

**IETF 90 – RADIUS Extensions WG Meeting**  
**Toronto, 23 Jul 2014 (remote)**



draft-winter-radext-populating-  
eapidentity

# Document Overview



- So you've configured multiple EAP types on a client.
- And you think EAP type negotiation will figure out which one works for any given authentication attempt.
- You're wrong.
- draft-winter-radext-populating-eapidentity lists conditions in which EAP behaviour may not be how you expect it to be ; and suggests workarounds.
- In particular, the EAP-Response/Identity which gets copied into a RADIUS or Diameter User-Name needs special care.

# Example setup



## SUPPLICANT

EAP-AKA'  
User = 1234@...3gpp.org

EAP-TTLS  
User = anon@rälml

TEAP  
User = anon@realm2

EAP-PWD  
User = realname@realm3

## AUTHENTICATOR (+ possibly PROXY)

RADIUS Access-Request  
User-Name = ...

RADIUS Access-Request  
User-Name = ...

## EAP SERVER

EAP-AKA'  
(supported?)

EAP-TTLS  
(supported?)

TEAP  
(supported?)

EAP-PWD  
(supported?)

« Pick any of those usernames for EAP-Response/Identity, EAP type negotiation will figure out which client-side identity matches which supported EAP type on the server » ? FAIL !

# FAIL, Pt. 1



## SUPPLICANT

**EAP-AKA'**  
User = 1234@...3gpp.org

EAP-TTLS  
User = anon@rälml

TEAP  
User = anon@realm2

EAP-PWD  
User = realname@realm3

## AUTHENTICATOR (+ possibly PROXY)

**RADIUS Access-Request**  
User-Name =  
1234@...3gpp.org

**RADIUS Access-Reject**  
(sorry, we don't do  
business with 3gpp.org)

## EAP SERVER

EAP-TTLS  
(supported)

TEAP  
(supported)

EAP-PWD  
(supported)

Supplicant connects to an authenticator which would get him authenticated via TTLS, PEAP, or PWD.

If supplicant chooses to send the « wrong » username, no EAP type negotiation will ever take place → DoS for the user, in spite of having valid credentials.

# FAIL, Pt. 2



## SUPPLICANT

EAP-AKA'  
User = 1234@...3gpp.org

EAP-TTLS  
User = anon@rälml

TEAP  
User = anon@realm2

EAP-PWD  
User = realname@realm3

## AUTHENTICATOR (+ possibly PROXY)

Can't form valid RADIUS  
packet !

## EAP SERVER

EAP-AKA'  
(supported)

EAP-TTLS  
(supported)

TEAP  
(supported)

EAP-PWD  
(supported)

Supplicant chooses username from one EAP-Type ; not UTF-8 encoded (and doesn't have to be).  
Sends it in EAP-Response/Identity  
Authenticator drops – malformed.  
Username might have worked for EAP server – inside TTLS tunnel.  
Never gets this far though → DoS for user, inspite of having valid credentials.

# Solution



- Twofold :
- When EAP terminates with failure, check if more usernames from other configured EAP types are available and not tried yet.
  - If yes, re-start EAP state machine and try that username silently.
  - If no, failure is final, inform user.
- When using username from an EAP type, convert to UTF-8 if necessary when populating EAP-Response/Identity.