PROTECTING IMSI AND USER PRIVACY IN 5G NETWORKS

Karl Norrman and Mats Näslund
Ericsson Research, Stockholm

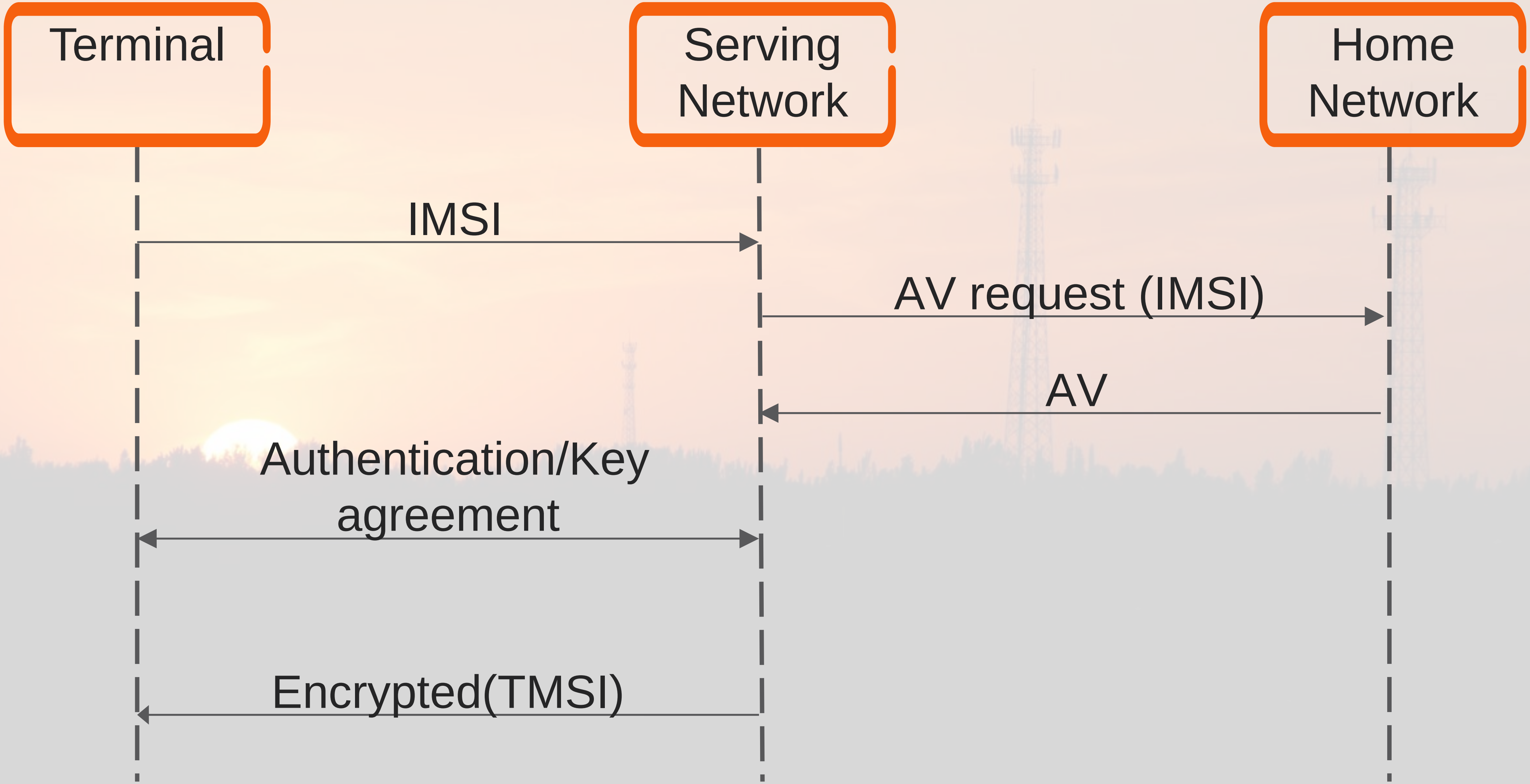
Elena Dubrova
Royal Institute of Technology (KTH), Stockholm

OUTLINE

- 3GPP Identity Handling
- IMSI Catchers
- Related Work
- Our Construction
- Applicability to 3GPP Systems
- Conclusions

3GPP IDENTITY HANDLING

FIRST CONNECT


Terminal

Serving Network

Home Network

IMSI

AV request (IMSI)

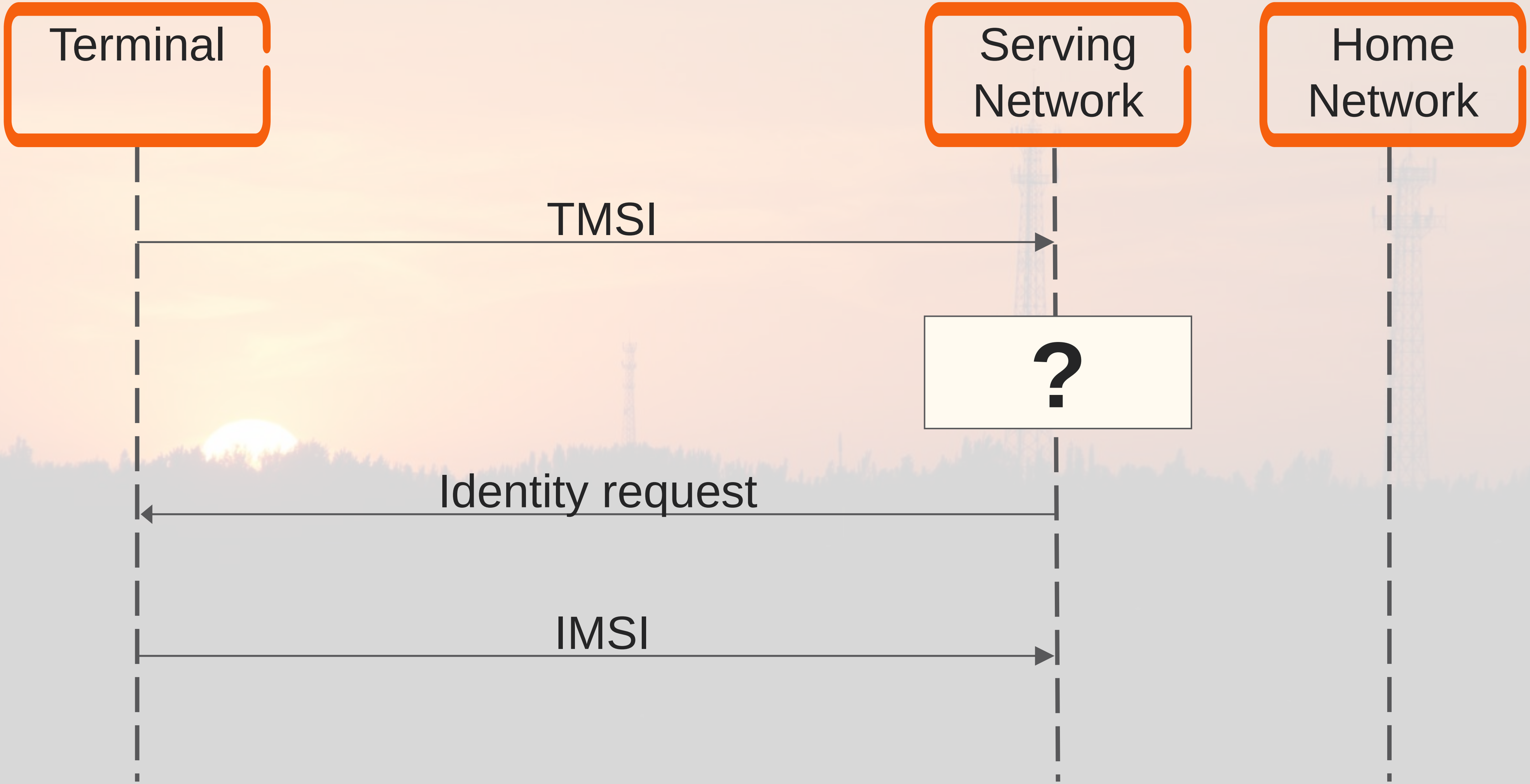
AV

Authentication/Key agreement

Encrypted(TMSI)

3GPP IDENTITY HANDLING

CONNECT WITH TMSI



Terminal

Serving Network

Home Network

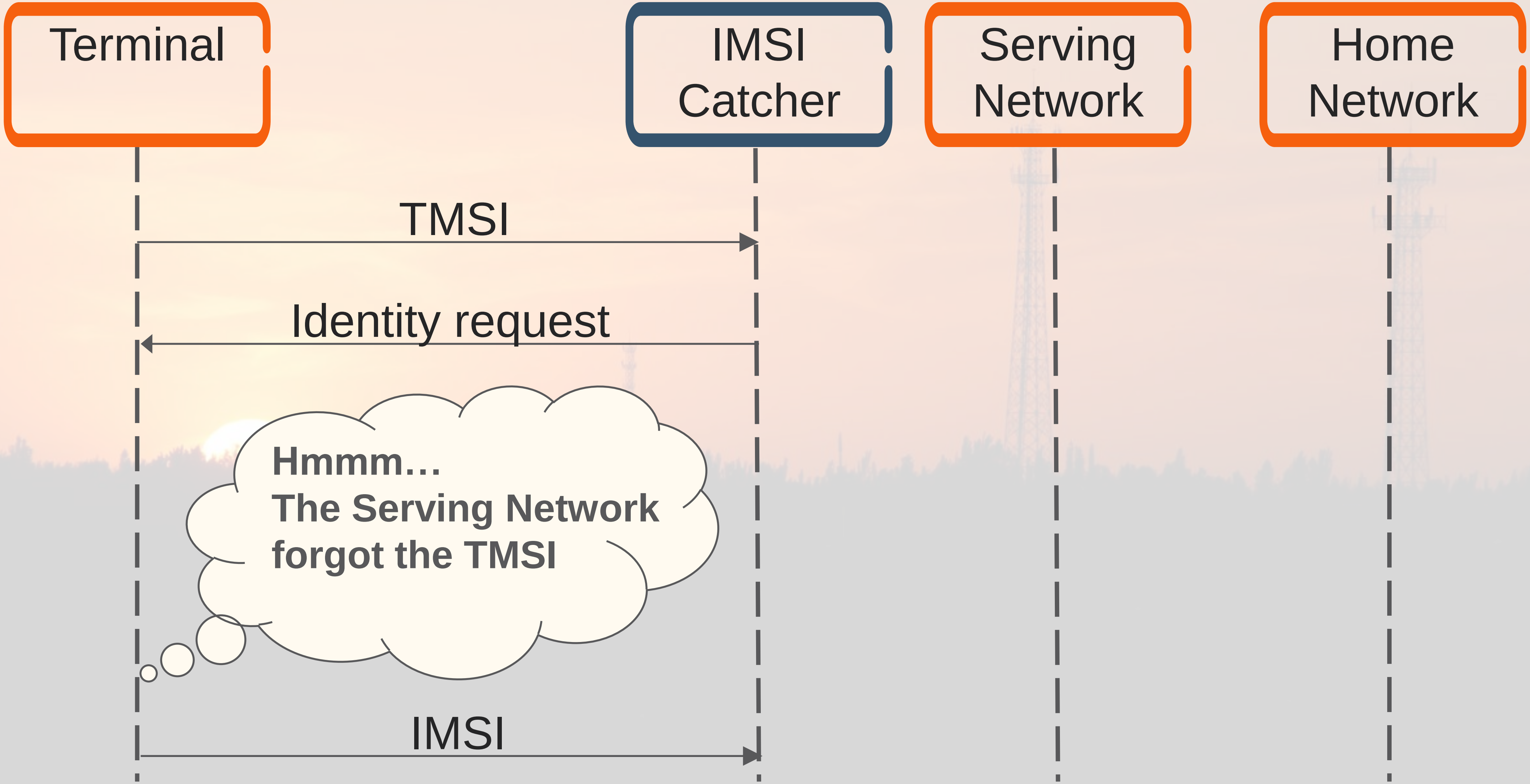
TMSI

?

Identity request

IMSI

IMSI CATCHERS



IMSI CATCHERS

A NOTE ON TERMINOLOGY…

- IMSI catching works in all 3GPP access networks (including LTE)

- Sometimes "IMSI catcher" is used also for eavesdropping false base stations
  - Such attacks **only** work against 2G

RELATED WORK
(PREVENTING IMSI CATCHING)

- A lot of academic work done in early/mid 90s
- Discussed by 3GPP when 3G/LTE was designed

- Main reasons for not being used
  - Complexity (e.g., mix networks)
  - Computationally weak terminals (e.g., public key crypto)
  - No recovery mechanisms (risk of “bricking” terminals)
  - Active attacks still work

PRIVACY TRUST MODEL MAINTAINED BY THE PROTOCOLS

- Today: 3GPP terminal trusts “the network”
- Moving towards:
  - Access network may be operated by Shopping mall, Coffee shop, Smaller VMNOs…
  - 3rd parties access to interconnect network, e.g., Analysis functions, caching functions, …

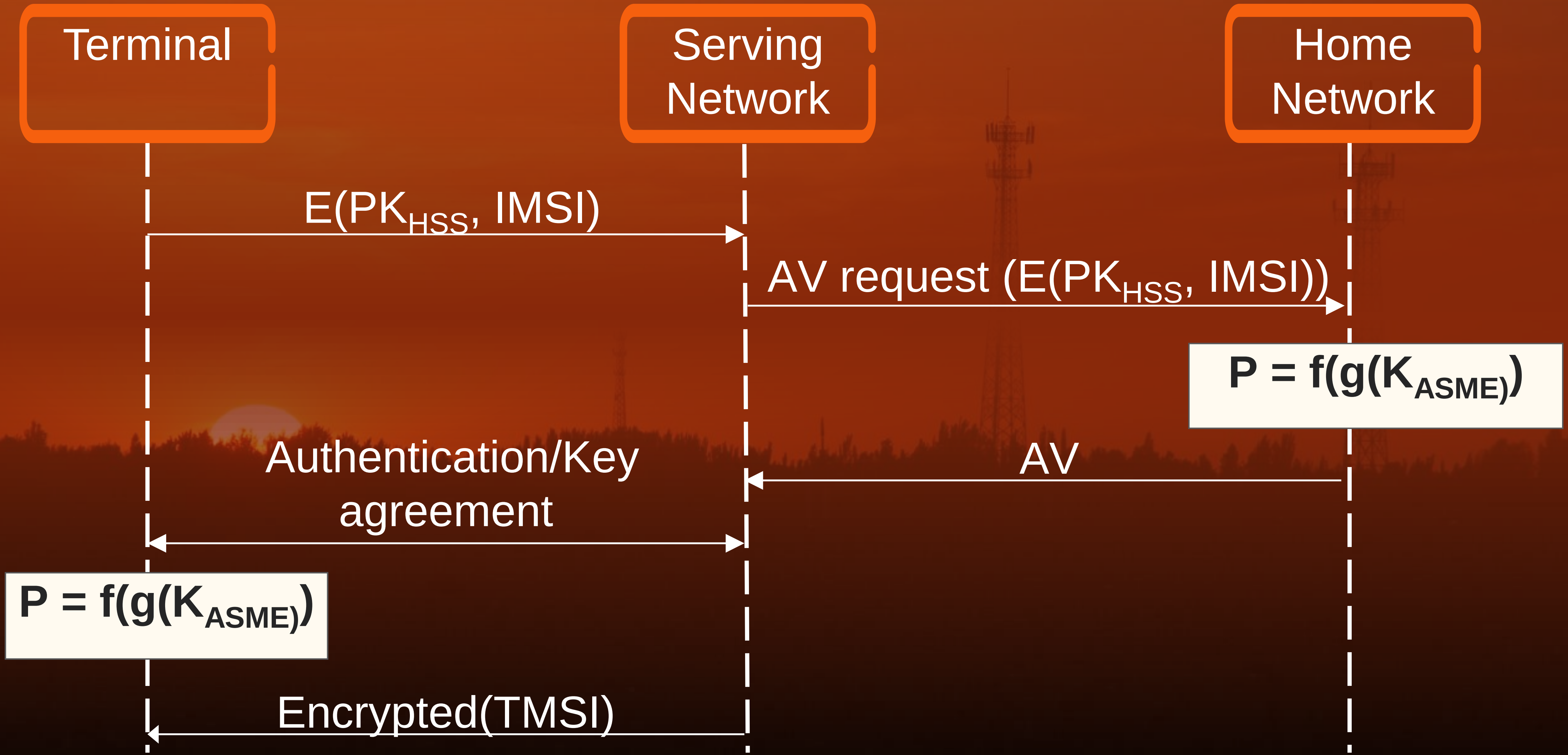
–=> Serving NW and interconnect NW may not be trusted

OUR CONSTRUCTION

- Would be good to hide IMSI from any party between UE and home network

- We give a construction for this
  - Technically and business-wise small impact
  - However, regulatory issues…

OUR CONSTRUCTION



Terminal

Serving Network

Home Network

$E(PK_{HSS}, IMSI)$

AV request $(E(PK_{HSS}, IMSI))$

$P = f(g(K_{ASME)})$

Authentication/Key agreement

AV

$P = f(g(K_{ASME)})$

Encrypted(TMSI)

OUR CONSTRUCTION
BENEFITS

- Public key operation only needed for recovery purposes (which **is** important)
- No need to roll-out new USIMs to almost all users (which is expensive and has not been done frequently in the past)
- Relatively small protocol changes
- Protect against honest-but-curious attackers in the interconnect NW and serving NW

OUR CONSTRUCTION
PRIVACY

- IMSI is protected **in *the authentication and identification procedures***

- However, many ***other*** ways an attacker with access to interconnect NW can obtain user ID
  - DIAMETER, SS7, …
- No solution for this yet…

OUR CONSTRUCTION
PRIVACY AND REGULATION

- Lawful Intercept (LI) specifications in 3GPP:
  - Terminal shall be identifiable in serving NW using IMSI
  - Intercept in serving NW shall be possible without home NW knowing about it

- Seems impossible to reconcile with IMSI privacy from attackers in serving NW or interconnect NW using current 3GPP architecture

CONCLUSION

- Possible to provide IMSI confidentiality for the authentication and identification protocols
- Relatively small protocol/business model impacts

- Not comprehensive privacy protection
- Solutions could be illegal to operate in some jurisdictions

QUESTIONS?

ERICSSON