3GPP TSG SA WG3 Security — S3#25 **S3-020579**
8 - 11 October 2002
Munich, Germany

Title:	**LS on protected 'user authentication failure' messages and unprotected REGISTER messages**
Response to:	
Release:	Release 5
Work Item:	IMS
Source:	SA3
To:	CN1
Cc:	

Contact Person:
Name: Monica Wifvesson
Tel. Number: +46 46 193634
E-mail Address: monica.wifvesson@emp.ericsson.se

Attachments: S3-020555, S3-020558

---

1. Overall Description:

SA3 would like to inform CN1 that the following attached change requests in S3-020555 and S3-020558 to TS 33.203 REL-5 has been approved. These late changes may have impact on the stage 3 specifications.

In S3-020555 a new requirement has been added that if the UE considers the SA no longer active at the P-CSCF, e.g., after receiving no response to several protected messages, then the UE should send an unprotected REGISTER message.

In S3-020558 a new requirement has been added, that mandates the 'user authentication failure' messages to always be sent protected to the UE.

2. Actions:

To CN1 group.

ACTION: SA3 kindly asks CN1 to take the new requirements into account and check whether new changes are required to the stage 3 specifications.

3. Date of Next TSG-SA3 Meetings:

SA3	19-22 November 2002	Oxford, UK
SA3	25-28 February 2003	Sophia Antipolis, FR

3GPP TSG-SA3 Meeting #25
Munich, Germany, October 8-11, 2002

Tdoc ⌘S3-020555

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **5.3.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	Indication in the UE that the SA is no longer active in P-CSCF
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	26/09/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

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:

2	*(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)*

Reason for change:	⌘	One of the requirements in chapter 7.4 states that: ***"In particular, if the UE has an indication that the SA is no longer active at the P-CSCF side, it shall send an unprotected REGISTER message."*** This requirement could be misinterpreted as the UE can receive an explicit indication from the P-CSCF, that a SA is no longer active in the P-CSCF. This was not the intention with the requirement though and therefore is it proposed to clarify it.
Summary of change:	⌘	The sentence discussed above is clarified to say that the UE after receiving no response to several protected messages, then the UE can assume that the SA is no longer active in the P-CSCF and therefore send an unprotected REGISTER message.
Consequences if not approved:	⌘	The current sentence in chapter 7.4 discussed above could be misinterpreted

Clauses affected:	⌘	7.4

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	24.228, 24.229
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

7.4 Authenticated re-registration

Every registration that includes a user authentication attempt produces new security associations. If the authentication is successful, then these new security associations shall replace the previous ones. This clause describes how the UE and P-CSCF handle this replacement and which SAs to apply to which message.

If the UE has an already active security association, then it shall use this to protect the REGISTER message. If the S-CSCF is notified by the P-CSCF that the REGISTER message from the UE was integrity-protected it may decide not to authenticate the user by means of the AKA protocol. However, the UE may send unprotected REGISTER messages at any time. In this case, the S-CSCF shall authenticate the user by means of the AKA protocol. In particular, if the UE considers the SA no longer active at the P-CSCF, e.g., after receiving no response to several protected messages ~~has an indication that the SA is no longer active at the P-CSCF side~~, ~~it~~ then the UE ~~shall~~ should send an unprotected REGISTER message.

Security associations may be unidirectional or bi-directional. This clause assumes that security associations are unidirectional, as this is the general case. For IP layer SAs, the lifetime mentioned in the following clauses is the lifetime held at the application layer. Furthermore deleting an SA means deleting the SA from both the application and IPsec layer. The message numbers, e.g. SM1, used in the following clauses relate to the message flow given in section 6.1.1.

3GPP TSG-SA3 Meeting #25
Munich, Germany, October 8-11, 2002

Tdoc ⌘S3-020558

CR-Form-v7

CHANGE REQUEST

⌘ **33.203** **CR** **CRNum** ⌘ **rev** **-** ⌘ Current version: **5.3.0** ⌘

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

Proposed change affects: UICC apps⌘ [ ] ME [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	The use of SAs in user authentication failures
Source:	⌘	SA WG3
Work item code:	⌘	IMS-ASEC
Date:	⌘	03/10/2002
Category:	⌘	**F**
Release:	⌘	Rel-5

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:

2	*(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)*

Reason for change:	⌘	Use authentication failure messages are sent unprotected to the UE if SM1 was unprotected. An attacker may also issue such authentication failure messages and consequently Protecting these messages is possible using the new security association (SA) created during the unprotected registration. An attacker may also modify the SA parameters, however, receiving no authentication failure messages is more secure than receiving unprotected failure messages.
Summary of change:	⌘	Use authentication failure messages are always sent protected to the UE.
Consequences if not approved:	⌘	UE can not trust on authentication failure messages if the error messages are not protected.

Clauses affected:	⌘	7.4.1a, 7.4.2a			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	24.228, 24.229
		X /	Other core specifications		
		/ **X**	Test specifications		
		/ **X**	O&M Specifications		
Other comments:	⌘				

7.4.1a Management of security associations in the UE

The UE shall be involved in only one registration procedure at a time, i.e. the UE shall remove any data relating to any previous incomplete registrations or authentications, including any SAs created by an incomplete authentication.

The UE may start a registration procedure with an existing pair of SAs. This will be referred to as the old SAs. The authentication produces a pair of new SAs. These new SAs shall not by used to protect non-authentication traffic until noted during the authentication flow. In the same way, certain messages in the authentication shall be protected with a particular SA. If the UE receives a message protected with the incorrect SA, it shall discard the message.

A successful authentication proceeds in the following steps:

- The UE sends the SM1 message to register with the IMS. If SM1 was protected, it shall be protected with the old outbound SA.
- The UE receives an authentication challenge in a message (SM6) from the P-CSCF. This message shall be protected with the old inbound SA if SM1 was protected and unprotected otherwise.
- If this message SM6 can be successfully processed by the UE, the UE creates the new SAs, which are derived according to section 7.1. The lifetime of the new SAs shall be set to allow enough time to complete the registration procedure. The UE then sends its response (SM7) to the P-CSCF, which shall be protected with the new outbound SA. If SM1 was protected, the new SAs can now be used to protect messages other than those in the authentication. Furthermore for outbound traffic, the new SA shall be used.
- The UE receives an authentication successful message (SM12) from the P-CSCF. It shall be protected with the new inbound SA.
- After the successful processing of this message by the UE, the registration is complete. The UE sets the lifetime of the new SAs using the registration timer in the message. The old SAs are now deleted. The new SAs are used to protect all traffic.

A failure in the authentication can occur for several reasons. ~~means the UE shall delete the new SAs.~~ If the SM1 was not protected, then no protection shall be applied to the failure messages, except the user authentication failure message which shall be protected with the new SA. If SM1 was protected, the old SAs shall be used to protect the failure~~se~~ messages. In both cases, after processing the failure message, the UE shall delete the new SAs.

The UE shall delete any SA whose lifetime is exceeded.

7.4.2 Void

7.4.2a Management of security associations in the P-CSCF

When the S-CSCF initiates an authentication by sending a challenge to the UE, the P-CSCF may already contain an existing pair of SAs from a previously completed authentication. It may also contain an existing pair of SAs from an incomplete authentication. These will be referred to as the old and registration SAs respectively. The authentication produces a pair of new SAs. These new SAs shall not be used to protect non-authentication traffic until noted during the authentication flow. Similarly certain messages in the authentication shall be protected with a particular SA. If the P-CSCF receives a message protected with the incorrect SA, it shall discard the message.

The P-CSCF associates the IMPI given in the registration procedure and all the successfully registered IMPUs related to that IMPI to an SA.

A successful authentication proceeds in the following steps:

- The P-CSCF receives the SM1 message. If SM1 is protected, it shall be protected with the old inbound SA.
- The P-CSCF forwards the message containing the challenge (SM6) to the UE. This shall be protected with the old outbound SA, if SM1 was protected and unprotected otherwise.
- The P-CSCF then creates the new SAs, which are derived according to section 7.1. The expiry time of the new SAs shall be set to allow enough time to complete the registration procedure. The registration SAs shall be deleted if they exist.

- The P-CSCF receives the message carrying the response (SM7) from the UE. It shall be protected using the new inbound SA. If SM1 was protected, the new SAs can now be used to protect messages other than those in the authentication.

- The P-CSCF forwards the successful registration message (SM12) to the UE. It shall be protected using the new outbound SA. This completes the registration procedure for the P-CSCF. The P-CSCF sets the expiry time of the new SAs equal to the registration timer in the message and deletes the old SAs. The new SAs are used to protect all traffic.

A failure in the authentication can occur for several reasons. ~~means the P-CSCF shall delete the new SAs.~~ If the SM1 was not protected, then no protection shall be applied to the failure messages, except the user authentication failure message which shall be protected with the new SA. If SM1 was protected, the old SAs shall be used to protect the failure~~se~~ messages. In both cases, after processing the failure message, the P-CSCF shall delete the new SAs.

The P-CSCF shall delete any SA whose lifetime is exceeded.