中国2010年上海世博会全球合作伙伴
Global Partner of Expo 2010 Shanghai China

Relay Node Discussion

China Mobile

Outline

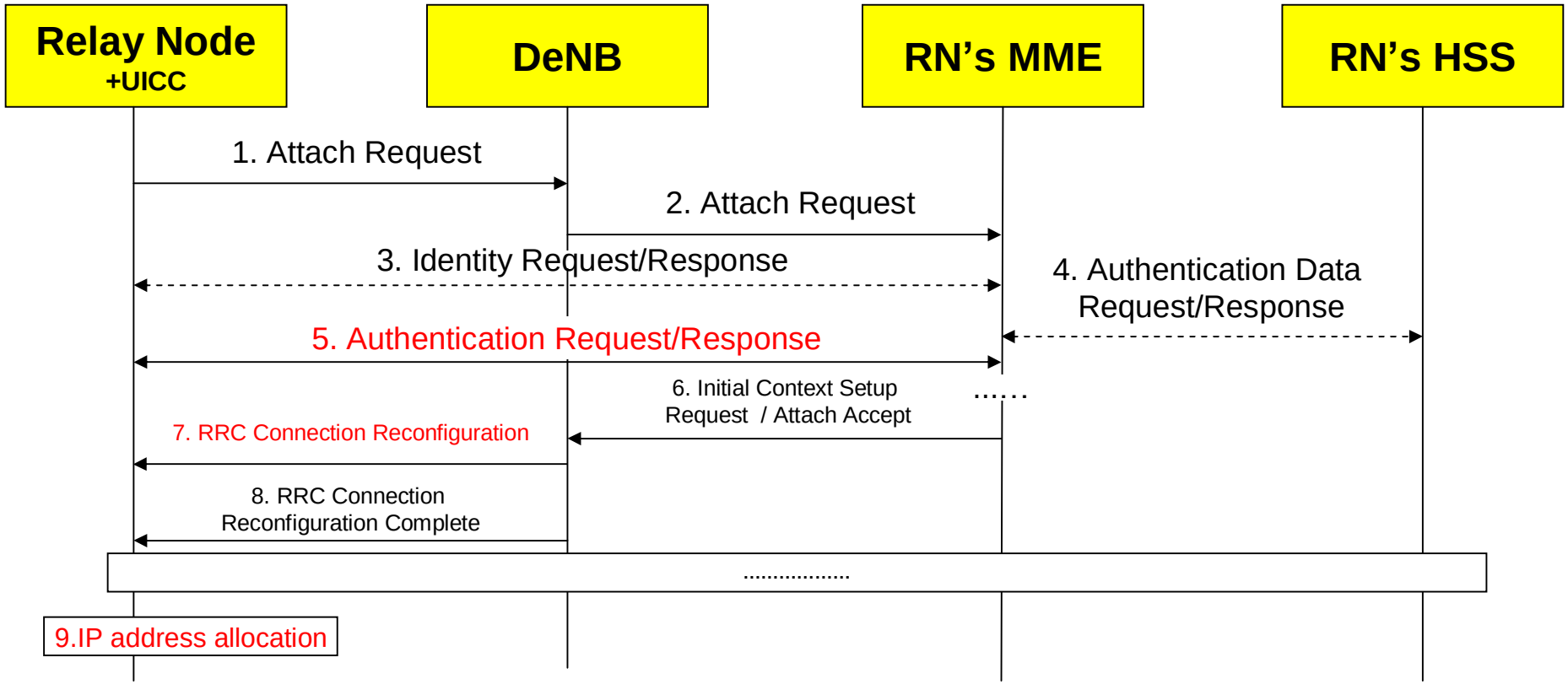
1. Relay Node user authentication/device authentication
2. AKA bootstrapping in IPsec vs certificate based IKE
3. New Proposals for Relay Node authentication and protection

1/Part 1---Double or single authentication

- **UICC based**
  1. **Removable**
     - UICC shall be authenticated when RN is attached to the network as a legacy UE. It can be seen as User Authentication.
     - RN device should be authenticated when IP connection between RN and network is established after the wireless bearer set up. It can be seen as Device Authentication.
     - Because UICC is removable, user authentication and device authentication is independently.
     - **So the double authentication is needed.**
  2. **Non-removable**
     - UICC shall be authenticated when RN is attached to the network as a legacy UE. It can be seen as User Authentication.
     - Because the UICC is non-removable (physically), it means the RN device is identified when UICC is authenticated.
     - **So single user authentication is enough for non-removable UICC based RN.**

Proposal 1: We propose to mandate the user authentication by UICC and single authentication when there is physical binding

2/Part 1---RN initial attach procedure



So conclusion 1: User AKA authentication is prior to the device authentication if both user and device authentication exist.

3/Part 1--AKA cannot be performed without UICC

1. RAN2/3 specifies RN should connect the network as legacy UE. So AKA shall be performed。
2. If RN does not contain a UICC and want to perform AKA, there are some kinds of problems as follows

1. AKA root key is permanent and should not be decomposed from a soft device.

1. Device is not like card, attacker can easily get the root key from the device environment. .

2. There is no secure root key provisioning solution to the device.

2. There is mature provisioning scheme for the card

3. CK and IK can be in the same level to be disclosed in the UICC or not. But K will be more easily disclosed without UICC case, so it is more dangerous in the case without UICC.

3. So UICC and not UICC are different in the protection of K

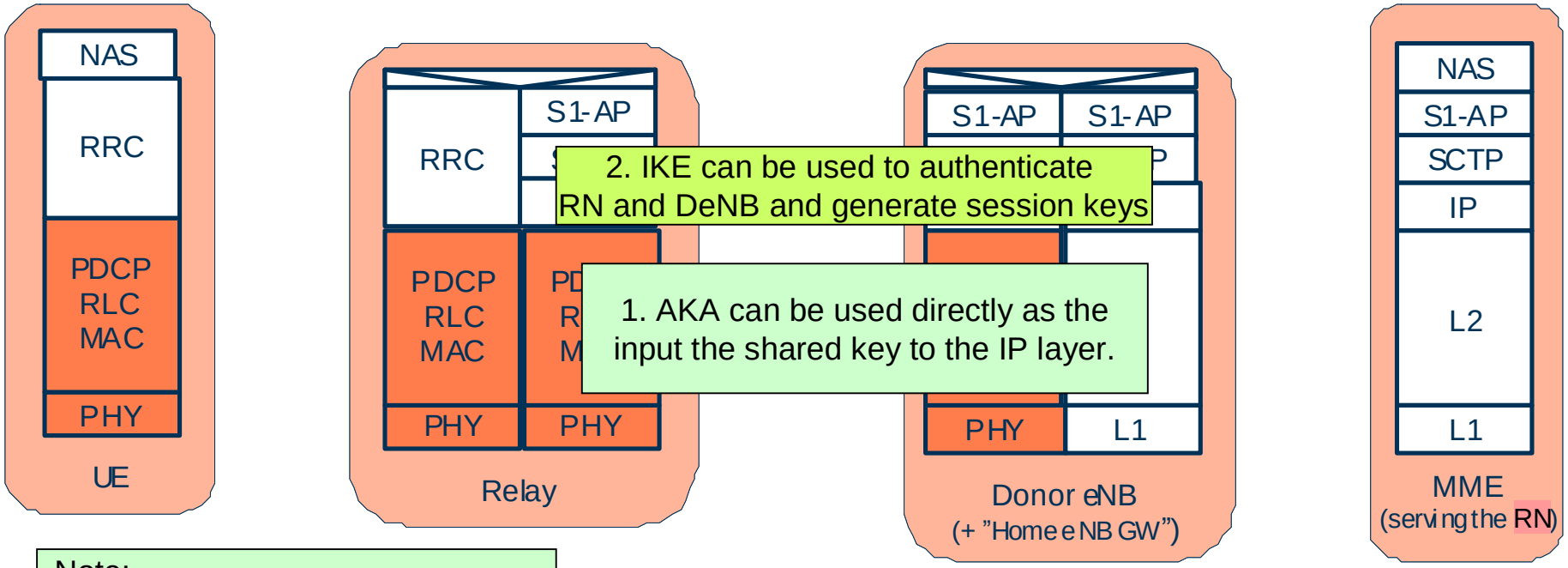
3. Yet based on RAN3, AKA is needed.

So conclusion 1: as for the user authentication, it performs the AKA, then UICC is a pre-requisite

4/Part 1---conclusions

1. **We propose to mandate the user authentication by UICC, single authentication when there is physical binding**
   - **User authentication is prior to the device authentication if both are needed.**
2. **AKA without UICC is not possible and not secure**

1/Part 2---IKE may not necessary when AKA is run



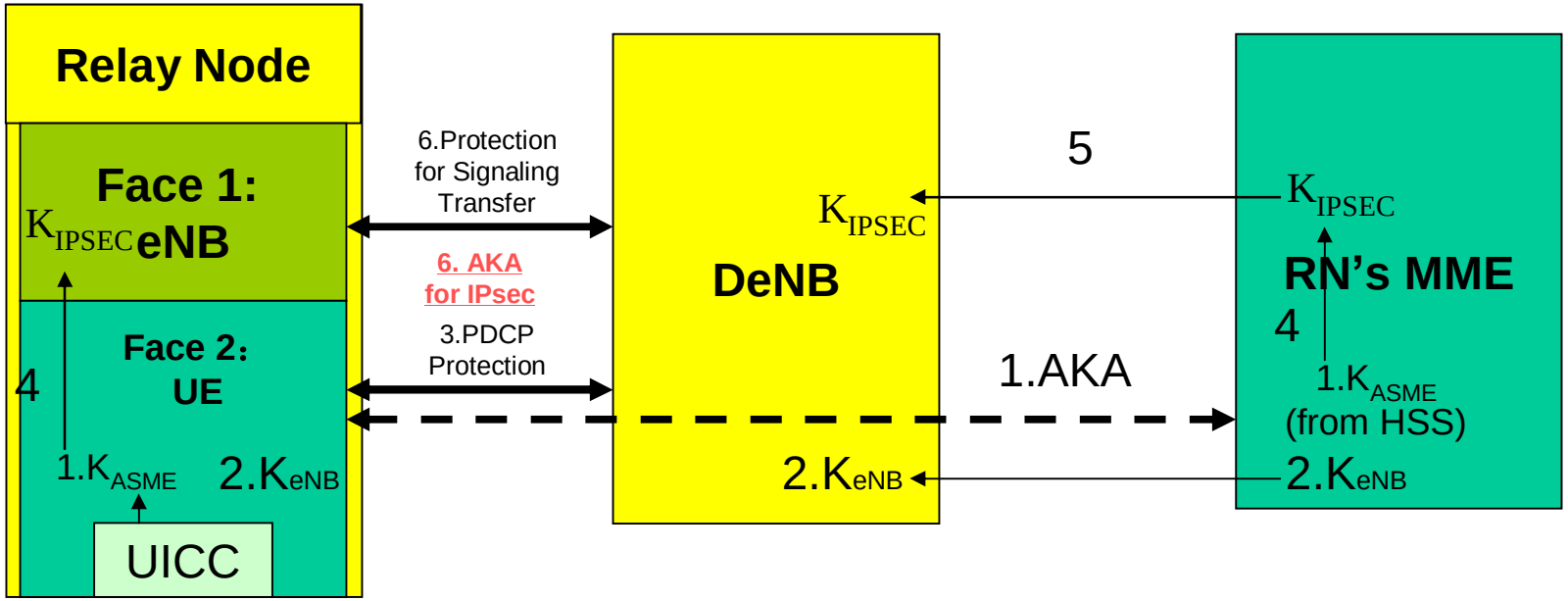
Note:
But considering IKE can make algorithm, key fresh time etc parameters negotiation easily, it is also worthy to use it.

Conclusion: IKE can be necessary or not when AKA is run as they provide duplicated functions.

2/Part 2---conclusion: problem with the current proposals

1. Current proposal analysis
   - They are focus on how to protect the signalling and user data.
   - It is not clear how the security protection is set up.
   - All proposed solution are talking about how the IPsec tunnel is made and how the IPsec is used. But no proposal describes what would be happened before IP connection is made.
2. IKE can be necessary or not when AKA is run as they provide duplicated functions.

1/Part 3. New Proposal for Relay Node authentication and protection (UICC is bound with Relay Node)



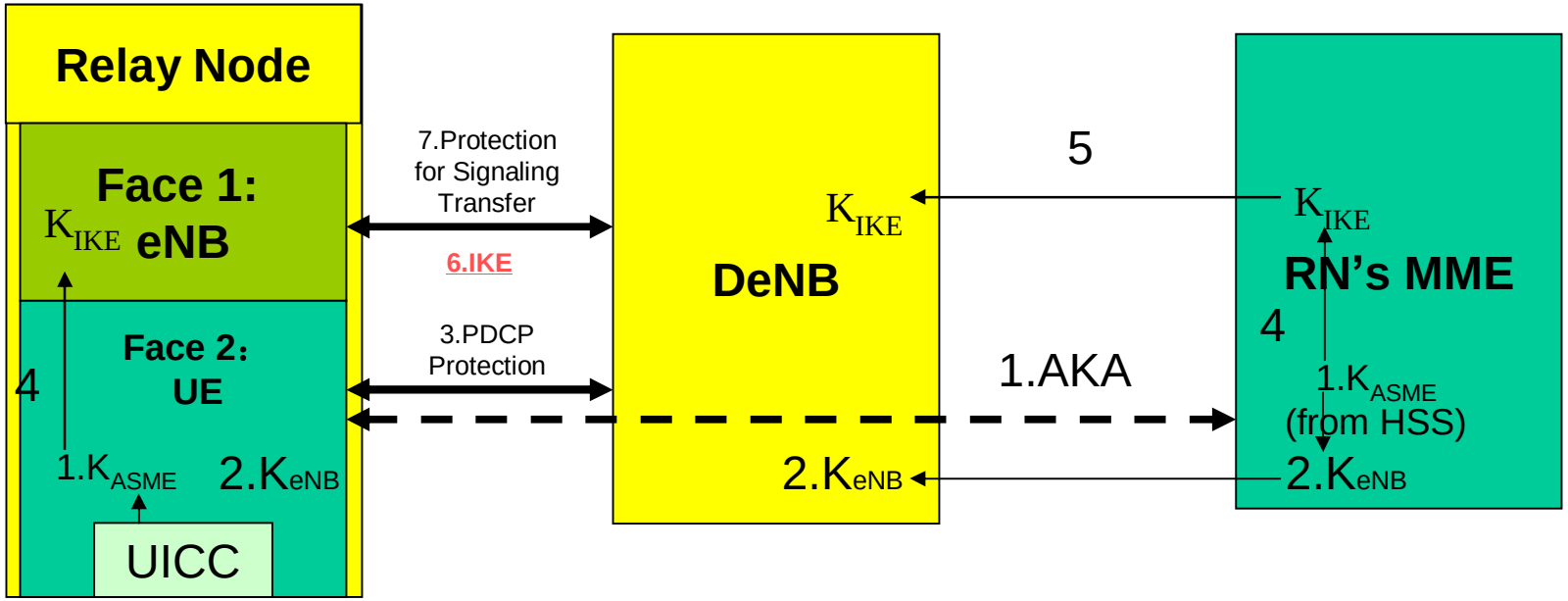
Procedure

1. When RE connects network as a legacy UE, AKA shall be performed, and K_{ASME} is generated by Relay Node and its HSS. MME will get K_{ASME} from HSS.
2. RN and MME generate the K_{eNB} independently, MME send the K_{eNB} to DeNB, then both RN and DeNB share K_{eNB} and related keys like K_{RRCenc}, K_{RRCint}, etc.
3. SMC negotiation is complete between RN and core network. And PDCP bearer will be generated and protected
4. A special K_{IPSEC} will be generated by K_{ASME} in RN and RN's MME simultaneously. Or generated by K_{eNB} in the DeNB.
5. This K_{IPSEC} will be transferred from RN's MME to DeNB if the key is generated in MME.
6. IPsec protection can be established between RN and DeNB by using K_{IPSEC}.

Advantage

1. There is no duplicated authentication between Relay Node and DeNB.
2. Certificate is not needed and provisioned in Relay Node and DeNB.
3. K_{IPSEC} is generated by K_{ASME} and independent with AS security keys. So it is independent between AS protection and IP protection.

2/Part 3---New Proposal for Relay Node authentication and protection (UICC is bound with Relay Node)



Procedure

1. When RE connects network as a legacy UE, AKA shall be performed, and K_{ASME} is generated by Relay Node and its HSS. MME will get K_{ASME} from HSS.
2. RN and MME generate the K_{eNB} independently, MME send the K_{eNB} to DeNB, then both RN and DeNB share K_{eNB} and related keys like K_{RRCenc}, K_{RRCint}, etc.
3. SMC negotiation is complete between RN and core network. And PDCP bearer will be generated and protected
4. A special K_{IKE} will be generated by K_{ASME} in RN and RN's MME simultaneously. Or generated by K_{eNB} in the DeNB.
5. This K_{IKE} will be transferred from RN's MME to DeNB if the key is generated in MME.
6. The key K_{IKE} can be used for IKE authentication pre-share key instead of certificate.
7. IP protection is esetablished and used after IKE negotiation.

Advantage

1. Certificate is not needed and provisioned in Relay Node and DeNB.
2. There is a bind relationship between AKA and IKE.
3. K_{IKE} is generated by K_{ASME} and independent with AS security keys. So it is independent between AS protection and IP protection.

Thank you!