RFC 5448bis
EAP-AKA' Update

Jari Arkko, Vesa Lehtovirta, Vesa Torvinen
Ericsson Research
(+ RFC 5448 author Pasi Eronen)

draft-ietf-emu-rfc5448bis-03.txt

http://www.arkko.com/ietf/eap/
draft-ietf-emu-rfc5448bis-from-rfc5448.diff.html

Reminders — What was this about, again?

EAP-AKA (RFC 4187) & revised EAP-AKA’ (RFC 5448)

These have been very widely implemented, somewhat widely used for WLAN access authentication

- 2/3/4G access uses native SIM card and AKA, not EAP
- 5G access authentication introduces the use of EAP for 5G access

What we thought we needed to do

- Identifier usage is special for 5G
- Network name bindings changed for 5G
- Definition of exported parameters is required by RFC 5247

…

What we actually needed to do

- Identifier usage is special for 5G
- Network name bindings changed for 5G
- Definition of exported parameters is required by RFC 5247

…

- Security, privacy, and pervasive monitoring considerations
- Document vulnerabilities
- Requirements on the generation of pseudonym and fast re-authentication identifiers
- References need updates

Recent Updates in -02 & -03

Status:

- Believed to be in sync with 3GPP specs

5G related:

- Specification of peer identity usage in EAP-AKA’
- Specified the format of 5G-identifiers when they are used within EAP-AKA’
- Clarified when 5G- related procedures apply

General:

- Requirements on the generation of pseudonym and fast re-authentication identifiers
- Reference updates

Security considerations:

- Defined privacy and pervasive surveillance considerations,
- A summary of vulnerabilities brought up in the context of AKA or EAP-AKA’
- Specified what Peer-Id value is exported when no AT_IDENTITY is exchanged within EAP-AKA’

Identifiers

- Previously this was clear for all cases — use the name that was sent; clarity is important since identifiers are used in KDF
- With 5G, this changes for two reasons:
  - The EAP session is inside the native 5G network attachment procedure which does not use EAP identity request & response
  - In 5G, there are two distinct identifiers for users, the permanent, private one (SUPI) which is never sent, and a temporary one that can be sent over the wire (SUCI)

    Use SUPI for key generation; SUCI for all other cases

Identifiers — Identity Req/Resp

When the EAP peer is connecting to a 5G access network and uses the 5G Non-Access Stratum (NAS) protocol [TS-3GPP.24.501], the EAP server is in a 5G network. The EAP identity exchanges are generally not used in this case, as the identity is already made available on previous link layer exchanges.

In this situation, the EAP server SHOULD NOT request an additional identity from the peer.

Identifiers — Unexpected Identity Req

If the peer for some reason receives EAP-Request/Identity
or EAP-Request/AKA-Identity messages:

EAP-Request/AKA-Identity with AT_PERMANENT_REQ

> For privacy reasons, the peer should follow a "conservative" policy and **terminate the authentication exchange rather than risk revealing its permanent identity.**
>
> The peer SHOULD respond with EAP-Response/AKA-Client-Error with the client error code 0, "unable to process packet".

…

Identifiers — Key Generation

If the AT_KDF_INPUT parameter contains the prefix "5G:", the AT_KDF parameter has the value 1, and this authentication is not a fast re-authentication, **then the peer identity used in the key derivation MUST be the 5G SUPI** for the peer.

Identifiers — Format

A SUPI is either an IMSI or a Network Access Identifier [RFC4282]. The **SUPI MUST be as specified in [23.003]** Section 28.7.2. The **SUCI MUST be as specified in [23.003]** Section 28.7.3.

Example. For IMSI 234150999999999 (MCC = 234, MNC = 15), the NAI format for the SUPI takes the form:

234150999999999@nai.5gc.mnc015.mcc234.3gppnetwork.org

For the “Profile <A> protection scheme” the SUCI takes the form:

type0.rid678.schid1.hnkey27.ecckey<ECC ephemeral public key id>.
cip<encryption of 0999999999>.mac<MAC tag value>@nai.5gc.
mnc015.mcc234.3gppnetwork.org

Network Name Bindings

Network Name

This field contains the network name of the access network for which the authentication is being performed.

The value is **sent as specified in [TS-3GPP.24.302] for non-3GPP access networks, and as specified in [TS-3GPP.33.501] for 5G access networks.**

Exported Parameters

```
Session-Id = 50 || RAND || AUTN
Session-Id = 50 || NONCE_S || MAC   (for fast re-auth)
Peer-Id = contents of identity field from AT_IDENTITY or
          contents of identity field from EAP Identity Response or
          empty string
Server-Id = empty string
```

Pseudonym/Fast re-auth Id Generation

The p**seudonym usernames and fast re-authentication identities MUST be generated in a cryptographically secure way** so that that it is computationally infeasible for at attacker to differentiate two identities belonging to the same user from two identities belonging to different users. This can be achieved, for instance, by using random or pseudo-random identifiers such as random byte strings or ciphertexts.

Note that the pseudonym and fast re-authentication usernames also **MUST NOT include substrings that can be used to relate the username to a particular entity or a particular permanent identity.**

…

Privacy Considerations

Entirely new Section 7.1:

- Basic implications of using different identifier types
- Sets limits on using pseudonyms in 5G (would lead to a privacy compromise, if same pseudonym were used multiple times)
- Discusses the implications of using different SUCI protection profiles (the null profile does not provide any privacy!)
- Domain or operator typically visible even if subscriber identity is hidden

Pervasive Surveillance Considerations

Entirely new Section 7.3:

- Discusses the attacks reported in 2015

  All protocols are of course vulnerable to compromise of the primary key material

- Discusses SIM-card specific manufacturing and provisioning practises that may help address some of these attacks

- Also suggests that some form of perfect forward secrecy protection may also be useful (either in form of tunnels that provide PFS or AKA PFS)

Discovered Vulnerabilities

Entirely new Section 7.2

No known attacks that violate the primary properties of the AKA exchange under the original assumptions. However,

- Key material leakage obviously leads to breakage, e.g., the “SIM Heist” attacks reported in 2015
- Protocol participants may also misbehave, e.g., visited networks may allow authentication to succeed, but then use session keys to pretend they are the node (e.g., to send traffic on behalf of the node).
- Not relevant for EAP-AKA’, but the use of AKA authentication without keys leads to MITM vulnerabilities (RFC 3310 => 4169).
- …

Next Steps

- Give us feedback & discuss!
- Ongoing discussion with 3GPP (including asking them to reference this draft rather the now out of date RFC…)
- We think we understand all the interdependencies and believe this version of draft is in sync with current 3GPP Release 15 specifications
- WGLC now would align nicely with upcoming 3GPP discussions and finalization of R15