HELSINGIN YLIOPISTO
HELSINGFORS UNIVERSITET
UNIVERSITY OF HELSINKI
MATEMAATTIS-LUONNONTIETEELLINEN TIEDEKUNTA
MATEMATISK-NATURVETENSKAPLIGA FAKULTETEN
FACULTY OF SCIENCE

Gizem Akman
Valtteri Niemi
Department of Computer Science,
University of Helsinki
Philip Ginzboorg
Huawei, Finland
Aalto University

Privacy-Preserving Access for MEC Applications

Scenario

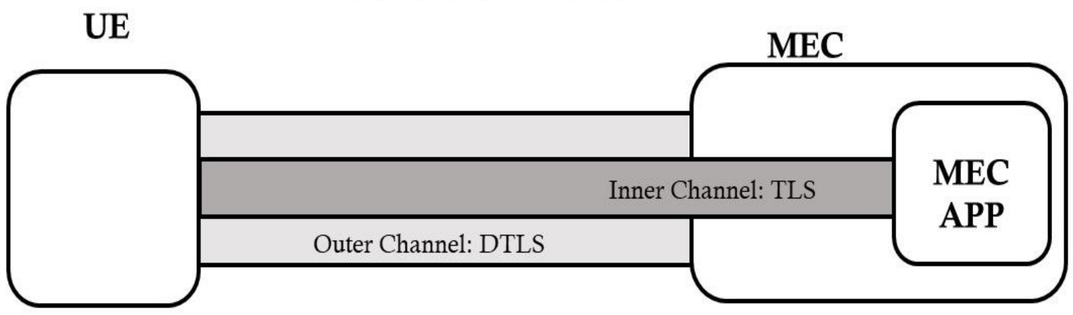
Alice is a subscriber of a Mobile Network Operator, MNO. Alice wants to use a MEC application, APPIFY.

- Messages between Alice and APPIFY go through MNO and MEC host.
- MNO and MEC host can see the encrypted message flow between Alice and APPIFY.
- Alice does not want to reveal the identity of APPIFY, the identities of herself, and the content of the messages to other parties.
- For example, outsiders should not learn anything, while MEC should only know the identity of APPIFY. MNO should only know IMSI of Alice.

Adversary Models

Honest-but-Curious – a party in a communication protocol who does not deviate from the protocol, but still tries to learn all possible information through the legitimately received messages.
Dolev-Yao – an adversary that can see, delete, replay, reroute, and reorder the messages transmitted in the network.

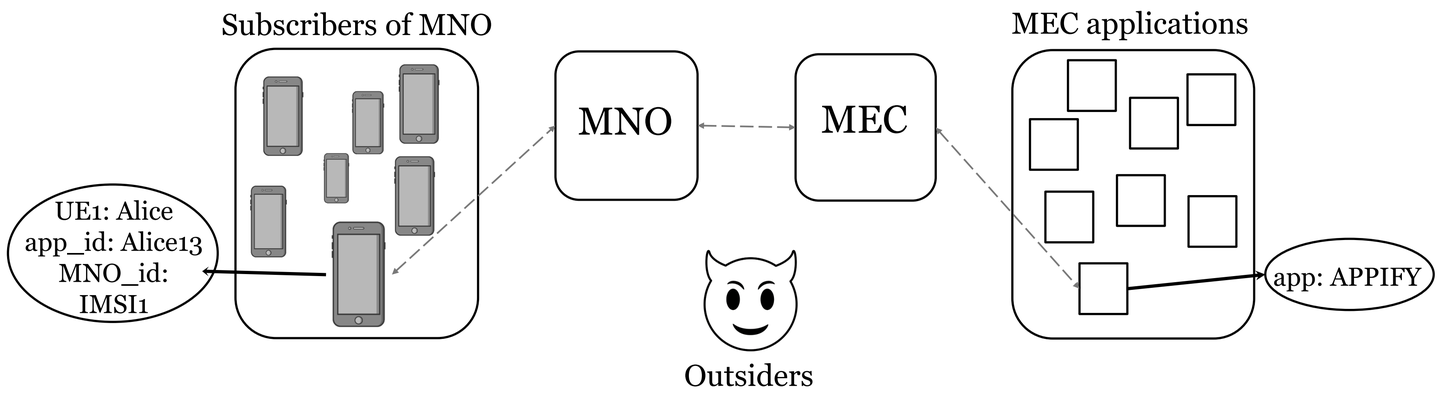
Solution Idea



Analysis

- Solution includes secure inner and outer channels. Various protocols could be used to secure these channels, e.g., outer channel is DTLS/UDP and the inner channel is TLS/TCP.
- All requirements related to data and identity confidentiality are fulfilled, except that the identity of the APPIFY might be learned by MNO and outsiders via traffic analysis.
- Unlinkability requirements are partially fulfilled, but traffic analysis may reveal relation between messages, e.g., if the same IP address is used.

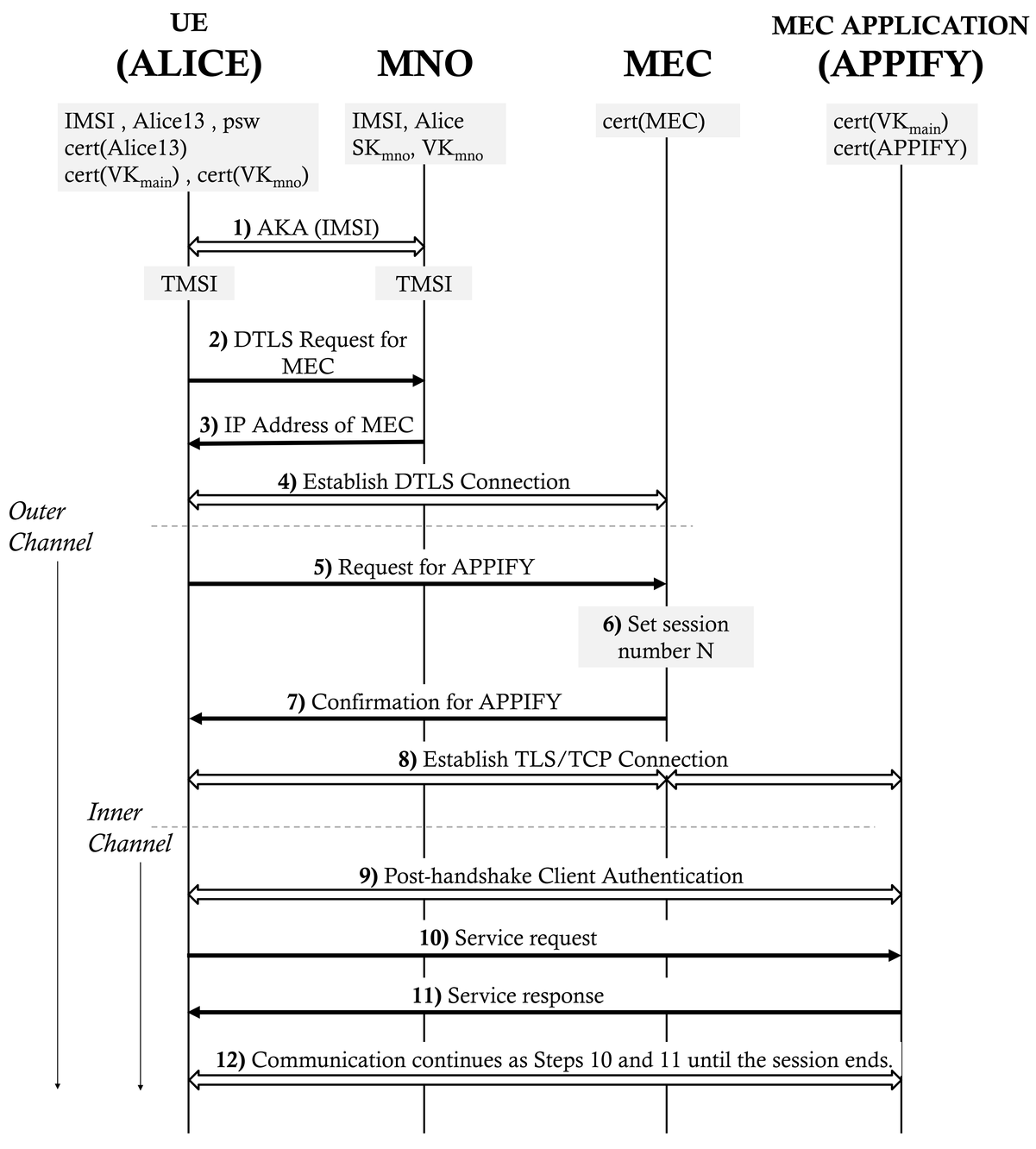
System Model



Privacy notions

Data Confidentiality (D) – to provide data of the user to the parties who need it for providing service and not revealing the data to other parties.
Identity Confidentiality (I) – to protect the identities of the user from the parties who do not need for providing the service.
Unlinkability (U) – to prevent distinguishing whether two messages belong to the same user, same destination, or have the same identifier.

Solution Details



MEC is one of the emerging key technologies in 5G Mobile Networks, providing reduced end-to-end latency for applications and reduced load in the transport network.