University of Applied Sciences

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

# Certficate Extensions and Attributes Supporting Authentication in PPP and Wireless LAN

Daniel Schwarz

# Overview:



1. Introduction
   I. PKIX
2. Basics
   I. PPP
   II. EAP
   III. 802.1x
   IV. X.509 – certificate extensions
3. PKIX Internet Draft – certificate extensions and attributes supporting authentication in PPP and wireless LAN
   I. EAP extended key usage values
   II. WLAN SSID Public Key Certificate Extension
   III. WLAN SSID Attribute Certificate Attribute
4. EAP & 802.1x
   I. EAPOL
   II. EAP-TLS
   III. Alternatives
5. Conclusion

# 1.1 PKIX

- established in 1995
- intent of developing Internet standards needed to support an X.509-based PKI
- the scope of PKIX work has expanded beyond this initial goal
- PKIX not only profiles ITU (International Telecommunication Union) PKI standards, but also develops new standards apropos to the use of X.509-based PKIs in the Internet.

# 2. Basics

# 2.1. PPP

- standard-method for communication between two hosts
- most commonly used for dial-up internet access
- part of the Layer 2 Tunneling Protocol
- integrated error correction
- compression of the IP-header
- LCP (link configuration protocol):
  responsible for the configuration, for the establishment and the clearing of a PPP-connection

# 2.2. EAP

- sits inside of PPP's authentication protocol
- provides a generalized framework for several different authentication methods
- does not select a specific authentication mechanism at Link Control Phase (LCP) but rather postpones this until the Authentication phase
  -> this allows the authenticator to request more information before determining the specific authentication mechanism

# 2.2. EAP



three communication steps:

a) after the Link Establishment phase is complete, the authenticator sends one or more Requests to authenticate the peer
   - examples of Request types: Identity, MD5-challenge, One-Time Passwords, Generic Token Card,…

b) the peer sends a Response packet in reply to each Request

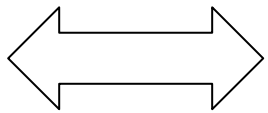
c) the authenticator ends the authentication phase with a Success or Failure packet

# 2.2. EAP

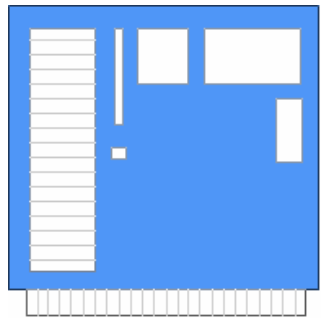
a)

peer

Link Establishment



LCP-packets

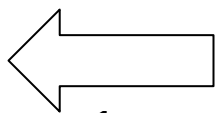


authenticator

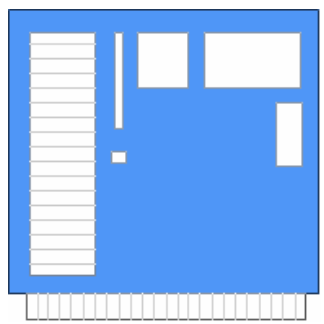
b)

peer

Request phase



1..n
Requests



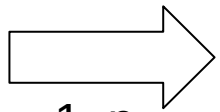
authenticator

# 2.2. EAP

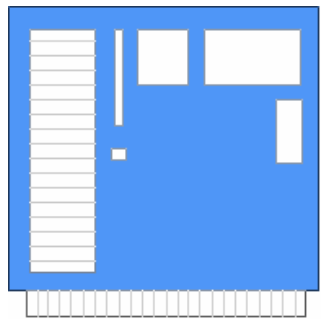
c)

peer

Response phase



1..n
Responses

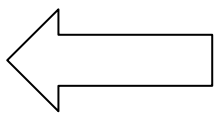


authenticator

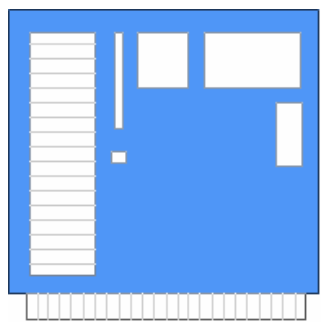
d)

peer

End of authentication



success or
failure packet



authenticator

# 2.2. EAP

University of Applied Sciences

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

**advantages:**

- multiple authentication mechanisms without having to pre-negotiate a particular one during LCP phase
- certain devices do not necessarily have to understand each request type and may be able to simply act as a passthrough agent for some kind of “back-end” server on a host

**disadvantages:**

- PPP implementation needs to be modified
- focus on authenticating a peer to an authenticator:
  -> the peer doesn’t request any authentication from the authenticator
  -> **EAP-TLS**

# 2.3. 802.1x



- enables authenticated access to IEEE 802 media (Ethernet, Token Ring, 802.11 WLAN, …)
- RADIUS support is optional but it is expected that many IEEE 802.1x Authenticators will function as RADIUS clients
- provides “network port authentication” for IEEE 802 media (including Ethernet, WLAN, …)
  -> port-based network access protocol
- standard “for passing EAP messages over LAN or WLAN”
- EAP messages are packed in Ethernet frames without using PPP
- used in situations where other protocols than TCP/IP are needed or the overhead and complexity of using PPP is undesirable

# 2.3. 802.1x

- three important terms:

  1.) **supplicant:** user or client that wants to be authenticated
  2.) **authentication server:** actual server doing the authentication
  3.) **authenticator:** device in between

- authenticator can be simple and dumb
  -> ideal for WLAN access points (little memory and processing power)

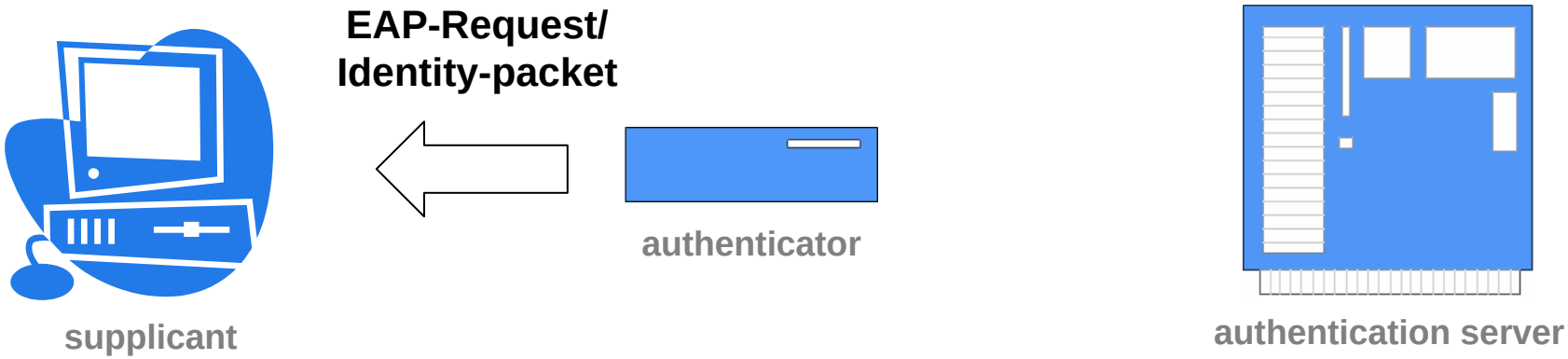
- the protocol in 802.1x is called EAP encapsulation over LANs (EAPOL)

- it is defined for Ethernet-like LAN (802.11 WLAN, Token Ring, …)

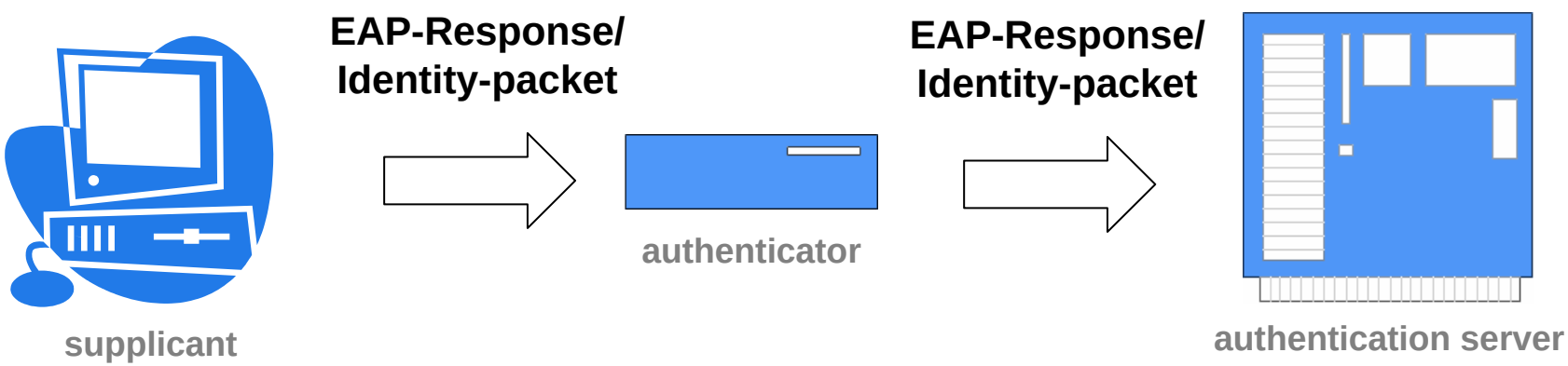
- different modes of operation (the most common one acts as follows)

# 2.3. 802.1x

a)

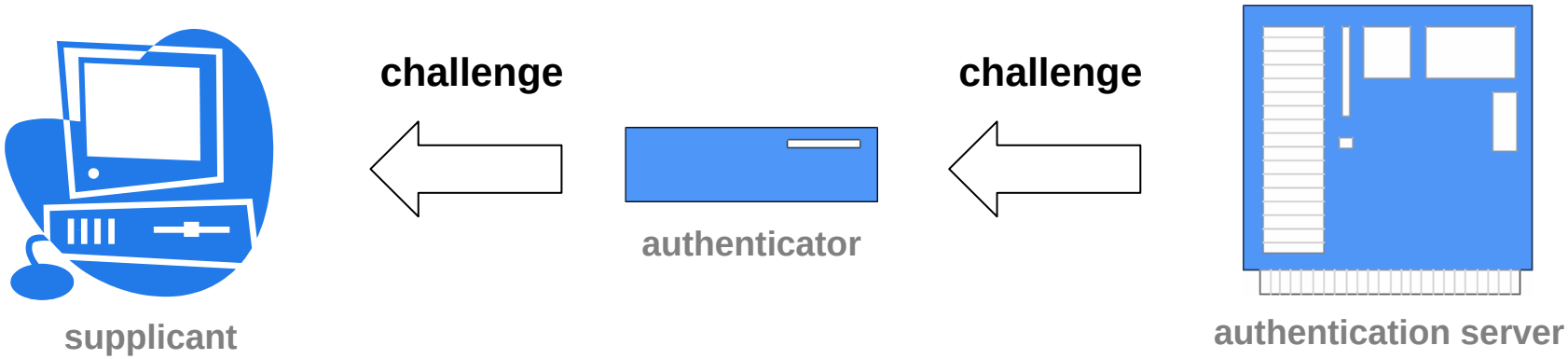

EAP-Request/
Identity-packet
authenticator
supplicant
authentication server

b)

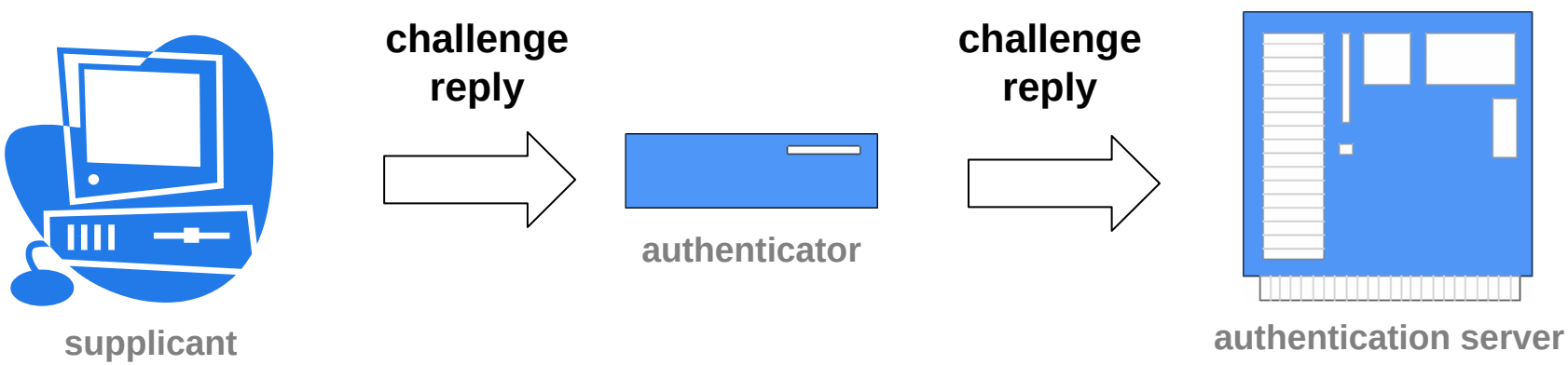

EAP-Response/
Identity-packet
EAP-Response/
Identity-packet
authenticator
supplicant
authentication server

# 2.3. 802.1x

c)

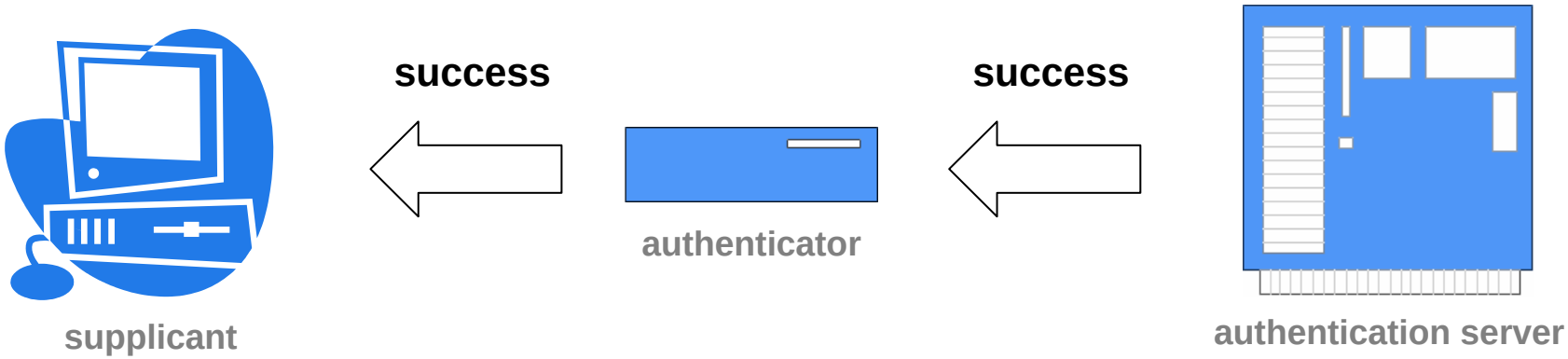

challenge
challenge
supplicant
authenticator
authentication server

d)

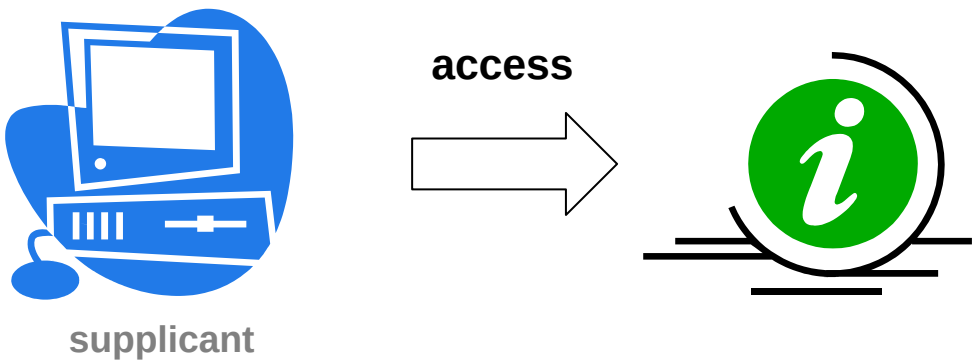

challenge
reply
challenge
reply
supplicant
authenticator
authentication server

# 2.3. 802.1x

e)


success
success
supplicant
authenticator
authentication server

f)


access
supplicant

# 2.4. X.509

- **X.509 is an ITU standard for PKI (Public Key Infrastructure)**
- **X.509 specifies, amongst other things, standard formats for public key certificates**
- **X.509 is part of the hierarchical X.500 standard and thus assumes a strict hierarchical system of certificate authorities (CAs) for issuing the certificates**
- **X.509 usually refers to the X.509 v3 certificate specified in RFC2459**

# 2.4. X.509 - certificate extensions

- **the extensions defined for X.509 v3 certificates provide methods for associating additional attributes with users or public keys**

- **it is also allowed for communities to define private extensions to carry information unique to those communities**

- **each extension in a certificate is specified as either *critical* (system must reject the certificate if it doesn't recognize the extension)**
  **or *non-critical* (system may ignore the extension)**

# 2.4. X.509 - certificate extensions

University of Applied Sciences

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

## key usage extension:

- defines the purpose of the key contained in the certificate
- should be marked critical

## extended key usage extension:

- this extension indicates one or more purposes for which the certified public key may be used
- it is used in addition or in place of the basic purpose indicated in the key usage extension
- may be marked critical or non-critical

# 2.4. X.509 - certificate extensions

University of Applied Sciences

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

**predefined values in RFC 3280:**

```
id-kp-serverAuth            OBJECT IDENTIFIER ::= { id-kp 1 }
-- TLS WWW server authentication
-- Key usage bits that may be consistent: digitalSignature,
-- keyEncipherment or keyAgreement

id-kp-clientAuth            OBJECT IDENTIFIER ::= { id-kp 2 }
-- TLS WWW client authentication
-- Key usage bits that may be consistent: digitalSignature
-- and/or keyAgreement

id-kp-codeSigning           OBJECT IDENTIFIER ::= { id-kp 3 }
-- Signing of downloadable executable code
-- Key usage bits that may be consistent: digitalSignature
```

# 2.4. X.509 - certificate extensions

University of Applied Sciences

GEORG-SIMON-OHM FACHHOCHSCHULE NÜRNBERG

**predefined values in RFC 3280:**

```
id-kp-emailProtection        OBJECT IDENTIFIER ::= { id-kp 4 }
-- E-mail protection
-- Key usage bits that may be consistent: digitalSignature,
-- nonRepudiation, and/or (keyEncipherment or keyAgreement)

id-kp-timeStamping           OBJECT IDENTIFIER ::= { id-kp 8 }
-- Binding the hash of an object to a time
-- Key usage bits that may be consistent: digitalSignature
-- and/or nonRepudiation

id-kp-OCSPSigning            OBJECT IDENTIFIER ::= { id-kp 9 }
-- Signing OCSP responses
-- Key usage bits that may be consistent: digitalSignature
-- and/or nonRepudiation
```

# 3. PKIX Internet Draft

certificate extensions and attributes supporting authentication in PPP and wireless LAN

# 3.1. EAP extended key usage values



**new values from the Internet Draft:**

**1) id-kp-eapOverPPP OBJECT IDENTIFIER ::= { id-kp 13 }**

**indicates that the certified public key is appropriate for use with EAP in the PPP environment**

**2) id-kp-eapOverLAN OBJECT IDENTIFIER ::= { id-kp 14 }**

**indicates that the certified public key is appropriate for use with EAP in the LAN environment**

**-> inclusion of both values indicates that the certified public key is appropriate for use in either of the environments**

# 3.2. WLAN SSID Public Key Certificate Extension

- always non-critical
- contains a list of SSIDs
- more than one certificate includes an extended key usage extension indicating that the certified public key is appropriate for use with the EAP in LAN environment

  -> the list of SSIDs MAY be used to select the correct certificate for authentication in a particular WLAN

- SSIDs are unmanaged

  -> the same SSID can appear if different certificates that are intended to be used with different WLANs

  -> user-input or “trial-and-error”

# 3.3. WLAN SSID Attribute Certificate Attribute

- **What to do when the PK certificate does not include the WLAN SSID certificate extension?**

  **-> use of an attribute certificate**

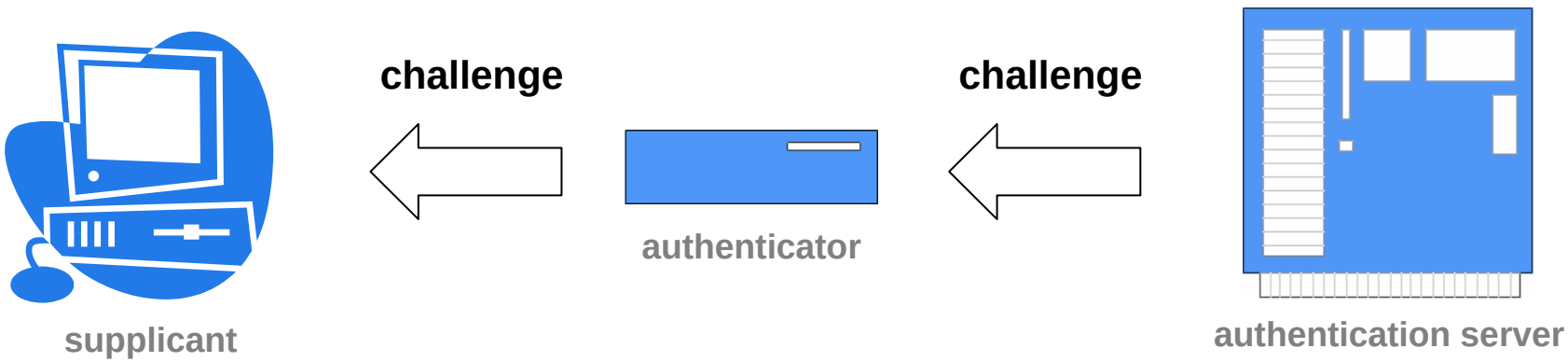
- **acts the same way as the extension**
- **contains a list of SSIDs**
- **can be used to select the correct certificate**

# 4. EAP & 802.1x

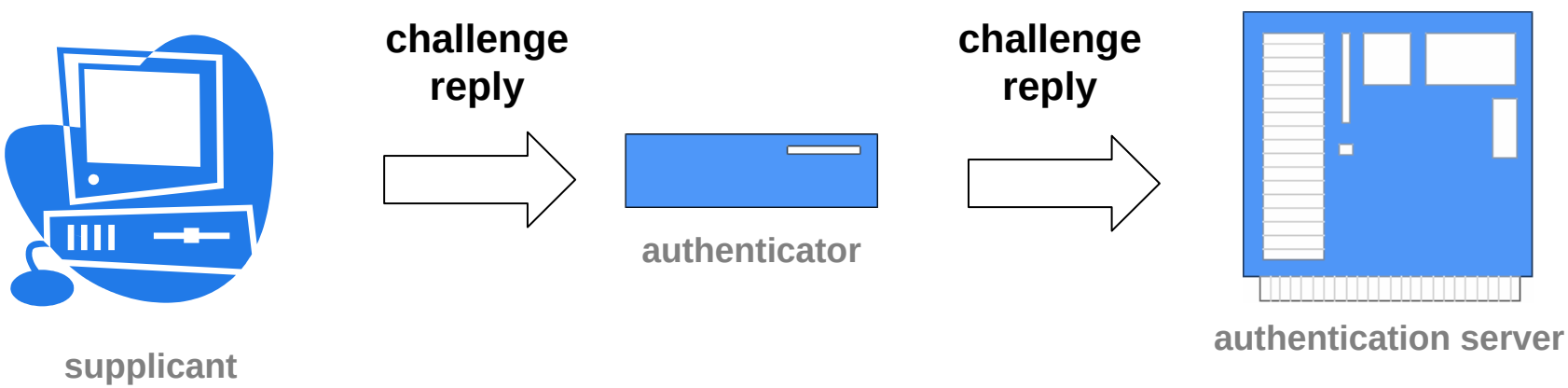
# 4.1. EAPOL (802.1x)

steps c) and d) – authentication server challenging the peer

c)

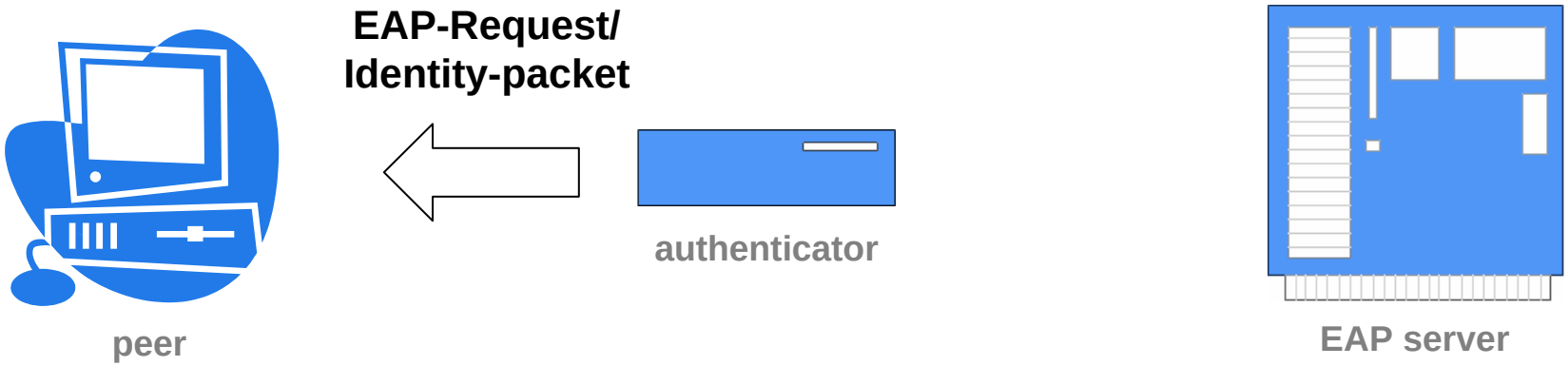



d)

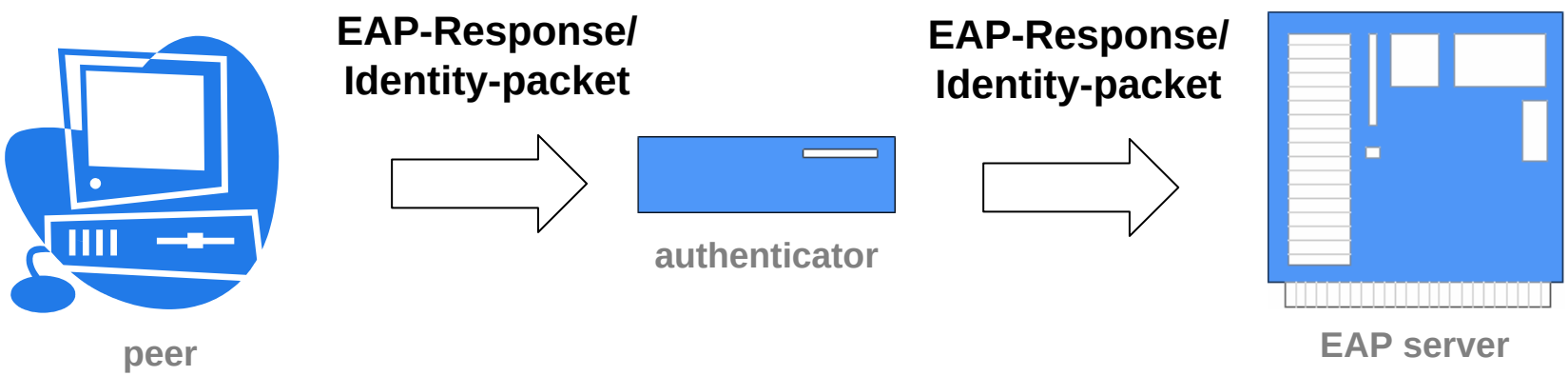


# 4.2. EAP-TLS - mutual authentication

a)




b)

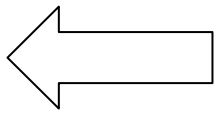


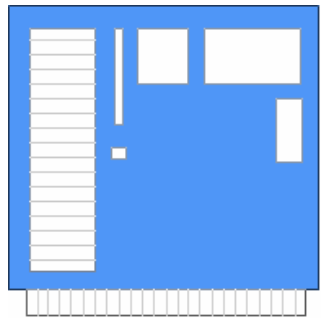
# 4.2. EAP-TLS - mutual authentication

c)

peer

**EAP-Request**
**(TLS Start)**



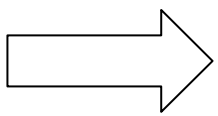


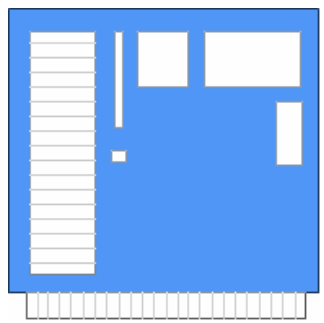
EAP server

d)

peer

**EAP-Response**
**(TLS client_hello)**





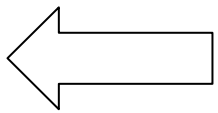
EAP server

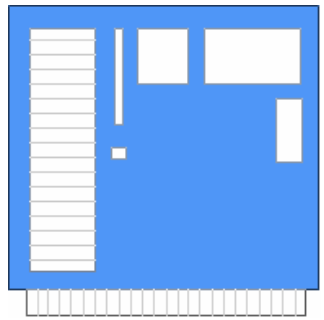
# 4.2. EAP-TLS - mutual authentication

e)

peer

**EAP-Request**
**(TLS server_hello,**
**TLS certificate,**
**TLS certificate_request**
**TLS server_hello_done)**



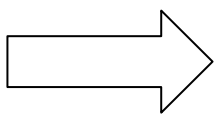


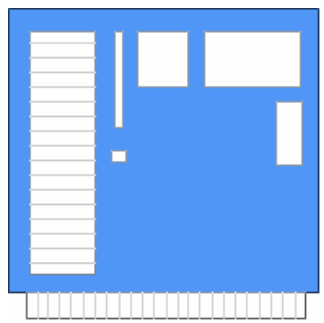
EAP server

f)

peer

**EAP-Response**
**(TLS certificate,**
**TLS client_key_exchange,**
**TLS finished)**





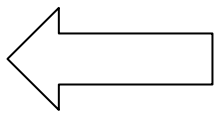
EAP server

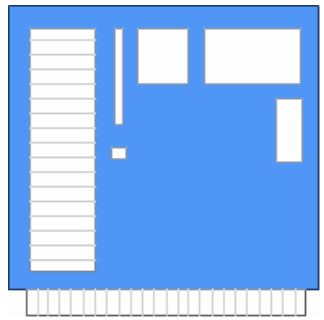
# 4.2. EAP-TLS - mutual authentication

g)

peer

**EAP-Request**
**(TLS finished)**



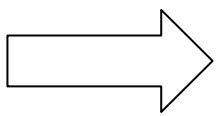


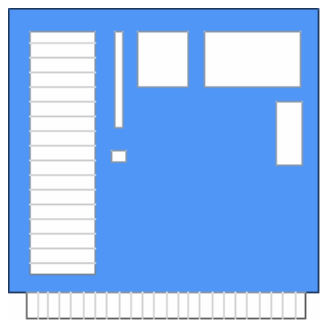
EAP server

h)

peer

**EAP-Response**
**(TLS)**





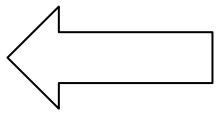
EAP server

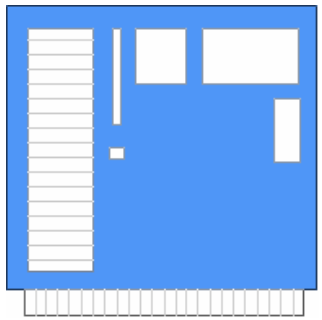
# 4.2. EAP-TLS - mutual authentication

i)

peer

**EAP-Success**





EAP server

# 4.3. EAP-Alternatives



EAP-MD5:

Lets a RADIUS server authenticate LAN stations by verifying an MD5 hash of each user's password

LEAP (Lightweight EAP):

Cisco's solutions goes a notch beyond EAP-MD5 by requiring mutual authentication and delivering keys used for WLAN encryption

EAP-TTLS and PEAP:

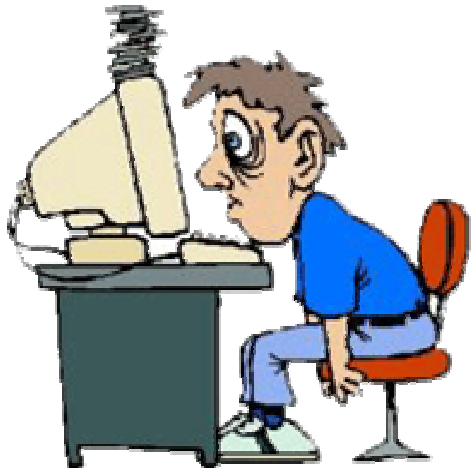
Have been proposed to simplify 802.1x development. Both require certificate-based authentication only for the RADIUS server. In addition an extensible set of different user authentication methods is offered

# 5. Conclusion

# 5. Conclusion



- **EAP-TTLS and PEAP are not yet finalized (Internet Drafts)**
- **EAP-MD5 and LEAP are simple but not that safe**
- **EAP & 802.1x has a huge effort with the administration of public keys for the users**
- **EAP & 802.1x is currently the best way to protect your WLAN via the EAP protocol**



# Thank you for your attention!