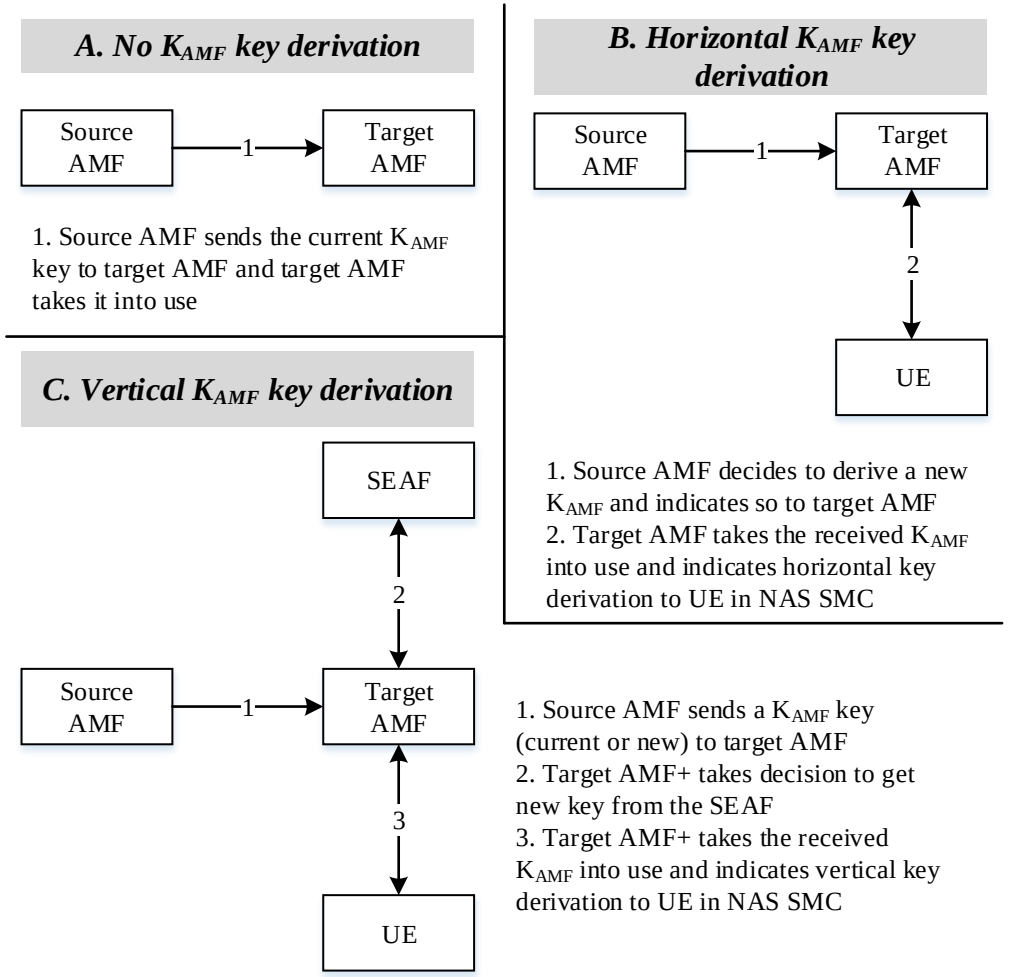
COEXISTENCE OF PHASE 1 AND 2 AMF WITH STANDALONE SEAF

Ericsson

PHASE 2 EXPECTED BEHAVIOUR WITH STANDALONE SEAF

- UE indicates support of feature = phase 2 in UE sec caps
- Source AMF takes decision based on local policy:
  1. forward current key
  2. or do horizontal key derivation
- Target AMF takes decision based on local policy:
  1. trigger a new authentication
  2. or, use received key
- Target AMF+ takes decision based on local policy:
  1. fetch a new key from SEAF
  2. or, continue using received key
- SEAF takes decision based on local policy and UE support indication:
  1. trigger a new authentication
  2. or if K_SEAF available do vertical key derivation

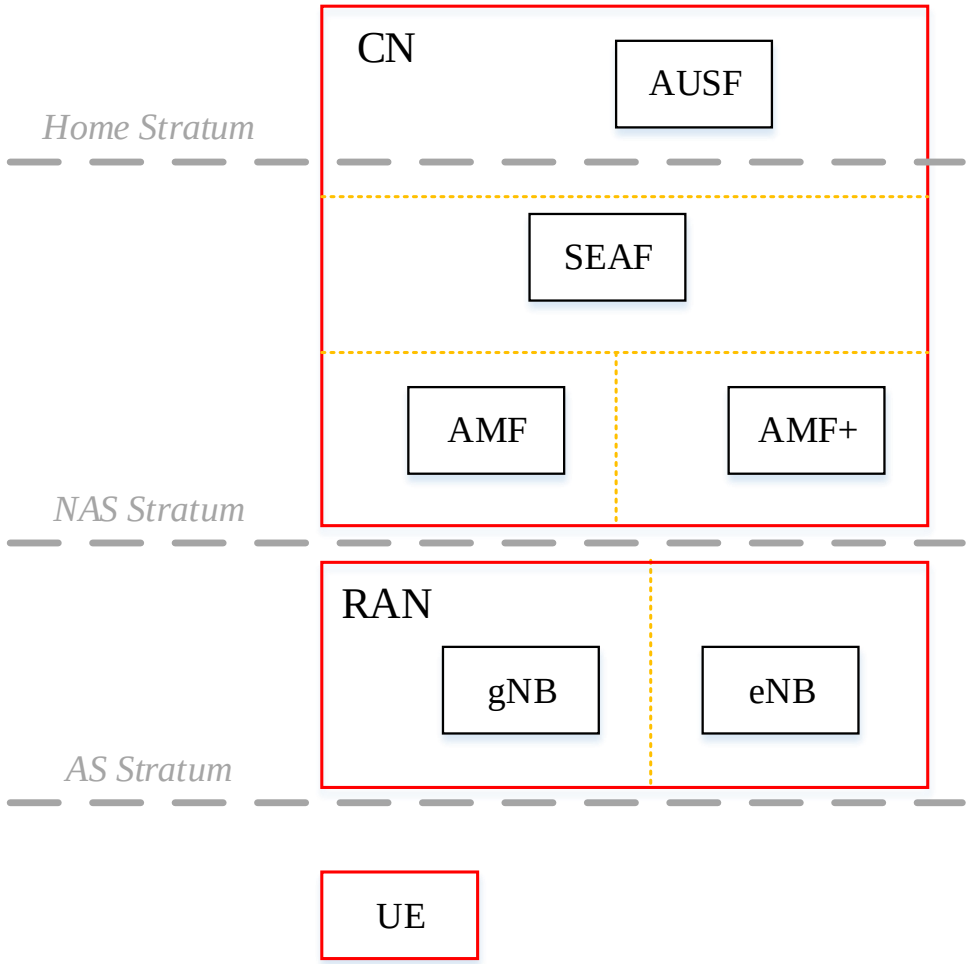


5G TRUST MODEL

Fundamental assumptions: Domains

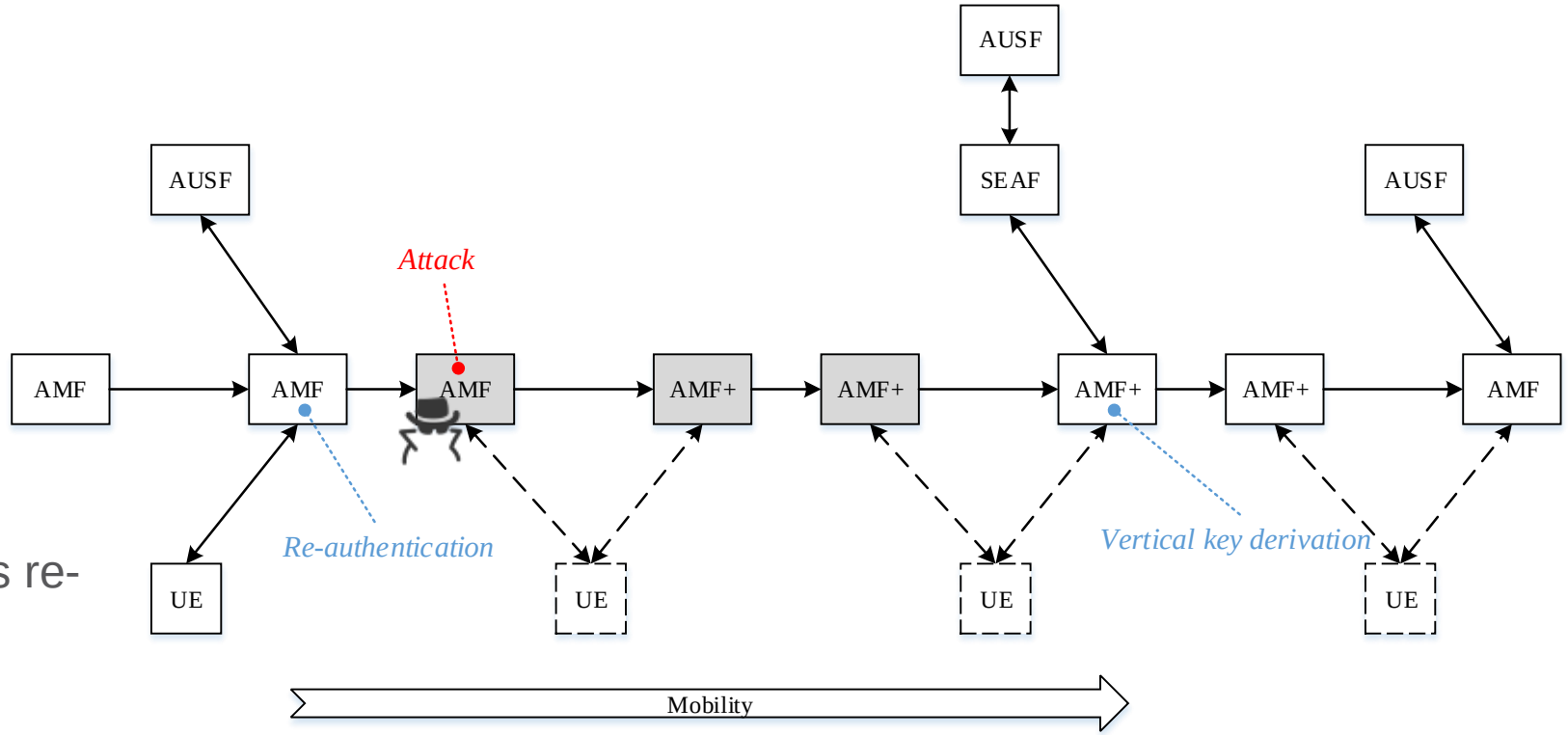
- (Authenticated) UE trusted
- Core Network (AMF) trusted
  - NAS security
- Radio Access Network (gNB, eNB) trusted
  - PDCP security
- Cater for exposure of RAN Nodes
  - Key separation between NAS and AS: separate NAS and AS keys
- Cater for compromize of nodes
  - Key separation between nodes: Horizontal and vertical key derivation during mobility or re-authentication

Enhancements: Compartments



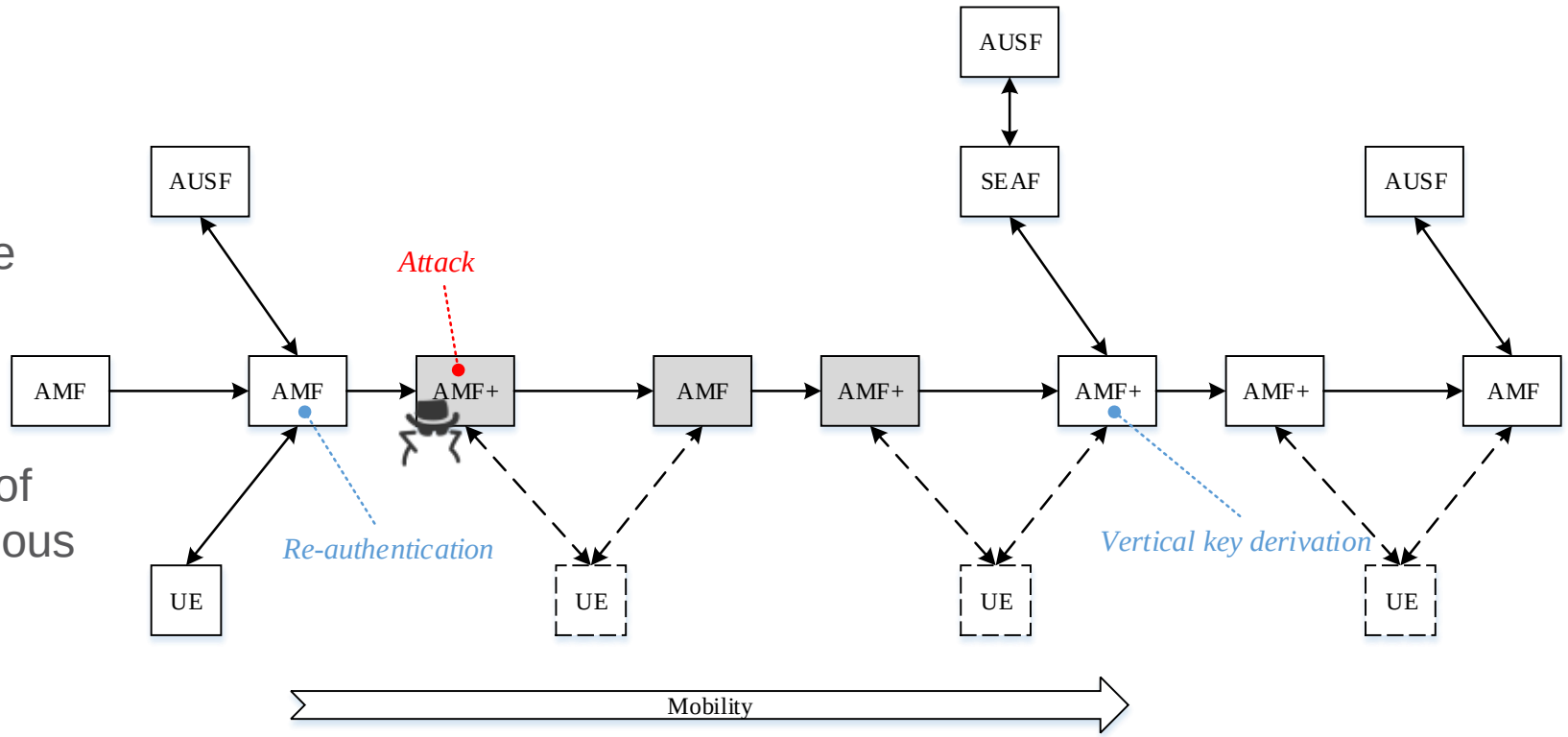
AMF COMPROMISE

- Consequences:
  - Compromise of all NAS and AS keys
- Extent:
  - Forwards in time until next re-authentication or vertical key derivation
  - Backwards in time until previous re-authentication or horizontal key derivation
- Limitation:
  - Recovery mechanism relies on mobility



FEATURE SET

- Use of feature set does not mitigate against (phase 1) AMF compromise
- Use of feature set only relevant for AMF+
- In the event of AMF+ compromise, AMF+ does not need to *lie* about the feature set
- Even when it does, the same observation on the consequences, extent of the attack, and limitations of the security mechanisms as in previous slide



ERICSSON

2018-02-08