Privacy Protected Subscriber Identification in 5G Network

Mohsin Khan, Kimmo Järvinen, and Valtteri Niemi

University of Helsinki, Department of Computer Science,
P.O. Box 68 (Gustaf Hällströmin katu 2b)
FI-00014 University of Helsinki
Finland
{mohsin.khan,valtteri.niemi}@helsinki.fi

Abstract.

1 Introduction

2 Authentication

Applicability of Existing Authentication Practices in 5G: TR 33.899 discusses that existing authentication practices wouldn't readily be applicable in 5G. Because of the complex business model and diversified end-user devices, the authentication requirements become wide and complex. Unlike the legacy networks, the user equipment identifiers are required to be authenticated in 5G. There will be UEs which would not have 3GPP subscription credentials. So, 5G needs authentication mechanism that can authenticate non-3GPP credentials. Based on different functionalities, the network will be splitted into different slices. A netwok slice can be operated by a 3rd party different from its HN. Authentication is required in between these 3rd parties and UE. UEs will connect through multiple access networks simultaneously and the access networks might or might not be trustes non-3GPP access networks, e.g. WiFi, Blutooth. There will be large number of IoT devices activated almost simultaneously. These bulk activations would create a huge pressure on a central authentication server if such a server's involvement is required in every authentication run. So, requirement of authentication at the edge of the network seems necessary. And like the other legacy networks, the user subscription authentication is also required in 5G. All these concerns are under discussion in 3GPP TR 33.899, where the contributors are discussing about developing authentication frameworks that would support all the different scenario. Potential solutions have also been proposed based on EPS-AKA, EAP-AKA, EAP-AKA' etc.

Mutual Authentication

1. In 3GPP TR 33.899, in Solution 1.11, it discusses about the high level security architecture. Here it proposes that the UE and the network (AUSF) should perform mutual authentication

2. in 3GPP TR 33.899, in Solution 2.6, it discusses the solution to key issue 2.2 and 3.1. Key issue 2.1 is the impact of the secret key leakage. And key issue 3.1 is the interception of radio interface keys sent between operator entities. To solve these issues, in solution 2.6, it proposes to bind a serving network public key into the derivation of the radio interface session keys. In the detail of the solution it requires mutual authentication in between UE and the network (CP-AU)
3. In Solution 2.9, it discusses the authentication framework based on EAP. It proposes two alternatives in both of the alternatives it uses mutual authentication in between the UE and the network.
4. Solution #2.12, it discusses to solve the following key issues:
   a) Authentication framework
   b) AS security during RRC idle mode
   c) Concealing permanent or long-term subscription identifier
   d) Concealing permanent or long-term equipment identifier

   This solution uses mutual authentication
5. Solution #1.11, it discusses about the high level security architecture.
6. Solution #2.9, it discusses the authentication framework based on EAP.
7. Solution #2.14 solving key issue 2.5 of Non-AKA based authentication is using mutual authentication
8. Solution #2.16: Mutual Authentication between Remote UE and Network over A Relay based on ID-based Credentials
9. Solution #2.17: Equipment identifier Authentication using the (IMEI, Device Certificate) binding
10. Key issue #3.10: Trusted non-3GPP access
11. Solution #3.1: Including a key exchange protocol into the derivation of the radio interface session keys
12. Solution #3.3: Security Context Management for UE with Multiple Access Technologies
13. Solution #3.7: Algorithms Negotiation Procedure
14. Solution #4.1: Network signs selected signalling messages
15. Solution #8.2: UE Authentication only by AUSF
16. Solution #8.4: UE Authentication by NSI
17. Solution #8.7: Security architecture for network slice
18. Solution #8.9: Security mechanism differentiation for network slices
19. Key Issue #9.1: Mutual authentication of remote UE and network over a relay
20. Solution #12.1: Remote credential provisioning Add Headless IoT device to existing users MNO subscription
21. Solution #12.3: Secure Mechanism to Achieve Remote Credential Provisioning for IoT devices
22. Solution #12.4 Authentication Procedure for credential provisioning

Effective use of mutual authentication to protect 5G Networks Against Unauthorized Access:

Effective use of mutual authentication to protect End-user Device against attaching to malicious network components:

Perceived Limitations and Drawbacks of mutual authentication:

What are the specific considerations applicable to 5G:

Circumstances when mutual authentication is essential:

Circumstances when Mututal Authentication would not be benefical:

Other Authentication Methodologies:

Authentication Challenges in IoT Networks:

Authentication in IoT:

Identity Credentialing and Access Management:

References