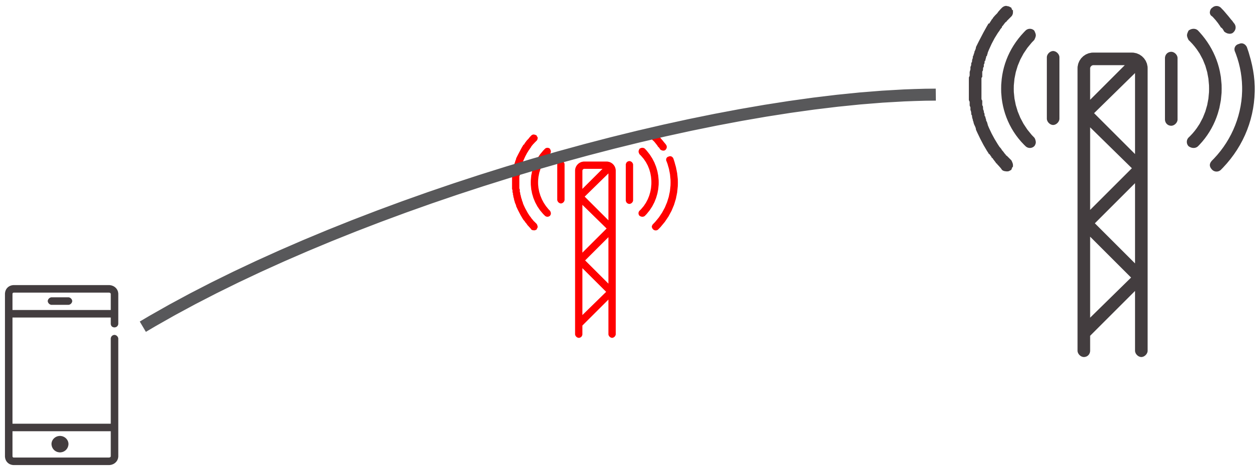
A USIM COMPATIBLE 5G AKA PROTOCOL WITH PERFECT FORWARD SECRECY

Jari Arkko, Karl Norrman, Mats Näslund and Bengt Sahlin

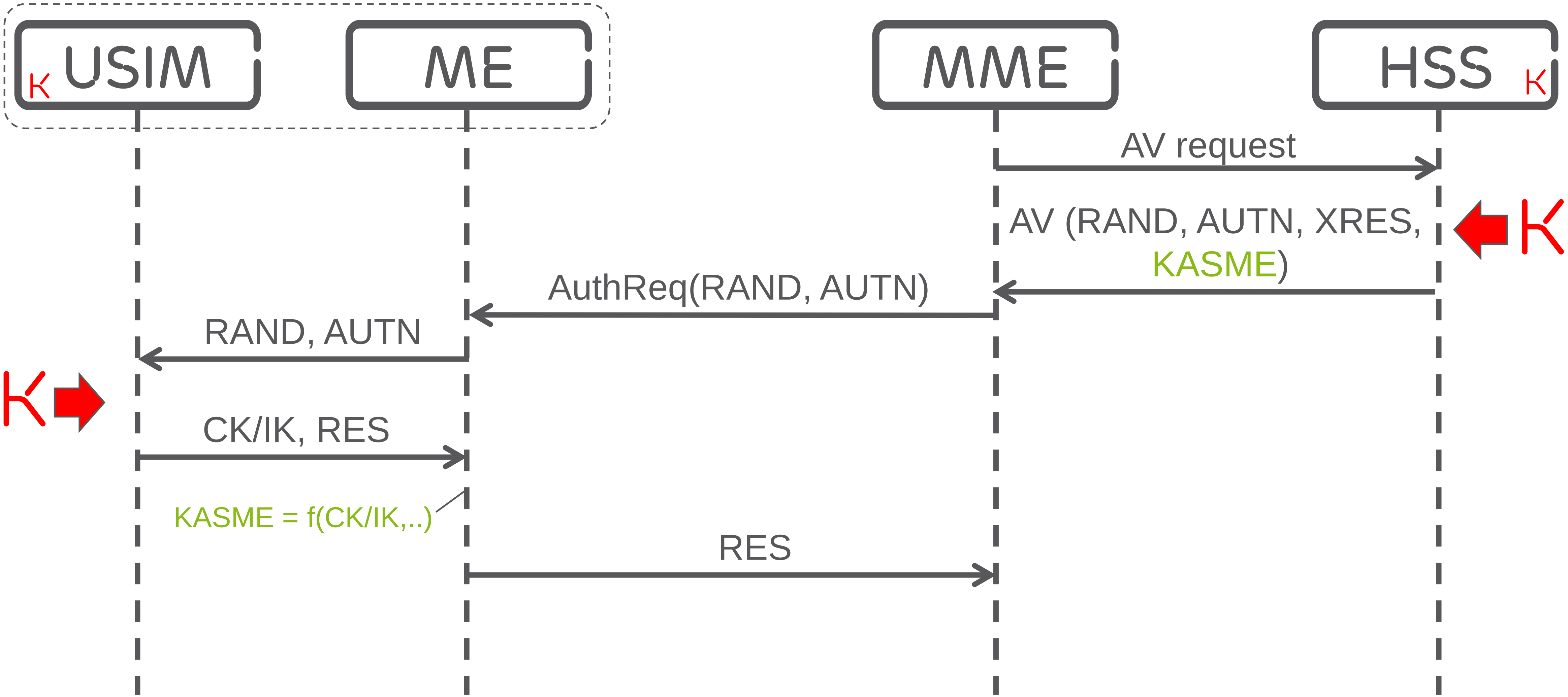
CONTENTS

MOTIVATION

- Recent reports of compromised subscriber authentication keys in mobile networks
- Compromised authentication keys imply passive attacker can eavesdrop and decrypt traffic



BACKGROUND - AKA



PERFECT FORWARD SECRECY

- PFS – term has been used to mean different things in discussions lately
- In this paper we use the classic definition of PFS, namely
  - The session key (KASME) is secure even if the long-term key (K) is compromised in the future [4]

- According to this definition: PFS gives no guarantees for session keys generated **AFTER** the long-term key is compromised

These have PFS

KASME1, KASME2, KASME3

K compromise

These do not have PFS

KASME4, KASME5, KASME6

time

[4] W. Diffie, P. van Oorschot and M. Wiener, "Authentication and Authenticated Key Exchanges," Designs, Codes and Cryptography 2 (2): pp. 107–125, June 1992.

PERFECT FORWARD SECRECY

- PFS is good, but not the only property we are looking for
- Also want to make it more difficult to obtain KASMEs generated after K has been compromised
- Diffie-Hellman helps with that too, in addition to giving PFS

DIFFIE-HELLMAN

- Using DH for session key establishment gives PFS, but also:

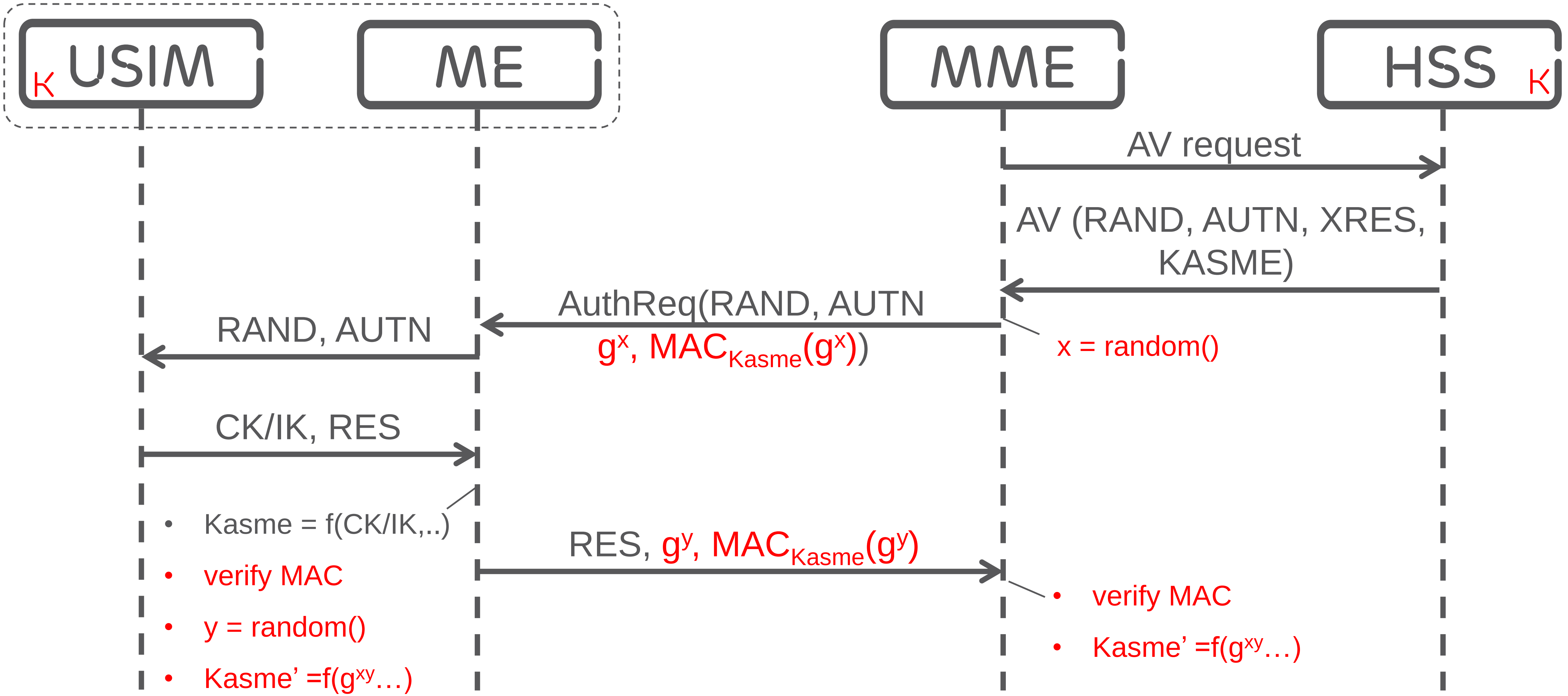
- **Even if attacker has long-term key: passive attacks remain ineffective**

- To make efficient attack, <u>active</u> MITM is required

DIFFIE-HELLMAN

- We propose two options, A and B
- Option A: use KASME to authenticate a DH exchange between MME and UE
- Option B: use K to authenticate DH exchange between HSS and UE

OPTION A

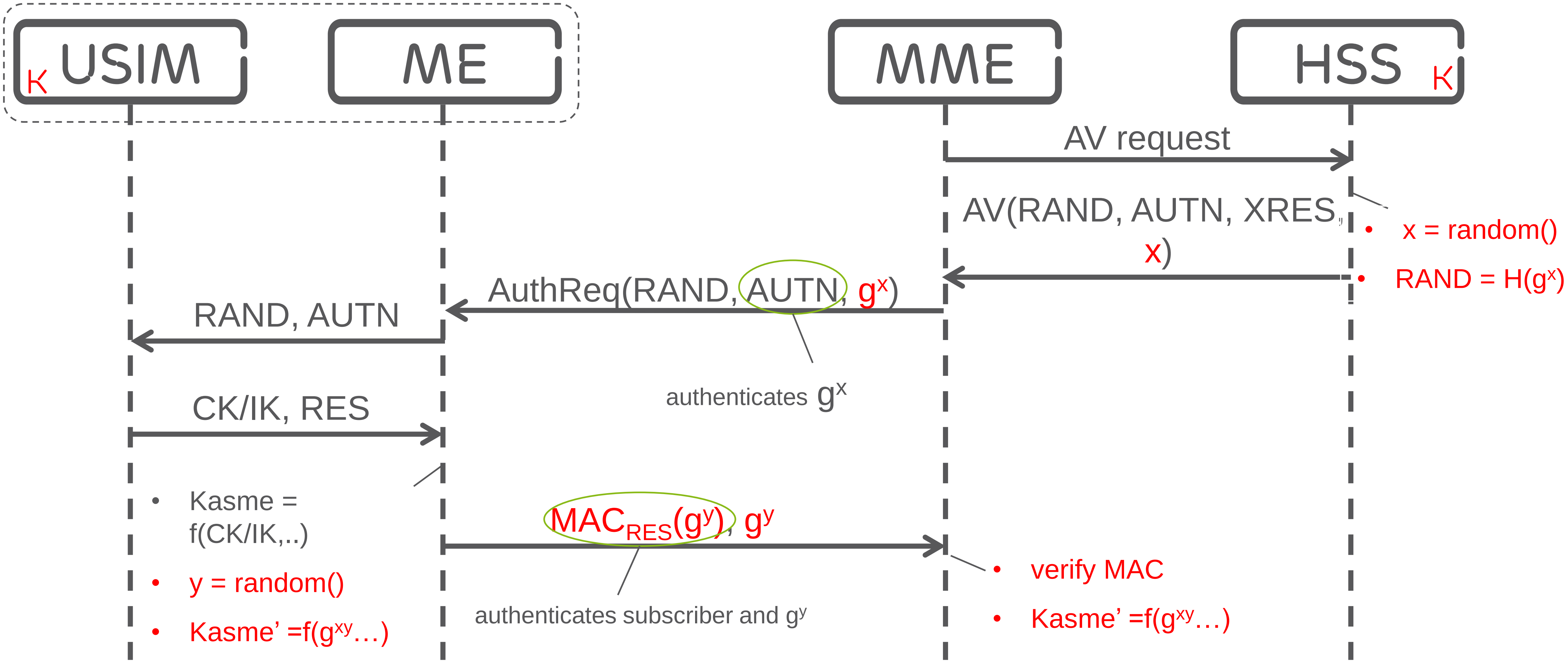


K
USIM
ME
MME
HSS
K
AV request
AV (RAND, AUTN, XRES, KASME)
AuthReq(RAND, AUTN g^x, MAC_Kasme(g^x))
x = random()
RAND, AUTN
CK/IK, RES
• Kasme = f(CK/IK,..)
• verify MAC
• y = random()
• Kasme' =f(g^xy…)
RES, g^y, MAC_Kasme(g^y)
• verify MAC
• Kasme' =f(g^xy…)

OPTION A - ANALYSIS

- No changes to HSS
- No changes to HSS-MME interface (S6)
- No changes to USIM
- Some overhead over air interface
- DH processing in ME and MME

OPTION B


USIM
K
ME
MME
HSS
K
AV request
AV(RAND, AUTN, XRES, x)
x = random()
RAND = H(g^x)
AuthReq(RAND, AUTN, g^x)
RAND, AUTN
authenticates g^x
CK/IK, RES
Kasme = f(CK/IK,..)
y = random()
Kasme' =f(g^{xy}…)
$MAC_{RES}(g^y)$, g^y
authenticates subscriber and g^y
verify MAC
Kasme' =f(g^{xy}…)

OPTION B - ANALYSIS

- USIM is unchanged
- Smaller overhead over air interface
- AUTN serves as MAC of g^x (since RAND depends on g^x)
- RES is replaced by $MAC_{RES}(g^y)$, serves both as MAC of g^y and as authentication response

BENEFITS

- Can be introduced in 5G without updating (U)SIMs
- Even if attackers get hold of K, they still effectively need to be an active MITM to get the session key
- Fits in the message framework used in 2G/3G/4G with minor updates to message formats
- Does not require rolling out a PKI

CONCLUSION

- Shown effective ways to limit effects of compromised K
- Most attractive for future systems due to amount of deployed legacy equipment
- Protection of long-term secret still important, regardless of which protocols are used

ERICSSON