LTE Radio Security Diagrams

C2146

P1 Security Training

Prerequisites

- Mandatory
  - P1security-Training-C2130-NAS Security
  - P1Security-Training-C2145 Radio Security
- Optional
  - P1security-Training-C2140-LTE-Radio
  - P1security-Training-C2000-LTE-Security-Introduction

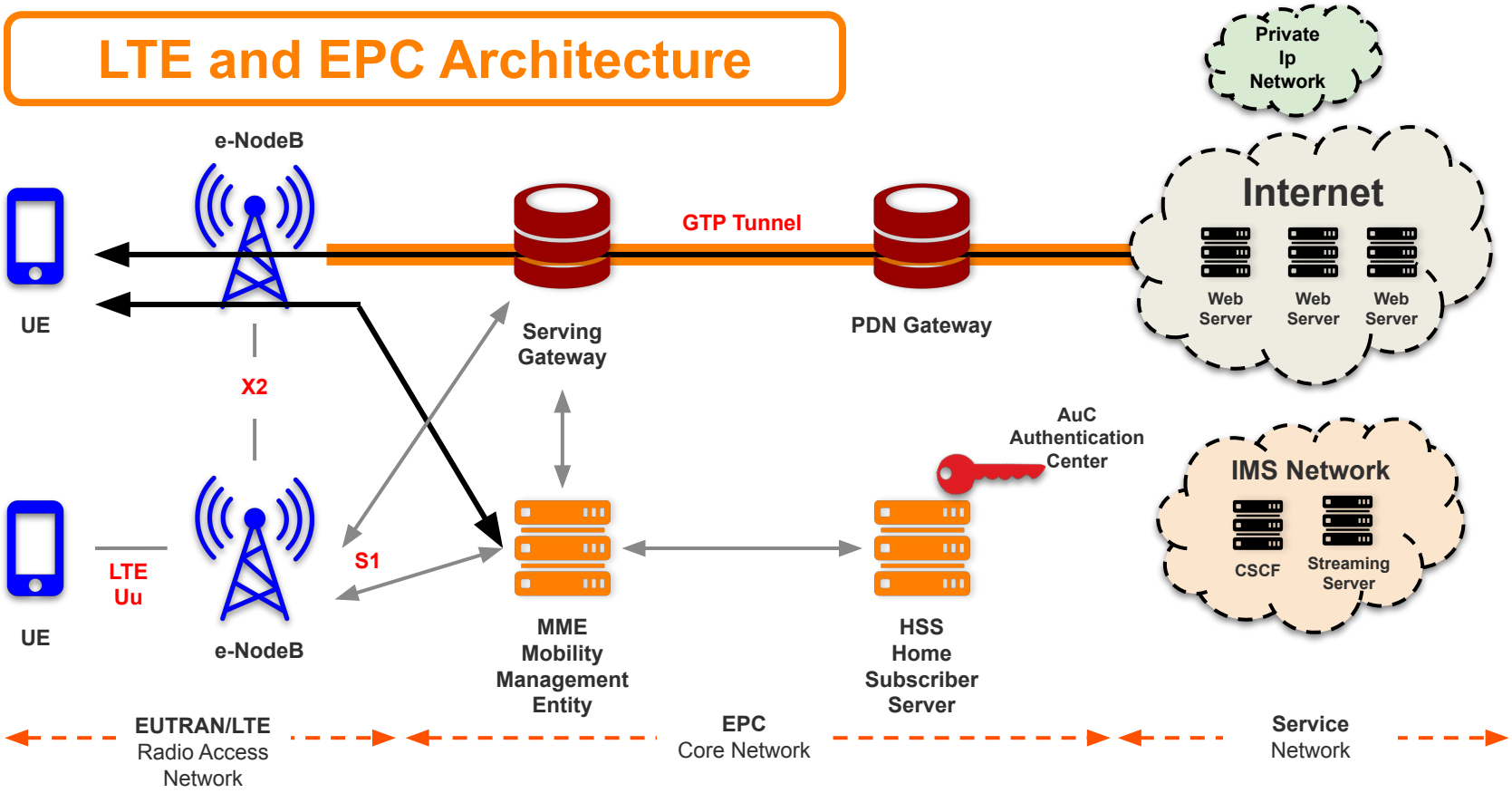
Agenda

- LTE network architecture diagram
- LTE network security architecture diagram
- LTE connection and security establishment diagram sequence
- Fake eNodeB exploiting EIA0 at the RRC layer diagram sequence

LTE Network Diagram

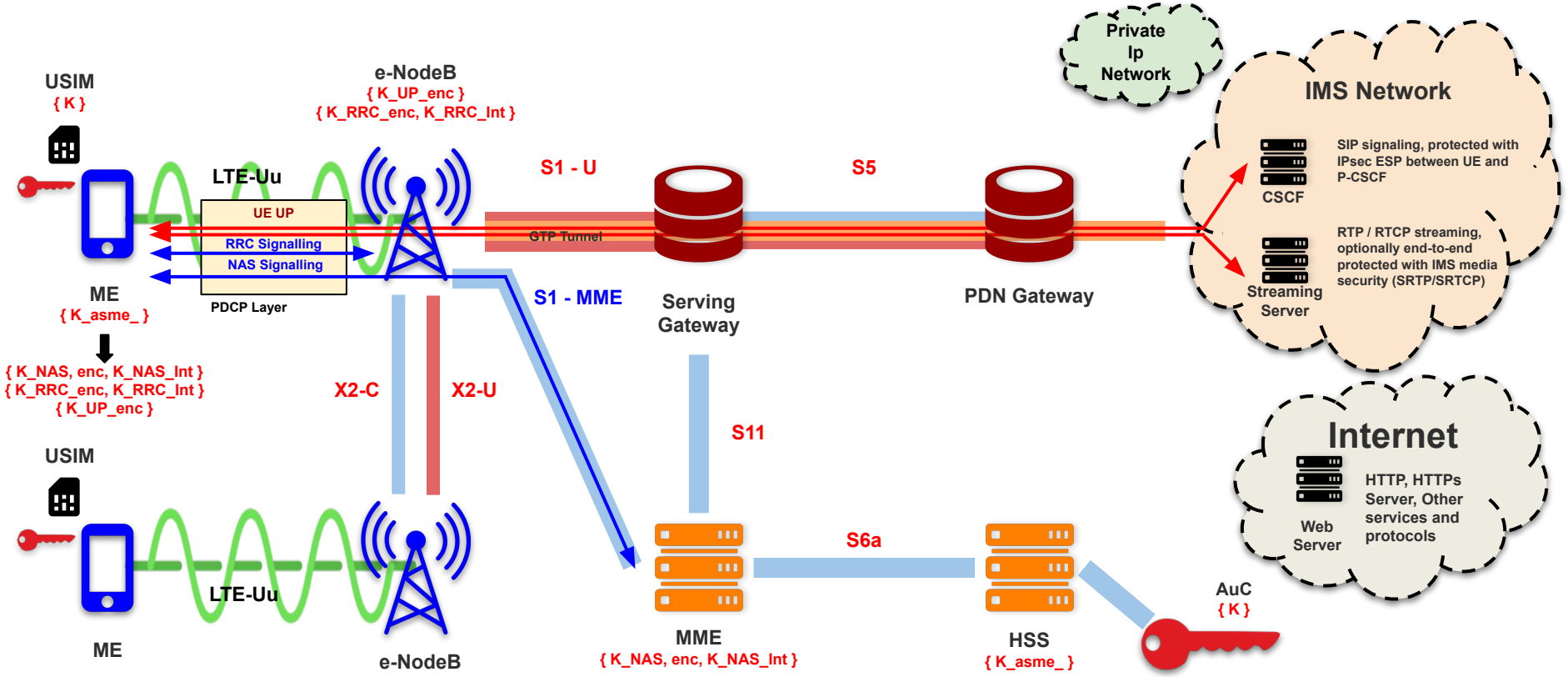
LTE Network Diagram

LTE and EPC Architecture



LTE Security Diagram

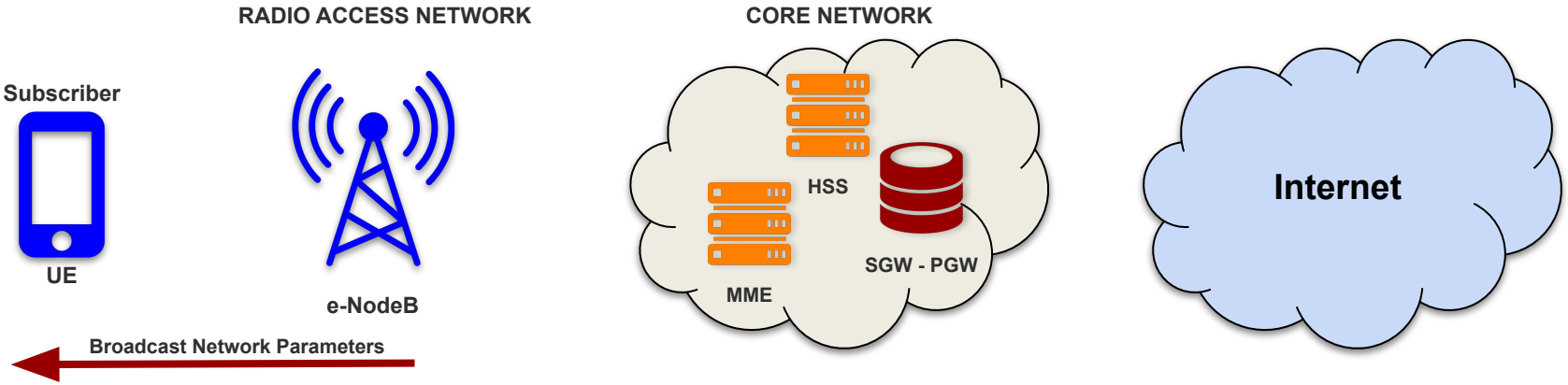
LTE Network Security Architecture



LTE Connection and Security

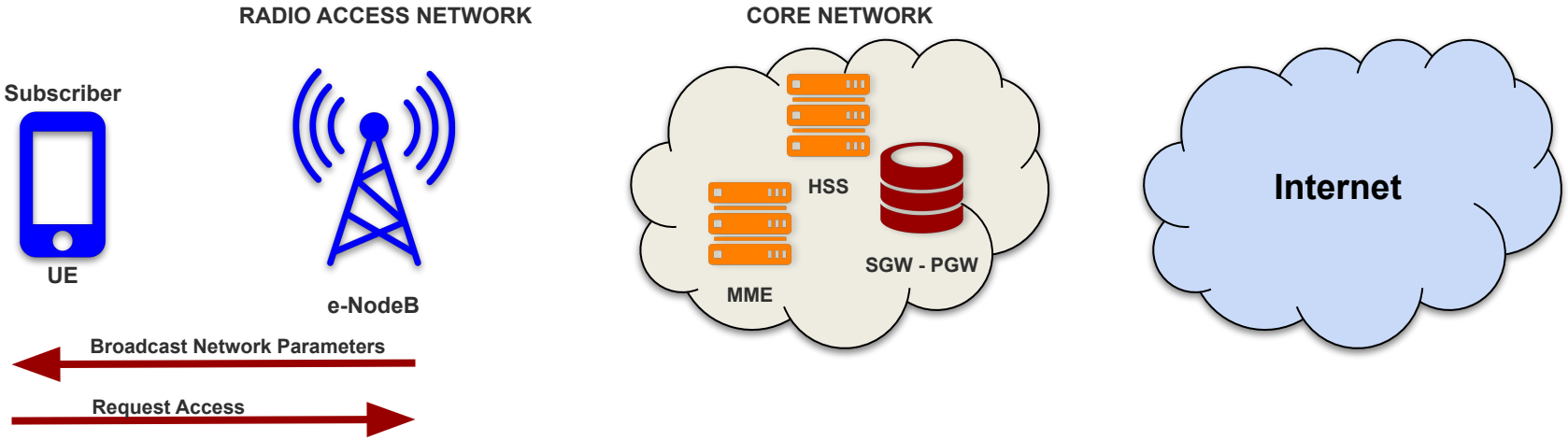
LTE Network Security Architecture

LTE connection: Broadcasting Network Information



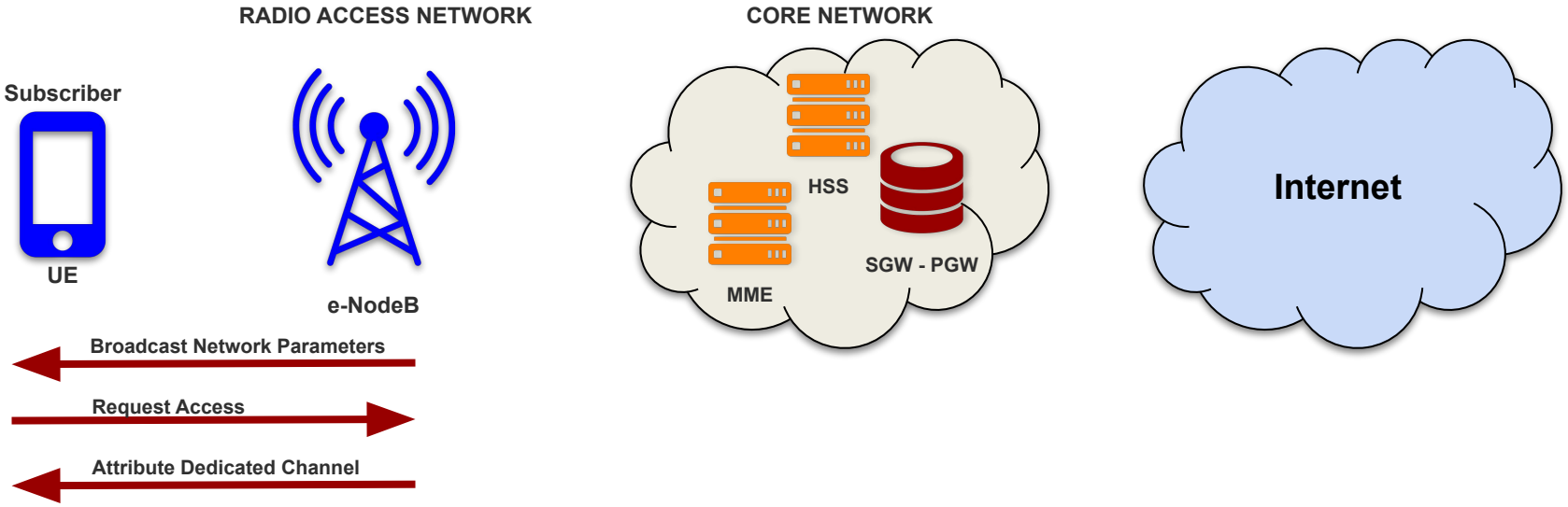
LTE Network Security Architecture

LTE connection: Access Network Request



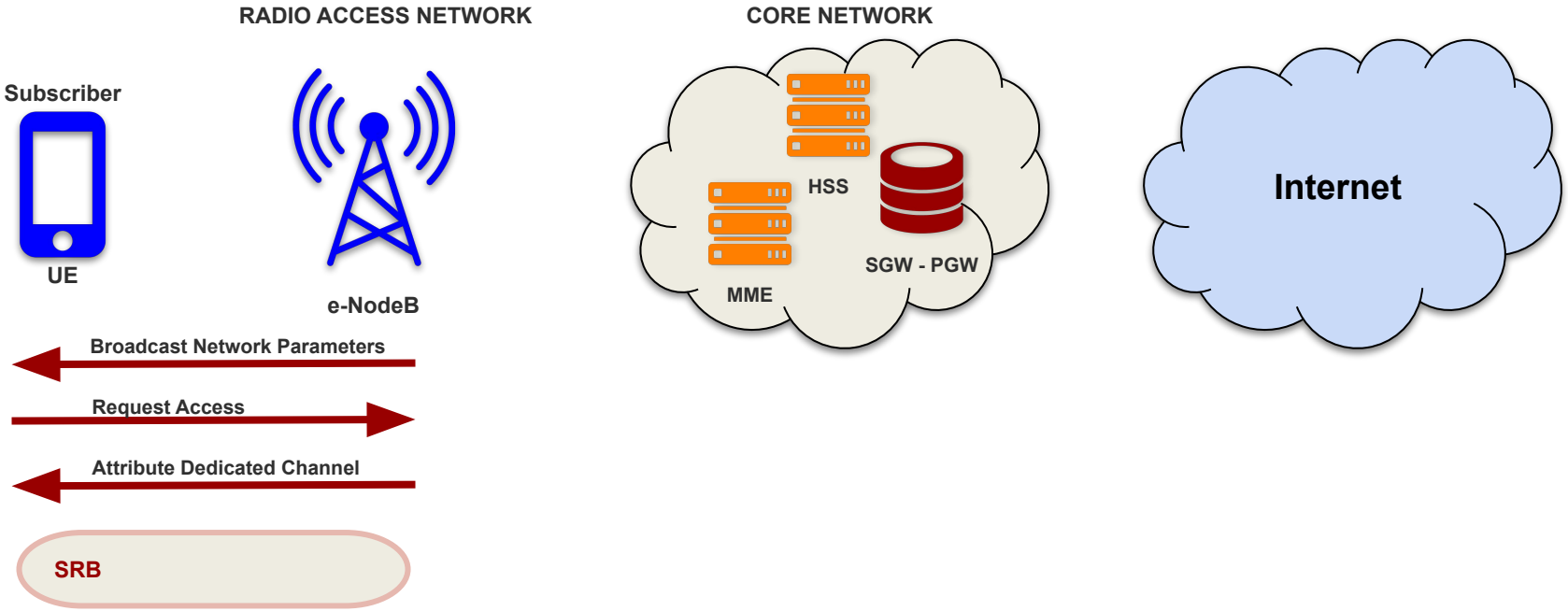
LTE Network Security Architecture

LTE connection: Dedicated Channel Assignment



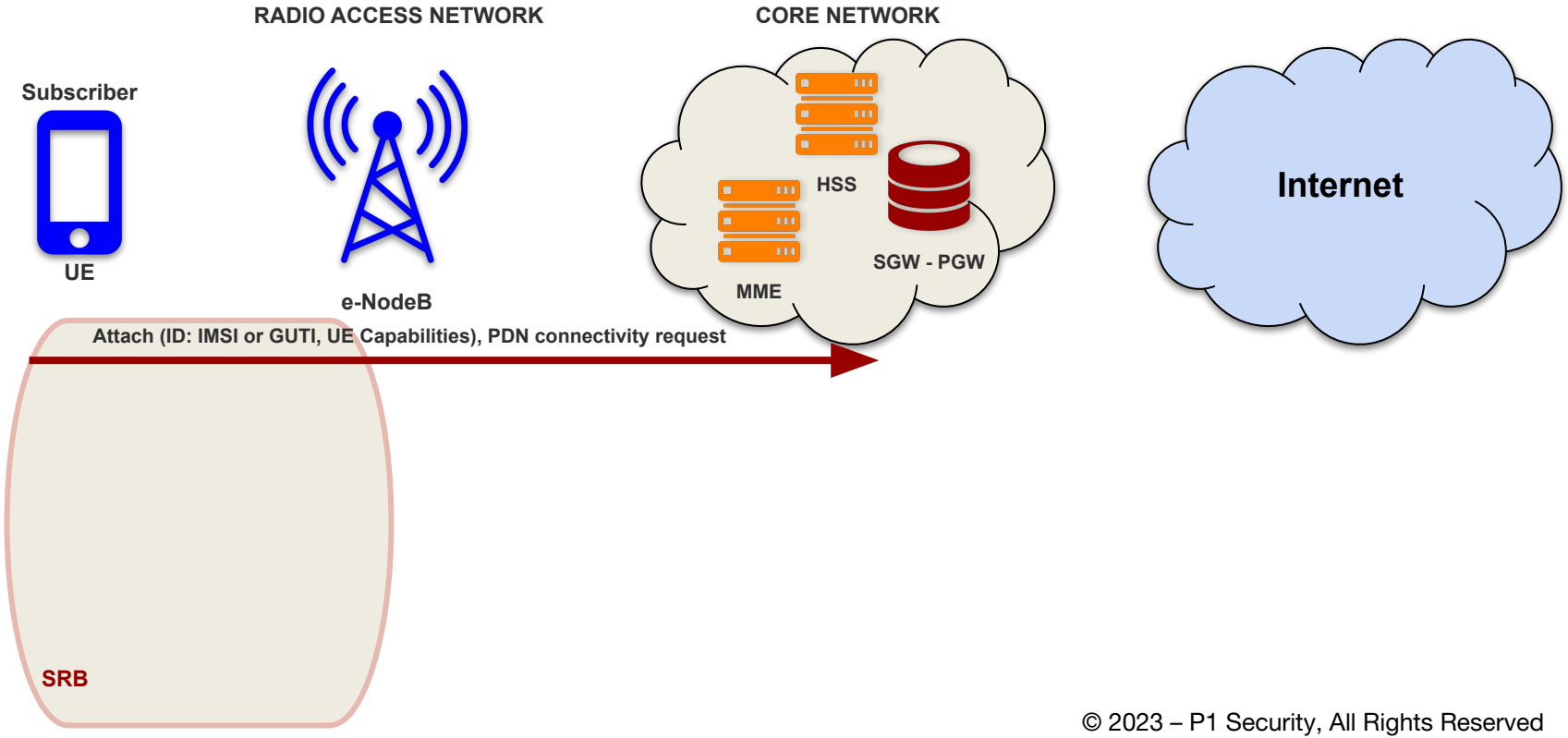
LTE Network Security Architecture

LTE connection: Dedicated Duplex Channel Established



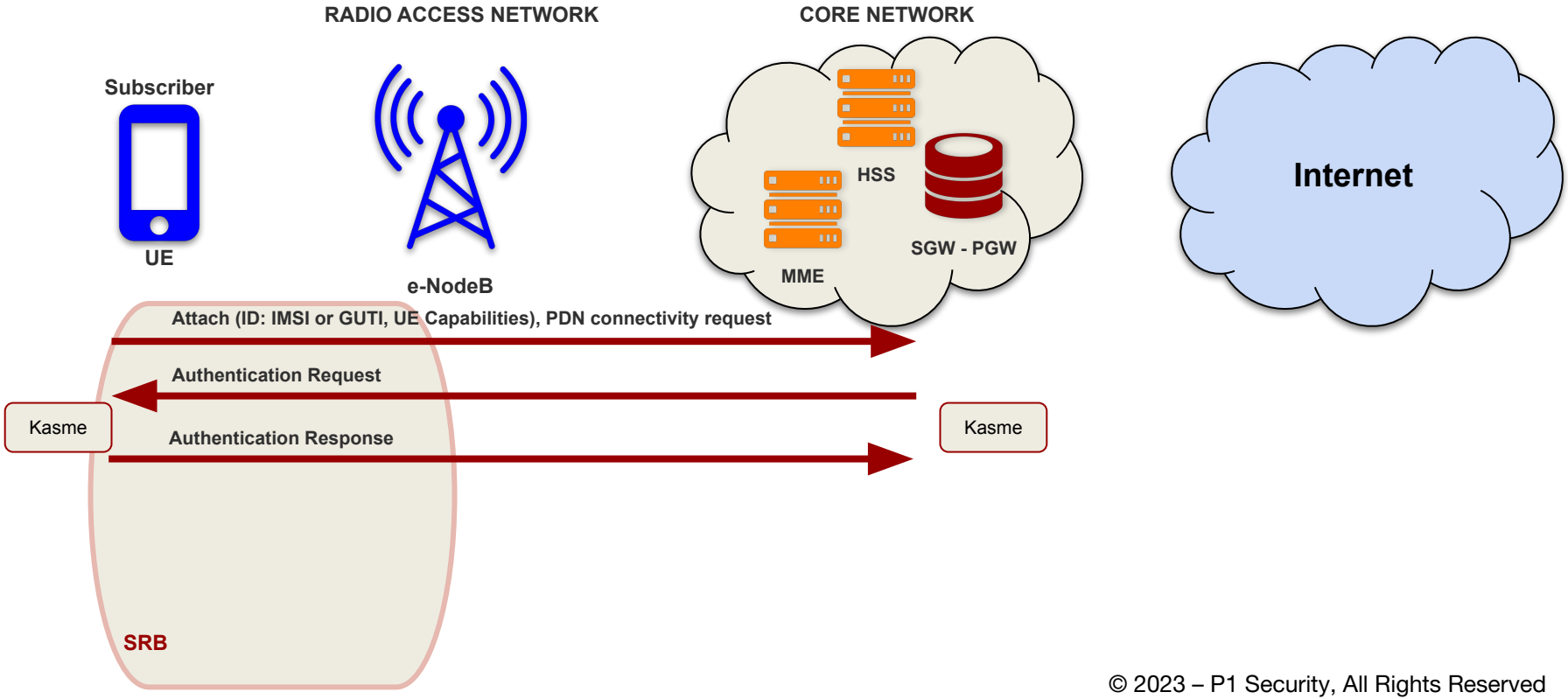
LTE Network Security Architecture

LTE connection: Attached and IP Connectivity Request



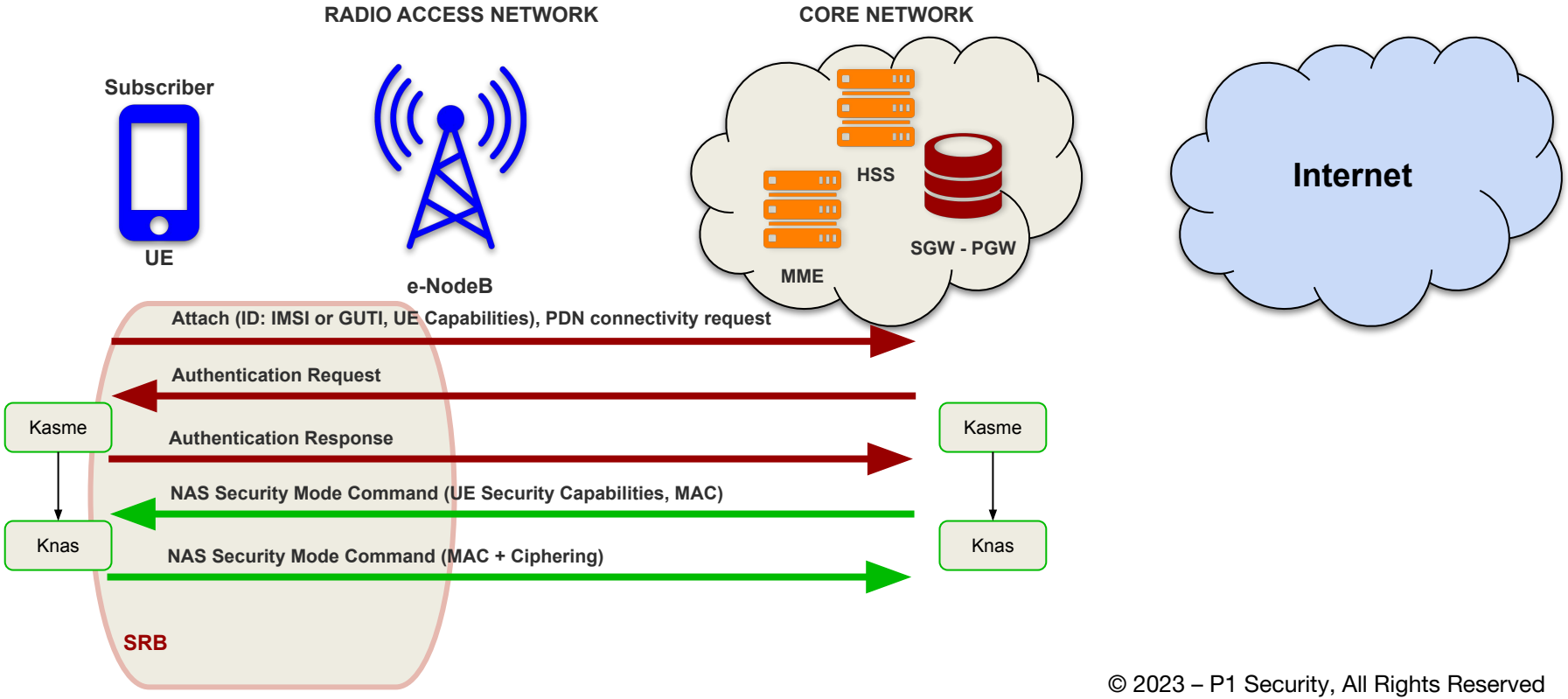
LTE Network Security Architecture

LTE connection: Mutual authentication and Master Key establishment



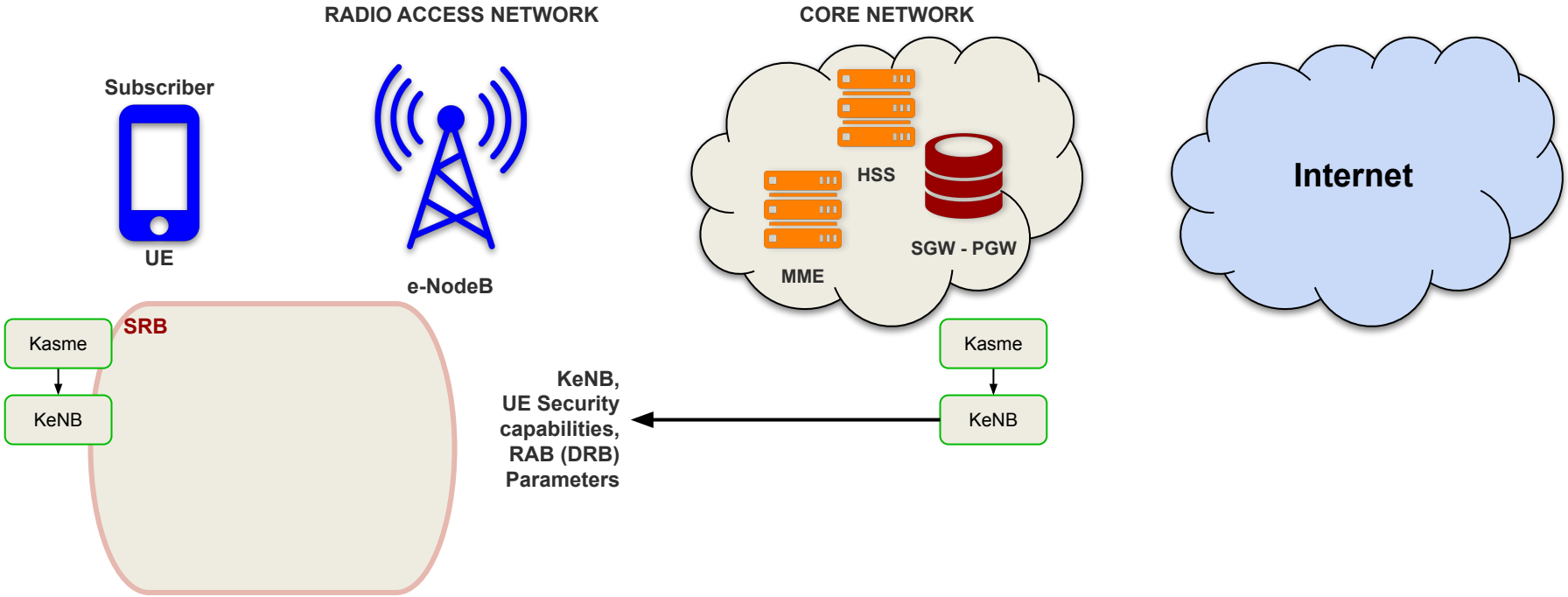
LTE Network Security Architecture

LTE connection: NAS Security Activation



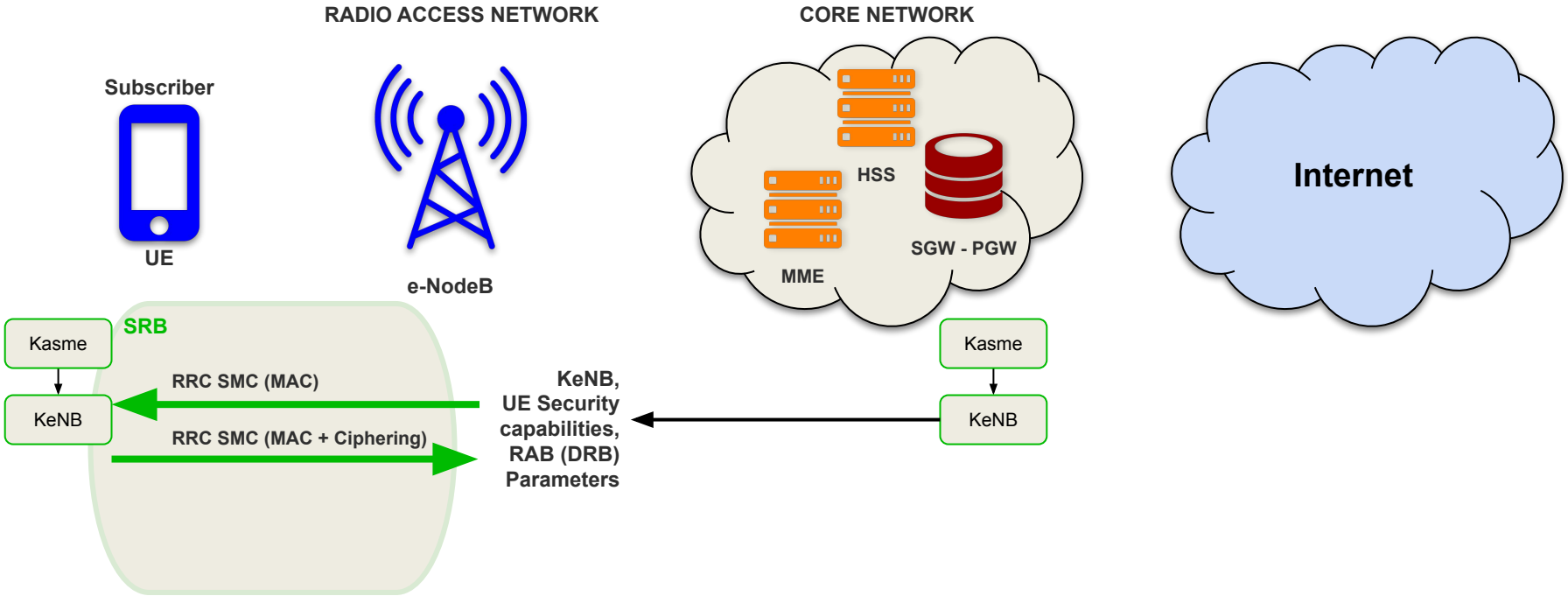
LTE Network Security Architecture

LTE connection: Transfer of Session and Security Parameters to eNodeB



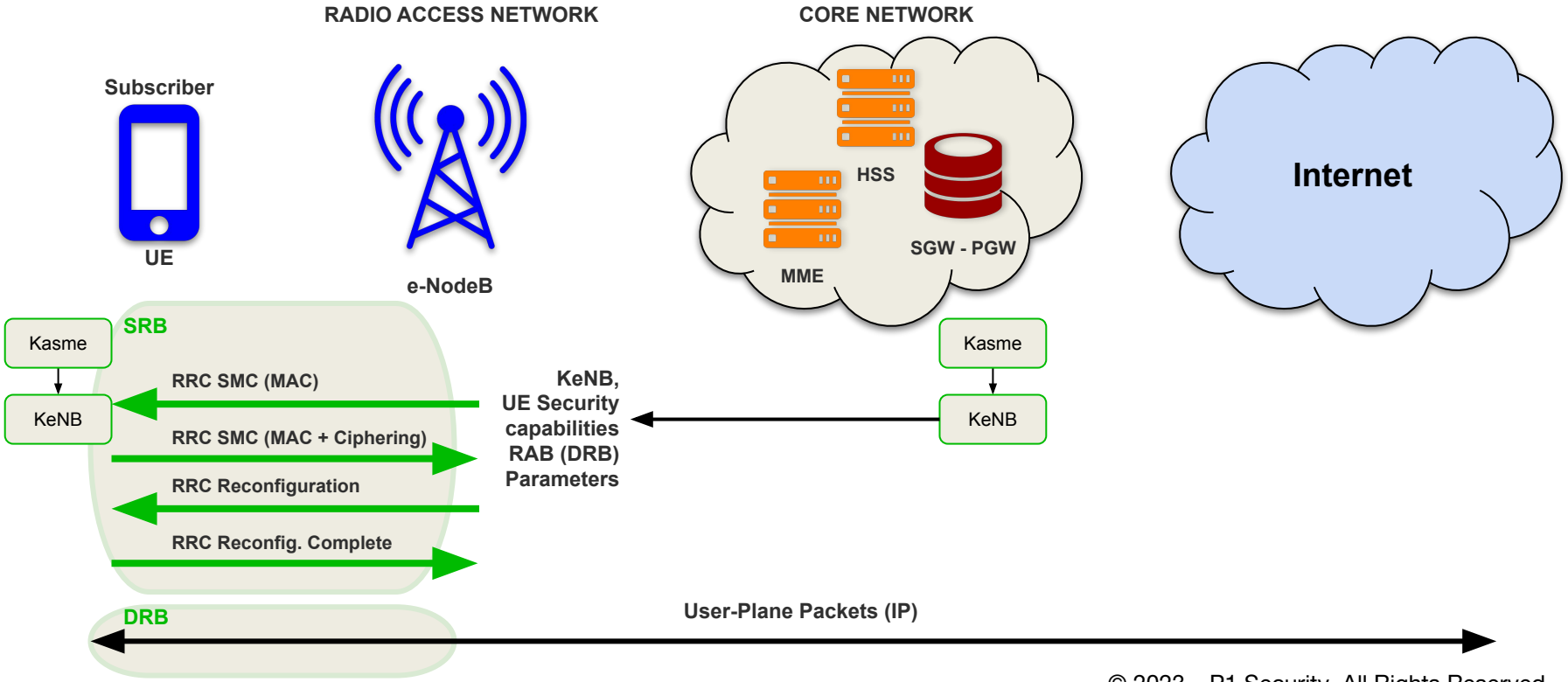
LTE Network Security Architecture

LTE connection: Radio Channel Security Activation



LTE Network Security Architecture

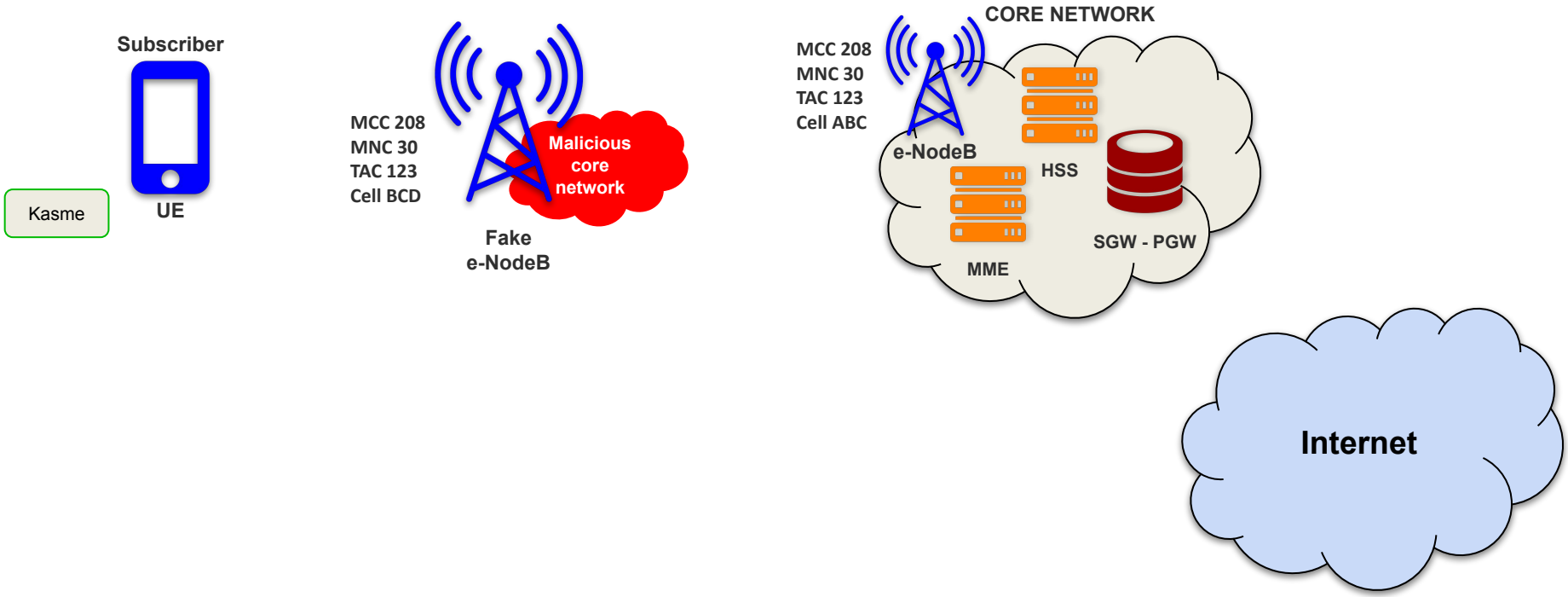
LTE connection: User-Plane Data Channel Establishment



Fake EnodeB Exploitation

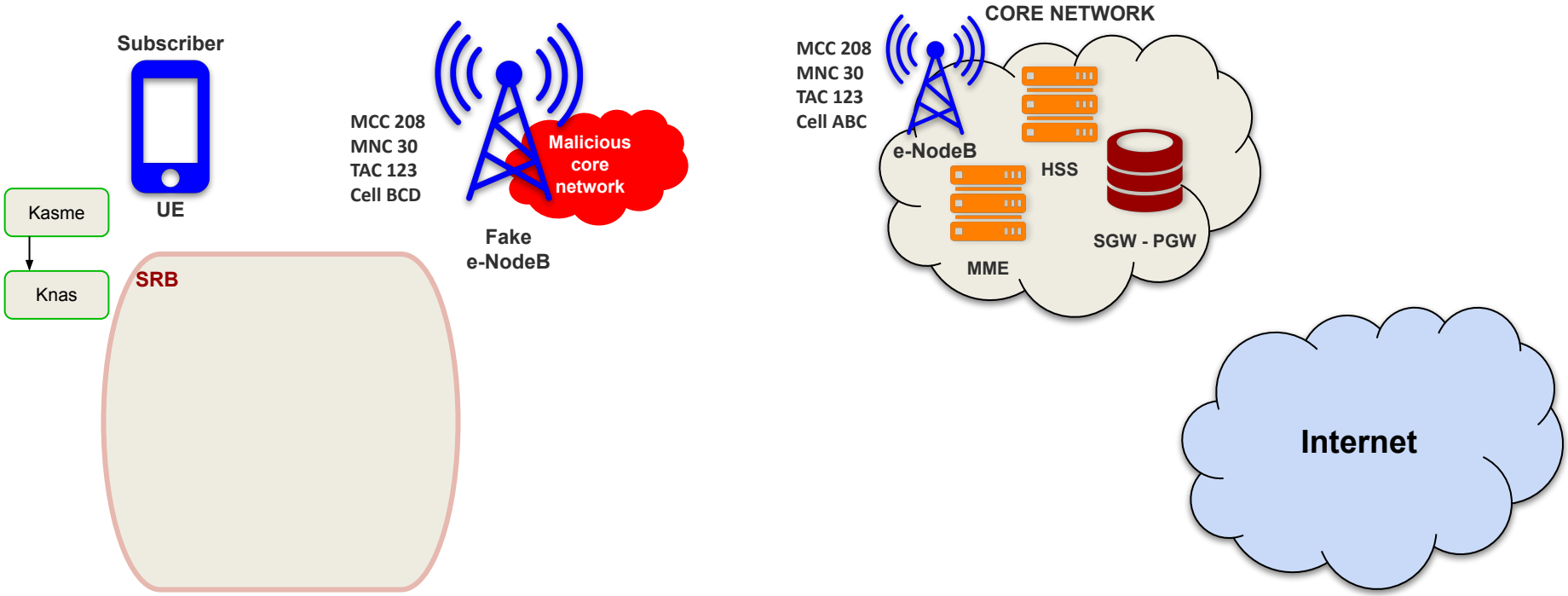
Fake eNodeB exploiting EIA0 at the RRC layer

LTE Interception: Spoofing Legitimate Network Codes (PLMN & TAC)



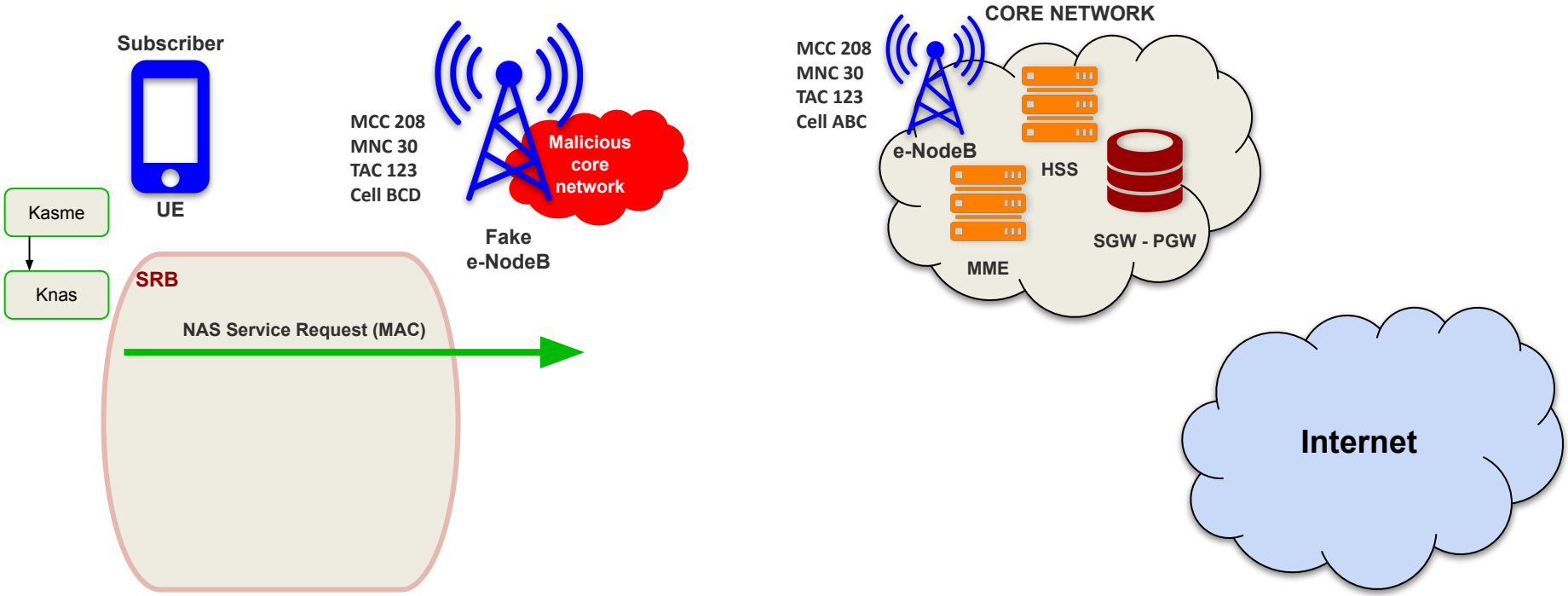
Fake eNodeB exploiting EIA0 at the RRC layer

LTE Interception: Radio Channel Establishment by Targeted Subscriber



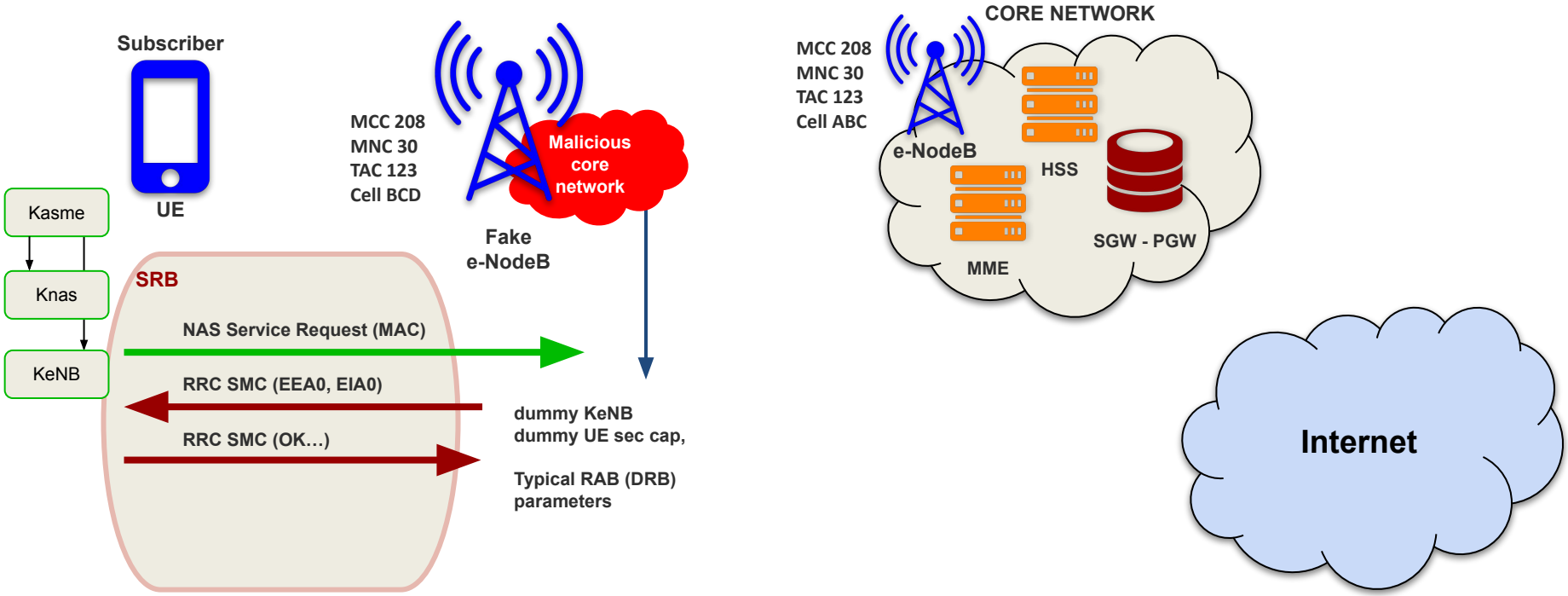
Fake eNodeB exploiting EIA0 at the RRC layer

LTE Interception: Request for Re-establishing the data connection through NAS



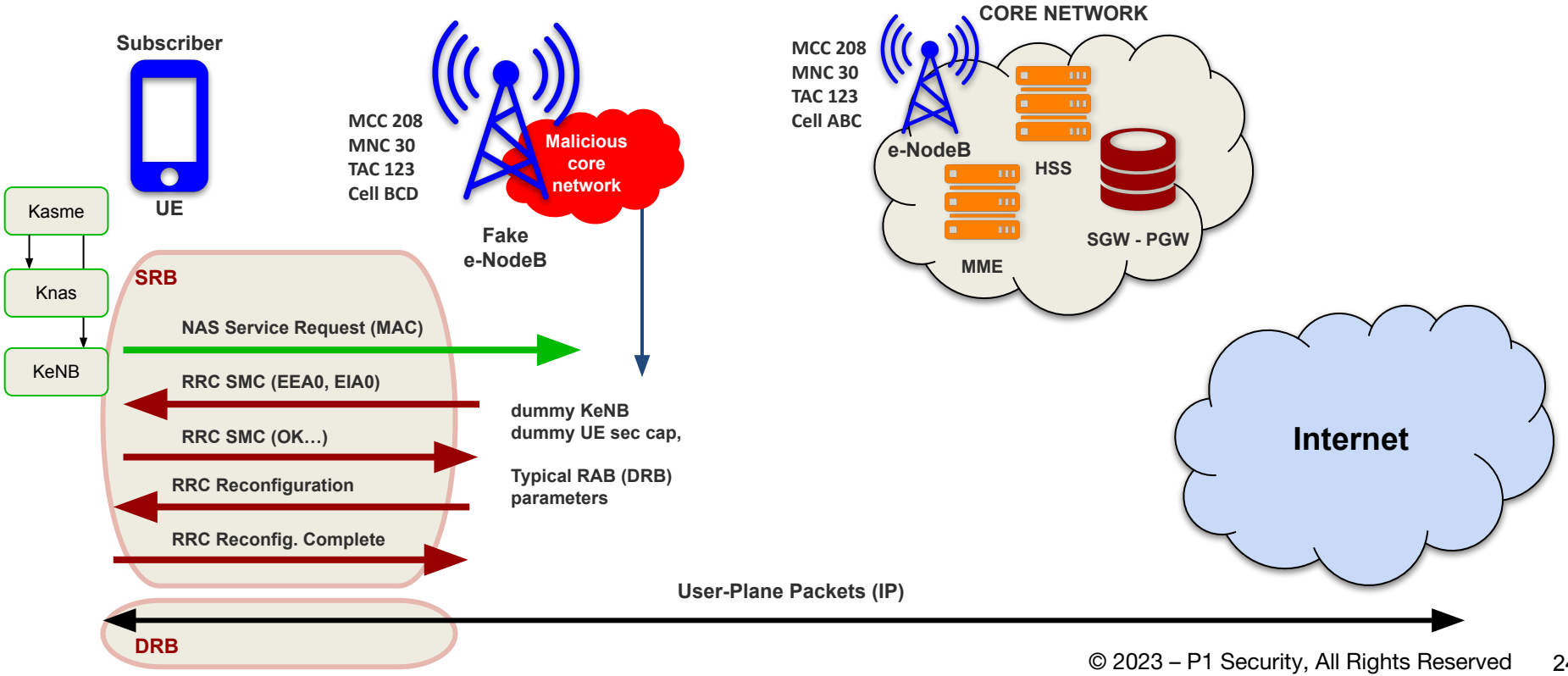
Fake eNodeB exploiting EIA0 at the RRC layer

LTE Interception: Creation of a Typical Session Context using EEA0 / EIA0



Fake eNodeB exploiting EIA0 at the RRC layer

LTE Interception: User-Plane Data Channel Established without Security



Questions?

Thank you for attention!

contact@p1sec.com