ETSI Security Conference 2022

Side Link and Relay Security in 5G

Marcus Wong

OPPO

03/10/2022

Agenda

- Introduction
- Sidelink Security
- Relay Security
- Q & A

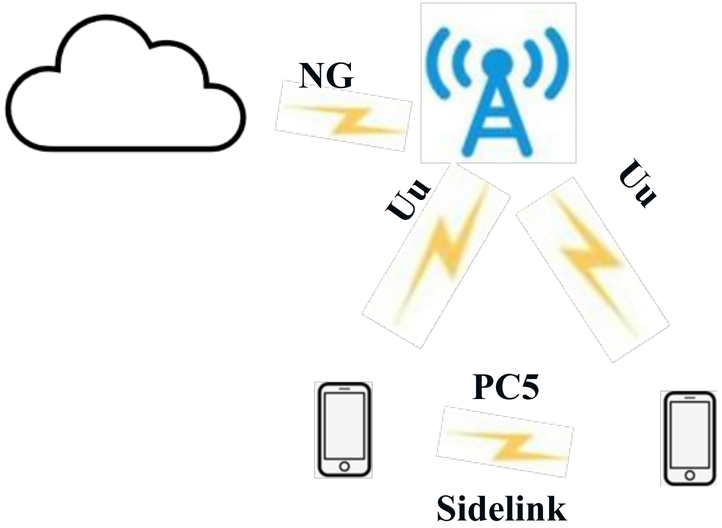
Introduction: Sidelink

- An interface between two devices (e.g., handsets or UEs) that allows the two devices to communicate directly without the help of either the network or a base station.

- 3GPP defines Sidelink as the PC5 interface, which uses licensed spectrum for the devices to communicate.

Use cases for Sidelink

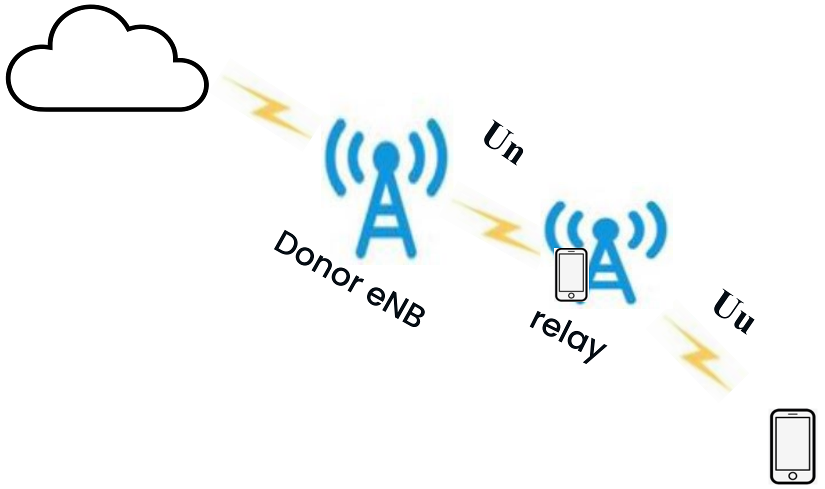
- Proximity service
- V2X services
- Location services
- Sensing
- Etc.



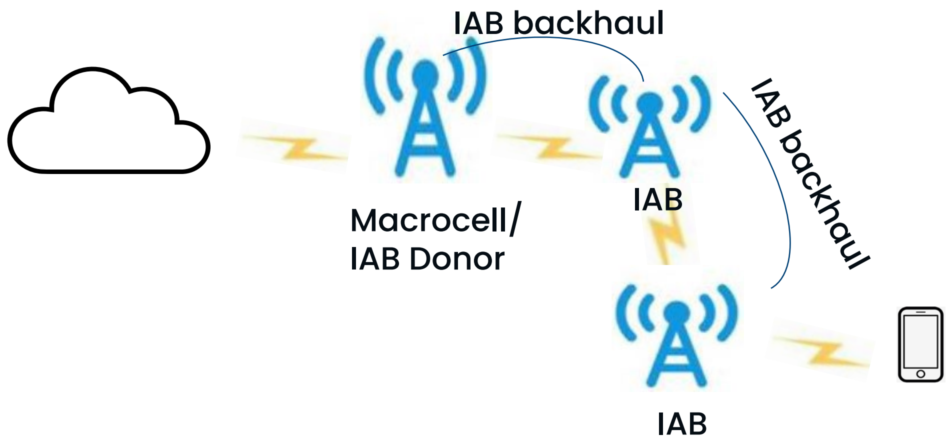
Sidelink Network Architecture

Introduction: (e)(g)NB-based relay nodes

- **Relay node in LTE**
  - **Relay node (eNB on UE-facing side and UE on eNB-facing side) connects wirelessly to a eNB (called Donor eNB) for extending the network coverage**

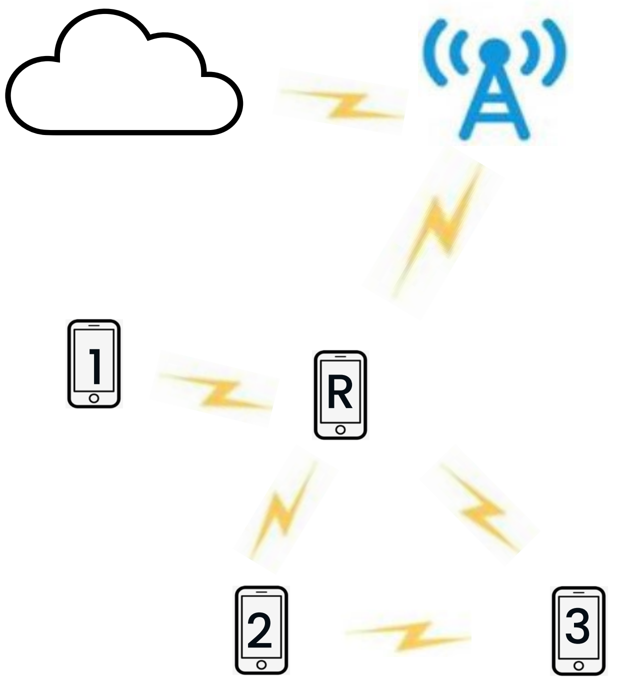


- **Relay in wireless backhaul**
  - **Integrated Access Backhaul (IAB) extends backhaul over multiple hop(s) of wireless access**

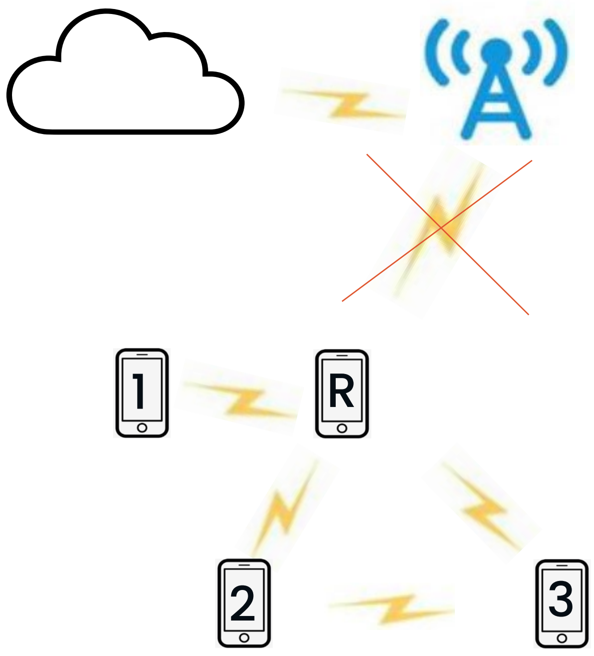


Introduction: UE-based relay nodes

- A relay node (i.e., relay UE that relays gNB signaling in either L2 or L3) extends the network and network services to UEs that are no longer able to access the network directly or indirectly.
- Relay nodes include UE-to-Network relay and UE-to-UE relay



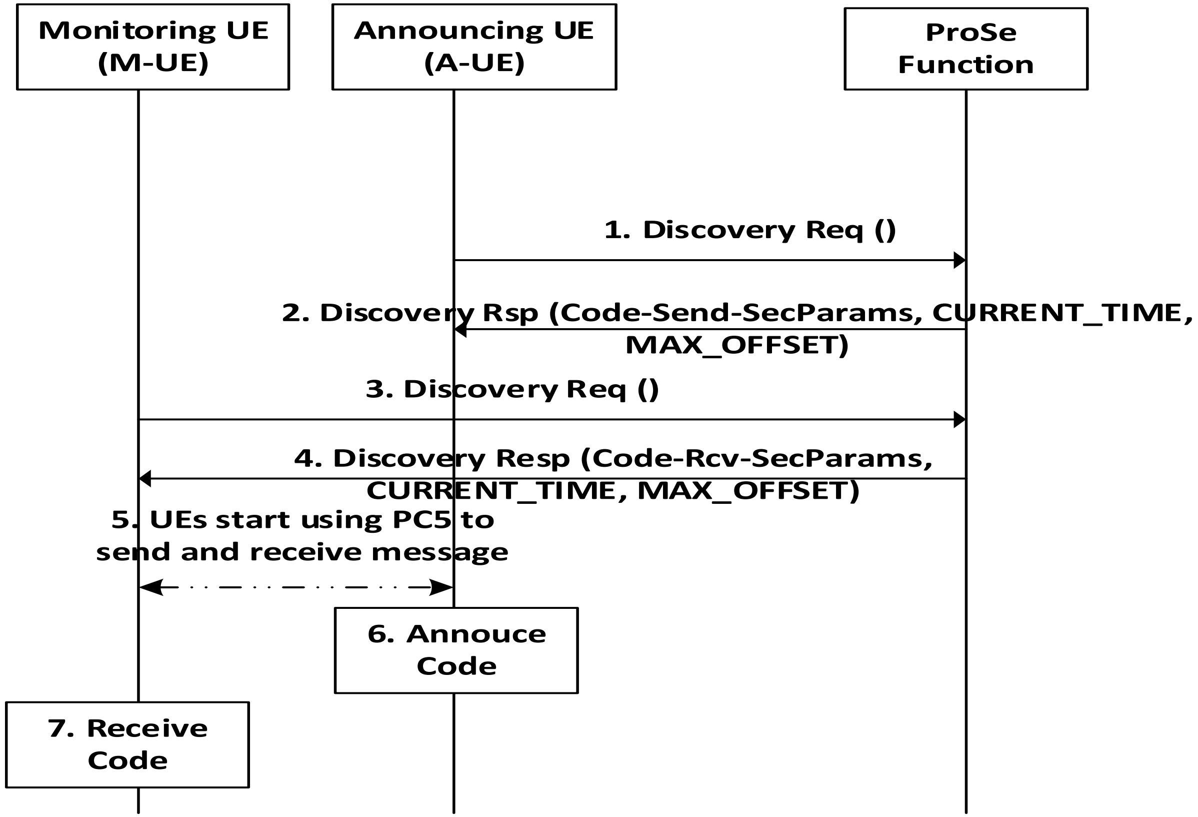
UE-to-Network Relay



UE-to-UE Relay

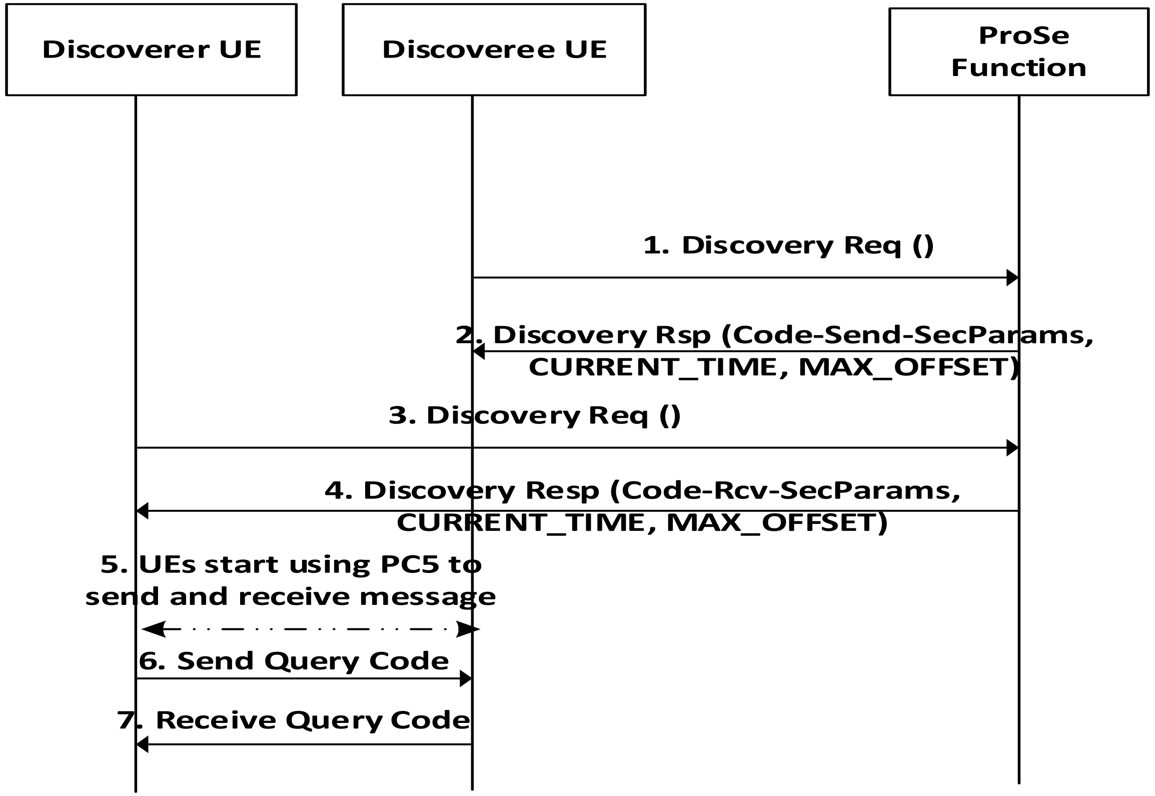
Sidelink Security: model A discovery

Announcing UE: I'm providing a service

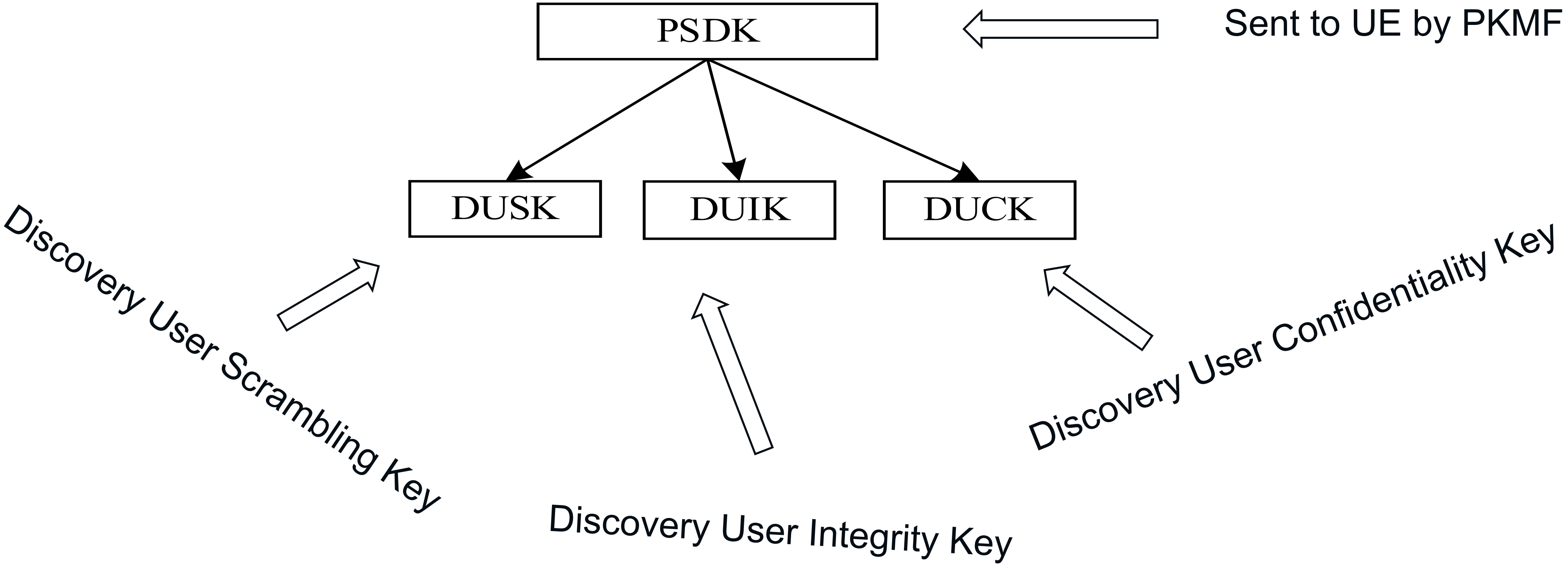

Monitoring UE (M-UE)
Announcing UE (A-UE)
ProSe Function
1. Discovery Req ()
2. Discovery Rsp (Code-Send-SecParams, CURRENT_TIME, MAX_OFFSET)
3. Discovery Req ()
4. Discovery Resp (Code-Rcv-SecParams, CURRENT_TIME, MAX_OFFSET)
5. UEs start using PC5 to send and receive message
6. Annouce Code
7. Receive Code

Sidelink Security: model B discovery

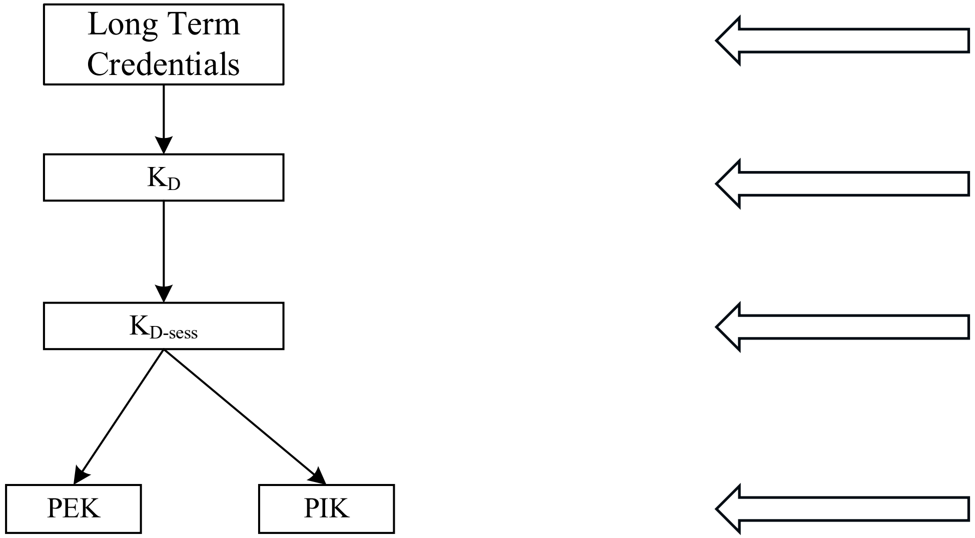
Discoveree UE: I'm looking for a service


Discoverer UE
Discoveree UE
ProSe Function
1. Discovery Req ()
2. Discovery Rsp (Code-Send-SecParams, CURRENT_TIME, MAX_OFFSET)
3. Discovery Req ()
4. Discovery Resp (Code-Rcv-SecParams, CURRENT_TIME, MAX_OFFSET)
5. UEs start using PC5 to send and receive message
6. Send Query Code
7. Receive Query Code

Sidelink Security: Discovery Message Protection


PSDK
Sent to UE by PKMF
DUSK
DUIK
DUCK
Discovery User Scrambling Key
Discovery User Integrity Key
Discovery User Confidentiality Key

Sidelink Security: Keys for one-to-one Security



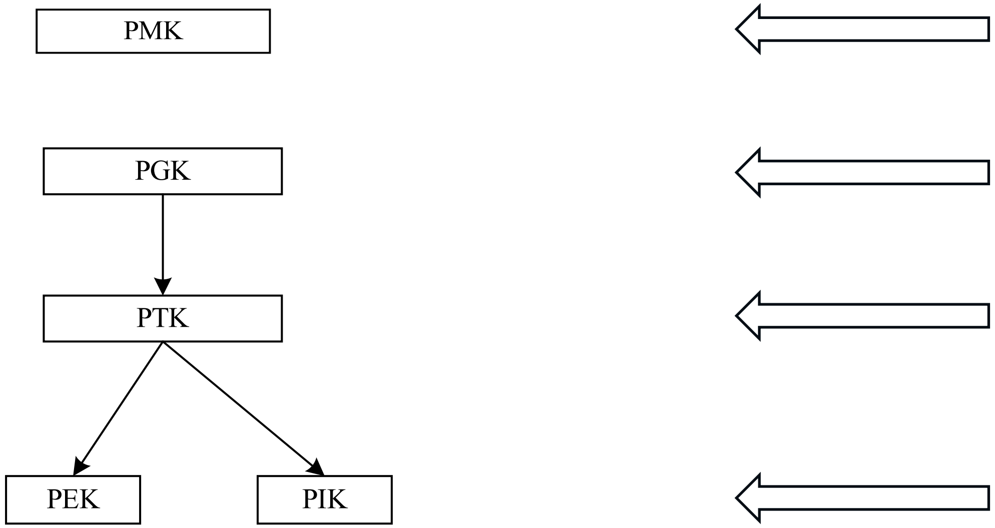
Provisioned into UE (symmetric or asymmetric)

Generated shared secret between 2 UEs

Generated session key

Actual traffic protection keys

Sidelink Security: Keys for One-to-Many Security



Generated between UE and PKMF

UE gets PGK from PMKF for the group

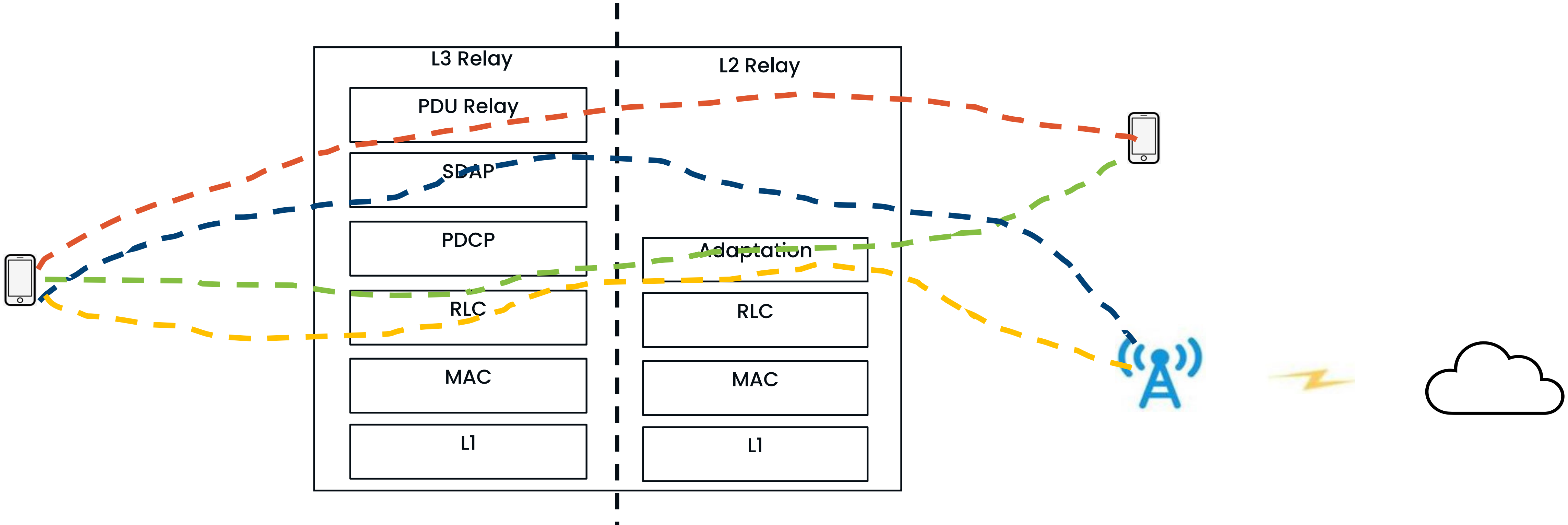
Generated session key

Actual traffic protection keys

Sidelink Security: re-cap

- Provisioning
    - Security keys and security related parameters (e.g, Discovery Code, ProSe Restricted Code, Discovery Keys, timing information, etc.)
- discovery
    - Open and restricted discovery: Model A and Model B
    - Discovery message protection
        - Integrity protection in open discovery
        - Scrambling protection
        - Confidentiality
- one-to-one communication
    - 4-layer of keys
    - One-to-one communication protected over PDCP layer
- one-to-many communication
    - Group key distribution protected by MIKEY
    - Group message protection using PDCP layer protection or application layer protocol
- Privacy protection
    - Randomization and synchronization of source Layer-2 identifier and upper layer identifier

Relay Security: L2 and L3 relays



L3/L2 Relay Protocol Stack

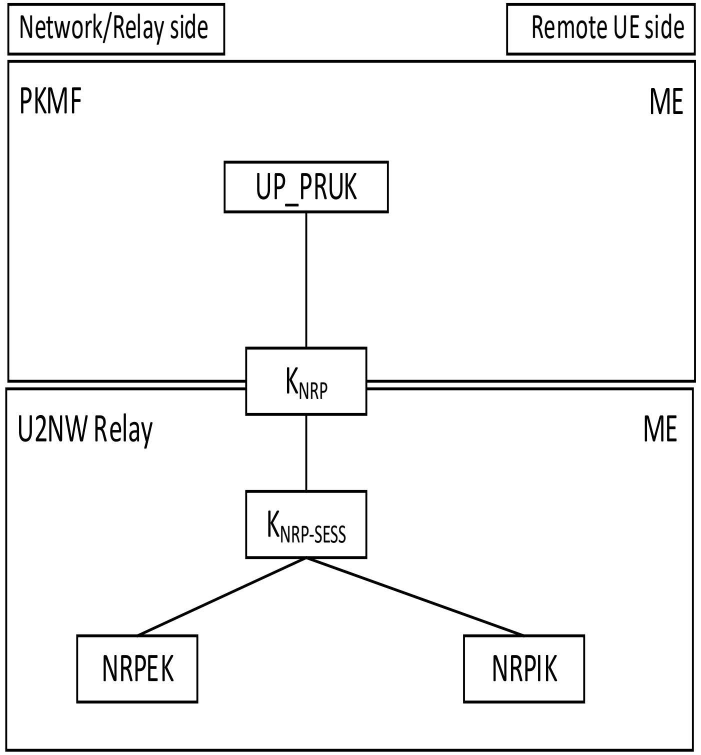
UE-UE via L3 U2U relay

UE-UE via L2 U2U relay

UE-UE via L3 U2N relay

UE-UE via L2 U2N relay

Relay Security: U2N Relay UP key Hierarchy



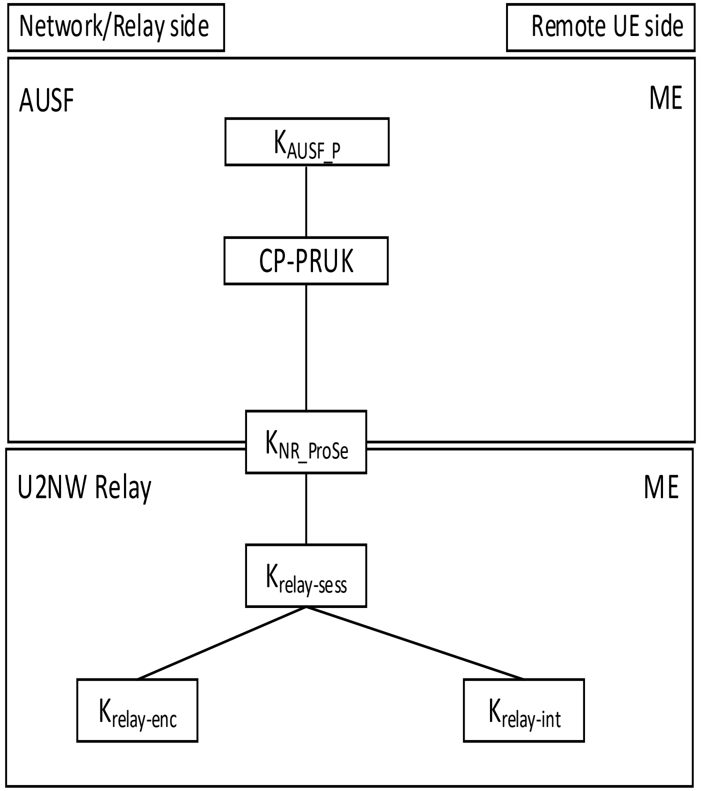
Provisioned into UE as a “long” lived key

Generated shared secret between relay and UE

Generated session key

Actual traffic protection keys

Relay Security: U2N Relay CP key Hierarchy



Based on mutual authentication of UE

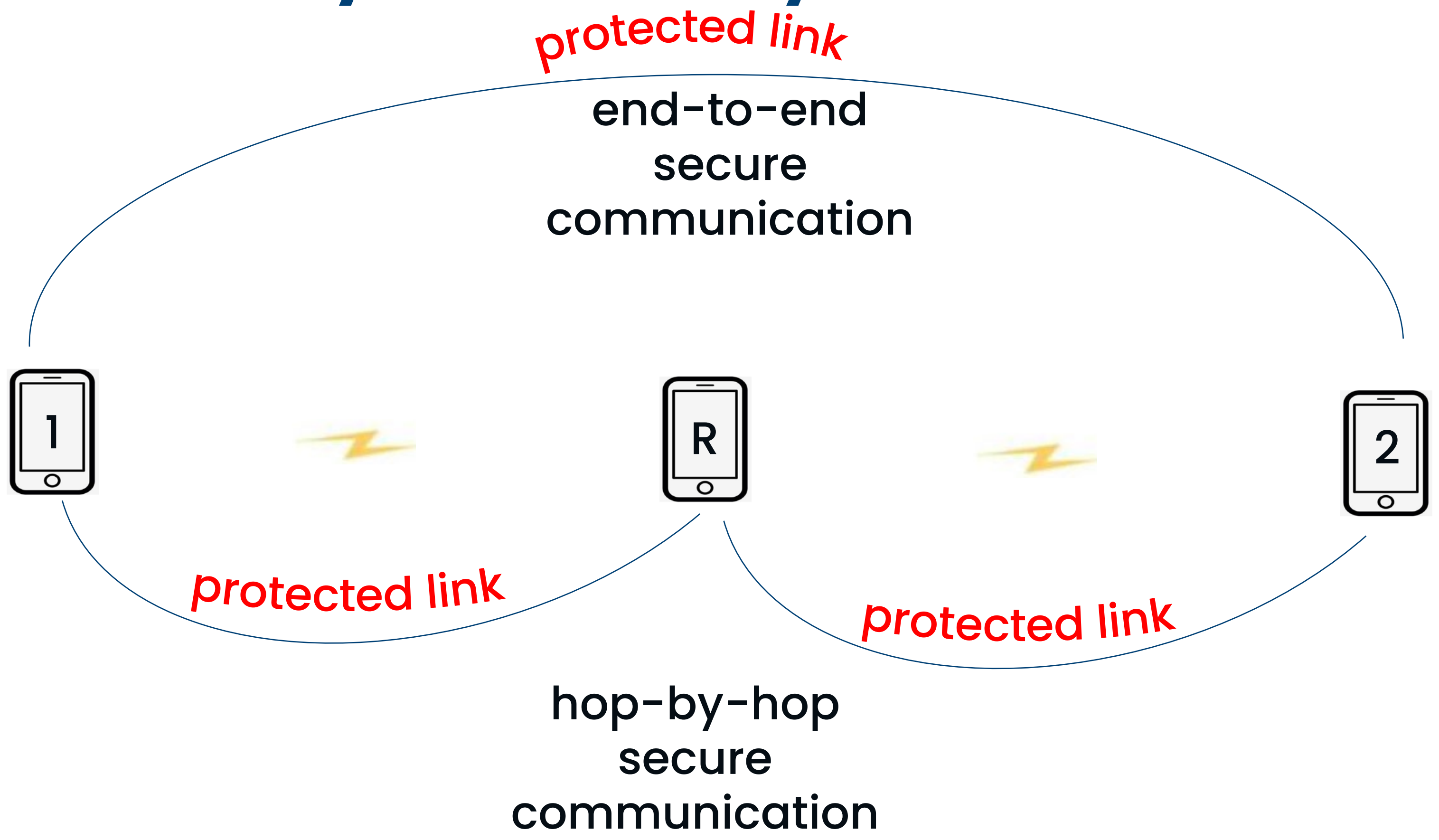
Generated based on K_{ausf_p}

Generated shared key

Generated session key

Actual traffic protection keys

Relay Security: U2U Relay Traffic Protection



protected link

end-to-end secure communication

protected link

protected link

hop-by-hop secure communication

protected link: link can be encrypted, integrity-protected, and replay-protected.
Keys in U2U: similar key hierarchy as in one-to-one sidelink communication

Relay Security: recap

- L2 relay
  - Adaptation capability
  - AS security over relay between UE and gNB (or another UE)
- L3 relay
  - User Plane
    - Use of UP connection and UP security to connect to PKMF for relay security establishment
  - Control Plane
    - Use of CP connection and CP security to connect to ProSe Function for relay security establishment
- Reuse sidelink security features
  - Relay discovery
  - UE discovery
- UE-to-UE communication via U2U relay
  - Hop-by-hop
  - End-to-end
- Privacy protection
  - Similar to that of sidelink protection (i.e., Randomization and synchronization of source Layer-2 identifier and upper layer identifier)

QUESTIONS?

marcus.wong@oppo.com