3GPP TSG-SA3 Meeting #25
Munich, Germany, October 8-11, 2002

Tdoc ⌘S3-020559

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **5.3.0** ⌘

*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:	⌘	Clean up one Editor's note in 33.203
Source:	⌘	AT&T Wireless
Work item code:	⌘	IMS-ASEC
Date:	⌘	07/10/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

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 an old Editor's note identified some issues for further study on hiding mechanism. However, the actual hiding mechanism defined for release 5 does not depend on those issues being solved. Some issues identified by the Editor's note are not really issues for hiding.

- "use of a key identifier for support of mutiple encryption keys"
  The hiding mechanism does not depend on supporting mutiple encryption keys. In case one implementation wants to implement multiple encryption keys for hiding, the mechanism for key identifier can be implementation dependent.
- "possible use of a MAC to protect integrity of the resulting cipher text"
  The hiding mechanism does not any new requirement for integrity protection. Just as the non-hiding case, the integrity protection of the SIP message is performed by NDS/IP.
- "impact on compressibility of incoming SIP messages"
  The cipher text resulting from hiding does not go over the air interface, e.g., between the UE and P-CSCF, so it does not have any impact on compressibility of the SIP messages between Ue and P-CSCF.
- "key management and distribution amongst I-CSCFs"
  Hiding mechanism does not depend on a key management and disctribution mechanism amongst I-CSCFs being implemented.
- "implications on development of SIP are to be considered"
  No implications have been identified.

Summary of change: ⌘ Delete the above mentioned Editor's note.

Consequences if not approved: ⌘ There will still be a Editor's note in the approved spec.

Clauses affected:	⌘	6.4			
		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	
Other comments:	⌘				

6.4 Hiding mechanisms

The Hiding Mechanism is optional for implementation. All I-CSCFs in the HN shall share the same encryption and decryption key Kv. If the mechanism is used and the operator policy states that the topology shall be hidden the I-CSCF shall encrypt the hiding information elements when the I-CSCF forwards SIP Request or Response messages outside the hiding network's domain. The hiding information elements are entries in SIP headers, such as Via, Record-Route, Route and Path, which contain addresses of SIP proxies in hiding network. When I-CSCF receives a SIP Request or Response message from outside the hiding network's domain, the I-CSCF shall decrypt those information elements that were encrypted by I-CSCF in this hiding network domain.

The purpose of encryption in network hiding is to protect the identities of the SIP proxies and the topology of the hiding network. Therefore, an encryption algorithm in confidentiality mode shall be used. The network hiding mechanism will not address the issues of authentication and integrity protection of SIP headers. The AES in CBC mode with 128-bit block and 128-bit key shall be used as the encryption algorithm for network hiding. In the CBC mode under a given key, if a fixed IV is used to encrypt two same plaintexts, then the ciphertext blocks will also be equal. This is undesirable for network hiding. Therefore, random IV shall be used for each encryption. The same IV is required to decrypt the information. The IV shall be included in the same SIP header that includes the encrypted information.

~~[Editor's note: The following open issues are still to be resolved:~~

- ~~use of a key identifier for the support of multiple encryption secret keys~~
- ~~possible use of a MAC to protect integrity of the resulting cipher text~~
- ~~impact on compressibility of incoming SIP messages~~
- ~~key management and distribution amongst I-CSCFs~~
- ~~implications on development of SIP are to be considered~~

~~]~~