3GPP TSG SA WG3 Security — S3#15 **S3-000506**

12-14 September, 2000

Washington D.C., USA

TSG-RAN Working Group 2 (Radio L2 and Radio L3) ***R2-001871***
Sophia Antipolis, France, 21 – 25 August, 2000

Source:	**TSG-RAN WG2**
To:	**TSG-T WG3**
Cc:	**TSG-SA WG3, TSG-CN WG1, TSG-T WG2**
Title:	**Response to LS (T3-000433) on Parameters to be stored in the USIM**
Contact:	Marko Mahkonen, Nokia
	Email: Marko.Mahkonen@nokia.com
	Tel.: +358 40 768 2650

TSG-RAN WG2 would like to thank TSG-T3 for their questions for clarification about network related parameters to be stored in the USIM.

Ciphering information

RAN WG2 does not have a specific requirement to store the old security parameters. According to the understanding of RAN WG2, storing the old security parameters would give the benefit of reducing the number of authentication procedures. Nevertheless, RAN WG2 also sees the need to reduce the size of required memory for the preconfiguration information in the USIM.

RAN WG2 proposes that this issue is agreed between T WG3 and SA WG3.

Frequency information

There might be a case that the user moves the USIM from a UE to another UE – then it would be useful to have available the preconfiguration information stored in the USIM. Storing the information in the USIM is also how it is done in GSM. RAN WG2 proposes to let UE decide about storing optionally the information in the USIM or the UE.

Also RAN WG2 would like to propose some optimization to parameters to be stored in the USIM:

- Scrambling code information is set optional since it may not be needed in cell selection procedure.

- Downlink UARFCN is set mandatory instead of uplink UARFCN, since downlink UARFCN information is needed in cell selection before uplink UARFCN is needed.

Cell parameters ID is set optional since it may not be needed in cell selection procedure.

The configuration includes values which are considered to be optional (OP) and mandatorily present (MP). If all values are present, this configuration would require approximately 5 kbits of memory.

RAN WG2 also would like to get recommendation from T WG3 about the available memory for these parameters. There is possibility to further optimise multiplicity and type constraint values – the configuration presented now just describes the current state of RAN WG2 specifications.

Annex B (informative): USIM parameters

B.1 Introduction

This annex contains recommendations about the network parameters to be stored in the USIM.

B.2 Ciphering information

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Cipher key for each CN domain	MP	<1 to maxCNDomains>		Cipher key is described in 33.102.
> Old CK	MP		Bitstring (128)	
> New CK	MP		Bitstring (128)	
Integrity key for each CN domain	MP	<1 to maxCNDomains>		Integrity key is described in 33.102.
> Old IK	MP		Bitstring (128)	
> New IK	MP		Bitstring (128)	
START value for each CN domain	MP	<1 to maxCNDomains>		START value is described in 33.102.
> Old START	MP		Bitstring (20)	
> New START	MP		Bitstring (20)	
KSI, Key set identifier for each CN domain	MP	<1 to maxCNDomains>		Key set identifier is described in 33.102.
> Old KSI	MP		Bitstring (3)	
> New KSI	MP		Bitstring (3)	

B.3 Frequency information

Neighbour cell list

Information Element/Group name	Need	Multi	Type and reference	Semantics description
FDD cell list	OP	<1 to maxFDDFreqList>		
>UARFCN uplink (Nu)	OP~~MP~~		Integer(0.. 16383)	[25.101] If IE not present, default duplex distance of 190 MHz shall be used.
>UARFCN downlink (Nd)	MP~~OP~~		Integer(0 .. 16383)	[25.101]
> Primary scrambling code	OP~~MP~~	<1 to maxFDDFreqCellList>	Primary CPICH info 10.3.6.51	
TDD cell list	OP	<1 to maxTDDFreqList>		
>UARFCN (Nt)	MP		Integer(0 .. 16383)	[25.102]
> Cell parameters ID	OP~~MP~~	<1 to maxTDDFreqCellList>	Integer (0..127)	The Cell parameters ID is described in 25.223.
GSM Neighbour cell list	OP			
>GSM neighbour cell info	MP	<1 to maxGSMCellList>		
>> BSIC	MP			
>> BCCH ARFCN	MP			

B.4 Multiplicity values and type constraint values

Constant	Explanation	Value
Ciphering information		
maxCNDomains	Maximum number of CN domains	4
Frequency information		
maxFDDFreqList	Maximum number of FDD carrier frequencies to be stored in USIM	4
maxTDDFreqList	Maximum number of TDD carrier frequencies to be stored in USIM	4
maxFDDFreqCellList	Maximum number of neighbouring FDD cells on one carrier to be stored in USIM	~~8~~32
maxTDDFreqCellList	Maximum number of neighbouring TDD cells on one carrier to be stored in USIM	~~8~~32
maxGSMCellList	Maximum number of GSM cells to be stored in USIM	~~8~~32