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

Embedded UICC in 5G AKMA

eSIM and eUICC

eSIM (Embedded Subscriber Identity Module) – SIM technology that does not come in physical card, instead it is embedded in the device.

eUICC (Embedded Universal Integrated Circuit Card) – A removable or non-removable UICC which enables remote management of Profiles in a secure way.

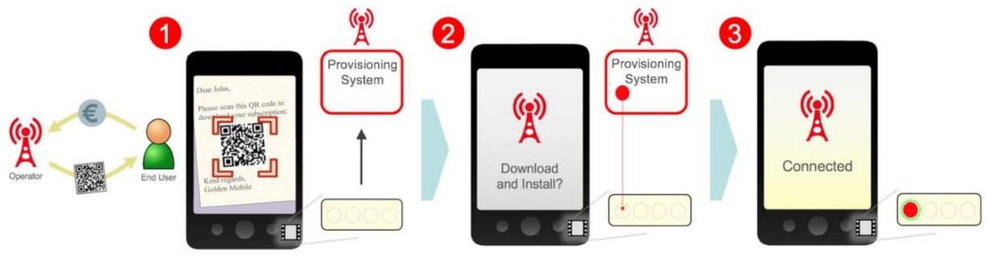
AKMA (Authentication and Key Management for Applications)

- The 3GPP authentication infrastructure is a very valuable asset of mobile operators. It could be leveraged to enable application server and user application for establishing shared keys.
- In the past: 3GPP provided the "bootstrapping of application security" to authenticate the subscriber by Generic Bootstrapping Architecture (GBA) based on Authentication and Key Agreement (AKA) protocol.
- The AKMA feature is intended to leverage the 5G authentication infrastructure for similar purpose.
- GBA would be one of the starting points for the architectural design of AKMA.

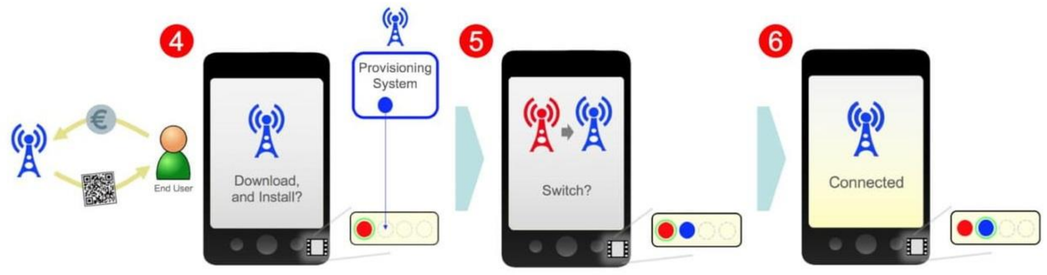
Remote SIM Provisioning (RSP)

RSP – the downloading, installing, enabling, disabling, switching, and deleting of a Profile on an eUICC.

Profile – A combination of data and applications to be provisioned on an eUICC for the purpose of RSP.



Remote SIM Provisioning Operation – Operator Profile Installation



Remote SIM Provisioning Operation – Operator Profile Selection

Profiles in eUICC

- The eUICC contains zero or more Profiles.
- No limitations for number of Profiles that can be stored in eUICC; depends on the capacity of the eUICC.
- At most **one Profile is enabled** at any point in time.

Problem

We focus on the case, where the eUICC contains two (or more) Profiles, and the user's primary Profile, which defines network connectivity, is different from the Profile, which is used for authentication in an application (AKMA). We want to provide a service that will complete AKMA procedure without dropping the connection of the primary Profile. However, specifications allow only one Profile to be active at a time.

Solution

We have studied how to remove the limitation of only one active Profile. During the setup of a network connection, eUICC is active for authentication and key agreement, or at minimum gives the keys to the device. After the connection has been established, eUICC does not actively participate in the process. Therefore, we suggest that eUICC may temporarily disable the Profile for network connection if there is a request to enable the AKMA Profile. The AKMA Profile in eUICC completes authentication and key management, and gives the key to the device. Then, eUICC disables the AKMA Profile and retains the Profile for network connection.

REFERENCES

1. GSMA SGP.21 V2.1 (2017) – "RSP Architecture".
2. GSMA (2018) – "eSIM Whitepaper".
3. 3GPP TR 33.835 V0.4.0 (2019) – "Study on authentication and key management for applications based on 3GPP credential in 5G".
4. 3GPP TS 33.220 V15.4.0 (2018) – "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".