UNIVERSITY OF HELSINKI
FACULTY OF SCIENCE

HUAWEI

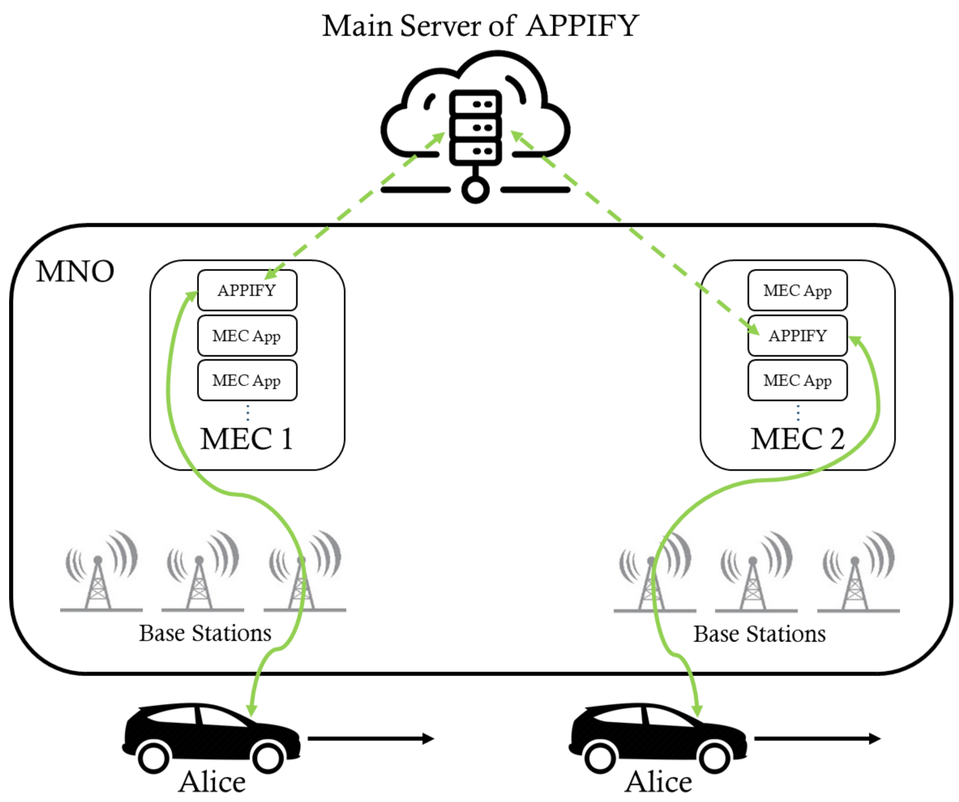
Gizem Akman, Valtteri Niemi
Department of Computer Science, University of Helsinki
Helsinki Institute for Information Technology (HIIT)
Philip Ginzboorg
Huawei, Finland

AKMA for Secure MEC Mobility in 5G

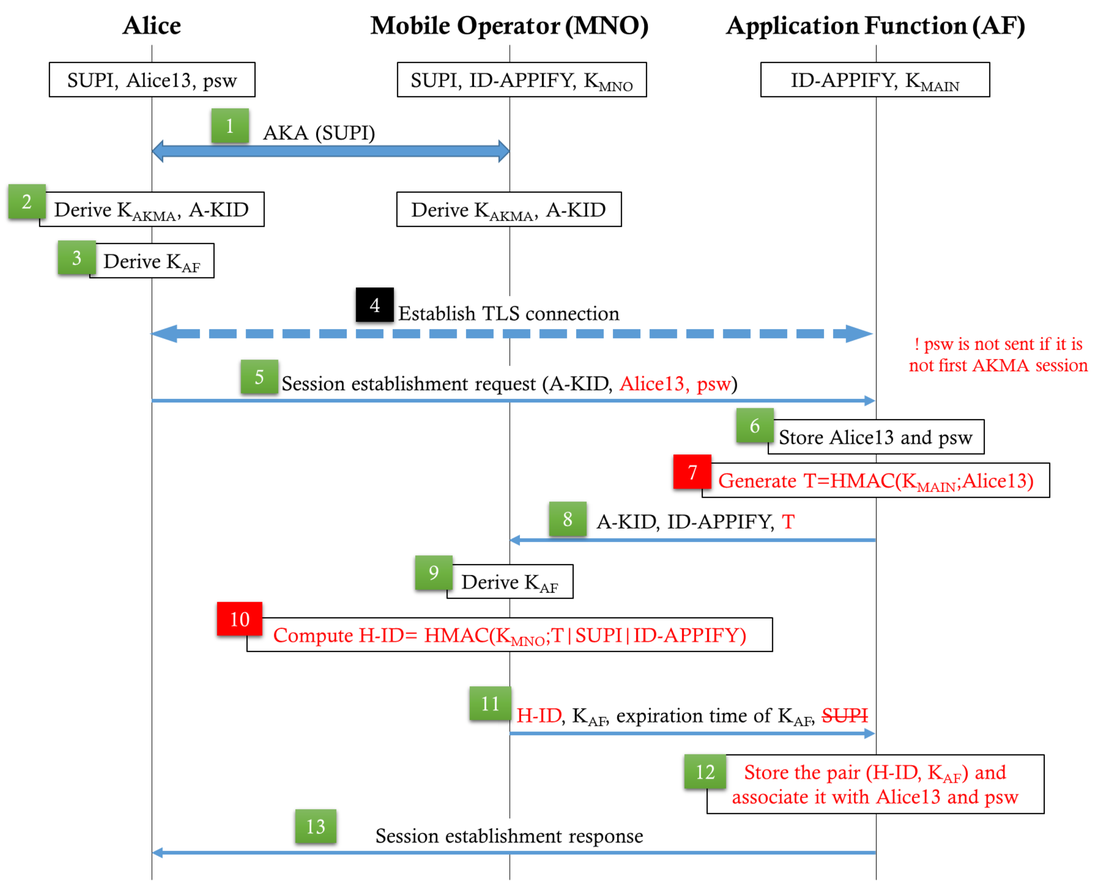
Scenario

Alice is a subscriber of a Mobile Network Operator (MNO). Alice uses a MEC application APPIFY.

- She wants to continue using APPIFY with the benefits of MEC services while she is traveling.
- Meanwhile, she wants to protect her information, e.g., the name of APPIFY and the content of her communication with APPIFY should not be visible to MNO.



Privacy Enhanced AKMA



- Black text is AKMA as described in 3GPP TS 33.535 V17.4.0 (2021)
- Red text is our contribution for improving user privacy against MNO

Authentication and Key Management for Applications (AKMA)

- AKMA is a service in the 5G system to support authentication and secure channels between the UE and applications.
- AKMA relies on the credentials and identities of the mobile subscriber, which are pre-established with MNO for 5G access.

Mobile Connection to MEC Applications

- We use AKMA between Alice and the main server of the MEC application. The keys derived from AKMA are used for the mutual authentication between Alice and local MEC application.
- Application key management of the mobile user is through the application's main server.
- Protocols:
  - Registering new users or new devices at the main server
  - Establishing a secure connection with the main server
  - Establishing a secure connection with the MEC application in the mobile network (shown on the right)

This study is accepted to the PCEIoT 2022 and will be published in Proceedings of International Conference on Computational Science and Its Applications – ICCSA 2022 .