3GPP TSG-CT WG1 Meeting #112bis
Vilnius (Lithuania), 15-19 October 2018

C1-186089

Discussion on Routing ID Update Solutions

Nokia, Nokia Shanghai Bell

 © 2018 Nokia

NOKIA

Routing ID Update Issue

- SA2 and CT recently discussed the following deployment issue related to Routing ID (See incoming LS C1-186309/S2-188870, C1-186302/CP-182238):

  operators need to reconfigure the Routing ID in the UE due to subscriber migration i.e. in the order of millions of UE(s).

  - Note that Routing ID provisioning in USIM and association of USIM to the subscription may happen at completely different times. Routing ID that is initially provisioned in USIM will most likely be a default value. Unless the Routing ID is updated, it cannot point to the right AUSF/UDM/UDR group that store UE's subscription information.

    =>Update can be required any time (can be during registration or after registration)

© 2018 Nokia
NOKIA

CT#81 Guidance

- In CT#81 plenary, CT tasked SA3 to evaluate the issue and provide guidance on the security aspects. CT also asked CT1 to work with SA3 to evaluate potential solutions
- According CT plenary guidance, any solution needs to provide end2end security

  concluded that any solution where the network initiates an update of the Routing ID needs to provide end2end security. Therefore related security requirements need to be available before a stage-3 solution can be specified.

© 2018 Nokia
NOKIA

End2End Security Requirements

- In SA3 reply LS (C1-186338/S3-183074), SA3 listed the following security requirements:

  SA3 see the need for the Routing ID management messages to be:

  Mandatory – Integrity protected between the Home network and the UE

  Mandatory – Replay protected between the Home Network and the UE

  Optional – Confidentiality protection between the Home Network and the UE (Note: the Routing ID will be sent in the clear to the Serving Network at next registration anyway).

  As it is good practice to confirm the change of the Routing ID, any return confirmation message shall be protected to at least the same level of security as the request message and preferably contain some reference from the request message so that the request and confirmation message can be correlated.

  SA3 noted that if the Routing ID becomes corrupted or misaligned, the UE will never recover without some other mechanism either in the UE or the Home network to rectify this situation.

  SA3 requires that any chosen mechanism does not break the security of the USIM.

© 2018 Nokia

Summary of Requirements

- Summary of requirements for Routing ID update:
  - Req 1: Support dynamic reconfiguration of Routing ID for potentially large number of UEs.
    - Req 1.1: Scalability: potentially large number of UEs (*i.e. in the order of millions of UE(s)*)
    - Req 1.2: Any time update (during or after registration)
  - Req 2: Ensure end2end security when the network initiates an update of the Routing ID
    - Req 2.1: Security is terminated at the USIM
    - Req 2.2: Routing ID management messages shall be Integrity protected between the Home network and the UE
    - Req 2.3: Routing ID management messages shall be replay protected between the Home network and the UE
    - Req 2.4: (optional) Confidentiality protection of Routing ID management messages
  - Req 3: UE ack confirmation
    - Req 3.1: Ack confirmation message from the UE shall be supported
    - Req 3.2: Ack confirmation message is protected to at least the same level of security as the request message

- Requirements are similar to SoR requirements

© 2018 Nokia

Potential Solutions

- Potential mechanisms that could be used to update the Routing ID:
  - Option 1: Switching between pre-stored values in the USIM
  - Option 2: Management using the New SoR secure packet mechanism
  - Option 3: Management using SIM OTA
  - Option 4: Extending the SoR to ME mechanism

© 2018 Nokia
NOKIA

Potential Solutions

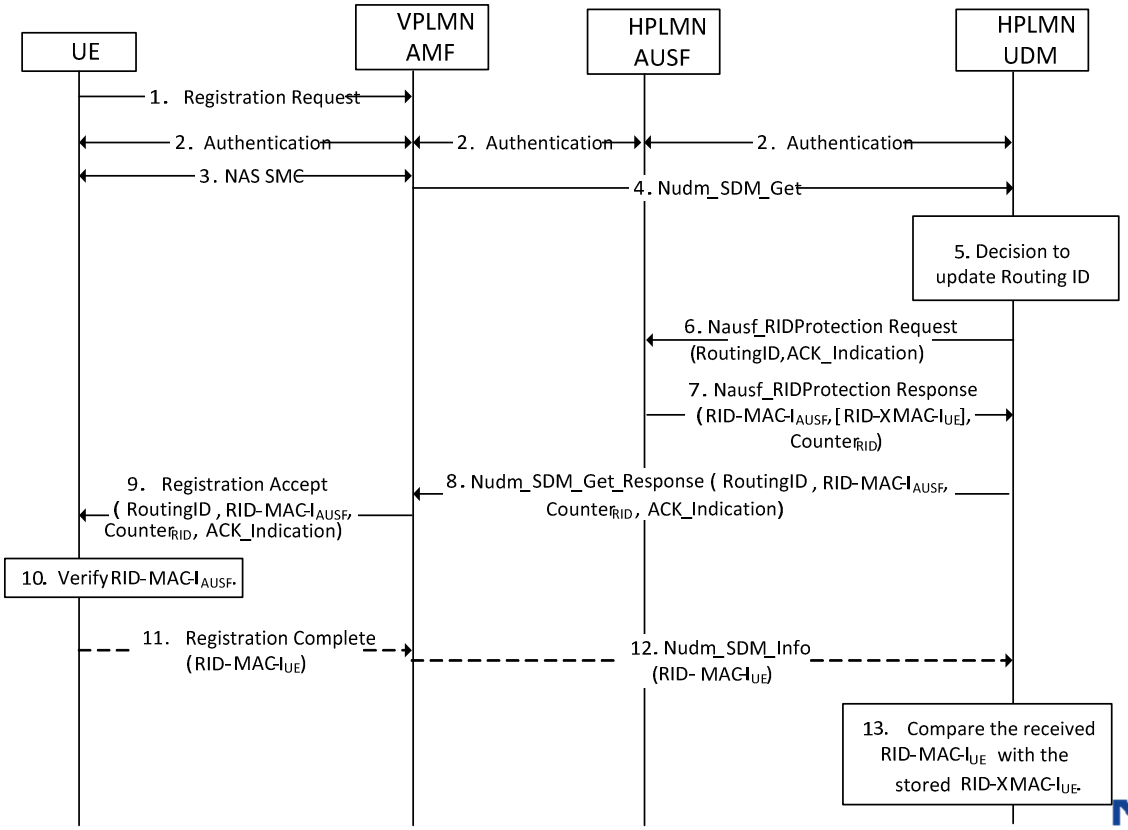
- Option 4: Extending the SoR to ME mechanism
  - Description:
    - ❖ Control plane solution to provide Routing ID update to the ME via explicit signalling. Similar to the SoR terminate at ME mechanism.
      - Network provides security protected Routing ID in a NAS transparent container to the UE
      - The NAS transparent container is terminated at the ME
    - ❖ Routing ID update is initiated by UDM and can be provided during registration or after registration
      - Use an Registration Accept message to transport the update during registration.
      - Use a DL NAS transport message to transport the update after registration.

© 2018 Nokia
NOKIA

Potential Solutions

- Option 4: Extending the SoR to ME mechanism

Callflow during registration:

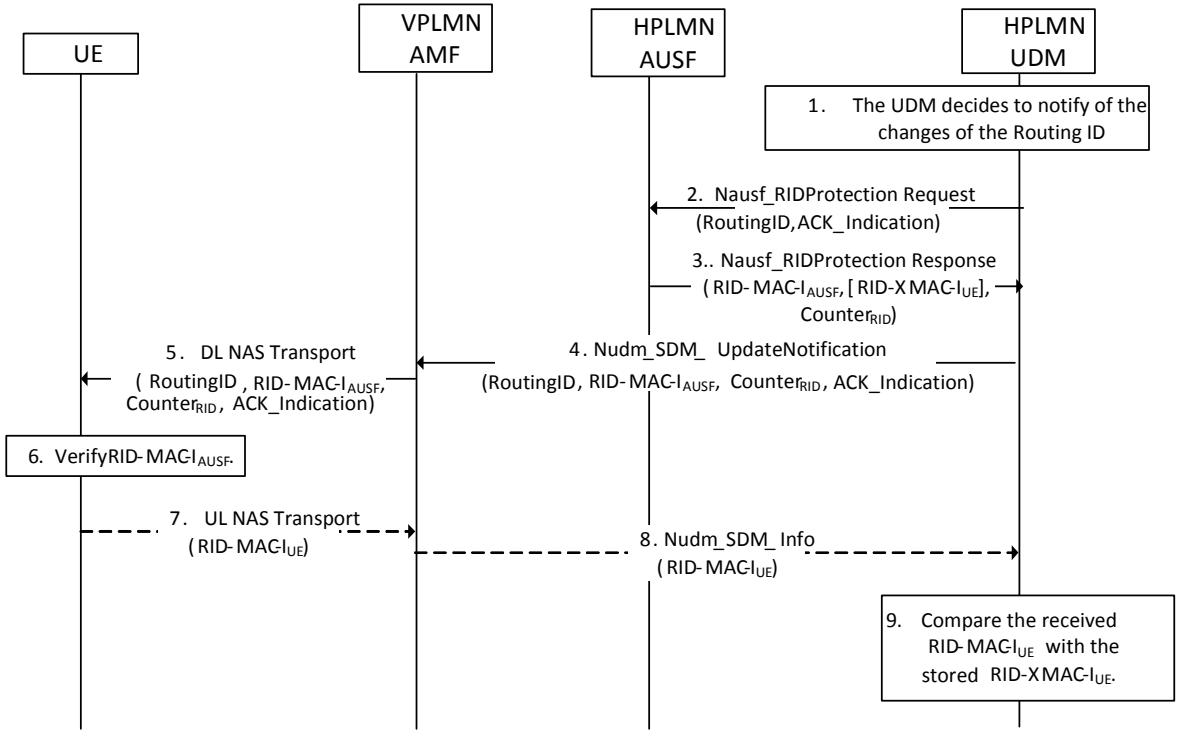


© 2018 Nokia

Potential Solutions

- Option 4: Extending the SoR to ME mechanism

Callflow after registration:



© 2018 Nokia

Potential Solutions

- Option 4: Extending the SoR to ME mechanism
  - Evaluation:
    - Based on the SoR mechanism as specified in 3GPP TS 23.122 and 3GPP TS 24.501.
    - Same mechanism for roaming or non-roaming case. Require the visited network to support the transparent container mechanisms.
    - Dynamic update: Yes
    - End2End Security : No*
      - **The security is terminated at the ME**
      - e2e protection between the home network and the ME, however possible misalignment of Routing ID configuration between the ME and the USIM.
      - The Routing ID information is integrity and replay protected
        - The UDM performs Routing ID update and invokes the AUSF to get the MAC-I and the Counter. The UDM then responds the RI update container (new RI, MAC-I, Counter) to the UE. The ME checks the integrity of the message.
    - UE ack confirmation: Yes
      - Support of UE Ack confirmation from ME to the network.
      - UE Ack confirmation message is sent integrity protected and replay protected
    - Specification impact: Yes
      - Reusing similar SoR to ME mechanism, similar specification updates expected
      - Additional mechanism is needed to update USIM with the routing ID received at the ME
      - Additional mechanism is needed to resolve possible misalignment between the ME and USIM.

© 2018 Nokia

Potential Solutions

- Option 3: Management using USIM OTA
  - Description:
    - Based on existing USIM OTA mechanism
    - Routing ID update is sent via “secure packet” as specified in 3GPP TS 31.115 (with an API to action file updates and USIM Toolkit commands).
    - Many different bearers that can be used to deliver OTA secured packets (including SMS, packet data, HTTPS, and USSD).
    - Generalized secured packet structure for both command packet and response packet. ACK confirmation is supported for OTA mechanism

© 2018 Nokia

Potential Solutions

- Option 3: Management using USIM OTA
  - Evaluation:
    - ❖ Based on the secure packet SoR mechanism as specified in 3GPP TS 23.122 and 3GPP TS 24.501.
    - ❖ Same mechanism for roaming or non-roaming case. Require the visited network to support the transparent container mechanisms.
    - ❖ Dynamic update: Partially* (after registration, not practical)
      - Some bearers can be used to push OTA updates at any time and a USIM can be setup to PULL updates
      - SA2: Given the largescale UE/USIM reconfiguration needed e.g. to possibly millions of UEs, using existing mechanisms such as OTA SIM, will not be practical from SA2 point of view (S2-188870) .
    - ❖ End2End Security : Yes
      - **The security is terminated in the USIM**.
      - The Routing ID information is integrity protected and replay protected (with confidentiality protection)
    - ❖ UE ack confirmation: Yes
      - Secure packet can go either direction. Sending Ack confirmation messages (PoR) is supported
      - Integrity and replay protection of Ack confirmation message are supported
    - ❖ Specification impact: Minimal
      - Reuse existing standardized USIM OTA mechanism,
      - Update to 31.102 expected
    - ❖ Deployment
      - Require additional network element OTA Gateway

© 2018 Nokia
NOKIA

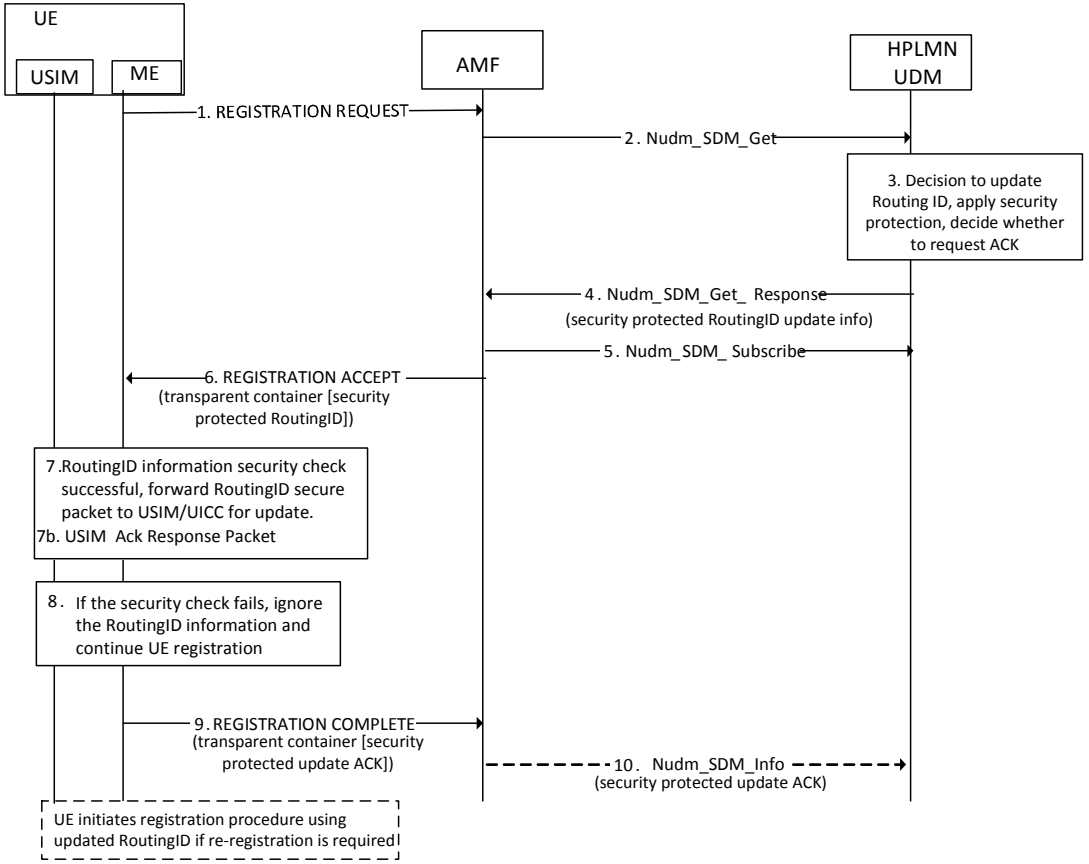
Potential Solutions

- Option 2: Management using the New SoR secure packet mechanism
  - Description:
    - ❖ Based on the secure packet SoR mechanism
      - Network provides a “Routing ID transparent container” in a new to define IE which can be used e.g. in REGISTRATION ACCEPT
      - Routing ID transparent container can contain “secure packet”
      - The secure packet contains Routing ID and is coded as specified in TS 31.115
      - On reception of a secure packet, the ME would behave as if it has received an SMS with SIM data download and forwards the SMS payload to the UICC
      - UICC updates the Routing ID information with the received data
    - ❖ The SoR transparent container can contain secured packet as specified in 3GPP TS 31.115. This secured packet could contain the relevent commands to update the Routing Information in the USIM and to initiate the REFRESH (File Change Details) to inform the ME that this file has changed.
    - ❖ Update supported during registration or after registration
      - Use an Registration Accept message to transport the update during registration.
      - Use a DL NAS transport message to transport the update after registration.

© 2018 Nokia
NOKIA

Potential Solutions

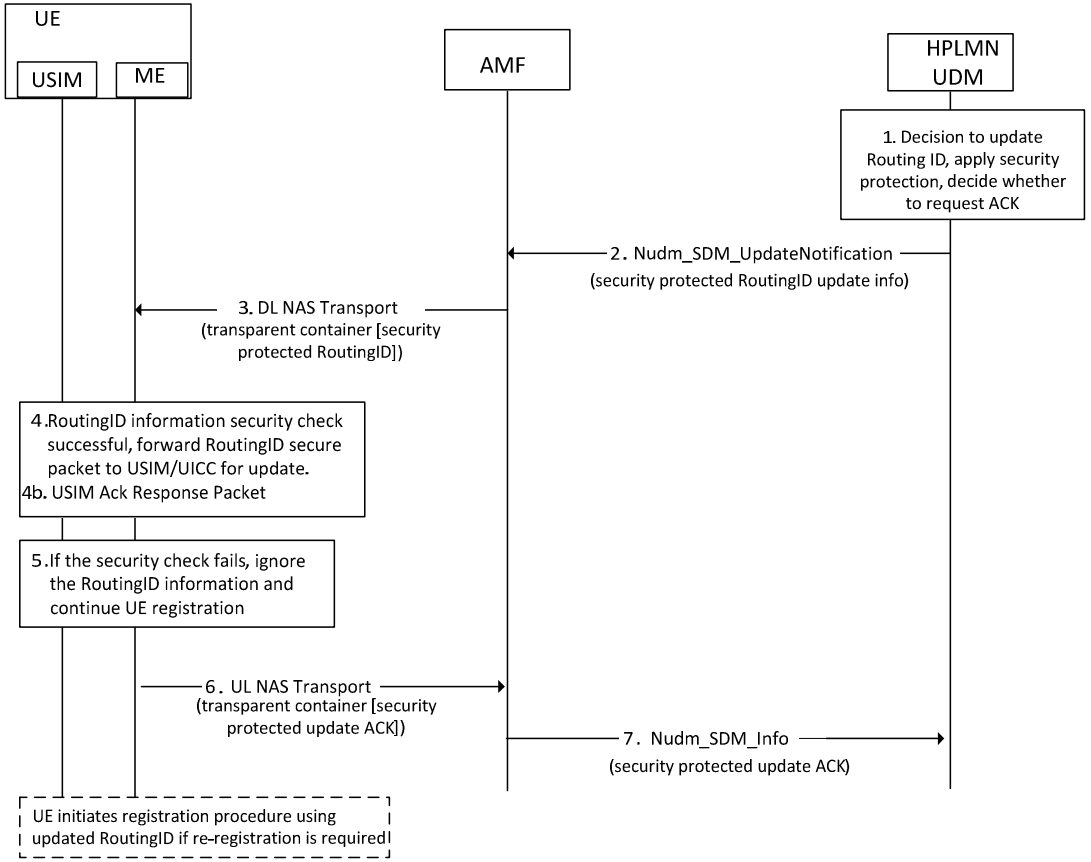
- Option 2: Management using the New SoR secure packet mechanism
  - Callflow during registration: Similar to Option 4 (with additional step for the ME to forward the received secure packet to the USIM)



© 2018 Nokia

Potential Solutions

- Option 2: Management using the New SoR secure packet mechanism
  - Callflow after registration: Similar to Option 4 (with additional step for the ME to pass the received secure packet to the USIM)



© 2018 Nokia

Potential Solutions

- Option 2: Management using the New SoR secure packet mechanism
  - Evaluation:
    - ❖ Based on the secure packet SoR mechanism as specified in 3GPP TS 23.122 and 3GPP TS 24.501.
    - ❖ Same mechanism for roaming or non-roaming case. Require the visited network to support the transparent container mechanisms.
    - ❖ Dynamic update: Yes
    - ❖ End2End Security : Yes
      - **The security is terminated in the USIM.** Handling of secure packet is already specified in standards, the ME just upload the secured packet to the USIM upon receiving secure packet in the transparent container.
      - e2e protection between the home network and the USIM.
      - The Routing ID information is integrity and replay protected
        - The UDM performs Routing ID update and invokes the AUSF to get the MAC-I and the Counter. The UDM then responds the RI update container (new RI, MAC-I, Counter) to the UE. The ME checks the integrity of the message.
    - ❖ UE ack confirmation: Yes*
      - Support of UE Ack confirmation from ME to the network.
      - UE Ack confirmation message is sent integrity protected and replay protected
    - ❖ Specification impact: Yes (relatively easy)
      - Reusing similar SoR to ME mechanism, similar specification updates expected

© 2018 Nokia
NOKIA

Potential Solutions

- Option 1: Switching between pre-stored values in the USIM
  - Description:
    - ❖ Pre-configure and store multiple Privacy information sets (Routing ID, Algorithm to use and Public key) on the USIM.
    - ❖ Use specific bits in the AMF part of the AUTN to indicate which preprogrammed Privacy information set is to be used from the next time. These could either be in the standardised and/or proprietary part of the AMF part of the AUTHENTICATE message.
    - ❖ Routing ID update is initiated by UDM during registration procedure
      - Use an AUTHENTICATION message to transport the update.

33.102:

The 16 bits in the AMF are numbered from "0" to "15" where bit "0" is the most significant bit and bit "15" is the least significant bit (see subclause 3.4)

Bit "0" is called the "AMF separation bit".

Bits "1" to "7" are reserved for future standardization use. Bits "1" to "7" shall be set to 0 while not yet specified for a particular use.

Bits "8" to "15" can be used for proprietary purposes. See Annex F for examples usages.

 © 2018 Nokia

NOKIA

Potential Solutions

- Option 1: Switching between pre-stored values in the USIM
  - Evaluation
    - ❖ Based on reusing existing AMF bit fields
    - ❖ Same mechanism for roaming or non-roaming case. No dependency on VPLMN capability.
    - ❖ Dynamic update: No
      - Update can only be initiated during registration
    - ❖ End2End Security : Yes
      - Routing ID update is integrity and replay protected as the AMF is integrity and replay protected in the AUTHENTICATION procedures
      - The security is terminated in the USIM.
    - ❖ UE ack confirmation: No
      - Support of UE Ack confirmation needs to be added.
      - Integrity and replay protection for UE Ack confirmation needs to be added.
    - ❖ Specification impact: Yes
      - Reusing existing AMF bit fields and existing signalling of AMF via AUTHENTICATION Request and Response message
      - Support of UE Ack confirmation needs to be added
      - Provisioning of the Privacy Information sets is outside the scope of the specification =>Partially standardized solution

© 2018 Nokia
NOKIA

Solution Evaluation Summary

Evaluation Criteria	Option 1 (Switching between pre-stored values in the USIM)	Option 2 (the SoR like secure packet mechanism)	Option 3 (Management using SIM OTA)	Option 4 (Extending the SoR to ME mechanism)
Dynamic reconfiguration	support	Support	Partial Support	support
Scalability (large number of UEs)	Yes	Yes	Not practical	Yes
Any time update	Yes (during and after registration)	Yes (during and after registration)	Partially (after registration)	Yes (during and after registration)
End2End security	Yes	Yes	Yes	No
Termination at USIM	Yes	Yes	Yes	No
Integrity and replay protection	Yes	Yes	Yes	Yes
UE ACK Support	No	Yes	Yes	Yes
Send UE ACK Confirmation	No	Yes	Yes	Yes
UE ACK Confirmation Security protection	No	Yes	Yes	Yes
Deployment	No additional network element required	No additional network element required	Require additional network element	No additional network element required

© 2018 Nokia
NOKIA

Conclusion

- It is proposed to standardize Option 2) to support Routing ID update towards USIM using the secure packet mechanism.

© 2018 Nokia

NOKIA