# MAC Layer Key Hierarchies and Establishment Procedures

**Jukka Valkonen**

jukka.valkonen@tkk.fi

**17.11.2006**

# Agenda

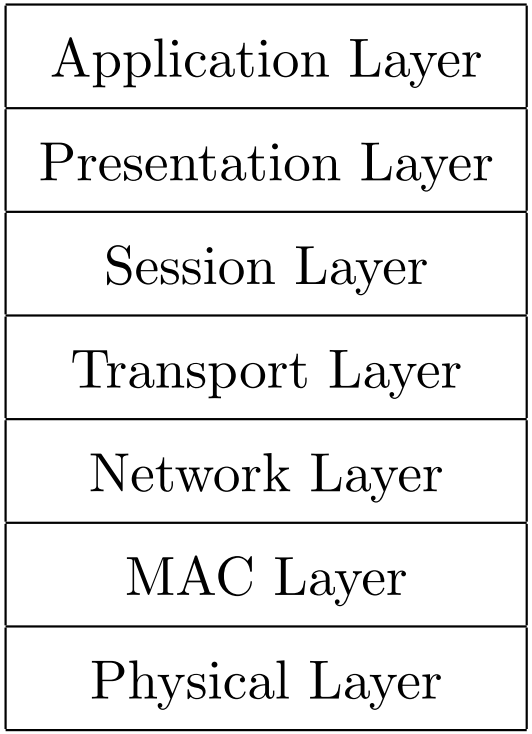
1. Introduction and Background
2. Pair-wise associations
3. Group associations
4. Different layers
5. Conclusions

# Introduction

- Key negotiation methods and hierarchies based on standards
- WiMedia's UWB
  - Short range radio platform
  - Speeds up to 480 Mbit/s
  - For example Wireless USB
- WLAN
  - Set of standards
  - Speeds up to 540 Mbit/s (802.11n)

# Key exchange in different layers

- MAC-layer
  - For example the standards in the paper
- Upper layers
  - For example MANA-protocols
- Keys need to be distributed between the levels



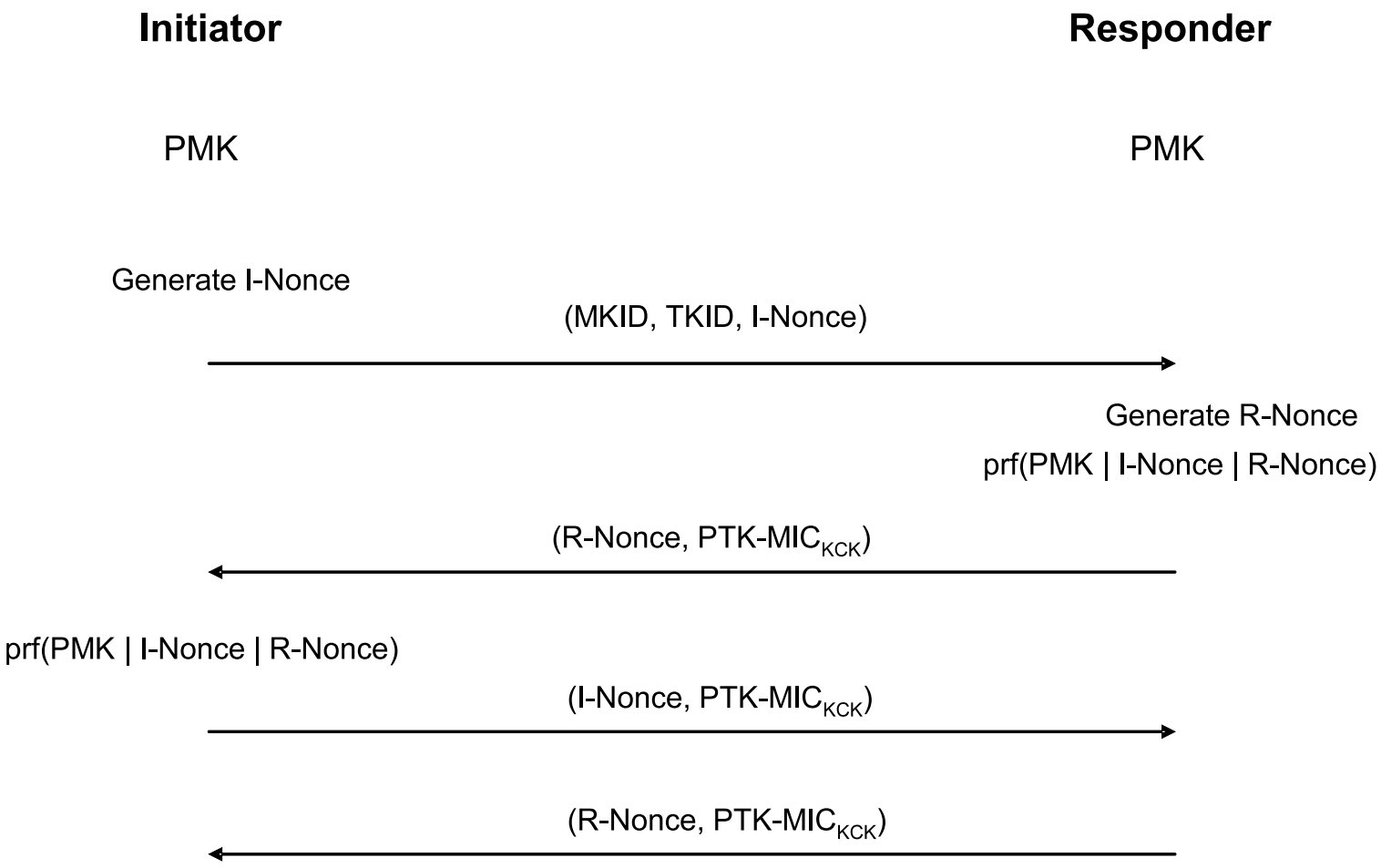
## Pair-wise keys

- Both standards use a pre-shared key (PSK)
  - Also known as pair-wise master key (PMK)
- Devices exchange random nonces using a 4-way handshake
- Keys are derived from the PMK and random nonces
  - Also information such as addresses are used

# UWB 4-way handshake (1/2)

- Initiator and Responder
- PMK is identified by master key identifier (MKID)
- PTK is identified by temporal key identifier (TKID)
  - Unique at the moment
- Devices exchange fresh random nonces
- After the devices have exhanged the data, the derive the keys using pseudo-random function
  - Pair-wise temporal key (PTK)
  - Key confirmation key (KCK)

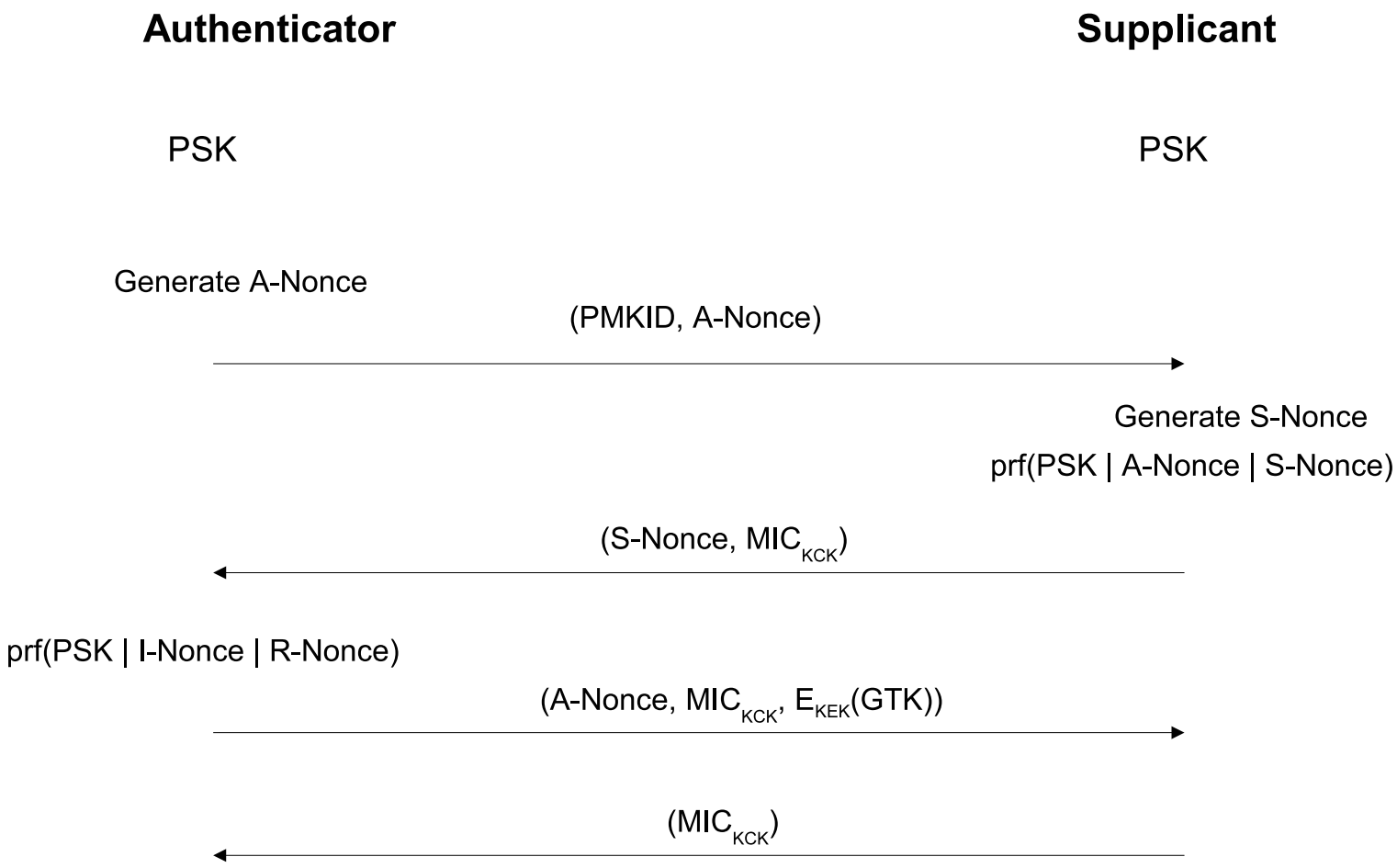
# UWB 4-way handshake (2/2)



# WLAN 4-way handshake (1/2)

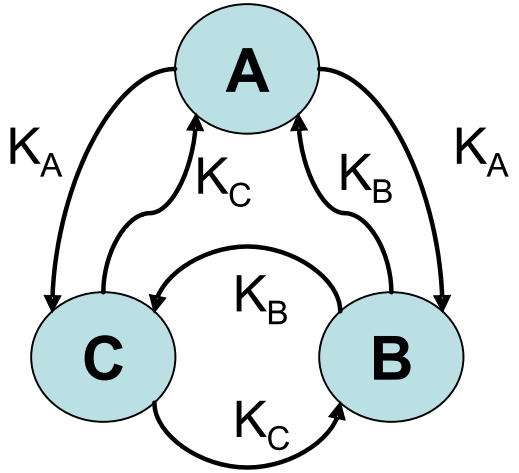
- Authenticator and Supplicant
- Associations can be built between two stations or between a station and an access point
  - Ad-hoc or infrastructure mode
- Devices share pair-wise master key security association (PMKSA) identified using PMKID
- From known and exchaned material devices derive three keys: Key confirmation key (KCK), key encryption key (KEK) and temporal key (TK)

# WLAN 4-way handshake (2/2)



# What about groups?

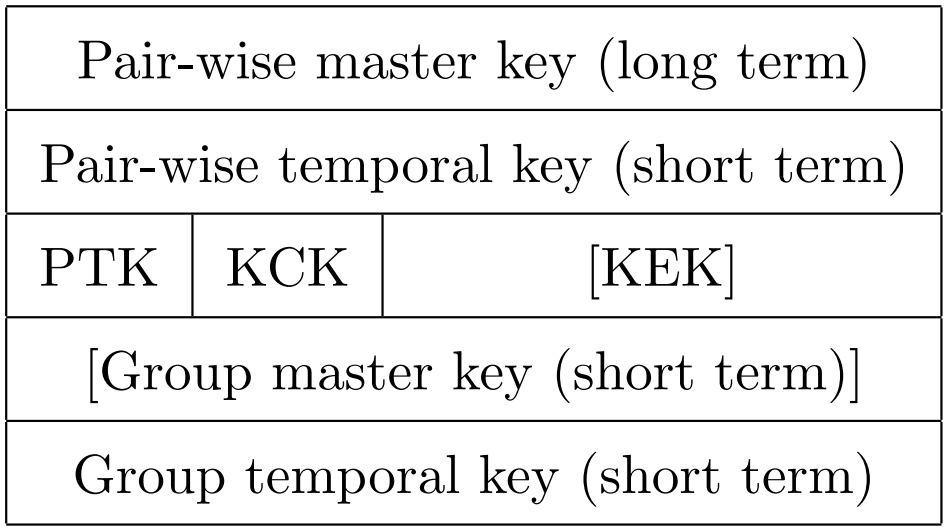
- Both standards provides means to negotiate multicast groups
- Groups are built using pair-wise associations
- Groups are unidirectional
  - Same key is never used for encryption and decryption
  - A device distributes the key it uses for encryption, the recipients save the key to use for decryption



# Distribution of group keys

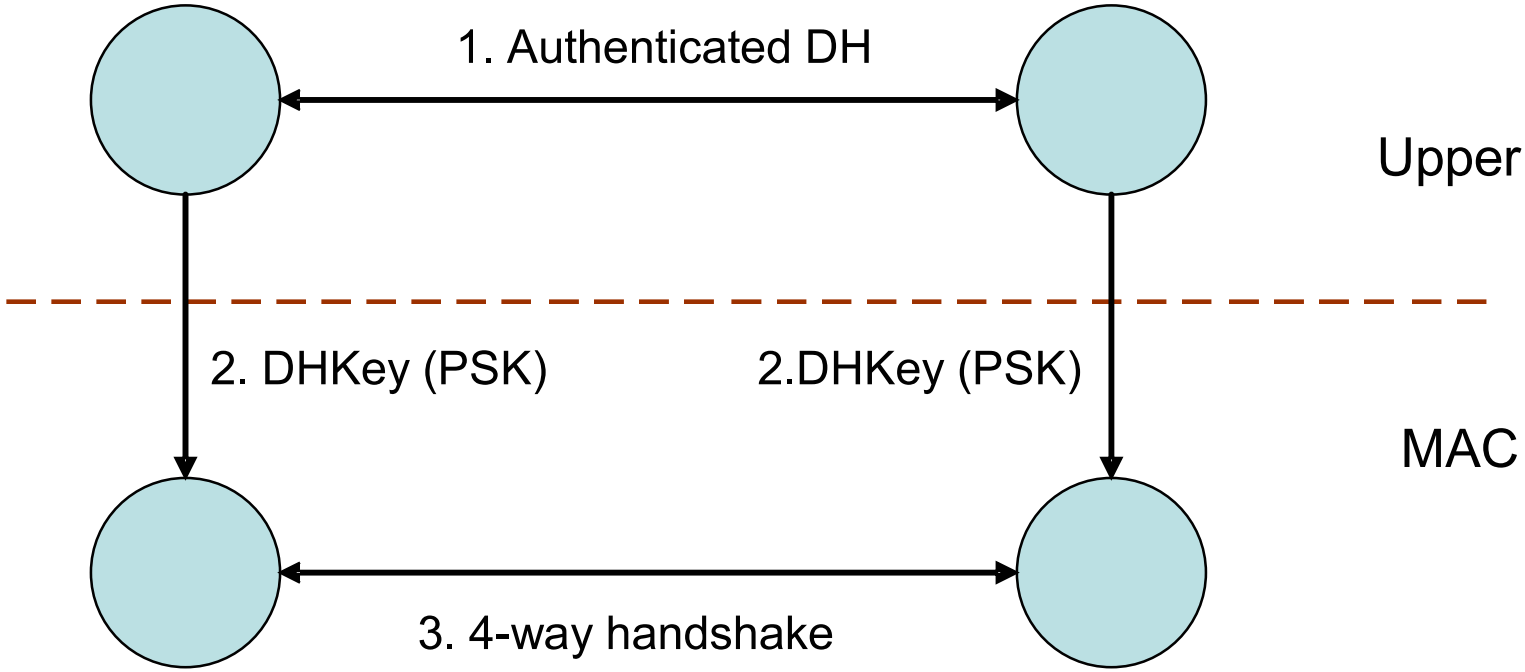
- UWB
  - Devices exchange group keys after the handshake is performed
  - Possible to exchange keys using one association
- WLAN
  - Devices send the group key in the third message of the handshake
  - To exchange key to both directions, two associations must be built
  - Also provides so called Group Key handshake

# Key hierarchies



# Negotiation of PMKs

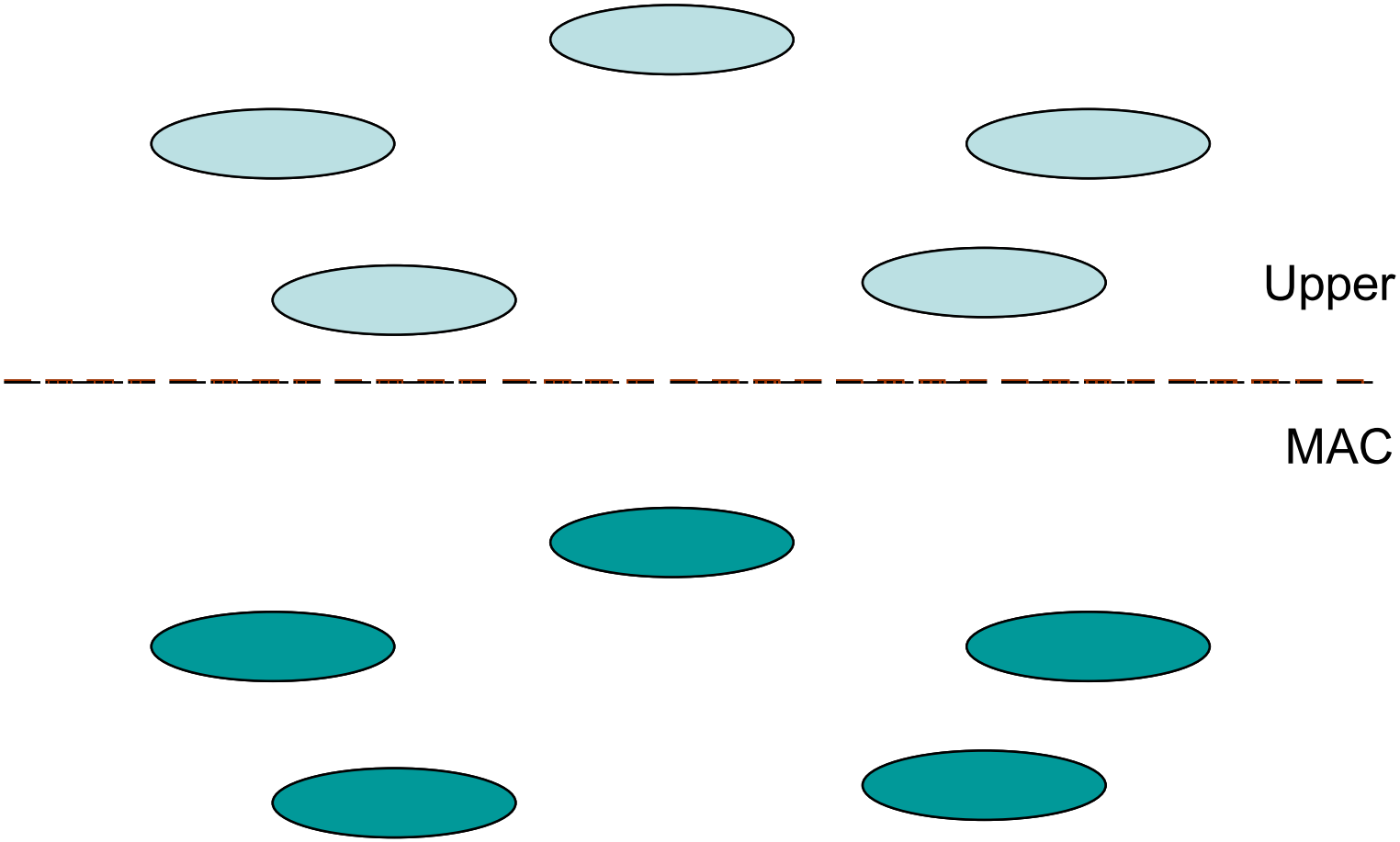
- The PSK can be negotiated using upper layer protocols



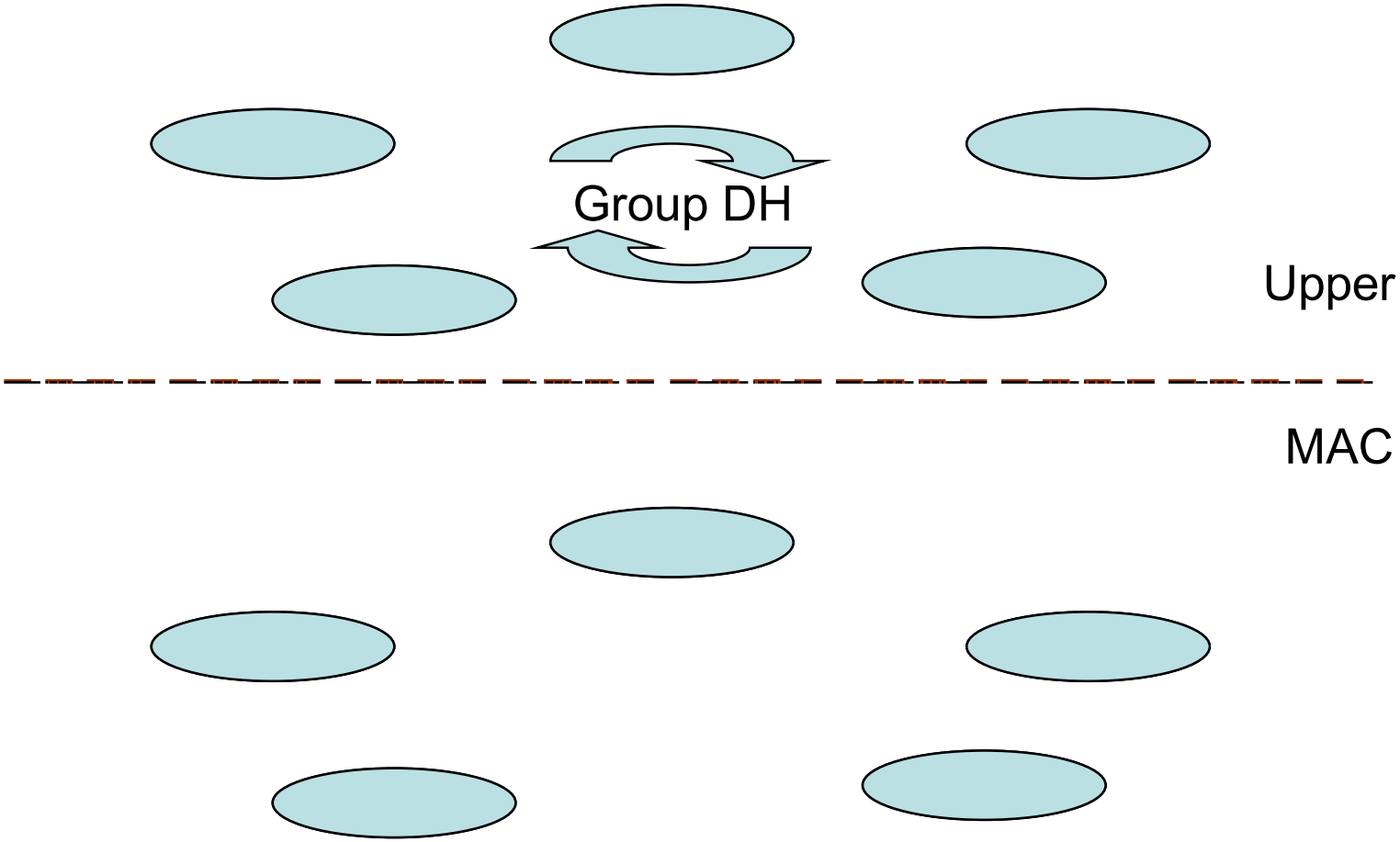
# Forming groups on upper layers

- WLAN in ad-hoc mode or UWB
- Make devices share same PSK
  - Devices use the same PSK to derive the pair-wise keys
  - The PSK identifies the group
    - An attacker is not able to force devices to belong to a group without they knowing
  - Each device possessing the key can take new members
  - Only devices having the same key can join the group

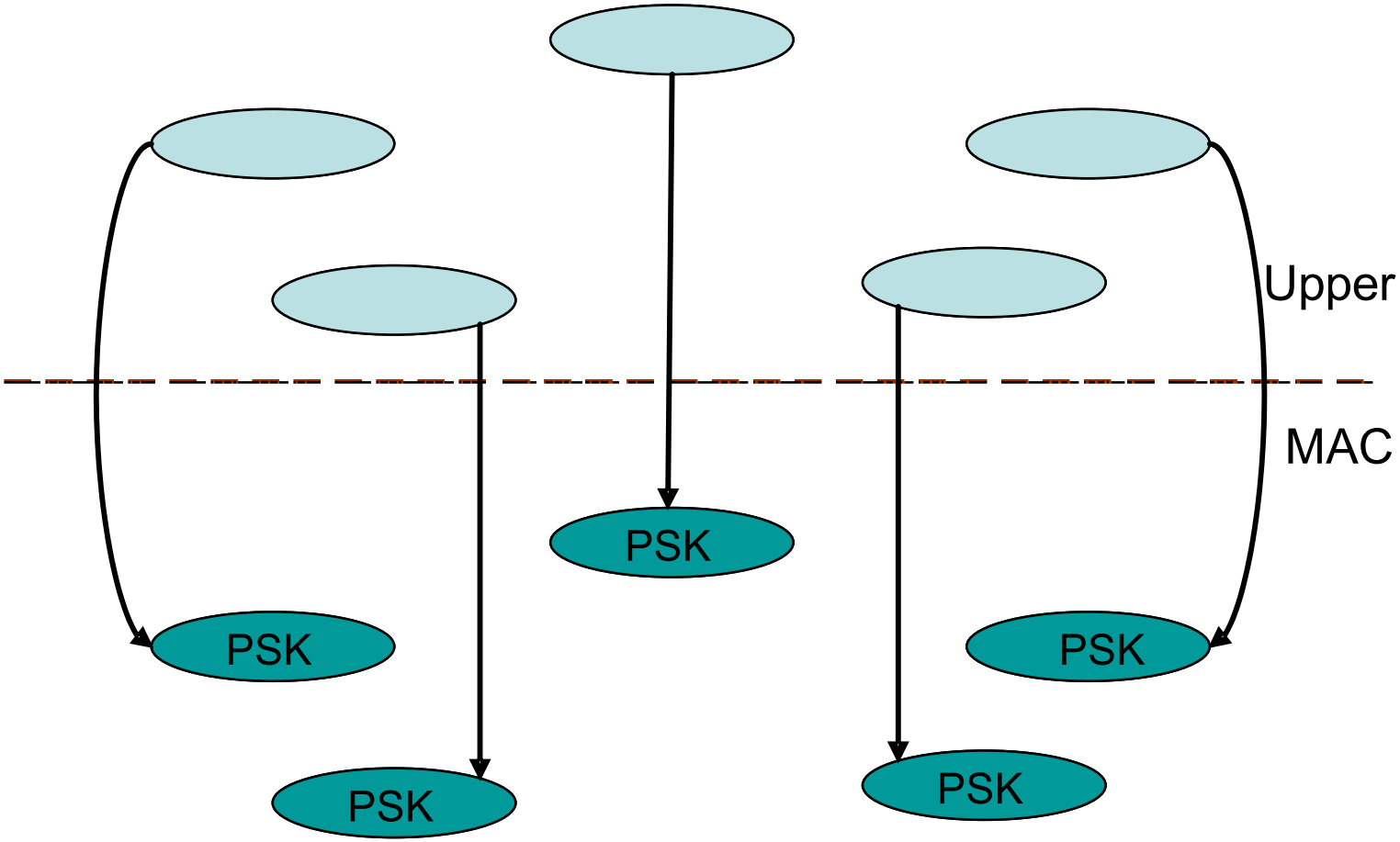
# Distribution of the group PSK (1/5)



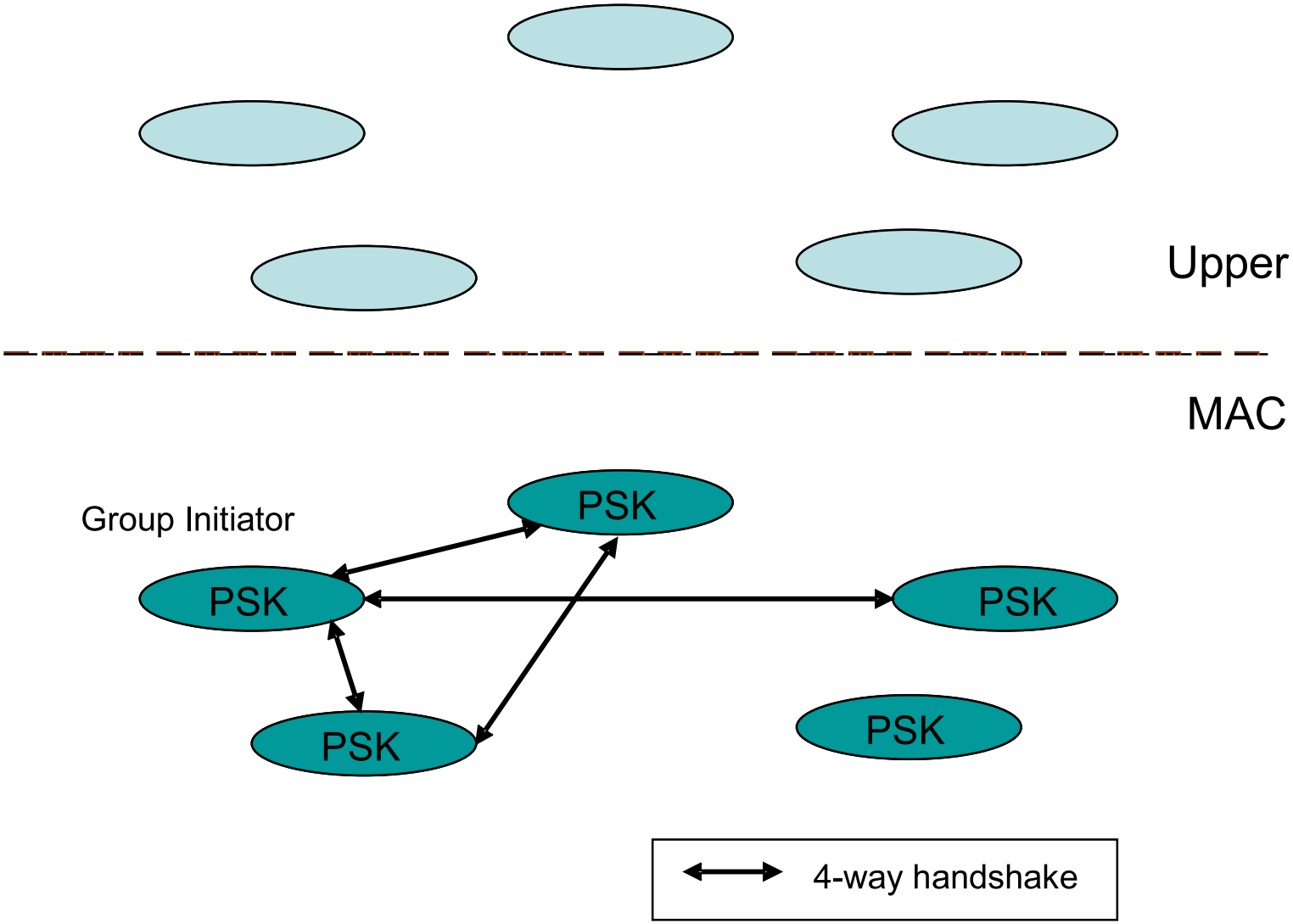
# Distribution of the group PSK (2/5)



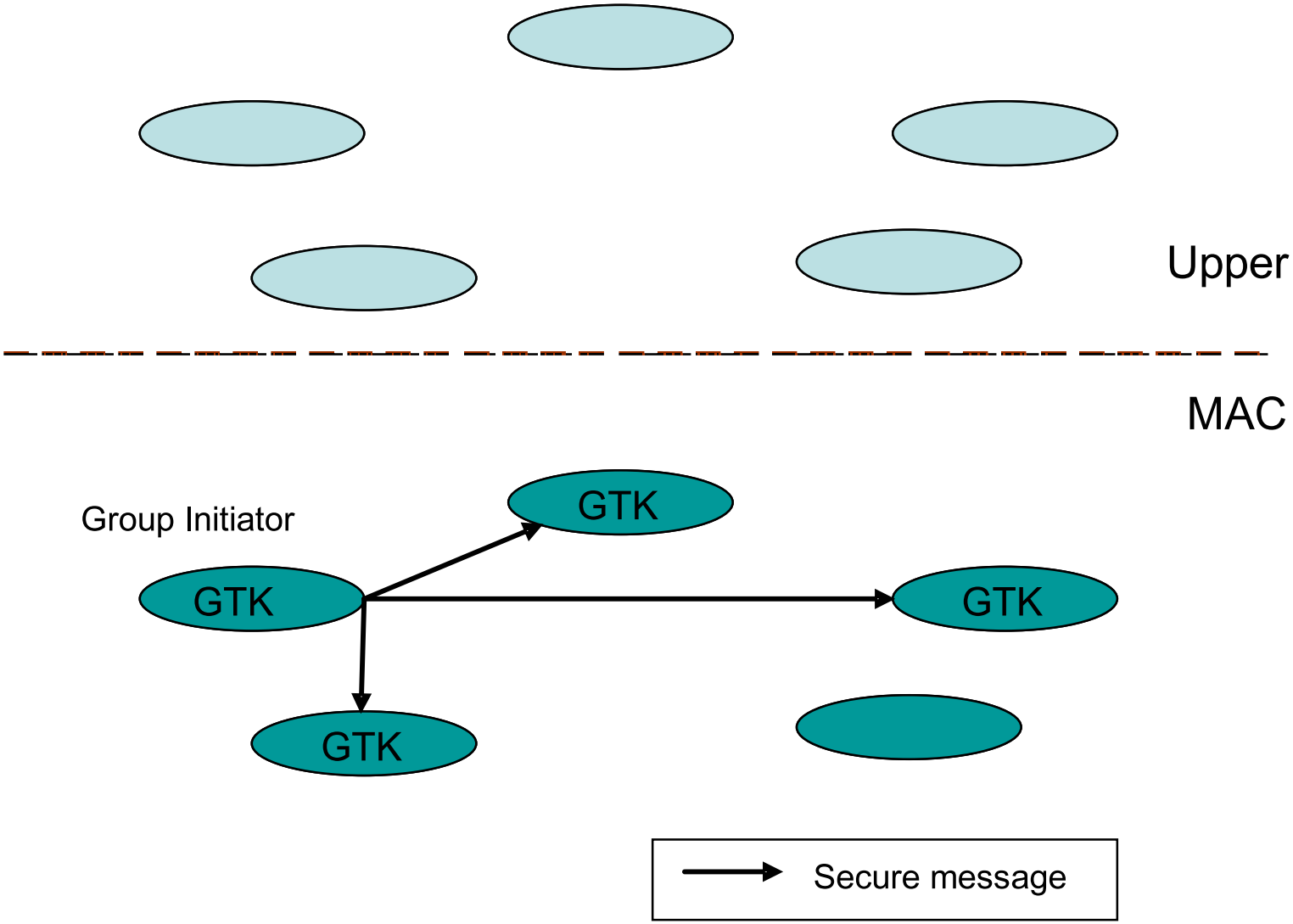
# Distribution of the group PSK (3/5)



# Distribution of the group PSK (4/5)



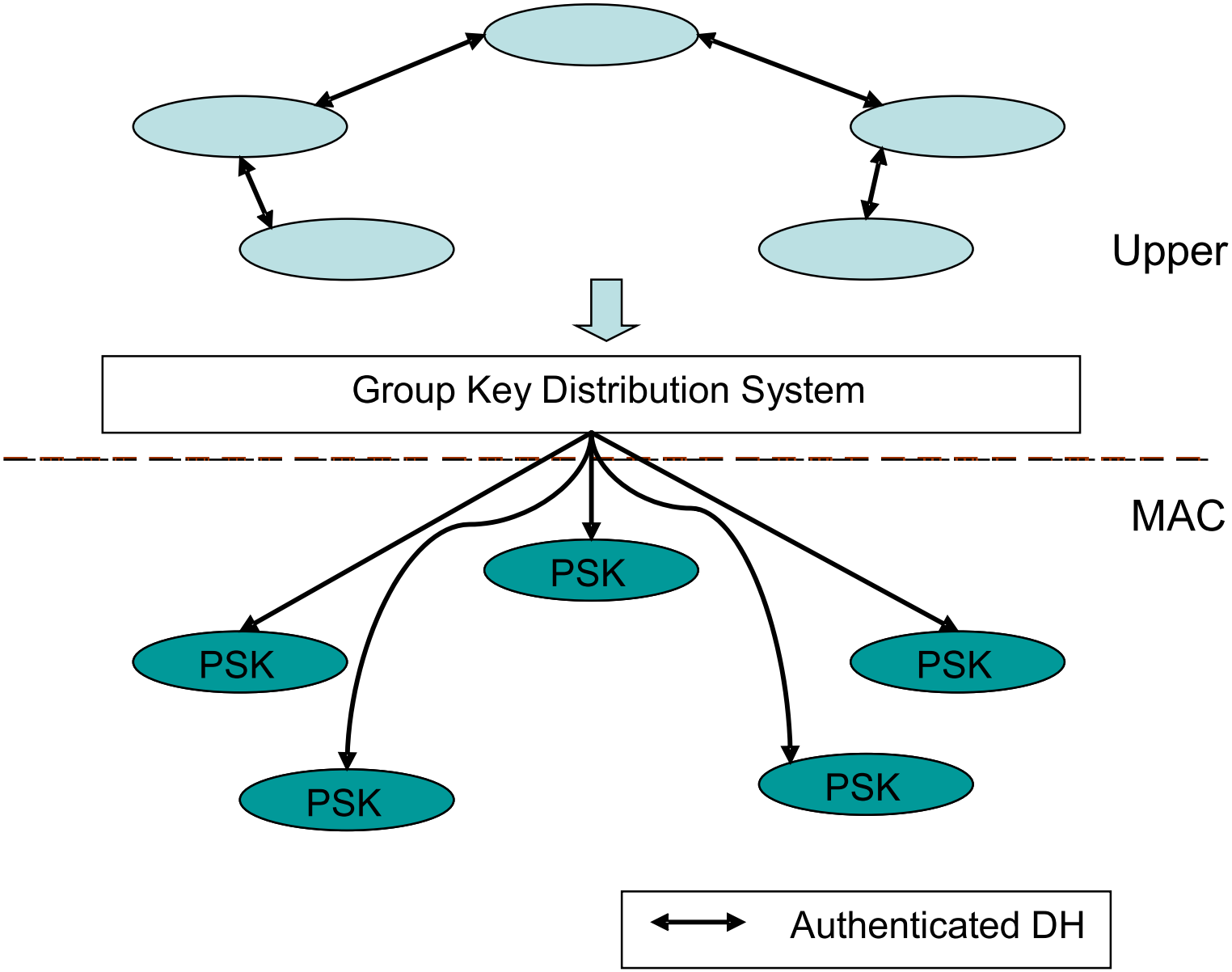
# Distribution of the group PSK (5/5)



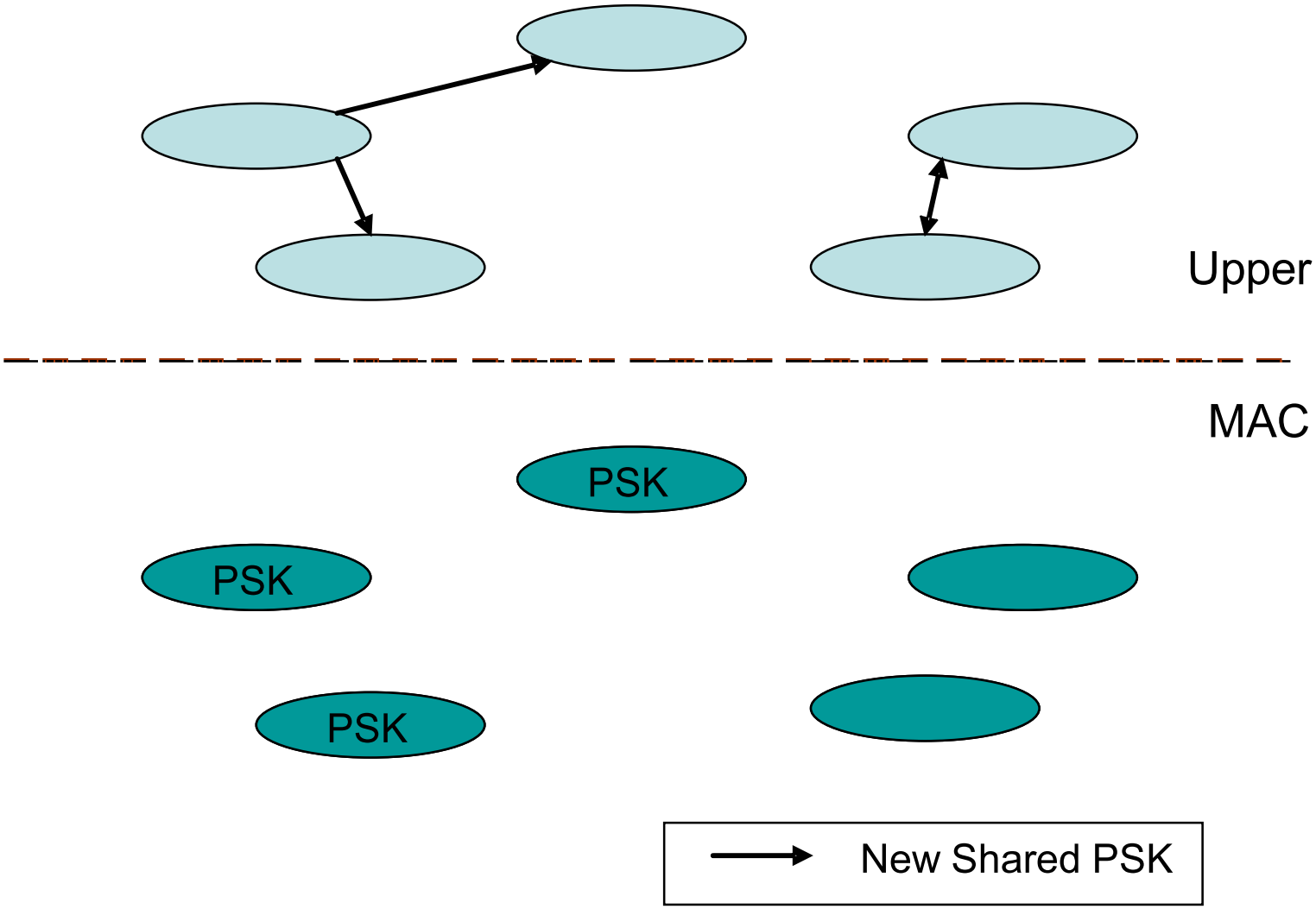
# Issues

- Revoking a device
  - All devices (are able to) know all secrets
  - New associations must be built in the upper levels
- What if we use pair-wise associations on the upper level?

# Group Keys using pair-wise associations



# Revoking a device



# Conclusions

- Group key negotiation has its problems
- The standards don't provide perfect forward secrecy
- The methods seem to be appriopriate for deriving session keys

# Thank You!

# Questions?