Trust Model in Media Independent Handover Service:

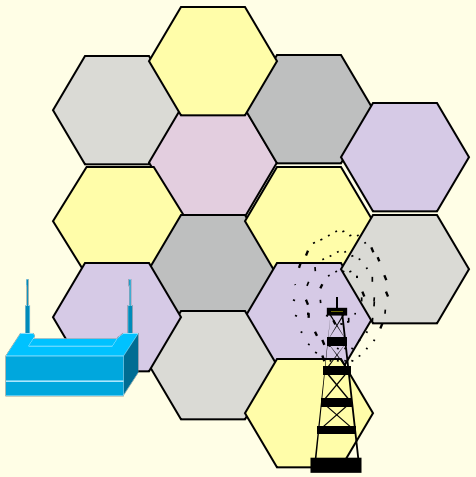
- Can the security of MIH service be media independent?

Lily Chen

Lily.chen@nist.gov

Key Words

- Media Independent (e.g. 802.11 or 802.16)
- Handover
- Service (explanations will come next)

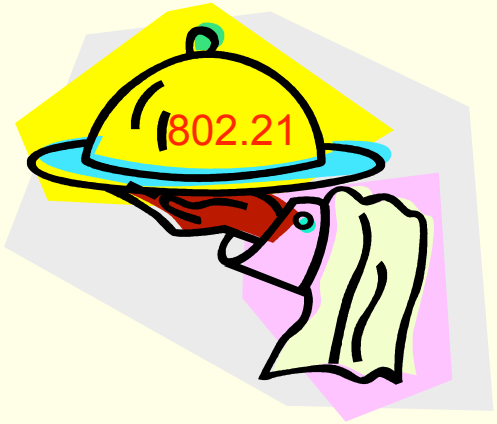


Scope

- Protect Media Independent Handover (MIH) Service

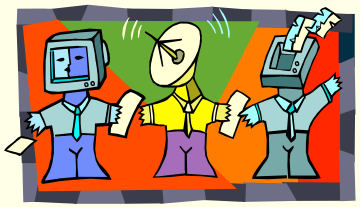
- MIH is a set of services to support the handover. It includes
  - Information Service – provide information to facilitate the handover;
  - Event Service – detect the need for handover; and
  - Command Service – deliver handover decisions.

- This talk is all about how to protect the services.
  - It should not be confused with media traffic protections.



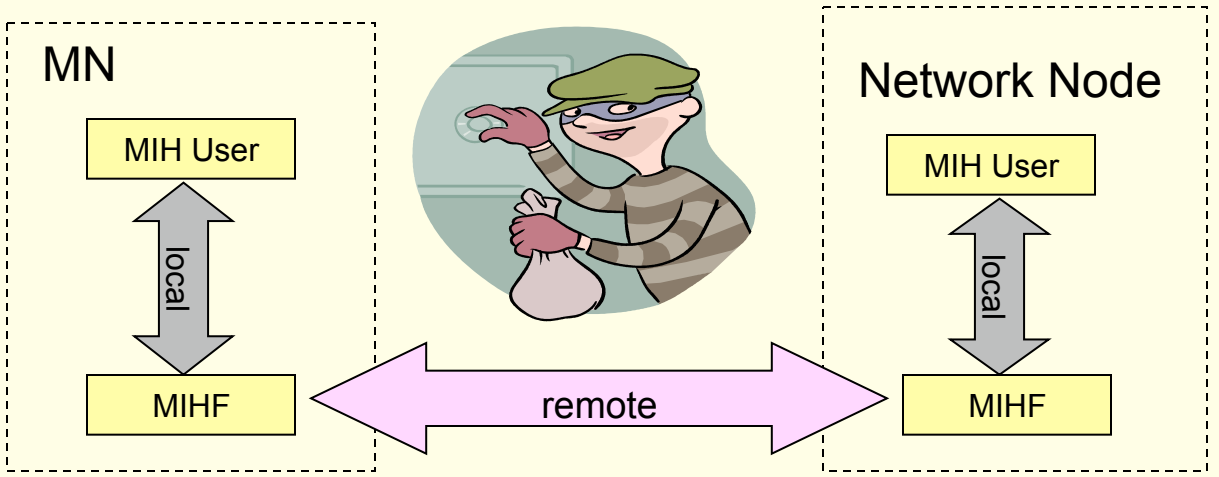
MIH Service
– As Specified in IEEE 802.21

- IEEE 802.21 specifies
  - The information elements to be exchanged.
  - Information structure and its representation.
- MIH Function (MIHF)
  - The entity to process MIH information elements.
  - It can be located in Mobile Nodes which support MIH and also the network entities, called Point of Services (PoSs).
- MIH User
  - The entity using MIH service.

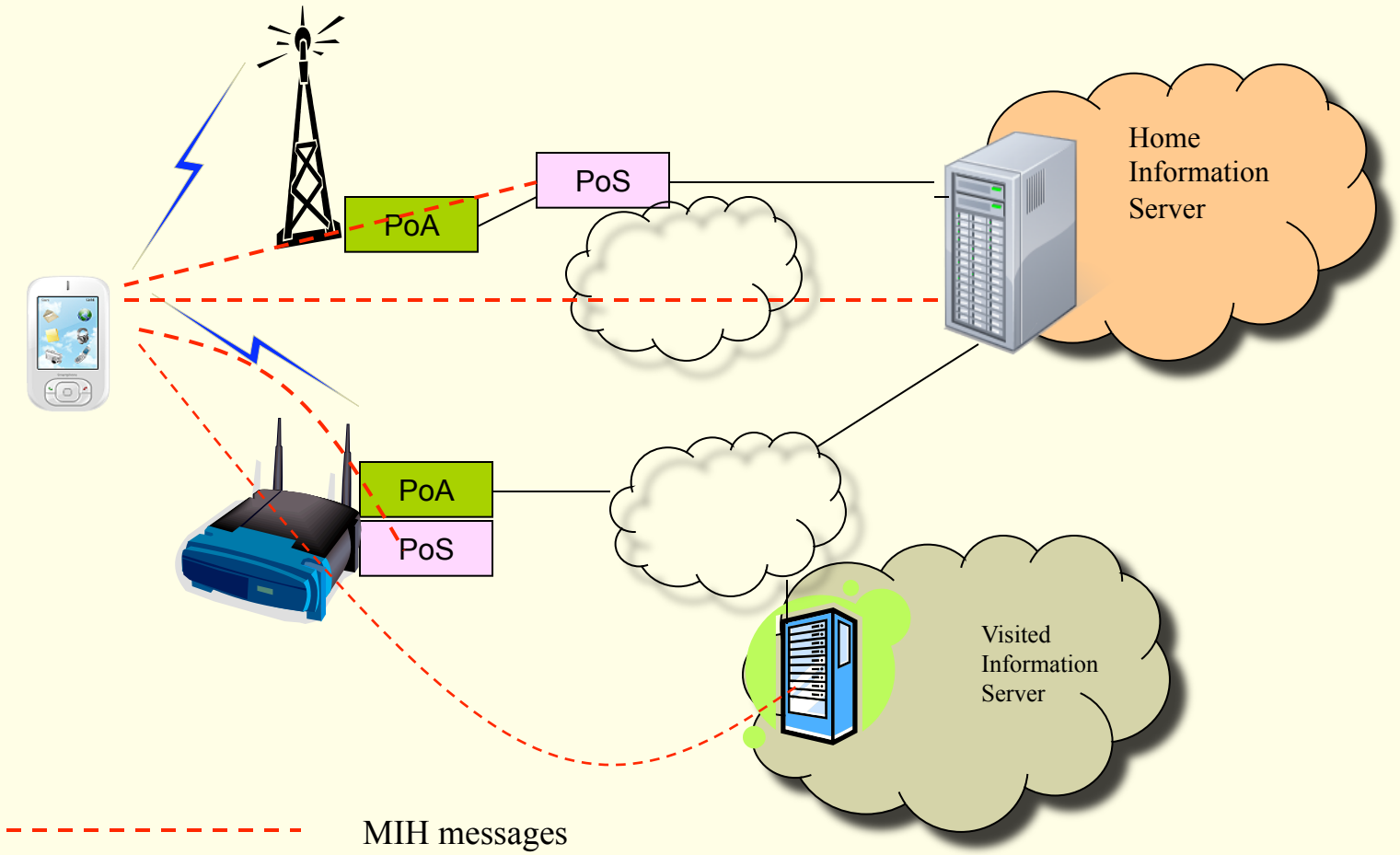


MIH Service
– Protocol Interface

- The MIH information elements can be communicated
  - Locally (inside an MN or a network node); or
  - Remotely (between an MN and a network node).
- The remotely communicated information needs to be protected.

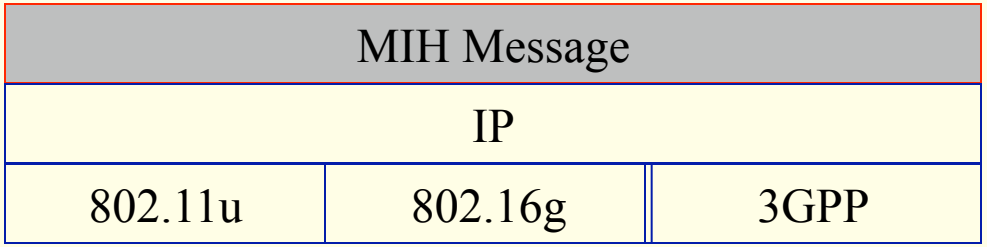


MIH Service – Network Architecture



Transport MIH Messages

- MIH messages can be transported by
  - Layer 3 protocols (work in IETF mipshop);
  - 802.11 (containers in 802.11u)
  - 802.16 (containers in 802.16g)
  - 3GPP - SAE



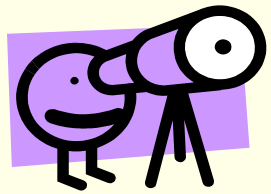
Key Questions

- In order to protect MIH messages, we need to determine
  - Should an MIHF be authenticated as an entity?
  - At which layer, should the messages be protected?
  - Should or shouldn't it depend on transport protocol for the protections?
- Who will make the decision?

MIH Message		
IP		
802.11u	802.16g	3GPP

A Close Look

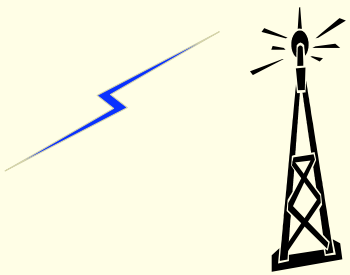
- In order to establish a trust model, we will need information on
  - Who will provide MIH service.
    - Media service provider, e.g. operators; or
    - MIH Service provider, if it is different from media service provider.
  - How the services are provided.
    - Subscription based; or
    - Free of charge.
- Do these matter? Yes.



For Media Service

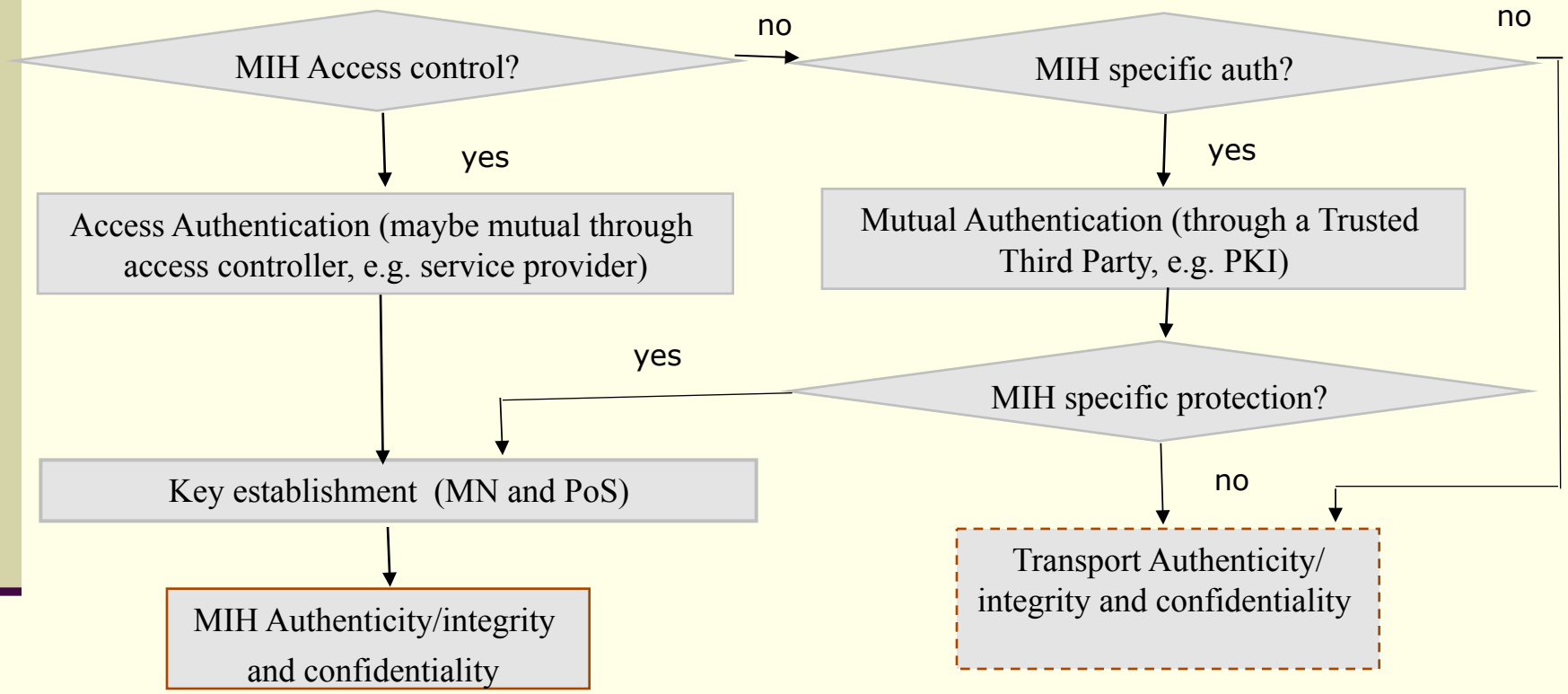
– Make a comparison

- The services are usually subscription based.
- Home service domain determines the trust model, authentication protocols, and protection profile.
  - The service provider will facilitate a centralized server to
    - Authenticate the users (for access control); and
    - Establish keys (e.g. 3GPP AKA, EAP, etc).
  - The protections are media specific, e.g.
    - 3GPP uses Kasumi; and
    - 802.11i uses AES CCM.



Possible Situations

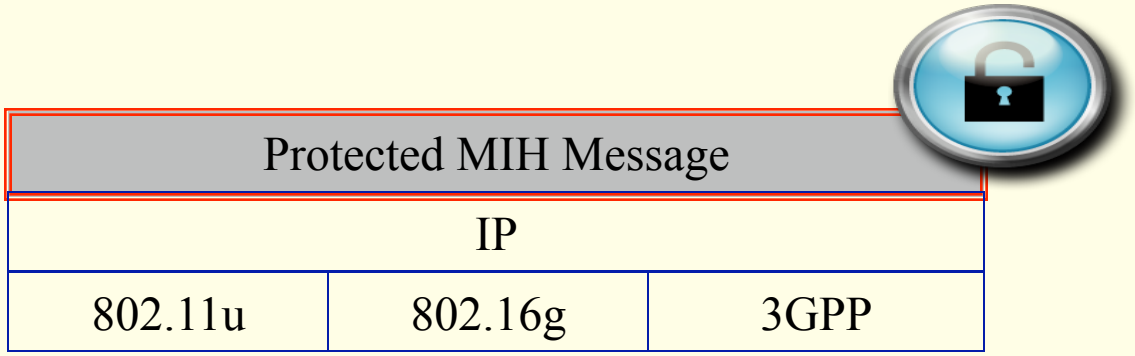
- A way to think



MIH Specific Protections

- Secure features

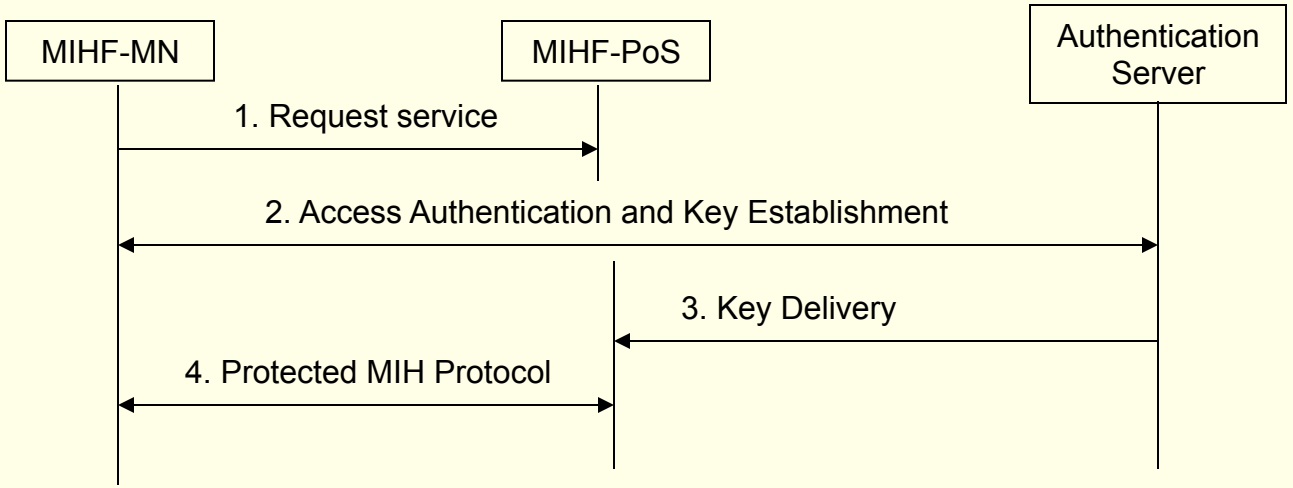
- The authentication is conducted on MIHF identity.
- The protections are end-to-end (from MIHF-MN to MIHF- PoS or from MIHF-PoS_1 to MIHF-PoS_2).
- It provides protection in uniform strength without depending on the transport protocols.



MIH Specific Protections

- With access control (use centralized server)

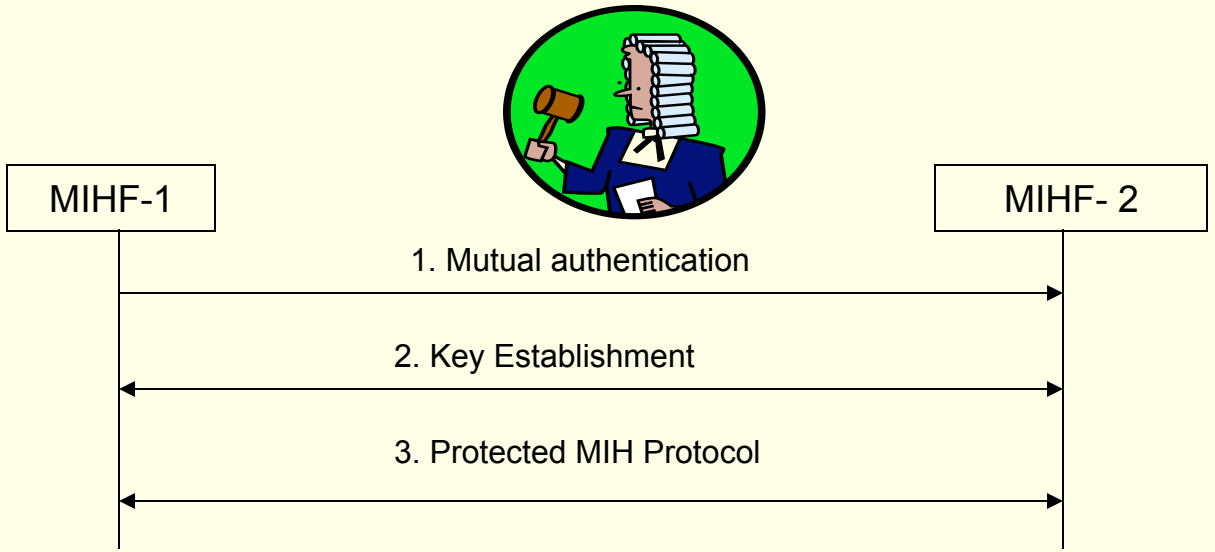
- If access control is applied, then a centralized authentication server or EAP server is needed.
- MIH specific keys can be established with the authentication server.
- The keys can be delivered to PoS so that MIH specific protections are applied.



MIH Specific Protections

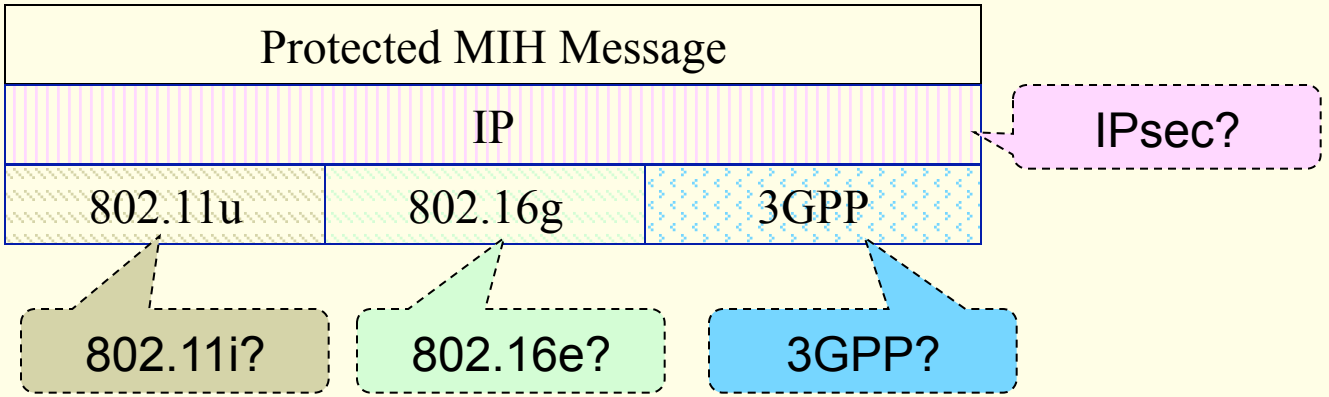
- Without access control (use a trusted third party)

- MIHF-MN and MIHF-PoS (or MIHF-POS_1 and MIHF-POS_2) authenticate each other using a trusted third party, e.g. Certificate Authority (CA).
- MIHF-MN and MIHF-PoS establish MIH specific keys.



However,

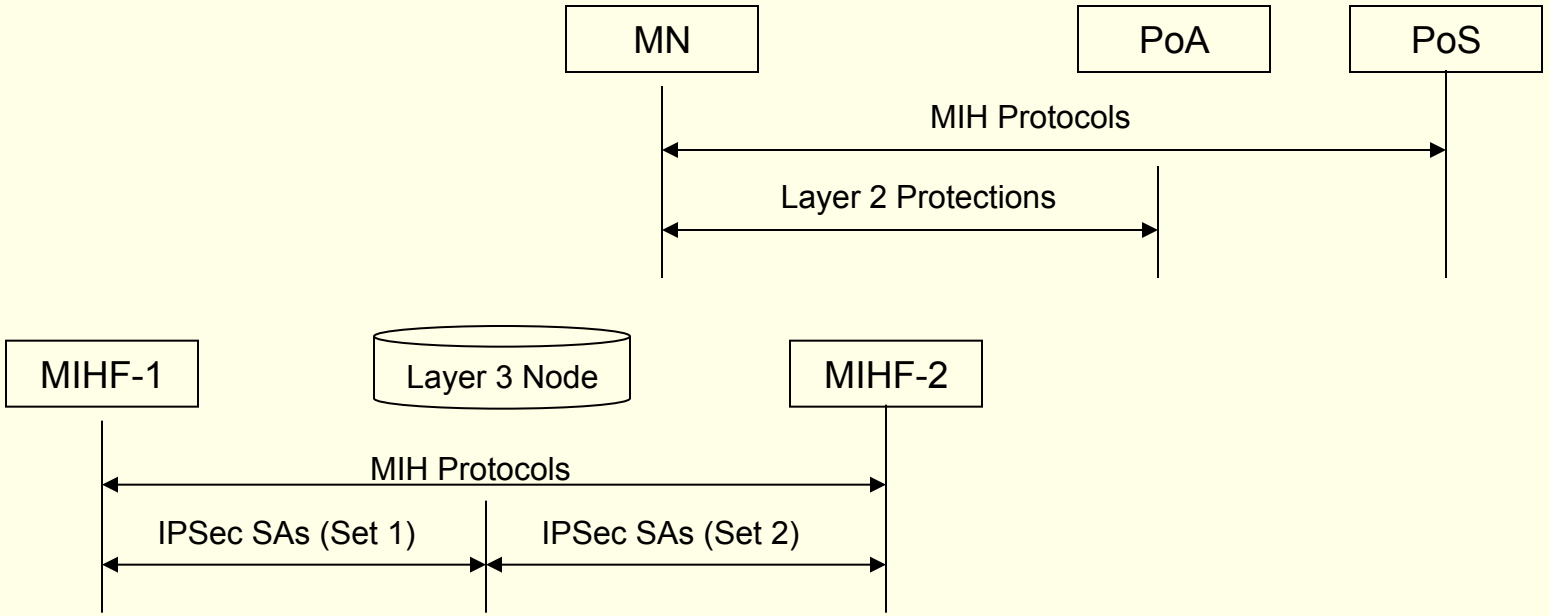
- If MIH is not subscription based, then
  - who will run the server? – No centralized database.
- If it is not a profitable service, then
  - why invest on infrastructure for security?
- Therefore, it is possible that the MIH messages have to depend on the transport protocols to be protected, e.g. IPsec, 802.11i, or 802.16.



Depend on Transport Protocol

- What are the issues?

- The protections are not MIH specific
  - The source ID for message authentication may be an IP address or a MAC address. It may not have anything to do with MIH.
- The protections may not be end-to-end.
- The security strengths may not be the same for different transport protocols.
- When the transport protocols are not protected, then MIH messages are not protected.



Depend on Transport Protocol

- Possible way to handle the issues

- Include MIH service as a feature in media access authentication.
  - Maybe also include MIH service as a roaming parameter.
- Apply media service provider supported identity binding
  - Bind MIHF identity to IP address or MAC address.
- Look into MIH specific threat model for countermeasures
  - The threats to MIHF service need to be detailed to apply countermeasures
- Enhance protections on transport protocols
  - This is a win-win approach.

Conclusion

- Media Independent Handover services are intended to provide media independent mobility.
- The way the services are delivered will determine the trust model and security protections. It is not a pure technical decision.
- MIH Protections may not be media independent !