Secure Systems Group, Aalto University

Abu Shohel Ahmed, Aleksi Peltonen, Mohit Sethi, Tuomas Aura

Security Analysis of the Consumer Remote SIM Provisioning Protocol

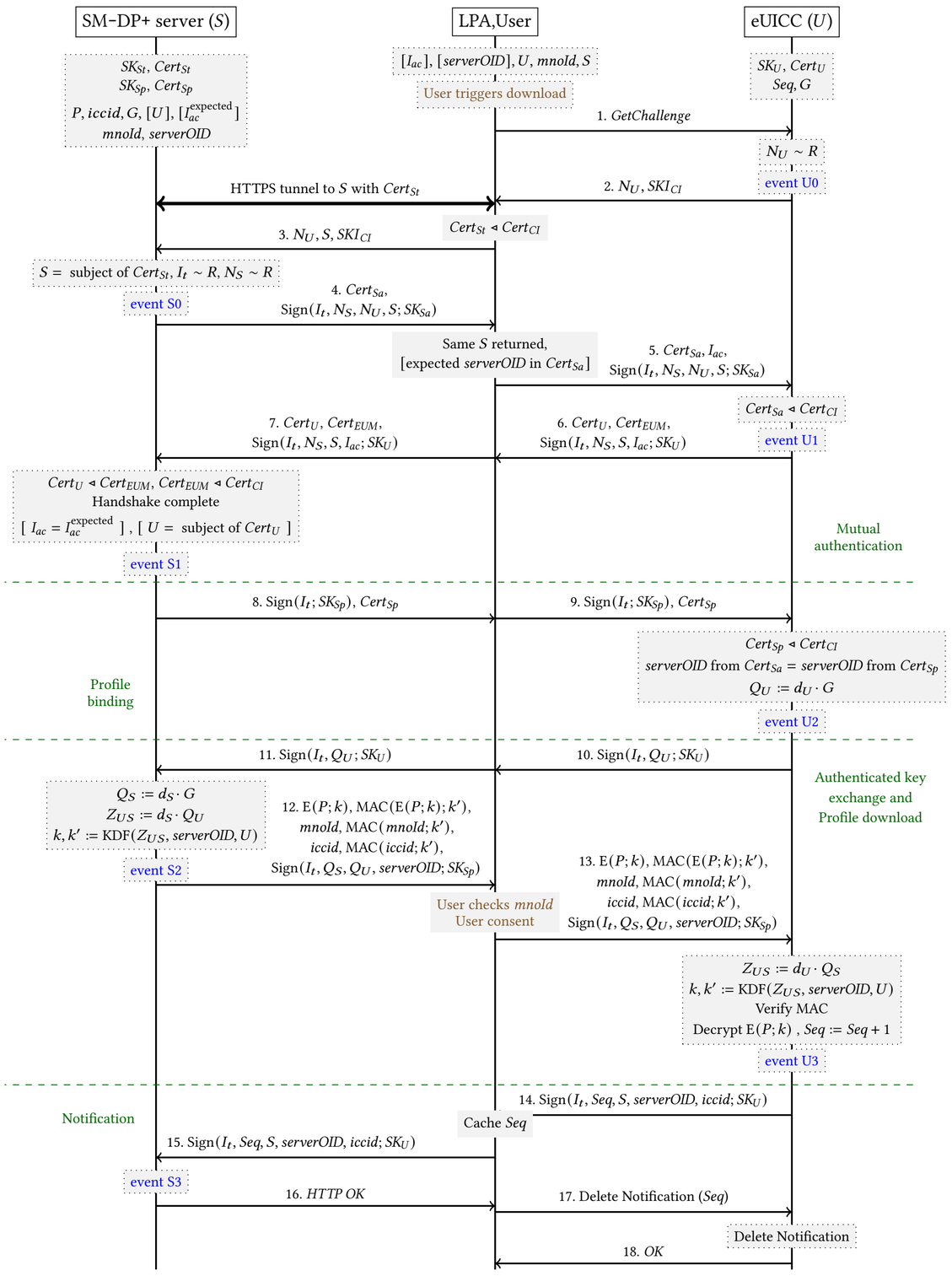

Figure 1: Common handshake and profile download

Remote SIM Provisioning

- The embedded SIM (eSIM) is a modern alternative to the physical SIM card
- It can be programmed with SIM profiles that contain the identifiers and credentials used to gain access to the operator's network
- Profiles are downloaded and installed with the Remote SIM Provisioning (RSP) protocol

Formal Verification

- We model the security of the RSP protocol with the ProVerif verification tool
- We analyze the protocol under partial compromise scenarios where one or more of the system components is not trustworthy
  - 11 authentication goals, 4 secrecy goals
  - 11 partial compromise scenarios
  - In total, 570 verification targets

Verification results

- Five major vulnerabilities discovered
- Based on our results, we provide practical recommendations for future development of the specification and implementation guidelines

Partial compromise scenario	Authentication goals											Secrecy goals			
	A	B	B′	C	D	E	F	G	I	J	K	W	X	Y	Z
1: —	✓	✓	O[1]	✓	✓	✓	✓	O[1]	✓	✓	O[1]	✓	✓	✓	✓
2: server	X[2]	X[c]	X[1,f]	X[2]	X[c]	X[2]	X[2]	X[1,f]	X[2]	X[2]	X[1,f]	✓	X[2]	✓	X[2]
3: eUICC	✓	X[4]	X[1,6]	O[d]	X[4]	O[e]	O[e]	X[1,4,6]	O[e]	O[e]	X[1,6]	X[4]	✓	X[4]	(✓)
4: LPA	✓	✓	X[1,9]	✓	✓	(✓)	(✓)	X[1,9]	✓	X[9]	X[1,9]	✓	✓	✓	✓
5: 2nd server	O[3]	O[c]	O[1]	O[3]	O[c]	O[3]	O[3]	O[1]	O[3]	O[3]	O[1]	✓	O[3]	✓	O[3]
6: 2nd eUICC	✓	O[5]	O[1]	O[d]	O[5]	✓	✓	O[1,5]	✓	✓	O[1]	O[5]	✓	O[5]	(✓)
7: 2nd MNO	✓	✓	O[1]	✓	✓	✓	✓	O[1]	✓	✓	O[1]	✓	✓	✓	✓
8: order as user	✓	✓	X[1,7]	✓	✓	✓	✓	X[1,7]	✓	✓	X[1,7]	✓	✓	✓	✓
10: code leaks	✓	✓	X[1,8]	✓	✓	✓	✓	X[1,8]	✓	✓	X[1,8]	✓	✓	✓	✓
11: code spoofed	✓	✓	X[1,b]	✓	✓	✓	✓	X[1,b]	✓	X[b]	X[1,b]	✓	✓	✓	✓

Attacker owns some eUICCs in all the scenarios 1–11. Client-side goals are gray. No security is expected in Scenarios 2-3.

Table 1: Results for the activation-code approach

Aalto University
School of Science

Contact: {abu.ahmed, aleksi.peltonen, mohit.sethi, tuomas.aura}@aalto.fi