Datenschutzhinweis

Eine an sich bequeme Funktion des Android-Betriebssystems kann unter Umständen Passwörter und sonstige Zugangsdaten in falsche Hände liefern. Lesen Sie, wie Sie diese Möglichkeit deaktivieren.

Hintergrund ist, dass Sie sich im WLAN „eduroam“ mittels ihrer Klinikums-Zugangsdaten (Windows-Benutzername und –Passwort) authentifizieren. Dieser Zugang bietet für Sie auch Zugriff auf weitere Dienste des SMI (SAP, E-Mail, etc.).

Eigentlich hört sich das ganz komfortabel an, jedoch hat die Sache einen entscheidenden Haken: **Bei den meisten Smartphones und Tablets mit dem Android-Betriebssystem ist eine Funktion zur Sicherung der Zugangsdaten und Passwörter standardmäßig aktiviert.**

Diese Daten werden bisher noch im **KLARTEXT** auf den Servern von Google gespeichert, was bei der Diskussion um Datenweitergabe an Geheimdienste eine besondere Note erhält. Hierdurch kann Dritten Zugriff auf sensible Daten Ihres Klinik-Benutzerzugangs gewährt werden, ohne dass Sie davon Kenntnis erlangen.

Bitte passen Sie die Einstellungen Ihres Androiden entsprechend an.

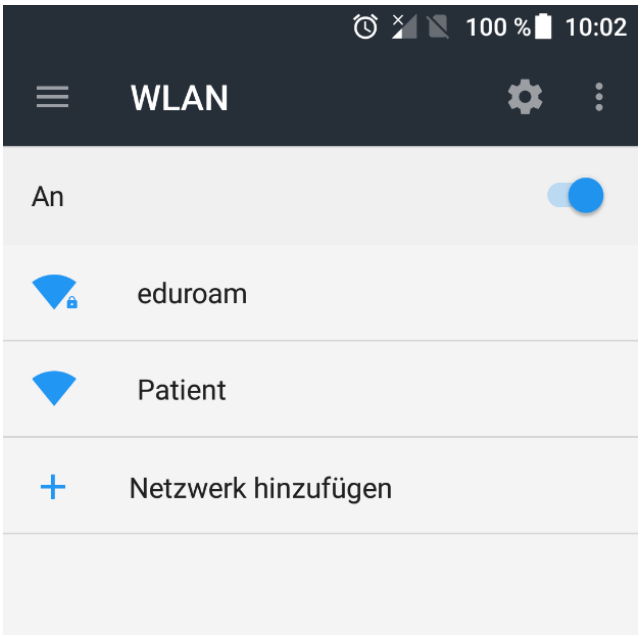
Wo Sie diese Einstellung auf Ihrem Android-Smartphone finden, wird nachfolgend beschrieben:

- **Android 2.x:** Unter "Einstellungen" den Punkt "Datenschutz" auswählen und den Unterpunkt "Meine Daten sichern" deaktivieren.
- **Ab Android 4.x:** Unter "Einstellungen" den Punkt "Sichern und Zurücksetzen" auswählen und den Unterpunkt "Meine Daten sichern" deaktivieren.

TIPP: Legen Sie stattdessen ein Backup auf Ihrem privaten Rechner an. Sinnvollerweise sollten Sie nach der Deaktivierung der Funktion „Meine Daten sichern“ zusätzlich alle auf Ihrem Android-Smartphone gespeicherten Passwörter ändern.

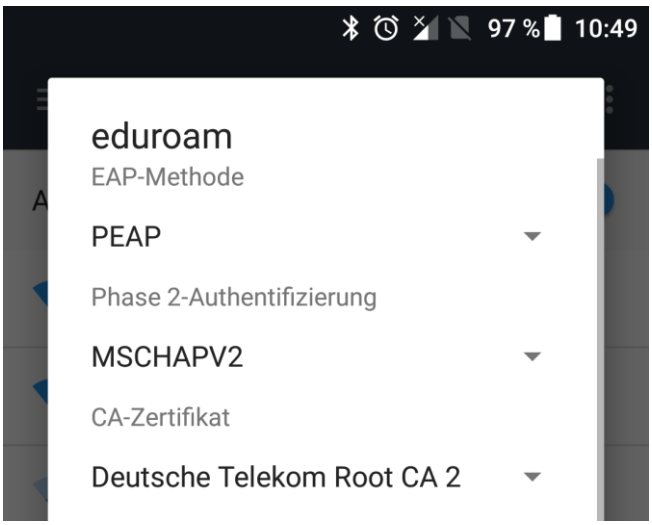
Einrichtung des Drahtlosnetzwerks „eduroam“ ab Android 4.x

1 In den Einstellungen das WLAN „eduroam“ auswählen



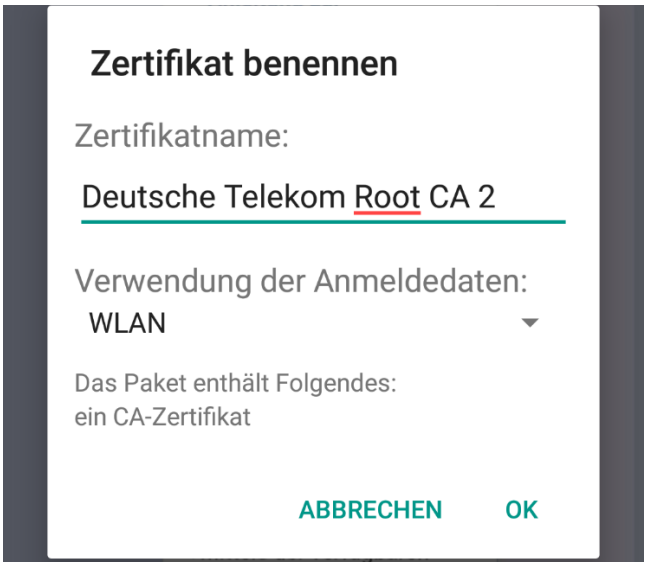
2 Kontrollieren der Authentifizierungsmethode sowie des CA-Zertifikats

EAP-Methode: ***PEAP***
Phase 2-Authentifizierung: ***MSCHAPV2***
CA-Zertifikat: ***Deutsche Telekom Root CA 2*** (Installationshinweis auf der nächsten Seite)



Wieso brauche ich dieses Zertifikat?
Nur so hat Ihr Android-Smartphone die Möglichkeit die Authentizität des UKW-Anmeldeservers zu überprüfen. Ist die Echtheit verifiziert, werden anschließend die Benutzerdaten übertragen.
Ist dieses Zertifikat nicht hinterlegt, könnte sich theoretisch ein technisch versierter Angreifer in die Kommunikationskette zwischen Android-Smartphone und UKW-Anmeldeserver schalten und die Benutzerdaten abgreifen.

Hinweis zur Installation des CA-Zertifikats:
Das Zertifikat „Deutsche Telekom Root CA 2“ via des Browsers Google Chrome auf das Android-Smartphone heruntergeladen. Anschließend startet automatisiert eine Zertifikatsinstallationsroutine, welche nachfolgend mit der notwendigen Konfiguration gezeigt wird:



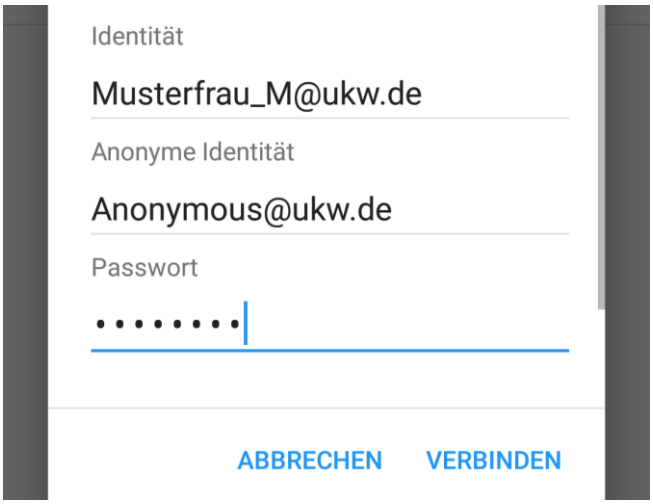
3 Benutzername und Passwort eingeben

Der Benutzername und das Passwort sind identisch mit der normalen Windows Anmeldung am UKW, es muss lediglich beim Benutzernamen der Zusatz **@ukw.de** mit angehängt werden.

Identität: *Musterfrau_M*@ukw.de
Passwort: *„Windows-Passwort“*

Um die Sicherheit der Datenübertragung zu erhöhen, wird empfohlen zusätzlich eine anonyme Identität zu verwenden.

Anonyme Identität: ***Anonymous*@ukw.de**



4 Erweitere Optionen kontrollieren

Für die dynamische IP-Adresszuweisung muss die Option **DHCP** aktiviert sein.