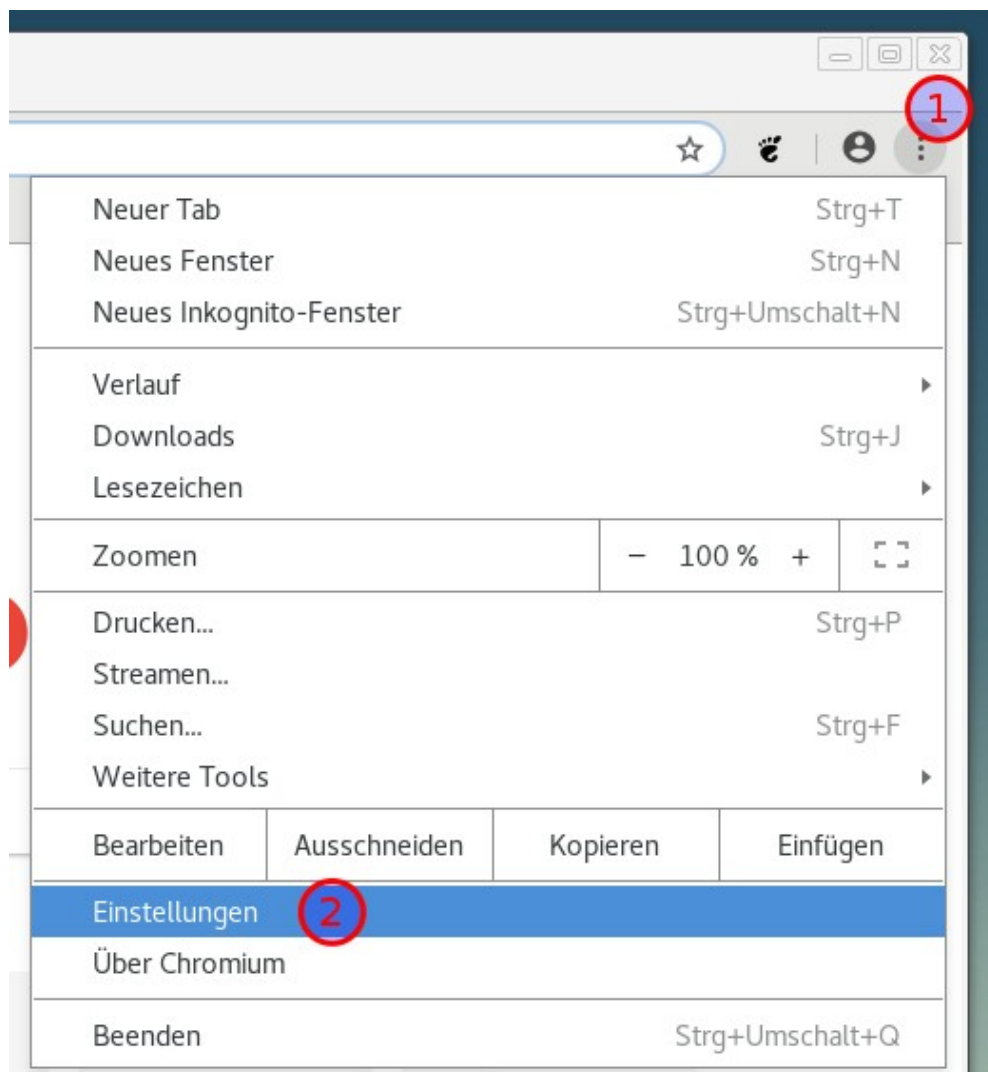
- unten auf «Entfern.» tippen und Sicherheits-Dialog bestätigen.



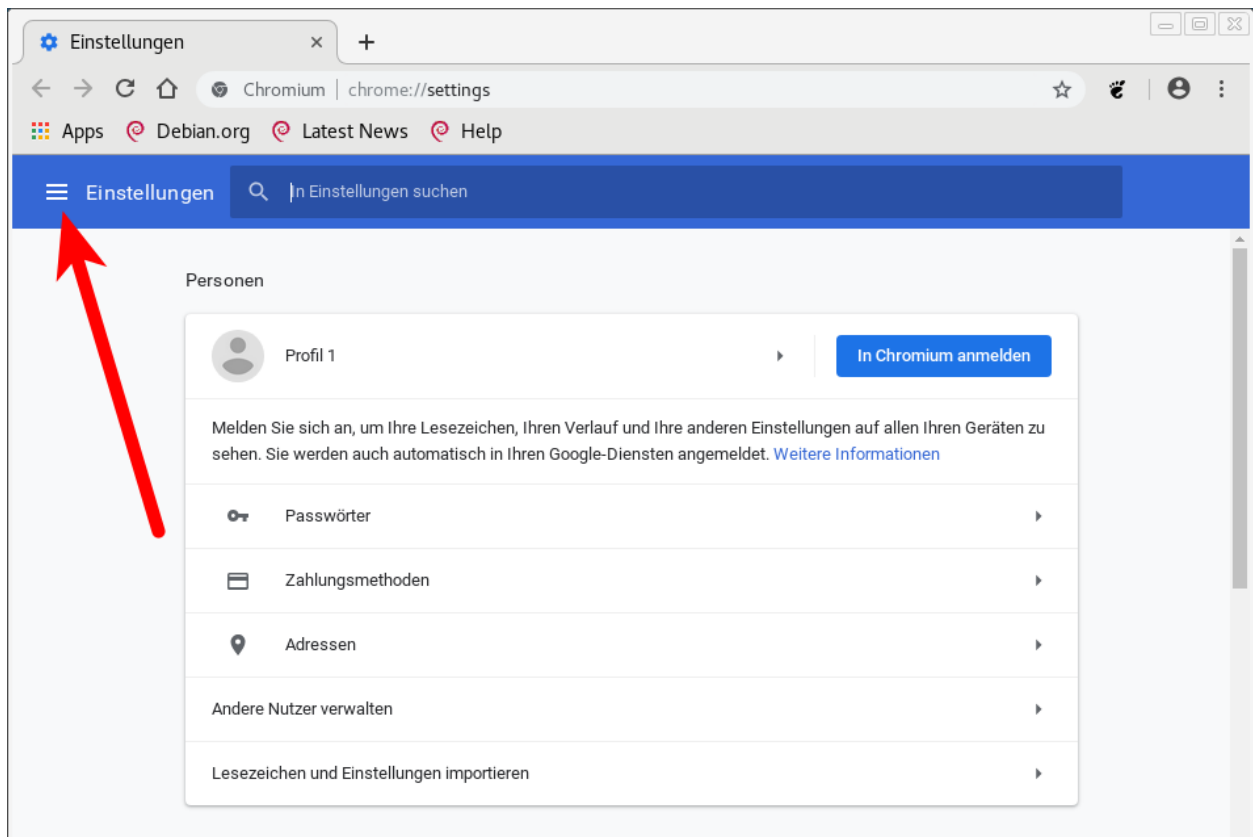
6 Deinstallation aus Chrome/Chromium

Unter Windows verwenden Chrome bzw. Chromium die gleichen Zertifikate wie Edge. Unter anderen Betriebssystemen, wie z. B. Linux, haben Chrome und Chromium eine eigenständige Zertifikatsverwaltung, bei der die Zertifikate wie folgt entfernt werden können:

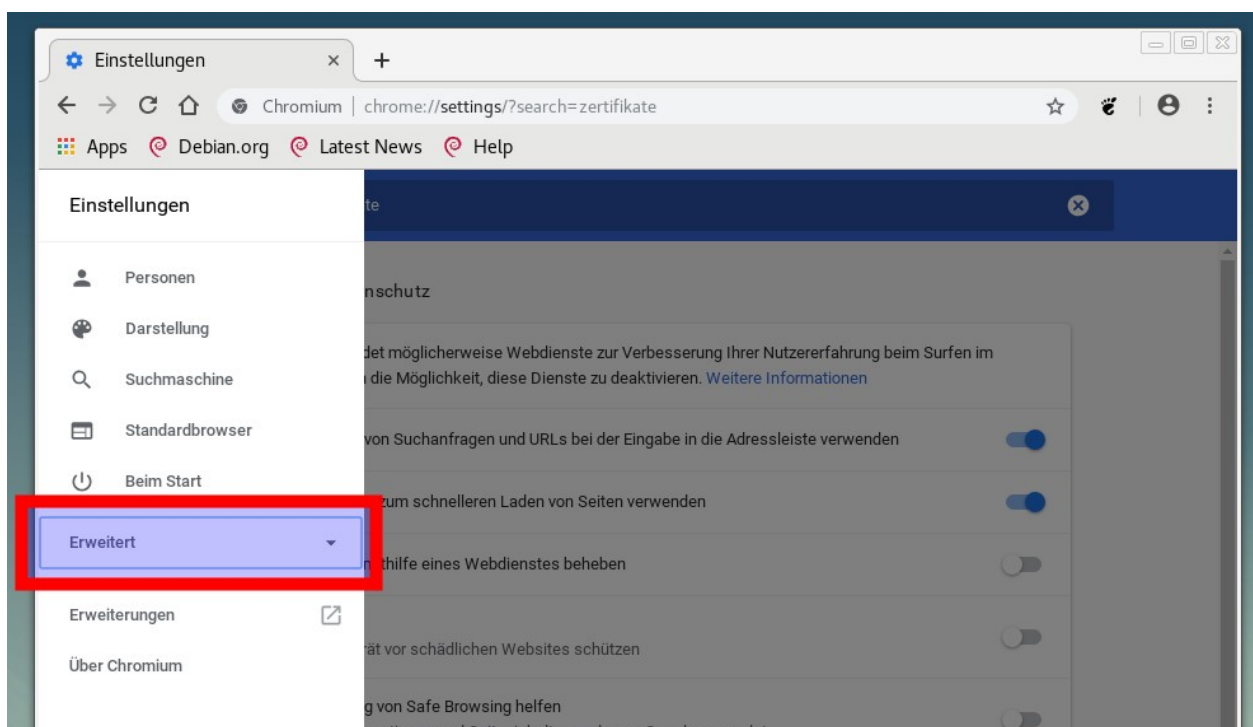
- das Menü (drei Punkte) oben rechts öffnen (1)
- den Menüpunkt «Einstellungen» (2) auswählen



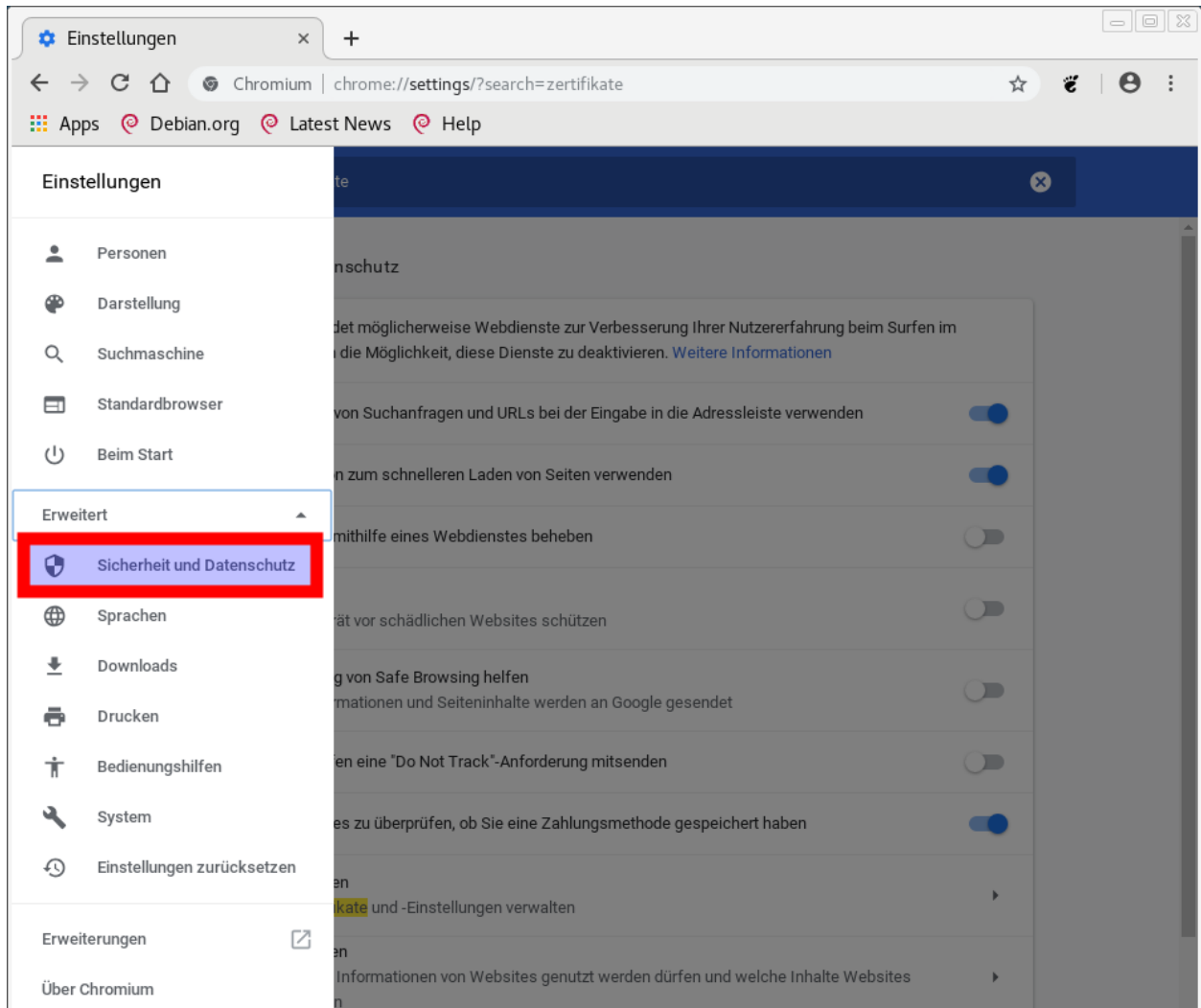
- auf der linken oberen Seite das Einstellungsmenü (drei waagerechte Striche) öffnen



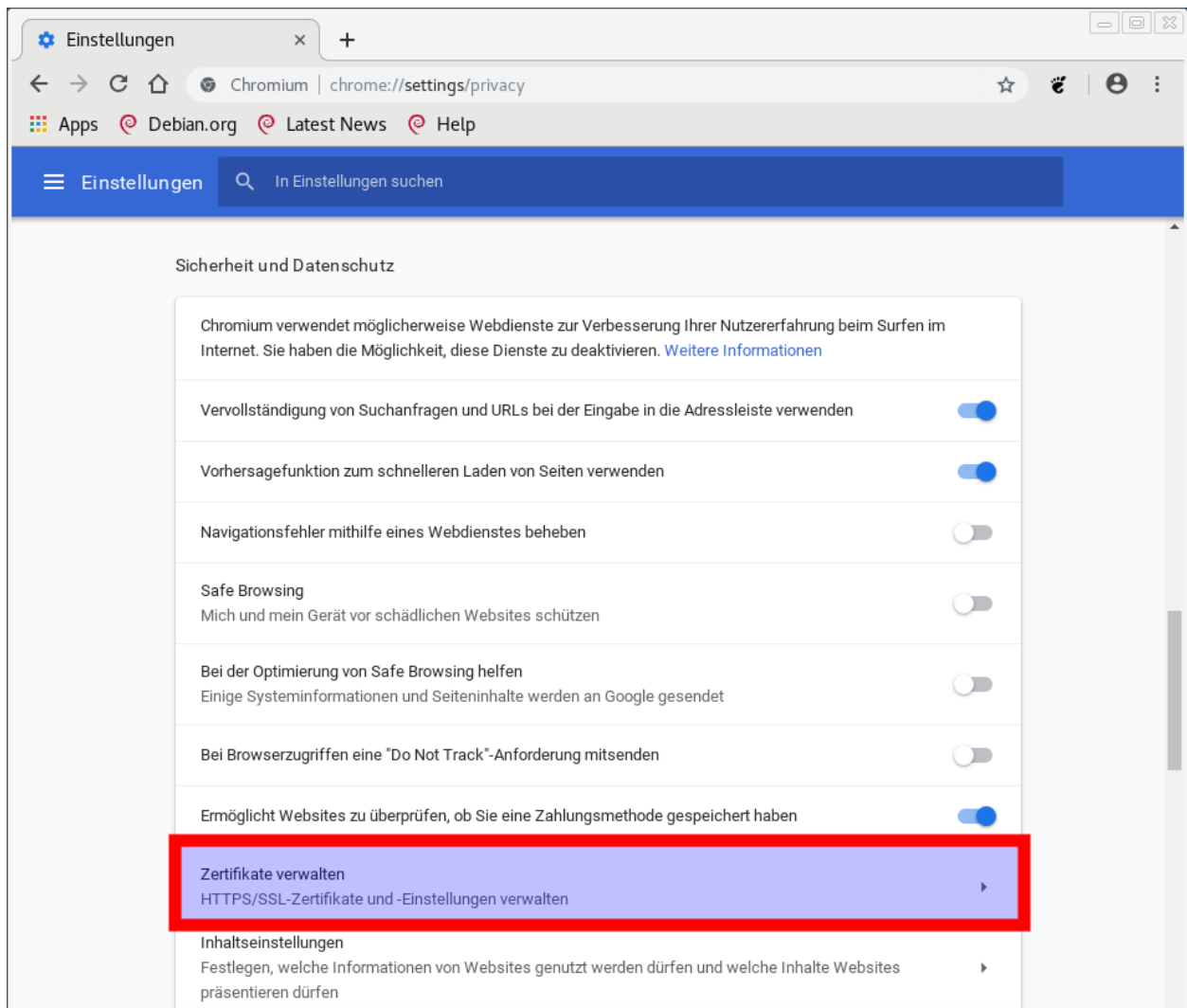
- den Menüpunkt «Erweitert» anklicken



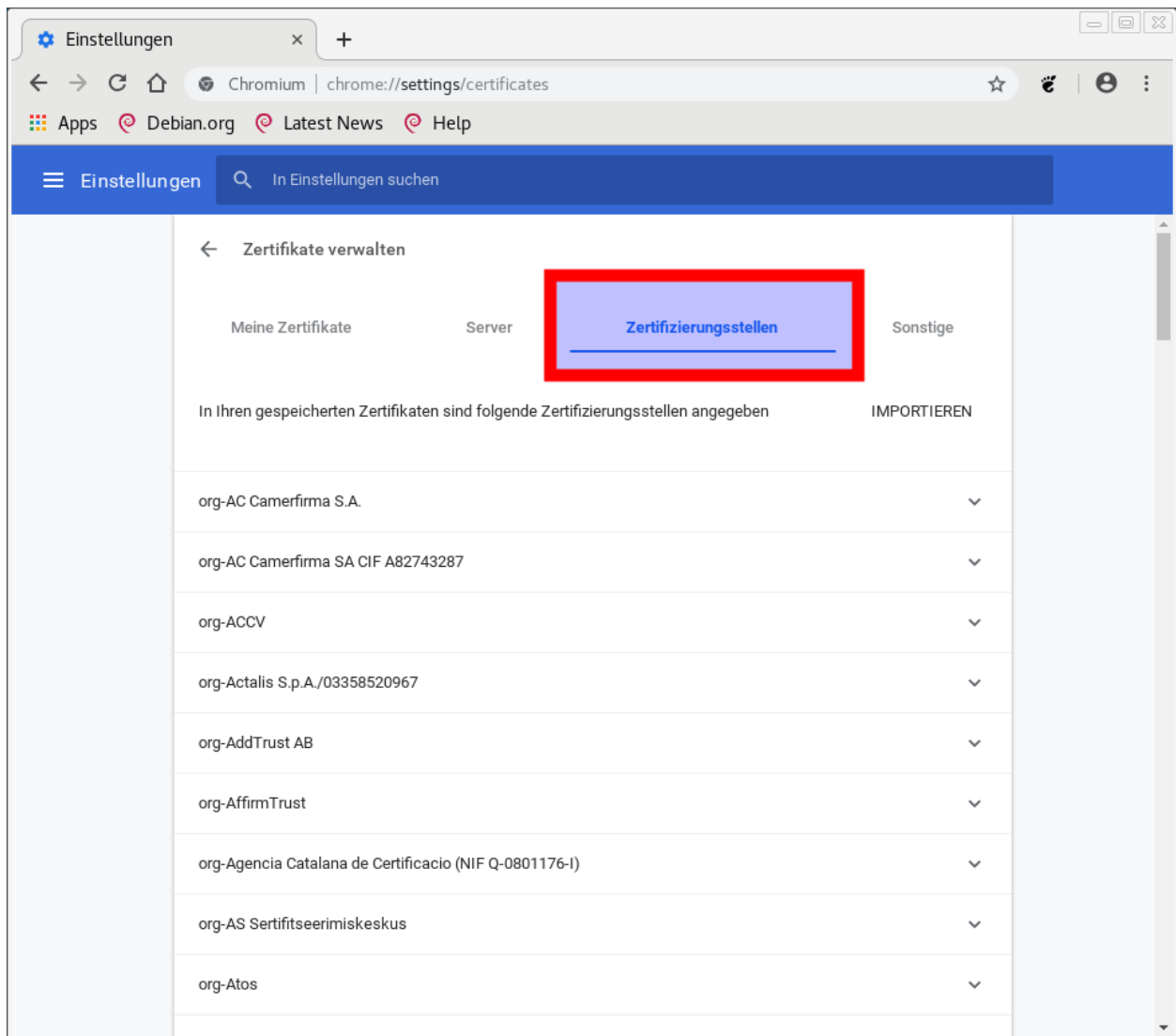
- den Menüpunkt «Sicherheit und Datenschutz» auswählen



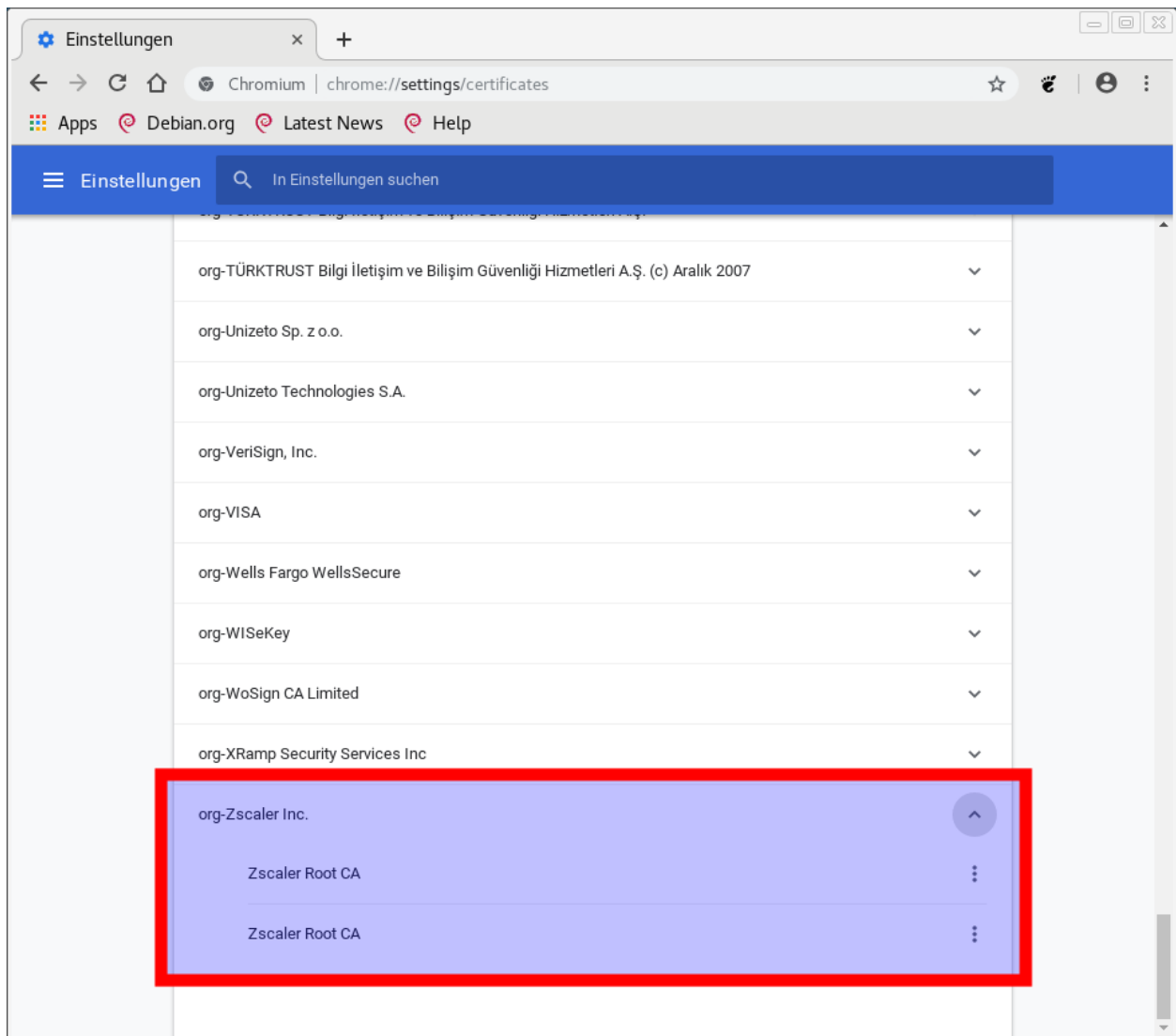
- den Menüpunkt «Zertifikate verwalten» anklicken



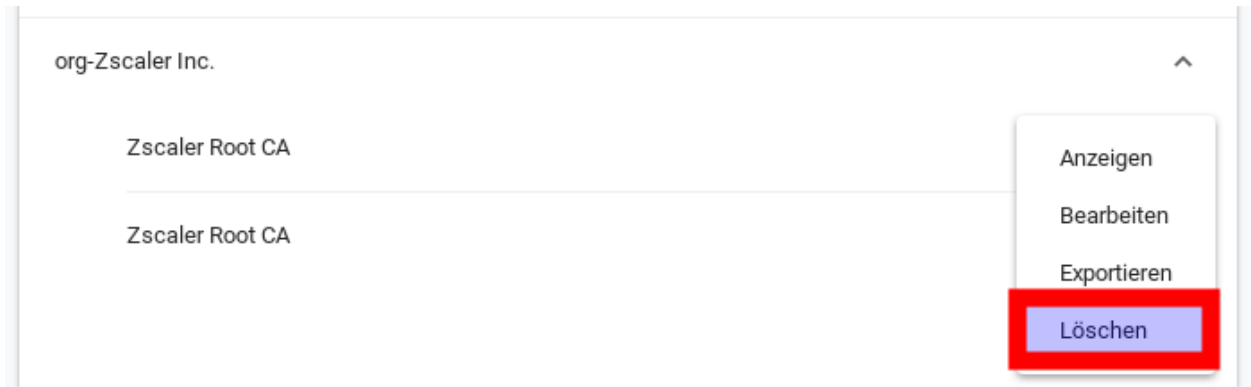
- den Reiter «Zertifizierungsstellen» auswählen



- ganz nach unten zu den Zscaler-Zertifikaten scrollen



- jeweils die drei vertikalen Punkte auf der rechten Seite neben den Einträgen «Zscaler Root CA» anklicken und den Menüpunkt «Löschen» auswählen



- die Warnung durch Drücken auf den «OK»-Knopf bestätigen

