

Work Item Description

Visibility of configurability of security

1 3GPP Work Area

	Radio Access
X	Core Network
X	Services

2 Linked work items

None identified

3 Justification

Greater visibility of security features (ciphering, security context) and configurability of some of these features is seen as an important way to inform and protect the user and the network operator from certain types of attacks, in particular potential breach of the confidentiality of user data.

4 Objective

Due to the fact that security is not homogenous in mobile networks, a roaming user may need to be informed of the security level applied within a network. Therefore it is necessary to be able to provide greater visibility of active security features to the user. This includes an indication of ciphering and an indication of the security context (3G security context or 2G security context).

Furthermore, it can be desirable to provide means to configure a user equipment to request certain security features in order to access a service.

This may include :

- Rejection of non ciphered connections for both incoming calls and set-up calls
- Possibility to select which ciphering algorithm(s) can be used (amongst the ones available in the terminal), and a rejection of the connection in case none of the selected ones can be used
- Requiring an authentication before getting access to a certain service
- Rejection of connections established in a 2G security context instead of a 3G one (case where a 2G authentication has been performed)

Emergency calls shall be an exception and shall not be rejected.

A more complete description of the feature can be found in section 5.5 of document TS 33.102.

The objective is to make this feature available for PS connections whatever the access network (GSM BSS/GERAN or UTRAN).

5 Service Aspects

Input from S1 will probably be required in order to define precisely which options of configuration of security shall be offered to user and/or network operators.

6 MMI-Aspects

None identified

7 Charging Aspects

None identified

8 Security Aspects

The work item is a security item.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes	X	X		X	
No			X		X
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
S3#14	August 1-4, 2000	First draft of a mechanism to handle rejection of non-ciphered connections
S3#15	September 2000	Approval of CR to S3 specifications for rejection of non-ciphered connections
TSG#10	December, 2000	Approval of complete CR for rejection of non ciphered connections

New specifications						
Spec No.	Title	Prime resp. WG	2ndary resp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
Affected existing specifications						
Spec No.	CR	Subject	Approved at plenary#		Comments	
33.102					The feature already exists in section 5, mechanisms should be provided in section 6.	

11 Work item rapporteurs

Sébastien Nguyen Ngoc, France Telecom
Sebastien.nguyenngoc@francetelecom.fr
Tel: +33 145 29 47 31
Fax: +33 145 29 65 19

12 Work item leadership

TSG SA WG3

13 Supporting Companies

France Telecom...
Telia
T-mobil

(X)	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

The WI is listed as a feature in S3-000318, but has no building block defined.

It might need a building block to reject a connection (regardless of what criteria are used to reject the call, ciphering on/off, valid algorithm or not...).