Sehr geehrte Damen und Herren,

am 9.7.2019 läuft das bisher im WLAN der DHBW Karlsruhe (eduroam und DHBW-KA) verwendete Stammzertifizierungsstellenzertifikat „Deutsche Telekom Root CA2“ aus. Daher erhalten die Authentifizierungsserver im WLAN am 28.8.2018 neue Zertifikate, die die Stammzertifizierungsstelle „T-Telesec Global Root Class 2“ als Wurzel haben. Die meisten Benutzer aktueller Betriebssysteme werden die Umstellung kaum bemerken, sie werden lediglich gefragt, ob sie die Verbindung wirklich herstellen wollen. Dabei wird Ihnen ein Fingerprint gezeigt, der wie folgt aussehen sollte:

5f a5 18 a2 a1 dd da 66 08 03 4c d3 ad a8 3b eb bc 4b 51 96 oder
e0 b8 c9 25 c4 fd 5e cd 32 7f 08 df d9 f3 64 61 0e 5d 15 28 oder
f3 45 20 31 cc a3 7c 25 5b bc 46 07 1b e8 ad f8 35 ec c1 0d
Dann ist alles in Ordnung und Sie können die Verbindung herstellen.

Bei etwaigen Problemen ist es am einfachsten, das WLAN-Profil zu entfernen und neu einzurichten. Dabei wird die neue Stammzertifizierungsstelle automatisch erkannt. Eine entsprechende Anleitung finden Sie im Web und im Portal der DHBW (https://portal.dhbw.de/ws/karlsruhe/intern/allgemeinedokumente/WLAN_DHBW-KA_eduroam_Einrichtung.pdf oder https://www.karlsruhe.dhbw.de/fileadmin/user_upload/documents/content-de/Einrichtungen/IT.Service-Center/WLAN-DHBW-KA-eduroam-Einrichtung.pdf). Beachten Sie unbedingt, dass Sie die Benutzerdaten aus der Lehredomäne dh-karlsruhe.de nehmen und nicht die aus der Verwaltungsdomäne dhbw-karlsruhe.aa. Die Verwendung von Verwaltungsaccounts für die Anmeldung im WLAN ist aus Sicherheitsgründen nicht möglich.

Für die Einrichtung von eduroam können Sie das Tool cat.eduroam benutzen, die entsprechende Beschreibung finden Sie ebenfalls im Portal. Sollten Sie cat.eduroam bereits früher benutzt haben, müssen Sie das Tool nach dem 27.08.2018 erneut herunterladen und ausführen.

Hintergrund für Interessierte
Bei der Anmeldung im WLAN müssen Sie einem Server Ihre Benutzerdaten geben. Um sicherzustellen, dass Sie diese Daten wirklich dem richtigen Server zeigen (ein Fakeserver könnte die Daten ja abfangen und missbräuchlich verwenden), muss dieser sich bei Ihrem Client ausweisen. Das tut er mit einem Zertifikat. Nun kann sich jeder ein Zertifikat selbst erstellen. Daher muss das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle signiert werden. Diese Zertifizierungsstelle hat sich geändert.

Mit freundlichen Grüßen

Enrico Hüneborg

Netzteam DHBW Karlsruhe
netz@dhbw-karlsruhe.de