acticom_802.1x: Authentication in WLAN-based Wireless Access Networks

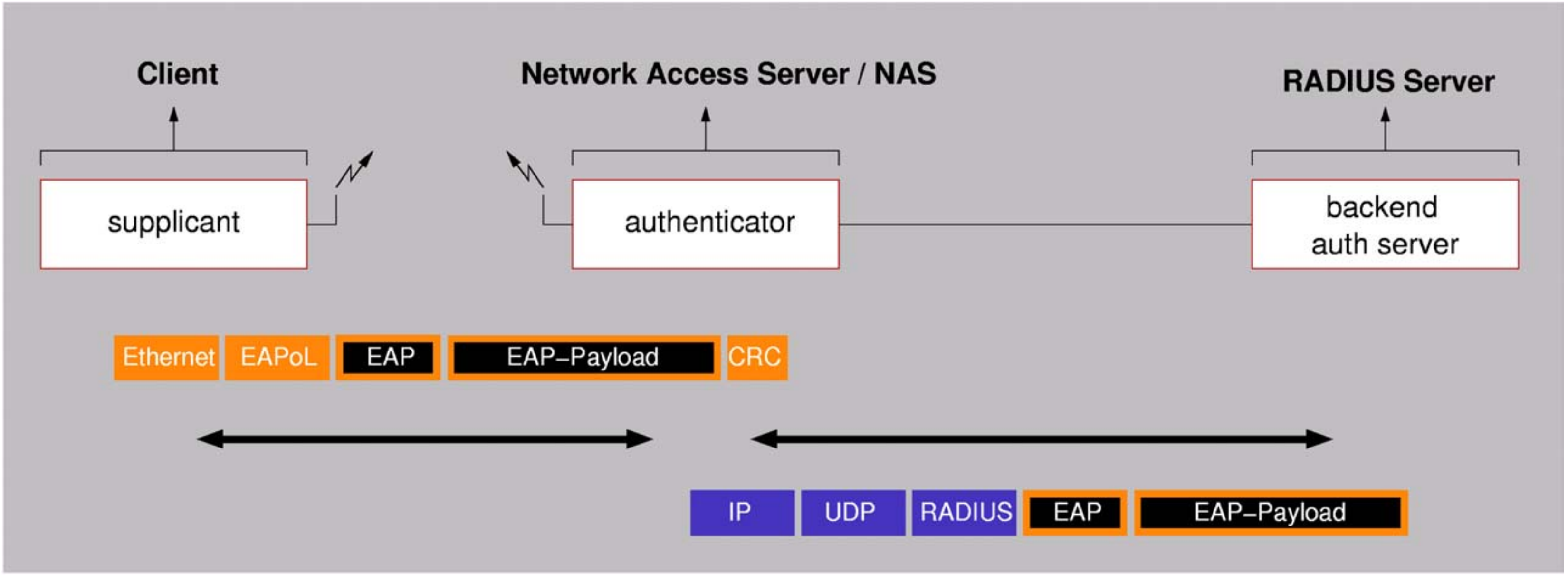
Frank Fitzek
acticom GmbH
Am Borsigturm 42
13507 Berlin
Germany
security@acticom.de

Wireless Authentication

- IEEE802.1x
  - defines authentication of network ports in non-shared 802 media environments
  - devices: supplicant (client), authenticator (network access server) and backend authentication server
    - supplicant (mobile device) requesting service
    - authenticator blocks network access until an exchange of authentication PDUs has succeeded
    - backend authentication server offering authentication information via RADIUS interface
  - authentication container
    - Extensible Authentication Protocol (EAP) defined in RFC2284 to convey arbitrary authentication mechanisms without the need to implement each mechanism on the authenticator

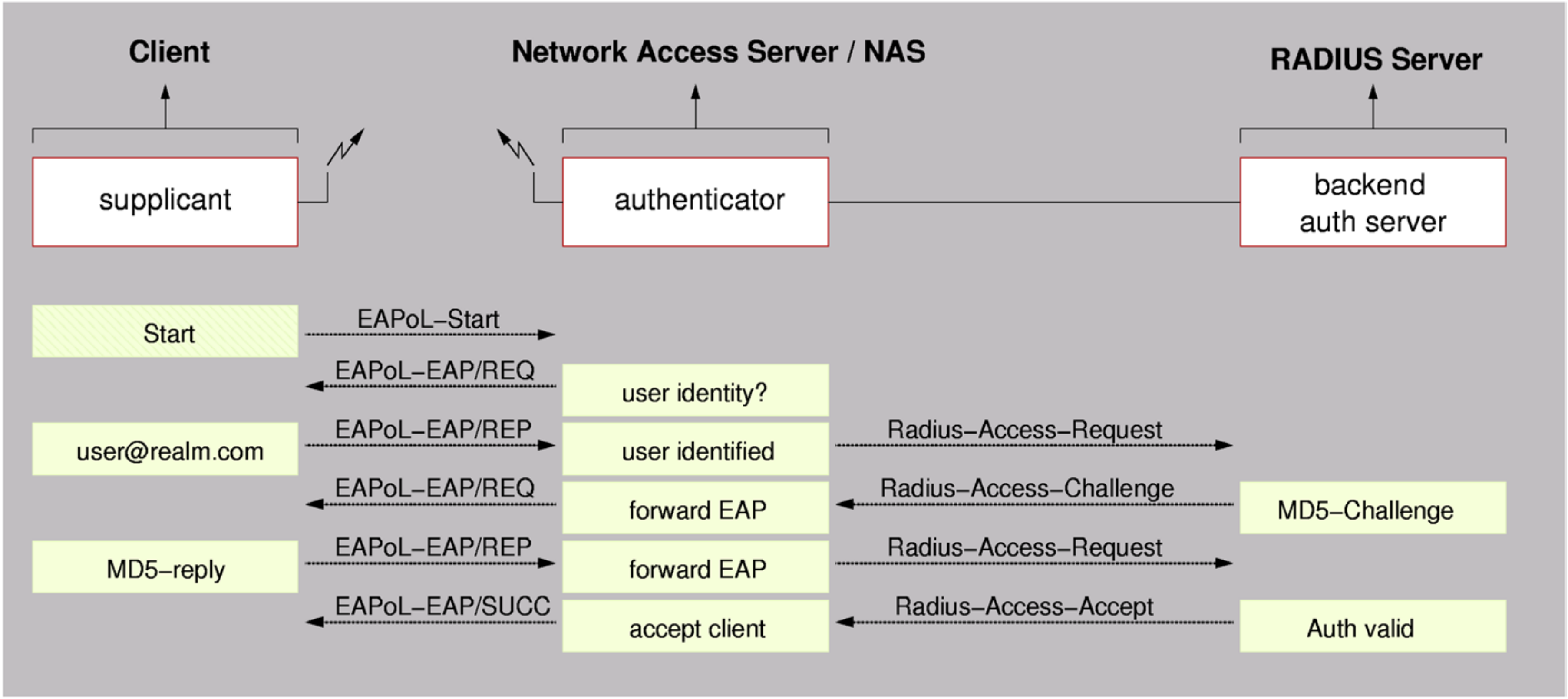
EAPoL/EAP/RADIUS

- Container protocols:
  - EAP-over-LAN (defined in IEEE802.1x standards document) encapsulated EAP messages in ethernet frames
  - EAP over RADIUS (defined in RFC2869) encapsulates EAP messages in RADIUS PDUs



IEEE802.1x example

- Sequence for authenticating a wireless device using MD5 challenge/response

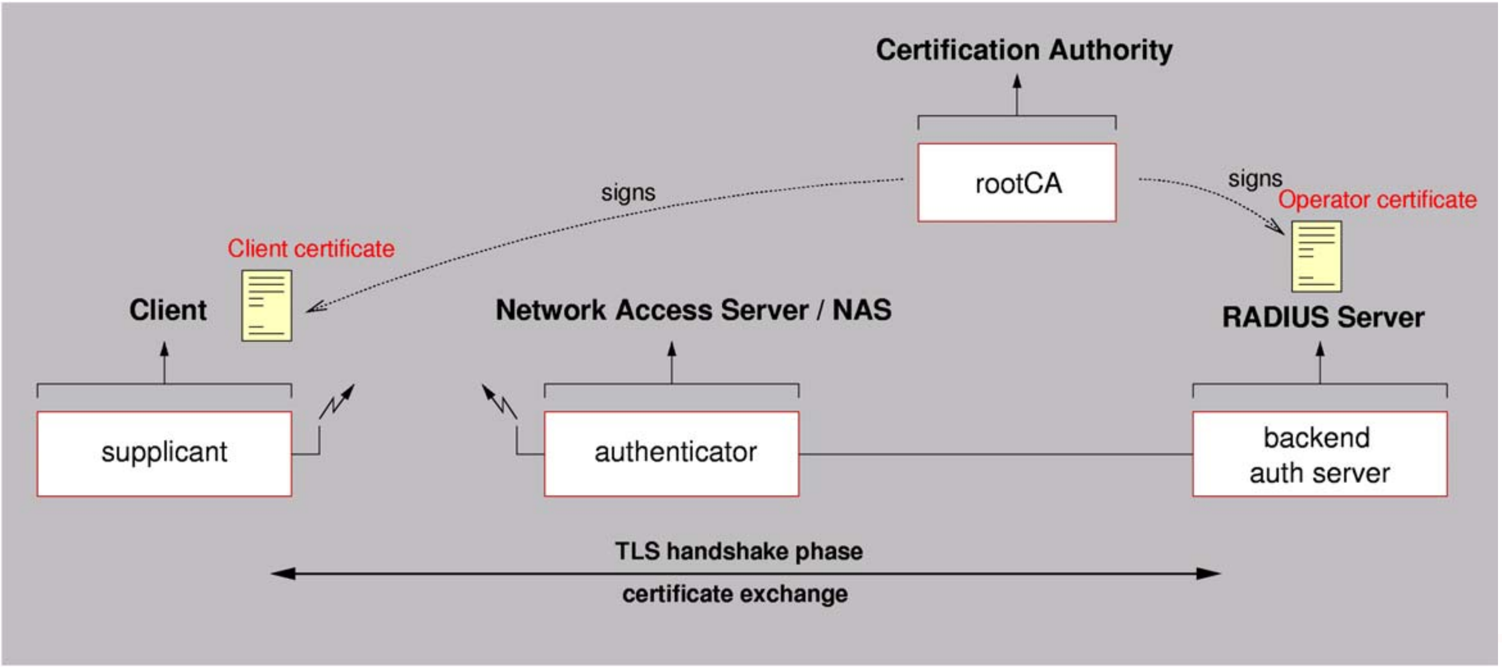


IEEE802.1x and WLAN

- IEEE802.1x/EAP in a wireless environment
  - from a users perspective:
    - offers (re-)authentication without user interaction even when handover events occur
  - from the network operators perspective:
    - uses existing backend authentication infrastructure
    - builtin feature in most WLAN-802.11 hardware equipment nowadays
  - open issues:
    - EAPoL requires encryption on the air interface for secure operation / WEP(2), missing Message Integrity Checks (MIC), think of EAPoL-START/LOGOFF messages (DoS)
    - mutual authentication required to prevent rogue APs from „offering‟ service to customers (data privacy)

EAP-TLS

- EAP-Transport Layer Security
  - Transport Layer Security (TLS - RFC2246) designed to prevent eavesdropping, replay attacks, message tampering, IETF successor to Secure Socket Layer
  - EAP-TLS (RFC2716) defines a mechanism to use TLS handshaking phase for mutual authentication within EAP
  - certificate management required for secure operation, an example:



PEAP

- Protected EAP (PEAP)
  - draft-standard: draft-josefsson-pppext-eap-tls-eap-02.txt
  - extend TLS connection, once encrypted channel is established, start second EAP auth process inside tunnel
  - TLS handshake phase authenticates network operator to customer
  - customer is authenticated in second EAP authentication phase running in TLS connection using any EAP auth mechanism (MD5, Generic Token Card, One-Time-Password)
  - draft posted by RSA, Microsoft, Cisco
  - lightweight on client side, optional hiding of user identity for improved privacy, quick reauthentication, general key generation mechanism for data connections

802.1x/PEAP in WLAN

- Drawbacks of Protected EAP without WEP/WEP2
  - a supplicant leaving a Basic Service Set (BSS) by user interacticon sends EAPoL-Logoff message, authenticator blocks traffic
    - Logoff might be used as a Denial-of-Service attack by third party
    - PEAP connection is terminated once the backend auth server signals success or failure of the auth operation, continue PEAP/TLS-connection until EAPoL-Logoff message has been exchanged ! Handover ?
    - handover events leave the authenticator in state –AUTHENTICATED-, third party might use sniffed MAC address to gain access without being authorized until reauthentication occurs

→ handover **reauthentication gap**

data privacy

- Data privacy
  - integration of WEP/WEP2 and keys generated during TLS connection
    - base station terminates PEAP connection, keying material locally available
    - backend auth server terminates PEAP connection, keying material must be conveyed to base station
      → interface, protocol ?
      problem statement: draft-aboba-pppext-key-problem-01.txt
    - dynamic key management on base stations per station required to separate client devices from each other
  - IP security
    - standardized security mechanism, widely supported
    - integrated on proxying device between authenticator and backend auth server, terminates PEAP connection

www.acticom.de
security@acticom.de

Am Borsigturm 42
13507 Berlin
Germany

The only situation we recommend to be wired!