CR-Form-v7.1

CHANGE REQUEST

⌘	**33.220** CR **037**	⌘ **rev**	**-**	⌘	Current version:	**6.2.0**	⌘

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⌘ **X**   ME **X** Radio Access Network ☐ Core Network **X**

Title: ⌘	Key lifetime clarifications	
Source: ⌘	Nokia	
Work item code:⌘	GBA	***Date:*** ⌘ 16/11/2004

Category: ⌘ **C**	***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:
Ph2 (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)
Rel-7 (Release 7)

Reason for change: ⌘	Extension on key lifetime information
Summary of change:⌘	Extending the key lifetime information with key generation date.
Consequences if not approved: ⌘	Different understandings in key lifetime definition and key freshness requirements from NAF might result in: - that NAFs always request new bootstrapping to ensure key-freshness (overusage of AV, especially when there are a lot of NAFs) - Key freshness can not be indicated from BSF to NAF - Key lifetime is not exactly the same between BSF and UE

Clauses affected: ⌘	4.4.6

	Y	N		⌘	
Other specs affected: ⌘	X		Other core specifications	⌘	TS 31.102, TS 31.103, TS 29.109
		X	Test specifications		
		X	O&M Specifications		

Other comments: ⌘	

===== **BEGIN CHANGE** =====

4.4.6   Requirements on reference point Zn

The requirements for reference point Zn are:

- mutual authentication, confidentiality and integrity shall be provided;

- If the BSF and the NAF are located within the same operator's network, the Zn reference point shall be secured according to NDS/IP [13];

- If the BSF and the NAF are located in different operators' networks, the Zn' reference point between the D-Proxy and the BSF shall be secured using TLS as specified in RFC 2246 [6];

Editor's Note: The TLS Certificate profiling needs to be completed and will be added into an Annex.

- The BSF shall verify that the requesting NAF is authorised;

- The NAF shall be able to send a key material request to the BSF, containing NAF's public hostname used by the UE's corresponding request. The BSF shall be able to verify that a NAF is authorized to use this hostname, i.e. the FQDN used by UE when it contacts the NAF;

- The BSF shall be able to send the requested key material to the NAF;

- The NAF shall be able to get a selected set of application-specific user security settings from the BSF, depending on the policy of the BSF and the application indicated in the request from the NAF over Zn;

- The NAF shall be able to indicate to the BSF the single application or several applications it requires user security settings for;

NOTE: If some application needs only a subset of an application-specific user security setting, e.g. only one IMPU, the NAF selects this subset from the complete set of user security settings sent from BSF.

- The BSF shall be able to configure on a per NAF or per application basis if private subscriber identity and which user security settings may be sent to a NAF;

- The BSF shall be able to indicate to the NAF the lifetime of the key material. The key lifetime sent by the BSF over Zn shall indicate both the bootstrapping time and the expiry time of the key, and shall be identical to the expiry time of the key lifetime sent by the BSF to the UE over Ub.

NOTE: This does not preclude a NAF to refresh the key before the expiry time according to the NAF's local policy.

Editor's note: It is ffs which actions are to be taken over Zn when the BSF receives a user security settings update from the HSS over Zh.

===== **END CHANGE** =====