Source:	**SA WG3**
Title:	**1 CR to 33.203 (Rel-5): The use of SAs in user authentication failures**
Document for:	**Approval**
Agenda Item:	**7.3.3**

SA doc#	Spec	CR	R	Phase	Subject	Cat	Current Version	WI	SA WG3 doc#
SP-020712	33.203	026		Rel-5	The use of SAs in user authentication failures	F	5.3.0	IMS-ASEC	S3-020558

CR-Form-v7

CHANGE REQUEST

| ⌘ | **33.203** CR **026** | ⌘ **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

	Y	N		
Other specs affected: ⌘	X		Other core specifications ⌘	24.228, 24.229
		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 failurese 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.