Source:	**SA WG3 (Security)**
Title:	**CR to 33.203: Terminology alignment (Rel-6)**
Document for:	**Approval**
Agenda Item:	**7.3.3**

SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Workitem
SP-030601	33.203	057	-	Rel-6	Terminology alignment	F	6.0.0	S3-030613	IMS-ASEC

CR-Form-v7

CHANGE REQUEST

| ⌘ | **33.203** CR **057** | ⌘**rev** | **-** | ⌘ | Current version: | **6.0.0** | ⌘ |

*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: ⌘	Terminology alignment	
Source: ⌘	SA WG3	
Work item code: ⌘	IMS-ASEC	**Date:** ⌘ 25/09/2003
Category: ⌘ **F**		**Release:** ⌘ Rel-6

Use <u>one</u> 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 <u>one</u> of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
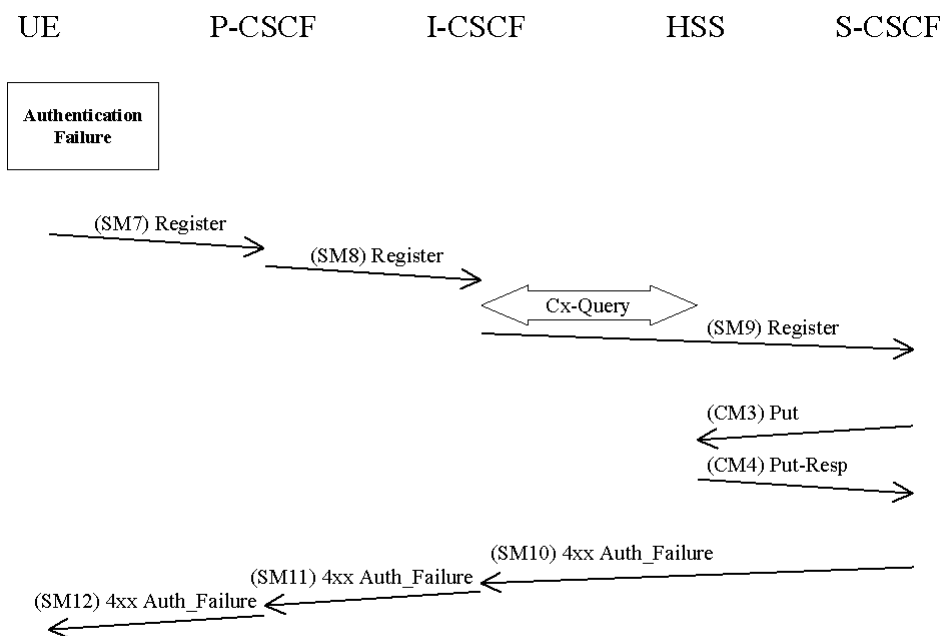Rel-5 (Release 5)
Rel-6 (Release 6)

Reason for change: ⌘	Minor clarifications to the text were added in order to improve the readability.	
Summary of change: ⌘	A sentence about the registration information storage was deleted. 'Terminate' was changed to 'abandon'. The word 'challenge' was added.	
Consequences if not approved: ⌘	Incorrect formulations, unnecessary text.	

Clauses affected: ⌘	6.1.2, 6.1.3, 7.3	

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

Other comments: ⌘		

*** FIRST CHANGE ***

6.1.2.2   Network authentication failure

In this section the case when the authentication of the network is not successful is specified. When the check of the MAC in the UE fails the network can not be authenticated and hence registration fails. The flow is identical as for the successful registration in 6.1.1 up to SM6.

UE   P-CSCF   I-CSCF   HSS   S-CSCF

```
        ┌──────────────┐
        │ Authentication│
        │   Failure     │
        └──────────────┘

        (SM7) Register
        ───────────────▶
                    (SM8) Register
                    ───────────────▶
                              ◁══ Cx-Query ══▷
                                          (SM9) Register
                                          ───────────────────────▶

                                                    (CM3) Put
                                          ◀───────────────────────
                                                    (CM4) Put-Resp
                                          ───────────────────────▶

                                (SM10) 4xx Auth_Failure
                    (SM11) 4xx Auth_Failure ◀───────────────────────
        (SM12) 4xx Auth_Failure ◀───────────────
        ◀───────────────
```

The UE shall send a Register message towards the HN including an indication of the cause of failure in SM7. The P-CSCF and the I-CSCF forward this message to the S-CSCF.

> SM7:
> REGISTER(Failure = *AuthenticationFailure*, IMPI)

Upon receiving SM9, which includes the cause of authentication failure, the S-CSCF shall set the registration-flag in the HSS to *unregistered*, if the IMPU is not currently registered. To set the flag the S-CSCF sends in CM3 a Cx-Put to the HSS. If the IMPU is currently registered, the S-CSCF does not update the registration flag.

> CM3:
> Cx-AV-Put(IMPI, Clear S-CSCF name)

The HSS responds to CM3 with a Cx-Put-Resp in CM4.

In SM10 the S-CSCF sends a 4xx Auth_Failure towards the UE indicating that authentication has failed, no security parameters shall be included in this message.

> SM10:
> SIP/2.0 4xx Auth_Failure

~~Upon receiving SM10 the I-CSCF shall clear any registration information related to the IMPI.~~

6.1.2.3   Incomplete authentication

If the S-CSCF does not receive a response to an authentication challenge within an acceptable time, it considers the authentication to have failed. If the IMPU was not already registered, the S-CSCF shall send a Cx-Put to the HSS to set the registration-flag for that IMPU to unregistered (see message CM3 in clause 6.1.2.2). If the IMPU was already registered, the S-CSCF does not change the registration-flag.

*** NEXT CHANGE ***

7.3   Error cases in the set-up of security associations

7.3.1   Error cases related to IMS AKA

Errors related to IMS AKA failures are specified in section 6.1. However, this section additionally describes how these shall be treated, related to security setup.

7.3.1.1   User authentication failure

In this case, SM7 fails integrity check by IPsec at the P-CSCF if the IK_{IM} derived from RAND at UE is wrong. The SIP application at the P-CSCF never receives SM7. It shall delete the temporarily stored SA parameters associated with this registration after a time-out.

In case IK_{IM} was derived correctly, but the response was wrong the authentication of the user fails at the S-CSCF due to an incorrect response. The S-CSCF ~~will~~ shall send a 4xx Auth_Failure message to the UE, via the P-CSCF, which may pass through an already established SA. Afterwards, both, the UE and the P-CSCF shall delete the new SAs.

7.3.1.2   Network authentication failure

If the UE is not able to successfully authenticate the network, the UE shall send a REGISTER message which may pass through an already established SA, indicating a network authentication failure, to the P-CSCF. The P-CSCF deletes the new SAs after receiving this message.

7.3.1.3   Synchronisation failure

In this situation, the UE observes that the AUTN sent by the network in SM6 contains an out-of-range sequence number. The UE shall send a REGISTER message to the P-CSCF, which may pass through an already established SA, indicating the synchronization failure. The P-CSCF deletes the new SAs after receiving this message.

7.3.1.4   Incomplete authentication

If the UE responds to an authentication challenge from a S-CSCF, but does not receive a reply before the request times out, the UE shall start a registration procedure if it still requires any IM services. The first message in this registration should be protected with an SA created by a previous successful authentication if one exists.

If the P-CSCF deletes a registration SA due to its lifetime being exceeded, the P-CSCF should delete any information relating to that registration procedure.

7.3.2   Error cases related to the Security-Set-up

7.3.2.1   Proposal unacceptable to P-CSCF

In this case the P-CSCF cannot accept the proposal set sent by the UE in the Security-Set-up command of SM1. The P-CSCF shall respond to SM1 indicating a failure, by sending an error response to the UE.

7.3.2.2   Proposal unacceptable to UE

If the P-CSCF sends in the security-setup line of SM6 a proposal that is not acceptable for the UE, the UE shall ~~terminate~~ abandon the registration procedure.

7.3.2.3   Failed consistency check of Security-Set-up lines at the P-CSCF

The P-CSCF shall check whether authentication algorithms list received in SM7 is identical with the authentication algorithms list sent in SM6. If this is not the case the registration procedure is aborted. (Cf. clause 7.2).

*** END OF CHANGES ***