h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

IT-DIENSTE UND -ANWENDUNGEN

Zentrale Serverdienste

Installationsanleitung für die h_da Zertifikate

Dokumentennummer: IT-ZSD-008

Version 1.4
Stand 14.03.2016

Historie

Version	Datum	Änderung	Autor
1.0	22.10.2008	Dokument angelegt	tbo
1.1	08.01.2009	Aufnahme weitere Browser	tbo
1.2	12.01.2009	Aufnahme weitere Browser	tbo
1.3	23.05.2013	Anpassungen an neue URLs, Entfernen veraltete Browser	Tst
1.4	14.03.2016	Anpassung der Vertrauensstellung unter Mac OS X	cma

Inhalt

1 Vorbemerkung zu Server-Zertifikaten

1.1 Grundsätzliche Funktionalität

Server-Zertifikate dienen dazu, die Authentizität von Servern zu bestätigen. Dazu wird auf dem Server ein privater Schlüssel erzeugt, mit dem die Zertifikats-Anforderung verschlüsselt wird.

Dieses Zertifikat wird dann von einer sogenannten CA (Certification Authority) unterschrieben und auf dem Server mit der Unterschrift abgelegt.

Genau dieses unterschriebene Zertifikat präsentiert Ihnen der Server, wenn Sie sich mittels SSL (zum Beispiel beim Surfen) mit diesem Server verbinden.

Das unterschriebene Zertifikat ist quasi der Personalausweis des Servers und die CA kann man als Einwohnermeldeamt verstehen, welches nach Prüfung der Identität diesen Ausweis ausgibt.

1.2 CA-Ketten

Nicht jedes Zertifikat wird direkt von einer im Internet aufgelisteten CA unterschrieben, sondern es kommen hier oft CA-Ketten mit einer hierarchischen Anordnung zum Einsatz.

Am Beispiel der h_da:
- Serverzertifikate werden von der h_da CA unterschrieben.
- Das CA-Zertifikat der h_da ist von der CA des DFN (deutsches Forschungsnetz) unterschrieben.
- Das CA-Zertifikat des DFN ist von der CA der Deutschen Telekom unterschrieben.

1.3 Prüfung der CA-Zertifikate

Erhält eine Client-Anwendung ein Server-Zertifikat, dann ist in diesem Zertifikat auch eine Information über die CA-Kette, mit der das Zertifikat unterzeichnet wurde, enthalten.

Die Anwendung prüft dann, ob die CA-Zertifikate dieser Kette gültig sind. Dazu sind in allen Anwendungen Listen der weltweit gültigen Root-CA´s (im Fall der h_da die Telekom) enthalten. Ist das root-CA-Zertifikat nicht bekannt, erhält der Benutzer eine Warnung, dass das Server-Zertifikat nicht auf seine Richtigkeit geprüft werden konnte.

1.4 Problematik an der h_da

Dieses Problem ist übereinstimmend an allen deutschen Hochschulen und Universitäten zu finden, da diese bis auf wenige Ausnahmen über die DFN PKI signieren: Ist das Telekom Root Zertifikat in einem Softwareprodukt nicht als vertrauenswürdige CA hinterlegt, so werden Serversignaturen mit einer Warnung quittiert oder die Verbindung verweigert.

Des Weiteren ist nicht jede Software in der Lage, Zertifikatsketten zu prüfen, sondern verarbeitet nur die signierende CA der untersten Stufe (h_da CA). Da diese CA dann nicht bekannt ist, erfolgt auch hier eine Warnung zum Zertifikat oder die Verbindung ist nicht möglich.

Zur Behebung dieses Zustands beschreiben wir mit diesem Dokument das Vorgehen, um die Zertifikate in den entsprechenden Produkten zu integrieren.

1.5 Download der Zertifikate

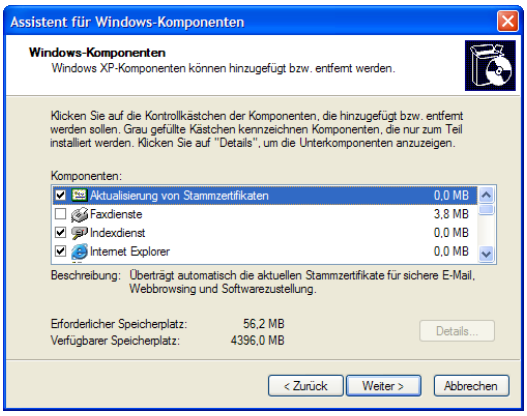
Rufen Sie bitte die Seite **http://wlan.h-da.de** auf. Dort sehen Sie dort rechts die 3 Zertifikate. Laden Sie diese bitte herunter und speichern Sie diese auf Ihrem Rechner ab:

2 Installation der Zertifikate

2.1 Vorbemerkung zu Microsoft Windows / Internet Explorer / Outlook (Express)

In den Microsoft Produkten ist das Telekom Zertifikat bereits enthalten, sofern Sie ein regelmäßiges Update der Stammzertifizierungsstellen durch den Microsoft Update Dienst vornehmen.

Sollten Sie sich hier nicht sicher sein, dann rufen Sie bitte die Systemsteuerung auf und klicken Sie auf „Windows Komponenten hinzufügen oder entfernen“. Dort sollten Sie das „Update von Stammzertifikaten“ sehen, das aktiviert sein sollte:



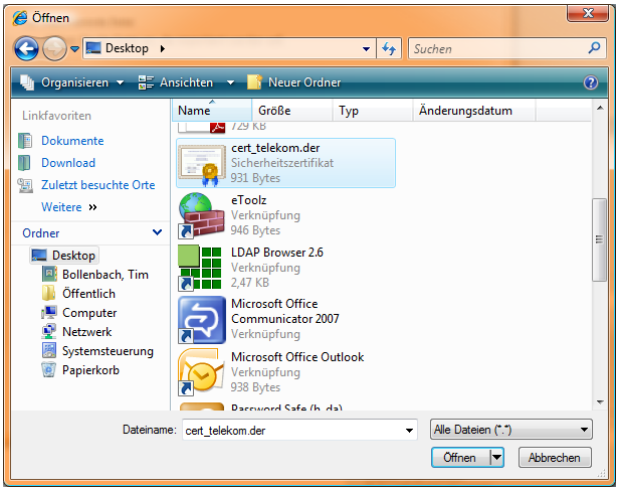
2.2 Installation im Browser

2.2.1 Internet Explorer

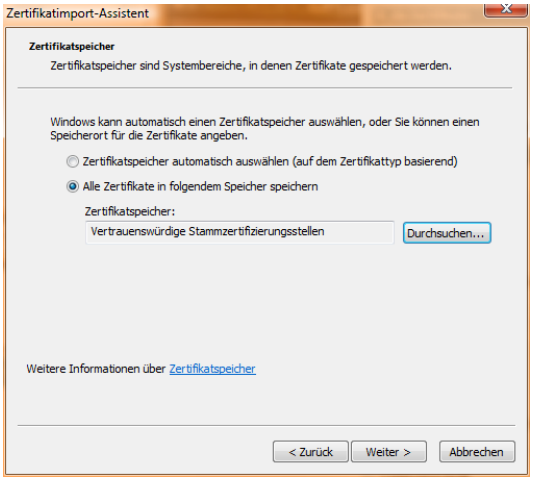
Wie im vorherigen Kapitel erwähnt ist die Installation normalerweise nicht notwendig, so lange nur https-Seiten aufgerufen werden sollen. Sind jedoch andere Komponenten (z.B. Citrix ICA Client) betroffen, welche ihre Informationen aus dem Windows Zertifikatsspeicher beziehen, ist ggf. eine Installation der Zertifikate sinnvoll.

Rufen Sie bitte im Internet Explorer die **Internetoptionen** auf und wechseln Sie zur Registerkarte „**Inhalte**“. Klicken Sie dort auf „**Zertifikate**“. Klicken Sie auf „Importieren“:

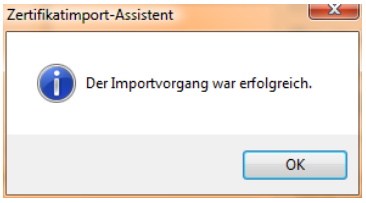
Klicken Sie auf „**Weiter >**“. Klicken Sie auf „**Durchsuchen**“ und wählen Sie ein heruntergeladenes Zertifikat aus (wiederholen Sie diesen Schritt **für alle 3 Zertifikate**). Ggf. müssen Sie noch beim Dateityp „**Alle Dateien**“ einstellen:



Klicken Sie auf „**Weiter >**“. Aktivieren Sie die Option „**Alle Zertifikate in folgendem Speicher speichern**“, klicken Sie auf „**Durchsuchen ...**“ und wählen Sie „**Vertrauenswürdige Stammzertifizierungsstellen**“ aus:

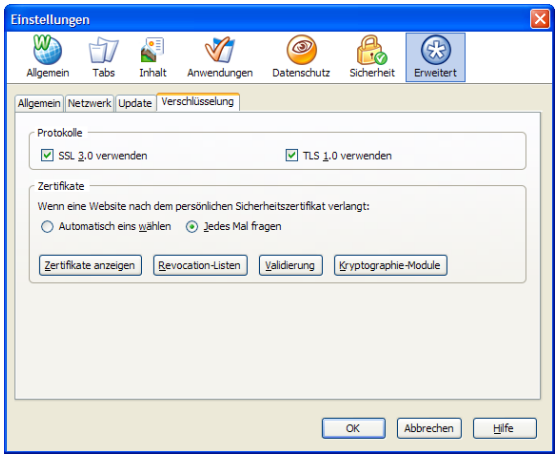


Klicken Sie auf „**Weiter >**“ und im Bestätigungsdialog auf „**Fertig stellen**“. Es sollte folgende Meldung erscheinen:

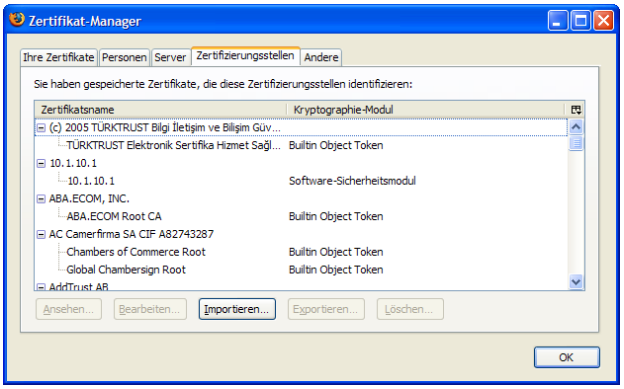


2.2.2 Mozilla Firefox

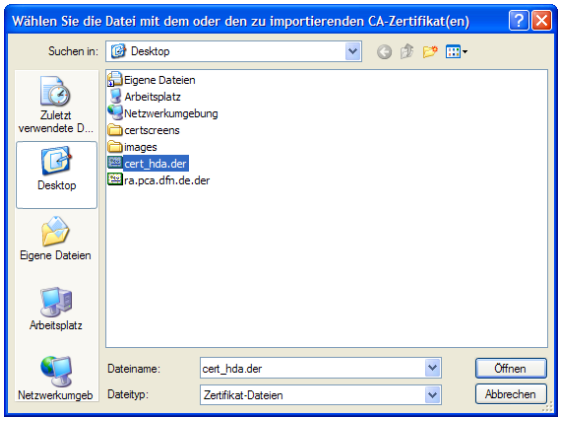
Rufen Sie bitte die Firefox-Einstellungen auf und wechseln Sie zur Registerkarte „**Erweitert**“, dort auf „**Verschlüsselung**“:



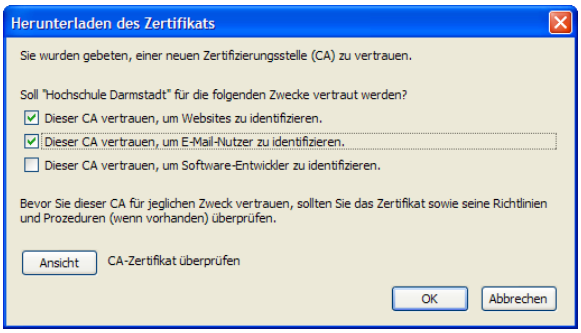
Klicken Sie auf „**Zertifikate anzeigen**“:



Klicken Sie auf „**Importieren**“ und wählen Sie die zuvor abgespeicherten Zertifikate aus (wiederholen Sie also die Schritte für alle 3 Zertifikate):



Setzen Sie bei der Rückfrage die ersten 2 Haken und bestätigen Sie mit „**OK**“:



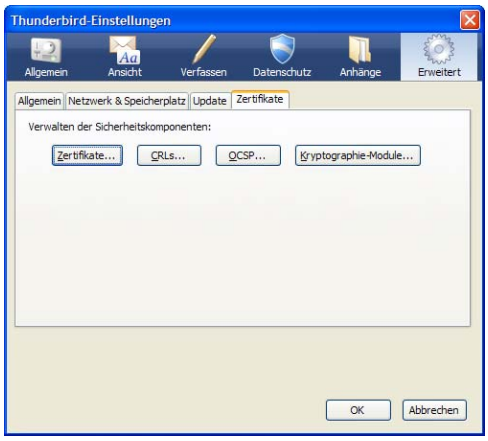
2.2.3 Google Chrome

Rufen Sie bitte die Optionen des Chrome Browser, dort die **erweiterten Optionen** und dort „**Zertifikate verwalten**“ auf. Ab diesem Punkt können Sie die Anleitung zu „**Internet Explorer**“ verwenden, da Chrome auf den Zertifikatsspeicher des Internet Explorers zurückgreift.

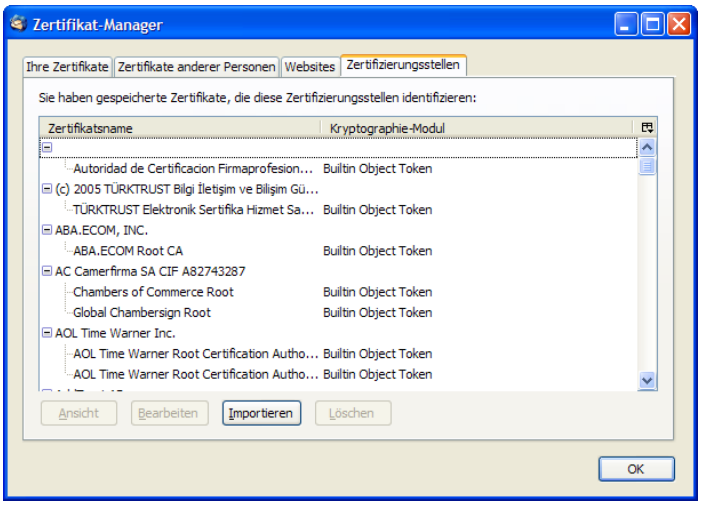
2.3 Installation im E-Mail-Client

2.3.1 Mozilla Thunderbird

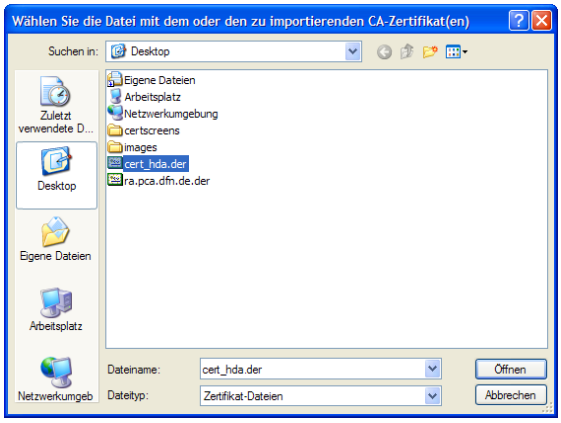
Rufen Sie bitte die Thunderbird-Einstellungen auf und wechseln Sie zur Registerkarte „**Erweitert**“, dort auf „**Zertifikate**“:



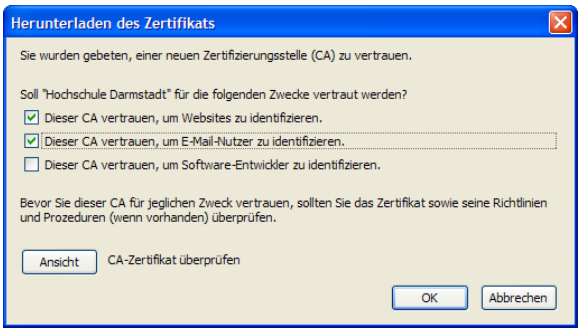
Klicken Sie auf „**Zertifikate**“:



Klicken Sie auf „**Importieren**“ und wählen Sie die zuvor abgespeicherten Zertifikate aus (wiederholen Sie also die Schritte für alle 3 Zertifikate):



Setzen Sie bei der Rückfrage die ersten 2 Haken und bestätigen Sie mit „**OK**“:

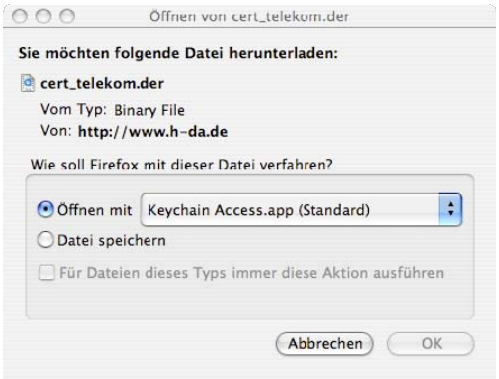


2.4 Installation im Betriebssystem

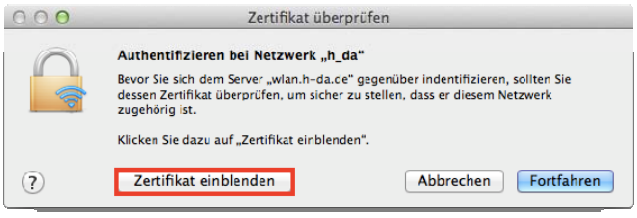
2.4.1 Mac OS X

Rufen Sie bitte die Seite **http://wlan.h-da.de** auf. Dort sehen Sie dort rechts die 3 Zertifikate. Klicken Sie nacheinander auf die 3 Links zu den Zertifikaten:

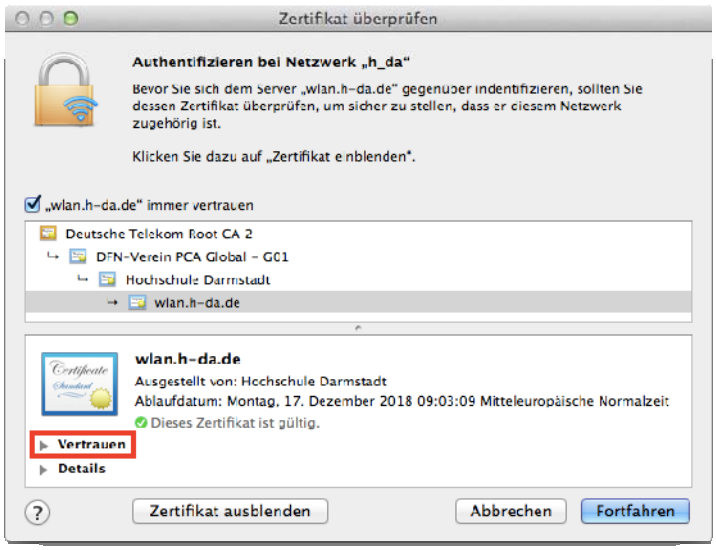
Es sollte folgende Nachfrage erscheinen. Öffnen Sie das Zertifikat dann bitte mit der Keychain Applikation:



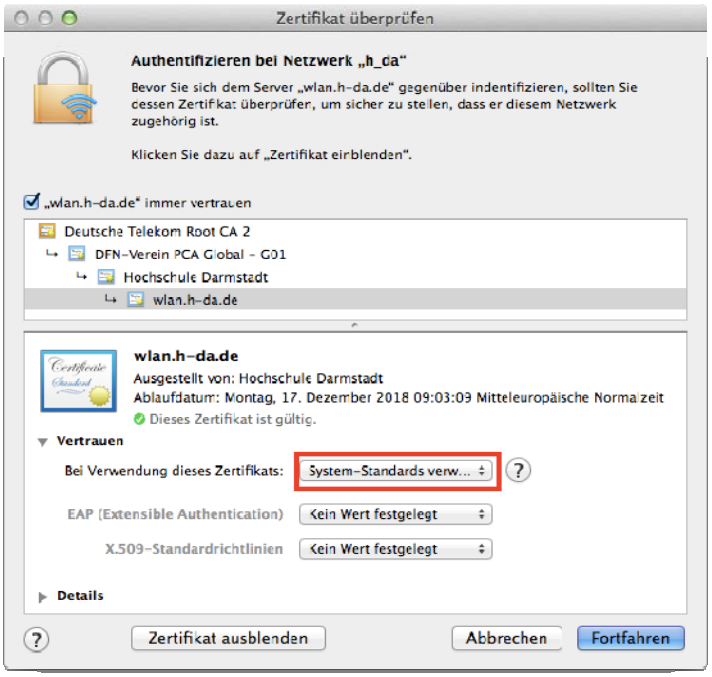
Nun lassen Sie sich das Zertifikat anzeigen:



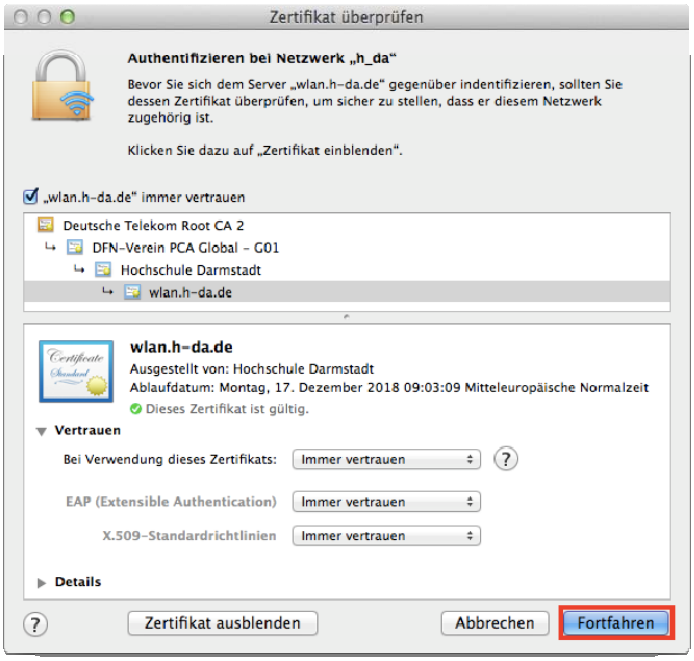
Hier öffnen Sie den Menüpunkt „Vertrauen“ über einen Klick auf das kleine Dreieck:



Im folgenden Menü klicken Sie auf den markierten Bereich und klicken im darauf angezeigten Menü auf den Punkt „Immer Vertrauen“:



Nun klicken Sie auf „Fortfahren“:



Sie müssen die Änderung mit dem lokalen Administratorkennwort bestätigen: