**3GPP TSG-SA3 Meeting #101e *S3-203528***

**e-meeting, 9 – 20 November 2020** revision of S3-203072

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **DRAFT** | **rev** | **1** | **Current version:** | **16.3.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | IMS SCAS: living doc for the threats |
|  |  |
| ***Source to WG:*** | Huawei, Hisilicon |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_IMS |  | ***Date:*** | 2020.10.23 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | 17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | Add assets and threat description to TR 33.926 in support of IMS SCAS work.S3-101852: adding the asset of P-CSCF/S-CSCF.S3-201853: Adding threats related to de-registration during the authentication.S3-202078: Adding threats related to high-priority algorithm selection in the P-CSCF.S3-202154: Adding threats related to bidding down on security association set-upS3-201859: Adding threats related to unprotected register messageS3-203530: Adding threats related to IMS signalling transportS3-203532: adding threats related to Resynchronization failureS3-203541 pCR Threat of bidding down attack on security association |
|  |  |
| ***Summary of change:*** | Add assets and threats related to P-CSCF/S-CSCF  |
|  |  |
| ***Consequences if not approved:*** | No reference of critical assets and threats for IMS SCAS. |
|  |  |
| ***Clauses affected:*** | 2, Annex X(new). |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 1st changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TR 33.916: "Security Assurance Methodology for 3GPP network products classes".

[3] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[4] 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolution (LTE) RAN/3GPP System Architecture Evolution (SAE)".

[5] 3GPP TS 33.116: "Security Assurance Specification for MME network product class".

[6] 3GPP TS 33.511: "5G Security Assurance Specification (SCAS); NR Node B (gNB)"

[7] 3GPP TS 38.300 v15: "NR; NR and NR-RAN Overall Description; Stage 2".

[8] 3GPP TS 23.501 v15: "System Architecture for 5G System; Stage 2".

[9] 3GPP TS 38.323 v15: "NR; Packet Data Convergence Protocol (PDCP) specification".

[10] 3GPP TS 38.322 v15: "NR; Radio Link Control (RLC) protocol specification".

[11] 3GPP TS 33.250: "Security assurance specification for the PGW network product class".

[12] 3GPP TS 33.516: "5G Security Assurance Specification (SCAS) for the AUSF network product class".

[13] 3GPP TS 33.517: "5G Security Assurance Specification (SCAS) for the Security Edge Protection Proxy (SEPP) network product class".

[14] 3GPP TS 33.501 Release 15: "Security architecture and procedures for 5G system".

[15] 3GPP TS 33.518: "5G Security Assurance Specification (SCAS) for the Network Repository Function (NRF) network product class".

[16] 3GPP TS 33.519: "5G Security Assurance Specification (SCAS) for the Network Exposure Function (NEF) network product class".

[17] 3GPP TS 33.117: "Catalogue of general security assurance requirements".

[18] 3GPP TS 33.513: "5G Security Assurance Specification (SCAS); User Plane Function (UPF)".

[19] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN);Overall description;Stage 2."

[20] 3GPP TS 33.216: "Security Assurance Specification (SCAS) for the evolved Node B (eNB) network product class."

[21] 3GPP TS 33.514: "5G Security Assurance Specification (SCAS) for the Unified Data Management (UDM) network product class".

[22] 3GPP TS 33.512: "5G Security Assurance Specification (SCAS); Access and Mobility management Function (AMF)".

[XX] 3GPP TS 33.226: "Security assurance for IP Multimedia Subsystem (IMS)".

[YY] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the 1st changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the 2nd changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Annex X (normative):
Aspects specific to the IMS network product classes

# X.1 Network product class description for the IMS

## X.1.1 Introduction

This Annex covers the aspects specific to the IMS network products with specific threats.

## X.1.2 Minimum set of functions defining the IMS network product classes

As part of the IMS network products, it is expected that the IMS network product classes (e.g. P-CSCF) contains IMS network product classes application, a set of running processes (typically more than one) executing the software package for the IMS network product functions and OAM functions that are specific to the IMS network product model. Functionalities specific to the IMS network product introduce additional threats and/or critical assets as described below. Related security requirements and test cases have been captured in TS 33.226 [XX].

Note:For the purposes of the present Annex, this common set is defined to be the list of functions contained in clause 4.0 in 3GPP TS 23.228 [YY].

# X.2 Assets and threats specific to the P-CSCF

## X.2.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the P-CSCF to be protected are:

- P-CSCF Application;

- IMS signalling;

- Security data, i.e. cryptographic materials for Gm, Mw, Mx, and Iq interfaces

- The interfaces of the P-CSCF to be protected and which are within SECAM scope:

- Gm interface between the P-CSCF and UE

- Mw interface between the P-CSCF and the C-CSCF/I-CSCF

- Mx interface between the P-CSCF and IBCF

- Iq interface between the P-CSCF and IMS AGW

- Console interface, for local access: local interface on the P-CSCF

- OAM interface, for remote access: interface between the P-CSCF and the OAM system

NOTE 1: The detailed interfaces of the P-CSCF class are described in clause 4 of the present document.

- P-CSCF Software: binary code or executable code

NOTE 2: P-CSCF files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, P-CSCF application, user plane security mechanism, or cryptographic materials.

## X.2.2 Threats related to set-up of security associations

### X.2.2.1 High-priority algorithm selection

- Threat name: High-priority algorithm selection

- Threat Category: Tampering of data, Information Disclosure, Denial of Service

- Threat Description: If the P‑CSCF does not select the highest priority algorithm combination on its own list which is also supported by the UE to protect the messages between the P‑CSCF and the UE, the P‑CSCF could end up using a weaker algorithm forcing the system into a lowered security level making the system easily attacked and/or compromised.

- Threatened Asset: IMS signalling

### X.2.2.2 Bidding down on security association set-up

- Threat name: Bidding down on security association set-up

- Threat Category: Tampering of data, Information Disclosure, Denial of Service

- Threat Description: If the P‑CSCF does not check whether the integrity and encryption algorithms list, SPI\_P and Port\_P received in SM7 is identical with the corresponding parameters sent in SM6, and check whether SPI\_U and Port\_U received in SM7 are identical with those received in SM1, the attacker can force the system to reduce the security level by tampering the integrity and encryption algorithms list. Then, weaker security algorithms may be selected, which will make the system easily attacked. Tampering the SPI will cause the negotiated SA cannot be indexed. As a result, the following security association fails to be established, leading to Denial of Service attack. The port number is generally used to identify different applications. Tampering the Port\_P number by the attacker will cause messages to be sent to the UE or P-CSCF through the tampered port. These messages including some sensitive parameters may be leaked to another application, which is not intended to receive this message.

- Threatened Asset: IMS signalling, security data

## X.2.3 Threats related to IMS signalling transport

***-*** *Threat name:*  No protection or weak protection for IMS signalling data.

***-*** *Threat Category:* Tampering,Information Disclosure.

***-*** *Threat Description:* The following behaviours may lead to bidding down attacks

 - If the protection implemented for the IMS signalling over Gm interface uses the wrong security profile, which may contain weak security algorithms or protocol versions known to be vulnerable, the level of the security of the IMS signalling data may be degraded and fail to fulfil the required security.

- The P-CSCF may be configured to never apply confidentiality, because e.g. it trusts the encryption provided by the underlying access network. The P-CSCF may also be configured to apply confidentiality whenever the UE supports it. During security associateion set-up, the first message SM1 “Register” may not be protected, hence the information within SM1 could be tampered by an attacker, e.g. by removing the encryption algorithms in the “*UE integrity and encryption algorithms list*”. In such case, the P-CSCF will not receive the encryption algorithms supported by the UE and may mistakenly believe that the UE does not support any encryption algorithm, hence will select NULL algorithm for encryption. If the P-CSCF configured to apply confidentiality does not includes the encryption algorithms it supports in SM6 when receiving no supported encryption algorithms from the UE, the UE may mistakenly believe that the P-CSCF is configured to not apply confidentiality when receiving SM6 and will select NULL algorithm for encryption. Therefore, NULL encryption algorithm is negotiated between the UE and the P-CSCF and confidentiality will eventually not be provided for the security association, in which way the attacker can launch the bidding down attack. In another word, if the P-CSCF configured to apply confidentiality does not include its encryption algorithms in SM6 when receiving no encryption algorithms of the UE in SM1, such behavior of P-CSCF will fail to thwart the bidding down attack.

NOTE: The threat above applies to UEs supporting at least one encryption algorithm other than NULL algo, as an attacker cannot launch such bidding down attack on UEs only supporting NULL algo.

Editor’s Note: The handling of the P-CSCF in the case where the P-CSCF receives SM1 with no encryption algo of UE but receives SM7 protected by the UE with an encryption algo different than NULL algo is to be further analysed.

***-*** *Threatened Asset:* IMS signalling data.

# X.3 Assets and threats specific to the S-CSCF

## X.3.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the S-CSCF to be protected are:

- S-CSCF Application;

- IMS signalling;

- Security data, i.e. cryptographic materials for Mw, Mx, Mm, Mg, ISC, Cx, Dx, Mr, and Mi interfaces

- The interfaces of the S-CSCF to be protected and which are within SECAM scope:

- Mw interface between the S-CSCF and I-CSCF/P-CSCF

- Mx interface between the S-CSCF and IBCF

- Mm interface between the S-CSCF and IP multimedia network

- Mg interface between the S-CSCF and MGCF

- ISC interface between the S-CSCF and AS

- Cx interface between the S-CSCF and HSS

- Dx interface between the S-CSCF and SLF

- Mr interface between the S-CSCF and MRFC

- Mi interface between the S-CSCF and BGCF

- Console interface, for local access: local interface on the P-CSCF

- OAM interface, for remote access: interface between the P-CSCF and the OAM system

NOTE 1: The detailed interfaces of the S-CSCF class are described in clause 4 of the present document.

- S-CSCF Software: binary code or executable code

NOTE 2: S-CSCF files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, S-CSCF application, user plane security mechanism, or cryptographic materials.

## X.3.2 Threats related to de-registration during the authentication

***-*** *Threat name:*  No de-registration during the authentication.

***-*** *Threat Category:* Denial-of-service attack.

***-*** *Threat Description:* Assume that a legal UE has already been registered into the IMS network with the IMPU. An attacker could try to register an already registered IMPU and respond with an incorrect authentication response in order to make the HN de-register the IMPU of the legal UE. In this case, the legal UE will be de-registered in the HSS. Therefore, the attacker could open up a potential denial-of-service attack deny a legitimate user access to the system.

***-*** *Threatened Asset:* Sufficient Processing Capacity.

## X.3.3 Threats related to authenticated re-registration

### X.3.3.1 Unprotected register message

- Threat name: Unprotected REGISTER messages

- Threat Category: Tampering of data, Information Disclosure, Denial of Service

- Threat Description: If the S‑CSCF does not authenticate the user by means of the AKA protocol in case of the UE sends unprotected REGISTER messages, the attacker without a legal certificates, or pre-shared key could be able to access the network. The data and resources stored in the network may be exposed to an attacker, making the system easily attacked and/or compromised.

- Threatened Asset: S-CSCF Application, Security data

### X.3.3.2 No resynchronization

* *Threat name:* No resynchronization
* *Threat Reference*: Denial of Service
* *Threat Description*: In the synchronization failure scenario, after receiving the CM4 message from HSS, the UE may not be able to access to the network if no new authentication procedure is triggered by the S-CSCF, i.e. the UE is given no opportunity to resynchronize with the network. This can result in waste of system resources and deny a legitimate user access to the system.
* *Threatened Asset*: Sufficient Processing Capacity

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the 2nd changes \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*