



谷歌手机无线8021.x认证报证书认证错误

iMC

Radius

802.1X

张兴龙

2022-01-25 发表

组网及说明

不涉及

问题描述

现场使用谷歌手机做无线802.1x认证 (eap-peap/mschapv2)认证, 认证时报证书认证错误, 故障截图如下:



过程分析

1、查看eia侧证书配置，看是否已导入预置证书，现场已经导入预置证书，且证书校验合法



2、收集uam debug日志，查看对应的debug日志有如下报错，一般这个报错像是客户端服务器内部错误，一般为手机设置问题

```
%% 2022-01-25 13:36:49.768 ; [ERR] ; [36424] ; EAP ; cbTlsInf: [TLS Alert] read:fatal:internal error.
```

```
%% 2022-01-
```

```
25 13:36:49.768 ; [ERR] ; [36424] ; EAP ; cbTlsInf: [cbexit] TLS_accept:failed in SSLv3 read client key exchange A(Ret=0)!
```

```
%% 2022-01-25 13:36:49.768 ; [ERR] ; [36424] ; EAP ; EapTlsAuth.chkSsl: SSL:SSL_read returned -1 SslErrSsl(1).
```

```
%% 2022-01-25 13:36:49.768 ; [ERR] ; [36424] ; EAP ; EapTlsAuth.chkSsl: SSL-Err:error:14094438: SSL routines:ssl3_read_bytes:tlsv1 alert internal error.
```

```
%% 2022-01-25 13:36:49.768 ; [ERR] ; [36424] ; EAP ; EapTlsAuth.chkSsl: SSL-Err:error:140940E5: SSL routines:ssl3_read_bytes:ssl handshake failure.
```

```
%% 2022-01-25 13:36:49.768 ; [ERR] ; [36424] ; EAP ; EapTlsAuth.procHshakeData: SSLread error.
```

```
%% 2022-01-
```

```
25 13:36:49.768 ; [HINT] ; [36424] ; EAP ; EapTlsAuth.oprEapTls: procHshakeData returned FAIL.
```

```
%% 2022-01-
```

```
25 13:36:49.768 ; [WARN] ; [36424] ; EAP ; EapTlsAuth.oprEapTls: unsafe set errno 0xff00050.
```

3、一般eap-peap/mschapv2认证，客户端是可以不验证服务器证书的，只需要EIA侧配置根证书和服务证书即可。但是现场是个谷歌手机，查看该手机官网说明，有如下提示，也就是说从安卓11版本开始，客户端侧不能选择不验证CA证书的选项了，也就是客户端必须有CA证书

对“不验证”的更改和修正

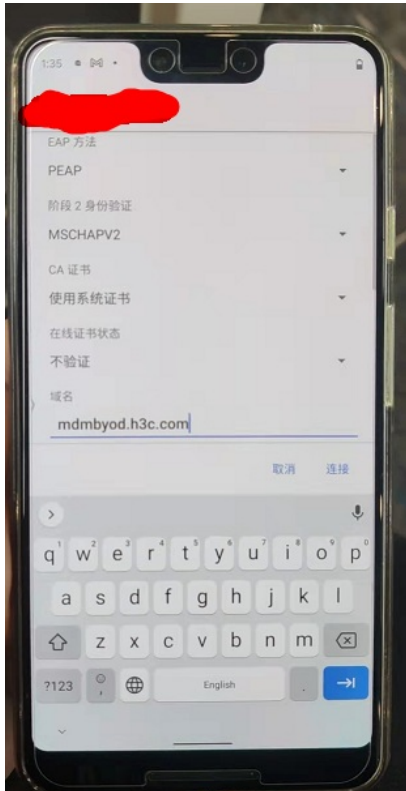
重要提示：出于安全原因，我们移除了 EAP-PEAP、EAP-TLS 和 EAP-TTLS 配置中使用的“不验证”设置选项。在 Android 11 功能更新版本中，此选项已被移除。

4、因为EIA侧的CA证书，是购买的商业证书，现场谷歌手机上已经预置了此证书。因此不需要在额外导入，如果手机没有预置该证书，可以导入eia提供的CA证书，eia提供的CA证书有两级机构（topRoot CA以及ScendRoorCA，两个都需要导入，选择时选择二级CA即可）。

5、现场预置了EIA CA证书后，还是出现证书认证错误，经检查是域名配置错误导致。

解决方法

1、按照下图进行配置，其中域名配置为mdmbyod.h3c.com



2、另外附件附上普通安卓手机的设置方法，其他句点如果有需要也可以参考

附件下载: 安卓手机演示配置视频.rar