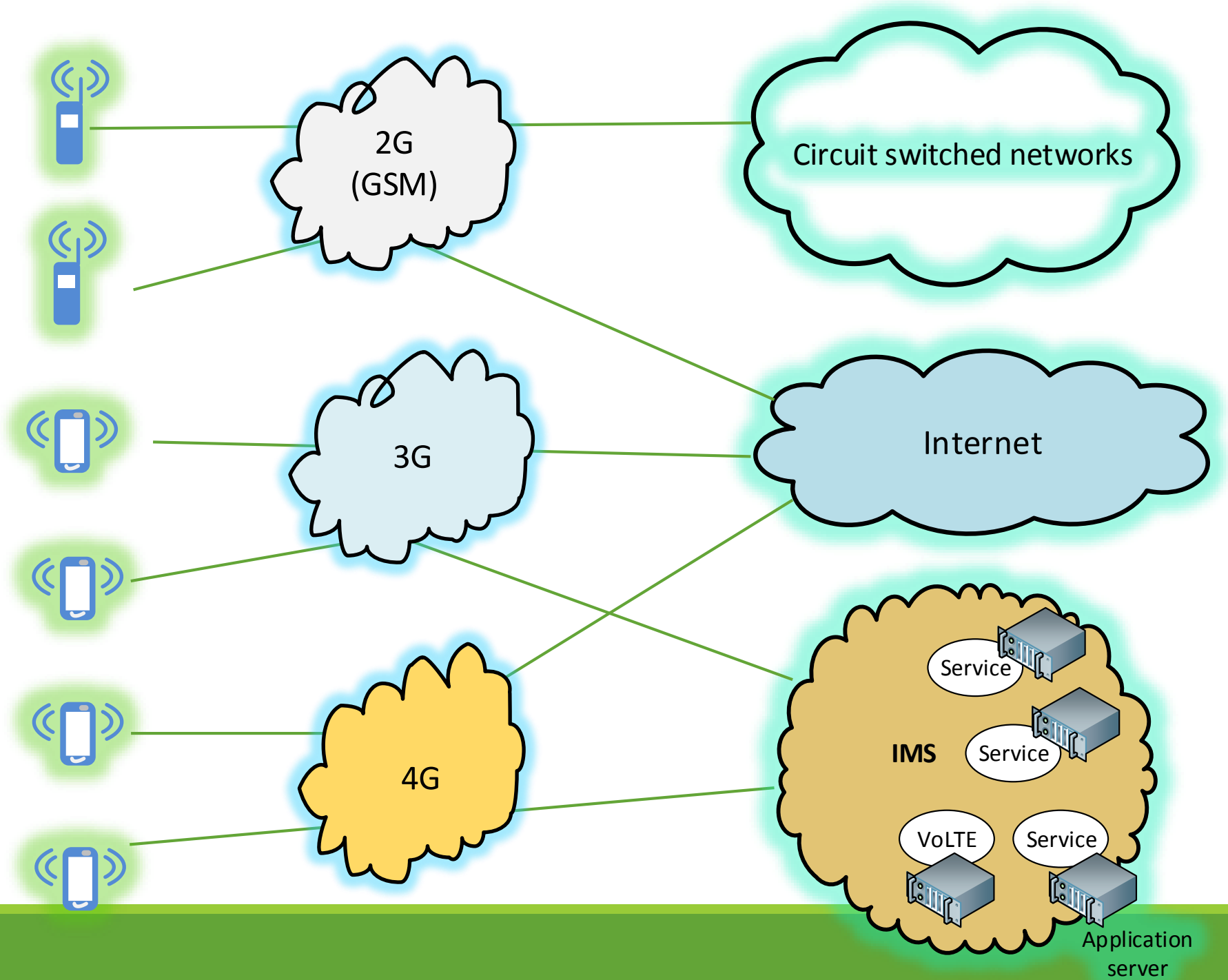
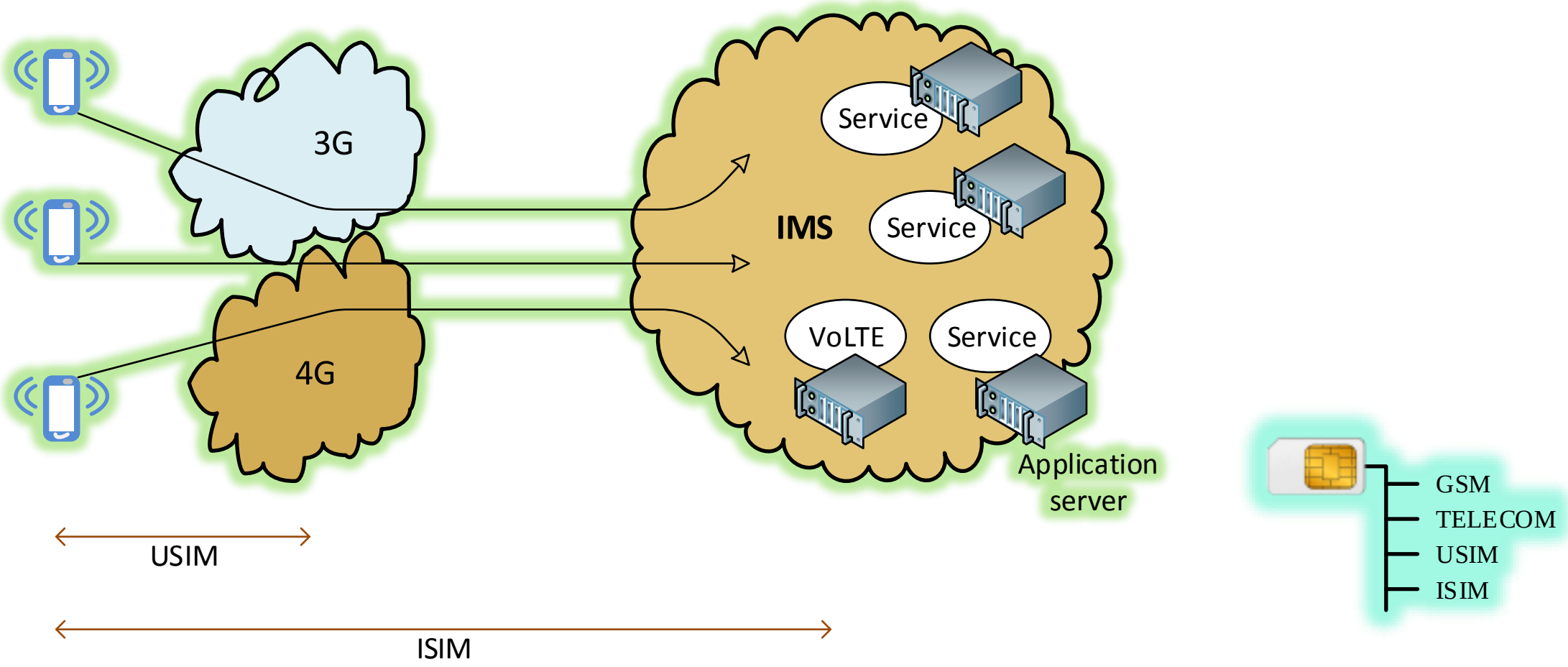
Nové možnosti autentizace aplikací v nových generacích mobilních sítí

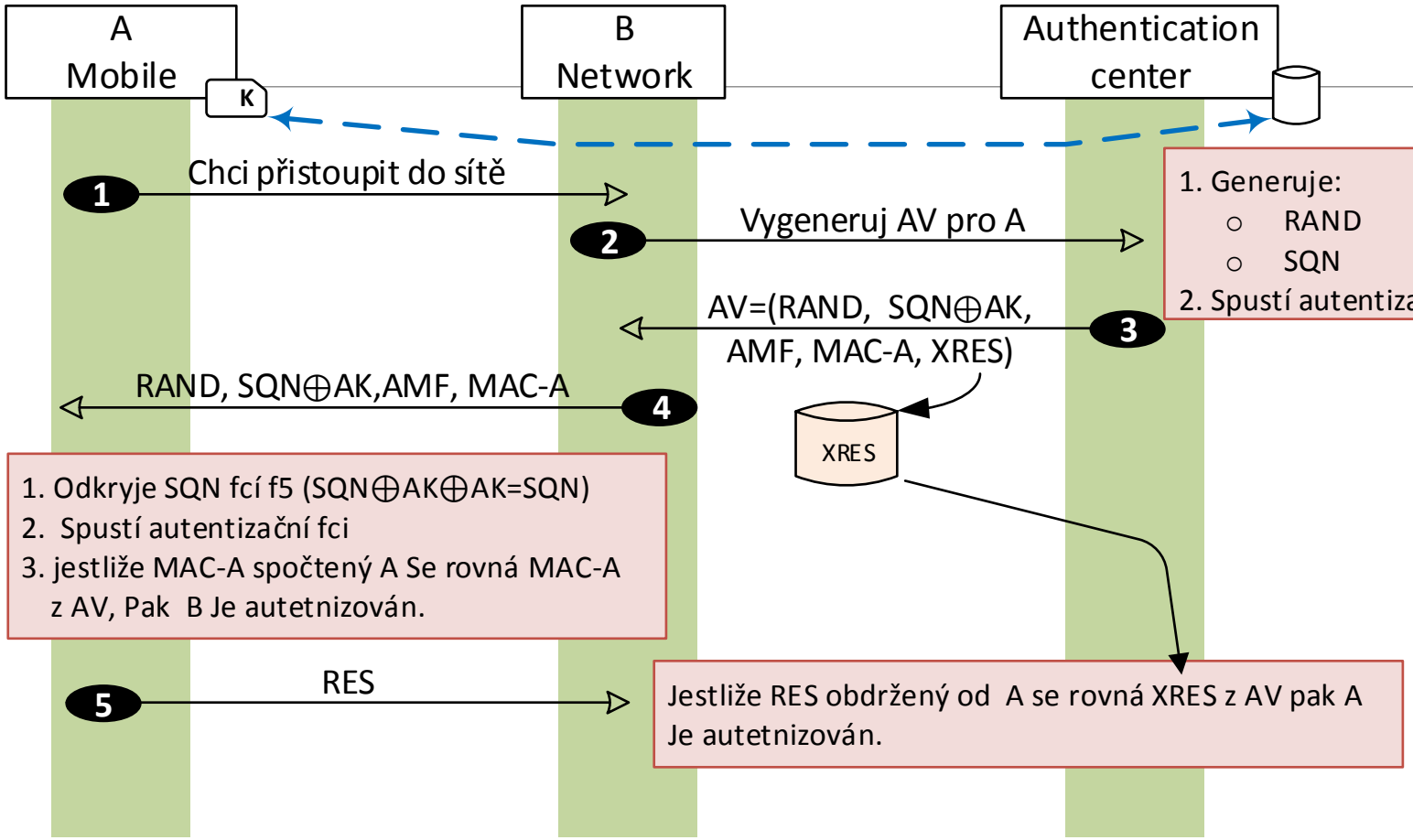
LIBOR DOSTÁLEK


2G
(GSM)
Circuit switched networks
3G
Internet
4G
IMS
Service
Service
VoLTE
Service
Application
server

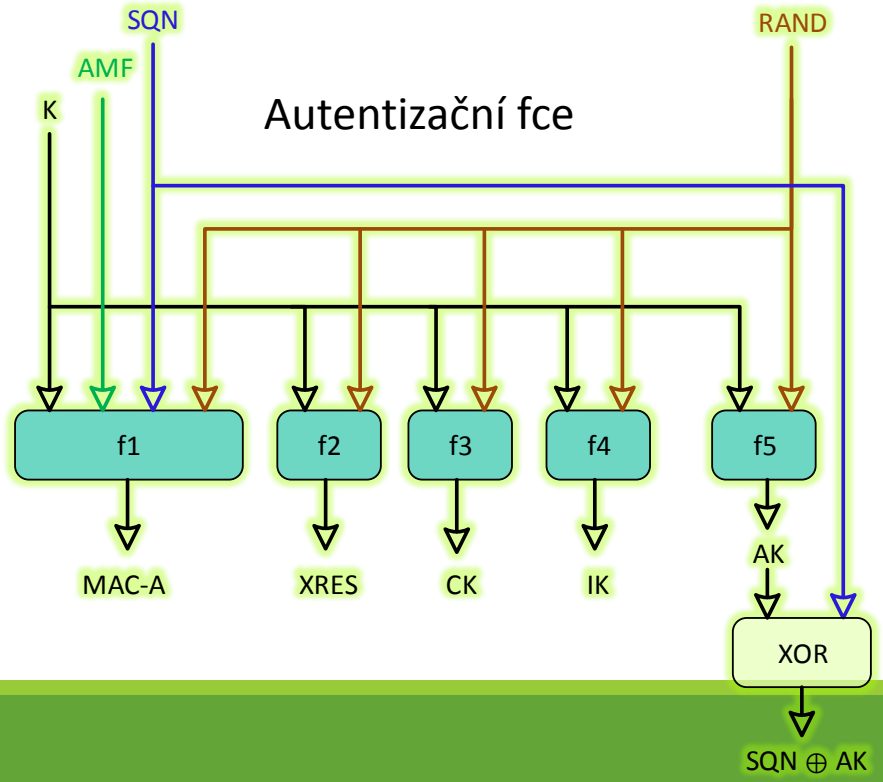
Autentizace v 3G/4G/IMS



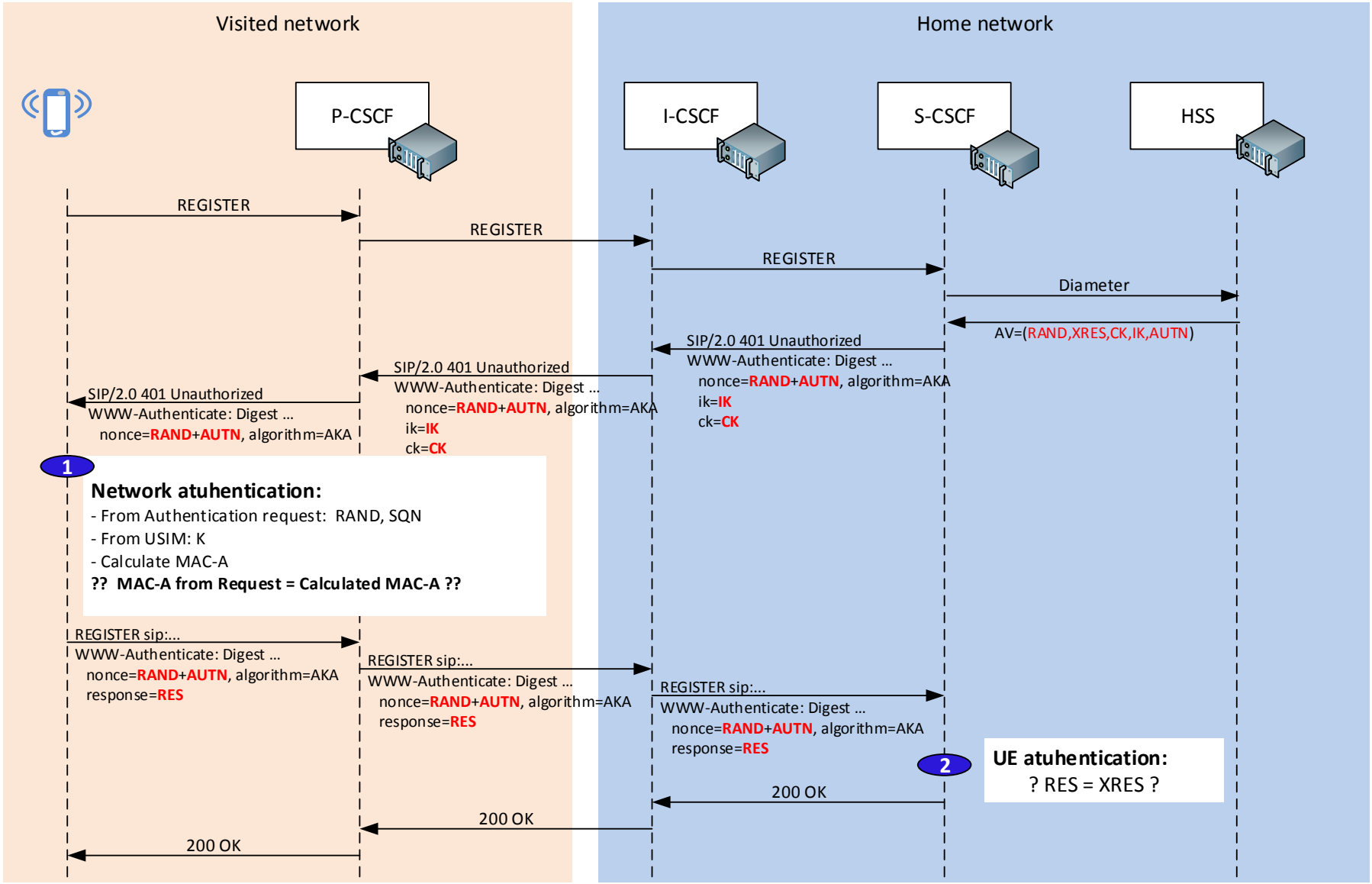
AKA (Authentication and Key Agtreemnet)



f1 až f5	jednocestné funkce
K	sdílené tajemství
RAND	náhodné číslo
SQN	Sequence number (udržuje síť i klient)
AK	Anonymizační klíč SEQ
AMF	Authentication Management Field (předem známý řetězec)
MAC-A	Jednorázové heslo pro autentizaci sítě
XRES	Jednorázové heslo pro autetnizaci klienta
CK	Cypher Key
IK	Integrity Key
KASAME	Základ pro derivaci šifrovacích klíčů



Konkrétně v IMS

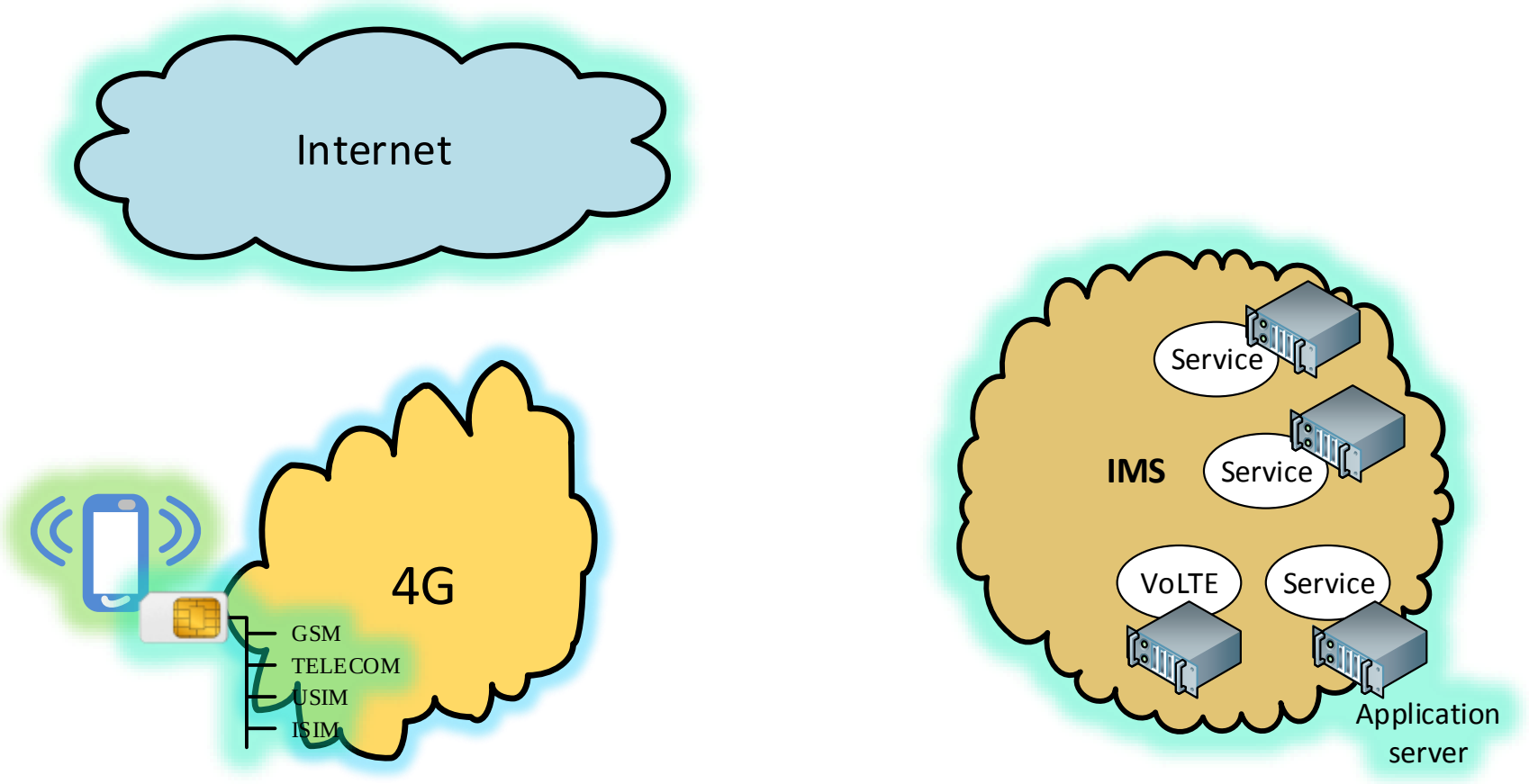


Důkaz AKA autentizací

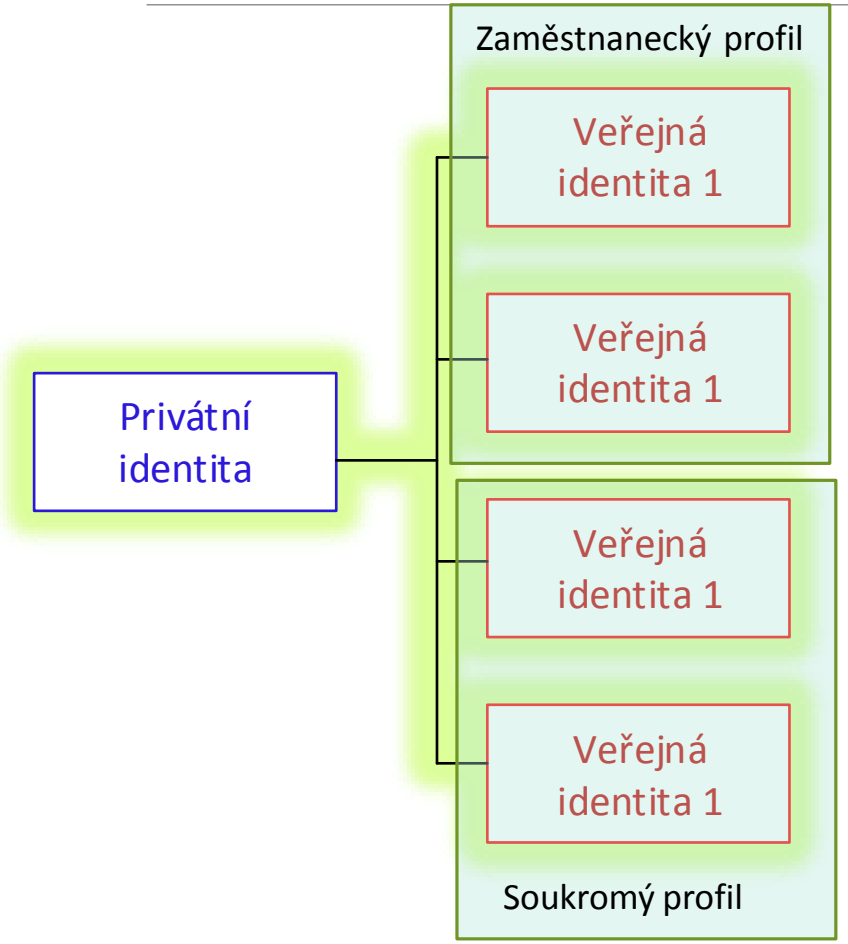
Operátor má ověřeno, že komunikujete z mobilu se SIM o daném tajemství

Operátor má ověřeno, že komunikuje ověřená veřejná identita

Internet x LTE (bezpečnostní zóny)



Privátní a veřejná identita



Privátní identita:

<imsi>@<mcc>.<mnc>.IMSI.3gppnetwork.org

Příklad pro MSIN=0123456789:
230010123456789@230.01.IMSI.3gppnetwork.org

Veřejná identita:

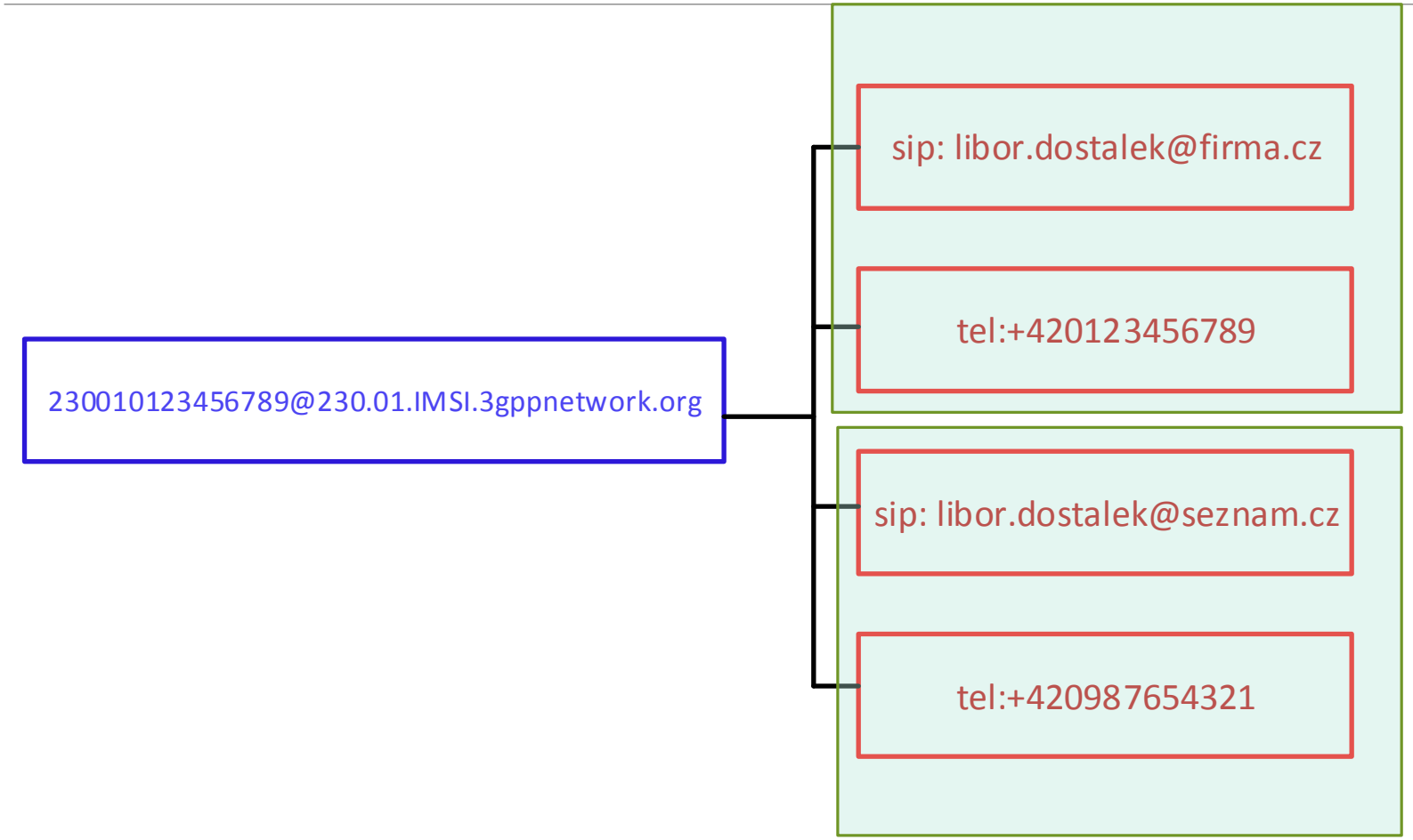
SIP URI nebo TEL URI

Příklady:
sip:Libor.Dostalek@example.com
tel:+420333333333

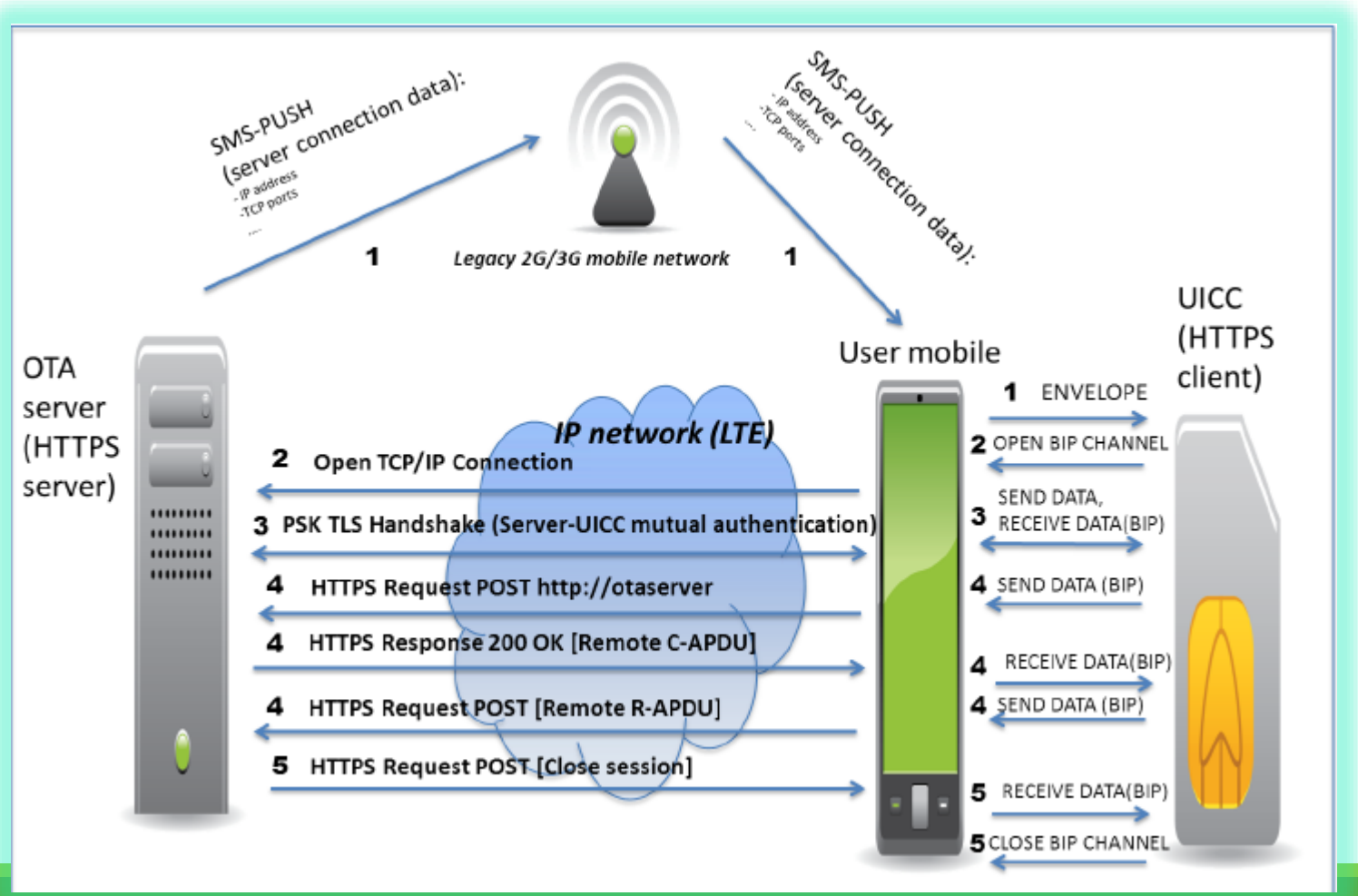
IMSI
(International Mobile Subscriber Identity)

- **MMC** (Mobile Country Code)
  - ČR: MCC=230
- **MNC** (Mobile Network Code)
  - MNC=01 (T-Mobile)
  - MNC=02 (O2)
  - MNC=03 (Vodafone)
- **MSIN** (Mobile Subscription Identification Number)

Privátní a veřejná identita



OTA (**Over The Air**)



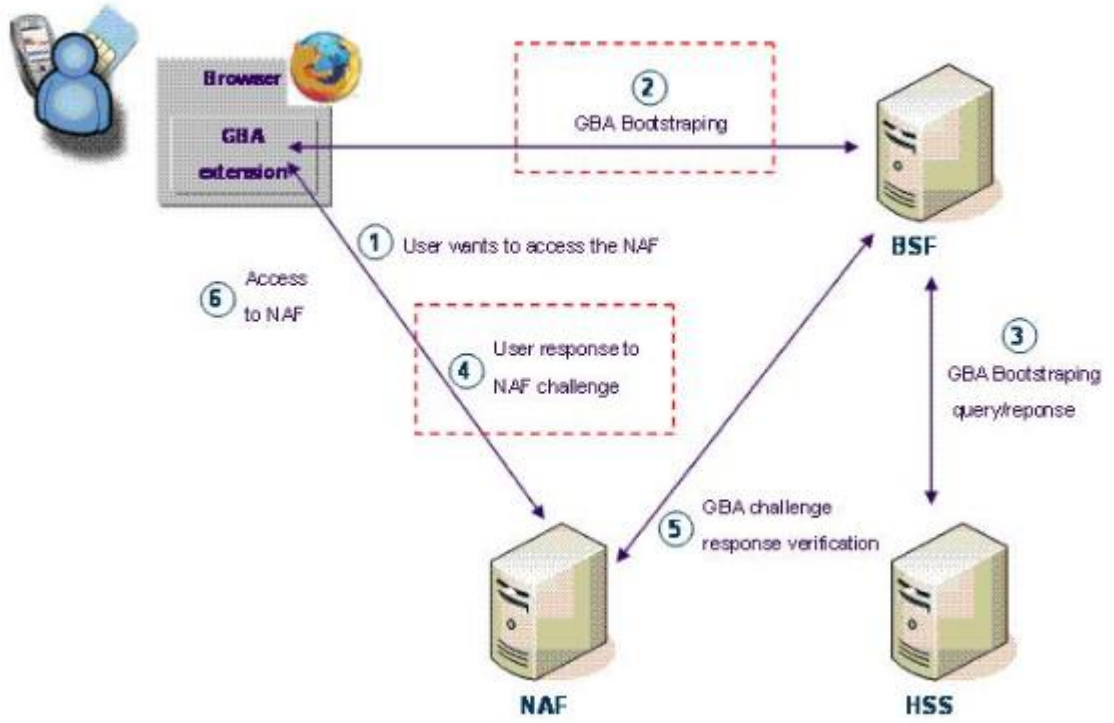
Aplikace (protokoly)

Aplikace na bázi SIP protokolu

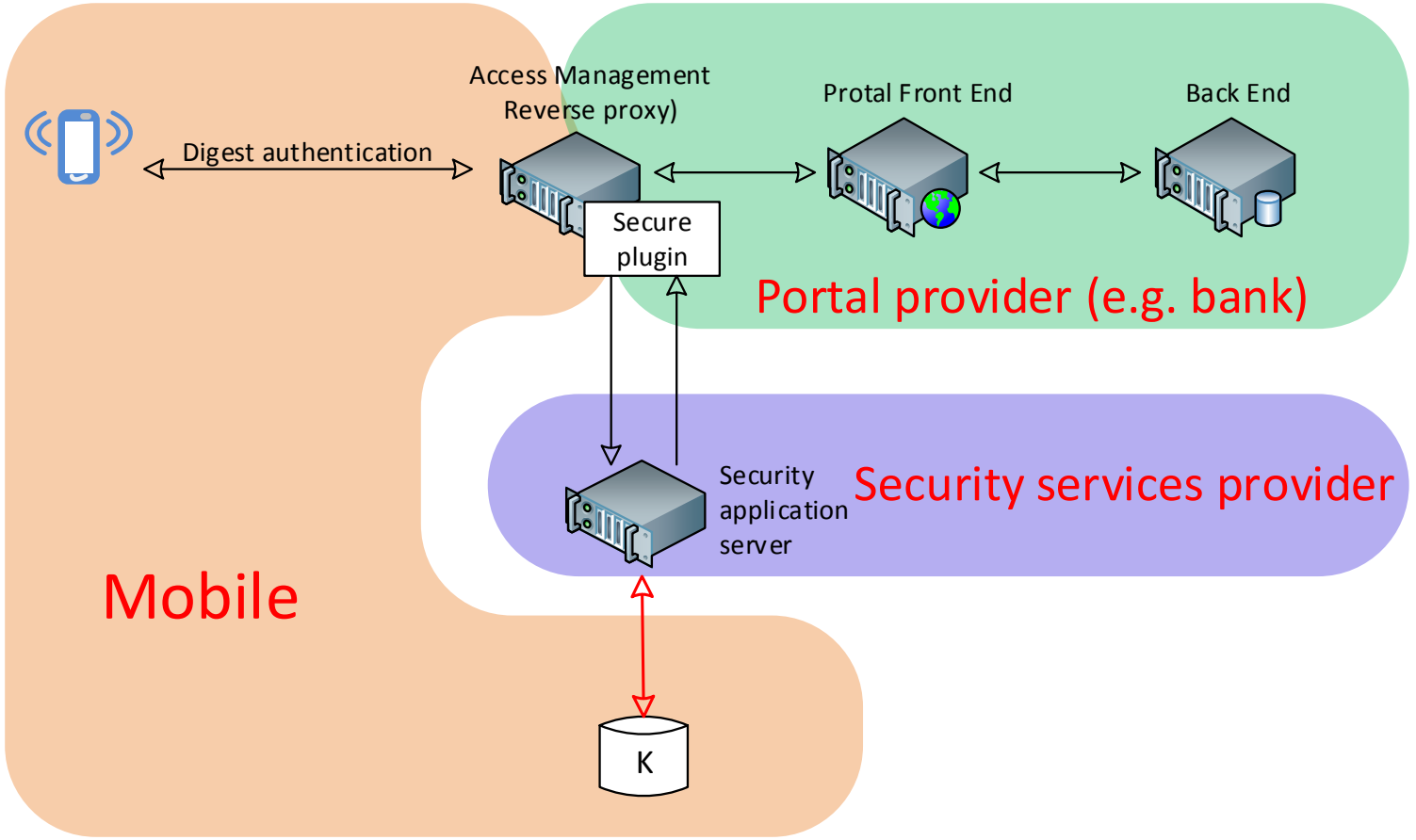
- Instatnt messaging, konference, prezentace …
- Multimediální aplikace
- TETRA/TETRApol

Aplikace na bázi HTTP protokolu

- Referenční bod Ut
- Generic Bootstrapping Architecture (GBA)



Sen


Access Management
Reverse proxy)
Protal Front End
Back End
Digest authentication
Secure
plugin
Portal provider (e.g. bank)
Security
application
server
Security services provider
Mobile
K

Praktické aplikace

Rozdíl mezi PC a mobilem (mobil bude něco jako PC s čipovou kartou – není běžné)

Elektronické jízdenky

Elektronické bankovnictví

… je to vás

Závěr

Problém rozšíření ISIM

Problém rozšíření veřejných identit

Ochota operátorů implementovat AKA autentizaci i pro HTTP aplikace

Proč by veřejná identita nemohla být mojeID???

Q & A

Děkuji za pozornost ☺