

Title: LS on Security aspects of ECIES for concealing IMSI or SUPI

Response to:

Release: 15

Work Item: 5GS_Ph1-SEC

Source: SA WG3

To: ETSI SAGE

Cc:

Contact Person:

Name: Pasi Saarinen

E-mail Address: pasi.saarinen@ericsson.com

Send any reply LS to: 3GPP Liaisons Coordinator, <mailto:3GPPLiaison@etsi.org>

Attachments: S3-171788 (SUCI -- ECIES scheme normative Annex)

1. Overall Description:

1.1 IMSI and SUPI

Up to the fourth generation of mobile networks (called the LTE or popularly the 4G) the subscriber's long-term identifier was called the IMSI (International Mobile Subscriber Identity). Starting from the next generation of mobile networks (called the 5G), a new and general term called the SUPI (Subscription Permanent Identifier) will be used to denote the globally unique 5G subscription permanent identifier.

1.2 Privacy issue and corresponding solution using asymmetric cryptography

In the context of the 5G networks, the 3GPP SA WG3 has been actively working to enhance subscriber's privacy. The reason in doing so is that better privacy will certainly benefit subscribers, operators, equipment vendors and application service providers alike.

One of the most pressing privacy concerns in the 5G networks relates to untraceability of IMSI or SUPI. And the biggest threat to it is arguably the so called "IMSI catcher" which is the collective name given to devices used to eavesdrop and track subscribers. Over the past years, these "IMSI catchers" have received much attention in media and hacker conferences. Some examples are following: [CBC News](#) in Canada, [Aftenposten](#) in Norway, [The Washington Free Beacon](#) and [Vice News](#) in the US, [DEF CON 24](#) and [Black Hat EU 2015](#).

Towards solving this, the SA WG3 has made an important agreement to conceal IMSI or SUPI over-the-air in 5G. This is arguably one of the major privacy enhancements in 5G compared to LTE. The said agreement is specifically to use asymmetric cryptography based on the home network's public key.

SA3 would like the input from ETSI SAGE on which asymmetric encryption scheme to use. One candidate that has been discussed in SA3 is ECIES as described below. When considering encryption schemes, please note the following potential requirements.

- Fast computation on low end devices such as IoT devices.
- Short length of transferred data including the encrypted SUPI and other required parameters.
- Possible limitations on the size of the home network public key

1.3 Proposal to use ECIES (Elliptic Curve Integrated Encryption Scheme)

In order to implement the said agreement of using asymmetric cryptography, there is a need of preferably more than one, but at least one, standardized public key encryption schemes that have properties suitable for the particular use case of concealing IMSI or SUPI.

Consequently, the attached contribution (S3-171788) has been presented in the 3GPP SA WG3. The contribution proposes a well-known and popular scheme called the ECIES (Elliptic Curve Integrated Encryption Scheme). The ECIES has been suggested to be particularly suitable for mobile devices because of fast computation time (meaning longer battery time) and short key size (meaning less radio resource).

In this regard, 3GPP SA WG3 would like to request ETSI SAGE to kindly review the proposal in the attached contribution (S3-171788) and advice on the security aspects. Some Microsoft-WORD comments have been put in the contribution for highlighting important aspects.

2. Actions:

To ETSI SAGE group.

ACTION: SA WG3 kindly asks ETSI SAGE to take above description into account and give feedback on the choice of public key encryption scheme and the security and efficiency aspects of the ECIES scheme described in the attachment.

3. Date of Next TSG-SA WG3 Meetings:

SA3#88Bis (Adhoc on 5G)	9-13 October 2017	Singapore
SA3#89	27 November - 1 December	Reno, Nevada (US)