# (U)SIM based PCP Authentication
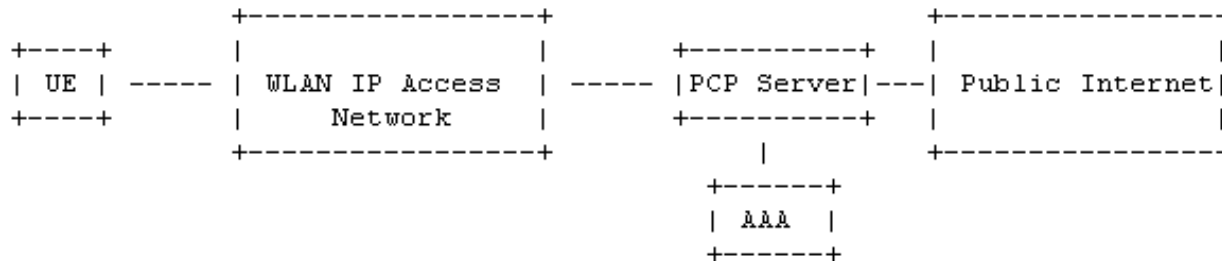
## draft-chen-pcp-authentication-sim-00
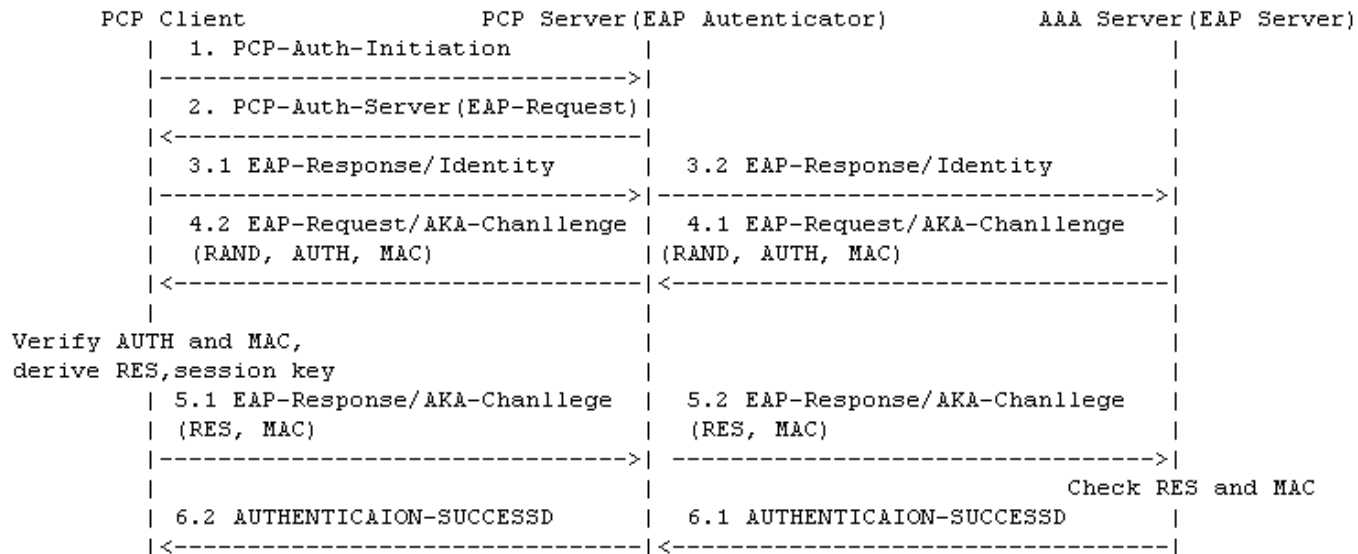
Gang Chen

China Mobile

# Overview

- The document details PCP authentication considerations based on (U)SIM support.

- With (U)SIM support, PCP authentication could leverage the credentials stored in (U)SIM

- The authentication procedures in EAP and GBA framework have been described

# EAP Framework

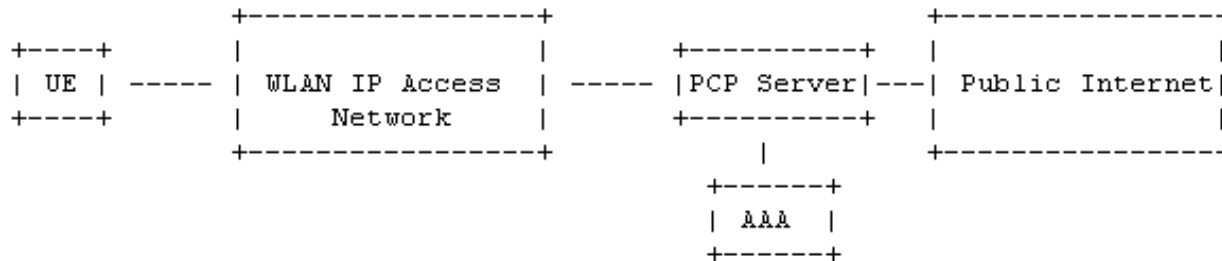*The scenario: WLAN Access with EAP Support*

```
                             +----------------+                   +---------------+
     +----+                  |                |    +----------+   |               |
     | UE | ----- | WLAN IP Access |  ----- |PCP Server|---| Public Internet|
     +----+                  |     Network    |    +----------+   |               |
                             |                |         |         +---------------+
                             +----------------+      +------+
                                                     | AAA  |
                                                     +------+
```

*PCP authentication process with EAP-AKA/EAP-AKA'*

```
PCP Client                        PCP Server(EAP Autenticator)        AAA Server(EAP Server)
     |    1. PCP-Auth-Initiation      |                                |
     |------------------------------->|                                |
     |    2. PCP-Auth-Server(EAP-Request)|                             |
     |<------------------------------|                                 |
     |    3.1 EAP-Response/Identity    |   3.2 EAP-Response/Identity    |
     |------------------------------->|------------------------------->|
     |    4.2 EAP-Request/AKA-Chanllenge |  4.1 EAP-Request/AKA-Chanllenge |
     |    (RAND, AUTH, MAC)            |   (RAND, AUTH, MAC)            |
     |<------------------------------|<-------------------------------|
     |                                |                                |
Verify AUTH and MAC,                 |                                |
derive RES,session key               |                                |
     |    5.1 EAP-Response/AKA-Chanllege |  5.2 EAP-Response/AKA-Chanllege |
     |    (RES, MAC)                   |   (RES, MAC)                   |
     |------------------------------->| ------------------------------>|
     |                                |                     Check RES and MAC
     |    6.2 AUTHENTICAION-SUCCESSD   |   6.1 AUTHENTICAION-SUCCESSD   |
     |<------------------------------|<-------------------------------|
```

3

# GBA Framework

*The scenario: 3GPP Access with GBA Support*

```
                    +-----------------+                    +-----------------+
+----+              |                 |                    |                 |
| UE | ----- | WLAN IP Access  | ----- |PCP Server|---| Public Internet|
+----+              |    Network      |        +----------+  |                 |
                    +-----------------+                    +-----------------+
                                                 |
                                           +------+
                                           | AAA  |
                                           +------+
```

*PCP authentication process in the GBA*

```
PCP Client                        PCP Server                 BSF            HSS
   |    1. PCP-Auth-Initiation         |                      |              |
   |---------------------------------->|                      |              |
   |2. PCP-Auth-Server(bootstrapping)  |                      |              |
   |<---------------------------------|                      |              |
   |                  3.Request(User Identity)                |  4.Retrieve AV |
   |-------------------------------------------------------->|<--------------->|
   |                5.401 Unauthorized WWW-Authenticat        |              |
   |                    Digest (RAND, AUTH)                   |              |
   |<-------------------------------------------------------|              |
   |            6.Request Authorization: Digest (RES is used) |              |
   |-------------------------------------------------------->|              |
   |                                   |        Server checks the given Digest |
   |                                   |              and drive Ks           |
   |                7.200 OK, B-TID, Key lifetime             |              |
   |<-------------------------------------------------------|              |
   |    8. PCP-Auth-Request    |    9. Authentication Request |              |
   |       (B-TID)             |       (B-TID)                |              |
   |-------------------------->|---------------------------->|              |
   |                           |    10.Authentication Answer  |              |
   | 11.AUTHENTICAION-SUCCESSD |    (Ks, Key lifetime)        |              |
   |<-------------------------|<----------------------------|              |
```

# Proposals

*One result code is required:*

*TBD BOOTSTRAPPING-INITIATION*

*B-TID option:*

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Option Code   |   Reserved    |        Option-Length          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                              B-TID                             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```
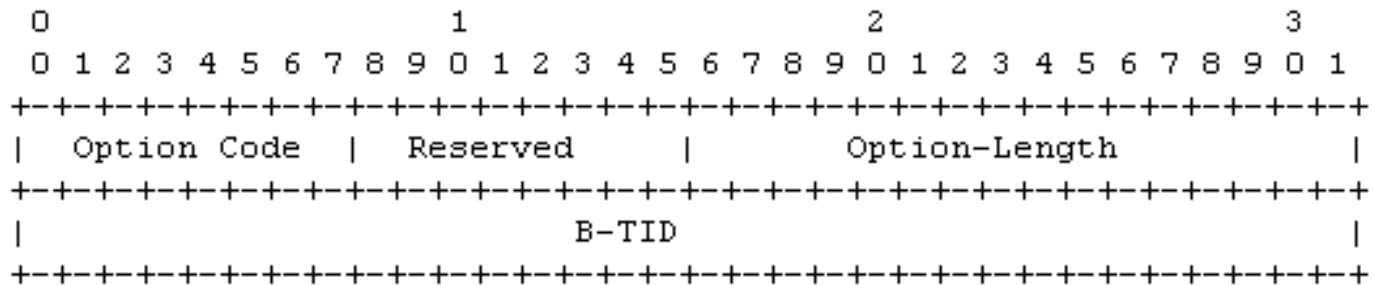
# Comments

- Regarding the GBA framework, what is the need for this mechanism when EAP-SIM can be used ?
  - EAP is out of 3GPP-access security architecture [TS 33.401], which describes the security framework of 3GPP access
  - EAP is normally used at non-3GPP access [TS 33.402]
- It deviates from REQ-6 of fate sharing http://tools.ietf.org/html/draft-reddy-pcp-auth-req-04

  REQ-6: To ease troubleshooting and ensure fate sharing, PCP authentication and PCP messages MUST be multiplexed over the same port.

  - There is no request to use different port for PCP authentication and PCP message. This document is compliant with draft-ietf-pcp-authentication

# What's Next?

- Is it valid statement to wg?
- Should we continue the work within wg?

# Comments/Questions?