Privacy Preserving AKMA in 5G

UNIVERSITY OF HELSINKI
Department of Computer Science

Mohsin Khan[1]
Philip Ginzboorg[2,3]
Valtteri Niemi[1]
[1]University of Helsinki
[2]Huawei Technologies, [3]Aalto University

AKMA

AKMA (Authentication and Key Management for Applications) is a solution currently under development by 3GPP. AKMA will support authentication and key management aspects for applications and 3GPP services based on 3GPP credentials in 5G, including the IoT use case [1].

GBA

GBA (Generic Bootstrap Architecture) was developed by 3GPP during standardization of previous generations of mobile system. GBA has purposes which are similar to AKMA. AKMA solution candidates can be seen as an evolution of GBA [1].

AKMA Requirements Identifed by 3GPP

(1) Delegating Authentication

(2) AKMA is Access Independent

(3) Freshness of AKMA authenticated sessions

(4) Privacy of long term identity

(5) Privacy of sensitive content

(6) Lawful Interception

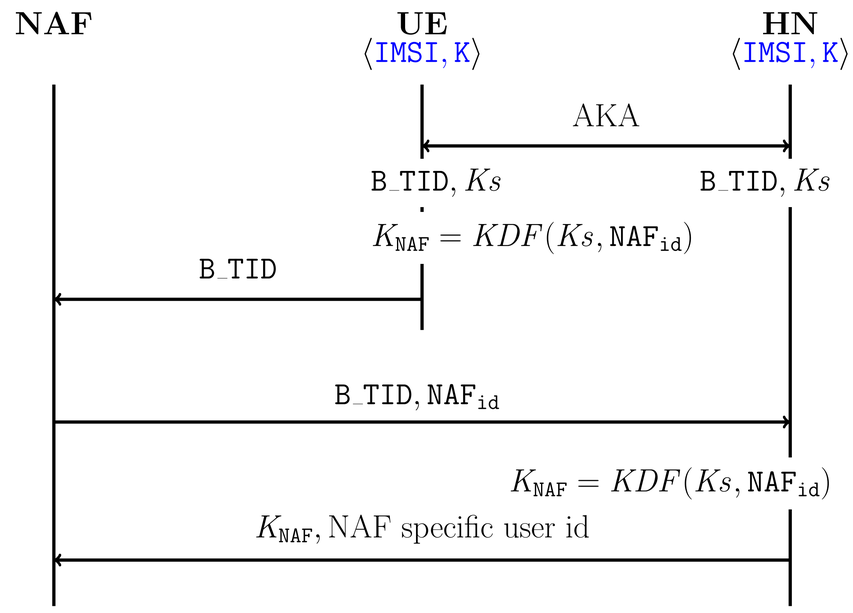

Fig: GBA (Highly Abstracted)

Additional Requirements

(7) HN should not know what are the NAFs a user is using

(8) HN should not know the identity used between a user and a NAF

(9) NAF should not know if two of its users are the same user of an HN

(10) Linking between a user's NAF identity and HN identity is not possible

(11) A NAF user should be able to connect to the NAF seamlessly using any of the many USIMs the user owns even if multiple NAFs collude

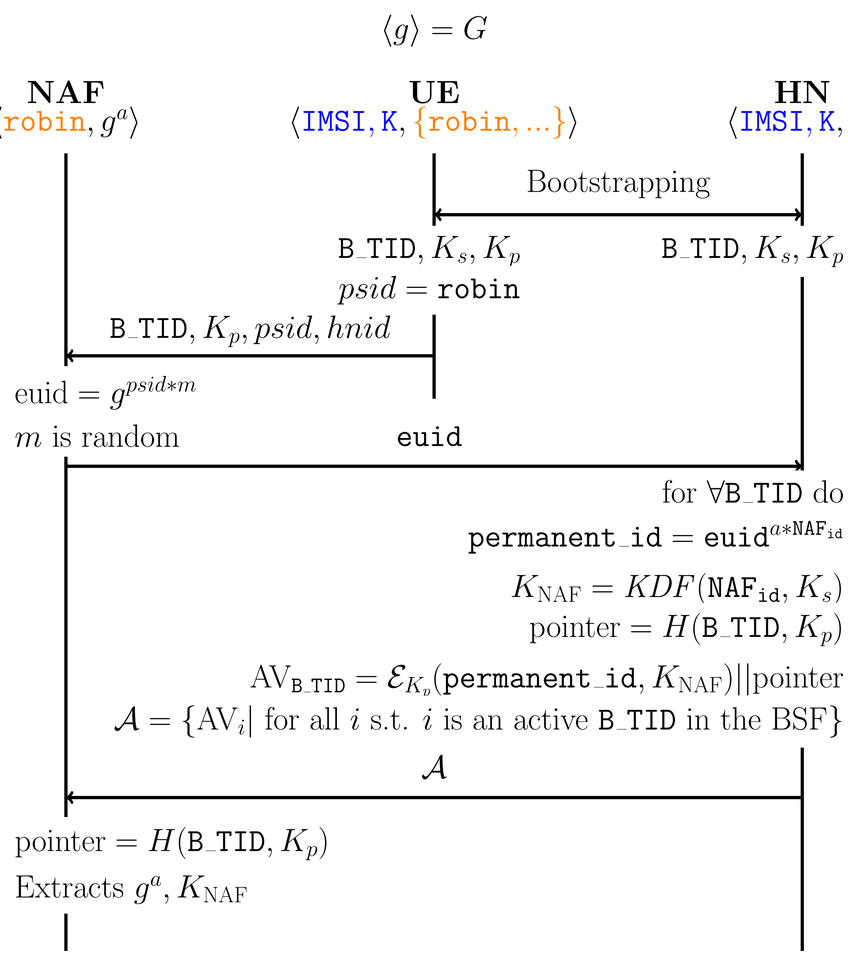

Fig: Privacy Preserving Variant AKMA

(Fulfills all the 3GPP-identified and most of the newly identified requirements of AKMA)

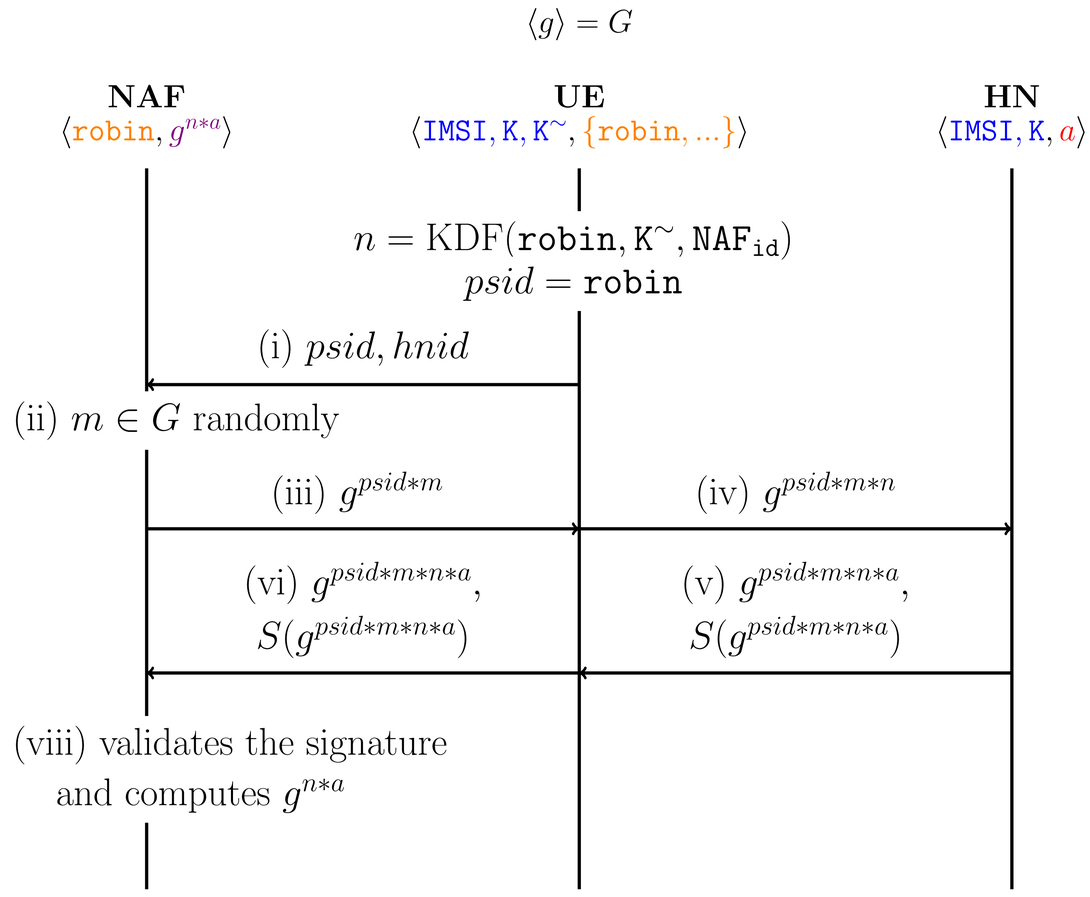

Fig: AKMA Based on Delay Target DHP

(Fulfills all but one of the new requirements. Further research needed to conclude if it fulfills all of the 3GPP requirements)

References

[1] 3GPP: 3GPP TR 33.835 Study on authentication and key management for applications; based on 3GPP credential in 5G V0.4.0 (March 2019)