eduroam und der Ablauf des DT Root CA 2 Zertifikats

Einleitung

- (vgl. Vortragsfolien https://owncloud.gwdg.de/index.php/s/RNEru01vpcmIk4W und die Zusammenfassung von Christian Strauf auf https://www.dfn.de/fileadmin/3Beratung/Betriebstagungen/BT67/BT67_MobileIT_FreeRADIUS_Migration_Neue_DFN_CA_Strauf.pdf)
- Was ist eigentlich das Problem? Root-CA (DT Root CA2) läuft 2019 aus. Neue Root-CA und neue DFN-PKI (ist schon da) muss benutzt werden.
- Was erwarten wir von dieser Diskussion? Sammeln von Ideen und Migrationswegen.
- Was passiert, wenn man die RADIUS-Zertifikate auf den RADIUS-Servern tauscht und die neuen Zertifikate mit der neuen CA signiert sind?
    - Alle Endgeräte, die auf die alte CA prüfen, können sich nicht mehr anmelden.
    - Testplan:
        - In welchem Zertifikatsspeicher liegen Root-CA-Zertifikate?
        - Wie wird ausgewählt, welchen Root-CA-Zertifikaten für die 802.1x-Authentifizierung getraut wird?
        - Werden Server-Namen festgelegt?
        - Können Endgeräte mit Cross-Signed Intermediates umgehen? (Cross-Signed DFN Intermediate liegt vor)
        - Kann das CAT-Tool multiple CA eintragen?
- Vermutlich: Es müssen alle Clients angefasst werden?
- Zusätzlich wichtig: Der Vertrag mit der T-Systems *für die neuen PKI-Zertifikate könnte auch vor 2038 ablaufen.*

Mögliche Auswege

Cross-Signed Zertifikat

- Getestet von R. Paffrath: funktioniert mindestens nicht auf Android und iPhone

Alternativen zu TTLS und PEAP

- EAP-pwd bisher nur auf ANDROID/Linux und Windows (Entwicklung erforderlich)
    - Klartext-Passwörter notwendig (zukünftig nicht mehr, neuere wpa_supplicant-Releases werden auch mit Hashes arbeiten können).
    - Eigenes Passwort für eduroam?
- EAP-TLS (ggf. komplexer für Nutzer)
    - Eigene PKI / DFN PKI?
    - Root-CA kann auch ablaufen.

User-Weichen die zu 'neuem' TLS-Tunnel führen

- Neuer Realm @edu2.alter-realm.foo [Implementierung ggf. analog zu den Bsp unten]
- Neue anonyme Identität 'eduroam2@realm' [Erste Bsp-Implementierungen, siehe unten]
- Vorteil:
    - Ermöglicht Parallelbetrieb.
    - Wie bekommt man alle neuen User dazu, die neue Variante / das CAT-Tool zu verwenden?
        - Flag für neue Nutzer im IDM/LDAP/AD, der im Radius geprüft wird?

        - neue User dürfen NUR noch dieses Wort als äußere Identität bzw diesen neuen Realm verwenden
        - Sorgt auch dafür, dass die Automatismen von iOS und Win 8+ nicht mehr funktionieren
        - Mehr Support-Aufwand...

Radius vorschalten und beide Certs probieren

- Geht das?
- sk: Angeblich gibt es Zertifikatswarnungen analog zu verschiedenen Certs auf den Fallback-Radius'

App entwickeln. Neue Carrier Settings kann ich doch auch erhalten.

- App für Geräte entwickeln, die die eduroam-Einstellungen remote ändert.

Status Quo Endgeräte-OS

- Windows:
    - Wenn CAT-Tool verwendet wird, wird die CA fest ausgewählt.
    - Multiple CA aber möglich
    - Vollständiger CN kann angegeben werden
    - TODO:
        - Kann man zweite Root-CA im CAT mitgeben?
- macOS:
    - kein Cross-Signed
    - TODO:
        - Kann man zweite Root-CA im CAT mitgeben?
- iOS:
    - Siehe macOS.
- Linux:
    - NetworkManager
        - CAT-Tool muss angepasst werden
        - Multiple CA möglicht
        - Vollständiger CN kann angegeben werden
    - EAP-PWD (stabil)
- Android:
    - kein Cross-Signed
    - Ab 7.1: System Zertifikatsspeicher für WLAN-Konf auswählbar
        - Abhängig vom Hersteller auch in Vorversionen.
    - EAP-PWD (stabil)
    - Vollständiger CN kann angegeben werden

Implementierungen einiger Ideen

(Ohne Gewähr, aber getestet!)

Anonyme-Identität - User-Weiche

Mit radsec-proxy und 2 (beliebiger Hersteller) Radius-Instanzen -- von Ralf Paffrath (DFN)

1. Bisherige Radius Server Konfiguration klonen.

2. Dem geklonten Server die neue DFN-PKI verpassen, also neues Server - Zertifikat unter der neuen DFN-PKI Generation 2 und die UDP Ports für Radius Kommunikation anpassen, also beispielhaft statt 1812 1912 und anstatt 1813 1913.
3. radsecproxy konfigurieren:

....

```
###### neue PKI #######
server radius-107-new {
      host ip-addresse
      type udp
      secret foryoureyesonly
      port 1916
}
server radaccount-107-new {
      host
      type udp
      statusServer on
      secret hugo
      port 1917
}
#### End neue PKI ####
```

und den Realm Eintrag aber vor den SubRealm, also:

```
realm /newPKI@NameDerEinrichtung\.de$/ {
    server radius-107-new
    accountingServer radaccount-107-new
}
realm /@NameDerEinrichtung\.de$/ {
      server radius-107
      accountingServer radaccount-107
}
```

Mit Freeradius und 2 verschiedenen EAP-Modul Instanzen -- von Christian Strauf (TU Clausthal)

1. In mods-available/eap die Sektion "eap {}" nach "eap eapoldca {}" kopieren.
2. In mods-available/eap die Sektion "eap {}" so anpassen, dass dort die von der neuen CA signierten Zertifikate verwendet werden.
3. In der Virtual-Server-Konfiguration ('äußere" sites-enabled) folgende Ersetzungen machen:

```
- - - -ALT - - - - -

authorize {
       ...
       eap {
             ok = return
       }
       ...
}


+ + + +NEU + + + + +

authorize {

       if ( &User-Name == "eduroam@einrichtung.de" ) {
             eap {
```

```
                ok = return
            }
        } else {
            eapoldca {
                ok = return }
        }
        ...
}
```

WICHTIG: Man kann die unlang-if-Abfrage nicht in "authenticate {}" machen. Da muss man mit dem Auth-Type arbeiten, der ja durch die Verwendung des korrekten Moduls in "authorize {}" bereits richtig gesetzt ist:

- - - -ALT - - - - -

```
authenticate {
        ...
        eap
        ...
}
```

+ + + +NEU + + + + +

```
authenticate {
        ...
        Auth-Type eap {
            eap
        }
        Auth-Type eapoldca {
            eapoldca
        }
        ...
}
```