S3-010620

Extensible Authentication Protocol (EAP) progress in IETF

Tao Haukka

NOKIA

S3 #21

Sophia

Contents

- EAP SIM Authentication for GSM (Henry Haverinen) draft-haverinen-pppext-eap-sim-02.txt
  - version 02 now
  - Used in WLAN access authentication already
  - New added: IMSI privacy support, new message formatting
- EAP AKA for UMTS (Jari Arkko, Henry Haverinen) draft-arkko-pppext-eap-aka-01.txt
  - draft in PPPEXT wg
  - version 01 now
  - New added: IMSI privacy support, new message formatting
- HTTP Authentication with EAP (Jari Arkko, Vesa Toivanen, Aki Niemi) draft-torvinen-http-eap-01.txt
  - Version 01 now
  - HTTP connections to be authenticated using any of the authentication schemes supported through EAP.

To be presented to next IETF meeting

So far no opponency

The goal is standards or experimental track RFC

Background for EAP

- EAP is originally a Point-to-Point Protocol (PPP) authentication scheme
- EAP supports multiple authentication schemes such as smart cards, Kerberos, Public Key, TLS, One Time Passwords, etc.
- EAP hides the details of the authentication scheme from those network elements that need not know
  - For example in PPP, the client and the AAA server only need to know the EAP type, and the Network Access Server does not
- EAP is currently being used for PPP, Wireless LAN and Virtual Private Network (VPN) authentication

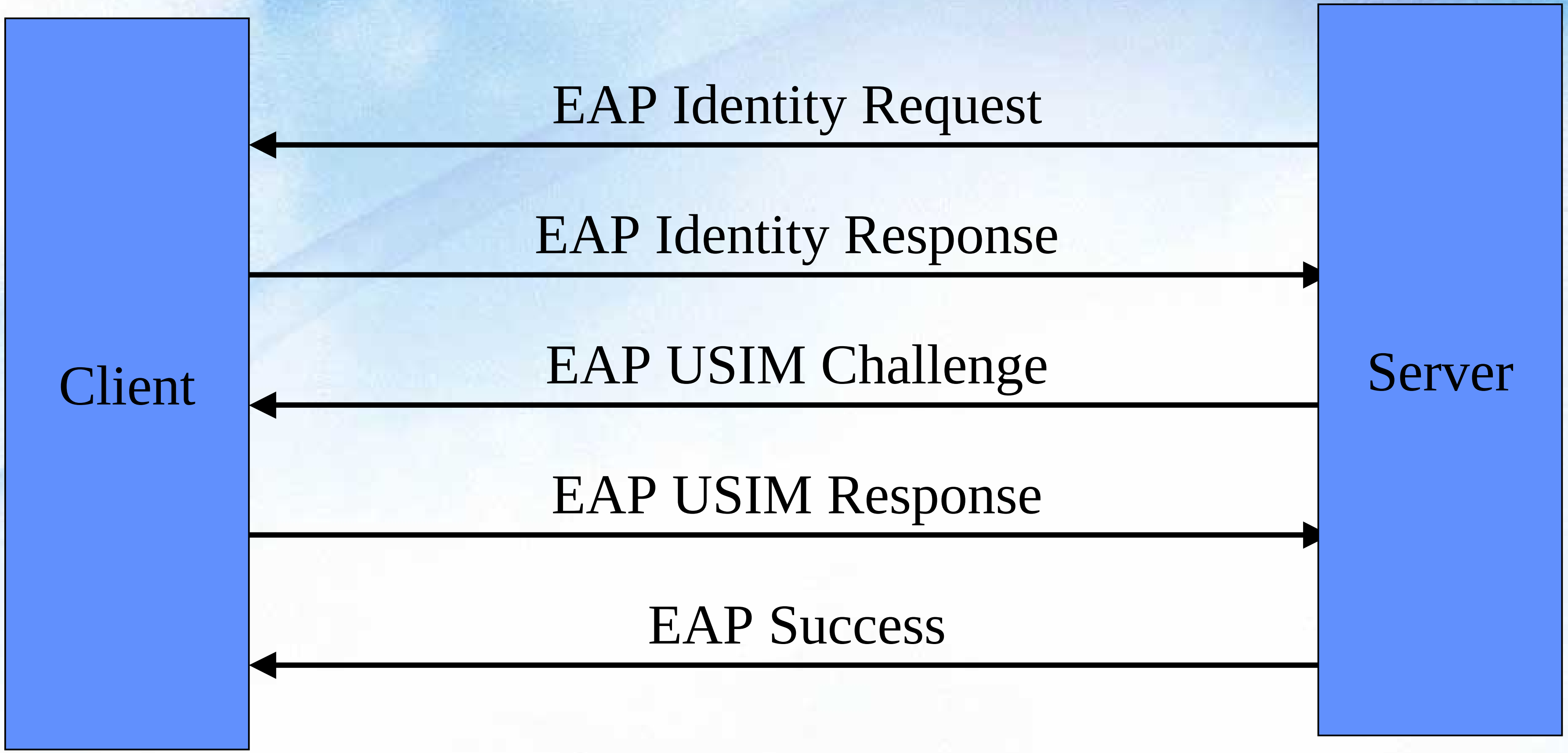
EAP/SIM

- EAP/SIM is an EAP type for GSM authentication
- Can be implemented with an authentication gateway - no other changes required to GSM network
- GSM operator roaming can be used
- Key distribution as part of the authentication procedure
- Enhancements to GSM authentication:
  - EAP/SIM includes a MAC_RAND parameter for mutual authentication and to prevent an active attacker from querying SRES's from the client
  - EAP/SIM can use several GSM triplets at a time for stronger authentication and to generate longer keys
  - IMSI privacy supported
- Usage scenarios: PPP, WLAN access authentication

EAP/AKA

- EAP/AKA is an EAP type for the UMTS Authentication and Key Agreement (AKA)
- EAP/AKA supports all the UMTS AKA scenarios
  - basic authentication, sequence number synchronization etc.
- Similar IMSI privacy support as in EAP/SIM
- EAP/AKA includes GSM compatible mode
  - basic GSM authentication without the enhancements of EAP/SIM
  - The home server knows if this particular user has been given an old GSM SIM or a newer UMTS USIM
  - Client can refuse GSM-only authentication

Basic Message Sequence for EAP AKA



Client

Server

EAP Identity Request

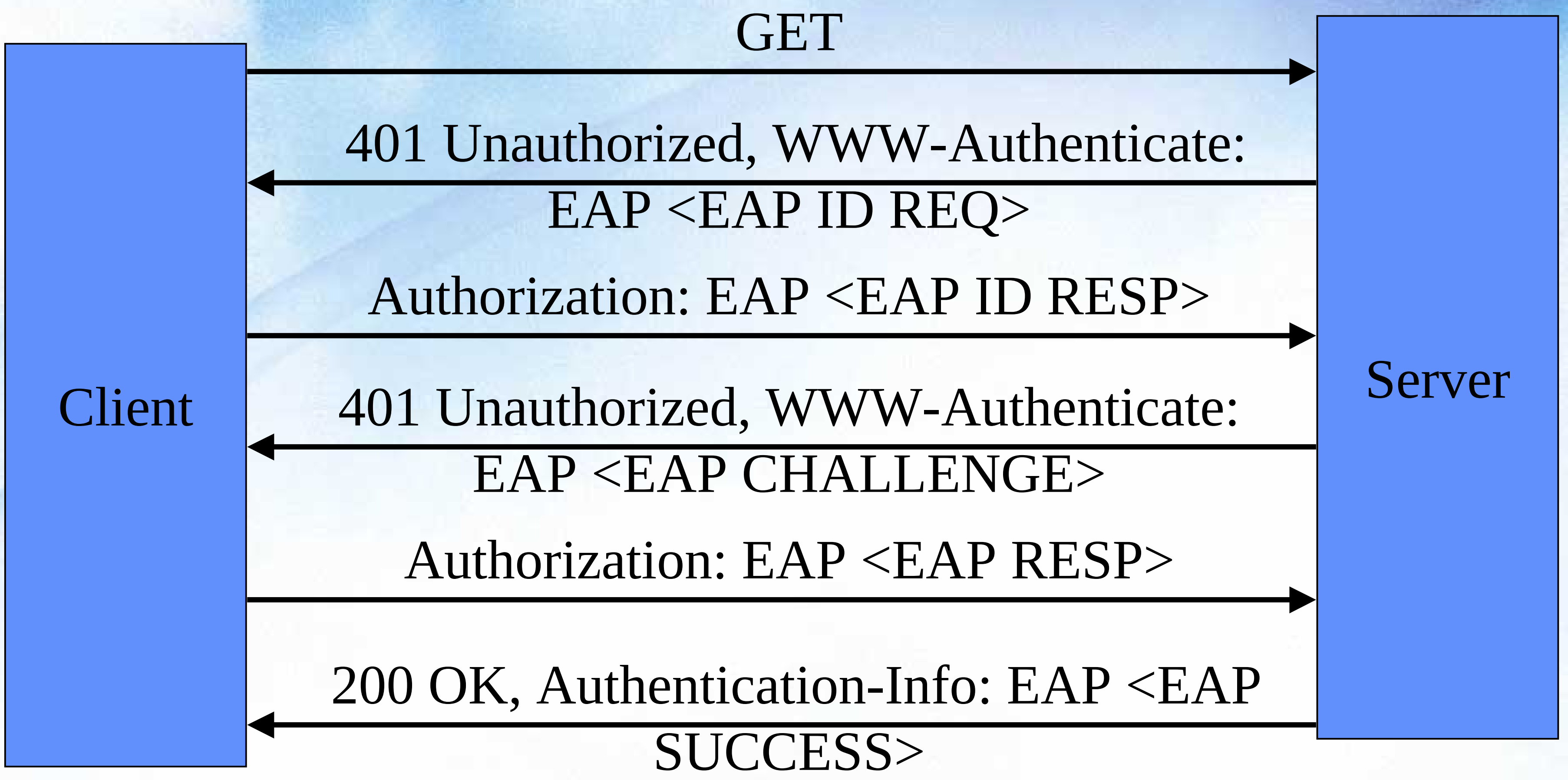
EAP Identity Response

EAP USIM Challenge

EAP USIM Response

EAP Success

Basic Message Sequence for HTTP EAP


GET

401 Unauthorized, WWW-Authenticate: EAP <EAP ID REQ>

Authorization: EAP <EAP ID RESP>

401 Unauthorized, WWW-Authenticate: EAP <EAP CHALLENGE>

Authorization: EAP <EAP RESP>

200 OK, Authentication-Info: EAP <EAP SUCCESS>

EAP messages encapsulate in WWW-Authenticate Response headers and Authorization Request headers

HTTP/EAP

- HTTP EAP provides a flexible authentication scheme for SIP, and allows us to leverage existing EAP methods
- New headers defined for making EAP as an independent HTTP authentication scheme.
  - WWW-Authenticate Response Header, Authorization Request Header and Authentication-Info Response Header
- Each EAP mechanism offers its specific protection schemes for the exchanged credentials.
- HTTP EAP does not inherently provide the integrity protection qualities present in Digest, namely the protection of Request-URI and request-method (and possibly the payload).

The target is to be a work item of the WG

Thank you

Questions?