
Source: SA WG3
Title: CRs to 33.102: Clarification of ciphering indicator (Release 1999 / Rel-4)
Document for: Approval
Agenda Item: 7.3.3

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-020341	33.102	167		R99	Clarification of ciphering indicator	F	3.11.0	Security	S3-020250
SP-020341	33.102	168		Rel-4	Clarification of ciphering indicator	A	4.3.0	SEC1	S3-020251

CHANGE REQUEST

⌘ **33.102 CR 167** ⌘ rev **-** ⌘ Current version: **3.b.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: ⌘ (U)SIM ME/UE Radio Access Network Core Network

Title:	⌘ Clarification of ciphering indicator		
Source:	⌘ SA WG3		
Work item code:	⌘ Security	Date:	⌘ 10 May 2002
Category:	⌘ F	Release:	⌘ R99
	Use <u>one</u> 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 <u>one</u> 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)

Reason for change:	⌘ The status of the ciphering indicator is unclear in 33.102.
Summary of change:	⌘ A reference is made to the fact that the ciphering indicator is defined as a mandatory UE feature in 22.101.
Consequences if not approved:	⌘ Inconsistent specifications may lead to misunderstanding and incorrect implementation.

Clauses affected:	⌘ 5.5.1		
Other specs affected:	<input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	
Other comments:	⌘ 22.101 reads: "Ciphering Indicator for terminals with a suitable display; The ciphering indicator feature allows the ME to detect that ciphering is not switched on and to indicate this to the user. The ciphering indicator feature may be disabled by the home network operator setting data in the SIM/USIM. If this feature is not disabled by the SIM, then whenever a connection is in place, which is, or becomes unenciphered, an indication shall be given to the user. Ciphering itself is unaffected by this feature, and the user can choose how to proceed;" The parameter on the USIM for activating and deactivating the ciphering indicator is defined in 31.102.		

5.5 Security visibility and configurability

5.5.1 Visibility

Although in general the security features should be transparent to the user, for certain events and according to the user's concern, greater user visibility of the operation of security features should be provided. This yields to a number of features that inform the user of security-related events, such as:

- indication of access network encryption: the property that the user is informed whether the confidentiality of user data is protected on the radio access link, in particular when non-ciphered calls are set-up ([this indicator is defined as a mandatory UE feature in TS 22.101 \[21\]](#));
- indication of the level of security: the property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with lower security level (3G → 2G).

5.5.2 Configurability

Configurability is the property that that the user can configure whether the use or the provision of a service should depend on whether a security feature is in operation. A service can only be used if all security features, which are relevant to that service and which are required by the configurations of the user, are in operation. The following configurability features are suggested:

- Enabling/disabling user-USIM authentication: the user should be able to control the operation of user-USIM authentication, e.g., for some events, services or use;
- Accepting/rejecting incoming non-ciphered calls: the user should be able to control whether the user accepts or rejects incoming non-ciphered calls;
- Setting up or not setting-up non-ciphered calls: the user should be able to control whether the user sets up connections when ciphering is not enabled by the network;
- Accepting/rejecting the use of certain ciphering algorithms: the user should be able to control which ciphering algorithms are acceptable for use.

CHANGE REQUEST

⌘ **33.102 CR 168** ⌘ rev **-** ⌘ Current version: **4.3.0** ⌘

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

Proposed change affects: ⌘ (U)SIM ME/UE Radio Access Network Core Network

Title:	⌘ Clarification ciphering indicator		
Source:	⌘ SA WG3		
Work item code:	⌘ SEC1	Date:	⌘ 10 May 2002
Category:	⌘ A	Release:	⌘ REL-4
	Use <u>one</u> 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 <u>one</u> 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)

Reason for change:	⌘ The status of the ciphering indicator is unclear in 33.102.
Summary of change:	⌘ A reference is made to the fact that the ciphering indicator is defined as a mandatory UE feature in 22.101.
Consequences if not approved:	⌘ Inconsistent specifications may lead to misunderstanding and incorrect implementation.

Clauses affected:	⌘ 5.5.1		
Other specs affected:	<input type="checkbox"/> Other core specifications <input type="checkbox"/> Test specifications <input type="checkbox"/> O&M Specifications	⌘	
Other comments:	⌘ 22.101 reads: "Ciphering Indicator for terminals with a suitable display; The ciphering indicator feature allows the ME to detect that ciphering is not switched on and to indicate this to the user. The ciphering indicator feature may be disabled by the home network operator setting data in the SIM/USIM. If this feature is not disabled by the SIM, then whenever a connection is in place, which is, or becomes unenciphered, an indication shall be given to the user. Ciphering itself is unaffected by this feature, and the user can choose how to proceed;" The parameter on the USIM for activating and deactivating the ciphering indicator is defined in 31.102.		

5.5 Security visibility and configurability

5.5.1 Visibility

Although in general the security features should be transparent to the user, for certain events and according to the user's concern, greater user visibility of the operation of security features should be provided. This yields to a number of features that inform the user of security-related events, such as:

- indication of access network encryption: the property that the user is informed whether the confidentiality of user data is protected on the radio access link, in particular when non-ciphered calls are set-up ([this indicator is defined as a mandatory UE feature in TS 22.101 \[21\]](#));
- indication of the level of security: the property that the user is informed on the level of security that is provided by the visited network, in particular when a user is handed over or roams into a network with lower security level (3G → 2G).

5.5.2 Configurability

Configurability is the property that that the user can configure whether the use or the provision of a service should depend on whether a security feature is in operation. A service can only be used if all security features, which are relevant to that service and which are required by the configurations of the user, are in operation. The following configurability features are suggested:

- Enabling/disabling user-USIM authentication: the user should be able to control the operation of user-USIM authentication, e.g., for some events, services or use;
- Accepting/rejecting incoming non-ciphered calls: the user should be able to control whether the user accepts or rejects incoming non-ciphered calls;
- Setting up or not setting-up non-ciphered calls: the user should be able to control whether the user sets up connections when ciphering is not enabled by the network;
- Accepting/rejecting the use of certain ciphering algorithms: the user should be able to control which ciphering algorithms are acceptable for use.