Technical Specification Group Services and System Aspects
Meeting #9, Hawaii, USA, 25-28 September 2000

TSGS#9(00)0421

Source: **SA WG3**

Title: **6 new Work Item descriptions**

Document for: **Approval**

Agenda Item: **7.3.3**

The attached Work Irtem desciption sheets have been created and agreed by SA WG3 and are presented to TSG SA#09 for approval:

Document & Work Item	
S3-000488	UE triggered authentication during connections
S3-000490	Enhanced home control of security by HE
S3-000599	USIM toolkit security
S3-000609	Location services security
S3-000610	VHE security
S3-000611	Study on network-based denial of services attacks

3GPP TSG SA WG3 Security — S3#14 **S3-000488**

2-4 August, 2000

Oslo, Norway

Source: **Vodafone**

Title: **WI description for UE triggered authentication during connections**

Document for: **Approval**

Agenda Item: **12**

Work Item Description

Title

UE triggered authentication during connections

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2 Linked work items

None identified

3 Justification

The R99 security architecture specifies a mechanism to allow the UE to force an authentication at the start of an RRC connection if the value of the hyperframe number at the end of the previous RRC connection exceeds an operator determined threshold value contained on the USIM. The mechanism is used to help control the lifetime of the cipher and integrity keys, CK and IK, by reducing the reliance on the serving network to implement an appropriate authentication policy.

It is intended to enhance this mechanism is R00 so that the authentication and key agreement procedure can be triggered by the UE during a connection if the threshold hyperframe number is reached. This may be useful if long connections are expected (e.g. in the PS domain).

4 Objective

The objectives of this work item are:

- to produce the necessary stage 2 specifications
- to ensure that the stage 3 specifications are developed by the relevant groups

In order to implement this feature, it is required that the UE is able to indicate to the core network during a connection that the authentication procedure should be run.

5 Service Aspects

None identified.

6 MMI-Aspects

None identified.

7 Charging Aspects

None identified.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

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

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

Meeting	Date	Activity
S3#15	September 2000	Stage 2 specifications complete.
S3#16	November 2000	

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				

11 Work item raporteurs

Peter Howard, Vodafone

Peter.Howard@vf.vodafone.co.uk

Tel +44 1635 676206

Fax +44 1635 231721

12 Work item leadership

TSG SA WG3

13 Supporting Companies

??

14 Classification of the WI (if known)

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

3GPP TSG SA WG3 Security — S3#14 **S3-000490**

2-4 August, 2000

Oslo, Norway

Source: **Vodafone**

Title: **WI description for enhancing home environment control of security**

Document for: **Approval**

Agenda Item: **12**

Work Item Description

Title

Enhancing home environment control of security

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2 Linked work items

None identified

3 Justification

In order to facilitate global roaming the 3GPP authentication and key agreement mechanism has been adopted by the TIA TR-45 group. TR-45 have identified requirements for enhancing the degree of control the home environment can exert on the serving network with respect to authentication and key agreement. In particular, two security features are required by TR-45:

- Authentication vector revocation
- Positive authentication result reporting

4 Objective

The objectives of this work item are:

- to assess the requirements identified by TR-45 to determine what functional changes should be made to the R00 security architecture
- to produce the necessary stage 2 specifications
- to ensure that the stage 3 specifications are developed by the relevant groups

5 Service Aspects

None identified.

6 MMI-Aspects

None identified.

7 Charging Aspects

None identified.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

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

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

Meeting	Date	Activity
S3#15	September 2000	Responses to liaison statements on the feasibility of the identified features expected from N4. S3 to assess the requirements identified by TR-45 to determine what functional changes should be made to the R00 security architecture.
S3#16	November 2000	Stage 2 specifications complete.

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				

11 Work item raporteurs

Peter Howard, Vodafone

Peter.Howard@vf.vodafone.co.uk

Tel +44 1635 676206

Fax +44 1635 231721

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Telenor

Nokia

Vodafone

14 Classification of the WI (if known)

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

3GPP TSG SA WG3 Security — S3#15 **S3-000599**

12-14 September, 2000

Washington DC, USA

Source: **Vodafone**

Title: **WI description for supporting USIM toolkit security enhancements in T3**

Document for: **Approval**

Agenda Item: **8.3**

Work Item Description

Title

USIM toolkit security enhancements

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2 Linked work items

T3 work item “Enhancements to 03.48” approved at T#8 as TP-000116.

3 Justification

GSM03.48 describes a protocol for secure message exchange between the SIM and other elements. The release 99 version of this specification is however limited to the use of secret key techniques. Studies of the requirements for message security for mobile commerce have shown that there is a clear need to extend 03.48 to support public key techniques. In addition, with the advent of other "Toolkits" such as WAP and MExE, and the need for these Toolkits to communicate securely with the SAT, it is felt that a "many-to-one" solution for the secure transmission of messages to and from the SAT is required.

4 Objective

To monitor T3 work to enhance 03.48 and to provide the necessary security expertise where required.

5 Service Aspects

None identified.

6 MMI-Aspects

None identified.

7 Charging Aspects

None identified.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

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

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

T3 aim to provide CRs at T3#15 (August) for information and at T3#16 (13-15 November) for approval.

Meeting	Date	Activity
S3#16	28-30 November 2000	Review T3 CRs.

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				
03.20				

11 Work item raporteurs

Peter Howard, Vodafone

Peter.Howard@vf.vodafone.co.uk

Tel +44 1635 676206

Fax +44 1635 231721

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Vodafone, Motorola, BT, Orange

14 Classification of the WI (if known)

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

3GPP TSG SA WG3 Security — S3#15 **S3-000609**

12-14 September, 2000.

Washington, D.C.

Source: **S3**

Title: **Updated WI description for LCS security**

Document for: **Approval**

Agenda Item: **tbd**

Work Item Description

LCS security

1. 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2. Linked Work Items

LCS work items

3. Justification

This is a building block for a more general work item of Location Services. The need of a work item for security aspects was identified already when defining the general WI.

1.
2.
3.

4. Objective

Security-related problems identified by other groups are studied and necessary mechanisms are provided. The concepts developed for LCS are reviewed from security point of view.

5. Service Aspects

There may be security issues related to service aspects.

6. MMI Aspects

There may be security issues related to MMI, e.g. user privacy issues.

7. Charging Aspects

There may be security issues related to charging, e.g. new fraud types.

8. Security Aspects

The work item is a security item.

9. Impacts

Affects :	USIM	ME	AN	CN	Others(S2, S5)
Yes		X	X	X	X
No					
Don't know	X				

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

Meeting	Date	Activity
S3#15	September 2000	Approval of the WI
S3#16	November, 2000	LCS R4/R5 security issues identified.
	March 2001	Security for GERAN LCS approved
	December 2001	Security for LCS R5 security approved

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
TS 23.271		Functional stage 2 description of location services in UMTS and GSM		
TS 43.059		Functional Stage 2 Description of Location Services in GERAN, (Release 2000)		

11. Work Item Raporteurs

Nokia - Valtteri Niemi

12. Work Item Leadership

TSG SA WG3

13. Supporting Companies

It is expected that the companies supporting the general work item also support the security work.

14. Classification of the WI (if known)

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

14b. The WI is a Building Block: parent Feature

Location Services (UMTS)

3GPP TSG SA WG3 Security — S3#15 **S3-000610**

12-14 September, 2000

Washington DC, USA

Source: **BT**
Title: **WI description for VHE Security**
Document for: **Approval**
Agenda Item: **8.3**

Work Item Description

VHE Security

1 3GPP Work Area

	Radio Access
X	Core Network
X	Services

2 Linked work items

MExE Security
USIM Toolkit security enhancements
OSA Security

3 Justification

Virtual Home Environment (VHE) is defined as a concept for personal service environment portability across network boundaries and between terminals. The concept of the VHE is such that users are consistently presented with the same personalised features, User Interface customisation and services in whatever network and whatever terminal (within the capabilities of the terminal and network), where ever the user may be located. The key requirements of the VHE are to provide a user with a personal service environment which consist of:

- Personalised services;
- Personalised User Interface (within the capabilities of terminals);
- A consistent set of services from the user's perspective irrespective of access e.g. (fixed, mobile, wireless etc. Global service availability when roaming.

VHE is intended to provide:

- A common access for services in future networks;
- An environment for the creation of services;
- The ability to recover a personal service environment (e.g. in the case of loss/damage of user equipment).

4 Objective

The objective of this work item is to ensure that VHE service requirements and service features for Release 2000 incorporate appropriate security. The work item will allow S3 to review the work carried out in the S1 VHE adhoc group, specifically security aspects of: -

- The definition, storage and transmission of the VHE user profile including confidentiality and Integrity issues for personal data

- Extensions to existing toolkits, and new toolkits, that concern the Protection of sensitive user data, Integration with Location Services and the retrieval of terminal capabilities and display of terminal capabilities information.

- Interaction between toolkits and IP multimedia services

- The requirement to make roamed-to network capability available to services

5 Service Aspects

None identified

6 MMI-Aspects

Not yet investigated

7 Charging Aspects

none

8 Security Aspects

The work item is a security item.

9 Impacts

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

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

Meeting	Date	Activity
S3#16	November, 2000	Complete review of VHE specifications
	December 2000	CR's to 22.121 and 22.127 if required Final CR's to Security Architecture TS 33.102 approved at TSG level
	April 2001	Integration of security architecture Complete CRs
	June 2001	CRs approved at TSG level

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				Possible expanded scope and place of use for existing security features
TS 22.121		Virtual Home Environment R99		Possible CR,s depending on result of threat analysis
TS 23.127		VHE/OSA for R99		Possible CR,s depending on result of threat analysis

11 Work item raporteurs

Colin Blanchard
Network Security Design
MLB1 PP8
BT Advanced Communications Technology Centre
Adastral Park
Ipswich
IP5 5RE
Phone +44 1473 605353
Fax +44 1473 623910
colin.blanchard@bt.com

12 Work item leadership

TSG SA WG3

13 Supporting Companies

BT, Motorola, Ericsson, France Telecom, Nortel Networks

14 Classification of the WI (if known)

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

3GPP TSG SA WG3 Security — S3#15 **S3-000611**

12-14 September, 2000

Washington D.C., USA

Source: **Motorola**

Title: **WI proposal on UMTS network vulnerabilities to DoS attacks**

Document for: **Discussion**

Agenda Item: **tbd**

(S3#13 - TD S3-000457revised)

Work Item Description

A Study of UMTS network vulnerabilities to Denial of Service (DoS) attacks

1. 3GPP Work Area

	Radio Access
X	Core Network
X	Services

2. Linked Work Items

- Network-based end-to-end security
- Core network security – full solution

3. Justification

The convergence of mobile communication and Internet brings Internet-like services directly to mobile users, while it also exposes the UMTS network to various Internet attacks. Eavesdropping, tampering, impersonation and communication interruption can happen anywhere along the end-to-end route.

This WI aims to address the communication interruption issue caused by Internet Denial-of-Service attacks to the UMTS network. The UMTS PLMN can be easily congested and therefore paralysed by bogus traffic from the Internet. Examples of denial-of-service attacks to the UMTS networks are:

1. Launching massive UDP packets to a PLMN: This can be done by finding a few IP addresses of a PLMN, sending massive UDP packets to those addresses until the traffic reaches its capacity limit at Gn interface(or Iu, Iub etc), and then the UMTS network will be flooded.
2. Utilising the well-known Internet SYN flood attack to send massive TCP Connection Request packets(TCP packets with SYN=1 and ACK=0) to many mobile stations.
3. Utilising the well-known Internet smurf or broadcast attacks, or Path-Discovery to launch massive ICMP traffic to the UMTS network, and hence to flood the network. Those attacks will happen only if those Internet diagnostic services are supported by UMTS.

The current UMTS system architecture and protocols are designed to accommodate some Internet services, including informative service, job dispatching, information casting, home automation, and messaging services etc. Most of the services are *PULL* type services, which are invoked by the MS. Other services are *PUSH* type that are invoked by the Network Node and delivered to the MS without negotiation with the MS on a case-by-case basis.

If the service is based on UDP/IP(video or audio services) no matter whether it is PULL or PUSH type, the UMTS border gateway(or firewall residing at the UMTS border) can only perform packet filtering based on IP source and

destination addresses, or in conjunction with UDP port numbers. However, it is quite easy to spoof an address on the Internet and also very easy to forge an IP address.

For the PUSH type services, although they may be implemented on top of TCP/IP, the UMTS network can be flooded easily by SYN flood attacks. A 2 Mbps UMTS air interface can be totally blocked when a 200-octet TCP Connection Request packet is sent to an MS at 1 millisecond intervals. A feature designed in the UMTS R99 permits the launching of this type of attack because the core network allows network initiated PDP context activation(for supporting PUSH type services).

The network initiated PDP context activation is triggered by an arriving UDP or TCP Connection Request PDU under the condition that there has not been any PDP Context established for the UDP flow or TCP connection. After the GGSN initiates the Network-Requested PDP Context Activation, an RAB-setup is performed over air interface to build a signal connection and to reserve the necessary radio resources for the traffic. Hence this can overload the DCCH channel and RACH buffer; and exhaust RAB.

From the network operator's perspective, business success largely depends on the fact that networks run properly so that the services can be delivered to customers. It is also essential that their network be utilised as much as possible in order to produce maximum profit. The former point requires limitation of traffic types coming into UMTS network(i.e., limit the service type offered to the end-user) in order to reduce the chance of DoS attacks. However, the later point determines that the UMTS network has to support all user-demanded services. The issue is how to protect Network Operator's UMTS network whilst allowing various services being provided to end-users.

It should be noted that DoS attacks are not limited to UMTS networks but may be launched against some current data services (e.g., Short Message Service) in GSM networks and the signalling network SS7. In these~~is~~ cases there is~~are~~~~is~~ evidences to support the concern that DoS attacks are a real threat to the business success of wireless data services.

4. Objective

This WI aims to study the mechanisms of communication interruption caused by Internet Denial-of-Service attacks to UMTS and GSM networks. The output of the WI will be a risk analysis study. Further outputs may include a set of recommendations for CRs to existing standards, and/or a short "guideline" document that is produced for the benefit of UMTS and GSM network operators.

The objective of the risk analysis is to:

- Understand DoS attacks and therefore conduct a threat analysis for PUSH type services, other services build on top of UDP/IP, ~~and~~ Internet diagnostic messages (ICMP Echo Req, ICMP Echo Resp, Path MTU discovery, etc.), SMS in GSM, and SS7 signalling.
- Consider what countermeasures may be available via good operating procedures, such that a set of guidelines may counter many attacks. Drafting of a "Guidelines" document may be a component of this WI or it may become a new WI.
- Produce CRs to TS 33.900 to add greater detail to sections that describe DoS.
- Consider what CRs may be needed to other specification documents in order to implement practical DoS countermeasures. The drafting of CRs may be a component of this WI or may become a new WI.

5. Service Aspects

Input from S2 will be required on service architecture, type of services for UMTS and addressing in order to fully understand the nature of the services supported for UMTS R00. Also input from N3 will be required on the internetworking aspects in order to support various Internet services.

Input from and output to S5 on charging related DoS countermeasures.

6. MMI Aspects

Not yet investigated

7. Charging Aspects

Charging policy in UMTS and GSM networks is highly related to the WI. Careful selection of the charging policy can directly affect the probability that DoS attacks will be launched against a network.

- Flat-rate - This method is simple and easy to implement. Although radio resource is scarce, mobile subscribers do not expect to pay for signalling messages in managing mobile attachment and PDP context. However, this may cause radio interface congestion by both PULL and PUSH type services.
- Volume based - An alternative charging method is to count the bytes that are sent or received by the mobile. This seems to be accurate. However, we need to investigate how to charge the PUSH type services and signalling messages in order to prevent DoS attacks.
- Service based - Would operators be willing to charge differently for the use of different services? If YES, how to classify those services and attach different tariffs in order to prevent DoS attacks?

8. Security Aspects

The work item is a security item.

9. Impacts

Affects :	USIM	ME	AN	CN	Others(S2, S5)
Yes				X	X
No					
Don't know	X	X	X		

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

Note that work on either a Guidelines document or CRs to existing standards may be performed as a continuation of this WI or as a new WI.

Meeting	Date	Activity
S3#14	August 1-4, 2000	Presentation to S3 of the WI proposal
S3#15	September 2000	Presentation of Revised WI to S3 Approval of the WI CR to 21.133 examples ~~table of contents to add~~ of risk analysis study CR to be approved in SA3
S3#16	November, 2000	CRs to 21.133 to add text of risk analysis study CRs to 21.133 to be approved in SA3
	Dec 2000	CRs to 21.133 to be approved at SA level
	Feb 2001	CRs to 21.133 to be approved at TSG level

New specifications						
Spec No.	Title None anticipated as a result of risk analysis study	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
TR 21.133		A Guide to 3rd Generation Security		

11. Work Item Raporteurs

Rong Shi
Motorola
16 Euroway
Blagrove
Swindon, UK
SN5 8YQ
Rongshi1@email.mot.com

Dan Brown
Motorola
1501 W.SHURE DRIVE
Arlington Height
Illinois 60004
USA
ADB002@email.mot.com

12. Work Item Leadership

TSG SA WG3

13. Supporting Companies

Motorola, Lucent, BT, NTT DoCoMo ~~NTT DoCoMo~~
~~BT~~
~~Vodafone~~
~~Orange~~
~~T-Mobil~~
~~Telenor~~

14. Classification of the WI (if known)

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