**3GPP TSG-SA3 Meeting #28**
**San Fransisco, USA, July, 2003**

***Tdoc ⌘S3-030373***

*CR-Form-v7*

# CHANGE REQUEST

⌘ **33.203** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **5.6.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

***Proposed change affects:*** UICC apps⌘ ☐ ME ☒ Radio Access Network ☐ Core Network ☒

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Trust Doman and the definition of SPEC(T) |
| ***Source:*** | ⌘ | Ericsson |
| ***Work item code:*** | ⌘ | IMS-ASEC |
| ***Date:*** | ⌘ | 01/07/2003 |
| ***Category:*** | ⌘ | **D** |
| ***Release:*** | ⌘ | Rel-6 |

*Use one of the following categories:*
***F*** *(correction)*
***A*** *(corresponds to a correction in an earlier release)*
***B*** *(addition of feature),*
***C*** *(functional modification of feature)*
***D*** *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

*Use one of the following releases:*

| | |
|---|---|
| *2* | *(GSM Phase 2)* |
| *R96* | *(Release 1996)* |
| *R97* | *(Release 1997)* |
| *R98* | *(Release 1998)* |
| *R99* | *(Release 1999)* |
| *Rel-4* | *(Release 4)* |
| *Rel-5* | *(Release 5)* |
| *Rel-6* | *(Release 6)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | There is no privacy mechanism for IMS from Stage 2 point of view for Release 5. However it is proposed in another CR from Ericsson that this is incorporated in TS33.203 since this mechanism exists in Stage 3 already in Release 5. Since the privacy RFC3325 specifies that a SPEC(T) is defined this CR aims to define such SPEC(T). It should be noted that T:=3GPP-IMS by definition |
| ***Summary of change:*** | ⌘ | Introduces the SPEC(T) for 3GPP IMS in an informative annex |
| ***Consequences if not approved:*** | ⌘ | Given that the Privacy CR related to RFC3325 is approved there will be a gap in the IMS TS since the concept of the SPEC(T) is missingin the TS |

| | | | | | |
|---|---|---|---|---|---|
| ***Clauses affected:*** | ⌘ | | | | |
| ***Other specs affected:*** | ⌘ | **Y** | **N** | | |
| | | | **N** | Other core specifications | ⌘ |
| | | | **N** | Test specifications | |
| | | | **N** | O&M Specifications | |
| ***Other comments:*** | ⌘ | | | | |

# Informative Annex ~~B~~K: SPEC(*T*)

The RFC 3325 mandates a network operator to define SPEC(*T*) that specifies the behaviour in the nodes of the network. This Annex is an informative annex which highlights how the SPEC(*T*) is implemented in 3GPP networks as well as examplifies how certain behavour could be implemented.

Note: By definition *T*:=3GPP-IMS

The nodes that beleong to the Trust Domain *T* include the P-CSCF, I-CSCF, S-CSCF, SEG the HSS and all other nodes and interfaces that belong to the operators within 3GPP IMS. Applications Servers that are provided by suppliers outside the 3GPP IMS do not belong to *T*.

**1. The manner in which users are authenticated**

The subscribers and users are authenticated in the S-CSCF as specified in Clause 6.1. Based on this authentication a Security Association can be created between the UE and the P-CSCF based on IK and CK derived form IMS AKA. The P-CSCF will be able to verify the claimed identity and also able to assert identities based on the integrity protection using IK and applying either HMAC-MD5 or HMAC-SHA1 of the SIP message.

**2. The mechanisms used to secure the communication among nodes within the Trust Domain**

The mechanism to use for SIP and IMS between nodes belonging to different security domains is the use of a SEG (Security Gateway) as specified in TS33.210 [5]. Optionally an operator could use IPsec over the Zb interface as specified in TS33.210 [5].

**3. The mechanisms used to secure the communication between UAs and nodes within the Trust Domain**

The UE creates a Security Association between itself and the P-CSCF as specified in Clause 7. It is mandatory to use integrity protection and the confidentiality mechanism, which is used, is between the UE and the RNC as specified in 33.102 [1].

*[Editors Note: It has been agreed to put confidentiality protection into the Presence TR at IPsec level. This should be included later.]*

**4. The manner used to determine which hosts are parts of the Trust Domain *T***

Through the registration procedure the P-CSCF will get the name of the receiving SIP server e.g. the S-CSCF as specified in TS23.228 [3], which can be viewed as trusted, and belonging to *T* from a P-CSCF point of view. All similar mechanims as defined in TS23.228 [3] for determining hosts within 3GPP IMS are trusted and belong to *T*.

However the mechanims in TS23.228 [3] does not cover all cases e.g. when a node within ~~3GPP IMS~~*T* is receiving a SIP ~~message which~~message, which does not belong to the same administrative domain e.g. originating from the Internet. Note: It is important to distinguish incoming traffic from outgoing traffic. ~~In those cases an operator could~~There are several options possible in order to verify if a node belongs *T* or not ~~consider~~ e.g. the following approaches and/or a combination thereof ~~in order to verify if a node belongs *T* or not~~ (however this list does not aim to be an exhaustive list):

1. The use of TLS and a PKI
2. Implementation of the Zb interface as speficied in TS33.210 [5]
3. Dedicated I-CSCF's for the Internet access.
4. 'Trusted' and 'untrusted' interfaces in I-CSCF.
5. Physical protection measures or IP traffic filtering is applied as described in Annex J.

It is under the responsibility of the operator to choose adequate means to achieve the trust level required and ensure that the 3GPP network remains a closed network from the Trust Domain *T* point of view. The 3GPP specifications do not mandate any particular mechanism and is left as implementation and deployment choice.

**5. The default privacy handling when no Privacy header field is present**

The behaviour is specified in Clause 5.2 and Clause 6.5.

**6. That nodes in the Trust Domain are compliant to SIP**

All the IMS nodes in 3GPP are compliant with SIP RFC 3261 [~~XXXX~~6] cf. TS23.228 [3] and TS24.229 [8].

**7. That nodes in the Trust Domain are compliant to RFC 3325**

All nodes in IMS are compliant with RFC3325.

**8. Privacy handling for identity as described in Section 7 in RFC 3325**

The Privacy Handling is specified in in Clause 5.2 and Clause 6.5.