Contents

WEP (Wired Equivalent Privacy)

- No key management
- Authentication methods
- Encryption and integrity checking

WPA (WiFi Protected Access)

- IEEE 802.1X authentication framework
- Practical example using SSL/TLS

SIM/AuC authentication

WLAN security solutions

1. Wired Equivalent Privacy (WEP):

   Part of the original 802.11 standard. No key management, also several other weaknesses.

2. WiFi Protected Access (WPA):

   Interim solution offers key management using the 802.1X authentication framework, plus improved encryption and integrity checking.

3. IEEE 802.11i (WPA2):

   Same as WPA, except improved encryption (AES).

WLAN security using WEP

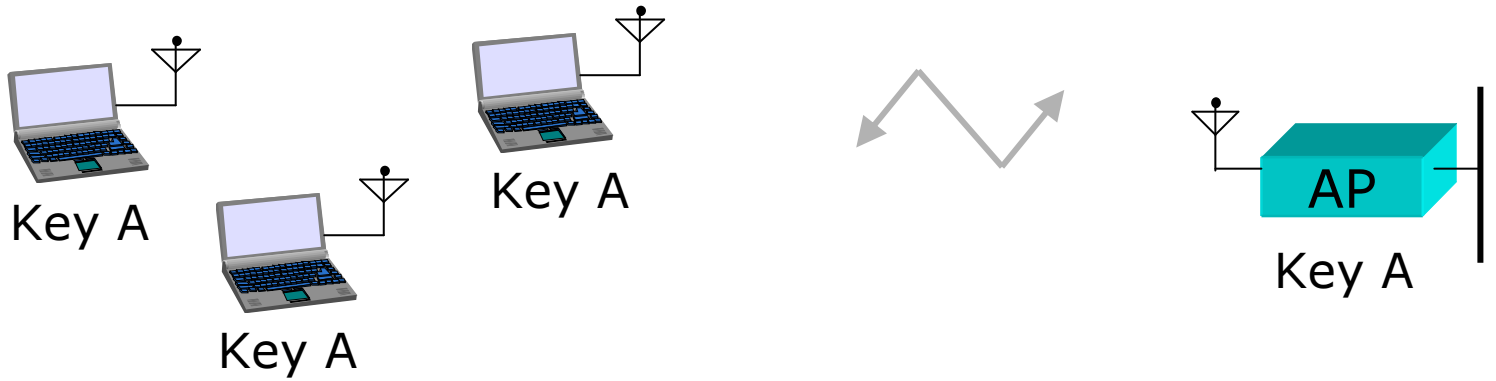
IEEE 802.11 specifies as an option usage of WEP which can take care of the following security mechanisms:

- Authentication ("shared key" user authentication)
- Confidentiality (RC4 stream cipher encryption)
- Integrity checking (CRC-32 integrity mechanism)

~~No key management~~

~~No protection against replay attacks~~

No key management in WEP



No key management in WEP ⇔ every wireless station and AP has the same "preshared" key that is used during authentication and encryption. This key is distributed manually (=> insufficient for enterprise applications).

Problems with preshared keys

Manual key management is not very flexible

Same key for everybody:

In a large network, users may wish to have independent secure connections. Just a single non-honest WLAN user can break the security.

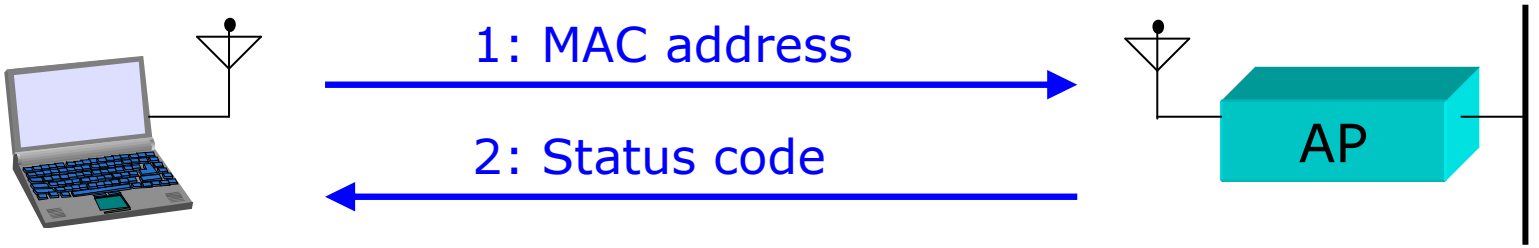
Static key:

Since it is relatively easy to crack WEP encryption in a reasonably short time, the keys should be changed often, but the preshared key concept does not support this.

WLAN authentication methods

1. Open system authentication (specified in WEP)
   - actually no authentication at all
2. Shared key authentication (specified in WEP)
   - weak due to non-existing key management
3. Authentication using SSID of AP
4. MAC address filtering
5. IEEE 802.1X authentication (specified in WPA)
6. SIM/AuC authentication (in operator-based network)

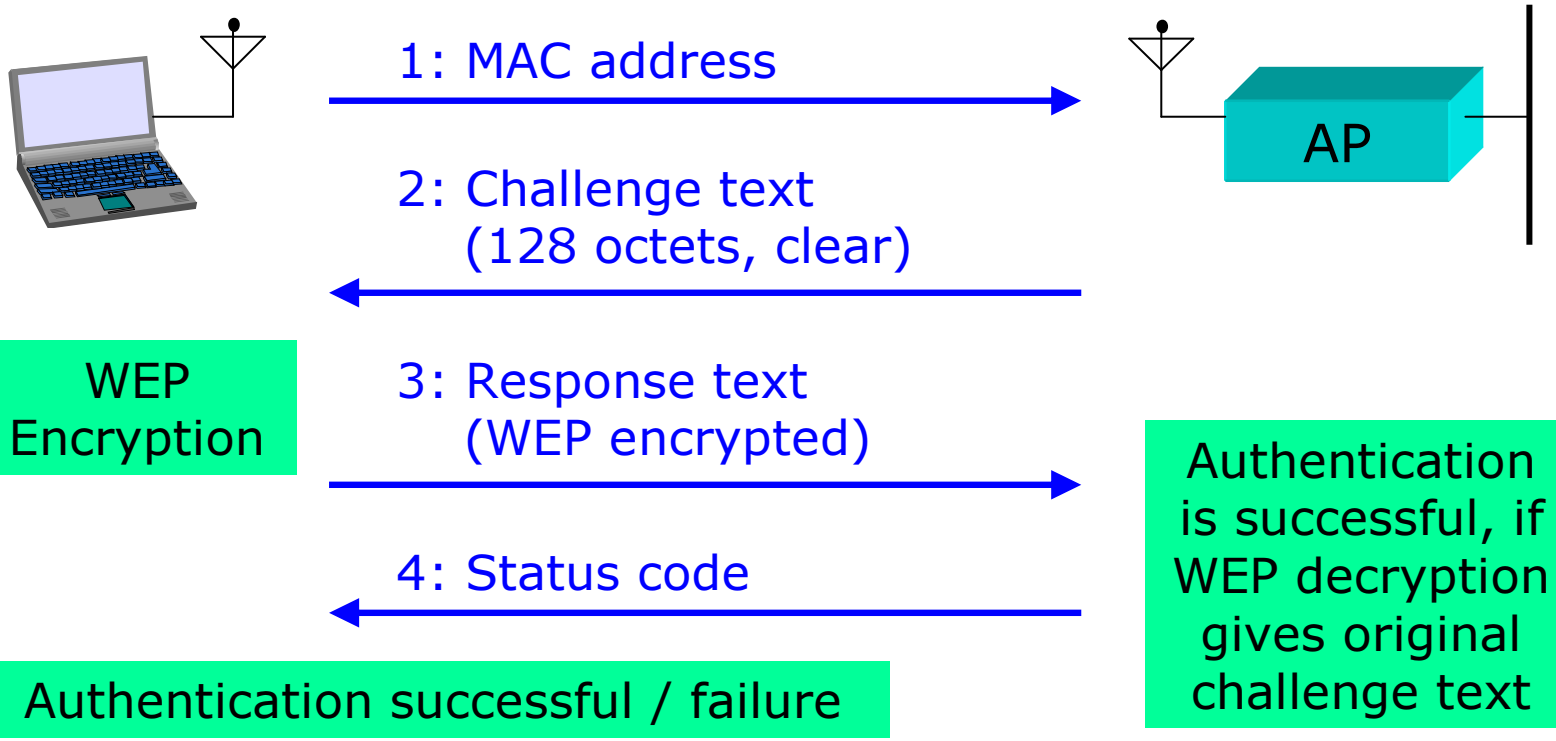
Open system authentication



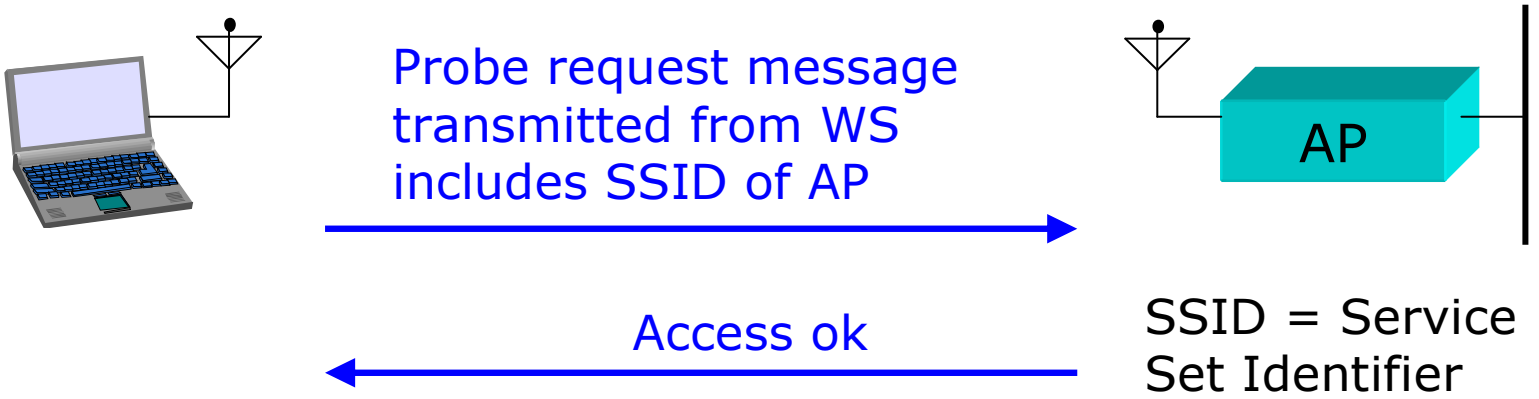
Status codes are defined in IEEE 802.11

Status code	Meaning
0	Successful
1	Unspecified failure
:	:
15	Authentication rejected (cause x)
:	:

Shared-key authentication

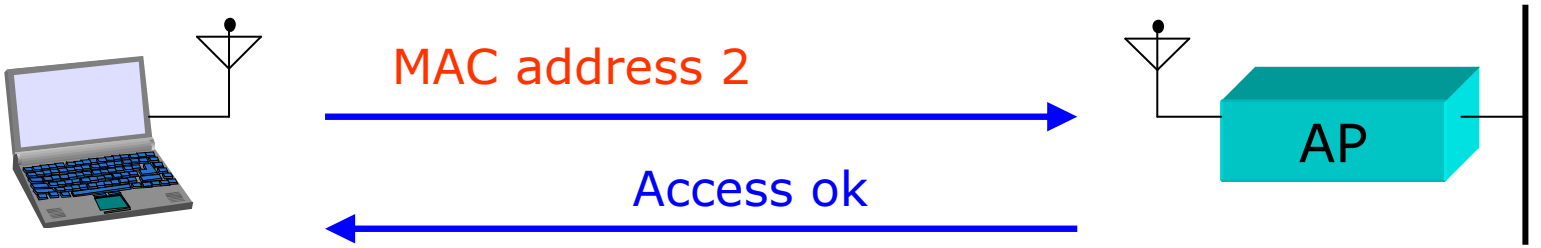


Authentication using SSID of AP



Not very secure: SSID is transmitted unencrypted over the wireless network and can be easily captured by an attacker.

MAC address filtering



Not very secure: Attacker can read MAC address of a wireless station attached to the WLAN and replace own MAC address with this stolen MAC address.

Accepted MAC addresses:

MAC address 1
MAC address 2
MAC address 3
MAC address 4
:

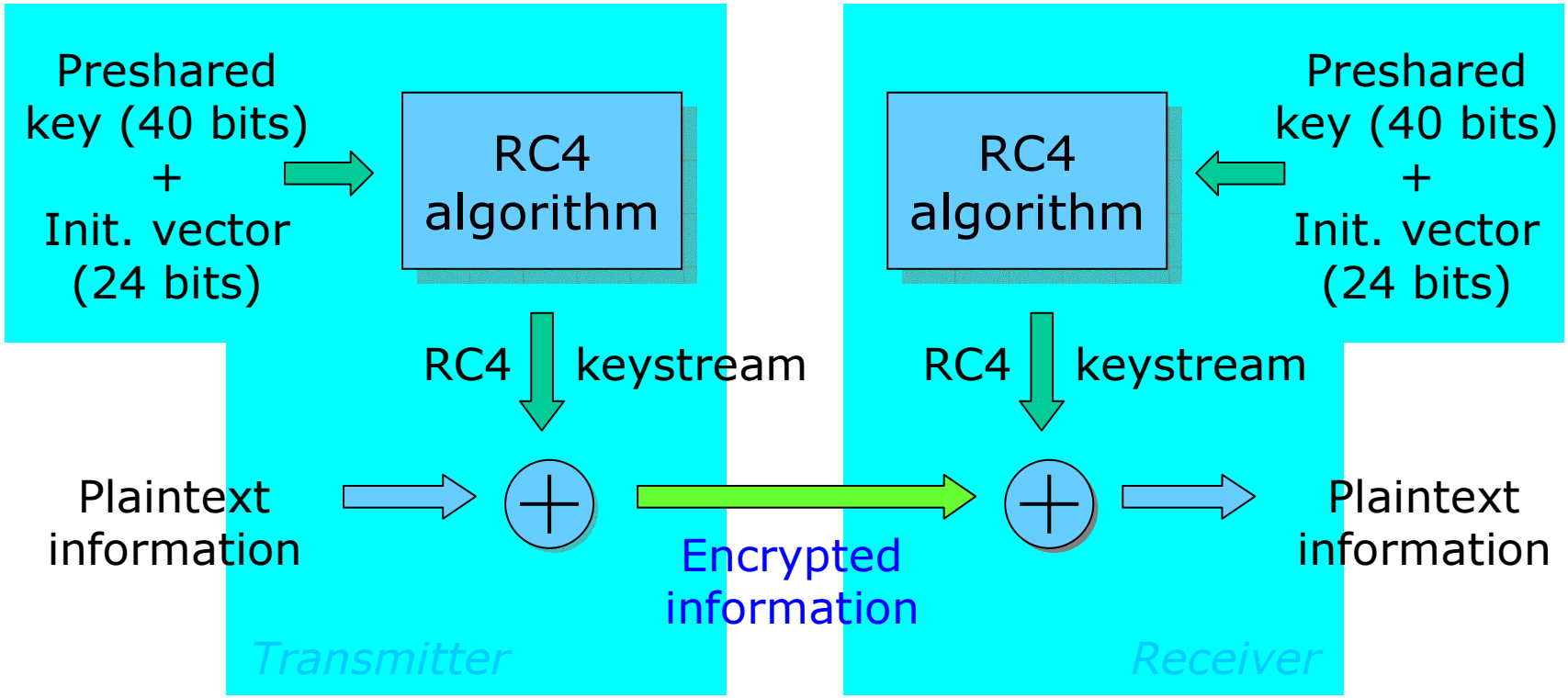
WEP encryption

WEP encryption is based on the RC4 stream cipher. First the preshared key (40 bits) is combined with a 24 bit initialization vector (IV) that should change from packet to packet (WEP does not specify how to select the IV).

The combined key (preshared key + IV) is fed to the RC4 algorithm that generates a continuous keystream.

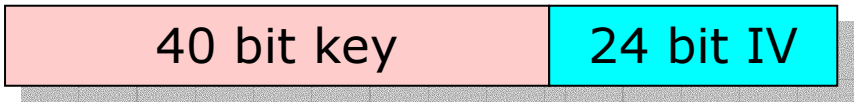
The plaintext information (+ ICV, see future slide) is bit-wise combined with the keystream by employing the XOR operation, thus producing the encrypted information.

WEP encryption and decryption

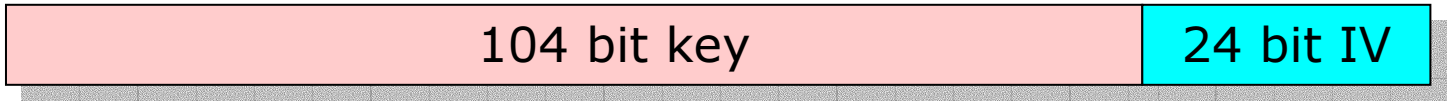


WEP key lengths

Standard solution:



Enhanced solution:



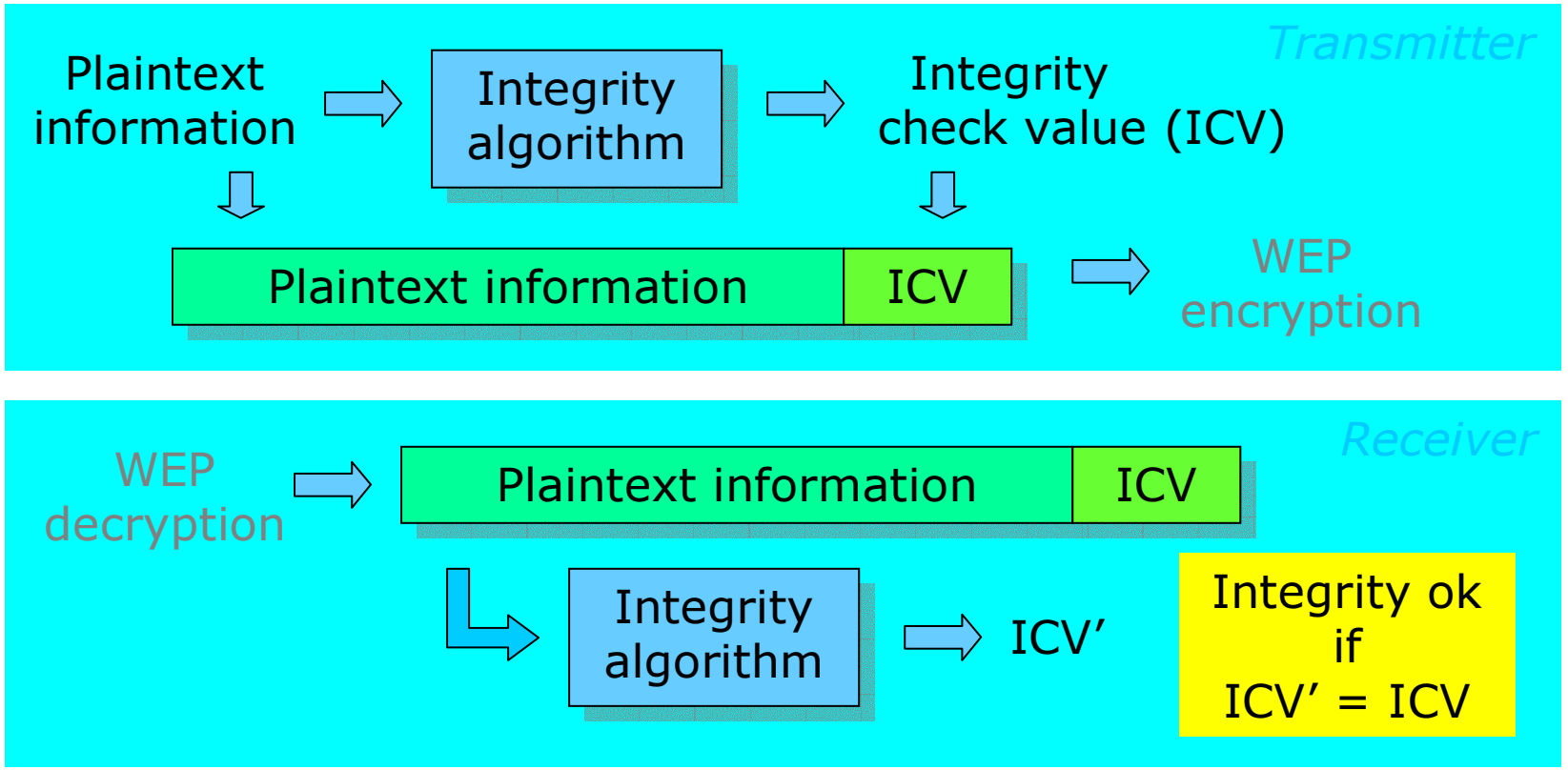
Initialisation vector (IV) is sent unencrypted over the wireless interface to the receiving end.

WEP integrity check

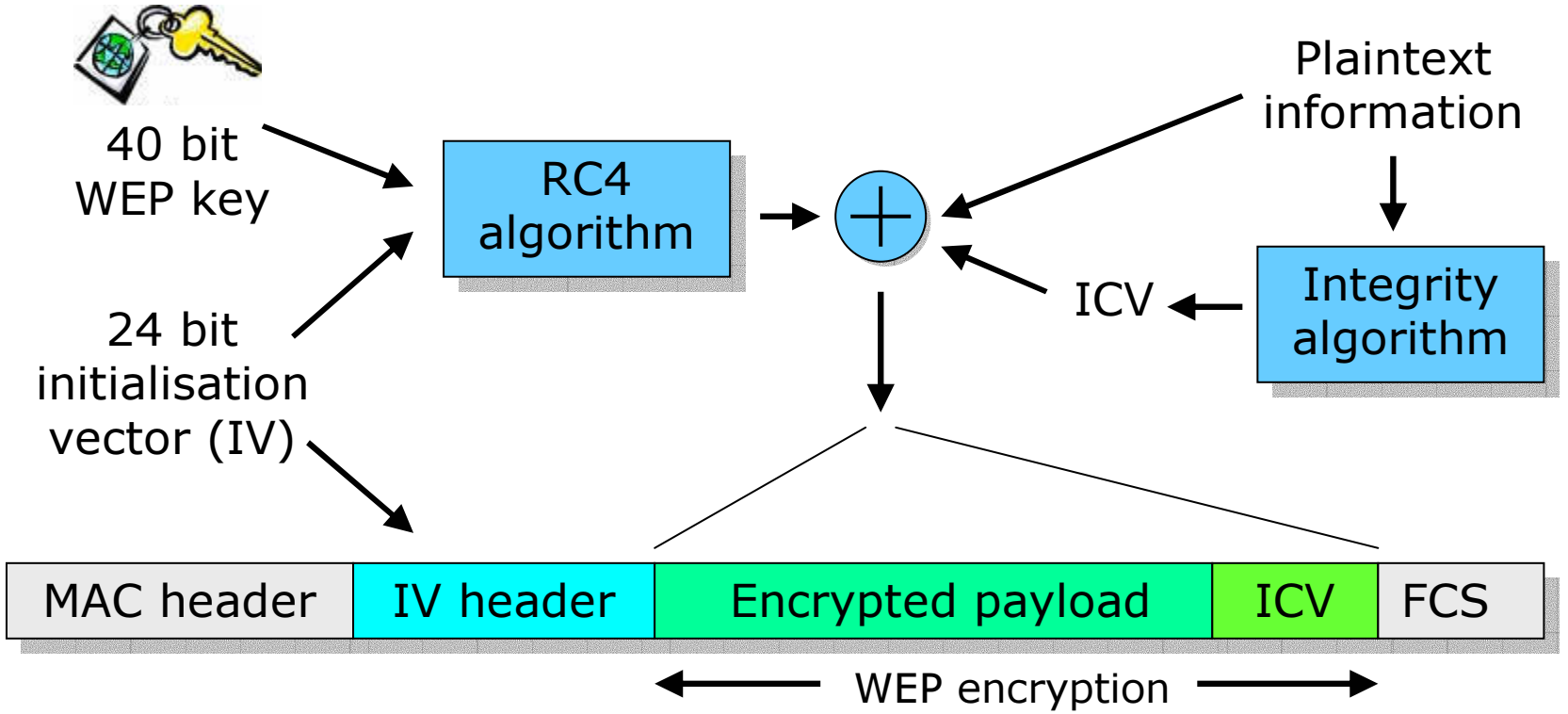
Integrity checking prevents man-in-the-middle attacks:

Integrity check is implemented in WEP by appending an integrity check value (ICV) bit sequence after the plaintext information before encryption at the transmitter.

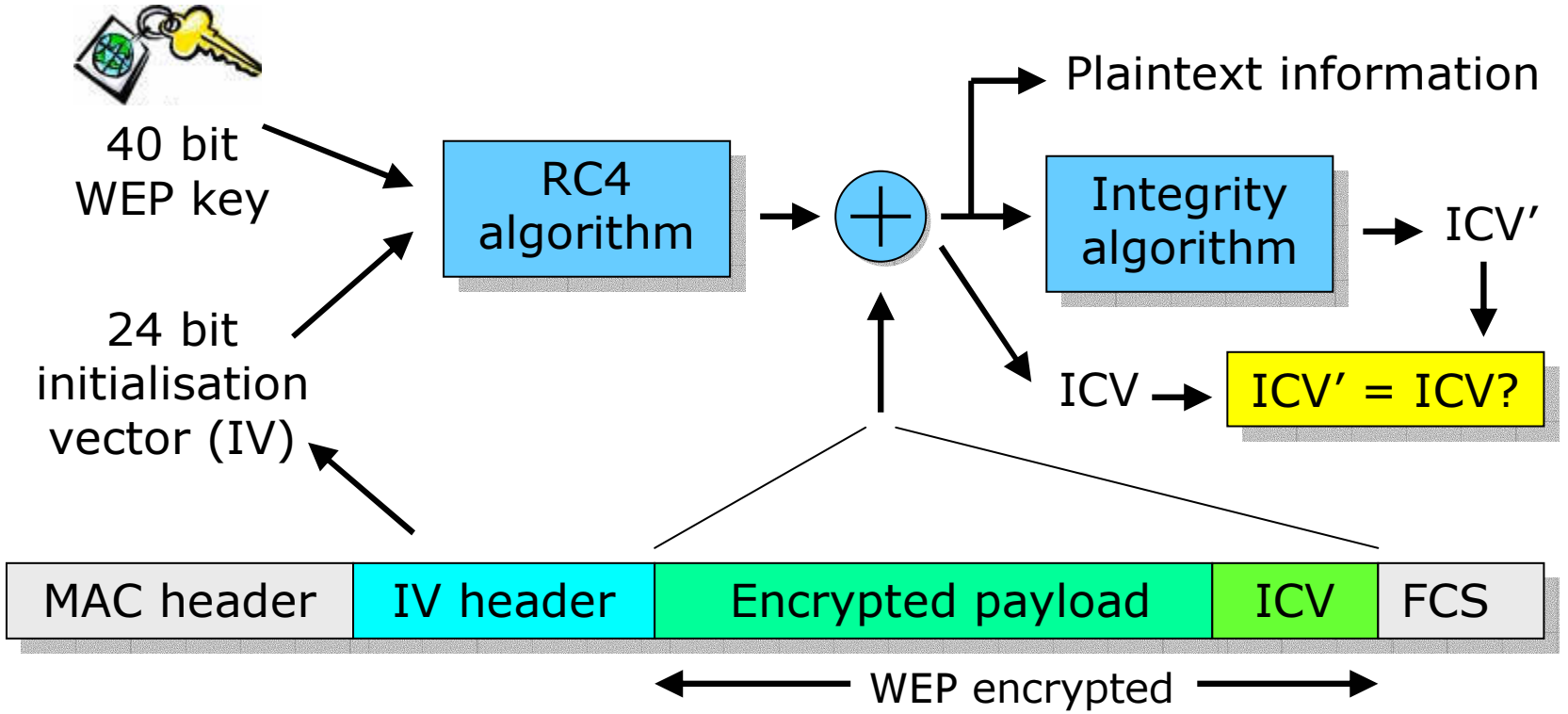
WEP integrity check



WEP operation: transmitter



WEP operation: receiver



WEP summary

Security measure	Features
Key management	WEP does not support key management
Authentication	Shared key authentication
Encryption	RC4 stream cipher, 40 bit key length is rather weak
Integrity protection	Rather weak in WEP
Replay attacks	No protection.

WLAN security using WPA

WPA is basically a pre-standard version of IEEE 802.11i as accepted by the WiFi alliance. WPA offers:

- Key management (using the 802.1X framework, it is also possible to use preshared keys)
- Authentication (using the 802.1X framework)
- Confidentiality (TKIP encryption)
- Integrity checking ("Michael" protocol)
- Protection against replay attacks.

Temporal Key Integrity Protocol (TKIP)

TKIP encryption is also based on the RC4 stream cipher, just like WEP encryption, with the following differences:

- The length of the initialization vector is 48 bit (instead of 24 bit in WEP)
- TKIP uses 104-bit per-packet keys, derived from a master secret and different for each packet (instead of a 40-bit or 104-bit static preshared key in WEP).

Note that AES (Advanced Encryption Standard) encryption used in IEEE 802.16i is significantly different.

IEEE 802.1X authentication framework

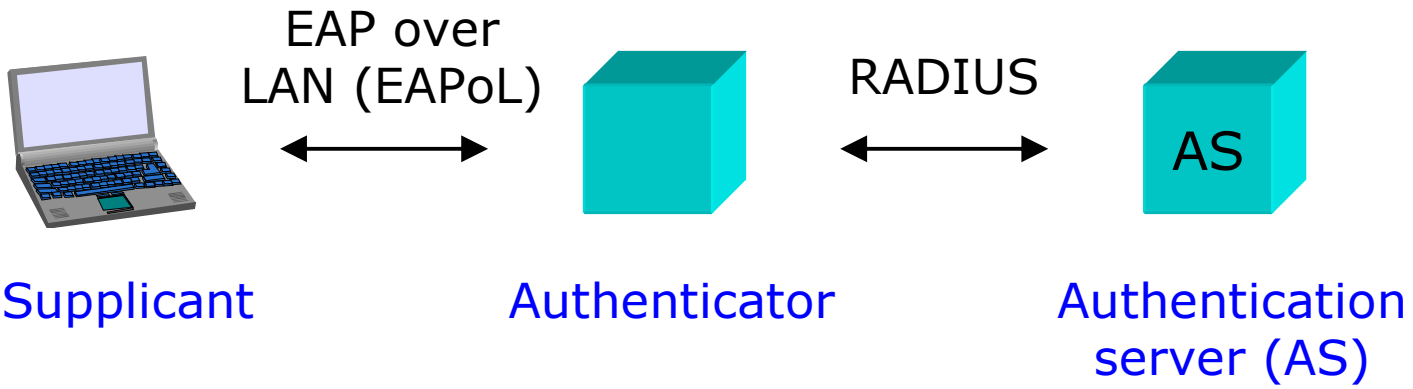
The 802.1X authentication framework protects wired and wireless networks from unauthorised use in open environments (such as university campus).

802.1X uses EAP (Extensible Authentication Protocol) to handle authentication requests. As the name implies, EAP is extensible and therefore should be future proof.

802.1X also uses RADIUS (Remote Authentication Dial-in User Service) for handling secure signalling between AP and authentication server.

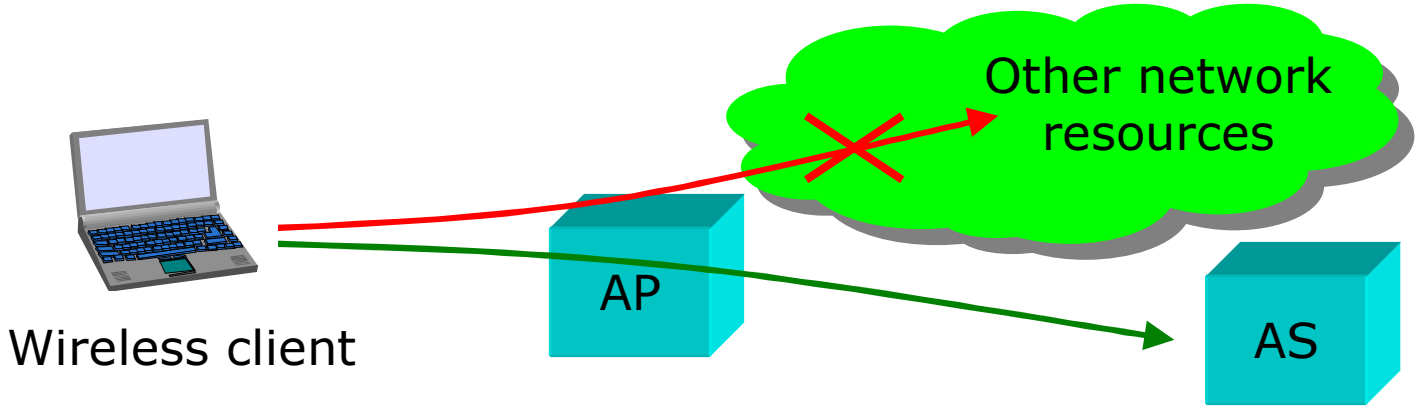
802.1X architecture

802.1X defines three network entities: Supplicant (the wireless client in the wireless station), authenticator (in a WLAN usually the AP) and authentication server (containing user-related authentication information).



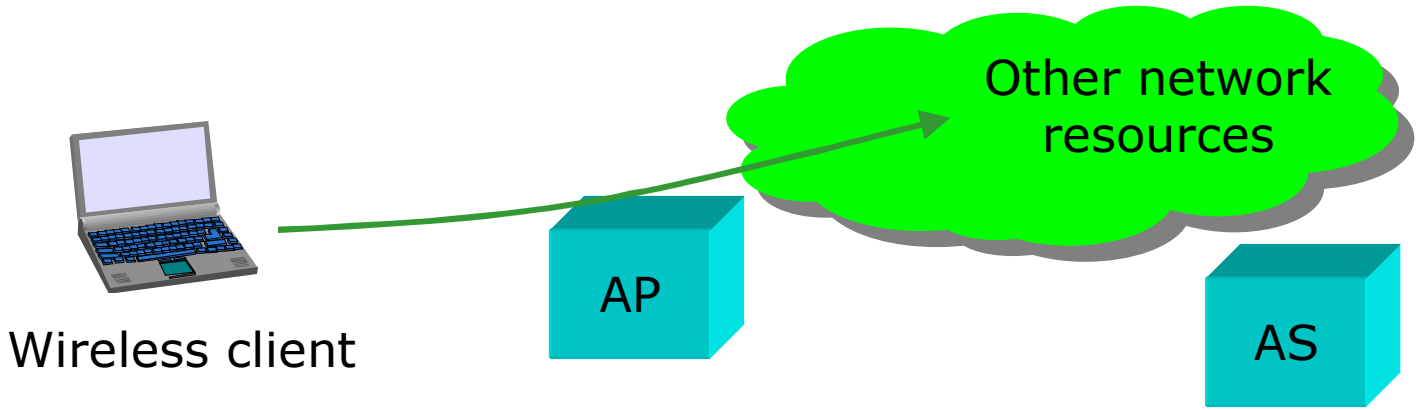
802.1X authentication procedure (1)

With 802.1X, authentication occurs after association. However, prior to successful authentication, a wireless client is only allowed access to the AS. All other traffic is blocked at the AP.



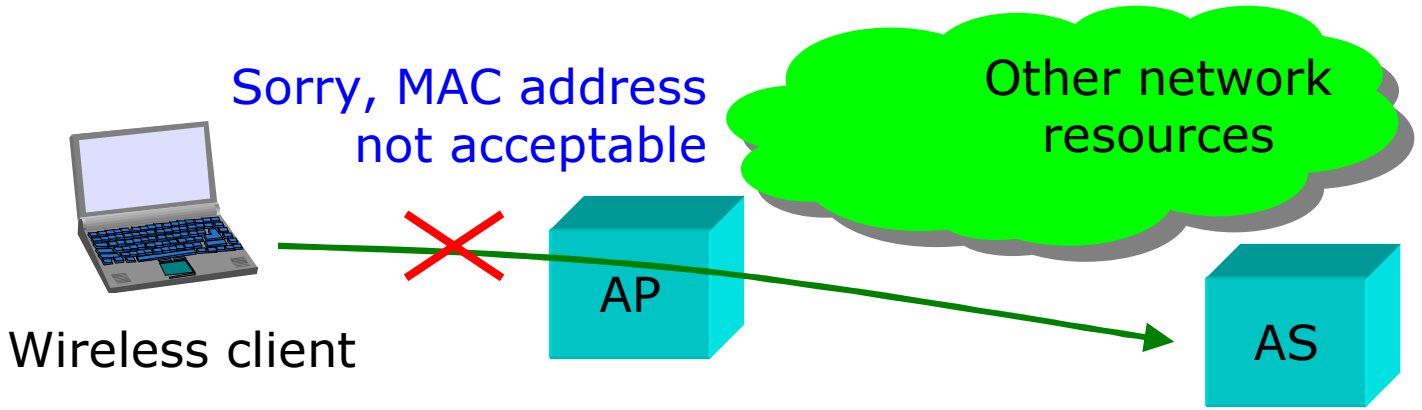
802.1X authentication procedure (2)

After successful authentication, the wireless client is granted access to other network resources by the AP.



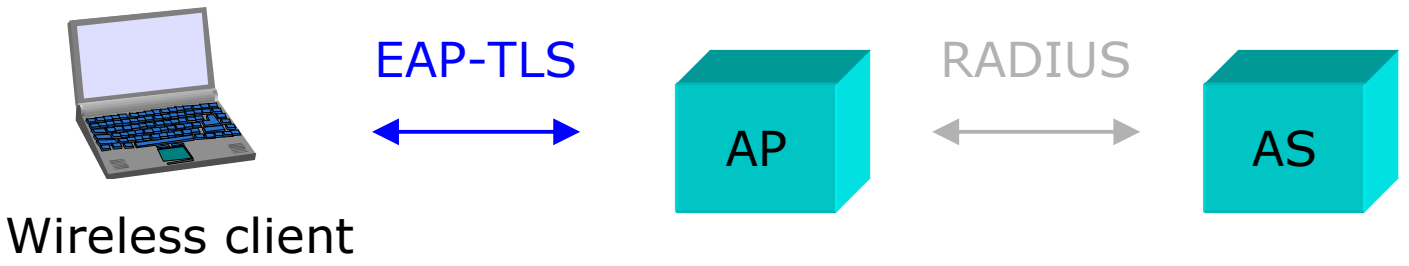
802.1X authentication procedure (3)

The authenticator (AP) can also perform authentication based on MAC address filtering (for preventing denial-of-service = DoS attacks) before starting the 802.1X authentication.

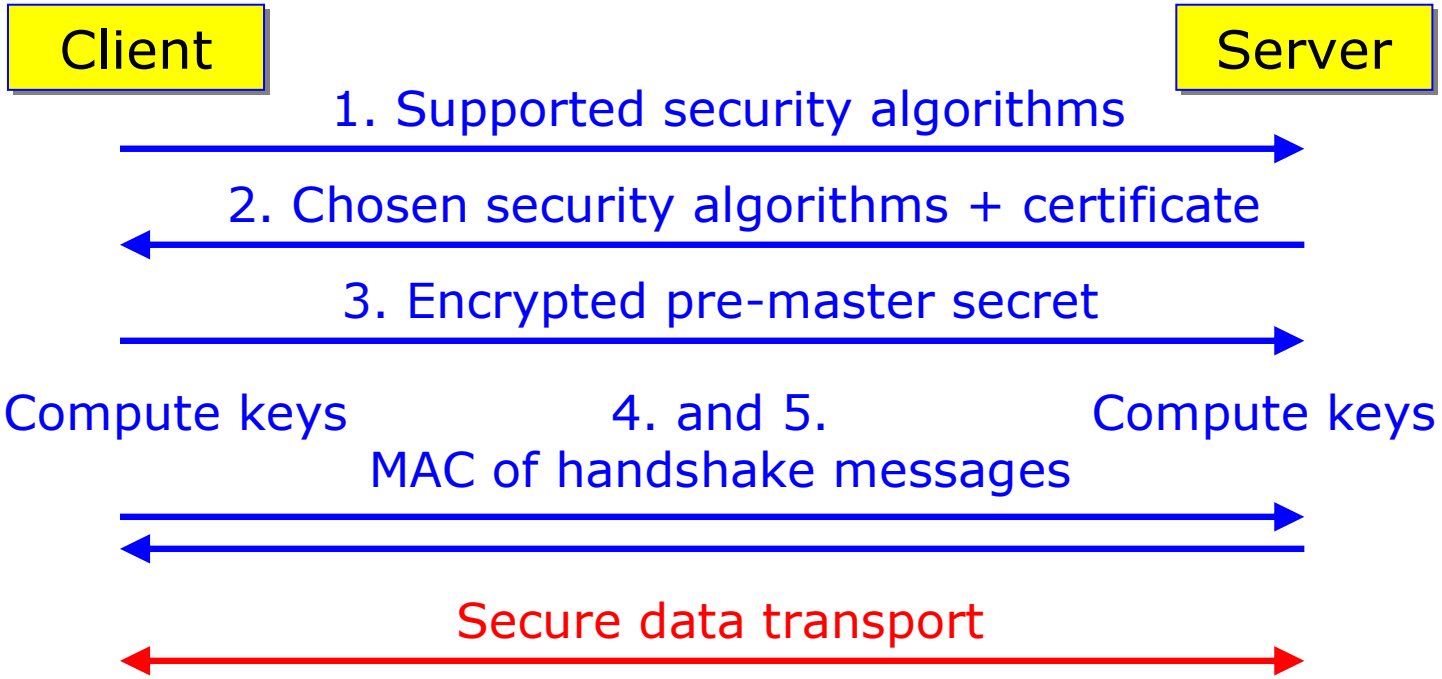


Example: EAP-TLS

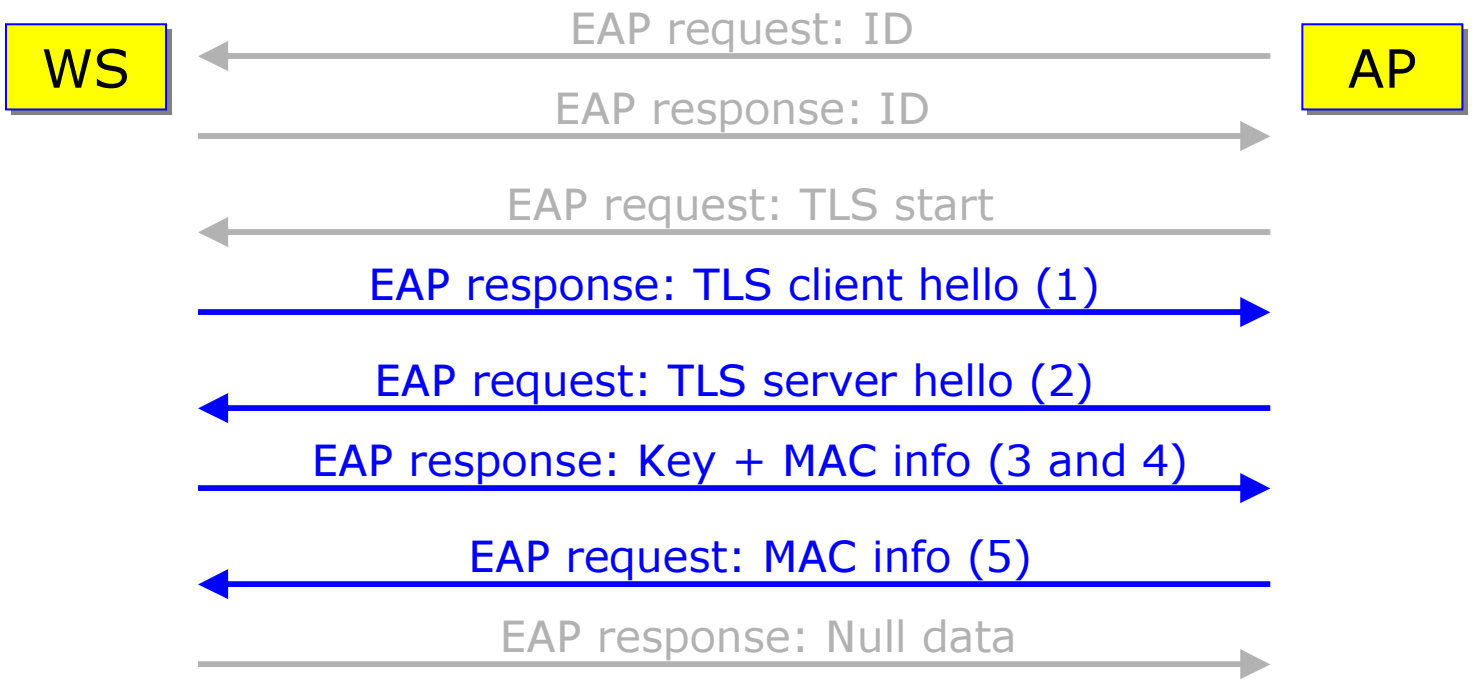
As an example, SSL/TLS is one of the various options defined to be used over EAP. The next two slides show how the SSL/TLS handshake sequence is embedded into a corresponding EAP sequence. (The RADIUS part of the signalling is not shown.)



Basic SSL/TLS handshake sequence

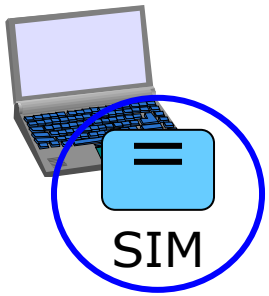


EAP-TLS signalling sequence



Authentication in operator-based network

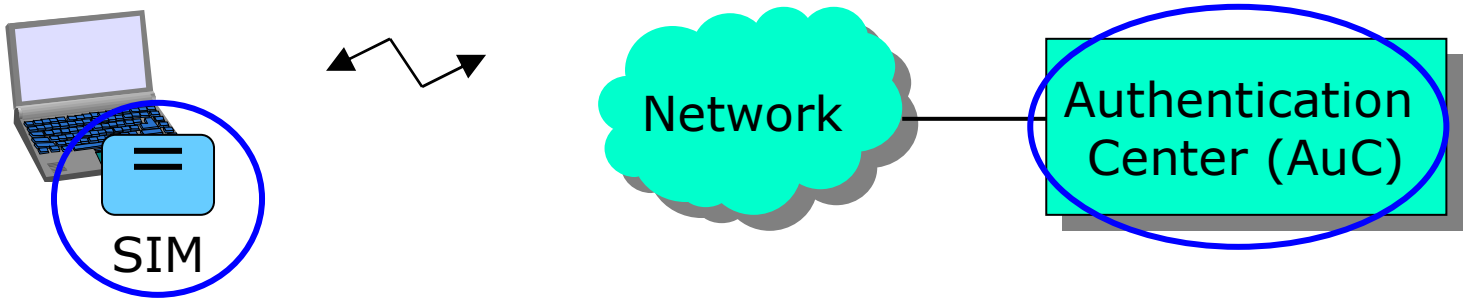
802.11 networks offer new possibilities when the wireless station includes a SIM (Subscriber Identity Module) that is provided by a certain network operator / service provider.



Through the SIM, operators can offer WLAN users added value applications such as secure authentication, nation-wide or worldwide roaming, and user-tailored charging solutions. Let us next see how SIM-based authentication works.

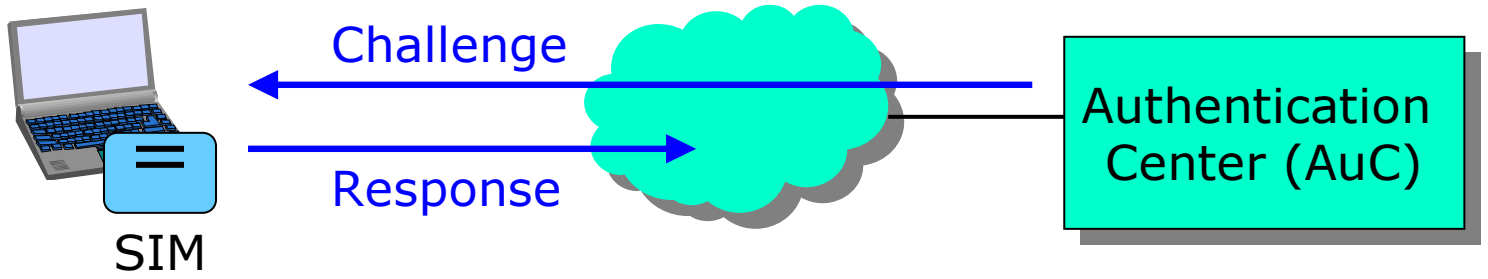
SIM/AuC authentication (1)

SIM/AuC authentication is based on storing a user-specific authentication key in two safe places: the authentication center (safely stored in the operator's premises) and the SIM in the user terminal.



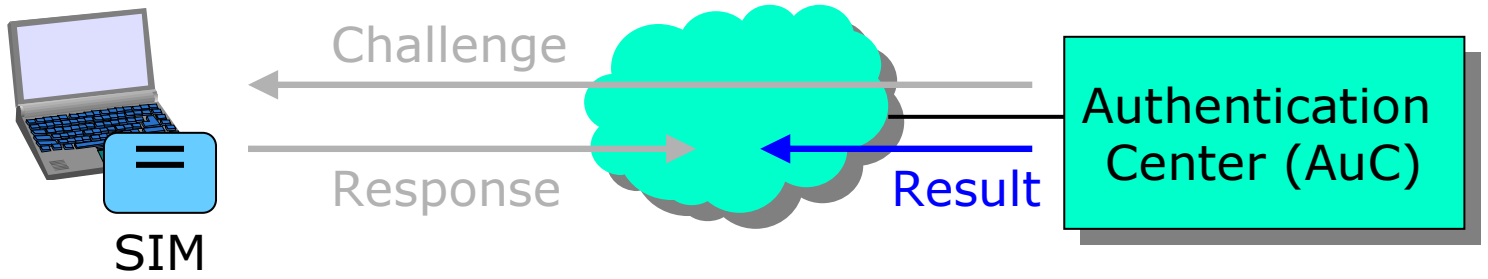
SIM/AuC authentication (2)

SIM/AuC authentication uses the challenge - response method. A challenge is sent to the SIM, where it is encrypted using the authentication key, and the result (response) is returned to the network (e.g. the AP).



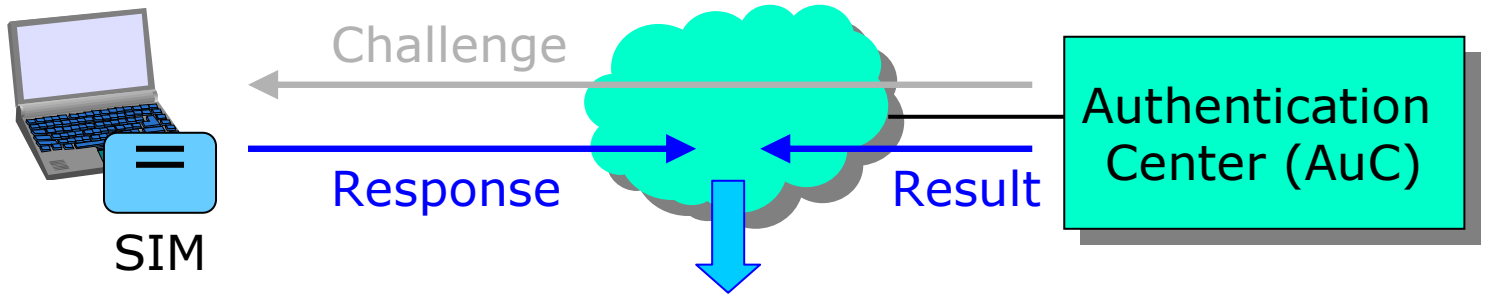
SIM/AuC authentication (3)

The challenge is also encrypted in the AuC using the same authentication key, and the result (which should be identical to the response from the SIM) is sent to the network (e.g. the AP).



SIM/AuC authentication (4)

If the result is the same, authentication was successful.



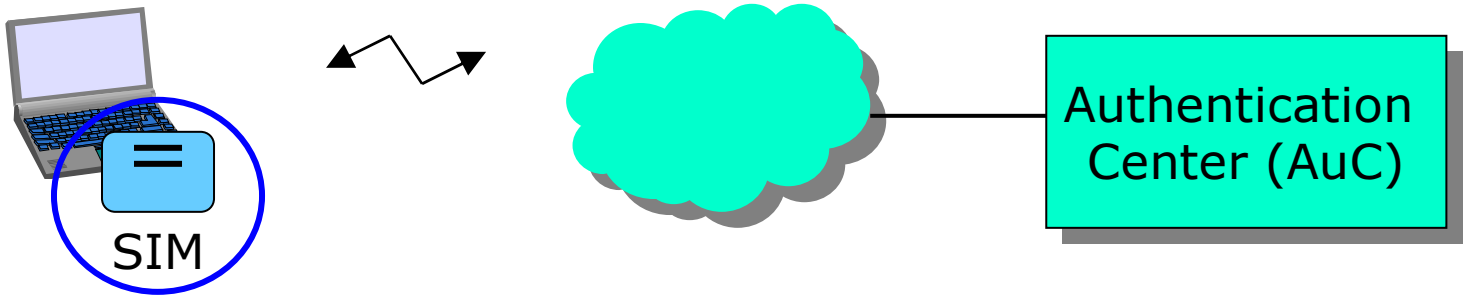
Same result => authentication successful

Different result => either the authentication key or encryption algorithm was different in SIM and AuC

SIM/AuC authentication (5)

The high security of this scheme is based on two facts:

1. The authentication key stored in the SIM can never be read from the SIM. The encryption algorithm is also running inside the SIM.



SIM/AuC authentication (6)

The high security of this scheme is based on two facts:

2. The authentication key is never removed from the AuC and the algorithm is running in the AuC. As long as there is no access to the AuC, security is assured.

Operator services

If operators want to offer new services or applications, distribution of SIM cards is not the only issue they must consider. In order to implement the services, various network resources must also be implemented (like AuC in the previous example).

Obviously, all this is not without cost, so there must be some way of charging subscribers (again requiring new network elements => charging center, etc.) for the services. Future will tell if operator services will ever be successful as far as 802.11 networks are concerned.