DESS 11_02

Liaison Statement reply to 3GPP S3-172175: DESS Update and Requirements for Securing Inter-PLMN Signalling Interfaces in 5G

Meeting Information	
Meeting Name and Number	DESS#11
Meeting Date	16 Nov 2017
Meeting Location	Conference call
Document Information	
Document Author	Ewout Pronk (KPN)
Additional Contributors	Sven Lachmund (Deutsche Telekom), David Maxwell (GSMA)
Document Creation Date	3 Nov 2017
Document Status	This document is for information only
Security Classification	Non-confidential
Document Summary	
GSMA LS updating 3GPP SA3 on its activity on securing Diameter interfaces in reply to S3-172175	

Version History (to be completed by editor)		
Date	Version	Author / Comments
3 Nov 2017	1	Ewout Pronk, KPN
9 Nov 2017	2	Ewout Pronk, KPN
15 Nov 2017	3	Ewout Pronk, KPN
17 Nov 2017	4	Ewout Pronk, KPN and Sven Lachmund, DT
17 Nov 2017	5	David Maxwell, GSMA

© GSMA © 2017. The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice. This document has been classified according to the GSMA Document Confidentiality Policy. GSMA meetings are conducted in full compliance with the GSMA Antitrust Policy.

Liaison Statement

Liaison Statement Title:	DESS Update and Requirements for Securing Inter-PLMN Signalling Interfaces in 5G
Security Classification:	Non-confidential

Source Meeting Information		
Meeting Number	Meeting Date	Meeting Location
DESS#11	16 Nov 2017	Conference call

Document Details		
Document Number:	Creation Date:	Document Author:
DESS#11 Doc 02	3 Nov 2017	Ewout Pronk, KPN
Originating GSMA Source:	Deadline for response:	Liaison Statement Contact
FASG DESS	N/A	David Maxwell, dmaxwell@gsma.com

Action Required by Recipient	
External Recipients:	To: 3GPP SA3 Cc: 3GPP SA1, 3GPP CT3, 3GPP CT4
Internal Recipients:	Cc: FSAG, RIFS, PACKET

1 Status update on Diameter End-to-end Security Subgroup (DESS)

In reply to LS S3-172175 GSMA FASG DESS would like to update 3GPP SA3 on its progress and would like to propose further actions from 3GPP SA3.

GSMA FASG DESS appreciates the 5G security work and the start of the normative work in TS 33.501.

As a starting point GSMA FASG DESS has analysed the IETF work on Diameter security. Although the IETF work indeed does provide a good starting point, it does not provide an exact solution for the problem that GSMA FASG DESS is facing. Instead, it is more a high level approach on how to represent digital signatures and encrypted AVPs in a JSON format. It does not describe protocols to be used in detail, or how to counter replay attacks. The fact that the IETF work relies on JSON objects can be seen as a benefit, at least for 5G.

GSMA FASG DESS has prepared a working document that provides requirements and solution directions to secure the inter-PLMN signalling interfaces for both LTE and 5G. The solution directions consist of both confidentiality and integrity measures that GSMA FASG DESS would like to see being deployed on the inter-PLMN signalling interfaces.

GSMA FSAG DESS initially had a distinct focus on LTE but shifted the priority to 5G when it learned that the 5G is likely to be built on a service-based architecture (SBA) with the usage of HTTP2 on top of TCP, represented in JSON objects.

Since the Diameter protocol may not be the intended protocol for 5G core networks, the document provided is now called “IPX Network End-to End Security Guidelines”, but the GSMA group name (i.e. Diameter End-to-End Security subgroup) has not changed.

A critical requirement is that IPX providers must also in 5G be able to change fields of a message in transit as they do in LTE. For LTE this includes non-3GPP specific AVPs such as the “Origin-Realm” and “Origin-Host” (for instance when LTE operators use lower case letters instead of capitals in the realm, or in case of the roaming hubbing service as described in GSMA permanent reference document IR.80). There are also numerous changes to 3GPP specific AVPs (mainly subscriber settings), for example deletion of the “STN-SR” AVP to prevent a VoLTE to 2G/3G handover. The non-3GPP AVPs are usually changed as a service to the LTE operator, when the LTE operator is not able to make those changes themselves.

The ideal solution shall be capable of handling these modifications, and it should also allow the recipient of the message to determine if these changes were legitimate and who performed them. The earlier mentioned IETF work does not describe a solution for this problem. Section 5.1 of the attached “IPX Network End-to End Security Guidelines” document describes a proposal (the *Extended Signature Scheme*) to fulfil that requirement. It describes a way for IPX providers to authoritatively change a limited set of fields, even though those fields are integrity protected by the sender. The Extended Signature Scheme will provide the receiver with proof that the message has not changed between the sender and the receiver (apart from the fields authoritatively changed by the IPX provider(s)).

To provide confidentiality, GSMA FASG DESS proposes an encryption container structure (the *Extended Confidentiality Scheme*) as described in section 5.2 of the attached document. It supports the flexibility to encrypt fields of a message, even if those fields are part of a grouped or layered structure, as it is the case with grouped AVPs in Diameter. Also here, the IETF work does not describe how to fulfil this requirement.

GSMA FASG DESS requires integrity protection and authenticity of all inter-PLMN signalling messages on all respective interfaces and confidentiality measures for authentication vectors (e.g. XRES, RAND) to be mandatory to implement *and* mandatory to use. Operators may still decide to encrypt additional fields end-to-end. That particular option is mandatory to implement but not mandatory to use.

GSMA FASG DESS is still drafting the strategy for LTE and will update 3GPP SA3 at a later stage on the outcome and potential actions for 3GPP SA3. An option for LTE could be to take similar measures as required for 5G but than in an optional fashion. Only new interfaces of Diameter messages may then be mandatorily equipped with the proposed security measures for 5G. GSMA NG SIGNAL is currently working on a white paper for SMS evolution that might result in new Diameter messages that only make sense if authenticity is guaranteed.

2 Action required

GSMA FASG DESS would like to ask 3GPP SA3 to apply a “security-by-design” methodology considering the requirements provided in section 3 below in order to secure the inter-PLMN interfaces between service providers for the 5G network. This means that the measures mentioned in the solution directions (Extended Signature Scheme and Extended Confidentiality Scheme) with the corresponding requirements mentioned in section 1 are mandatory to implement and mandatory to use.

GSMA FASG DESS would also appreciate feedback on this LS and on the attached document “IPX Network End-to-End Security Guidelines”.

3 Requirements

GSMA FASG DESS has the following requirements to secure the 5G inter-PLMN signalling interfaces:

1. The solution must:

    a) provide mandatory to implement and mandatory to use authentication *and* integrity protection on a per field basis as described in chapter 1

        i. including support of intermediate adding of fields by IPX providers
        ii. including support of intermediate modification and deletion of non-encrypted fields by IPX providers

    b) provide mandatory to implement and mandatory to use confidentiality protection of authentication vectors
    c) provide mandatory to implement and optional to use confidentiality protection on other fields

d) provide mandatory to implement and mandatory to use protection against replay attacks
e) be operationally feasible e.g. acceptable procedure for key management
f) include (at a minimum) the 5G successor of the Diameter 3GPP interfaces described as Network-Network interfaces by IR.88 (e.g. S6a)

2. The solution should:

a) impact a minimal amount of network elements
b) Have an acceptable performance and overhead
c) Support the ability to delegate security functionality to another entity.