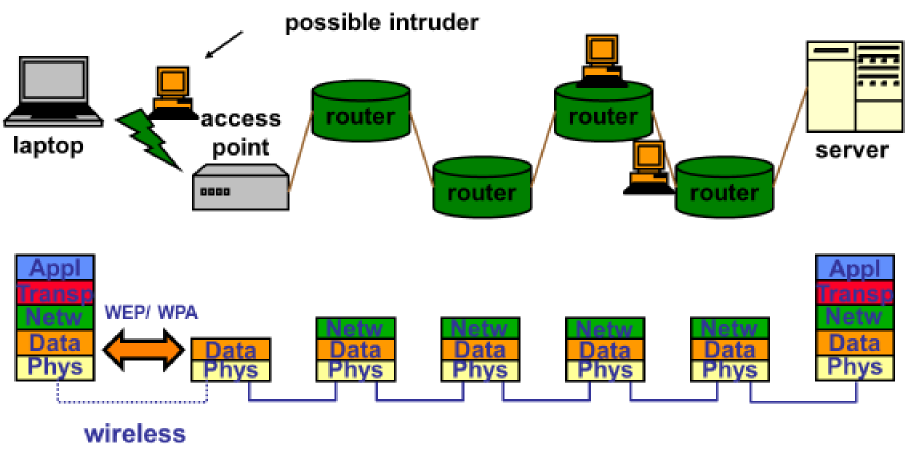
Overview

- Network model
- Secure configuration of devices
- Exchanging keys
- Secure networking protocols
  - Transport layer: TLS & SSL
  - Network layer: IPSec & VPN
  - **Data link layer: WEP & WPA**
- Firewalls

2

Datalink security



3

Data link security

- **Example data layer security protocols**
  - CHAP, PPTP, L2F, ECP, EAP
- **Example attacks**
  - Content Address Memory (CAM) table exhaustion attack
    - Through flooding, fill the CAM table that stores which device should be contacted through each switch port
    - Device defaults to broadcasting
    - Turns a switch into a hub
  - Address Routing Protocol (ARP) spoofing
    - Data link layer is responsible for mapping logical (IP) to physical (MAC) addresses
    - Broadcast spoofed IP packets
  - Dynamic Host Configuration Protocol (DHCP) starvation
    - Continue sending DHCP requests

4

The network interface layer, commonly referred to as the data link layer, is the physical interface between the host system and the network hardware. It defines how data packets are to be formatted for transmission and routing. Some common link layer protocols include IEEE 802.2 and X.25. The data link layer and its associated protocols govern the physical interface between the host computer and the network hardware. The goal of this layer is to provide reliable communications between hosts connected on a network.

Data link security: wireless

- **Additional attacks in wireless networks**
  - Packet overhearing
    - Shared medium
  - Deauth (deauthentication) attack
    - Send spoofed deauthentication messages
  - Hidden node attacks
    - See next slide

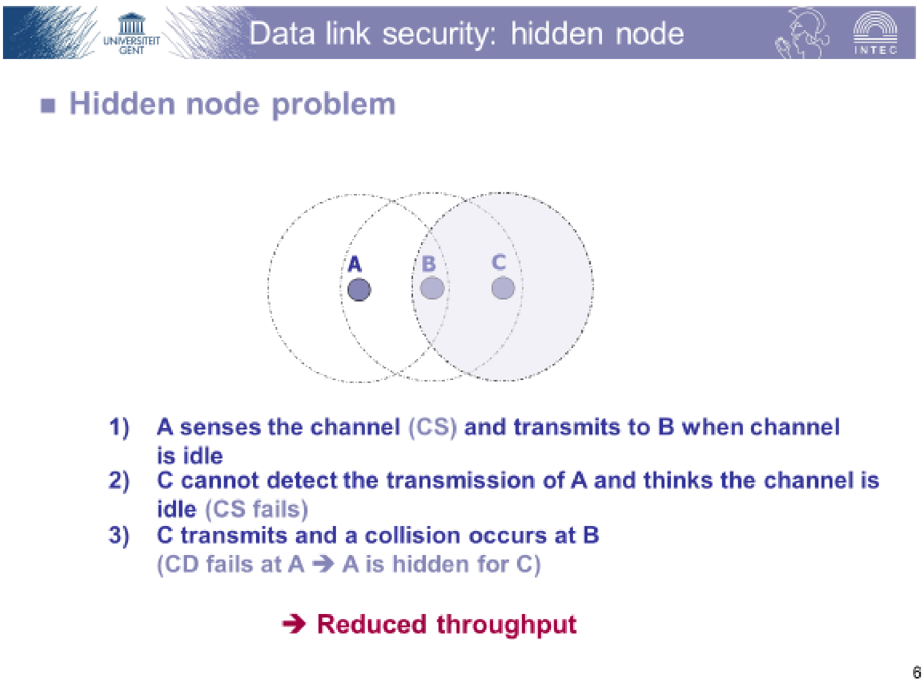
5

Packet overhearing

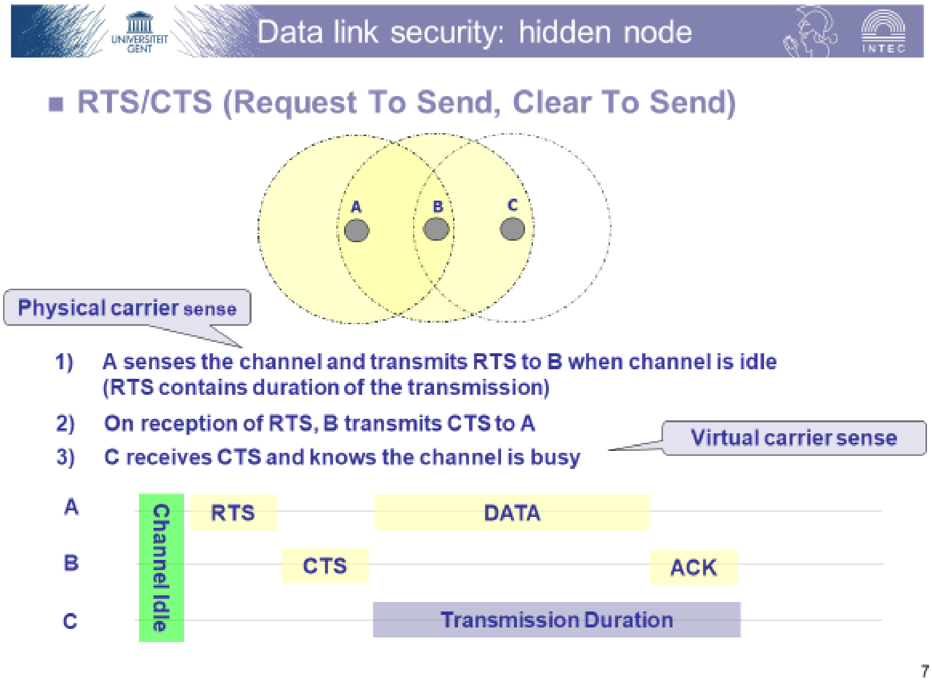
Due to the shared nature of the wireless medium, all packets can be overheard

Deauth (deauthentication) attack

Any client entering a wireless network must first authenticate with an access point (AP) and is thereafter associated with that access point. When the client leaves it sends a deauthentication, or deauth, message to disassociate itself with the access point. An attacker can send deauth messages to an access point tied to client IP addresses thereby knocking the users off-line and requiring continued re-authenticate, giving the attacker valuable insight into the reauthentication handshaking that occurs. To mitigate this attack, the access point can be set up to delay the effects of deauthentication or disassociation requests (e.g., by queuing such requests for 5–10 seconds) thereby giving the access point an opportunity to observe subsequent packets from the client. If a data packet arrives after a deauthentication or disassociation request is queued, that request is discarded since a legitimate client would never generate packets in that order



In a wireless network many hosts or nodes are sharing a common medium. If nodes A and C are both wireless laptop computers communicating in an office environment their physical separation may require that they communicate through a wireless access point B. Consider the scenario with three wireless devices as shown in the figure. The transmission range of A reaches B, but not C (the detection range does not reach C either). The transmission range of C reaches B, but not A. Finally, the transmission range of B reaches A and C, i.e., A cannot detect C and vice versa. A starts sending to B, C does not receive this transmission. C also wants to send something to B and senses the medium. The medium appears to be free, the carrier sense fails. C also starts sending causing a collision at B. But A cannot detect this collision at B and continues with its transmission. A is hidden for C and vice versa. Since only one device can transmit at a time in order to avoid packet collisions, packet loss occurs.



This slide shows the same scenario as previously shown in the slide on **hidden terminals**. Remember, A and C both want to send to B. A has already started the transmission, but is hidden for C, C also starts with its transmission, thereby causing a collision at B.

A frequently used solutions is to ensure A does not start its transmission at once, but sends a **request to send (RTS)** first. The access point B receives the RTS that contains the name of sender and receiver, as well as the length of the future transmission. This RTS is not heard by C, but triggers an acknowledgement from B, called **clear to send (CTS)**. The CTS again contains the names of sender (A) and receiver (B) of the user data, and the length of the future transmission. This CTS is now heard by C and the medium for future use by A is now reserved for the duration of the transmission. After receiving a CTS, C is not allowed to send anything for the duration indicated in the CTS toward B. A collision cannot occur at B during data transmission, and the hidden terminal problem is solved – provided that the transmission conditions remain the same. (Another station could move into the transmission range of B after the transmission of CTS.) Still, collisions can occur during the sending of an RTS. Both A and C could send an RTS that collides at B. RTS is very small compared to the data transmission, so the probability of a collision is much lower. B resolves this contention and acknowledges only one station in the CTS (if it was able to recover the RTS at all). No transmission is allowed without an appropriate CTS.

Hidden node attacks. An attacker can exploit this functionality by flooding the network with CTS messages. Then every node assumes there is a hidden node trying to transmit and will hold its own transmissions, resulting in a denial of service. Preventing hidden node attacks requires a network tool. Such a tool monitors access point traffic and develops a baseline level of traffic. Any spikes in CTS/RTS signals are assumed to be the result of a hidden node attack and are subsequently blocked.

Data link security: wireless

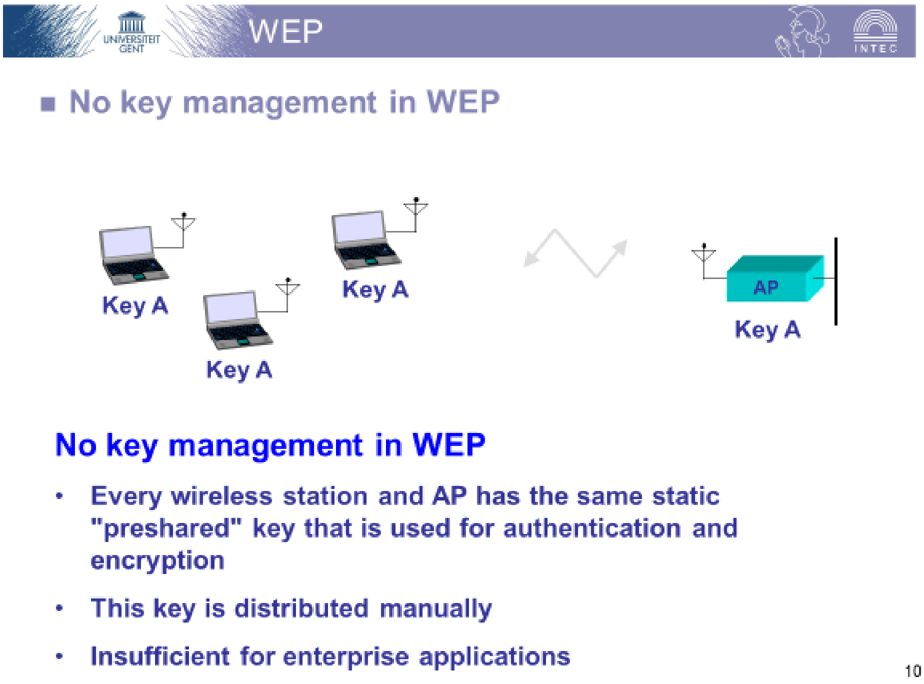
- Need for additional security mechanisms
- WLAN security solutions
  - Wired Equivalent Privacy (WEP):
    - Part of the original 802.11 standard. No key management, also several other weaknesses.
  - WiFi Protected Access (WPA):
    - Interim solution offers key management using the 802.1X authentication framework, plus improved encryption and integrity checking.
  - IEEE 802.11i (WPA2):
    - Same as WPA, except improved encryption (AES).

8

WEP

- IEEE 802.11 specifies **as an option** the use 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)
- It lacks
  - key management
  - protection against replay attacks

9



Some problems associated with preshared keys are the following

- 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.

WEP

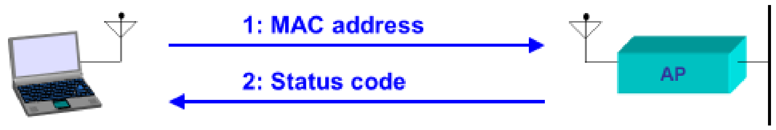
WLAN authentication methods

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

11

WEP

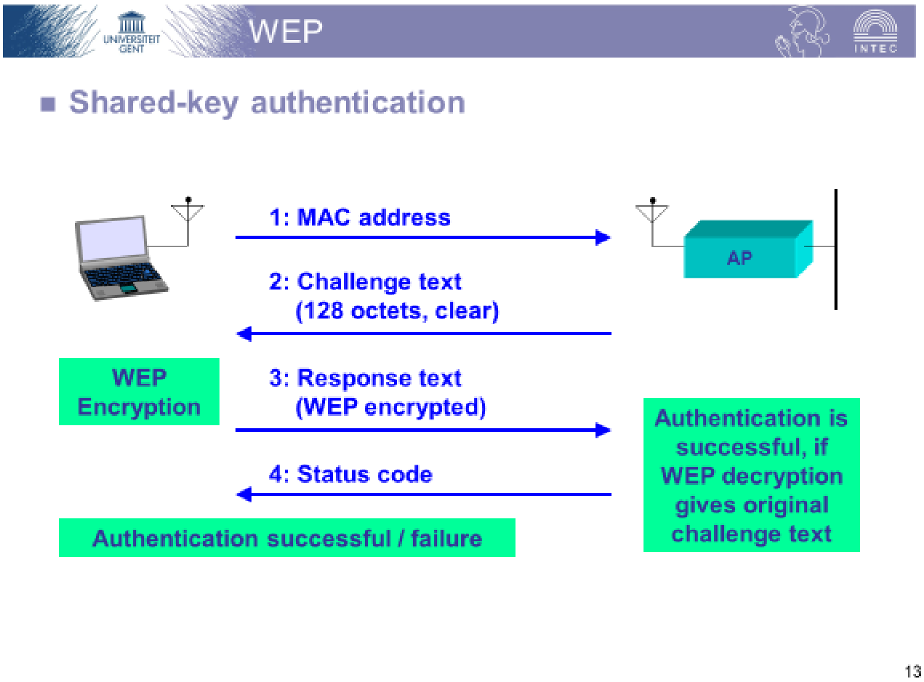
Open system authentication

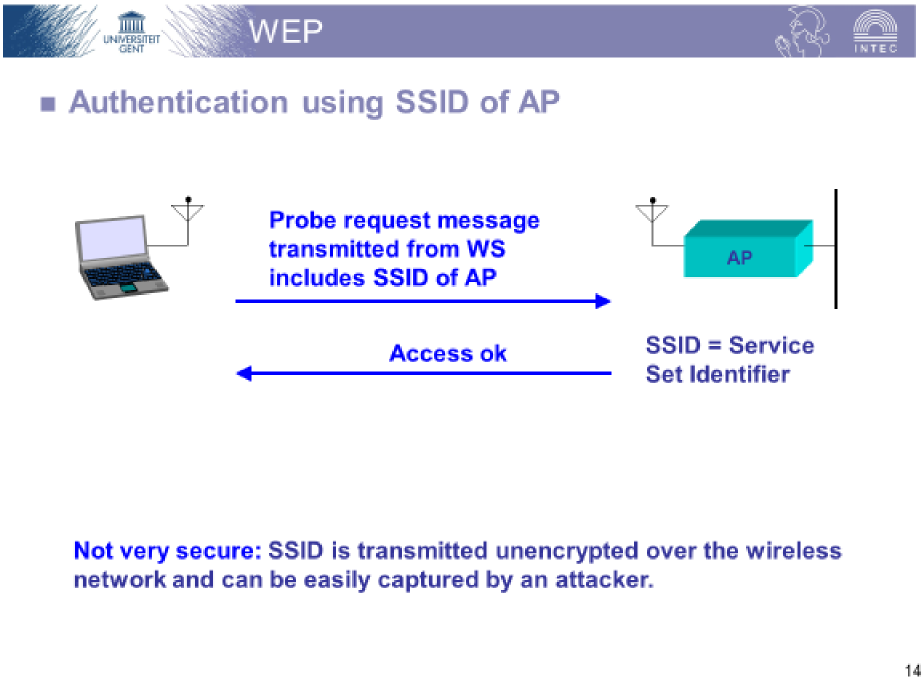


Status codes are defined in IEEE 802.11

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

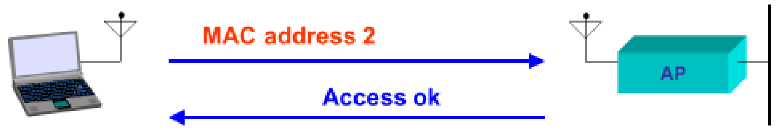
12


WEP
UNIVERSITEIT GENT
INTEC
Shared-key authentication
1: MAC address
AP
2: Challenge text
(128 octets, clear)
WEP Encryption
3: Response text
(WEP encrypted)
Authentication is successful, if WEP decryption gives original challenge text
4: Status code
Authentication successful / failure
13


WEP
UNIVERSITEIT GENT
INTEC
Authentication using SSID of AP
Probe request message transmitted from WS includes SSID of AP
AP
Access ok
SSID = Service Set Identifier
Not very secure: SSID is transmitted unencrypted over the wireless network and can be easily captured by an attacker.
14

WEP

- MAC address filtering



Accepted MAC addresses:

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

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.

15

WEP Vulnerabilities

- Small and static keys :
  - **Actual keyspace is 40 bits**
  - **No easy way to exchange and distribute keys.**
  - **Key change involves manually changing the key on each AP and Client.**
- Use of small, plaintext initialization vector (IV)
  - **IV is sent out in clear text usually at the starting of the packet.**
  - **Dictionary of IVs and keystreams**
    - Only 2^24 possibilities
    - Can be stored in 24GB disk space
    - Can be intercepted in a very short period of time on high traffic wireless networks.
- Weak encryption algorithms

16

To cracking the WEP key, typically the following steps are taken.

- The attacker sets the NIC drivers to Monitor Mode
- He begins capturing packets with Airsnort
- Airsnort quickly determines the SSID
- Sessions can be saved in Airsnort, and continued at a later date so you don't have to stay in one place for hours
- A few 1.5 hour sessions yield the encryption key

- Once the WEP key is cracked and his NIC is configured appropriately, the attacker is assigned an IP, and can access the WLAN

WLAN security using WPA (a precursor of IEEE 802.11i) is significantly improved compared to WEP security. WPA security includes the following features:

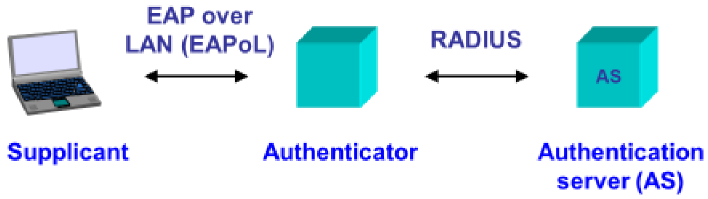
- Key management (using the 802.1X framework, it is also possible to use preshared keys)
- Authentication (using the 802.1X framework)
- Confidentiality (TKIP encryption)
- Integrity checking
- Protection against replay attacks.

Moreover, EAP (the authentication protocol) is extensible, making it more feature proof and allowing integration in custom company security systems.

WPA: authentication

802.1X defines three network entities:

- **Supplicant** (the wireless client in the wireless station),
- **authenticator** (in a WLAN usually the AP)
- **authentication server** (containing user-related authentication information).

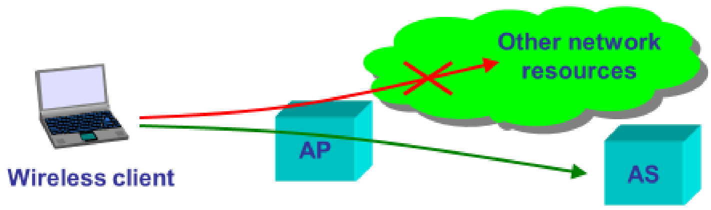


18

WPA authentication

802.1X authentication procedure (1)

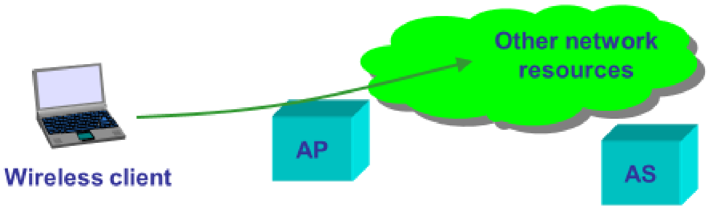
- With 802.1X, authentication occurs after association. However, prior to successful authentication, a wireless client is only allowed access to the AS. All other traffic is blocked at the AP.



19

WPA authentication

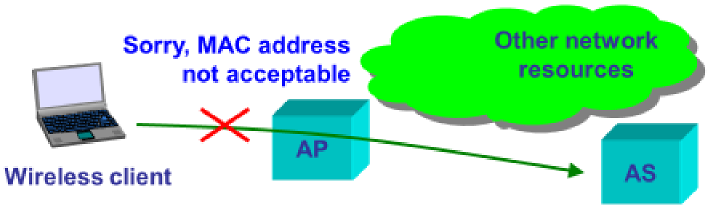
- 802.1X authentication procedure (2)
  - After successful authentication, the wireless client is granted access to other network resources by the AP.



20

WPA authentication

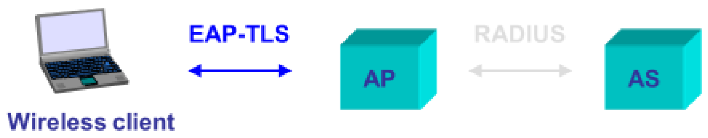
- 802.1X authentication procedure (3)
  - The authenticator (AP) can also perform authentication based on MAC address filtering (for preventing denial-of-service = DoS attacks) before starting the 802.1X authentication.



21

WPA authentication

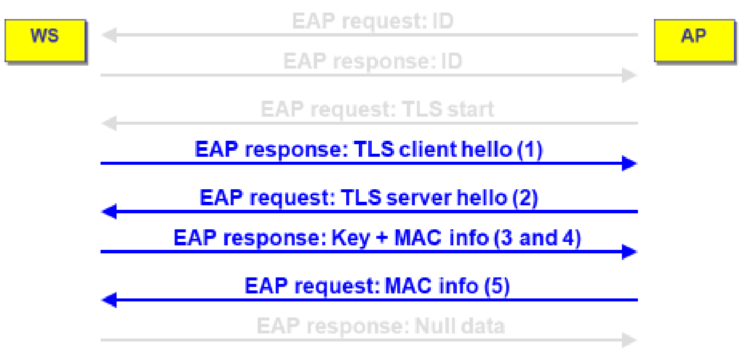
- **Example: EAP-TLS**
  - As an example, SSL/TLS is one of the various options defined to be used over EAP.
  - The SSL/TLS handshake sequence is embedded into a corresponding EAP sequence.



22

WPA authentication

- **EAP-TLS signaling sequence**



23

WPA authentication

- **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.**

24