

TERENA TF Mobility
20th meeting 20 oct 2009



EAP Tunnel Requirements

- an overview -

What? Why? Where?



- Define a set of criteria which a „proper“ tunneling EAP method **MUST, SHOULD, MAY** possess
- Everyone can then check existing EAP types for their fitness
 - PEAP
 - EAP-TTLS
 - EAP-FAST
- Requirements are defined in the IETF, EMU wg
 - [draft-ietf-emu-eaptunnel-req \(-04\)](#)

The Document



■ Defines

- a set of use cases
 - NEA, method chaining, password auth in tunnel
 - ... and a few more
- requirements for the tunnel (i.e. outer)
- requirements for the tunnel content (i.e. Inner)
- EAP channel binding requirements



Some specific MUST items (outer)



- Server-side authentication
- Identity privacy
- Crypto agility
 - If any one cryptographic algorithm is broken, method must be able to use a different one
 - requires crypto negotiation phase
 - and it has to be done right :-)
- Session resumption



Specific MUST items (inner, binding)



- Request/Challenge response
- Result indication

- EAP Channel Binding support
 - Intertwine inner and outer auth, so that the client can always detect if the two have been unbundled
 - Example: in TTLS-PAP, IdP (= TTLS endpoint) could proxy inner PAP to elsewhere – unprotected
 - PEAP can do channel binding quite nicely
 - Inner MS-CHAPv2 generates keying material
 - Can be „mixed“ with outer, and both have to match



And the winner is...

- ... undefined



- PEAP doesn't seem to be considered (not an IETF protocol)
- EAP-TTLS lacks some features (being worked on, to get on par with the reqs)
- EAP-FAST is closer, but maybe IPR encumbered
 - some even say it's ugly
 - and others say ugliness is irrelevant
 - (and the FAST uptake is SLOW, at least in eduroam :-))





This page intentionally left blank.