3GPP TR 33.868 V0.15.0 (2013-09)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security aspects of Machine-Type and other Mobile Data Applications Communications Enhancements;
(Release 12)

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.
The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

Security, M2M

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

The present document studies the security aspects of System Improvements for Machine Type Communication. In particular, the goals of this document are:

- To identify and analyze the threats to the MTC system within the scope of the service requirements, functionality and use cases as specified in TS 22.368 [9].
- To identify possible security and privacy impacts induced by the system architecture improvement for machine type communications based on TR 23.887 [26] and TS 23.682 [23].
- To determine possible security requirements based on the analysis above and describe the possible solutions to meet those requirements.

Machine-type communication aspects of (x)SIMs and/or new models for the management of (x)SIM are out of scope of the present document.

Editor's Note: Need to check which specifications are in scope of current SIMTC WID and need to update the scope with relevant TS and TR.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[3] 3GPP TS 23.060 (v a.2.0): "General Packet Radio Service (GPRS); Service description; Stage 2".

[4] 3GPP TS 23.401 (v a.2.1): "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[5] 3GPP TS 24.368 (v 1.0.1): "Non-Access Stratum (NAS) configuration Management Object (MO)".

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[7] Open Mobile Alliance OMA-TS-DM_Protocol V1.3: " OMA Device Management Protocol". http://www.openmobilealliance.org/

[8] Open Mobile Alliance OMA-TS-DM_Security V1.3: " Device Management Security ". URL: http://www.openmobilealliance.org/

[9] 3GPP TS 22.368: "Service requirements for Machine-Type Communications (MTC); Stage 1".

[10] 3GPP TR 23.888: "System improvements for Machine-Type Communications (MTC)".

[11] 3GPP TS 43.020: "Security related network functions".

[12] 3GPP TS 33.102: "3G security; Security architecture".

[13] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[14] 3GPP TS 33.234: "3G security; Wireless Local Area Network (WLAN) interworking security".

[15] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[16] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[17] ETSI TS 102 225: "Smart Cards; Secured packet structure for UICC based applications (Release 9)

[18] ETSI TS 102 226: "Smart cards; Remote APDU structure for UICC based applications (Release 6)"

[19] 3GPP TS 31.115: "Remote APDU Structure for (U)SIM Toolkit applications".

[20] 3GPP TS 31.116: "Remote APDU Structure for (Universal) Subscriber Identity Module (U)SIM Toolkit applications".

[21] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[22] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".

[23] 3GPP TS 23.682: “Architecture Enhancements to facilitate communications with Packet Data Networks and Applications”.

[24] 3GPP TS 23.012: "Location management procedures".

[25] 3GPP TS 33.224: "Generic Bootstrapping Architecture (GBA) Push Layer".

[26] 3GPP TR 23.887: “Machine-Type and other Mobile Data Applications Communications Enhancements”

[27] ETSI TS 102 690: “Machine-to-Machine communications (M2M); Functional architecture”

[28] IETF RFC 4186: "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)".

[29] IETF RFC 4187: "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)".

[30] IETF RFC 5448: "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')".

[31] IETF RFC 5191: "Protocol for carrying Authentication for Network Access (PANA)".

[32] 3GPP TS 33.320: "Security of Home Node B (HNB) / Home evolved Node B (HeNB)".

[33] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".

[34] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[35] 3GPP TS 24.301: "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3".

[36] ETSI TS 102 484: " Smart Cards; Secure channel between a UICC and an end-point terminal".

[37] 3GPP TS 29.109: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".

[38] 3GPP TS 23.048: "Security mechanisms for the (U)SIM application toolkit; Stage 2".

[39] 3GPP TS 23.840: "Study into routeing of MT-SMs via the HPLMN".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

MTC UE authentication: this is authentication of a MTC Device using GSM AKA, UMTS AKA, EPS AKA, EAP-AKA, or EAP-AKA' as defined in TSs 43.020 [11], 33.102 [12], 33.401[13], 33.234 [14], or 33.402 [15].

MTC IMS authentication: this is authentication of the MTC Device as an IMS UE by the IMS core as defined in TS 33.203 [16]. The need for such a form of authentication in the context of MTC is yet to be determined.

MTC ME authentication: this is authentication of the platform in the sense of device authentication as used in TS 33.320 [32]. The need for such a form of authentication in the context of MTC is yet to be determined, and, if needed, the appropriate mechanism would still have to be selected.

MTC application authentication: this is authentication between the MTC application on the MTC Device and the corresponding application on the MTC server.

NOTE: MTC application authentication is transparent to the 3GPP network (GSM, 3G, or EPS) and therefore out of scope of 3GPP. However, it is ffs to which extent key management mechanisms supporting MTC application authentication are within the scope of 3GPP.

MTC 3GPP access confidentiality / integrity: this is the feature provided by the confidentiality / integrity mechanisms defined for interfaces between the UE and the 3GPP network in TSs 43.020 [11], 33.102 [12], 33.401 [13], 33.234 [14], or 33.402 [15] including any possible enhancements for MTC purposes.

MTC IMS access confidentiality / integrity: this is the feature provided by the confidentiality / integrity mechanisms defined for interfaces between the UE and the IMS core in TS 33.203 [16] including any possible enhancements for MTC purposes.

MTC IMS media plane confidentiality / integrity: this is the feature provided by the confidentiality / integrity mechanisms in TS 33.328 [33] including any possible enhancements for MTC purposes.

MTC application confidentiality / integrity: this is a feature provided by confidentiality / integrity mechanisms used at the MTC application layer.

NOTE: MTC application confidentiality / integrity is out of scope of 3GPP.

MTC Security GW: Function entity in the operator’s security domain, terminating security association(s) for the external interface link between the network and the MTC server.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

MTC	Machine-Type Communications

4 Overview of Security Architecture

Editor's note: This section is intended to provide the high-level SIMTC security architecture to support the objectives of the WID

The MTC security architecture described in Figure 1 is based on the system architecture given in TS 23.682 [23] and is given here for helping to analyse the threats in the following clause.

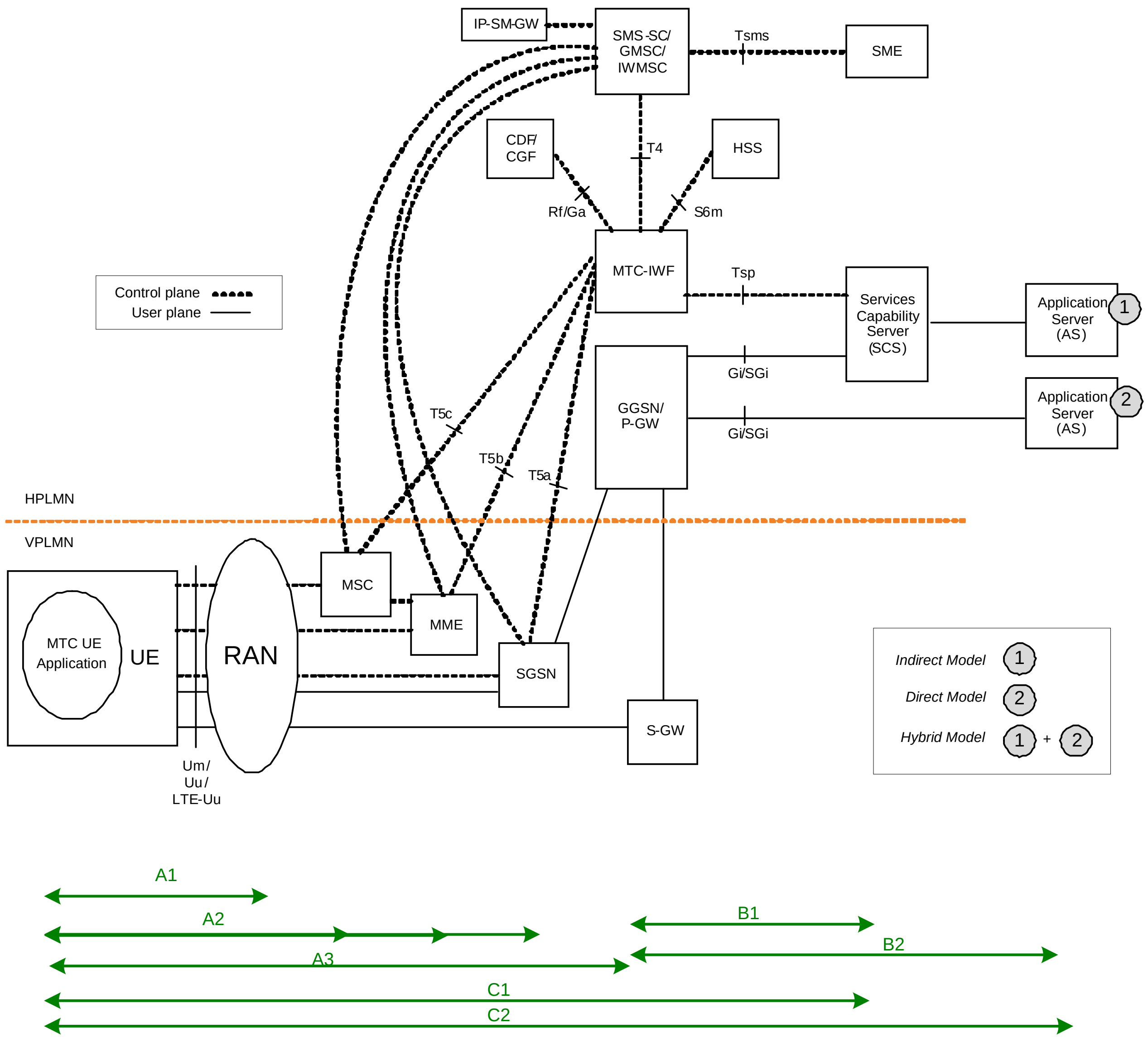


Figure 1: Potential high level security architecture for MTC Architecture for 3GPP Architecture for Machine-Type Communication

Editor’s Note: The termination point of security in the terminal side is FFS, i.e. whether it will be in the UE or in the MTC application.

The following defines one potential high level security architecture for MTC Non-Roaming Architecture. Three different areas are defined. When analysing the security aspects of the key issues it should be considered to which area(s) the key issues is impacting. It should also be noted that the analysed key issues could be related to more than one area, e.g. A and B.

Editor's Note: It is FFS whether single architecture can meet the requirements of all key issues.

Editor's Note: The security architecture needs further refinement.

A) Security for MTC communication between the UE and 3GPP network can be further divided to:

A1) Security for MTC communication between the UE and RAN.

A2) Security for MTC communication between the UE and NAS.

A3) Security for MTC communication between the UE and MTC-IWF.

B) Security for MTC communication between the 3GPP network and an entity outside the 3GPP network can be further divided to:

B1) Security for MTC communication between the MTC server and 3GPP network in indirect deployment model. This can be further divided into security aspects when the MTC server is within the 3GPP network and when it is outside the 3GPP network.

B2) Security for MTC communication between the MTC application and 3GPP network in direct deployment model.

Editor’s Note: B2 is currently FFS.

The communication between MTC server and MTC application is out of 3GPP scope.

C) Security for MTC communication between the an entity outside the 3GPP network and the UE can be further divided to:.

C1) Security for MTC communication between the MTC server and the UE in indirect deployment model.

C2) Security for MTC communication between the MTC application and the UE in direct deployment model.

Editor’s Note: C2 is currently FFS.

NOTE: The entity MTC server used in the present document corresponds to the entity Services Capability Server (SCS) used in TS 23.682 [23]. The entity MTC application used in the present document corresponds to the entity Application Server (AS) used in TS 23.682[23].

5 Description of envisioned security aspects of Machine-Type and other Mobile Data Applications Communications Enhancements

Editor's Note:This clause is intended to provide an overview of the security issues which arise from the use cases and functionalities specified by TS 22.368 [9] and TR 23.888 [10]. Also this clause is intended for the derivation of appropriate security requirements and the description of required solutions regarding the security architecture.

5.1 Device Triggering Enhancements

5.1.1 Issue Details

Editor's Note: This clause is intended to provide details of the security issues with the MTC features specified in the SA1/SA2 TS/TR, explanation of the assumptions and potential impact to the network and devices.

Device triggering issues are defined in TR 23.888 [10], clause 5.8. Several use cases should be considered in this TR as follows:

- A UE receives a trigger indication when it is in detached state.
- A UE receives a trigger indication when it is in attached state and the UE has no PDP context/PDN connection.
- A UE receives a trigger indication when it is in attached state and the UE has a PDP context/PDN connection.

NOTE: The security of Device triggering is covered in key issue-Device triggering and key issue-external interface security. In Device triggering key issue, only the security of trigger indication transferred from PLMN to the UE is considered. The security of trigger indication transferred form MTC server to the PLMN is considered in the key issue-external interface security.

5.1.2 Threats

Editor's Note: This clause is intended to capture the relevant threats and impacts of the issue detailed above.

False network attack: When a UE is in detached state, the attacker can impersonate a network to send a trigger indication to the UE.

Although there are existing mechanisms in the current network to prevent a UE to connect to a false network, there is still an issue. UE used only for MTC are different from normal UEs such that they may need to operate for a long time by using a single battery supply without recharging. False network triggering can awaken a UE and waste its power. So the false network attack is more serious for UE used only for MTC compared to non-MTC communications and therefore we need to improve the network to deal with this security threat.

By means of sending fake triggering messages, an attacker can also obtain information on whether a particular UE is at that particular location at that point in time. If the UE can be linked to an individual, this may have privacy implications.

Tamper attack: The trigger indication may contain the IP@ (or FQDN) and/or TCP (or UDP) port of the application server that the UE has to contact. If the IP@ (or FQDN) and/or TCP (or UDP) port of the application server is tampered by the attacker, the UE may establish the PDN connection to the wrong MTC server or be rejected by the MTC server. It will cause that UE is unable to communicate with the correct MTC server and it will also waste the UE’s power consumption.

When the SMS is used to trigger UEs, SMS spam could be exploited by the attackers to send fake trigger indication. Fake / fraudulent SMS trigger could be sent by malicious SME or by a man-in-the-middle (MitM) on Tsms. Although the human holding a normal UE can make his own judgment, the fake trigger indication sent in SMS spam could be a serious attack on the unattended UEs and will lead to battery draining (particularly for the devices with limited power supply) and improper action. Moreover the fake trigger indication sent in SMS will cause UEs trying to access the network and lead to the waste of network resources. In addition, malicious SMS flooding / spamming will adversely impact resources of HLR, network and UE. Replay of SMS trigger may also happen. It is possible that MitM happens on Tsms interface that can lead to several different attacks, some of which are mentioned above.

User Plane based triggering would be more prone to tampering and fake triggering attacks if application layer integrity solution is not employed, as there is no integrity and replay protection provided to the user plane traffic on the (radio) access link by the core network.

Tracking UEs: The 3GPP network has to keep track of the location of the UE in order to sent the Device trigger to it. Some types of UE can be linked to an individual. Contrary to normal UE, UE used only for MTC are often not under the control of the particular individual (i.e. can not turn it off). As such, the individual has no control over their privacy with respect to location information tracking by the network.

5.1.3 Security Requirements

Editor's Note: This clause is intended to capture the security requirements for solving the key issue. The requirements are mapped to the relevant threats.

5.1.3.0 General

It may not be possible to totally prevent an UE from receiving a trigger indication from a fake network. Therefore it should be studied further whether the device trigger could be protected so that the impact of fake device triggers to the battery lifetime and unauthorized tracking of the UE would be minimized.

The system should provide a mechanism such that only trigger indications received from authorized network entities(e.g. MTC Server, MTC Application, entities acting as a SME) will lead to triggering of UEs.

Upon receiving a trigger indication from a source that is not an authorised network entity, the network should be able to provide the details of the source (e.g. address) to the MTC User.

The system should provide a mechanism to the MTC User to provide a set of authorized network entities.

It has to be ensured that an UE responds only to genuine trigger messages.

The system should ensure that only authentic triggers will be conveyed to the UEs. For 3G/LTE system, trigger indication should be integrity protected.

The system should also provide a mechanism that doesn't require continues tracking of location information of the UE by the network. This prevents privacy implications for those UEs that can be linked to an individual and are not under the direct control of the particular individual.

5.1.3.1 SMS based triggering

There should be protection against malicious SMS flooding and spamming; all these check should be performed in the network.

When the trigger indication is sent in SMS via T_{sms}, the SMS-SC/IP-SM-GW may verify the source of the triggering SMS targeting on unattended UEs to ensure the SMS is from an authenticated and authorized source.

When the trigger indication is received via T_{sp} and sent as MT-SMS to SMS-SC/IP-SM-GW and T4, MTC-IWF should verify the source of trigger request (authenticated and authorized), ensure the integrity of the received trigger request, and ensure that the message has not been replayed, if it's sent from outside the 3GPP network. When SMS-SC/IP-SM-GW receives MT-SMS from MTC-IWF over T4 interface, it knows the short message is for MTC purpose and can be trusted.

When the trigger indication is sent in SMS to SMS-SC/IP-SM-GW via SMS-IWMSC, SMS-SC/ IP-SM-GW is required to distinguish and block MO MTC device trigger messages from normal UEs.

SMS-SC is required to distinguish ordinary short messages from short messages for triggering unattended UEs and act accordingly (e.g selectively block).

For SMS based device trigger, the MTC device trigger message contains TP-PID and Application Port ID. TP-PID is used as the device trigger indication to distinguish trigger message from normal short message, and the SMS Application Port Id is used to identify the application to receive the trigger.

Editor's Note: It is FFS how the SMS-SC/IP-SM-GW can distinguish ordinary short messages from short messages for triggering unattended UEs received over MTCsms interface.

Editor's Note: other suitable network elements for source authorization checking are FFS.

Editor's Note: The system should provide a mechanism to ensure that only intended trigger indications will be conveyed to the UEs.

5.1.3.2 NAS Signalling based triggering

When the trigger indication is sent in NAS signalling to SGSN/MME via MTC_{sp} and T5a/T5b, MTC-IWF should verify the source of trigger request and ensure the integrity of the received trigger request, if it's sent from outside the 3GPP network.

5.1.3.3 User Plane based triggering

The UP based triggering message should be integrity and replay protected. The UP based triggering message may be confidentiality protected.

5.1.4 Solutions

Editor's Note: This section is intended to describe solutions which fulfil the security requirements for the key issue.

5.1.4.0 General

The 3GPP network should keep a list of MTC servers authorized to send trigger to a given UE and the type of trigger the MTC server is authorized to send. The list should contain identity of the UE, MTC server identity and the related allowed triggering. This way, for each trigger, the 3GPP network can verify if the MTC server is allowed to send trigger and whether the trigger is authorized. Clause 5.1.3 describes how authorization is performed at different interfaces.

Editor's Note: Mapping of the device to the device classes is FFS.

5.1.4.1 For offline Device Triggering:

5.1.4.1.0 General

Solution 1: If the UE is in detached state, the UE should be able to validate the network identity when it receives a trigger indication.

The UE should store a temporary identifier of the network it has last attached. The identifier is known to the network side. The network sends the identifier it knows as part of the trigger indication to the UE. When the UE receives a trigger indication, it should compare the network identity from the received indication and the identity it has stored.

If the two network identities match, the UE accepts the trigger indication. Otherwise, the trigger indication is abandoned. When the UE has been successfully triggered, the temporary identifier should be discarded and replaced by a new temporary network identifier which is also known to the network.

Editor's Note: How to securely bind the temporary identity to the trigger message is FFS.

Editor’s Note: There is no valid temporary identifier in the initial state, i.e. when the UE first time attach to the network, this situation needs to be considered.

Solution 2: If the UE is in detached state, the network should protect the trigger indication message by using the last security context stored in the network and the UE.

The UE should store the last security context shared with the attached network. The trigger indication should be protected, at least for integrity (and may be for confidentiality too), by the last shared security context. Only a network that has a valid stored shared security context could generate a valid trigger indication message, and only the UE which has stored a valid security context would be able to validate (i.e., verify integrity and/or decrypt) the trigger indication from the trigger indication message protected by the same security context. If validation of the trigger indication is successful, the network is considered valid by the UE, and would accept the indication. Otherwise, the network is considered invalid, and the trigger indication is abandoned. After the UE has been successfully triggered, a new security context is established and stored at both the UE and the network, to be used to protect (on the network side) and validate (on the device side) a new trigger indication the next time.

Editor's Note: There may be multiple solutions. It is FFS if a new security context is needed.

5.1.4.1.1 Impacts on existing nodes or functionality

For solution 1, a UE should store the last attached network identity. When it receives a triggering indication, it should compare the network identity from the present indication and the stored identity.

For solution 2, a UE and network entities should store the last security context used when the UE was attached in the network.

5.1.4.2 For online Device Triggering

5.1.4.2.1 General description

For the concluded solutions (solutions in TR23.888 v1.6.0 section 7.2.2 [10] and solutions in TS 23.682 v0.1.0 annex A [23]), the current UMTS and LTE access security mechanisms (after the security mechanism is activated) can be used to protect the trigger indication on the radio access interface. The current mechanisms do not ensure that the trigger came from an authorized source.

But in GSM/GPRS network or for user plane based trigger, the trigger indication can only be confidentiality protected using the current security mechanism on the radio access interface.

For UP based triggering, the trigger can only be confidentiality protected using the current access security mechanism on the radio access interface.

In GSM/GPRS network, the trigger can only be confidentiality protected using the current security mechanism on the radio access interface.

In case of GSM/GPRS network or UMTS network using SIM authentication, there is no protection against false triggering on the radio access network.

Editor's Note: For any new SA2 solution on device triggering, SA3 need to do security analysis.

5.1.4.2.2 Solution 1: Triggering via NAS signalling

A Device triggering mechanisms currently being considered in SA2 TR 23.887 [26] is triggering via T5 and using NAS signalling (e.g. a new information element in an existing NAS message or a new NAS message). One possibility under discussion in SA2 is that the device trigger may possibly also be sent from the network to the UE using SMS format but NAS as a transport. In this case, current NAS security mechanisms can be used to provide the security for the NAS layer. After NAS SMC, NAS security is activated. All NAS signaling messages should be integrity-protected according to TS 33.401 [13], and therefore current LTE security mechanisms ensure that the trigger indication is not tampered with. In this case the SMS trigger will also benefit from the integrity protection of NAS signalling in LTE.

Source verification needs to be considered which in this context is understood to mean that the UE can verify that the source of the trigger is a valid MTC server. This could be achieved in the following ways:

Option A

UE trusts the 3GPP network sending the NAS integrity protected trigger. In this case the UE could be configured with identities of trusted visited 3GPP networks. (Somewhat analogically as trusted non3GPP access networks can be configured in the UE in TS 33.402 [15].) In this context trusted visited 3GPP network would mean networks which are trusted to have a secure path from the visited 3GPP network to the home 3GPP network to convey the device trigger. In addition the UE could be configured with information if there exists a secured Tsp interface from the MTC server to the 3GPP home network, so that it can be ensured that only trigger indications received from authorized MTC Servers will lead to triggering of UEs “belonging” to that MTC server.

When the UE then receives a NAS integrity protected trigger, it can, after verifying NAS integrity protection, verify whether the condition regarding the visited and home 3GPP network described above are met. If they are met, the trigger can be accepted.

MME should not send the trigger in a NAS message without integrity protection. If there is no NAS integrity protection of the trigger or if the 3GPP network is not trusted, the UE could discard the trigger and send a Reject message to MME and MTC-IWF with a proper cause or alternatively look deeper into the trigger if end-to-end protection was applied.

When MME receives a reject response from UE with a cause indicating no integrity protection or integrity check failure, MME can

- Initiate 3GPP AKA procedure towards UE so that when there is security context shared between them MME can forward the trigger;
- Or forward the reject message to MTC-IWF, so that MTC-IWF can choose another route to send the trigger.

Editor's Note: It is FFS how the network elements can distinguish ordinary short messages from short messages for triggering unattended UEs

Editor's Note: It is FFS if both of the following cases or only one of them are possible, i.e. that the device trusts the home network always to have the external interface in place or whether the device cannot always trust the home network to have the external interface in place.

Editor's Note: The above solution is intended for LTE, it is FFS how to protect trigger indication in GSM/UMTS.

Editor's note: The benefits of the proposed solution should be weighed against the cost of increased battery consumption.

An alternative approach is that the MTC server could trigger the UE through a GBA-push process via NAS signalling.

Option B

UE could verify whether the trigger is coming from an authorized MTC IWF.

When the UE receives the message from MTC-IWF, it should perform integrity check first to verify whether the message is sent from an authorized MTC-IWF. When the integrity check is completed successfully, the UE will decrypt the message and respond to it accordingly. The verification is done by performing integrity check of the received trigger message with the integrity key that the UE and the MTC-IWF share, as described in Solution 6.

5.1.4.2.3 Solution 2: Solution for fake SMS triggering from normal UE in the same network as UE used only for MTC

The fake triggering SMS can be blocked on the network side. As instructed in the following figure, the SMS-SC can receive short message from MTC Server via Tsms interface (as shown by the green line) or T4 interface (as shown by the blue line) or from SMS-IWMSC (as shown by the red line).

This solution is to block any SMS to UE that comes from SMS-GMSC

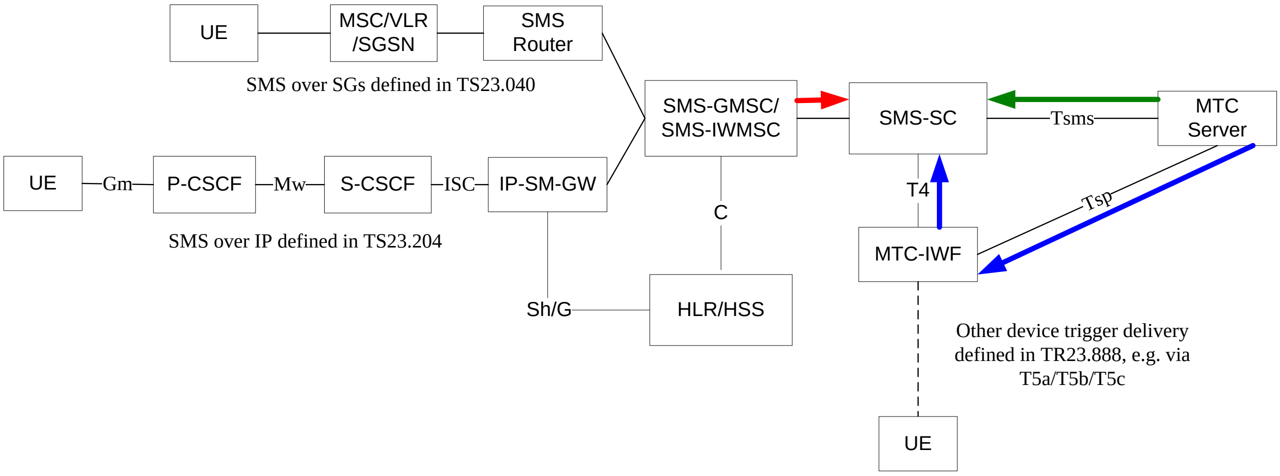

UE
MSC/VLR /SGSN
SMS Router
SMS over SGs defined in TS23.040
SMS-GMSC/ SMS-IWMSC
SMS-SC
Tsms
MTC Server
UE
Gm
P-CSCF
Mw
S-CSCF
ISC
IP-SM-GW
SMS over IP defined in TS23.204
C
T4
Tsp
MTC-IWF
Sh/G
HLR/HSS
Other device trigger delivery defined in TR23.888, e.g. via T5a/T5b/T5c
UE

Figure 7.1.3-1 Triggering short message delivery

When SMS-SC receives short message from MTC Server via Tsms, the current external interface security can check whether the MTC Server is authorized to send the trigger to the UE. If it is, the SMS-SC continues to send the short message. When SMS-SC receives short message which is forwarded by MTC-IWF via T4 interface, the SMS-SC considered T4 interface is trusted and continues to send the short message. Because the MTC-IWF can authenticate with MTC server and ensure that only the authorized MTC Server triggers the UE according functionality of MTC-IWF defined in TR23.888 [10] and external interface security solution defined in the current document. When the SMS-SC receives short message from SMS-IWMSC, it forwards the short message to SMS-GMSC following normal SMS procedure but with a check indication. Then SMS-GMSC forwards the target UE's identifier in the short message to HLR/HSS and obtains serving MSC/SGSN routing information for the target UE from HLR/HSS. After HLR/HSS receives the target UE's identifier, it inquires the corresponding subscription data and checks whether the target UE is UE used for MTC based on the target UE's identifier and inquiry result. If the target UE is used for MTC, HLR/HSS sends inquiry result or reject indication to the SMS-GMSC/IP-SM-GW and SMS procedure terminates. If the target UE is not used for MTC, HLR/HSS sends inquiry result or confirm indication to the SMS-GMSC/IP-SM-GW and SMS procedure continues.

Editor's Note 1: To get clarification from SA2, whether it is possible for the HSS to distinguish the target device is a normal UE or UE used only for MTC.

Editor's Note 2: It is FFS, whether this solution can be combined with home network routing as defined in TR 23.840 [39] so that SMSs from external networks towards UEs used only for MTC can also be blocked.

5.1.4.2.4 Solution 3: Solutions protecting SMS triggering

A. Network based SMS payload filtering

Protection against SMS spoofing can be provided if the HPLMN implements home network routing for SMS (TR 23.840 [39]) and implements filters in the home network SMS infrastructure to ensure that MTC trigger SMSs can only be sent from an authorised whitelist of senders. This approach requires that the SMS infrastructure can filter based on payload contents for all SMS from untrusted sources.

Data of routing information, serving node information can be pushed from HSS/HLR and saved locally in SMSC/SMS-GMSC.

Editor's Note: it's FFS how the HSS can push the info to the SMSC when there are changes of subscription.

B. UE based SMSC whitelisting

In the absence of SMS home routing, an UE could be configured to only accept MTC triggers from whitelisted HPLMN SMSCs. Assuming SMS filtering at these whitelisted HPLMN SMSCs then this could protect against the most basic form of SMS spoofing. Challenges with this solution are how to provision and maintain the SMSC whitelist on the UE and the SMS filtering at the whitelisted HPLMN SMSCs .

C. Source authentication

Even home network routed SMS combined with SMS payload filtering is vulnerable to attacks where network internal nodes or network signalling links are compromised. If such attacks need to be mitigated, or if home network routing is not provided, then some form of cryptographic protection of MTC triggers is needed between the MTC server and the UE. Three possible approaches are listed below:

NOTE: The assumption "if home network routing is not provided" does not hold when trigger source is outside network, because the trigger source does not and should not have knowledge whether network will perform payload filtering.

- **(U)SIM application toolkit security**: In this approach the trigger message is protected at the MTC server and sent directly to a (U)SIM application toolkit on the (U)SIM according to TS 23.048 [38]. If the message is authenticated by the (U)SIM (based on a pre-shared symmetric key), then the (U)SIM can forward the message to the UE for processing. With this method, UEs would need to be pre-provisioned to only act on triggering messages that have been verified by the (U)SIM application toolkit security mechanism.

Editor's Note: It is for further study whether USIM application toolkit security can be used when the MTC server is outside the operator's domain.

- **GBA push (either GBA_ME or GBA_U based)**: In this approach GBA_Push, as specified in TS 33.223 [22], is used to secure the trigger message between the MTC server and the UE. Compared to the (U)SIM application toolkit approach, a new pre-shared symmetric key is not needed – instead the UE can establish the GBA_Push keys by leveraging the existing AKA credentials that are used for network access security. With this method, UEs would need to be pre-provisioned to only act on triggering messages that have been verified using GBA push.

- **Application based End to End protection**: As mentioned in the TS 23.682 [23], when using Tsms based SMS triggering, the trigger to the UE is encapsulated in a MT SMS as over-the-top application by the SME. So when the trigger indication is sent over Tsms, the network entity acting as SME should apply end-to-end integrity and replay protection and the MTC application on the UE should verify the source of the trigger and ensure the integrity of the received trigger request. A possible mechanism for application layer key establishment between the UE and the MTC application may be using the GBA push mechanism. The mechanism to verify the integrity of the trigger message by the MTC application is out of scope of this specification.

5.1.4.2.5 Solution 4: Triggering via User plane

SA2 is considering solutions related to User plane based trigger delivery [TR 23.888 v1.6.0 [10]]. In order to prevent sending fake trigger message through the radio access link, the trigger message could be protected using the AS security mechanisms (User Plane confidentiality protection). UP based triggering messages could be confidentiality protected according to TS 33.401 [13] for LTE and according to TS 33.102 [12] for 3G, and therefore current LTE and 3G security mechanisms can ensure that the trigger indication is confidentiality protected.

When the trigger indication is sent in user plane, the MTC Server/ MTC application on the MTC user domain should apply end-to-end integrity and replay protection and the MTC application on the UE should verify the source of the trigger and ensure the integrity of the received trigger request. The mechanism to verify the integrity of the trigger message by the MTC application is out of scope of this specification.

The UE should discard the trigger if it is not end to end integrity and replay protected by the MTC server.

5.1.4.2.6 Solution 5: Using GBA Push to secure Device triggering procedure over Tsp and T4

End to end protection of the device trigger is regarded to be provided at the application layer and therefore be out of scope for 3GPP specifications. However, GBA push as defined in TS 33.223 [22] and e.g. Generic Push Layer as defined in TS33.224 [25] can be used to protect the device trigger.

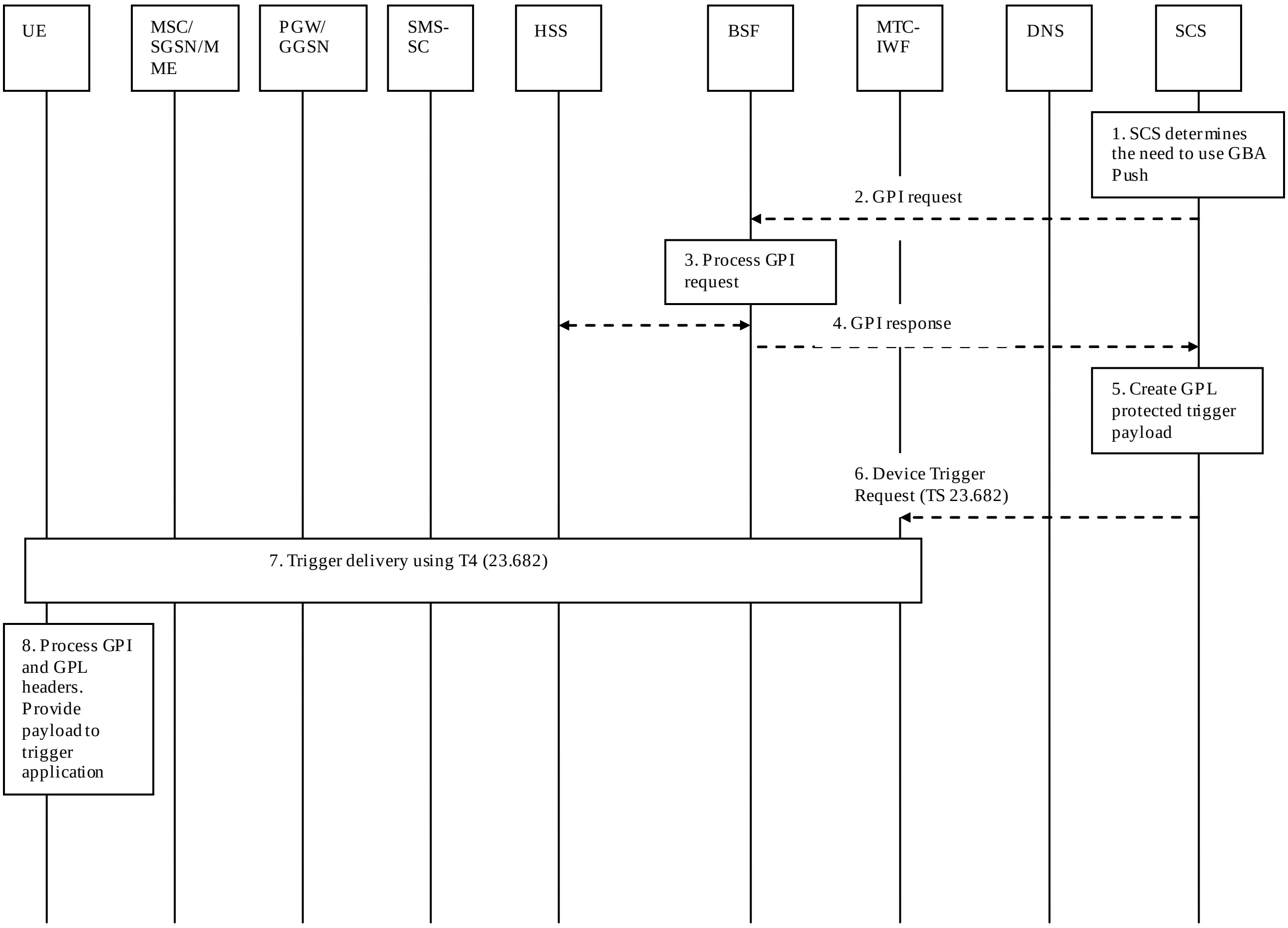

UE
MSC/ SGSN/MME
PGW/ GGSN
SMS-SC
HSS
BSF
MTC-IWF
DNS
SCS
1. SCS determines the need to use GBA Push
2. GPI request
3. Process GPI request
4. GPI response
5. Create GPL protected trigger payload
6. Device Trigger Request (TS 23.682)
7. Trigger delivery using T4 (23.682)
8. Process GPI and GPL headers. Provide payload to trigger application

Figure 5.1.4.2.6-1: Security for Device triggering procedure over Tsp

The following steps may be performed before step 2 in the Device triggering procedure over Tsp in clause 5.2.1.

Precondition: To be able to use GBA push -based services the SCS needs to be provided with the following information regarding the UE as is defined in Annex B of TS 33.223 [22]. The mechanism how the information is provided is out of the scope of the specification.

- *UE_id*: This is the External Identifier specified in TS 23.682 [23] or MSISDN.

NOTE: According to TS 23.682 [23] the use of IMSI outside the 3GPP operator domain is dependent on the operator policy.

NOTE: According to TS 33.223 [22] a public identity shall correspond uniquely to a single private identity.

- *Push delivery method*: This can be left empty as the MTC-IWF will select the trigger delivery method.
- *Transport address (UE_trp)*: This may be left empty as the MTC-IWF will select the trigger delivery method. In case the UE_id is MSISDN the transport address may indicate the same
- *BSF address*: FQDN of the BSF
- *UICC application to use*: This is the Appl_Lbl if the UICC application to use is not uniquely determined by the UE transport method and/or UE_Id.
- *ME is GPL capable or not*: ME needs to be GPL capable.
- *UICC is GPL capable or not*: UICC needs to be GPL capable when GPL protected message is delivered to targeted UICC application (e.g. USIM).
- *GPL_ME or GPL_U*: GPL_ME or GPL_U when the GPL protected message is delivered to targeted UICC application (e.g. USIM).

Editor's Note: This is FFS to determine what would be the applications that need to rely on GPL_U to benefit from higher level of security.

1. The SCS (acting as NAF) determines the need to use GBA Push in order to establish common security associations in the SCS and UE for the purpose of protecting the device trigger.
2. The SCS sends a GPI request to the BSF as defined in TS 33.223 [22]. The request is as defined in TS 33.223 [22] with the following profiling:
   - *UE_Id_type* indicates public user identity, i.e. External Identifier or MSISDN.
   - *Ua security protocol Id* in the NAF-Id indicates GPL.
   - *U/M* indicates the use of GBA_ME or GBA_U.
   - *GSID (GAA Service Id)* indicates the service requesting use of GBA push.

   NOTE: An appropriate value is ffs and needs to be registered in normative phase. This could be e.g. "MTC secure trigger".

3. The BSF processes the GPI request and contacts the HSS according to TS 33.223 [22].

4. The BSF sends the GPI response including e.g. GPI and NAF keys to the SCS according to TS 33.223 [22].

5. The processing at the SCS is as follows:
   - The SCS creates the GPL-SA as defined in TS 33.224 [25].
   - The SCS creates the protected GPL message including the trigger payload in the GPL payload as defined in TS 33.224 [25]. Combined GPL delivery is used, i.e. the GPI is included in the GPL message.

   NOTE: TS 33.224 [25] allows sending the GPI separately or combined with the GPL message. Since it is specified in TS 23.682 [23] that the SCS sends a (i.e. one) Device Trigger Request to the MTC-IWF and the transport method for the device trigger is selected by the MTC-IWF, it is recommended that combined delivery is used.

6. When the SCS sends the Device Trigger Request to the MTC-IWF (in step 2 of clause 5.2.1 in TS 23.682 [23]), the trigger payload includes the protected GPL message. Within the Device Trigger Request the SCS also indicates to

the MTC-IWF that the trigger is protected. In case of trigger delivery using T4 this allows the MTC-IWF to select an appropriate SMS header parameter or other parameter to differentiate the secure trigger from a normal trigger.

NOTE: An appropriate SMS header parameter or other parameter needs to be decided by stage 3 groups in normative phase.

7. The device trigger is transported to the UE as defined in TS 23.682 [23]. As the trigger may not fit into one SM the SMS-SC does any necessary segmentation for larger messages.

8. When the UE receives the device trigger, the trigger is destined to the secure trigger application based on appropriate SMS header parameter or other parameter indicating a secure trigger and indicate the used security protocol.

NOTE: An appropriate SMS header parameter or other parameter for application secured MTC trigger needs to be decided by stage 3 groups in normative phase.

- The GPL and GPI processing is performed as defined in TS 33.223 [22] and TS 33.224 [25].

- After this any information contained within the trigger payload is forwarded to the related or addressed UE-application as specified in TS 23.682 [23].

5.1.4.2.7 Solution 6: Secure Trigger Delivery with Security Association between MTC-IWF and UE

Application level security is out-of-scope of 3GPP SA3 activity thus only way to deliver a trigger securely is to secure all hops between the SCS and the UE. One of the solution is to have security association between the MTC-IWF and the UE. The MTC-IWF will verify whether Tsp is secured and then send the trigger together to the UE.

Editor's Note: Detailed solution for establishing the security association between MTC-IWF and UE is ffs.

5.1.4.2.8 Solution 7: Using regular GBA and GPL to secure Device triggering procedure over Tsp and T4

Editor's Note: This is an example for Tsp and T4. It is FFS how this solution can be generalized to cover also Tsms case and entities other than the SCS applying the regular GBA and GPL security.

End to end protection of the device trigger is regarded to be provided at the application layer between the MTC application in the UE and MTC application in the application server and therefore be out of scope for 3GPP specifications. When the device trigger protection is applied between the SCS and UE, then 3GPP is able to provide a trigger transport service to the SCS. This can be regarded as another value added service that the SCS offers to the MTC application servers in addition to any other value added services that the SCS provides.

In case GBA is used to provide device trigger protection between the SCS and UE, the SCS takes the role of NAF. The following describes how regular GBA as defined in TS 33.220 [21] and Generic Push Layer as defined in TS33.224 [25] with extensions as explained below can be used to protect the device trigger between the SCS and the UE.

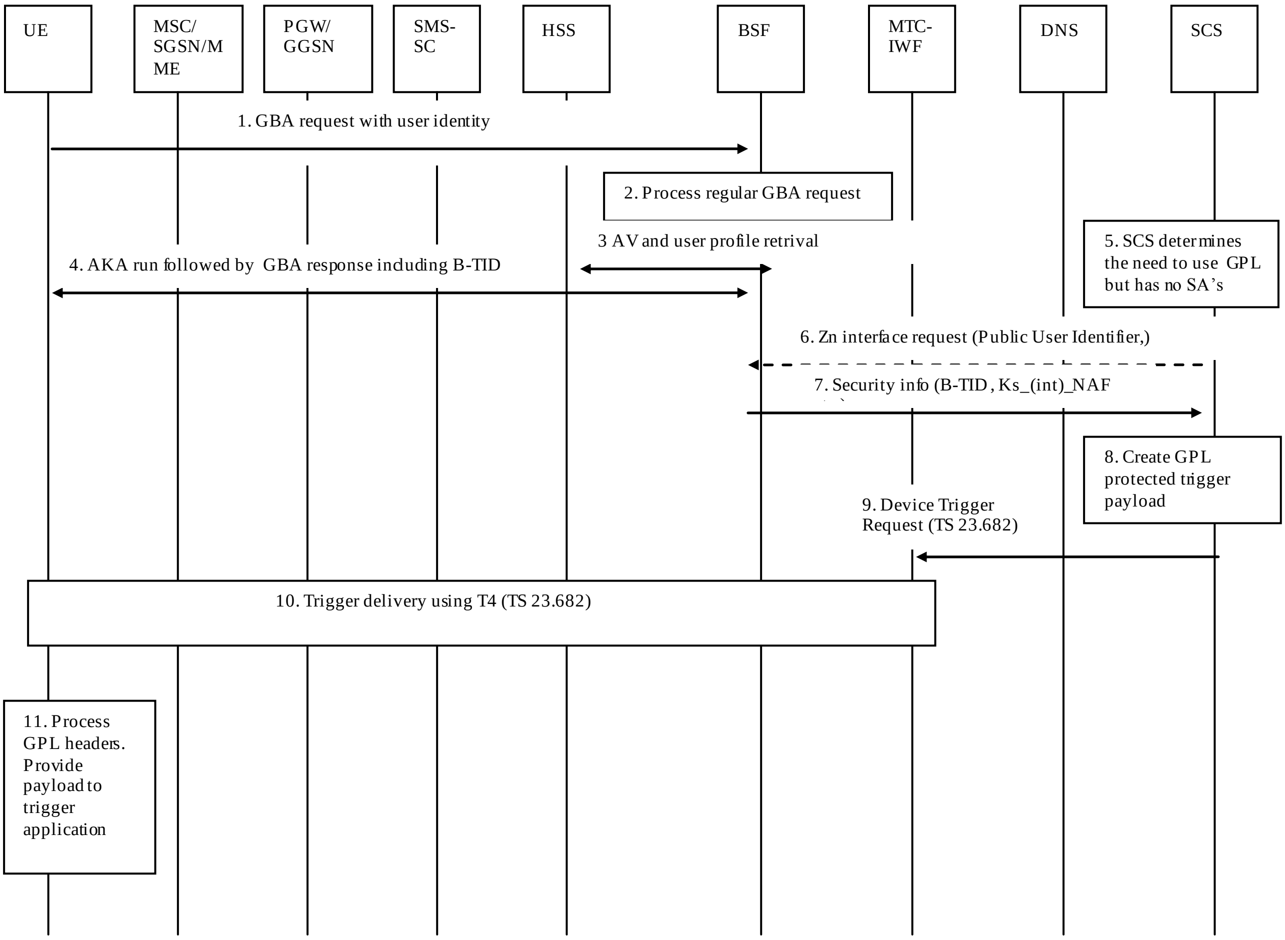

UE
MSC/ SGSN/MME
PGW/ GGSN
SMS-SC
HSS
BSF
MTC-IWF
DNS
SCS
1. GBA request with user identity
2. Process regular GBA request
3 AV and user profile retrival
4. AKA run followed by GBA response including B-TID
5. SCS determines the need to use GPL but has no SA's
6. Zn interface request (Public User Identifier,)
7. Security info (B-TID, Ks_(int)_NAF
8. Create GPL protected trigger payload
9. Device Trigger Request (TS 23.682)
10. Trigger delivery using T4 (TS 23.682)
11. Process GPL headers. Provide payload to trigger application

Figure 7.1.3-3: Security for Device triggering procedure using regular GBA and GPL over Tsp and T4

The following steps are performed following the Device triggering procedure over Tsp in clause 5.2.1 of TS 23.682 [23].

Precondition: To be able to use regular GBA -based services together with GPL the SCS needs to be provided with the following information regarding the UE. The information below is based on the information needed for GBApush in Solution 5. The mechanism how the information is provided is out of the scope of the specifications.

- *UE_id*: This is the External Identifier specified in TS 23.682 [23] or MSISDN.

NOTE 1: According to TS 23.682 [23] the use of IMSI outside the 3GPP operator domain is dependent on the operator policy.

According to TS 33.223 [22] a public user identity (External identifier or MSISDN) corresponds uniquely to a single private user identity (IMSI or IMPI). This restriction also applies in this solution even though GBA push is not used.

If MSISDN is used as delivery address, then the USIM associated with that MSISDN should be used. This is so because a SMS will only reach the UE when the USIM corresponding to the MSISDN is active in the UE.

- *Push delivery method*: This information is not needed for this solution as the MTC-IWF will select the trigger delivery method.
- *Transport address (UE_trp)*: This information is not needed as the MTC-IWF will select the trigger delivery method.
- *BSF address*: FQDN of the BSF
- *ME is GPL capable or not*: ME needs to be GPL capable.
- *UICC is GPL capable or not*: UICC needs to be GPL capable when the GPL protected message is delivered to targeted UICC application (e.g. USIM).

- *GPL_ME or GPL_U*: GPL_ME ME or GPL_U when the GPL protected message is delivered to targeted UICC application (e.g. USIM).

Editor's Note: This is FFS to determine what would be the applications that need to rely on GPL_U to benefit from higher level of security.

- *ME is regular GBA capable or not*: ME needs to be regular GBA capable. Whether the UE is regular GBA capable or not can be an optional configuration parameter in the SCS.

The UE is assumed to have run regular bootstrapping with BSF as shown in steps 1 – 4 for example as a result of having set up a Secure Connection between the UE and SCS.

1. The UE shall request bootstrapping via the Ub interface with the BSF in regular GBA as described in TS 33.220 [21].

2. The BSF shall process the GBA request from the UE as described in TS 33.220 [21].

3. The BSF shall retrieve AV and user profile from HSS as described in TS 33.220 [21].

4. The BSF and UE perform Ub run as described in TS 33.220 [21].

5. The SCS determines the need to trigger the device, e.g. due to that the MTC application server requested the SCS to trigger the device using GBA to protect the trigger. The SCS (acting as a NAF) shall determine the need to contact the BSF to find out if common security associations have been established in the BSF and UE in regular GBA, for the purpose of protecting the device trigger in GPL with these security associations.

6. The SCS shall send a Zn interface request to the BSF as defined in TS 33.220 [21] including Public User Identity (External Identifier or MSISDN) instead of B-TID. The request is defined with the following profiling:

Editor's Note: It must be clarified that the B-TID can be left out from the message exchange.

- *UE_Id_type* indicates public user identity (External Identifier or MSISDN)

- *Ua security protocol Id* in the NAF-Id indicates GPL.

- *GSID (GAA Service Id)* indicates the service requesting use of GBA.

Editor's Note: An appropriate value is ffs and needs to be registered in TS 29.109 [37]. This could be e.g. "MTC secure trigger".

7. The BSF shall process the modified Zn interface request and if the BSF has common security associations established with this UE as identified in the Zn request, then the BSF shall send the modified Zn response to the SCS (NAF) including, NAF keys (Ks_(ext/int)_NAF) and other security information to the SCS according to TS 33.220 [21] and extended with the B-TID.

8. When the SCS receives the Zn response including the B-TID from the BSF, then the processing at the SCS is as follows:

- The SCS shall create the GPL-SA by assigning the RAND@NAF-Id as the downlink security association identifier (DL SAID) in the GPL-SA. RAND is received from the B-TID. The UL GPL SAID is set to the same value as the DL GPL SAID.

NOTE: The DL GPL SA ID takes the form RAND@NAF-Id instead of RAND@'naf' defined in TS 33.223 [22] in order to provide the UE with NAF-Id for for the Ks_(int)_NAF computation.

- The SCS shall create the protected GPL message including the trigger payload in the GPL payload as defined in TS 33.224 [25]. Since SCS is re-using an existing bootstrapping run in this case, combined GPL delivery can not be used, i.e. the GPI can not be included in the GPL message.

9. When the SCS sends the Device Trigger Request to the MTC-IWF (clause 5.2.1 in TS 23.682 [23]), the trigger payload includes the protected GPL message. Within the Device Trigger Request the SCS also indicates to the MTC-IWF that the trigger is protected. In case of trigger delivery using T4 this allows the MTC-IWF to select an appropriate SMS header parameter or other parameter to differentiate the secure trigger from a normal trigger.

NOTE: An appropriate SMS header parameter or other parameter needs to be decided by stage 3 groups in normative phase

10. The device trigger is transported to the UE as defined in TS 23.682 [23]. As the trigger may not fit into one SMS the SMS-SC does any necessary segmentation for larger messages.

11. When the UE receives the device trigger, the trigger is destined to the secure trigger application based on appropriate SMS header parameter or other parameter indicating a secure trigger and indicate the used security protocol.

NOTE: An appropriate SMS header parameter or other parameter for application secured MTC trigger needs to be decided by stage 3 groups in normative phase.

- The secure trigger application in the UE prepares a NAF SA by computing the Ks_(int)_NAF from the Ks (established from regular GBA) identified by the RAND part in the downlink security association identifier in GPL. The NAF-Id for the Ks_(int)_NAF computation is received from the domain part of the DL GPL SA ID.

- The UE initialises the GPL SA and processes the GPL as described in in TS 33.224 [25].

- After this any information contained within the trigger payload is forwarded to the related or addressed UE-application as specified in TS 23.682 [23].

5.1.4.2.9 Solution 8: Using GBA Push to secure Device triggering procedure over Tsms

When entities other than the SCS apply GBA push security for device triggering (i.e. an SME in the generic case) over Tsms, the protection of the device trigger happens end-to-end on application level and therefore the exact security protocol and other mechanisms to protect the device trigger are out of scope of 3GPP. However, 3GPP can provide GBA push-based keys used for the protection.

The flow below illustrates how GBA push can be used to provide keys for protection of device trigger (and also to protect other application level communication) between the UE and an SME. SME act as a push-NAF. It should be noted that the MTC Application Server also may take the role of SME and send a device trigger over Tsms.

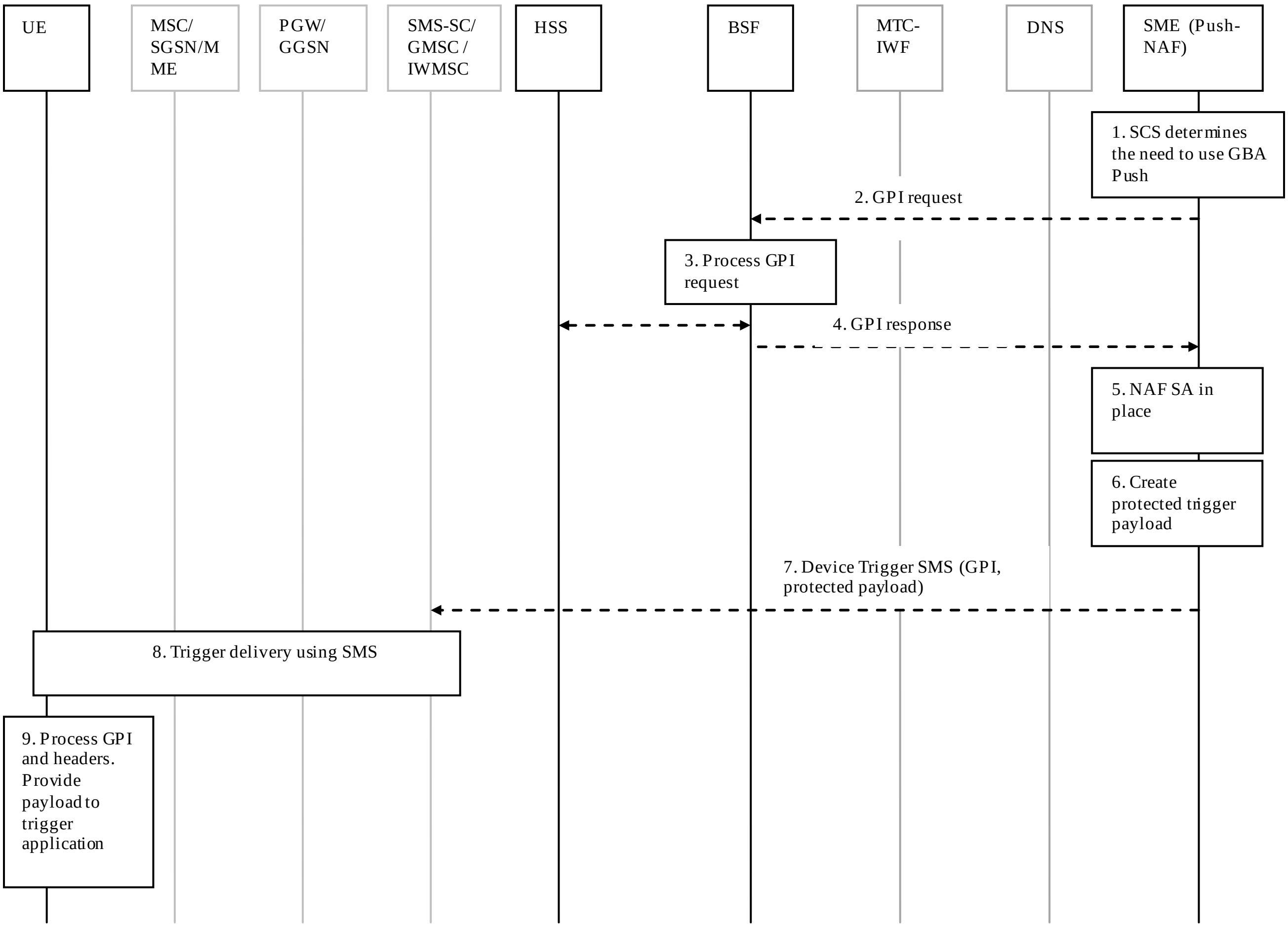

UE
MSC/ SGSN/MME
PGW/ GGSN
SMS-SC/ GMSC / IWMSC
HSS
BSF
MTC-IWF
DNS
SME (Push-NAF)
1. SCS determines the need to use GBA Push
2. GPI request
3. Process GPI request
4. GPI response
5. NAF SA in place
6. Create protected trigger payload
7. Device Trigger SMS (GPI, protected payload)
8. Trigger delivery using SMS
9. Process GPI and headers. Provide payload to trigger application

Figure 5.1.4.2.9-1: Security for Device triggering procedure over Tsms

The following steps may be performed before step 2 in the Device triggering procedure over Tsp in clause 5.2.1.

Precondition: To be able to use GBA push -based services the SME acting as a push-NAF needs to be provided with the following information regarding the UE as is defined in Annex B of TS 33.223 [22]. The mechanism how the information is provided is out of the scope of the specification.

- *UE_id*: This is the MSISDN.

NOTE 1: According to TS 23.682 [23] the use of IMSI outside the 3GPP operator domain is dependent on the operator policy.

NOTE 2: According to TS 33.223 [22] a public identity shall correspond uniquely to a single private identity.

- *Push delivery method*: This is set to SMS.
- *Transport address (UE_trp)*: This is set to External Identifier or MSISDN In case the UE_id is MSISDN the transport address may indicate the same.
- *BSF address*: FQDN of the BSF
- *UICC application to use*: This field may be left empty as the UICC application to use is uniquely determined by the UE transport method (i.e. SMS) and/or UE_Id (External Identifier or MSISDN).

NOTE 3: Since the security protocol to be used for protecting the device trigger is decided by the MTC application, the configuration information related to the security protocol is out of scope of 3GPP. However, if the MTC application decides to use, e.g. GPL, then the configuration considerations related to GPL from solution 5 “Using GBA Push to secure Device triggering procedure over Tsp and T4” would apply also here.

1. The SME (acting as push-NAF) determines the need to use GBA Push for the purpose of protecting the device trigger.

2. The SME sends a GPI request to the BSF as defined in TS 33.223 [22]. The request is as defined in TS 33.223 [22] with the following profiling:

- *UE_Id_type* indicates public user identity, i.e. External Identifier or MSISDN.
- *Ua security protocol Id* in the NAF-Id indicates the used security protocol.
- *U/M* indicates the use of GBA_ME or GBA_U.
- *GSID (GAA Service Id)* indicates the service requesting use of GBA push.

NOTE: An appropriate value is ffs and needs to be registered in TS 29.109 [37] in normative phase.

3. The BSF processes the GPI request and contacts the HSS according to TS 33.223 [22].

4. The BSF sends the GPI response including e.g. GPI and NAF keys to the SME according to TS 33.223 [22].

5. The SME stores the received information from the BSF in a NAF SA as described in TS 33.223 [22].

6. The SME uses the NAF SA to protect the device trigger. Any suitable protocol chosen by the MTC Application Server, for example GPL as defined in TS 33.224 [25], could be used.

- Depending on the used security protocol or other considerations, combined or separate GPI delivery is used. This is out of scope of 3GPP and eventually for the SME to decide.

7. When the SME sends the Device Trigger SMS to the SMS-SC, the trigger payload includes the protected message. Protection is indicated by means of the MTC application which are not visible to lower layers.

8. The device trigger is transported to the UE via SMS architecture. Trigger SMS filtering as defined in TS 23.682 [23] may be applied on the way. As the trigger may not fit into one SM the SMS-SC does any necessary segmentation for larger messages.

9. When the UE receives the device trigger, the trigger is destined to the MTC application based on the SMS header parameter or other parameter.

NOTE: An appropriate SMS header parameter or other parameter for application secured MTC trigger needs to be decided by stage 3 groups in normative phase.

- The GPI processing is performed as defined in TS 33.223 [22].
- After this any information contained within the trigger payload is processed by the MTC application.

5.1.4.2.10 Impacts on existing nodes or functionality

Solution 2:

- SMS-SC needs to differentiate the regular SMS from trigger SMS.
- SMS-GMSC/IP-SM-GW needs to differentiate the regular SMS from trigger SMS.
- HSS needs to store MTC related subscription data (i.e. whether a target UE is UE used only for MTC or not) and needs to judge whether a target UE is UE used only for MTC or not because SA2 has not defined this functionality for HSS.
- The interface between SMS-SC and SMS-GMSC and C/Sh/G interface needs to support the check indication during normal SMS procedure.

Solution 3-A: Network based SMS payload filtering:

- SMS-SC needs to differentiate the regular SMS and trigger SMS
- SMS-SC needs to support as SMS whitelist filtering based on TP Protocol Id to distinguish whether SMS is triggering or not.

Solution 3-B: UE based SMSC whitelisting:

- UE needs to support SMSC whitelist
- SMS filtering needs to be supported by the whitelisted HPLMN SMSCs.

5.1.5 Evaluation

Editor's note: This section contains evaluation (possibly including cost and benefit trade-off analysis) of candidate solutions enumerated in the preceding General Description subsections.

The following provides an evaluation of Device Triggering mechanisms on each interface. It does not take into account possible end to end protection of DT.

External interface:

T4 solution: Trigger indication is sent over Tsp from MTC server to MTC-IWF. Requirements exist in the current document that MTC-IWF should verify the integrity of the device trigger and that it is sent by an authorized source. This could be achieved with the help of the MTC-SEG. Checking a received device trigger that has come over the T4 to SMSC should not be a problem as MTC-IWF and SMSC are within the same operator.

Additionally, the MTC server may send a device trigger over Tsms to SMSC. This poses the problem identified in the current document "*SMS-SC is required to distinguish ordinary short messages from short messages for triggering unattended UEs and act accordingly (e.g. selectively block)*." The TP Protocol Id in the SM header is used to distinguish a device trigger SM from an ordinary SM in the SMS-SC (see for further details in TS 23.040). A new TP-PID value to identify a device trigger SM was defined for this purpose. The TP Protocol Id is conveyed all the way to the UE, and it can be used by the intermediate nodes as well as the UE to distinguish ordinary short messages from short messages for triggering. The SMSC should then check incoming SMSs and accept device trigger SMSs only from authorized MTC servers. This approach requires that the SMS infrastructure can filter based on SMS headers for all SMS from untrusted sources. This could be achieved with the help of the MTC-SEG.

T5 solution: Tsp interface is the same for T4 solution and T5 solution. Therefore the same considerations apply.

UP solution: Trigger UP message is sent over Gi/SGi from MTC server to GGSN/PGW. This seems to pose a requirement that the GGSN/PGW would need to filter out unauthorized triggers. This could be achieved by only allowing traffic to the UE from an authorized MTC server (which is assumed not to send false triggers) Alternatively achieving the requirement would require that trigger UP messages can be distinguished from other user plane data messages over Gi/SGi, and the GGSN/PGW would need to possibly check all incoming traffic over Gi/SGi and filter out unauthorized trigger UP messages. The latter seems a major task to do.

Interface between home and serving network:

T4 solution: The trigger SMS is sent from SMSC as follows: to MME via MSC in LTE, to SGSN in PS UTRAN, to SGSN in GPRS. This also poses the problem that the serving network node is required to distinguish ordinary short messages from short messages for triggering unattended UEs and act accordingly (e.g. selectively block). The TP Protocol Id in the SM header is used to distinguish a device trigger SM from an ordinary SM in the SMS-SC (see for further details in TS 23.040). A new TP-PID value to identify a device trigger SM was defined for this purpose. The TP Protocol Id is conveyed all the way to the UE, and it can be used by the intermediate nodes as well as the UE to distinguish ordinary short messages from short messages for triggering. The MME/SGSN in the serving network should then check incoming SMSs and accept device trigger SMSs only from an authorized source (e.g. SMSC) in the HPLMN. Checking a received device trigger SMSM should not be a problem when MME/SGSN and SMSC are within the same operator. This approach requires that the SMS infrastructure can filter based on SMS headers for all SMS from untrusted sources.

It seems additional measures may be needed in case of roaming to do the check. One possible solution is that trigger SMSs are always sent home routed via a dedicated SMSC. Then the MME/SGSN node, when it receives a trigger SMS, contacts the UEs HSS to get information about whether the trigger SMS was sent by an authorized source in the HPLMN. If the received information from the HSS matches the source information in the trigger SMS, the trigger SMS is forwarded to the UE. The requested information could include, e.g. address of the authorized SMSC, information if there is an outstanding trigger SMS for the UE, or the even the reference number of the trigger SMS.

T5 solution: SA2 is discussing two options: Device trigger can be sent over T5 as an SMS or as a generic signaling message. In case of SMS the same considerations apply as for T4 solution above with the exception that the source node is MTC-IWF and not SMSC. In case of generic signaling message is used it seems that "additional" checking is not needed when the trigger message is sent as a generic signaling message as it can be regarded as a normal signalling message and existing protection mechanisms for signalling messages should apply.

UP solution: Trigger UP message is sent from GGSN/PGW to SGSN/SGW. If filtering was not done at the GGSN/PGW, this would require that trigger UP messages can be distinguished from other user plane data messages at SGSN/SGW, and the SGSN/SGW would need to possibly check all incoming traffic and filter out unauthorized trigger UP messages. This seems a major task to do.

Radio interface:

T4 solution: Device trigger is sent as MT SMS. MT SMS in control plane is integrity protected in LTE and UTRAN but not in GERAN. MT IP-SMS (if applicable) does not provide integrity protection in any network.

T5 solution: Device trigger is sent as MT SMS or a NAS message (SA2 is discussing two options). In case MT SMS the same considerations as for T4 solution apply. In case of a NAS transport, NAS message in control plane is integrity protected in LTE and UTRAN but not in GERAN.

UP solution: Device trigger is sent over user plane. Integrity protection is not provided for user plane in any RAN.

The evaluation of the solutions is as following:

Editor's note: Even if the network charges the source of the device trigger message, there is still a potential charging integrity concern. For example, events at the device subsequent to the fake trigger e.g. send SMS, Send Data, may create disputed chargeable events on the devices subscription. This threat needs to be considered and evaluated.

- **Solution 1: Triggering via NAS signalling**

It has 3 benefits to use this solution, first, both NAS signalling messages and SMS messages over NAS signalling can be integrity-protected. Secondly, core network can verify MTC server and UE can verify and trust core network after authentication. As a result, the trusted source verification can be achieved by the UE based on core network verification. Thirdly, it re uses the current existing mechanism to provide this protection and does not need to deploy new security elements etc. In a word, this solution is simply and secure.

- **Solution 2: Solution for fake SMS triggering from normal UE in the same network as UE used only for MTC**

  Solution 2 needs improvements on SMS-SC, SMS-GMSC/IP-SM-GW, HSS, the interface between SMS-SC and SMS-GMSC and C/Sh/G interface, so it has wide impacts on existing network entities.

  Solution 2 actually disables UE sending normal SMS to UEs used only for MTC, while the architecture for MTC defined by SA2 allows any network entity acting as SME to send SMS, so it is not compliant with SA2's conclusion.

  From user view, this solution limits the network service that can be provided to the user and have negative impact on user experience because user UE cannot send SMS to MTC user then.

  One step further, as SMS is a possible and efficient way for MTC small data transmission, if MT SMS from UE is prohibited, it will have significant influence on the network enhancement for small data transmission in the future.

- **Solution3:**

3-A: Network based SMS payload filtering:

Benefits:

- This solution has low impacts on existing network entities, since whitelist based SMS filtering is supported by current SMS system.
- If a SMS spoofing happens, the SMS delivery can be terminated immediately by the network, network resource can be saved.

Drawbacks:

- Network node should inspect all received SMSs based on TP Protocol ID which will increase network processing load. One alternative way is that the HSS would check the TP Protocol ID for all received SMSs, because it can do the authorization per UE and also it is very accurate check. But HSS check will increase the load in the HSS since SME number will be very large compared to SCS number in the Tsp interface.
- Protection against SMS spoofing depends on home network if the HPLMN implements home network routing for SMS.
- Due to the size limit of whitelist maintained by SMS-SC, the granularity of whitelist is coarse-grained.

3-B: UE based SMSC whitelisting:

Benefits:

- Regardless of the routing way (HPLMN routing or VPLMN routing), protection against SMS spoofing can be provided.

Drawbacks:

- Configuration and modification of the whitelist on UE are difficult.
- UE used only for MTC is usually power sensitive or energy restricted, so this solution can introduce more energy consumption to the device whatever maintaining a whitelist or USIM application toolkit or GBA push.
- The granularity of this mechanism depends on the SMS filtering granularity supported by SMSC.
- Further details are required (this sentence can be placed into the original solution section)

3-C: GBA Push based approach

For this solution, the benefit is the mutual authentication between the UE and the MTC Server can be achieved. But it has the following problem:

✧ The specific BSF Server for SIMTC needs to be deployed in the operator's network. Currently, some operator does not deploy the BSF Server.

R11 MTC Trigger Security Optional Solution Analysis:

R11 MTC Trigger Security Optional Solution is in TS23.682 [23]. There are some constraints of this R11 MTC trigger security solution which list below.

Home routing: R11 solution mandates the HPLMN shall implement Home Network Routing which has the effect of forcing the delivery of the SMS to an SMS Router in the HPLMN rather than to the serving MSC/VLR, SGSN or MME of the destination UE. It's the normal standardized procedure that SMS routes from its SMS-SC to the target's MSC/VLR, SGSN or MME. Home routing forces every two operators has to have agreements to send their SMS to the target's SMS router or SMS-SC, not legacy SMS routing. This constraint requires operator's HPLMN supports new SMS routing path.

Filtering infrastructure: This filtering infra is used to block unauthorized SME to send trigger messages. However, how the solution to let filtering infra authorize SME according to the trigger SMS is not clear since it should not be stated in TS23.682 [23] and it should be studied in SA3's TS in R12. In common understanding, a whitelist is used to check the authorized SME. However, the granularity of this whitelist should be studied and stated in the solution to make the solution completed. Operators have to maintain such a filtering infra to support this R11 solution.

In NOTE 2 of this solution(S3-120543), "filtering is distributed between filtering infrastructure associated with the SMS Router, filtering infrastructure associated with the SMS-SC, and the filtering functions within the MTC-IWF". It also stated a constraint "the filtering needs to be invoked by an entity which can verify the source of the SM on a locally connected interface". That means SMS router, or SMS-SC or MTC-IWF has to support verifying the source of the SMS. SMS router does not have such capability. SMS-SC and MTC-IWF do not have this capability unless they have all the possible subscription/whitelist of SME who can send trigger message. We can also let filtering infra has this capability but the problem is the same that the filtering infra should know maintain the completed whitelist/subscription of the source of trigger messages. Moreover, a locally connected interface should be supported by the operators but it probably may be an internal interface and needs no standardization. But the mechanism of how the NE invokes the filtering and verify the source of the SM on a locally connected interface should be studied further.

5.2 Secure Connection

5.2.1 Issue Details

- The MTC Feature Secure Connection is intended for use with UEs that require a secure connection between the UE and MTC Server in indirect model or between the UE and MTC Application Server in direct model.
- In the context of MTC Feature Secure connection SA1 has stated the following (S3-100412):
- *The intention of the MTC Feature Secure Connection is to use the security features of the UICC to enable an exchange of security keys between the MTC Device and MTC Server. The actual encryption of data between the MTC Device and MTC Server would happen at application layer and be out of scope of 3GPP specifications.*
- In TS 22.368 [9] the requirement on secure connection is stated as follows:

> *The network operator shall be able to efficiently provide network security for connection between MTC Device and a MTC Server or between MTC Device and a MTC Application Server in case there is a direct connection with the MTC Application Server. This applies even when some of the devices are roaming i.e. connected via a VPLMN.*

Editor's Note: It needs to be decided that network efficiency should be a general security requirement for all SIMTC issues.

- The actual usage of the security keys for securing the application level functionality (including encryption of data as indicated above) between UE and MTC Server/MTC Application Server is out of scope of 3GPP specifications.

- Also other mechanisms can be used to provide security between the UE and MTC Server/MTC Application Server but they are regarded to be outside the context of the MTC Secure Connection feature and therefore out of scope of 3GPP specifications.

5.2.2 Threats

5.2.3 Security Requirements

Any 3GPP defined key management mechanisms for secure connection between the UE and the MTC Server/MTC Application Server should use UICC.

5.2.4 Solutions

5.2.4.1 GBA based solution

GBA, as specified in TS 33.220 [21], is used to bootstrap authentication and key agreement for application security based on the 3GPP AKA mechanism. It can be used to establish the end-to-end security and provide different security levels based on detailed requirements.

GBA Push, as specified in TS 33.223 [22], can be used for key establishing between an UE and an MTC server/MTC Application Server. Under SIMTC scenario, UE generates a NAF key derived from the bootstrap key Ks, and MTC server/MTC Application Server acts as NAF which received the NAF key from the BSF. Then UE and MTC server/MTC Application Server can set up secure connection based on this shared NAF key.

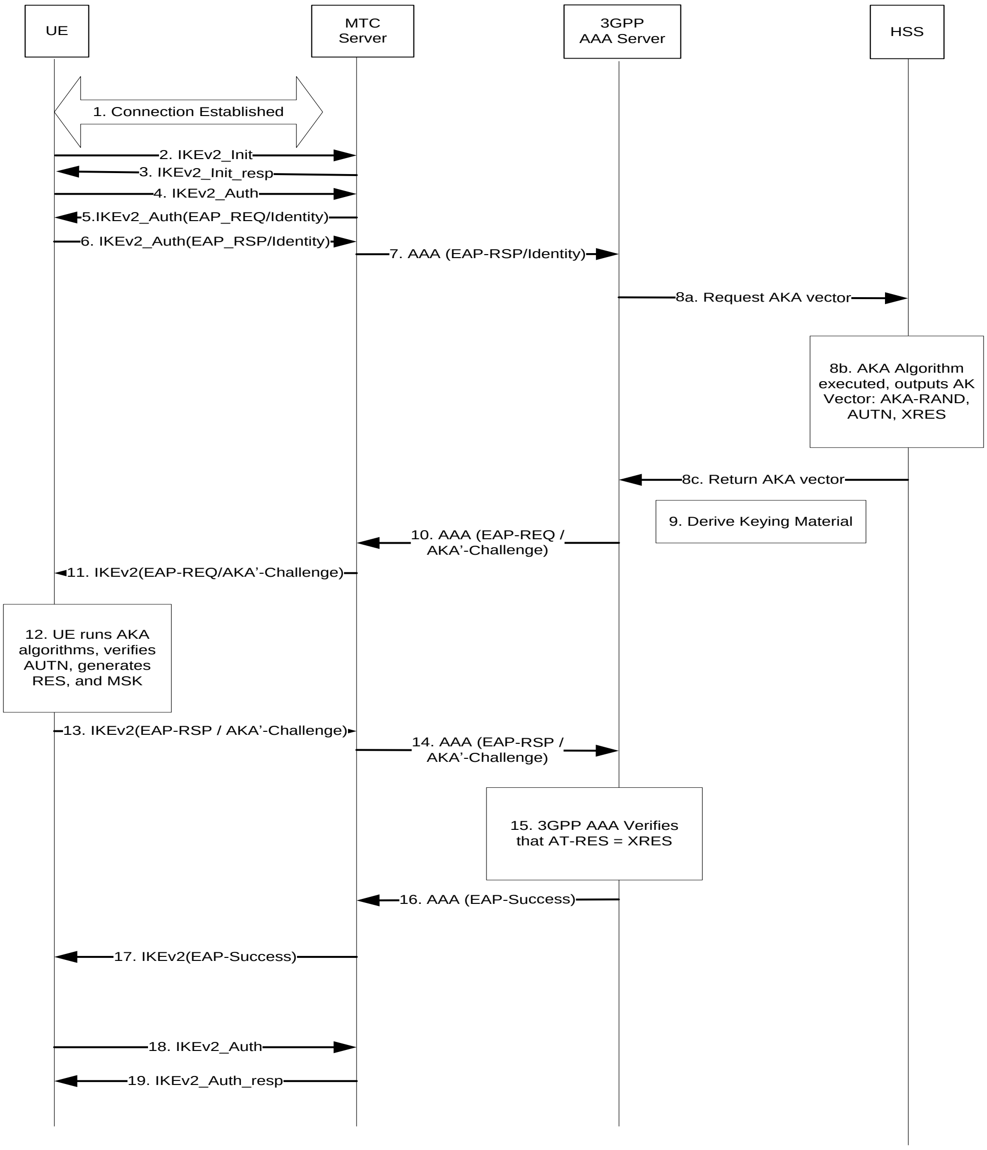
5.2.4.2 EAP based solution

5.2.4.2.1 IKEv2 based solution

When UE connects to the network, it will get an IP address for PS communication. Under this scenario, so IKEv2 or some other kinds of IP security protocol which can be used to carry EAP methods, can be used for establish the communication keys between UE and MTC service capability server.

Note: Here we can use many kinds of protocol to carry the EAP-AKA, for example we can use IKEv2 or other lightweight protocol. But here we just want to emphasize to use the EAP-AKA protocol.

In order to use the security features of the UICC to enable an exchange of security keys, an EAP-SIM/EAP-AKA method can be embedded into carrying protocol's procedure. The whole procedure can be as following:


UE
MTC Server
3GPP AAA Server
HSS
1. Connection Established
2. IKEv2_Init
3. IKEv2_Init_resp
4. IKEv2_Auth
5.IKEv2_Auth(EAP_REQ/Identity)
6. IKEv2_Auth(EAP_RSP/Identity)
7. AAA (EAP-RSP/Identity)
8a. Request AKA vector
8b. AKA Algorithm executed, outputs AK Vector: AKA-RAND, AUTN, XRES
8c. Return AKA vector
9. Derive Keying Material
10. AAA (EAP-REQ / AKA'-Challenge)
11. IKEv2(EAP-REQ/AKA'-Challenge)
12. UE runs AKA algorithms, verifies AUTN, generates RES, and MSK
13. IKEv2(EAP-RSP / AKA'-Challenge)
14. AAA (EAP-RSP / AKA'-Challenge)
15. 3GPP AAA Verifies that AT-RES = XRES
16. AAA (EAP-Success)
17. IKEv2(EAP-Success)
18. IKEv2_Auth
19. IKEv2_Auth_resp

1. UE establishes the connection with MTC server.

2. When UE wants to generate session keys with MTC server, it sends IKEv2 initialization message to MTC server.

3. After receiving IKEv2 initial message, MTC server will start the secure connection procedure and send IKEv2 initial response message back to UE.

4. UE sends IKE_AUTH message to MTC server. The message does not contain AUTH payload to trigger EAP procedure.

5. MTC server sends IKEv2 message with EAP payload for requesting the UE's identity.

6. UE sends back identity embedded into IKEv2 message.

7. MTC server forwards UE's identity by using EAP message to 3GPP AAA server.

8a. 3GPP AAA server send authentication vector request with UE's identity to HSS.

8b. HSS generates authentication vector based on UE's identity and its root key.

8c. HSS sends back authentication vector to the 3GPP AAA server.

9. 3GPP AAA server calculates the MSK based on the CK/IK inside the authentication vector.

10. 3GPP AAA server sends authentication request inside EAP message to MTC server.

11. MTC server encapsulates such EAP message into IKEv2 message and sends it out to UE.

12. After receiving the message, UE will run AKA algorithm to verify the AUTN and generates RES and MSK which is same with 3GPP AAA server. MSK will be used for secure connection.

13. UE creates EAP message, which carries AKA response information and encapsulates it into IKEv2 message and sends to MTC server.

14. MTC server forwards EAP message to 3GPP AAA server.

15. 3GPP AAA server verifies the RES contained in EAP message with XRES.

16. If the verification is success, 3GPP AAA server sends the MSK to MTC server with EAP-success message.

17. When received EAP-success message, MTC server knows the authentication is succeeded, then it extracts MSK for secure connection and sends IKEv2 authentication message with EAP-success message.

18. UE sends IKEv2 authentication message to MTC server.

19. MTC server sends IEKv2 AUTH message back to UE, and finish the procedure.

After the procedure, UE can get the MSK in step 12. In step 9, the same MSK can be calculated in 3GPP AAA server. In the next step 16, the MSK can be transferred from 3GPP AAA server to MTC server who is used for application usage.

Editor's Note: It needs check with SA2 whether there is an interface between the MTC server and the 3GPP AAA server.

5.2.4.2.2 EAP/PANA based Solution:

ETSI M2M specification [27] specifies EAP-based M2M Service Bootstrap procedure using EAP-SIM [28] with EAP/PANA or using EAP-AKA [29], [30] with EAP/PANA [31]. In order to harmonise with other SDOs for secure connection, mechanism using EAP/PANA using SIM or AKA-based credentials to be considered as potential solution for secure connection. When EAP/PANA based approached is used, the UE will support PANA Client (PaC) functionality and the SCS will support the PANA Authentication Agent (PAA) functionality.

5.2.5 Evaluation

Editor's note: This section contains evaluation (possibly including cost and benefit trade-off analysis) of candidate solutions enumerated in the preceding General Description subsections.

5.2.5.0 General

In order to evaluate the solution for secure connection, it proposes to make evaluation based on the criteria as: use case, security, cost, protocol dependency, and network impact.

5.2.5.1 Evaluation for GBA/GBA push based solution:

1. Use cases: GBA is triggered by UE only, so it can be applied in the scenario when a secure connection procedure is triggered by UE. In contrary, if the secure connection starts from network side, GBA push should be used instead of GBA. Furthermore, GBA and GBA push mechanisms will use 3GPP AKA mechanism that will involve UICC and network entity to generate security keys. As a result, if GBA and GBA push are used together for secure connection, they can fulfil the SA1's requirement that "The intention of the MTC Feature Secure Connection is to use the security features of the UICC to enable an exchange of security keys between the MTC Device and MTC Server".

2. Security: GBA/GBA push use AKA mechanism, and AKA protocol can resist attacking like replay, eavesdropping, tampering and any others. The key exchange between BSF and NAF will be through a secure

channel, so the key will not be disclosed in this interface. As a result, GBA / GBA push mechanism can effectively provide security protection for the exchange of security keys between UE and MTC server.

3. Cost: In the network side, MTC server need to support NAF features, and an additional BSF should be deployed. In the terminal side, the capability for a Ua application on the ME to indicate to the GBA function should be supported. Furthermore, a GBA-aware ME shall support both GBA_U and GBA_ME procedures.
4. Terminal supporting: Not all terminals can be considered to support GBA client. So it may require to add GBA features in SIMTC terminals.
5. Protocol dependency: GBA mechanisms except GBA push needs to be based on HTTP protocol.
6. Network impact: There is no need to deploy new feature on existing network entity, and no influence for protocol. So it has little impact for the existing network.

5.2.5.2 Evaluation for EAP-AKA method:

1. Use cases: Both UE and MTC server can trigger secure connection procedure. EAP-AKA can involve UICC and network entity to generate security keys. As a result, EAP-AKA can fulfil the SA1's requirement that "The intention of the MTC Feature Secure Connection is to use the security features of the UICC to enable an exchange of security keys between the MTC Device and MTC Server/MTC application Server".
2. Security: EAP-AKA method uses AKA mechanism embedded in EAP framework. The security protection is based on AKA. AKA protocol can resist attacking like replay, eavesdropping, tampering and any others. The key exchange between MTC server and 3GPP AAA server can be through a secure channel, so the key will not be disclosed in this interface. As a result, EAP-AKA mechanism can effectively provide security protection for the exchange of security keys between UE and MTC server.
3. Cost: When using IKEv2 to carry EAP-AKA method as an example, most of network entity supports IKEv2 function. So there is no additional requirement for MTC server. In the terminal side, UE must need to support theIKEv2 function mechanism.
4. Terminal supporting: Some kinds of terminals support EAP-AKA feature but not all kinds of..
5. Protocol dependency: EAP-AKA can't be used directly between UE and MTC server. It needs some protocols to carry EAP-AKA message.
6. Network impact: An interface between MTC server and 3GPP AAA server is needed, which is used to send AAA message.
7. Protocol overhead: It depends on the specific protocol which is used to carry EAP-AKA method. If some lightweight protocol can be used to carry EAP-AKA, the overhead can be limited.

Comparison of two methods:

Criteria	GBA-based method	EAP-AKA based method
Use cases	Fulfil SA1's requirement	Fulfil SA1's requirement
Security	Based on AKA,	Based on AKA,
Cost	Need additional network entity: BSF. Need to implement additional functions (NAF function) and related interfaces on MTC server. If UE does not support GBA, it needs to implement additional functions on terminal side	Need to have 3GPP AAA server. If UE does not support EAP-AKA, it needs to implement additional function on UE. Editor's Note: How this is secured is FFS
Terminal supporting	Most of terminal do not support GBA method	Some kinds of terminals support EAP-AKA method

Protocol dependency	It needs HTTP protocol, which is not implemented in some kinds of terminals	It needs some protocols to carry the EAP –AKA
Network impact:	No new feature is needed.	An interface is needed between MTC server and 3GPP AAA server.
Protocol overhead	It is much heavier than binary protocol.	It depends on the specific protocol which is used to carry EAP-AKA method.

5.3 External Interface Security

5.3.1 Issue Details

There are two scenarios of UEs communication with MTC server(s) illustrated in TS 22.368 [9], MTC Server(s) controlled by the network operator or MTC Server(s) not controlled by the operator. The interface between MTC Server and CN may be over an insecure link. Communication between the MTC Server and the CN for common and specific services (such as Device Triggering, MTC Monitoring) are carried on this insecure link. Attack on the communication between MTC Server and CN may cause false activities either to the MTC Server, UE or to the 3GPP network or privacy sensitive information such as identities may be eavesdropped, which may lead to serious problems.

5.3.2 Threats

For example the following threats are identified for external interface security:

For Device Triggering:

The network triggers UEs to initiate communication with the MTC Server based on a trigger indication sent from the MTC Server. This will open a chance for an attacker, especially when the MTC server is outside the operator domain.

The attacker can impersonate the MTC server to send a false trigger indication to the network, and then the network is utilized by the attacker to trigger the corresponding UE(s) used for MTC. This will cause false decision on the UE which may lead to the waste of the UE's power consumption and even a DOS attack to the network, as a large number of UEs are triggered and required authentication at the same time. Thus the attackers can manipulate this to achieve their attack target.

An authorized MTC server may not have full control over a UE and thus certain triggers from such MTC server to the UE might not be allowed. If such MTC server inadvertently triggers the UE with incorrect trigger then it can cause crucial damage to UE, for example UE triggered for software update by a MTC server which is not authorized to do so.

The attacker can eavesdrop privacy sensitive information such as UE identities on the external interface.

For MTC Monitoring:

In clause 7.2.8 of TR 22.368 [9] four monitoring events are defined：

Behaviour which is not aligned with activated MTC Feature(s)

Change in the point of attachment

Change of the association between the UE and the UICC

Loss of connectivity

Upon the detection of the above events, the network provides a warning notification to the MTC Server. Then the MTC User will execute the appropriate measure according to the detected event. If an attacker impersonates a network to send a fake monitoring warning notification to the MTC Server, the MTC Server can reject to provide service to the UE or it will cause wrong decision such as initiating false triggering procedure.

Analysis of device identity privacy issues

The attacker can eavesdrop privacy sensitive information such as UE identities on the external interface.

SA2 is discussing what device identifier that should be used between a MTC Service Provider and the network, see e.g. SA2 TR 23.888 V1.1.0 clause 6.38 (or the original agreed pCR in S2-111220) [10], where two types of identifiers, IMSI and a ISSI, are considered. Using these identifiers between an external MTC Service Provider may introduce privacy issues.

Using IMSI for network external identification purposes should, as is noted in S2-111220, of course as usual be avoided. Far reaching measures has for example been taken to avoid exposing the IMSI over radio interfaces by introducing temporary identifiers (TMSI, P-TMSI, S-TMSI, GUTI etc.).

The ISSI (International Service provider Subscription Identifier) is introduced as an alternative having a number of desired features.

One particular security advantage of use of ISSI compared to IMSI is that it would allow a network to easily check that a MTC Server is authorized to issue a request towards a particular device as this is clear from the service provider ID included in the identifier. Using IMSI the network would have to rely on information about device and Service provider association stored in the HSS. Note that the need to contact the HSS to get assurance that the Service provider is authorized for contacting a UE could be used to implement a DoS attack towards the Network/HSS. A prerequisite is of course that the network configured for MTC can securely authenticate the MTC server issuing a request.

Still, intercept of event reports or commands and responses sent over the external interface may reveal security/privacy sensitive information; it all depends on the information sent to or from the UE. But sometimes just understanding that a UE reports something, an event is trapped by the network or that a device is being triggered may have security/privacy consequences. However, it is easy to stop such leakage of security/privacy sensitive information by requiring that the communication between an external MTC Service Provider and the Network is confidentiality protected. As pointed out above it also has to be integrity protected so use of TLS or IPSec would solve this issue.

5.3.3 Security requirements

Editor's Note: The administrative burden of maintaining such lists for authorization information within the 3GPP needs further study.

When the MTC Server is located outside the 3GPP operator domain, the following security requirements apply:

The 3GPP network and the MTC Server should be able to mutually authenticate each other.

The network should explicitly reveal UE status, such as online/offline, idle or connected to authorized parties only, e.g. to an authorized SCS in relation to monitoring feature, cf. clause 5.11 Monitoring.

The 3GPP network should be able to determine whether the MTC server is authorized to send control plane requests.

The 3GPP network should be able to determine that the MTC server is authorized to send the given trigger to the given UE.

The signalling messages between the3GPP network and the MTC Server should be integrity protected.

The signalling messages between the3GPP network and the MTC Server should be confidentiality protected.

The level of security of the protection should not be lower than in the case when the MTC server is within the operator domain.

Security measures shall be applied to MTC reference points when communication extends beyond the boundary of the 3GPP system unless physical security is available.

Ensure the privacy of the 3GPP user, in particular the 3GPP private user identity (IMSI/IMPI)

The mobile network shall provide security mechanisms that can be used to (cf. TR 23.888 [10]):

- ensure that an MTC Server can only communicate with certain UEs;
- ensure that only authorized PDN entities can communicate with the UEs;
- ensure that a UE can only communicate with the MTC Server(s) of its subscriber, and that communication with any other entity is not possible.

MTC Security GW could be used between the MTC server and the core network as the first point of entry into a secure operator network. The MTC Security GW can be an independent node or co-located with an intermediate node (e.g. MTC IWF).

Editor's Note: The above requirement needs to be revisited as the level of security is not clear enough.

Editor's Note: The specific node in the 3GPP network side of the interface is FFS.

Editor’s Note: Requirement, “It shall be possible to provide secure and encrypted communication between PLMN and MTC Server” is reported in TR 23.888 [10]. It is FFS to detail this requirement.

5.3.4 Solutions

5.3.4.0 General

External interface is an interface that connects a network entity inside 3GPP network with another entity outside the 3GPP network. Therefore, the interface specified in MTC architecture in TS 23.682 [23] and need to be considered here includes:

1. Tsp interface between MTC-IWF and SCS.
2. Gi/SGi interfaces between GGSN/P-GW and AS and between GGSN/P-GW and SCS.
3. Tsms interface between SMS-SC/GMSC/IWMSC and SME.

NOTE 1: SME covers the SMS functionality of SCS.

5.3.4.1 Tsp interface security for MTC Server outside the operator domain

When the MTC Server is located outside the operator domain, the interface between the core network and the MTC Server may be protected using mechanisms like NDS/IP [2]. As the MTC server is located outside the operator domain it may not be possible to mandate the use of NDS/IP but the exact protection mechanism may be based on the agreements between the 3GPP network and MTC server.

Functional entity MTC Security GW may be used to authentication and authorization the MTC servers and to secure the external interfaces as shown in the Figure 3

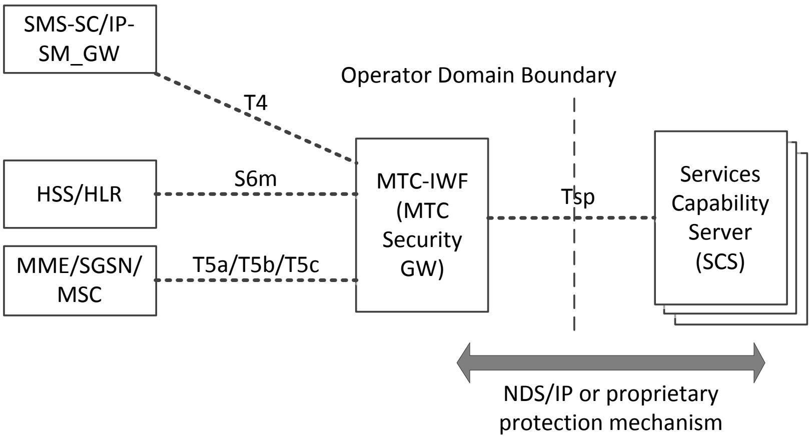

SMS-SC/IP-SM_GW
HSS/HLR
MME/SGSN/MSC
T4
S6m
T5a/T5b/T5c
MTC-IWF (MTC Security GW)
Operator Domain Boundary
Tsp
Services Capability Server (SCS)
NDS/IP or proprietary protection mechanism

Figure 3 Tsp interface security for Service Capability Server outside the operator domain

Thus the MTC Security GW within the MTC-IWF can perform access control functionality of MTCsp interface to prevent the unauthorized MTC server from accessing to the core network. It can authenticate with MTC server on behalf of the 3GPP network.

After successful mutual authentication between the MTC server and the MTC security GW, the MTC security GW connects the MTC server to the operator’s security domain. Any connection between the MTC server and the core network is protected through the MTC security GW. End-to-end security protection should be used for protection between the MTC server and the MTC security GW. Security protection is required between the MTC security GW and the MTC server placed outside the Operator's secure domain. Security protection should be used for any communication between the entities. Communication between the MTC server and the MTC security GW should be confidentiality, integrity and replay protected. The NDS/IP security mechanism [2] or proprietary security mechanism is used for mutual authentication and to protect the communication between the MTC security GW and the MTC server.

Any unauthenticated traffic from the MTC server should be filtered out at the MTC security GW.

For the MTC Security GW within the MTC-IWF, it can restrict the trigger request coming from the unauthorized MTC Servers to prevent the unauthorized MTC servers triggering the UE. When one MTC server needs to trigger a UE, it sends trigger request information to the MTC Security GW, and the MTC server identity and UE identity should be included in the request information or an authenticated identity of its group membership. On receiving the trigger request, MTC Security GW first verifies whether the MTC server is authorised to send trigger requests based on pre-configured information. If the MTC server is allowed to, the MTC Security GW further interrogates with HLR/HSS to determine whether the MTC server is authorized to trigger a particular UE. Based on the subscription of UE, HLR/HSS makes this decision and sends a response to the MTC Security GW. If the response indicates the MTC server is allowed to trigger the UE, the MTC Security GW deliver the SMS trigger message as normal. If either check fails, the trigger request should be rejected.

5.3.4.2 MTC Server inside the operator domain

When the MTC Server is located inside the operator domain, NDS/IP is mandatory to implement and optional to use.

5.3.5 Evaluation

Editor's note: This section contains evaluation (possibly including cost and benefit trade-off analysis) of candidate solutions enumerated in the preceding General Description subsections.

5.4 Restricting the USIM to specific UEs

5.4.1 Issues Details

The issue that led to the need to restrict the USIM to specific MEs is illustrated in a use case "Access control with billing plan" in Annex A of TS 22.368 [9].

Access Control with billing plan Use Case

In some configurations, it may be necessary to restrict the access of a UICC that is dedicated to be used only with machine type modules associated with a specific billing plan. It should be possible to associate a list of UICC to a list of terminal identity such as IMEISV so that if the UICC is used in another terminal type, the access will be refused. See the following configuration:

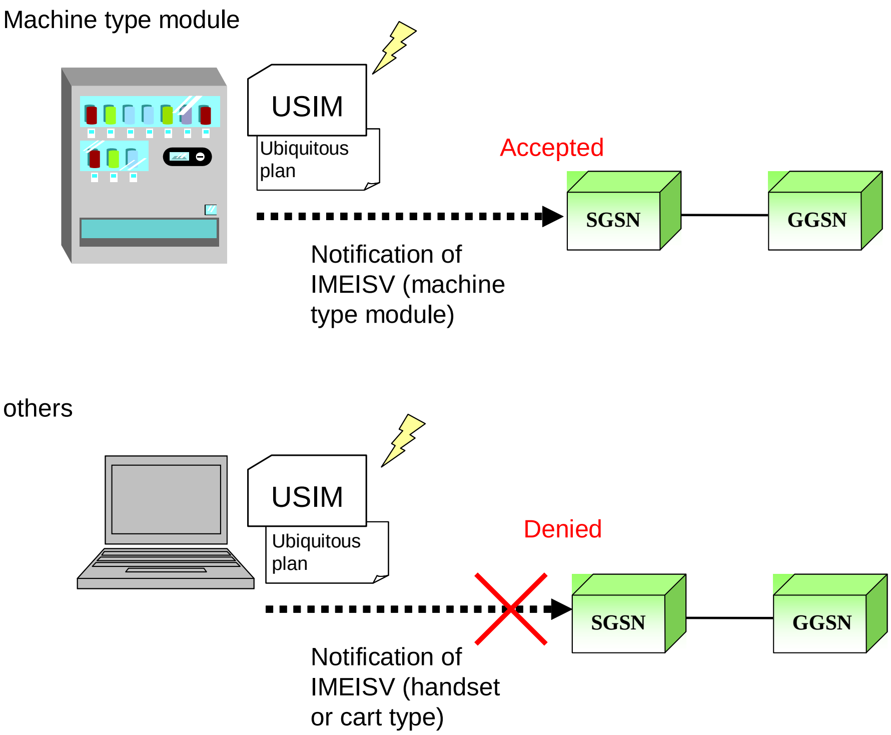


Figure 2: Access Control with billing plan

The restriction can be enforced by a one USIM to one UE binding or a one USIM to many UE binding. It is the operator that shall be able to enforce the restriction.

5.4.2 Threats

The following threat has been identified for this key issue:

- An attacker moves a UICC to a different device in order to use a subscription to get network access for himself, e.g. the attacker may try to insert a UICC with low data rate subscription, dedicated to MTC MEs, into a smartphone in order to download large files.

5.4.3 Security Requirements

In clause 7.1.1 of TS 22.368 [9] specifies the requirement to restrict the use of a USIM to specific UEs.

5.4.4 Solutions

5.4.4.0 General

Several mechanisms exist to address this issue.

Editor's Note: To consider the standard platform security robustness requirements for securely storing the private key is FFS

5.4.4.1 User Equipment-based pairings

5.4.4.1.0 General

CT6 discussed and considered three User Equipment-based mechanisms to restrict the use of UICC to specific MTC MEs, confer CT6 contribution C6-110182:

- Secure Channel pairing

- USAT application pairing
- PIN verification pairing

5.4.4.1.1 Secure Channel pairing

A secure channel pairing is successful when an Application-to-Application "Secured APDU" secure channel is completed as described in ETSI TS 102 484 [36].

CT6 mechanism proposes the use of pre-shared key (PSK) to establish the secure channel.

TS 102 484 [36] defines also a key agreement based on certificate exchange to establish the key material for the Master SA of the Application-to-Application "Secured APDU" secure channel, the key material results from a certificate-based TLS handshake. This key agreement based on certificate exchange is used in Rel-10 Relay Node security to define certificate-based secure channel between the Relay Node and the UICC, as described in TS 33.401 [13]. Consequently, the use of a key agreement based on certificate exchange, as described in ETSI TS 102 484 [36], is considered in this analysis as a possible solution to restrict the USIM to specific UEs. To ease the reading of this analysis, the Application-to-Application "Secured APDU" secure channel with a pre-shared key is named PSK-based secure channel, and Application-to-Application "Secured APDU" secure channel with key agreement based on certificate exchanged is named certificate-based secure channel.

SA1 allows restricting the use of a USIM to one MTC ME or many MTC MEs.

- In case of PSK-based secure channel, the same pre-shared key should be provisioned in the USIM and in one or several authorized MTC MEs to allow the use of a USIM to one MTC ME or a group of MTC MEs.
- In case of certificate-based secure channel, it may be needed to reinforce the one-to-one or one-to-multiple binding by means of MTC ME identity check if the root certificate used to verify the MTC ME certificate is not dedicated to the list of authorized MTC MEs for this USIM . In this case, the USIM stores in a dedicated file (EF_{IMEISV}) the list of authorized IMEI(SV) values or IMEI(SV) ranges of values to which the USIM is bound. During certificate verification the USIM checks that the IMEI(SV) received in MTC ME certificate matches the value or the range of values the UICC is configured with. The file of IMEI(SV) value or range of values to which the USIM is bound is described in CT6 contribution for USAT application pairing, this file can be updated by means of Over-The-Air mechanism.

The file $EF_{pairing}$ stores the status of the last pairing check performed by the UICC. The UICC checks the combination of USIM and MTC ME and sets the status flag to "OK" in case of successful pairing check. The UICC also stores in the file $EF_{pairing}$ the IME(SV) value of the MTC ME. In case of unsuccessful pairing check, the USIM sets the status flag to "KO" and stores in the file $EF_{pairing}$ the IME(SV) value of the unauthorized MTC ME.

The status flag of pairing check (with value "OK or "KO") stored in the file $EF_{pairing}$ can be read by any terminal hosting the UICC. But, the IMEI(SV) value stored in the file $EF_{pairing}$ is protected by ADM right, only the operator can retrieve this information. The information stored in the file $EF_{pairing}$ provide a mechanism to detect change of association between a USIM and a MTC ME. The information stored in the file $_{EFpairing}$ can be read out locally by the maintenance persons.

UICC OTA mechanism (as specified in 3GPP TS 31.115 [19] / TS 31116 [20] and ETSI TS 102 225 [17] and TS 102 226 [18]) is used to update the file EF $_{IMEISV}$ stored in the USIM. This mechanism provides dynamic management of the pairing to change the allowed combinations of USIM and MTC ME(s) by adding or removing authorized IMEI(SV) values or IMEI(SV) ranges the file EF $_{IMEISV}$.

The MTC ME stores a certificate where the subject name is the IMEI(SV) value. This certificate is signed by operator or vendor. To verify the MTC ME certificate, the UICC stores the associated root certificate corresponding to the operator or vendor who signed the MTC ME certificates.

The provisioning of certificates and pre-shared key can be performed during personalization phase of the MTC ME or the UICC. Provisioning during personalization phase is out of scope.

For UICC into the field it is possible to change the pre-shared key or root certificates stored in the UISM by means of UICC OTA as specified in 3GPP TS 31.115 [19] / TS 31116 [20] and ETSI TS 102 225 [17] and TS 102 226 [18]. The USIM could store several root certificates in the file dedicated to the storage of root certificates used to verify the combination of USIM and MTC ME.

For MTC ME into the field it is possible to modify the pre-shared key or certificate stored in the MTC ME by means of OMA DM.

Editor's Note: It is FFS Whether certificate is a vendor certificate or operator certificate.

5.4.4.1.2 USAT application pairing

USAT application pairing is successful when the IMEI or IMEISV retrieved from the terminal matches the value or the range of values the UICC is configured with. USAT application pairing fails if the terminal does not support USAT command PROVIDE LOCAL INFORMATION. After a UICC reset, the USIM shall have its PIN in a blocked state before USIM application selection. The PIN is unblocked and disabled after a successful USAT application pairing. An UE supporting USAT application pairing shall proceed to Profile download as specified in 31.111 [12]. The USIM shall immediately send a proactive command PROVIDE LOCAL INFORMATION requesting the UE's IMEI(SV). The UE shall then send the TERMINAL RESPONSE with its IMEI(SV) before starting USIM initialisation procedure.

The file EF_{IMEISV} stores the IMEI(SV) or range of value to which the USIM is bound.

The file $EF_{pairing}$ stores the status of the last pairing check performed by the UICC. The UICC checks the combination of USIM and MTC ME and sets the status flag to "OK" in case of successful pairing check. The UICC also stores in the file $EF_{pairing}$ the IME(SV) value of the MTC ME. In case of unsuccessful pairing check, the USIM sets the status flag to "KO" and stores in the file $EF_{pairing}$ the IME(SV) value of the unauthorized MTC ME.

The status flag of pairing check (with value "OK or "KO") stored in the file $EF_{pairing}$ can be read by any terminal hosting the UICC. But, the IMEI(SV) value stored in the file $EF_{pairing}$ is protected by ADM right, only the operator can retrieve this information. The information stored in the file $EF_{pairing}$ provide a mechanism to detect change of association between a USIM and a MTC ME. The information stored in the file $_{EFpairing}$ can be read out locally by the maintenance persons.

UICC OTA mechanism (as specified in 3GPP TS 31.115 [19] / TS 31116 [20] and ETSI TS 102 225 [17] and TS 102 226 [18]) is used to update the file EF_{IMEISV} stored in the USIM. This mechanism provides dynamic management of the pairing to change the allowed combinations of USIM and MTC ME(s) by adding or removing authorized IMEI(SV) values or IMEI(SV) ranges the file EF_{IMEISV}.

5.4.4.1.3 PIN presentation pairing

By having the PIN enabled and the UE provisioned with the PIN value, it is possible to restrict the usage of the USIM to this UE and therefore prevent unauthorized use of the USIM in another equipment. This mechanism can be used in conjunction with the USAT application pairing as an additional measure.

The file $EF_{pairing}$ stores the status of the last pairing check performed by the UICC. The UICC checks the combination of USIM and MTC ME and sets the status flag to "OK" in case of successful pairing check. In case of unsuccessful pairing check, the USIM sets the status flag to "KO".

The status flag of pairing check (with value "OK or "KO") stored in the file $EF_{pairing}$ can be read by any terminal hosting the UICC. The information stored in the file $EF_{pairing}$ provide a mechanism to detect change of association between a USIM and a MTC ME. The information stored in the file $_{EFpairing}$ can be read out locally by the maintenance persons.

The PIN value in the USIM could be change by UICC OTA mechanism. All specific MTC MEs authorized to be used with this USIM should be updated with the new PIN value, e.g. by means of OMA DM.

5.4.4.2 Network based pairings

5.4.4.2.1 IMSI-IMEI binding in HSS

5.4.4.2.1.1 General

In order to secure that only authorized combinations of USIMs and MEs are used, the HSS holds a list of authorized combinations of IMEI(SV)s per IMSI.

If an authorized IMSI/IMEI combination is detected by the HSS, the HSS shall accept the registration from the UE. If an unauthorized IMSI/IMEI combination is detected by the HSS, the operator should be notified and should then be able to take any further appropriate action, e.g. automatically denying access to the network by rejecting the Location Update procedure.

5.4.4.2.1.2 Restrict the use of a USIM to specific ME(s)

As an optional function to secure that only authorized ME's are used with a subscription (see sub clause 7.1.1 in 3GPP TS 22.368 [9] for corresponding stage 1 requirement), the HSS may hold a list of authorized IMEI(SV)'s per IMSI. During EMM/GMM/MM procedures the SGSN, MME or MSC indicates any new IMSI/IMEI(SV) pair to the HSS as described in TS 23.060 [3], TS 23.401 [4] and TS 23.012 [24]. For IMSI with a list of authenticated IMEI(SV) if the HSS detects an IMEI(SV) not in the authorized list then the HSS informs the MME, SGSN or MSC and the EMM/GMM/MM procedure is rejected.

NOTE: The function relies upon the Automatic Device Detection mechanism as specified in TS 23.060 [3] being supported in the MSC and SGSN for them to identify a new IMSI and IMEI combination and provide also the IMEI to the HSS.

If the UE roams into a visited network which does not support the Automatic Device Detection mechanism in the SGSN or MSC, as specified in TS 23.060 [3] and TS 23.012 [24], then it is a home operator choice whether to accept or reject the UE.

5.4.4.2.1.3 Procedure

Figure 5.4.4.2.1.3-1 shows how the HSS can check if the IMSI/IMEI pair is authorised.

In GERAN/UTRAN, the ADD (Automatic Device Detection) feature is optional to support in SGSN/MSC. If this feature is supported and enabled in the SGSN/MSC, the SGSN/MSC shall request the IMEI(SV) from the UE and provide the IMSI-IMEI(SV) pair to the HSS when the SGSN/MSC has detected that the IMEI(SV) has changed in the SGSN/MSC or the IMEI(SV) is new for the IMSI.

In LTE, the ADD feature is mandatory to support in the MME. When this feature is enabled in the MME, the MME shall request the IMEI(SV) from the UE and provide the IMSI-IMEI(SV) pair to the HSS when the MME has detected that the IMEI(SV) has changed in the MME or the IMEI(SV) is new for the IMSI.

This solution requires the ADD feature to be supported and enabled in SGSN/MME/MSC. Additionally the HSS/HLR needs to verify if an IMSI/IMEI pair is allowed.

Using ADD for requesting IMEI(SV) from the UE is commonly used in networks today to detect when a user has purchased a new UE so that e.g. appropriate MMS and internet access settings can be sent to user’s new UE.

Using this legacy feature also enables the HSS/HLR in the home network to check if the IMSI-IMEI(SV) pair received from the SGSN/MME/MSC is authorized.

If there is a need to change authorized combinations of IMSI/IMEI (e.g. due to billing plan change), only the HSS/HLR needs to be updated, There is no need to update other entities.

It should be noted that the list of authorized IMEI(SV)/IMSI pairs can be stored and the checking can also be performed in another node than HSS/HLR, e.g. a server connected to the HSS/HLR, It is however believed that HSS/HLR is the natural place to do the checking.

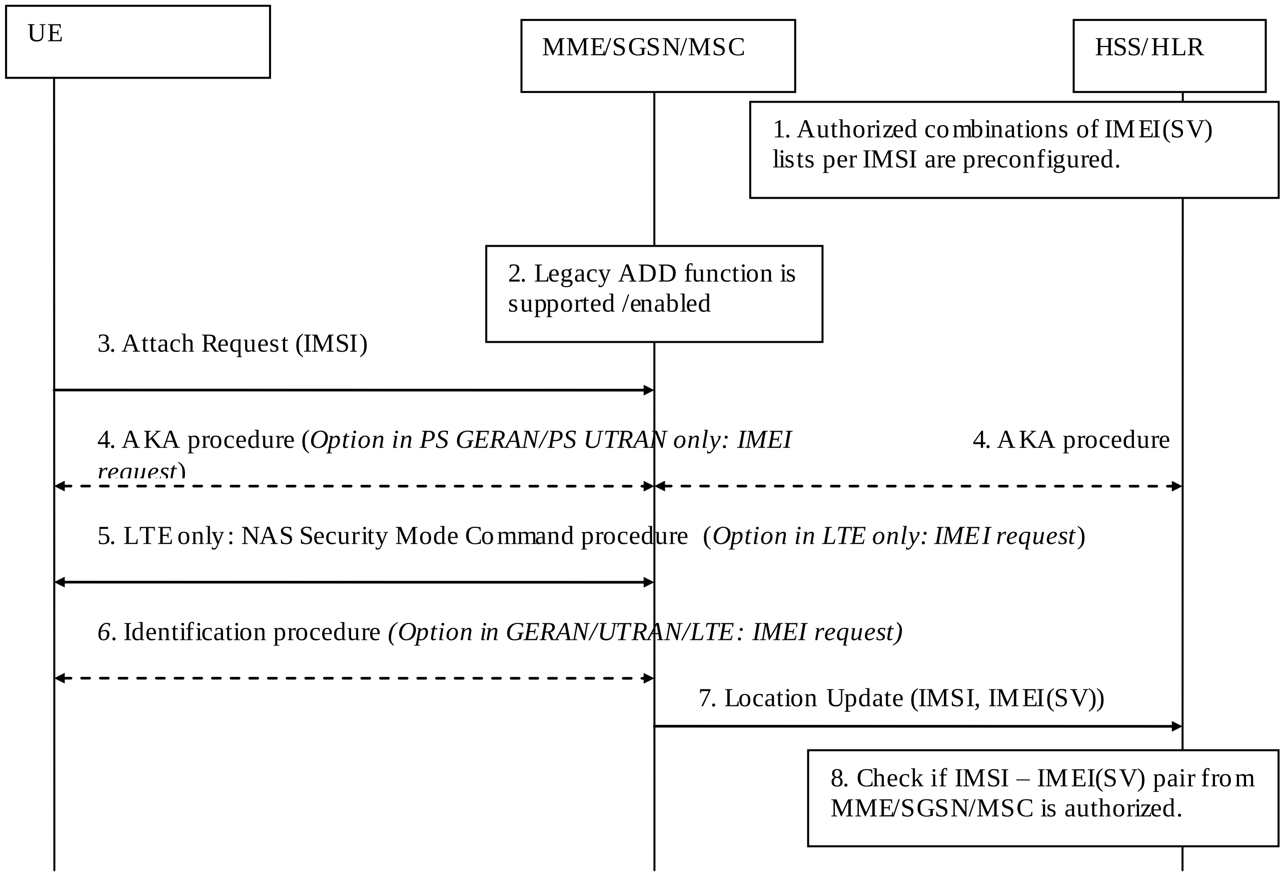

UE
MME/SGSN/MSC
HSS/HLR
1. Authorized combinations of IMEI(SV) lists per IMSI are preconfigured.
2. Legacy ADD function is supported /enabled
3. Attach Request (IMSI)
4. AKA procedure (Option in PS GERAN/PS UTRAN only: IMEI request)
4. AKA procedure
5. LTE only: NAS Security Mode Command procedure (Option in LTE only: IMEI request)
6. Identification procedure (Option in GERAN/UTRAN/LTE: IMEI request)
7. Location Update (IMSI, IMEI(SV))
8. Check if IMSI – IMEI(SV) pair from MME/SGSN/MSC is authorized.

Figure 5.4.4.2.1.3**-1: Solution for IMSI/IMEI in HSS**

The following is a description of the steps in figure 5.4.4.2.1.3-1.

Step 1: The authorized IMEI(SV) lists per IMSI are pre-configured in the HSS/HLR

Step 2: ADD function is supported and enabled in MME/SGSN/MSC.

Step 3: This is the normal Attach procedure as described in TS 24.008 [34] and TS 24.301 [35].

Step 4: This is the normal UMTS/EPS AKA procedure as described in TS 24.008 [34] and TS 24.301 [35].

In PS GERAN/PS UTRAN only: the IMEI request from the network can take place in this procedure.

In PS UTRAN, the security may not be enabled when AKA procedure is initiated, and the network can also request the IMEI from the UE after integrity protection and encryption has been enabled e.g. in step 6.

In PS GERAN, integrity protection is not supported, and encryption may not be enabled when AKA procedure is initiated. The network can request the IMEI from the UE after encryption is enabled e.g. in step 6.

Step 5: In LTE only: This is the normal NAS Security Mode Command procedure as described in TS 24.301 [35]. The IMEI request/response can take place in this procedure in an integrity protected way.

Step 6: In GERAN/UTRAN/LTE: This is the normal Identification procedure where the IMEI request/response can take place as described in TS 24.008 [34] and TS 24.301 [35].

In LTE: according to TS 33.401 [13] the UE shall provide its IMEI(SV) to the network if the network asks for it in an integrity protected request. According TS 33.401 [13] the IMEI(SV) should be encrypted.

In UTRAN: The network can request the IMEI(SV) from the UE in this procedure once the integrity protection and encryption is enabled.

In GERAN integrity protection is not supported. The GERAN network can request the IMEI(SV) from the UE in this procedure once the encryption is enabled.

Step 7. This is the normal Update Location procedure as described in TS 23.012 [24]. The SGSN/MME/MSC includes the IMEI(SV) and IMSI in the Update Location message to the HSS/HLR.

Step 8: The HSS/HLR checks whether the IMSI/IMEI(SV) pair is authorized according to the preconfigured lists. If the pair is not authorized in the HSS/HLR, the network operator is notified and may then take any appropriate action, e.g. the HSS/HLR may reject the Location Update procedure.

5.4.4.2.2 Enhanced AKA authentication

5.4.4.2.2.1 General

Two network based solution variants for restricting the USIM to certain UEs are provided. The variants are similar and only differ in how the network decides that the key used to authenticate the device is the correct one. Both solutions are based on enhancing the AKA procedure that runs between the UE and core network (see subclause 5.4.4.2.2.2) and use the same basic flows for initial attach and re-authentication (see subclause 5.4.4.2.2.3). Both solution variants also rely on the HSS/HLR checking that an IMSI/IMEI pair is authorised to attach to the network. The difference between the two solution variants are provided in subclause 5.4.4.2.2.4).

5.4.4.2.2.2 Enhanced AKA authentication Procedure

The existing AKA authentication procedure is enhanced to also perform device authentication that works in conjunction with the standard AKA authentication. Providing device authentication requires that the device has been provisioned with a *device_root_key* that can be used to send encrypted traffic to the device and that is uniquely associated to the IMEI of the device. The *device_root_key* is a public key of the device. A secure part of the device stores the sensitive device keys such as the private key and performs all cryptographic operations that make use of these sensitive keys.

The device authentication can be run either in parallel with the AKA procedures by adding new IEs to the AKA messages or can run separately by enhancing other NAS or in a new message (which is preferred is a stage 3 decision). The latter case allows the IMEI to be sent only after the security has been established and helps preserve the privacy of the IMEI.

Whenever a Core Network Node (CNN), e.g. SGSN in UTRAN/GERAN or MME in E-UTRAN, wishes to perform device authentication, it creates a *device_challenge* and sends it to the device in a relevant NAS message. The device computes the *device_response* and returns it to the network in a response NAS message. This allows the CNN to authenticate the device.

In addition, a root key, K_{Device}, for a particular access, e.g. a key that takes on the role of CK and IK in UTRAN or K_{ASME} in E-UTRAN, can be calculated from the device authentication. The calculation of K_{Device} includes using K_{Root}, the root key calculated from the concurrent AKA run or previous AKA run, if there is one, and hence K_{Device} is derived based on keys resulting from both the normal AKA run and the device authentication.

The calculation of *device_challenge*, *device_response* and K_{Device} are as follows:

$$device\_challenge = E_{device\_root\_key}\ (device\_temp\_key),\ network\_nonce$$

where $E_K(data)$ means *data* encrypted with key *K*, and *network_nonce* is a 128-bit random number chosen by the network. The *device_temp_key* is a 256-bit random number chosen by the network.

Both the UE and CNN keep *device_temp_key* while it has the security context that has a K_{Device} that was derived from it. This means that $E_{device\_root\_key}$ *(device_temp_key)* is optional to send in the case that the CNN knows the current security context being used by the UE has a K_{Device} as root key and hence the UE has a *device_temp_key* stored and the CNN is willing to re-use that key.

device_response is calculated as

$$device\_response = device\_nonce,\ device\_res$$

where *device_nonce* is a 128-bit random number (e.g., 128 bits) chosen by the device; and *device_res* is a 128-bit number that is calculated as follows:

$$device\_res = \mathrm{KDF}\ (device\_temp\_key,\ network\_nonce \parallel device\_nonce)$$

where KDF is a suitable pseudo-random function.

Finally, the calculation of K_{Device} is as follows:

$$K_{Device} = \text{KDF}\ (device\_temp\_key \,\|K_{Root},\ network\ nonce \,\|\, device\_nonce)$$

where K_{Root} is the key(s) freshly generated from a standard AKA authentication or the key(s) previously generated before the CNN initiates the device authentication.

A security context that has been created using enhanced AKA shall be kept in the ME and not stored on the UICC.

5.4.4.2.2.3 High-Level flows for the proposed method

5.4.4.2.2.3.1 General

The following subclauses contain attachment and re-authentication flows for the method at a high-level. The flows do not illustrate actual message but rather logical steps (except the device authentication step in each flow). The flows apply to both the proposed solution variants and are common for the different access networks (i.e., GERAN, UTRAN and E-UTRAN). The details of steps 2 and 3 of the attachment flow are provided in subclause 5.4.4.2.2.4 for each of the proposed solutions.

5.4.4.2.2.3.2 Attachment flow

Figure 5.4.4.2.2.3.2-1 shows how an UE can attach to a network with the addition of a device authentication step. The flow represents the most general case of attachment where the network holds no useful information about the UE from any previous connections.

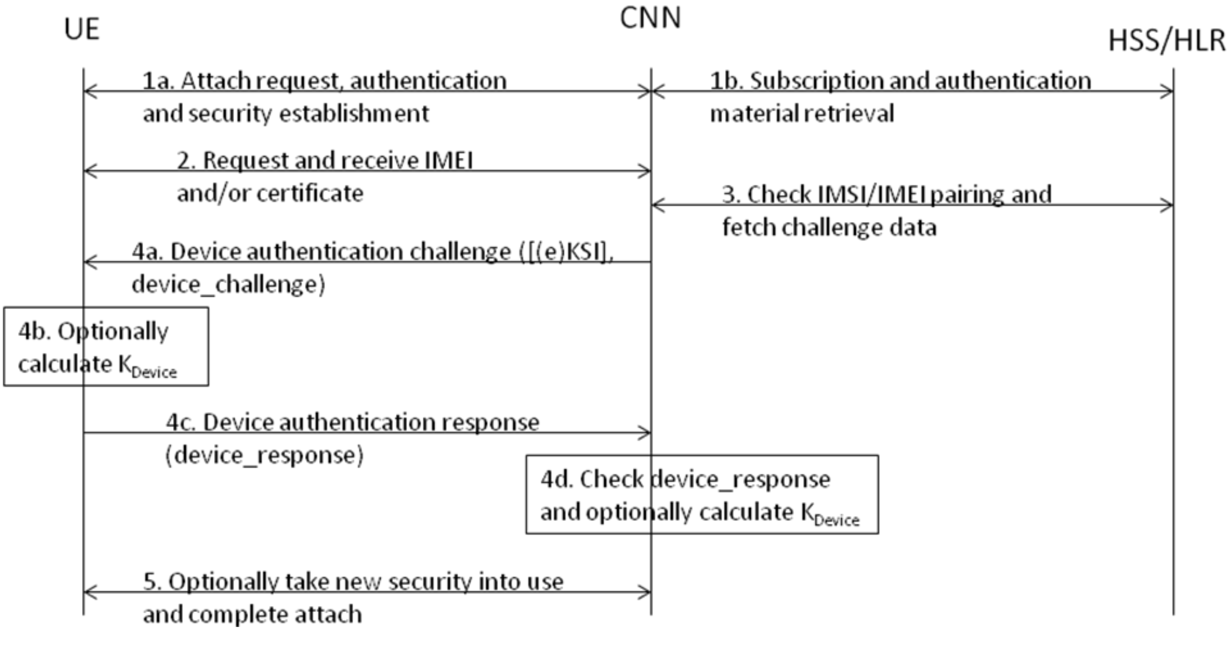

UE
CNN
HSS/HLR
1a. Attach request, authentication and security establishment
1b. Subscription and authentication material retrieval
2. Request and receive IMEI and/or certificate
3. Check IMSI/IMEI pairing and fetch challenge data
4a. Device authentication challenge ([(e)KSI], device_challenge)
4b. Optionally calculate K_{Device}
4c. Device authentication response (device_response)
4d. Check device_response and optionally calculate K_{Device}
5. Optionally take new security into use and complete attach

Figure 5.4.4.2.2.3.2-1: Attachment flow

The following is a description of the steps in figure 5.4.4.2.2.3.2-1.

Step 1: This is the normal messages for the access network except that the CNN informs the HSS/HLR that it is capable of performing device authentication for the UE and the HSS/HLR informs the CNN that device authentication is needed.

> Note: The HSS/HLR could hold the latest requested IMEI for each IMSI and provide this in Step 1. For second or subsequent attachments of a subscription, the HSS/CNN provides the CNN with the IMEI and challenge data. This would remove the need for step 3 in these cases. Whether the optimisation is necessary is FFS.

Steps 2: This step is solution dependent but only requires a change from standard behaviour in the case of solution that requires a device certificate from the UE. It should also be noted that for some access network, the IMEI request/response may happen in the same messages that are used for step 1.

Step 3: This step is solution variant specific; however in all variants, the CNN gets the HSS to check the whether the current IMSI/IMEI pair is authorised to access the network and also fetches any required device authentication data from the HSS.

Note: For variant 1, steps 3 and 4 can be performed in either order or simultaneously.

Step 4a: The CNN sends the device challenge to the UE. The *(e)KSI*, the normal key identifier, is sent by the CNN to indicate it wants the UE to create a security context with K_{Device} as its root key. The *device_challenge* always contain *network_nonce* but only contains $E_{device\_root\_key}$ *(device_temp_key)* if the CNN wants to change *device_temp_key* as described in subclause 5.4.4.2.2.2.

Step 4b: As *(e)KSI* was included in step 4a, the UE establishes a security context with K_{Device} as its root key

Step 4c: The UE responds to the CNN with *device_response* that contains both *device_nonce* and *device_res* (see subclause 5.4.4.2.2.2).

Step 4d: The CNN checks *device_res* is the expected value and establish a new security context if step 4a included *(e)KSI*.

Step 5: The CNN shall take any new security context into use before any user plane data is carried over the network. The attach procedure is completed.

5.4.4.2.2.3.3 Re-authentication flow

Figure 5.4.4.2.2.3.3-1 shows how to re-authenticate with device authentication.

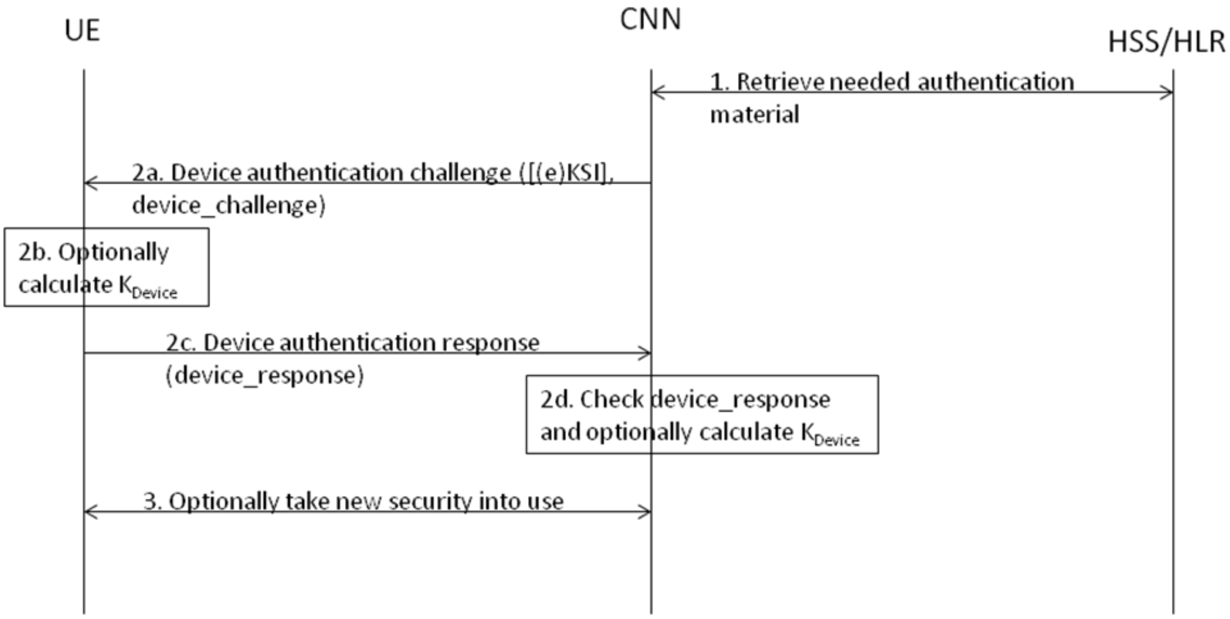

UE
CNN
HSS/HLR
1. Retrieve needed authentication material
2a. Device authentication challenge ([(e)KSI], device_challenge)
2b. Optionally calculate K_Device
2c. Device authentication response (device_response)
2d. Check device_response and optionally calculate K_Device
3. Optionally take new security into use

Figure 5.4.4.2.2.3.3-1: Re-authentication flow

The following is a description of the steps in figure 5.4.4.2.2.3.3-1.

Step 1: The CNN retrieves any needed authentication information from the HSS/HLR, e.g. an AKA authentication vector.

Steps 2a to 2d: The same as steps 4a to 4d in subclause 5.4.4.2.2.3.2.

Step 3: The CNN shall take the new security context into use before any user plane data is carried over the network.

5.4.4.2.2.3.4 Context transfer at handover, idle mobility and attach

Figure 5.4.4.2.2.3.4-1 shows the changes required to the legacy procedures between CN that transfer the UE's context at handover, idle mobility and attach when enhanced AKA is used. The difference is that if the context that is sent by the old CNN is one for a UE that requires enhanced AKA, then the old CNN includes some additional fields in the context transfer.

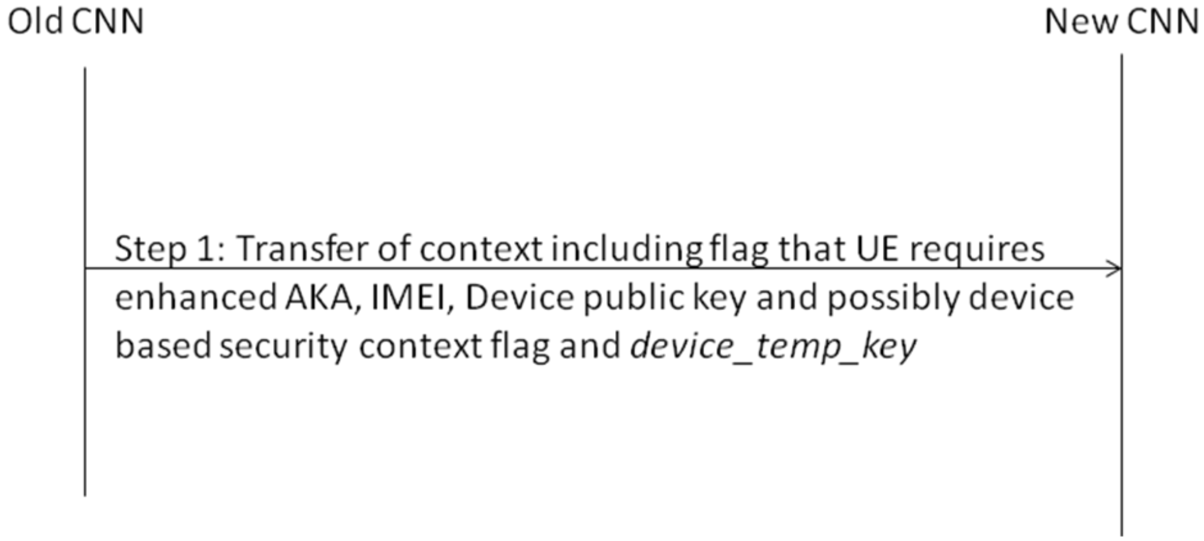

Old CNN
New CNN
Step 1: Transfer of context including flag that UE requires enhanced AKA, IMEI, Device public key and possibly device based security context flag and *device_temp_key*

Figure 5.4.4.2.2.3.4-1: Context transfer between CNNs

The following is a description of the steps in figure 5.4.4.2.2.3.4-1.

Step 1: If the context passed in a message to transfer context between CNNs is for a UE that requires enhanced AKA, then the old CNN passes the new CNN the following information; an indication that the UE requires enhanced AKA, IMEI and Device public key. In addition if the old CNN passes a UE security context, it shall also pass an indication that the security context is a device based one and the *device_temp_key*.

5.4.4.2.2.4 Differences between the solution variants

5.4.4.2.2.4.1 General

The following subclauses describe the different solution and in particular step 2 and 3 in those different solutions.

5.4.4.2.2.4.2 Variant 1: HSS/HLR provides the root certificate

In this solution, the HSS/HLR needs to be provisioned (or have access to a database) with the IMSI/IMEI pairs that are authorised for use and the associated root certificate that has been used to sign the UE's certificate. The following describes steps 2 and 3 for this solution.

Step 2: The CNN requests and receives the UE's certificate from the UE.

Step 3: The CNN sends IMSI and IMEI pair of the UE to the HSS/ HLR and also requests the root certificate related to that IMEI. Note that the request for root certificate can be skipped if the CNN has a local copy of the root certificate associated with the received IMEI. The HSS/HLR checks that IMSI/IMEI pair is authorised to attach to the network and if so returns authorisation success and the root certificate to the CNN (if requested by the CNN). The CNN uses the root certificate to check the UE's certificate is valid and hence gets the public key of the UE from the UE's certificate and is able to perform device authentication of the UE.

A particular IMSI/IMEI pair is revoked by removing it from the HSS or associated database. A particular device is revoked by removing all the IMSI/IMEI pairs that relate to that device.

5.4.4.2.2.4.3 Variant 2: HSS/HLR provides the UE's public key

In this solution, the HSS/HLR needs to be provisioned (or have access to a database) with the IMSI/IMEI pairs that are authorised for use and the public key of the UE. The following describes steps 2 and 3 for this solution.

Step 2: There is no change from the current standard behaviour.

Step 3: The CNN sends IMSI and IMEI pair to the HSS/ HLR and also requests the public key related to that IMEI from the HSS/HLR. The HSS/HLR checks that IMSI/IMEI pair is authorised and if so returns the public key associated with the IMEI to the CNN. The CNN uses the received public key to perform device authentication of the UE.

A particular IMSI/IMEI pair is revoked by removing it from the HSS or associated database. A particular device is revoked by removing all the IMSI/IMEI pairs that relate to that device.

5.4.4.2.3 Pairing based on symmetric shared secret

5.4.4.2.3.1 General

IMEI(SV) validation leverages a symmetric common secret, K_{ME}, between the UE and the 3GPP HSS. K_{ME} is used by the HSS for encrypting the RAND value that is sent to the UE during the AKA protocol. In particular, the RAND value that is included in each Authentication Vector, sent by the HSS to MME/SGSN, is encrypted using K_{ME} as the cipher key. Only the MEs that have the proper K_{ME} are able to decrypt the original value of the RAND before submitting it to the UICC. If ME manages to successfully decrypt RAND using K_{ME}, then the properly decrypted value will be provided to UICC and will be used for generating the RES value. Otherwise, AKA will fail. Specifically, if ME is not in possession of the K_{ME} that was used by the 3GPP network to encrypt RAND, ME will not be able to decrypt and obtain the value of RAND and therefore, UICC will not be able to compute the correct value of RES or other security context parameters.

When the HSS subscription record indicates that the IMSI is restricted to one specific device, then it is sufficient to provision one shared secret in the HSS and this device. When subscription is restricted to multiple devices, multiple shared secrets – one per device's IMEI(SV) – need to be provisioned in the HSS, and a particular secret is selected based on the knowledge of the IMEI(SV) reported by the UE.

5.4.4.2.3.2 Procedure

The steps of the verification process are depicted in Fig. 5.4.4.2.3.2-1 below, and are explained in what follows. It is assumed that HSS has been provisioned (or has access to a database) with the IMSI/IMEI pairs that are authorised for use. For all authorized IMEI values (and thereby authorized devices), HSS has associated the same K_{ME} key, which has been pre-provisioned into each authorized device (ME with corresponding IMEI).

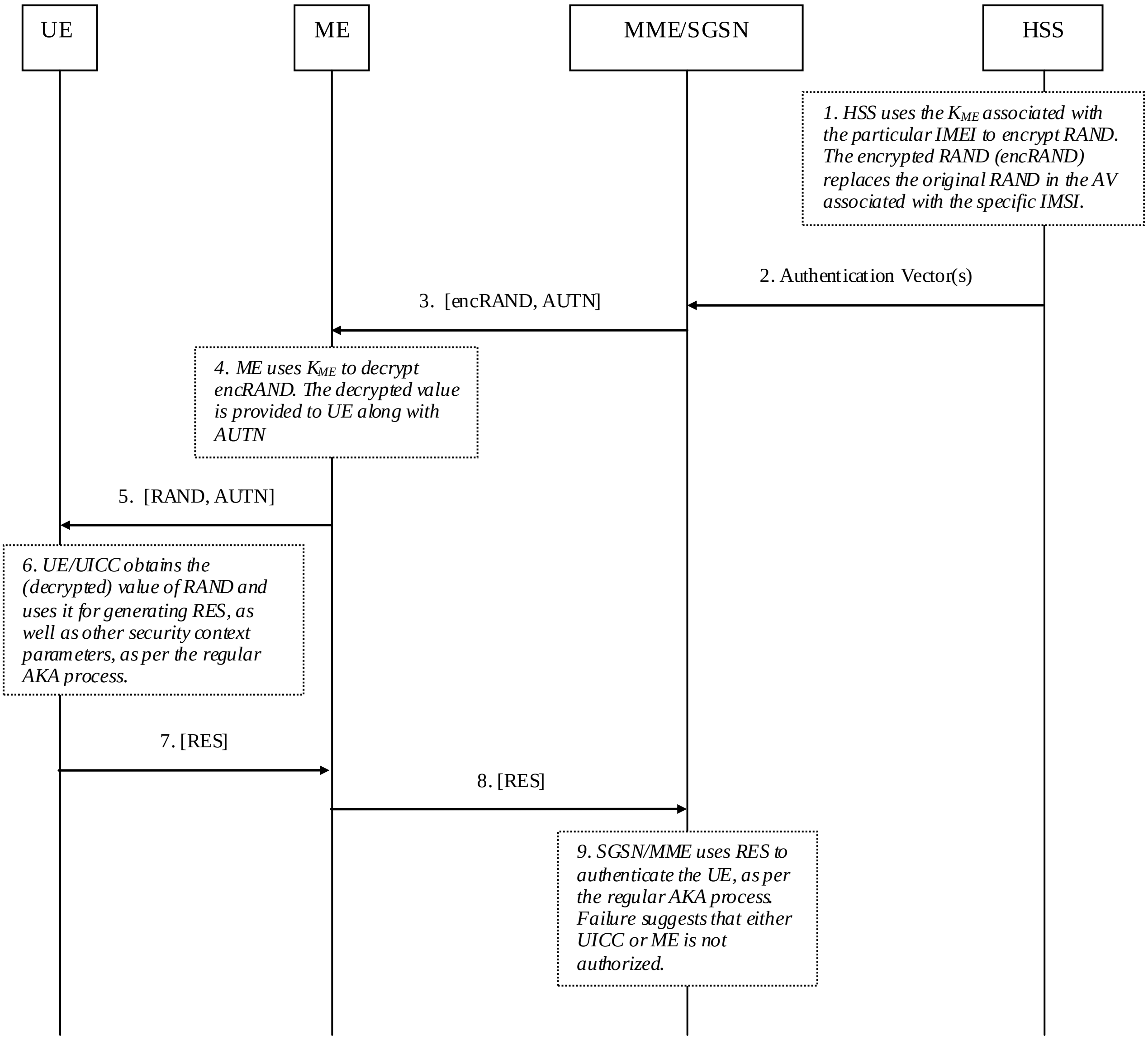

UE
ME
MME/SGSN
HSS
1. HSS uses the K_{ME} associated with the particular IMEI to encrypt RAND. The encrypted RAND (encRAND) replaces the original RAND in the AV associated with the specific IMSI.
2. Authentication Vector(s)
3. [encRAND, AUTN]
4. ME uses K_{ME} to decrypt encRAND. The decrypted value is provided to UE along with AUTN
5. [RAND, AUTN]
6. UE/UICC obtains the (decrypted) value of RAND and uses it for generating RES, as well as other security context parameters, as per the regular AKA process.
7. [RES]
8. [RES]
9. SGSN/MME uses RES to authenticate the UE, as per the regular AKA process. Failure suggests that either UICC or ME is not authorized.

Fig. 5.4.4.2.3.2-1: Binding using a shared secret between HSS and UE.

0. ***Optional step:*** ME reports the IMEI value to the 3GPP network (as per section 5.4.4.2.1).

1. When generating the Authentication Vector(s) associated with a specific IMSI, HSS uses the IMEI-IMSI association as an indicator of which K_{ME} to use for encrypting the RAND parameter that is included in each AV.

2. The AV with encrypted RAND is sent to the Serving System.

3. The MME/SGSN sends the (encrypted) RAND and AUTN parameters to the UE.

4. ME uses the pre-provisioned K_{ME} to decrypt the received encrypted value of RAND.

5. Once the RAND is decrypted, the ME forwards the (decrypted) RAND and AUTN to UICC.

6. UICC uses the received RAND value to calculate RES.

7. UICC returns the RES to the ME.

8. UE further sends the computed RES to MME/SGSN.

9. MME/SGSN compares the RES to the XRES (included in the AV sent by HSS), in order to authenticate the UE. If authentication is successful, then the IMSI-IMEI binding has been verified. If authentication is unsuccessful, then either UICC is not valid, or UICC has been installed into an unauthorised device. In either case, service will not be granted.

The K_{ME} key needs to be securely stored in the ME and in the HSS.

Editor's Note: Impact to HSS need further analysis.

5.4.4.2.3.3 Examples of KME Establishment Procedure

Provisioning of the same K_{ME} into the UE and into HSS is use-case dependent. For example, K_{ME} can be provisioned into the device by the manufacturer and then provisioned into the HSS using offline methods. As another example, K_{ME} can be provisioned into the device and into the HSS by the 3GPP operator. Alternatively, K_{ME} can be provisioned into the device and provided to the 3GPP operator by an affiliated third party. Depending on the business model, these use cases may be applicable in scenarios when operator is known and/or not known at manufacturing time. There are cases such that K_{ME} needs to be updated (e.g., device is sold or operator changes).

Typically, the exact details of K_{ME} provisioning into device and into the HSS are outside the scope of 3GPP. However, for the business model where the K_{ME} is established or updated by the 3GPP operator (e.g., device is sold or operator changes), the provisioning procedure may be specified to ensure interoperability. The following examples describe K_{ME} provisioning procedures for different use cases.

5.4.4.2.3.3.1 K_{ME} Generated and Provisioned by the HSS, and shared with the CNN

This procedure describes the case of a core network that has been enhanced to support the device binding function to load a new K_{ME} into a device.

The key highlights of this procedure:

- It does not require state in the HSS during the procedure of loading a (new) K_{ME}
- It separates the device authentication and loading of K_{ME} from the Location update procedure. This means that if there are other use cases that require Device authentication or loading of a K_{ME} then the procedures are more likely to apply without modification, e.g. no need to separate from Location update procedure. Similarly the Device authentication could be run at any time as it becomes a standalone procedure.
- It is aligned with the flow in section 5.4.4.2.1.3 for the simpler network binding in that everything is complete at serving core network once it sends the Location update complete and it only require the HSS to check the IMSI/IMEI binding here to complete the attach procedure.

This procedure follows the basic principles listed below:

- The HSS send KME to the serving core network
- The serving core network node (CNN) is responsible for generating the Nonce that is used to challenge the UE and checking the response.
- If the authentication of the UE is successful, then the serving network node sends the KME back to the HSS/HLR along with the IMSI and IMEI in the Update Location message

The following figure 5.4.4.2.3.3.1-1 shows the message flows:

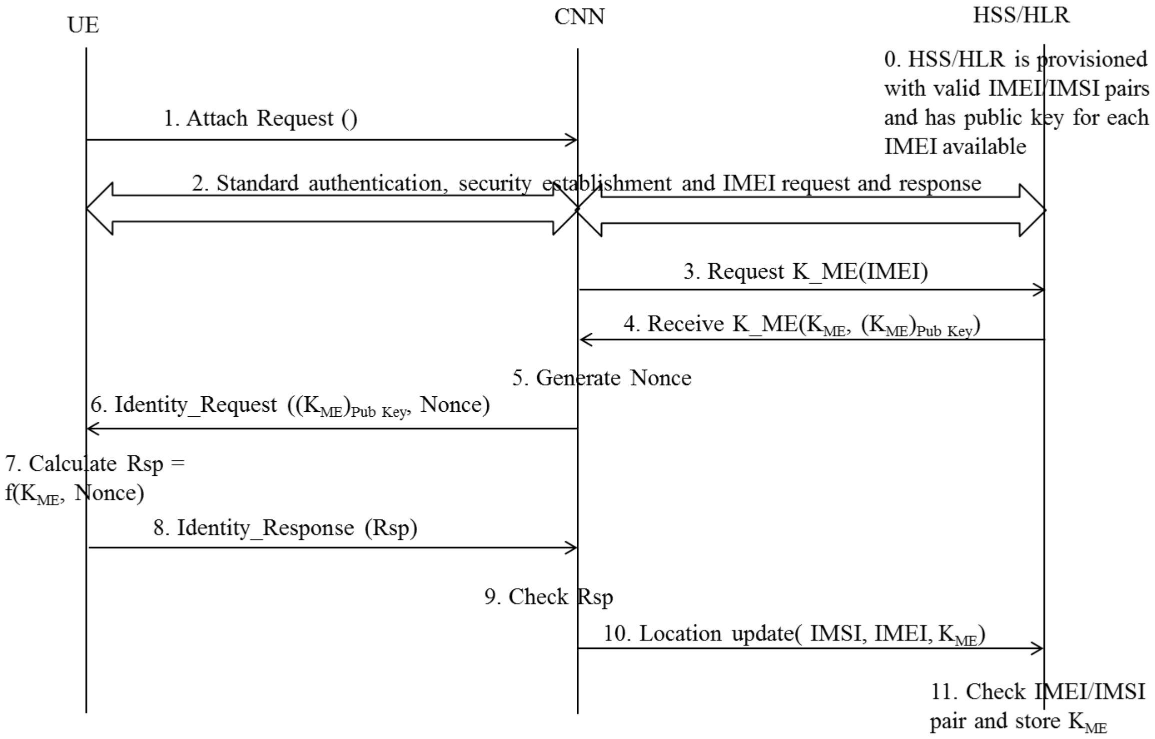

UE
CNN
HSS/HLR
0. HSS/HLR is provisioned with valid IMEI/IMSI pairs and has public key for each IMEI available
1. Attach Request ()
2. Standard authentication, security establishment and IMEI request and response
3. Request K_ME(IMEI)
4. Receive K_ME(K_ME, (K_ME)Pub Key)
5. Generate Nonce
6. Identity_Request ((K_ME)Pub Key, Nonce)
7. Calculate Rsp = f(K_ME, Nonce)
8. Identity_Response (Rsp)
9. Check Rsp
10. Location update(IMSI, IMEI, K_ME)
11. Check IMEI/IMSI pair and store K_ME

Fig. 5.4.4.2.3.3.1-1 K_{ME} Provisioned by the HSS with assistance of the CNN

The following only includes the changes to the legacy procedures.

0. The HSS/HLR has been pre-provisioned with a list of allowable IMSI/IMEI pairs and the public key associated with the IMEIs are available to the HSS/HLR.
1. The UE performs the normal attach procedure.
2. The CNN and UE complete an authentication, establishment of security. The core network node also request and receives the IMEI from the UE.
3. The core network node request an encrypted KME from the HSS/HLR. It does this by sending the HSS/HLR the IMEI.
4. The HSS/HLR generate a new KME and encrypts it with the public key of the received IMEI and sends both the encrypted KME and KME to the core network node.
5. The CNN generates a Nonce to challenge the UE.
6. The CNN sends the encrypted KME, Nonce to the UE.
7. The UE decrypts KME and calculates the Rsp from KME and Nonce.
8. The UE sends the Rsp back to the CNN.
9. The CNN checks the Rsp is correct
10. The CNN sends the location update including the new KME to the HSS/HLR.
11. The HSS/HLR stores the KME with the IMSI if the IMSI/IMEI pair is allowed.

5.4.4.2.3.3.2 K_{ME} Generated and Provisioned by the HSS, and not shared with the CNN

In this variation of the procedure, as in the 5.4.4.2.3.3.1, the core network that has been enhanced to support the device binding function to load a new K_{ME} into a device. However, it differs from the procedure in 5.4.4.2.3.3.1 in a way that the CNN does not know the provisioned K_{ME}.

As in 5.4.4.2.3.3.2, the key highlights of this procedure:

- It does not require state in the HSS during the procedure of loading a (new) K_{ME}
- It separates the device authentication and loading of K_{ME} from the Location update procedure.
- It is aligned with the flow in section 5.4.4.2.1.3 for the simpler network binding in that everything is complete at serving core network once it sends the Location update complete and it only require the HSS to check the IMSI/IMEI binding here to complete the attach procedure.

This procedure follows the basic principles listed below:

- The HSS sends the K_{ME} and a random Nonce, encrypted by the UE's Public Key, to the UE through the serving core network. The Nonce is used to challenge the UE for the response, Rsp, that is later checked.
- It order to avoid retaining the K_{ME} by the HSS until the completion of provisioning, the HSS also sends the "Cookie" that represents the privately encrypted value of the K_{ME}. Only the HSS knows the encryption/decryption key for this cookie.
- In addition, the HSS sends to the CNN the expected hash response from the UE, XRes.
- The serving core network node (CNN) simply forwards the encrypted payload to the UE, and keeps the Cookie and XRsp.
- Once the UE decrypted the K_{ME}, and generated the Rsp, the CNN is responsible for checking this response.
- To assure the HSS that the UE indeed properly decrypted the K_{ME}, the UE may optionally also generate a digital signature of the K_{ME} and return it to the CNN.
- If validation of the Rsp in the CNN is successful, the serving network node sends the DSA of K_{ME} as well as the Cookie back to the HSS/HLR along with the IMSI and IMEI in the Update Location message.
- The HSS decrypts the Cookie obtaining the K_{ME}, optionally validates received digital signature of the K_{ME}, and stores the K_{ME} in the subscription database.

The following figure 5.4.4.2.3.3.2-1 shows the message flows:

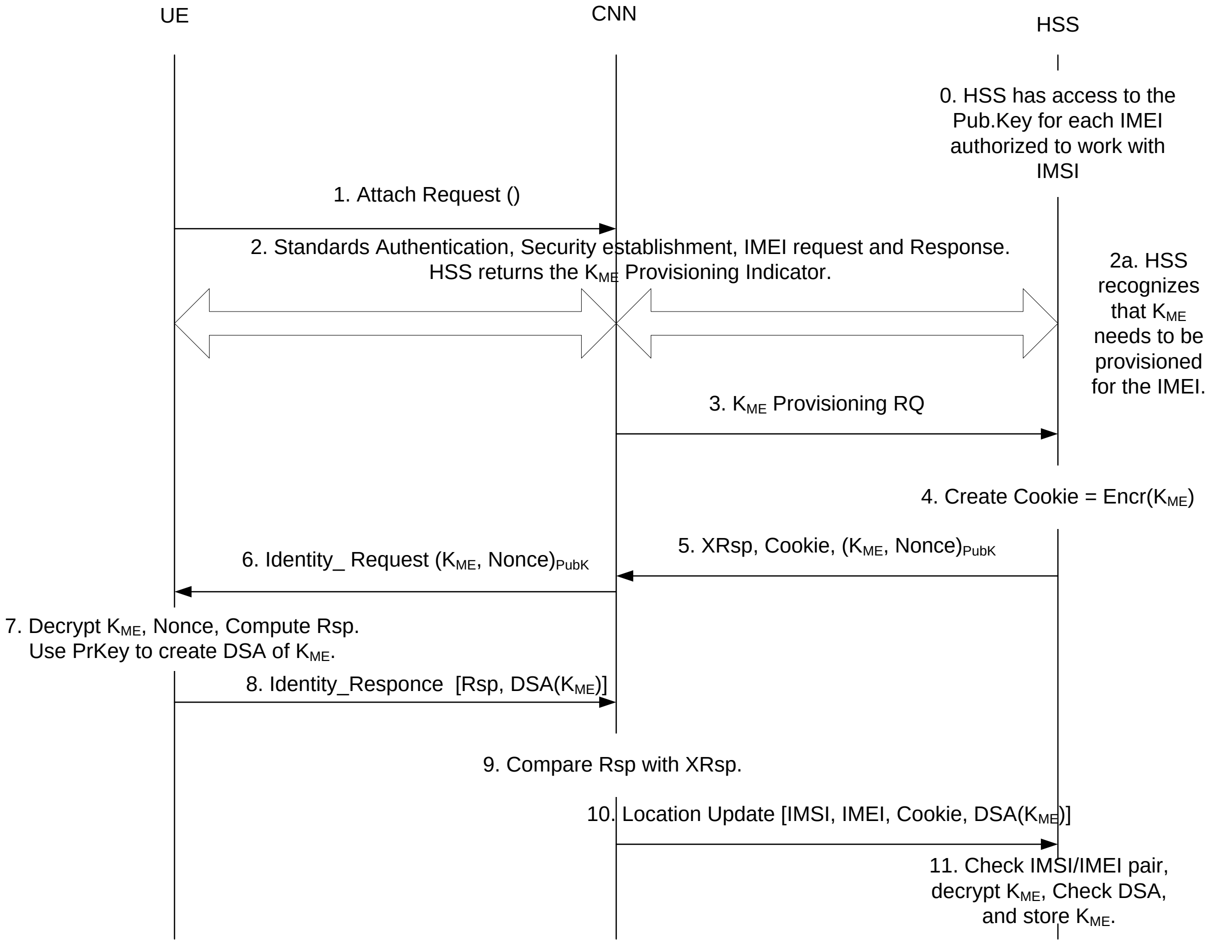

UE
CNN
HSS
0. HSS has access to the Pub.Key for each IMEI authorized to work with IMSI
1. Attach Request ()
2. Standards Authentication, Security establishment, IMEI request and Response. HSS returns the KME Provisioning Indicator.
2a. HSS recognizes that KME needs to be provisioned for the IMEI.
3. KME Provisioning RQ
4. Create Cookie = Encr(KME)
5. XRsp, Cookie, (KME, Nonce)PubK
6. Identity_ Request (KME, Nonce)PubK
7. Decrypt KME, Nonce, Compute Rsp. Use PrKey to create DSA of KME.
8. Identity_Responce [Rsp, DSA(KME)]
9. Compare Rsp with XRsp.
10. Location Update [IMSI, IMEI, Cookie, DSA(KME)]
11. Check IMSI/IMEI pair, decrypt KME, Check DSA, and store KME.

Fig. 5.4.4.2.3.3.2-1 K_{ME} Provisioned by the HSS, and not shared the CNN

0. The HSS/HLR has been pre-provisioned with a list of allowable IMSI/IMEI pairs and has an access to the public key associated with each IMEI.
1. The UE performs the normal attach procedure.

2. The CNN and UE complete an authentication, establishment of security. The core network node also request and receives the IMEI from the UE.
    a. The HSS realizes that the IMSI/IMEI Binding is required, but K_{ME} is not yet provisioned. The HSS indicates to the CNN that Provisioning of the K_{ME} is expected.
3. The CNN request an encrypted K_{ME} from the HSS/HLR. It does this by sending the HSS/HLR the IMEI.
4. The HSS/HLR generates a new K_{ME} and encrypts it with the public key (PubK) of the received IMEI. The HSS also encrypts the K_{ME} with the local block encryptor producing the Cookie. The encryption key for producing the Cookie is kept in the HSS, and not shared with any entity. It is only needed for decrypting the Cookie again when received back from the CNN. The HSS generates the random Nonce, and hashes it with K_{ME} producing expected response XRsp.
5. The HSS sends the encrypted $(K_{ME}$, Nonce$)_{PubK}$, Cookie, and XRsp to the CNN.
6. The CNN forwards the $(K_{ME}$, Nonce$)_{PubK}$ the UE.
7. The UE decrypts the K_{ME} using its Private Key (PrK). The UE hashes the K_{ME} and Nonce to produce the Rsp. The UE also uses it Private Key (PrK) to generate the DSA of K_{ME}. The reason for this is explained in Step 11.
8. The UE returns the Rsp and DSA(K_{ME}) to the CNN.
9. The CNN compares the Rsp with XRsp, and if match, proceeds to Step 10.
10. The CNN generates the Location Update Request towards the HSS, including the IMSI, IMEI, the Cookie, and the DSA(K_{ME}).
11. The HSS uses its internal secret to decrypt the Cookie and obtain the K_{ME}. The HSS then use the Public Key associated with the IMEI to verify the DSA of K_{ME}. If verification is successful, the HSS gets assured that the Cookie was not substituted by unscrupulous CNN and the K_{ME} was properly decrypted and accepted by the legitimate ME. The HSS stores the K_{ME} in association with the IMEI if the IMSI/IMEI pair is allowed.

5.4.4.2.3.3.3 K_{ME} Generated by the ME

As in 5.4.4.2.3.3.1, the device has been provisioned at manufacture with a pair of Private Key and associated Public Key that are uniquely associated with the IMEI of the device. The Private Key is stored in the device secure area, while the Public Key is deposited into a common database accessible to Network Operators, or their provisioning systems.

In addition, the device is provisioned at manufacture with the manufacturer-specific Modulus N which represents the product of two large prime numbers P and Q (N=PQ). Requirements for selection of prime factors P and Q are as defined in ANSI X9.31 for RSA algorithm. The Primes P and Q are secret, and known to the HSS as associated with specific manufacturer. Manufacturer may choose to vary the P, Q, and N on a per-manufacturing lot basis, or other criteria. But knowing the IMEI, the HSS should be able to obtain required P and Q.

When the newly subscribed UE accesses the network, and the HSS determines that it does not have the binding information for the subscription, or if the HSS needs to find out the IMEI of the device used by the subscription (IMSI), the HSS may decide to invoke the provisioning procedure to establish the K_{ME} in the device.

In order to conduct provisioning procedure, the HSS will allow authenticated access without using the device binding. For that the HSS issues the regular, un-processed AV (RAND not encrypted) because the binding association has not yet been established. The AV is indicated as regular (See sec.5.4.4.2.3.4) using Binding Feature Control. By using conventional LTE capabilities, the HSS requests and receives the device IMEI.

HSS indicates to the MME that the access is authorized only and exclusively for the special purpose of provisioning binding credentials. Therefore any bearer establishment is disallowed.

The air interface and NAS security can be invoked at this point, so all subsequent interactions with the UE will be protected.

The ME-based provisioning functionality does the following:

- the ME generates a random K_{ME},
- by using the provisioned Private Key, the ME generates the Digital Signature of the K_{ME} , the K_{ME}_SIG, as specified in FIPS-186-3.
- the ME generates a random nonce R_{ME}.
- the ME concatenates (K_{ME}|K_{ME}_SIG|R_{ME}) and encrypts it using the RSA algorithm

{K_{ME}|K_{ME}_SIG|R_{ME}}' = {K_{ME}|K_{ME}_SIG|R_{ME}}^e mod N,

where e is a predetermined Public Exponent, e.g. 2^{16}, and N is specific for the device manufacturer.

- In addition, the ME pre-computes the expected signature of the network, the xNW_SIG, as a hash of K_{ME} and R_{ME}.

  xNW_SIG = SHA256(K_{ME}|R_{ME})

The encrypted {K_{ME}|K_{ME}_SIG|R_{ME}}' is returned to the MME, which delivers it to the HSS along with the IMEI of the device.

The HSS decrypts the received {K_{ME}|K_{ME}_SIG|R_{ME}}' using the P and Q associated with the manufacturer of the device. The HSS then retrieves the Public Key associated with the IMEI of the device. Security of this retrieval is outside the scope of 3GPP, but it is expected that only legitimate MNO can request and receive the Public Key associated with the device. The HSS then validates the K_{ME}_SIG, and if valid – accepts the K_{ME}.

To prove to the ME that the HSS properly decrypted the K_{ME}, the HSS generates the NW_SIG:

NW_SIG = SHA256(K_{ME}|R_{ME})

The computed NW_SIG is returned to the ME which compares it to the pre-computed xNW_SIG. If validation succeeds the K_{ME} is activated in the ME, and is populated into the HSS subscription database and can now be used for pre-processing authentication vectors.

During the next network access the HSS will expect the device to use the binding feature, and will generate a pre-processed AV.

The general process of K_{ME} establishment is shown on Fig.5.4.4.2.3.3.3-1.

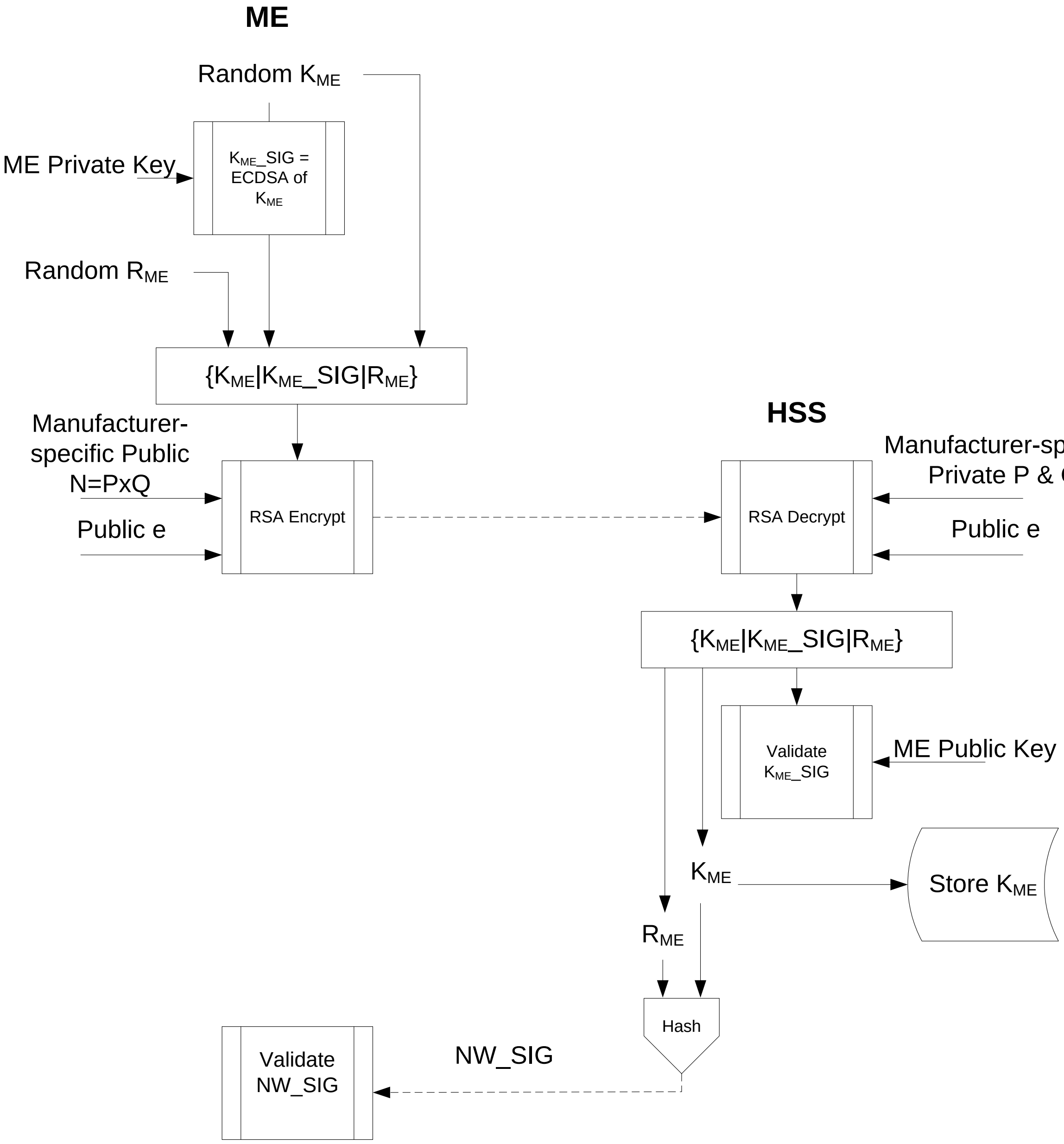


Fig.5.4.4.2.3.3.3-1 K_{ME} Establishment - General Process

The message flow for K_{ME} establishment is shown on Fig. 5.4.4.2.3.3.3-2.

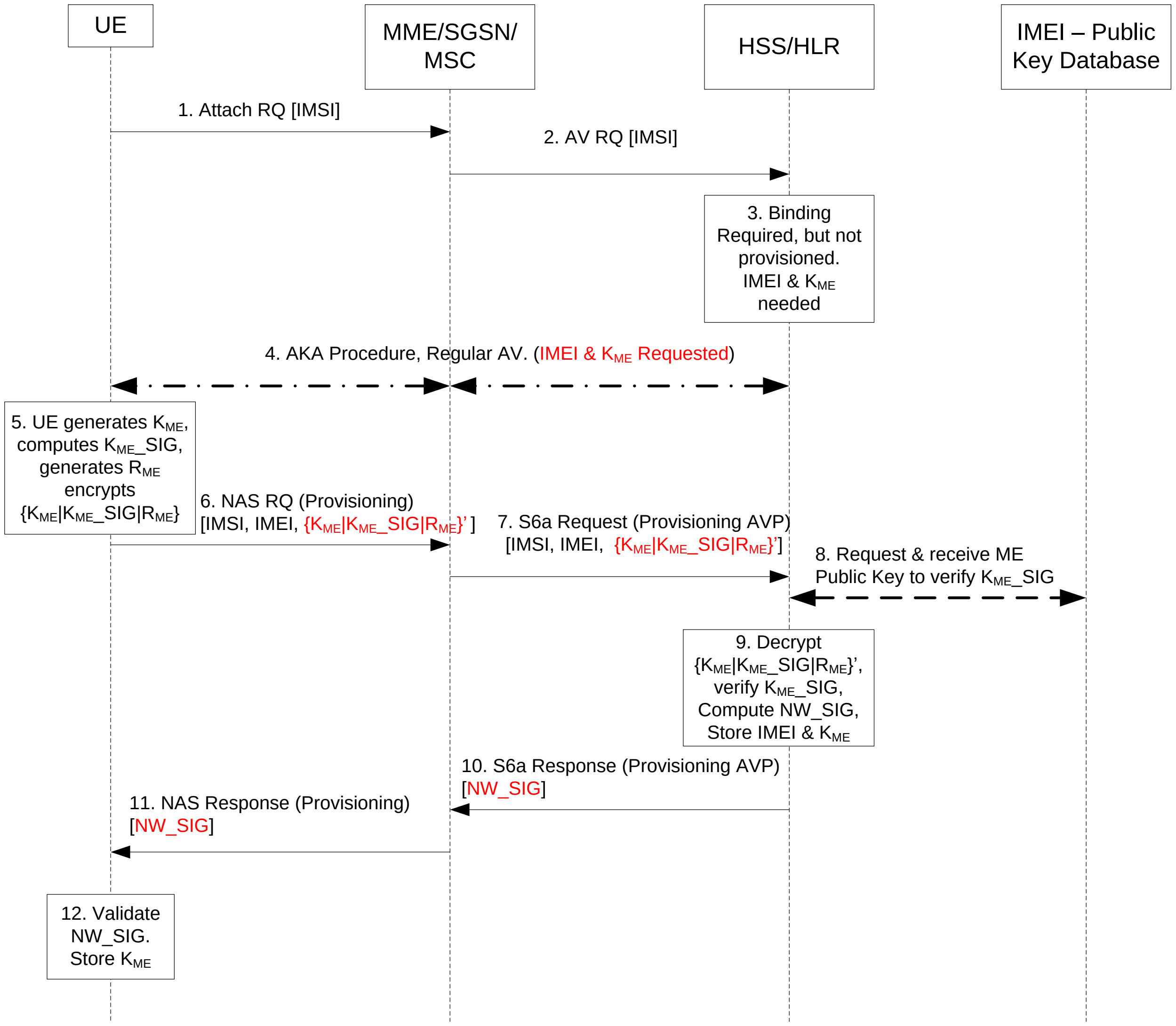

UE
MME/SGSN/ MSC
HSS/HLR
IMEI – Public Key Database
1. Attach RQ [IMSI]
2. AV RQ [IMSI]
3. Binding Required, but not provisioned. IMEI & K_ME needed
4. AKA Procedure, Regular AV. (IMEI & K_ME Requested)
5. UE generates K_ME, computes K_ME_SIG, generates R_ME encrypts {K_ME|K_ME_SIG|R_ME}
6. NAS RQ (Provisioning) [IMSI, IMEI, {K_ME|K_ME_SIG|R_ME}']
7. S6a Request (Provisioning AVP) [IMSI, IMEI, {K_ME|K_ME_SIG|R_ME}']
8. Request & receive ME Public Key to verify K_ME_SIG
9. Decrypt {K_ME|K_ME_SIG|R_ME}', verify K_ME_SIG, Compute NW_SIG, Store IMEI & K_ME
10. S6a Response (Provisioning AVP) [NW_SIG]
11. NAS Response (Provisioning) [NW_SIG]
12. Validate NW_SIG. Store K_ME

Fig. 5.4.4.2.3.3.3-2 K_{ME} Establishment – Message Flow

1. UE accesses the network for service. UICC with IMSI is installed in the ME. The K_{ME} is not provisioned, or is unknown to the Home Operator.
2. MME/SGSN/MSC requests the Authentication Vector to authenticate the IMSI of the UE.
3. HSS determines that reported IMSI needs to be bound to the device, but the Binding Credential (K_{ME}) is not yet established. In addition, the HSS needs to obtain the IMEI of the ME currently used by the subscription.
4. HSS issues the regular, un-processed Authentication Vector. The AKA Authentication procedure is initiated. The UE recognizes that the received Authentication Challenge is un-processed, and forwards it to the UICC. AKA Authentication is concluded with un-processed AV. In PS GERAN and PS UTRAN the SGSN/MSC can also request and receive the IMEI of the ME in this transaction.

   Note: HSS shall indicate to the MME that the access is authorized only and exclusively for the special purpose of provisioning binding credentials. Therefore any bearer establishment is disallowed.

   Note: The MME indicates to the ME that the provisioning of the K_{ME} is initiated.

   As in 5.4.4.2.3.3.1, the IMEI is obtained from the ME

5. The ME generates random K_{ME}, computes digital signature K_{ME}_SIG using device-specific Private Key, generates a random nonce R_{ME}, and encrypts the (K_{ME}|K_{ME}_SIG|R_{ME}) using RSA encryption with manufacturer-specific Modulus N.
6. The ME sends the NAS message to the MME containing the IMSI, IMEI, and encrypted (K_{ME}|K_{ME}_SIG|R_{ME})). Specific suitable NAS transaction can be selected by CT1.

7. The MME initiates the S6a transaction defined for establishment of binding credentials. In this message the MME sends the IMSI, IMEI, and encrypted (K_{ME}|K_{ME}_SIG|R_{ME}) in the new AVP to the HSS.
8. The HSS obtains the Public Key for the ME from a database associated with the received IMEI.
9. HSS obtains the P & Q factors of N associated with device manufacturer, and decrypts the (K_{ME}|K_{ME}_SIG|R_{ME}) payload. Using received factors, the HSS decrypts the (K_{ME}|K_{ME}_SIG|R_{ME}) payload. The HSS validates the K_{ME}_SIG using the ME Public Key. If validation succeeds, the HSS stores the K_{ME} in the subscription record database in association with the bound IMEI. The HSS generates its own hash of the K_{ME}, the NW_SIG, using decrypted R_{ME} as a freshness parameter.
10. The HSS sends the S6a response (e.g. Update Location Response) to the MME, including the NW_SIG in the new AVP.
11. The response is delivered to the UE in a NAS response.
12. The ME validates the received NW_SIG. If validation succeeds, the ME activates the K_{ME} in its secure memory for binding compliance.

5.4.4.2.3.4 Network Control of Binding Feature

For normal operation of the binding feature the HSS has to clearly know whether or not the K_{ME} is established in the device associated with authenticated subscription. If this knowledge is uncertain, e.g. the device is transferred from another MNO and K_{ME} cannot be obtained before the initial network access, or the HSS needs to obtain the device' IMEI before selecting the K_{ME}, the HSS has to assume that K_{ME} is unknown. In such case the binding verification has to be omitted for the initial network entry, i.e. the AV shall not be pre-processed (the RAND is not encrypted). Consequently, UE also must be made aware that binding verification is omitted, and post-processing (decryption) of RAND must be bypassed.

This constitutes Control of the Binding Feature retained by the HSS.

Several alternatives could be considered to indicate to the UE that the AV sent by the HSS is or is not pre-processed. Each alternative presented in this section leaves the use of binding feature completely under control of the HSS with no involvement of MME, eNB, or UICC. Other indication alternatives could be considered as well.

For example, indication can be provided by setting Bit 1 of AMF field to '1' for the AV with encrypted RAND. This means that HSS has to decide on setting this bit appropriately before the AV is computed. Setting this bit to '0' (default) would indicate a regular un-processed AV with original RAND. Upon receiving the Authentication Challenge the ME will examine the Bit 1 of the AMF and determine whether or not to post-process (decrypt) the RAND.

Alternatively, indication can be provided by using special value of 128-bit RAND. For example, while generating a RAND for the AV targeted to omit pre-processing, the HSS will truncate the RAND to 64 most significant bits, and then fill the remaining 64 least significant bits of RAND with the copy of the 64 most significant bits remaining random. Upon receiving the RAND, the ME will check if each half of the RAND is an exact copy of the other half, and if so, will pass the AV to the UICC unprocessed. Otherwise, the RAND will be decrypted before being sent to the UICC. To avoid possible collisions, after the RAND is encrypted the HSS has to check if the resulting encrypted RAND does not (with a negligible probability) follow the rule of the special RAND, and if so, HSS will have to purge this AV, and generate the new AV with another RAND.

In another alternative, the randomly generated 128 bit RAND is truncated to 96 bits, and the 32-bit hash is computed of it. The resulting 32 bit hash is appended to the retained 96 bits to produce the 128-bit RAND of the AV that does not have to be post-processed. The UE, upon receiving the AV, will compute the 32-bit hash of the 96 msb of the received RAND, and compare it to the remaining 32 bits of the RAND. If match is discovered, the AV is presented to the UICC unprocessed. Otherwise, the RAND is presented for decryption with whatever the K_{ME} value is programmed in the ME.

Although alternatives that use special RAND reduce unpredictability of RES, which may be undesirable, the use of the un-processed vector with special RAND is expected to be rare, and limited to cases when Binding feature must be bypassed for the specially equipped device. Indication by the Bit 1 in AMF does not have any effect on RES unpredictability, and is preferred.

5.4.5 Evaluation

Editor's Note: Denial of Service and resource exhaust attacks needs to be taken in to account.

5.4.5.1 User Equipment-based pairings

5.4.5.1.1 Secure Channel pairing

- The Secure Channel pairing prevents the connection of not-authorized UE to the network. When the UICC detects its presence in a not-authorized UE (not-authorized ME or a non-MTC ME), the UE stops working. The network operator or MTC application user has no information why the UE has stopped working.

- The exchanges to perform the secure channel pairing are only between the UICC and the MTC ME. The pairing does not require any additional signalling on the network.

- When the USIM detects its presence in not- authorized UE, the network resources are not consumed since the UE does not try to connect to the network.

  - o There is no signalling (e.g. for attach procedure, mutual authentication between the UE and the network), no authentication vector consumption.

- To establish the secure channel, a mutual authentication is performed between the USIM and the MTC ME.

- After the secure channel establishment, all the data exchanged between the USIM and the MTC ME are protected.

- A secure environment is required in the terminal part of the UE for the secure channel establishment.

- This solution create extra cost per MTC ME and per UICC and the UICC should support secure channel or TLS

- Secure channel pairing is the mechanism already selected and specified for Rel-10 Relay Node security to guaranty one-to-one binding between a USIM and a RN.

- Fulfills the SA1 requirement on restrict the use of a USIM to specific UEs and fulfils the requirement that operator shall be able to enforce the restriction.

  - o The UICC is under the control of the operator. The USIM checks if the combination of USIM and MTC ME is authorized and the list of authorized IMEI(SV) values or IMEI(SV) ranges stored on the USIM can be modified by the operator thanks to UICC OTA mechanism. In this way the operator can control the restriction of USIM to specific MTC MEs.

- Fulfills the SA1 requirement for monitoring that the system shall provide mechanisms to detect change of the association between the MTC ME and the UICC.

  - o The information stored in the file $EF_{pairing}$ provides a mechanism to detect change of association between a USIM and a MTC ME. The information stored in the file $EF_{pairing}$ can be read out locally by the maintenance persons.

- In case of operator change, i.e. when a new UICC from a new operator is inserted to a UE on the field, this solution does not provide a mechanism how to install the new shared secret or certificate in the UE needed for the secure channel.

- In case the UICC needs to be moved from an UE to a new UE which is on the field, the IMEI and shared secret or certificate need to be updated on the UICC when the UICC is still hosted by the old UE. If the old UE is no longer allowed to be associated to the UICC, then the old IMEI value should be removed from the UICCC when the UICC is hosted by the new UE.

- In case of certificate based secure channel, the certificate in the UE cannot in the general case be operator certificate since the operator is not always known at manufacturing time of MTC ME. In this case the UICC needs to be updated with the root certificate of the ME vendor when the UE is taken into use.

- It is not possible to manipulate the data that controls the pairing on the UICC from when the UICC is sent by the operator until the UICC is in a UE that can successfully attached to the network. This puts some limitations on management of allowable pairings, e.g. in cases when the device that will be paired with a UICC change between the UICC being supplied to the UE owner and the UICC being actually used to enable network connectivity.

- For the symmetric key case, if it is necessary to change all the keys that are held on one device, e.g. due to the device being considered compromised, then it is necessary to change the key on all UICCs that can be paired with that device. In addition, all the devices that require the key of the UICCs that have been updated would also need to be updated.

5.4.5.1.2 USAT application pairing

- The USAT application pairing prevents the connection of not-authorized UE to the network. When the UICC detects its presence in a not-authorized UE (not-authorized ME or a non-MTC ME), the UE stops working. The network operator or MTC application user has no information why the UE has stopped working.
- The data exchange to perform the USAT application pairing is performed only between the UICC and the MTC ME. The pairing does not require any additional signalling on the network.
- When the USIM detects its presence in not authorized UE, the network resources are not consumed since the UE does not try to connect to the network.
    - There is no signalling (e.g. for attach procedure, mutual authentication between the UE and the network), no authentication vector consumption.
- The security of the pairing depends on how secure the MTC ME is. The security requirements that it should not be possible to modify the IMEI already exist today (see [12] and [13]). There is no mechanism available to verify the integrity of the IMEI whether it is modified or not by the entity which enforce the pairing.
- There are existing methods today with which the IMEI may be modified in the storage and also during transmissions.
- Exchange of IMEI value between the ME and the UICC is not integrity protected and encrypted.
- Fulfills the SA1 requirement on restrict the use of a USIM to specific UEs and fulfils the requirement that operator shall be able to enforce the restriction.
    - The UICC is under the control of the operator. The USIM checks if the combination of USIM and MTC ME is authorized and the list of authorized IMEI(SV) values or IMEI(SV) ranges stored on the USIM can be modified by the operator thanks to UICC OTA mechanism. In this way the operator can control the restriction of USIM to specific MTC MEs.
- Fulfills the SA1 requirement for monitoring that the system shall provide mechanisms to detect change of the association between the MTC ME and the UICC.
    - The information stored in the file $EF_{pairing}$ provides a mechanism to detect change of association between a USIM and a MTC ME. The information stored in the file $EF_{pairing}$ can be read out locally by the maintenance persons.
- The MTC ME should support the USAT functionality
- In case the UICC needs to be moved from an UE to a new UE which is on the field, the IMEI needs to be updated on the UICC when the UICC is still hosted by the old UE. If the old UE is no longer allowed to be associated to the UICC, then the old IMEI value should be removed from the UICC when the UICC is hosted by the new UE.
- It is not possible to manipulate the data that controls the pairing on the UICC from when the UICC is sent by the operator until the UICC is in a UE that can successfully attached to the network. This puts some limitations on management of allowable pairings, e.g. in cases when the device that will be paired with a UICC change between the UICC being supplied to the UE owner and the UICC being actually used to enable network connectivity.

5.4.5.1.3 PIN verification pairing

- The PIN verification pairing prevents the connection of not-authorized UE to the network. When the UICC detects its presence in a not-authorized UE (not-authorized ME or a non-MTC ME), the UE stops working. The network operator or MTC application user has no information why the UE has stopped working.
- The exchanges to perform the PIN verification pairing are only between the UICC and the MTC ME. The pairing does not require any additional signalling on the network.

- When the USIM detects its presence in not authorized UE, the network resources are not consumed since the UE does not try to connect to the network.
    - There is no signalling (e.g. for attach procedure, mutual authentication between the UE and the network), no authentication vector consumption.
- PIN verification pairing could rely on existing PIN verification command already available on UE. But the PIN value should be stored in the MTC ME.
- The provisioning of PIN value in the MTC ME for pairing purpose is a new feature since the existing PIN verification is a user authentication without storage of PIN value in the ME. A secure environment is required in MTC ME for the storage of PIN value.
- The storage of PIN value in the MTC ME for pairing purpose requires a method to provision or personalize the PIN value in the MTC ME, which can be realized via off-line provisioning or remotely, e.g. sending PIN to UICC though OTA and to device via OMA DM..
- The entropy of the PIN secret is low, thus is subject to brute force attacks
- The security of the pairing depends on how secure the MTC ME is.
- PIN value is sent in clear on the interface between the MTC ME and the UICC, which makes it possible for an attacker to wire-tap on the interface and find out the PIN. This risk can partially be mitigated by the operator, e.g. the operator can change the PIN frequently.
- Fulfills the SA1 requirement on restrict the use of a USIM to specific UEs and fulfils the requirement that operator shall be able to enforce the restriction.
    - The UICC is under the control of the operator. The USIM checks if the combination of USIM and MTC ME is authorized and the list of authorized IMEI(SV) values or IMEI(SV) ranges stored on the USIM can be modified by the operator thanks to UICC OTA mechanism. In this way the operator can control the restriction of USIM to specific MTC MEs.
- Fulfills the SA1 requirement for monitoring that the system shall provide mechanisms to detect change of the association between the MTC ME and the UICC.
- The information stored in the file $_{\text{EFpairing}}$ provides a mechanism to detect change of association between a USIM and a MTC ME. The information stored in the file $_{\text{EFpairing}}$ can be read out locally by the maintenance persons.
- In case of UE-based pairings, the network operator is not able to detect unauthorized combinations of IMSI/IMEI or attempts to use such combinations.
- It is not possible to manipulate the data that controls the pairing on the UICC from when the UICC is sent by the operator until the UICC is in a UE that can successfully attached to the network. This puts some limitations on management of allowable pairings, e.g. in cases when the device that will be paired with a UICC change between the UICC being supplied to the UE owner and the UICC being actually used to enable network connectivity.
- PIN can be changed soon on the spot whenever the UICC is inserted to other UE, which can be used to manage the solution if an UE that holds the PIN for several UICCs is considered compromised, i.e. the operator believes all the PINs are known to an attacker. PIN can be changed on the spot, if there is an interface available in the UE for PIN change, otherwise it is not possible. Also one or more UEs to be visited to change the PIN.

Conclusion

- Pairing methods using Secure Channel , USAT mechanisms are based on existing 3GPP and ETSI standards,
- All UE-based pairing methods prevent MTC UE with not-authorized binding association from connection to the network and, as consequence, from consumption of signalling and network resources.
- Among the User Equipment-based pairings, the Secure Channel pairing offers the highest level of security and reliability to restrict the use of a USIM to specific UEs

- The PIN verification pairing mechanism can be used to restrict the USIM to specific UEs. It has comparatively simple implementation, and reliability to restrict the use of a USIM to specific UEs although there are some risks (e.g. only the USIM authenticates the UEs, PIN is low-entropy secret and sent in the clear), but they can partially be avoided by the operator.

5.4.5.2 Network based pairings

5.4.5.2.1 IMSI-IMEI binding in HSS

- Fulfills the SA1 requirement on restrict the use of a USIM to specific UEs and fulfils the requirement that operator shall be able to enforce the restriction.

- Fulfills the SA1 requirement for monitoring that the system shall provide mechanisms to detect change of the association between the MTC ME and the UICC.

- The network operator is able to directly detect if unauthorized combination of IMSI/IMEI is taken into use, and may then take any appropriate action in the network as e.g. trigger an alarm in the HSS.

- Signalling procedures for the network request of IMEI or IMEISV from the UE are already in place in 3GPP specifications for GERAN, UTRAN and E-UTRAN. But the current HSS/HLR does not support this new pairing function. This solution requires the ADD (Automatic Device Detection) feature to be supported and enabled in the SGSN/MME/MSC. Using ADD for requesting IMEI(SV) from the UE is commonly used in networks today to detect when a user has purchased a new UE so that e.g. appropriate MMS and internet access settings can be sent to user's new UE. Therefore in many cases the solution does not add signaling load in the network.

- As ADD is already defined and in use in many networks, the cost and complexity has been largely covered in those networks. Additionally the HSS/HLR needs to do IMSI/IMEI pair checking which is considered to be reasonably low effort and simple task comparing to what the HSS is already doing at an Attach.

- For the reasons above, the solution is not regarded to add DoS or resource exhaustion attack possibilities.

- The solution requires no new functionality on the UE.

- The operator can use their current UICCs

- According to existing security requirements in E-UTRAN (since Rel-8), the UE shall provide its equipment identifier IMEI or IMEISV to the network, only if the network asks for it in an integrity-protected request.

- According to existing security requirements in E-UTRAN (since Rel-8), the UE shall integrity protect the IMEI or IMEISV on the air interface to the network.

- The security of the IMEI/IMEISV in the MTC ME depends on how secure the MTC ME is. Already today there exist security requirements that it should not be possible to modify the IMEI (see [12] and [13]).

- This binding mechanism needs to be implemented in the network even though it is not be used for all UEs.

- All MTC UEs, including the ones with not-authorized binding, need to be authenticated by the network and consume HSS capacity.

- This solution enables network operator to remotely detect the binding.

- There are some network signalling impacts.

- If there is a need to change authorized combinations of IMSI/IMEI (e.g. due to billing plan change), only the information in the HSS/HLR needs to be updated, There is no need to update any other entities.
    - Therefore there is neither need for additional signalling nor need for developing solutions for updating the authorized combinations of IMSI/IMEI in network-based pairings.

Conclusion:

- The network operator is able to detect and reject unauthorized combinations of IMSI/IMEI in the HSS and take appropriate action thereby fulfilling the SA1 requirements.

- The needed functionally for the network to request IMEI or IMEISV from the MTC UE as part of ADD is already in place in 3GPP specifications and commonly used in networks. Additionally the HSS/HLR needs to do IMSI/IMEI pair checking which is considered to be reasonably low effort and simple task comparing to what the HSS is already doing at an Attach.
- Most of the functionalities needed is already available, new mechanism is needed in HSS for binding method.
- MTC UEs with not-authorized binding combination equally consume signalling and network resources.
- Dynamic management of allowed IMSI/IMEI pairs in concentrated on one point, the HSS/HLR. If there is a need to change authorized combinations of IMSI/IMEI (e.g. due to billing plan change), only information in the HSS/HLR nodes needs to be updated, There is no need to update any other entities.
- This does not prevent the usage of IMEI in the tampered UE where the IMEI can be modified.

5.4.5.2.2 Enhanced AKA

- The network operator is able to directly detect if unauthorised combination of IMSI/IMEI is taken into use, and may then take any appropriate action in the network.
- If there is a need to change authorised combinations of IMSI/IMEI (e.g. due to billing plan change), only the authorised combinations in the HSS/HLR need to be updated,
- The operator can use their current UICCs
- Changes to the current signalling that need to be standardised are required between the core network and UEs and between core network nodes for this solution
- A secure environment is required in ME for the storage of certificate/private key.
- The security of the IMEI/IMEISV in the ME is ensured by additional authentication executed after AKA authentication that also provides keys to protect the traffic sent between UE and network.
- This binding mechanism shall be implemented in the network ~~e~~even though it is not be used for all UEs.
- All MTC UEs, including the ones with not-authorized binding, shall be authenticated by the network and consume HSS capacity.
- These also enables network operator to detect the binding.

Conclusion:

- Fulfills the SA1 requirement on restrict the use of a USIM to specific UEs and fulfils the requirement that operator shall be able to enforce the restriction.
- Fulfills the SA1 requirement for monitoring that the system shall provide mechanisms to detect change of the association between the MTC ME and the UICC.
- The solution only needs to change authorized combinations of IMSI/IMEI in the HSS/HLR
- The solution introduces some signalling changes between network entities and the UE for the AKA enhancement that are not yet standardised.
- New mechanism is needed in HSS for binding method.
- MTC UEs with not-authorized binding combination equally consume signalling and network resources.
- This method prevents usage of IMEI in the tampered UE where the IMEI can be modified.

5.4.5.2.3 Pairing based on symmetric shared secret

- The network operator is able to directly detect if unauthorised combination of IMSI/IMEI is taken into use, and may then take any appropriate action in the network.
- If there is a need to change authorised combinations of IMSI/IMEI (e.g. due to billing plan change), only the authorised combinations in the HSS/HLR need to be updated,

- The IMEI value is not used for validating whether the UE can make use of a specific UICC. In particular, this approach binds IMSI with IMEI using a shared secret (K_{ME}) between ME and HSS that is not based on IMEI value.
- The operator can use their current UICCs
- ME and HSS need to be provisioned with shared secret (K_{ME})
- Changes to the current procedures in ME and HSS to encrypt/decrypt RAND value using shared secret (K_{ME})
- A secure environment is required in ME for the storage of shared secret (K_{ME}).
- This binding mechanism shall be implemented in the network ~~e~~even though it is not be used for all UEs.
- The network attempts to authenticate all MTC UEs, including the ones with not-authorized binding, which consume HSS capacity.

Conclusion:

- Fulfills the SA1 requirement on restrict the use of a USIM to specific UEs and fulfils the requirement that operator shall be able to enforce the restriction.
- Fulfills the SA1 requirement for monitoring that the system shall provide mechanisms to detect change of the association between the MTC ME and the UICC.
- The solution does not rely on IMEI value for validation whether the UE can make use of a specific UICC
- The solution only needs to change authorized combinations of IMSI/IMEI in the HSS/HLR
- The solution introduces impact to the current procedures in HSS, AuC and ME to encrypt/decrypt RAND value using shared secret (K_{ME}).
- New mechanism is needed in HSS, AuC if the AuC is located outside the HSS, and UE for binding control method based on Special RAND to indicate whether the AV is processed or not. The binding control method utilizing AMF impacts only the HSS and the UE.
- MTC UEs with not-authorized binding combination equally consume signalling and network resources.
- This method prevents usage of IMEI in the tampered UE where the IMEI can be modified.

5.5 Privacy concern

5.5.1 Issue Details

Some types of UEs can be linked to an individual. Contrary to normal UEs, UEs used for MTC are often not under the direct control of the particular individual (i.e. can not turn it off) and may be controlled by an other party. Therefore it is necessary to investigate privacy in the context of Machine Type Communication.

In 3GPP network layer, there are many types of sensitive information. When we analyse the privacy threats, it is necessary to distinguish privacy sensitive information from other sensitive data. In the context of MTC, identity information and location information can be considered privacy sensitive information.

Different parties could invade an individual's privacy due to excessive and/or unauthorised monitoring of privacy sensitive information.

Some types of UEs may be used to trace a child to prevent him/her from being lost or kidnapped. In this case the location information of the UE should be sent to the MTC application periodically. In this scenario if the UE detaches from the network or is detached by the network, the MTC server shall be noticed of this change and take proper action.

Note: There is a category of MTC applications that depend on legal location tracking. The MTC privacy concern feature does not apply to this category of MTC applications.

5.5.2 Threats

Privacy breach due to (unnecessary) collection of location information of an UE that can be linked to an individual.

Privacy sensitive information sent by a UE which is not allowed to do so.

Privacy sensitive information requested by or sent towards a MTC server which is not allowed to do so.

If eavesdropped, the temporary identity can be actually used by attackers to trace the actions of the subscriber of the UE over an extended period of time, which would seriously affect subscriber identity confidentiality.

5.5.3 Security Requirements

- It should be possible to prevent tracking of location information for some types of UE.
- The temporary identity allocated to an UE by the network should be reallocated based on operator policy, e.g. after it has been used more than a few number of times, or for longer time than a certain time span, or event triggering is received (e.g. periodic location update).
- The network should explicitly reveal UE status, such as online/offline, idle or connected to authorized parties only, e.g. to an authorized SCS in relation to monitoring feature, cf. clause 5.11 Monitoring.
- Network should be able to verify whether a message contains any privacy sensitive information.
- Network should be able to perform authorization check of (a) UE which is sending privacy sensitive information and (b) of MTC server which is requesting / is receiving the privacy sensitive information.
- Privacy sensitive information transmitted to MTC server via network should be protected.

Editor’s Note: The last three requirements above are FFS. It needs to be clarified why the network should be able to verify if a message contains privacy sensitive information, and what an authorization check in network helps if a device or MTC server has already sent privacy sensitive information.

- It should be possible to guarantee legal privacy information collection not to be interrupted or the interruption can be detected in time.

5.5.4 Solutions

5.5.4.0 General

UEs may be detached from the network when not communicating to prevent unnecessary collection of location information by the network. Hence the UE will not perform mobility management procedures. Only when the UE is triggered or when a given requirement is reached and the UE needs to transmit data to the MTC application, it will reconnect to the network.

The detach procedure can be either initiated by the UE or by the network. Furthermore, one can distinguish whether the UE or the network has control over the enforcement of the location privacy mechanism.

The UE may need to provide an ability that allows its user to set the transmission privacy configuration. The UE may need to provide an ability to transmit location tracking information in emergency case.

Editor Note: How to trigger the detached UE is FFS in SA2

In order to avoid temporary identity being used as a sobriquet of the UE by attackers to trace the actions of the subscriber over an extended period of time, a lifetime can be set for the temporary identity allocated for the UE and a timer can be started. When the timer expires, a new temporary identity should be allocated for the UE.

Editor Note: If the timer is set on UE side, new signalling procedure or modification of existing signalling procedure are needed.

5.5.4.1 UE based method

The UE will detach from the network when a given condition is reached, for example after a certain period of inactivity in communication. The condition may be configurable on the UE by its user.

NOTE 1: The mechanism has to be implemented such that the UE can not be forced to stay attached by, for example, transmitting certain signals to the UE.

NOTE 2: There may be cases where the MTC service provider does not want the UE to detach, for example, when receiving MTC application data or new software (e.g. device firmware). In those cases the MTC service provider can probably force the UE to stay attached. There are thus scenario's in which the mechanism can be bypassed.

5.5.4.2 Network based method

The network can detach the UEs based on the transmission privacy configuration which was configured by users.

When user adjusts the privacy configuration, the network should be notified.

Editor's Note: Additional security for privacy configurability, visibility and security for overriding of user-set privacy configuration is FFS. How to notify user's privacy configuration adjusting to the network (e.g. send it along with the NAS message during a period of time) is FFS.

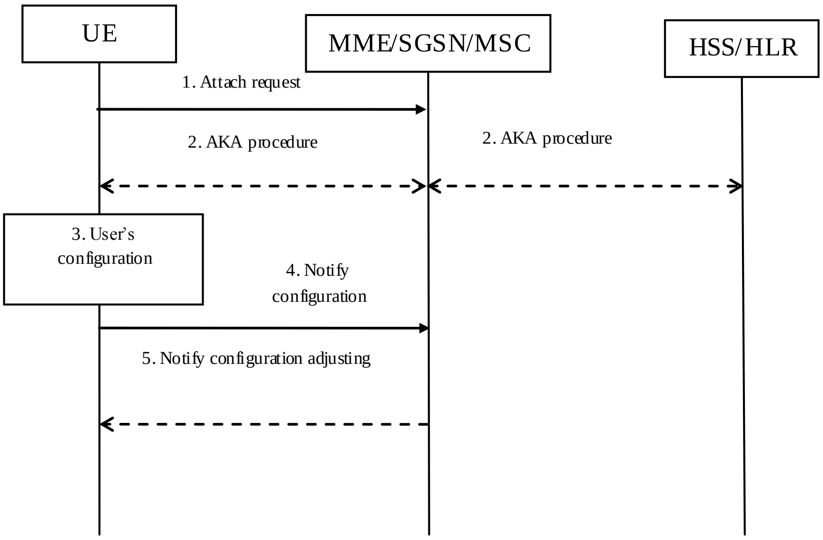


Figure 5.5.4.2-1**: Solution for network based method**

The following is a description of the steps in figure 5.5.4.2-1.

Step 1: This is the normal attach procedure as described in TS 24.008 [34] and TS 24.301 [35].

Step 2: This is the normal UMTS/EPS AKA procedure as described in TS 24.008 [34] and TS 24.301 [35].

Step 3: This configuration function allows user to configure his/her privacy detach conditions.

Step 4: UE notifies the configuration to MME/SGSN/MSC.

Step5: If user has adjusted the privacy configuration, UE sends the notification adjusting to MME/SGSN/MSC.

Editor's Note: the detail of how to notify user's privacy configuration adjusting to the network (e.g. send it along with the NAS message during a period of time) is FFS.

5.5.5 Evaluation

Editor's note: This section contains evaluation (possibly including cost and benefit trade-off analysis) of candidate solutions enumerated in the preceding General Description subsections.

Editor’s Note: Additional security for privacy configurability, visibility and security for overriding of user-set privacy configuration, for emergency transmission is FFS.

5.6 UE Power Consumption Optimizations

5.6.1 Issue Details

The Low Power Consumption is intended for use with UEs that work in cases of power sensitive, and some SIMTC mechanisms are critically required for low power consumption.

Low power consumption use cases are defined in TS 22.368 [9] where UEs are applied. These types of UEs include gas metering and animal, cargo, prisoner, elderly and children tracking. TS 22.368 [9] also states the critical requirements of low power consumption for UEs, because it is not easy to re-charge or replace the battery in these cases. This creates the need for system enhancements that would minimize the power consumption of UEs.

Some security impacts may exist induced by mechanisms for low power consumption. There is no need to have an independent security solution for low power consumption, but either MTC’s Network Solutions or end-to-end solutions should always consider security of low power consumption.

There is a type of UEs which has only a one-off battery. It’s impossible to replace or recharge the battery of the device. This type of UE is vulnerable for spamming SMS attack which may exhaust the battery of the device.

5.6.2 Threats

Some security impacts may exist induced by system improvement for low power consumption in the future.

5.6.3 Security Requirements

The system security improvement over 3GPP network security should consider lower power consumption for UEs.

Editor's Note: Further re-wording of the above requirement need to be considered.

The solutions of anti-spamming should be implemented at the network side. Solutions requiring UE involved will cause battery consumption inevitably.

5.6.4 Solutions

5.6.4.1 General description

Seven solutions have been proposed in SA2’s TR23.887 [26] and the main ideas for these solutions are extending Paging cycle/DRX cycle and initiating UE periodic registrations (Attach/Detach). The user data and control signalling transmission protection is using the legacy LTE security mechanism, and the analysis here focus on whether the transfer of parameters between UE and network is protected:

- Solution1 of “Paging cycles”: The characteristic of this solution is that the Maximum paging/DRX cycles are extended with longer values which can be negotiated between UE and network using attach procedure or TAU procedure. The paging/DRX parameters can be protected by NAS security context in UE and MME.

- Solution 2 of “Extending DRX using UE Assistance Information”: UE Assistance Information message is sent to eNB after RRC Connection Reconfiguration procedure, and UE extended DRX is delivered to UE through RRC Connection Reconfiguration setup message or RRC connection release message. The UE Assistance Information message and paging/DRX parameters can be protected by RRC security context between UE and eNB.

- Solution 3 of "Power Saving State for Devices": The basic idea is that a UE can be configured so that the UE is reachable for downlink data only during the time that the UE is in connected state plus an active time period reachable for paging after the UE changed to idle state, and UE will continue to perform periodic registrations procedures with the timer value given by the network. The periodic timer value is protected by NAS security.

- Solution 4 of "Attach/detach": Three methods: 1. UE periodically attaches to the network and waits to see if there is an MT SMS for the UE; 2. Based on the communication frequency, the network determines the periodic timer value and provides it to UE through Attach/Detach message; 3. UEs and the network are configured to enter detached state when the communication is over. Periodic timer value is protected by NAS security context and configuration data can be protected by OMA DM security.

- Solution 5 of "Transmission delay until better coverage conditions": When coverage conditions are not good in idle mode, delay data transmission until better coverage conditions. No security is related.

- Solution 6 of "Long DRX cycles in connected mode": Network provides extended DRX cycle for connected mode in RRC/MAC message. Extended DRX cycle can be protected by RRC security context.

- Solution 7 of "Factors for determining extended DRX": This solution gives the factors which may influence the decision of extended long DRX for both idle mode and connected mode. No security is related.

The UE Power Consumption Optimizations are mainly extending current messages with new parameters (paging/DRX cycle/Timer values/indicators) or configuring UE and network with new parameters, and the user data and control signallings transmission protection are using the legacy LTE security mechanism. From security point of view, the current EPS security mechanism can ensure the security of all these solutions.

5.7 Security of Small Data Transmission

5.7.1 Issue Details

SA2 is currently considering mechanism to transmit and receive small amount of data efficiently through 3GPP system [26] based on the Small Data Transmission requirements defined in TS 22.368 [9]. According to the current solutions under consideration in SA2, small data is transfer over the NAS signalling or using user plane (Fast Path/Connectionless) with reduced signalling caused by idle-connected mode transitions.

As the SA2 solutions consider that small data is transferred when the UE is in idle mode, it may be required to protect the small data messages.

Editor's Note: Further inputs are needed from SA2 on this issue

5.7.2 Threats

Editor's note: Threats due to unprotected neighbour cell measurements should be studied if those are supported for small data. To be checked with SA2 and RAN2.

5.7.2.1 Small data encapsulation in the NAS

NAS PDU based solutions under consideration in SA2 TR 23.887 [26] for "small data transmission" allow UEs to arbitrarily create NAS content and traffic. An increasing amount of devices creating NAS traffic is a scalability problem that has to be mitigated by existing or new methods..

Editor's note: Small data when transferred over the NAS signalling may overload the NAS, strictly control protocol, with UP content. Since such content will be generated by potentially hundreds of millions devices, overload protection and protection against DOS attacks might be necessary in MME. Further analysis of how to protect the MME is needed.Whether this is a valid threat is FFS.

There may be no pre-established NAS security context in transfer data via optimised SMS solution. Thus the small data transmission can not be protected by valid security context and can be easily tampered or intercepted by the attacker. Sometimes small data is sensitive and important because it may be related to emergency event or commerce. Once it is tampered or intercepted, the consequence can be serious.

The SCS is the source of MTC service applications. For MT small data transmission, SCS generates small data and delivers it to related UEs through operator network. In case the SCS is outside the operator domain, some security attacks on Tsp interface may exist. A forged SCS may send a fake small data to the network and then the network is utilized by the attacker to trigger UEs, or a SCS which is not authorized to deliver small data for UEs may proceed this illegal action. This may lead to a false action of UE, waste of the UE's power consumption, and even a DOS attack to the network. And for MO small data transmission, SCS is the destination of small data. The small data may be related to some users' sensitive privacy information, if the network connects to a forged or threatened SCS controlled by attackers, the small data will be delivered to that SCS and then the attacker can obtain the users' privacy information. In addition, a normal UE may send fake MO small data to SCSs through operator network to get some services, or a malicious but legitimate UE which is only permitted to receive small data (e.g. simple controller) may send UE MO small data to SCSs, or yet another malicious but legitimate UE which has MO small data function may deliver fake small data to SCSs with which UE has no MO small data service subscription, or millions of malicious UEs may send MO small data simultaneously to perform DoS attacks on the operator network or SCSs. These may lead to false action of SCSs, waste of network resources, waste of SCS resource, free service, wrong charging, privacy information leak from SCS, DoS attacks on Network or SCSs and so on

The threats regarding small data when not used in combination with device trigger are different. For device trigger, the source is always SCS and the device trigger message is used to ask UEs to take some action accordingly. The network aims to filter the fake trigger message from unauthorised SCS and common UEs. But for small data transmission, the source can be either SCS (Mobile Terminated sent to UE) or UE (Mobile Originated sent from UE). For MT small data the threats described above apply when it is not used in combination with device trigger and the threats in 5.1.2 apply when used in combination with device trigger. For MO small data, the threats described above apply.

Editor's Note: Threats regarding the small data when not passing through the SCS need further study.

5.7.2.2. Small data fast path in the user plane

Threats to sensitive network information

SA2 solution currently considered in SA2 TR 23.887 v0.6.0 (small data fast path) [26] is based on the principle of providing information to the UE about the end-point of the PDN Connection or its bearer(s) in the SGW (SGW S1-U F-TEID). From security perspective, information like SGW S1-U F-TEID reveals the network topology (like number of S-GWs) and also revealing network privacy information (core network internals like S-GW IP addresses) lead to attacks (like flooding) on the core network. The operational details of a core network are sensitive information that operators are reluctant to expose it to the rest of the world. In order to hide network topology, it is required that the information provided to the UE for small data transmission (small data fast path) should not provide the operational details of the core network entities like SGW IP address to the UE.

Editor's Note: It is ffs on this threats analysis topology and privacy issue.

Threats to small data user plane traffic

The intention with the Small data fast path solution ('Alternative A: Small Data Fast Path' in SA2 TR 23.887 [26]) is that small data can be sent in user plane when the UE is in idle mode without requiring the normal transition to connected mode in AS-layer in LTE systems. Therefore in this small data fast path setting, the UE would send user plane traffic without setting up the regular Access Stratum (AS) security and because of this, it is not possible to encrypt or integrity protect the user plane traffic between the UE and the eNB. As a result of this, an attacker can inject traffic and eavesdrop on subscribers' traffic. Protection of the small data transfer traffic would be desirable to protect the robustness of the charging and the integrity and confidentiality of the small data traffic on user plane. It should be noted that the above analysed threats for traffic injection and eavesdropping are also applicable to regular user plane, and therefore it can be questioned whether any additional protection is needed for small data traffic due to those threats.

Threats to Bearer Resource ID

Eavesdropping attacks

Small data fast path solution uses so called Bearer Resource ID which is sent by the UE to the eNB. The eNB derives the SGW S1-U F-TEID (i.e. S-GW UL TEID and S-GW IP address) from the Bearer Resource ID and uses this information to route small data on the backhaul link. Therefore the Bearer Resource ID cannot be carried in the encrypted payload part of the small data message (in case small data is encrypted), but it needs to be carried in the Uu radio protocol headers, for example as a new IE. Another reason for carrying the Bearer Resource ID in the Uu radio protocol headers is that the eNB is not assumed to interpret the payload part of the small data message, which is likely used to carry an IP packet. As there is no security association between the UE and eNB, the Bearer Resource ID cannot be integrity protected between the UE and eNB and consequently the eNB has no secure knowledge about which UE sent the small data message.

As a consequence the Bearer Resource ID is exposed for eavesdropping and modification on the Uu interface.

If an attacker eavesdrops and gets to know a valid Bearer Resource ID, the attacker could inject small data traffic on Uu interface by masquerading as the victim UE. The eNB passes on the small data to the S-GW using GTP-U. If the victim UE is still attached and under that S-GW, the EPS bearer for small data will be enabled at the S-GW and the S-GW will end the small data to the P-GW over the EPS bearer, and consequently the IP packet in the small data will be sent from the P-GW onwards, e.g. to the internet . If encryption was applied for small data in the case above, the S-GW will try to decrypt the fake small data payload (IP packet). Since the attacker is not assumed to have the encryption keys, the decryption will result to arbitrary trash. Therefore the fake small data payload (IP packet) will be discarded by the first node, e.g. P-GW, which tries to interpret the IP headers. However, if the small data payload (IP packet) is not encrypted, it will be sent onwards by the S-GW and P-GW, e.g. to the internet. It should be noted that the above analysed threats for traffic injection are also applicable to regular user plane, and therefore it can be questioned whether any additional protection is needed for Bearer Resource ID due to those threats.

Another threat related to Bearer Resource ID eavesdropping is as follows. If the fast path for a victim UE is enabled but not active, there is no state for the victim UE in the eNB. If the attacker now sends small data by masquerading as the victim UE, the RRC connection will be established with the attacker (It has not been decided how small data is sent over Uu but some RRC signalling is assumed to be needed). If encryption is used for small data in this case, the attacker likely cannot send small data to the internet (see previous threat), but if he is able to do so for some reason, e.g. encryption is not used, then also the possible downlink response small data message would be routed to the attacker over the Uu so in practice the small data session would be hijacked. On regular user plane set-up case an attacker is able to set-up RRC connection, but the attacker would be detected by the MME when NAS integrity check of the Service Request fails and the RRC connection would be aborted before any user plane data can be sent. One possible solution to mitigate this threat could be to integrity protect the small data messages between the UE and S-GW. It could be sufficient to integrity protect the small data payload (IP packet). Then, if the integrity check of uplink small data fails at the S-GW, the S-GW should discard the small data message and send a GTP-U error indication to the eNB, which would then know to abort the small data fast path and release the RRC connection . However, if integrity protection of small data would fail at the S-GW for an already active fast path, the S-GW could silently discard the small data packet. This is because otherwise one fake small data packet could be used to tear down the fast path.

Modification attacks

The case when an attacker modifies the Bearer Resource ID on Uu interface can be divided into two subcases. In the first subcase the Bearer Resource ID is modified by an attacker to a value for which there exists a small data enabled EPS bearer. This case is basically the same as the Bearer Resource ID eavesdropping threat above. In the second subcase the Bearer Resource ID is modified by an attacker to a value for which there does not exist any small data enabled EPS bearer. In this case the small data message will be discarded by the eNB if it is not able to derive a valid SGW S1-U F-TEID from the Bearer Resource ID (the details of how to derive SGW S1-U F-TEID from the Bearer Resource ID are FFS in SA2), or the small data message will be discarded at the latest at S-GW which will not recognize the SGW S1-U F-TEID as valid one.

The details of the Bearer Resource ID are under study in SA2. One possibility is that the Bearer Resource ID consists of S-GW UL TEID and a ”S-GW identifier” which the eNB then resolves to S-GW IP address. This way the S-GW IP address would not be exposed to the UEs, but the TEID would be. Having TEID “as is” in the Bearer Resource ID has the benefit that the eNB does not need to resolve the TEID from the Bearer Resource ID for each small data fast path establishment separately. Instead the eNB resolves the ”S-GW identifier” to S-GW IP address and may cache this information. Different mechanisms could be used so that eavesdroppers could not collude network topology information from the ”S-GW identifier” , e.g. there could be many to one mapping from several ”S-GW identifiers” to one S-GW IP address. TEID is a value which identifies a GTP-U tunnel endpoint and it is assigned by the node who is expecting to receive traffic on that tunnel. TEID is assigned per IP address and it has a meaning only when used together with that IP address. For example, an attacker would not gain anything by using a TEID from one Bearer Resource ID with ”S-GW identifier” from another Bearer Resource ID.

Threats to RRC security

Another threat is that due to lack of RRC security, RRC Connection Release is not protected and an attacker could drop an RRC connection which is used for small data by sending an RRC Connection Release to the victim UE. On the other hand the small data fast path is assumed to be quite short lived (SA2 TR 23.887 mentions timeout value 5 secs [26]) and is assumed to contain typically one uplink IP packet and one downlink packet. So with careful timing an attacker could prevent the victim UE to receive the downlink small data packet by an unauthorized release of the RRC connection. However, the attacker could do that anyway by doing radio jamming when he detects small data fast path being set up.

Editor’s Note: The details of the optimized Uu signalling are for further study by RAN and consequently the impact on RAN security architecture, e.g. how and whether to protect Uu signalling needs further study.

Editor’s Note: The intention is to turn this editor’s note into normal text as it gets resolved; therefore it is a bit lengthy. When the UE sends an uplink small data packet, the eNB associates the data radio bearer on which it received the packet with the UE. If there is a subsequent downlink message sent from the S-GW towards the UE, the eNB will use the same radio bearer for the downlink packet as was used by the UE for the uplink packet. If the uplink packet contains an identifier for the radio bearer a MITM attacker can change this identifier so that the down link message will not reach the UE. If the uplink packet does not contain an explicit identifier, but the eNB rather identifies the radio bearer based on timeslots, frequencies or similar, the MITM attacker will be allocated different timeslots, frequencies etc. by the eNB, so the effect is the same. The MITM attacker may reach the same effect, by simply dropping the downlink reply packet. The UE would not receive any downlink packets until the S-GW decided to page the UE via the MME instead of using the established path directly via the eNB. It therefore needs to be ensured that the timeout of an active fast path is reasonably short. The effect of this attack with respect to radio jamming is FFS. One effect is that an application server may believe that the downlink packet has reached the UE since the attack is not visible to the UE, the NW or the application server. However, IP networks are best effort by design so an application server assuming an IP packet reaches the destination host without getting an acknowledgement in return makes an incorrect assumption about the network properties.

5.7.3 Security requirements

The small data transmission using small data encapsulation in the NAS payload have to be protected against overloading attack on MME for EPS.

Editor’s Note: How to provide NAS DOS protection for small data transfer is FFS. Dedicated MME can be considered as one option.

The small data should be integrity protected (for 3G/LTE system). Integrity protection between the UE and S-GW should be applied to small data fast path messages to protect against fast path establishment with unauthorized UEs.

Editor’s Note: It is ffs for all small data solutions, whether to integrity protect either the payload of the small data message or the whole small data message for the benefit of protecting the network and/or the data itself.

The small data may be confidentiality protected.

Editor’s Note: How to provide confidentiality and integrity protection for small data transfer should be studied when there is no pre-established security context.

The 3GPP network should be able to determine that the SCS is authorized for small data transmission over Tsp interface.

Editor’s Note: It is ffs whether SCS can decide if downlink data is small data or not, or if this decision is to be done by 3GPP networks entities, e.g. SGW. This is to be decided by SA2 and it will have an impact if there needs to be authorization requirement for SCS or not.

Editor’s Note: It is FFS whether it is a security issue or not if the UE indicates to the network that it is sending small data but still sends a large amount of data.

The 3GPP network should be able to determine that the UE is authorized for MO uplink small data transmission.

The network information provided to the UE for small data transmission should not expose the network topology and network sensitive information (e.g., network nodes IP addresses).

5.7.4 Solutions

5.7.4.1 Small data transfer in NAS PDU

5.7.4.1.1 General description

MO analysis for small data transmission

According to TR23.887 [26], for the LTE procedure for MO IP packet delivery, small data and its EPS Bearer ID are delivered in NAS PDUs of a new initial layer 3 message, and this NAS PDU is sent in the NAS container in the RRC Connection Setup Complete message. For the first two solutions for MO IP packet delivery of small data solutions in TR23.887 [26] they says:

"*…The NAS PDU is a new form of initial layer 3 message that includes the IP packet and its EPS Bearer ID in an encrypted IE. This NAS PDU is sent in the NAS container in the RRC Connection Setup Complete message. The unencrypted part of this new initial layer 3 message in the NAS PDU carries the "KSI and sequence number" IE and the MME uses this, and the S-TMSI, to identify the security context to decrypt the IP packet and EPS Bearer ID*."

We can see that first two SA2 solution use partly ciphered security solution for initial L3 message. However, according to TS33.401 [13], initial L3 message shall be integrity protected but not ciphered. So it needs to find a method to solve this problem for SA2's solutions.

For the third solution in SA2's TR23.887 [26], it transmits small data in a "UPLINK_GENERIC_NAS_TRANSPORT". If it is initial L3 message, it also needs to find a method for partly ciphered small data transmission. If it is not initial L3 message, it can use current EPS security mechanism to protect.

MT analysis for small data transmission

For MT IP packets delivery in all three SA2's solution, small data is in a NAS PDU of S1 Downlink NAS Transport message after the paging procedure, so the IP packets can be protected by current EPS NAS security mechanism that provides confidentiality and integrity protection for the whole S1 Downlink NAS Transport message.

5.7.4.1.2 Solution 1: Partly ciphering

From the above analysis, we can see that the partly ciphered security mechanism is necessary for initial uplink layer 3 NAS message of MO IP packet delivery for SA2's solutions. The network (MME/SGSN) firstly needs to recognize that whether the initial layer 3 message from UE is ciphered or not. It can be achieved by UE set the current "Security header type" IE's reserved value, e.g. "0101" to "Integrity protected and partly ciphered". So the network can identify the initial L3 which carries the small data is partly confidentiality protected and then generate key stream to decipher this partly ciphered initial layer 3 message.

In the other hand, the generation of the key stream is another issue that should be considered. The method can be as following: the input parameter LENGTH is set to the real length of small data, and the small data length key stream is derived through EEA and the other input parameter remains the same. The plaintext small data is encrypted by applying the key stream using XOR of the plaintext and the key stream. The encrypted small data is encapsulated in NAS PDUs.

Based on above analysis, the partly secure protection of small data in NAS message for MO IP packets delivery can be done as followings: UE performs Attach activating a PDN connection or TAU (with an already active PDN a connection).Then UE sets the current "Security header type" IE's reserved value, e.g. "0101" to "Integrity protected and partly ciphered". Small data are included in NAS PDU which is a new form of initial layer 3 message. This NAS PDU is sent in the NAS container in the RRC Connection Setup Complete message. The eNB forwards the partly encrypted IP packets to the MME in the S1AP Initial UE message. The MME identifies the small data is integrity protected and partly confidentiality protected and then generates a key stream to decipher partly ciphered initial layer 3 message.

Editor's Note: It is FFS in SA3 for partial ciphering solutions as it may violate the current protocol layer security concepts.

5.7.4.1.3 Analysis of NAS signalling key management in LTE

5.7.4.1.3.0 General

For the small data transmission in LTE, according to definition in TR 23.887 clause 5.1.1.3.1 [26], KeNB will not be used because of the RRC security context shall be not established in the optimised LTE message sequence for the transfer of one IP packet pair. In this case, the procedures which pointed out in clause 7.2.6 of TS33.401 [13] can be omitted, i.e. MME remove the derivation of the KeNB and not initiate NCC, not derive NH etc. when the MME knows the UE is subscribed on the small data and transmitted one IP packet pair, and also eNB does not need to compute any AS keys; The UE skips the derivation of KeNB and keys of RRC and UP when the UE is subscribed on the small data service.

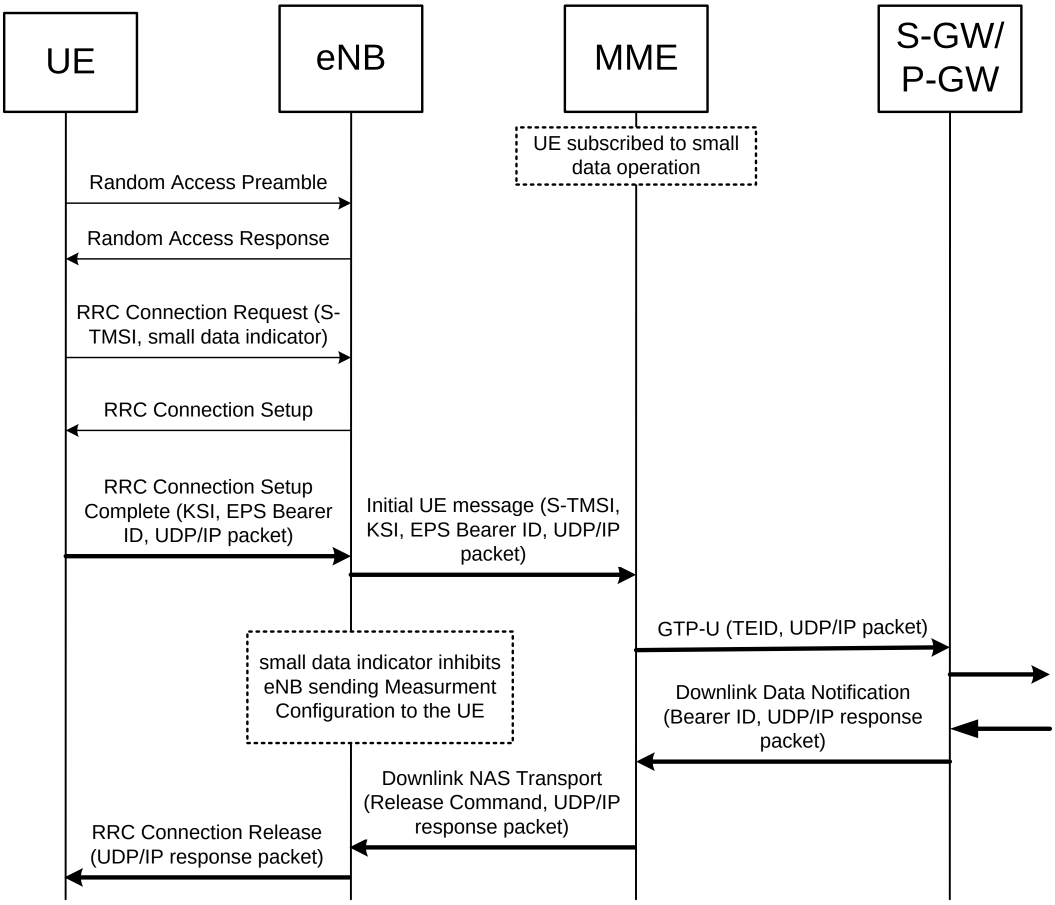

UE
eNB
MME
S-GW/
P-GW
UE subscribed to small data operation
Random Access Preamble
Random Access Response
RRC Connection Request (S-TMSI, small data indicator)
RRC Connection Setup
RRC Connection Setup Complete (KSI, EPS Bearer ID, UDP/IP packet)
Initial UE message (S-TMSI, KSI, EPS Bearer ID, UDP/IP packet)
GTP-U (TEID, UDP/IP packet)
small data indicator inhibits eNB sending Measurment Configuration to the UE
Downlink Data Notification (Bearer ID, UDP/IP response packet)
Downlink NAS Transport (Release Command, UDP/IP response packet)
RRC Connection Release (UDP/IP response packet)

Figure 5.7.4.1.3-1: LTE message sequence for the transfer of one IP packet pair

5.7.4.1.3.1 Optimised LTE key hierarchy for small data

For optimised LTE message sequence for the transfer of one IP packet pair, LTE key hierarchy can be optimised as follows by aligning with SA2.

Note: This optimization only means that the AS security contexts will not be used in this solution but the UE still have to support the AS security usage capability.

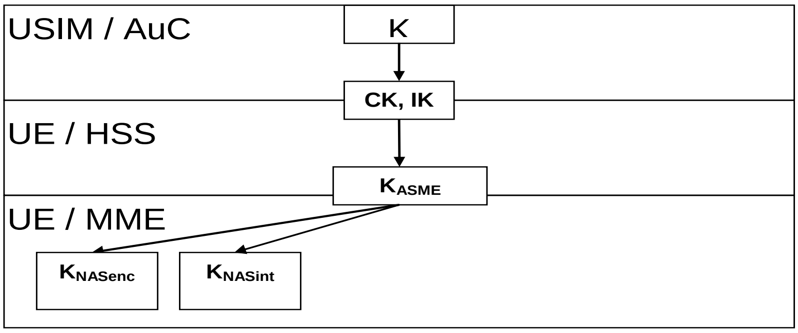


Figure 5.7.4.1.3.1-1: Optimised LTE key hierarchy

5.7.4.1.3.2 Evaluation of the optimised LTE key hierarchy

The optimised LTE key hierarchy does not impact the small data transmission. It has the following benefits:

- It is aligned with SA2 solution for Optimised LTE message sequence for the transfer of one IP packet pair;
- It can optimise the computing and storage resources of the UE, eNB and MME when the AS security contexts are not used

5.7.4.2 Small Data Fast Path in User Plane

5.7.4.2.0 General

This section provides a security solution for Alternative A: Small Data Fast Path solution in TR 23.887 [26].

5.7.4.2.1 Termination point of security for small data in the network

The basic principle of the Small data fast path solution is that small data can be sent when the UE is in idle mode without requiring the normal transition to connected mode in AS-layer in LTE systems. It describes how small data can be passed in a fast path of the user plane without the disproportional amount of signalling caused by idle-connected mode transitions in AS-layer

The LTE AS security context only exists when the UE is in connected mode. Therefore when the UE is in idle mode, the small data transferred in user plane traffic cannot be protected between the UE and the eNB with the regular LTE AS level security context. A new security context that is kept during idle-connected mode transitions is required for the small data feature. A new security protocol is also required. We call these small data transfer security context and small data transfer security protocol respectively.

The security protection of small data could be terminated either in the eNB or in the S-GW. The LTE AS security is terminated in the eNB and this may be secure enough also for small data just as it was for normal UP traffic in pre-Rel-12, but terminating the security in the core NW is clearly beneficial from a security perspective. In this solution security is terminated in the S-GW for the following reasons:

1) If the security for the small data would be terminated in the eNB, the MME would need to push down a new additional security context for small data to the eNB for each UE used for small data. The eNB would then need to keep a state and store a small data transfer security context for each UE used for small data even when the UE is in idle mode. The current concept in LTE is that the eNB does not keep a state for UEs in idle mode. Since the S-GW needs to keep a UE context anyway for small data fast path, the security context can be kept as a subset of that UE context, i.e., the security handling does not add anything in.

2) Also, if the security for the small data would be terminated in the eNB these security contexts would need to be transferred to the new eNB whenever an idle mode UE moves into a new cell served by a different eNB similarly as is done today for connected mode UEs.

Editor's Note: A similar issue needs to be considered also for solution A wrt mobility as the S-GW needs to be updated with the address of the eNB on which the UE currently camps when the UE moves. Otherwise, the S-GW could not deliver downlink small data to the idle UE in an efficient way. The issue of small data transfer at inter-eNB change needs further study in SA2.

Editor's Note: Terminating the security for small data in the S-GW may impact existing solutions like LIPA and SIPTO. Security issues related to LIPA and SIPTO@LN are ffs, cf. also Editor's note relating to LIPA and SIPTO in TR 23.887 [26].

5.7.4.2.2 General description of proposed solution

The figure 5.7.4.2.2-1 below depicts a solution for 'Alternative A: Small Data Fast Path' in TR 23.887 [26] by providing a new separate security protection between the UE and the S-GW (this is shown with the thick dotted line). This new security protection includes optional encryption and integrity protection.

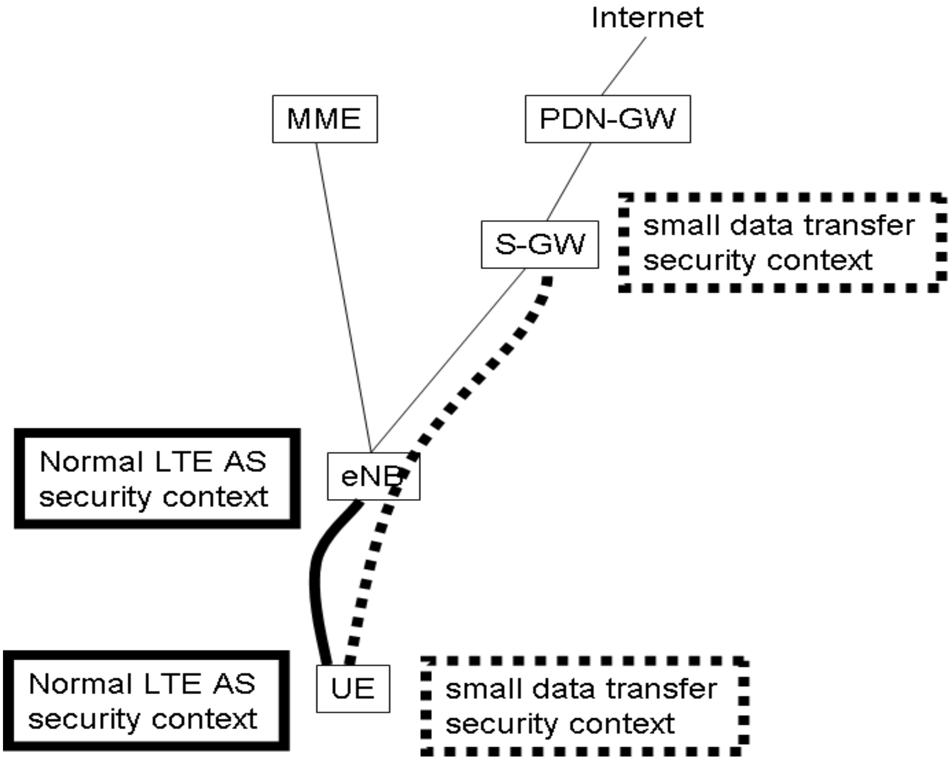

Internet
MME
PDN-GW
S-GW
small data transfer security context
Normal LTE AS security context
eNB
Normal LTE AS security context
UE
small data transfer security context

Figure 5.7.4.2.2-1: Security context for small data transfer of the user plane in LTE systems

NOTE: In the figure above, the thick lines show the normal LTE AS security protection of the user plane. The dotted lines show the small data transfer security protection of the user plane.

To enable the security protection of the user plane between the UE and the S-GW, the UE and S-GW have to establish a new security context for small data transfer.

It should be noted that the two types of security contexts (normal LTE AS security context and small data transfer security context) can be completely independent.

5.7.4.2.3 Small data transfer security context

The small data transfer security context is used whenever the S-GW and UE need to protect (or unprotect) small data.

When the UE attaches to LTE systems or is handed over from another radio access technology to LTE, the K_{ASME} is established between the UE and the MME. A new small data transfer security key K_{SDT} is derived from the K_{ASME} at attach and IRAT handover.

The K_{SDT} could for example be derived from the K_{ASME} using the Key Derivation Function (KDF) defined for LTE. The K_{SDT} could be derived as follows:

K_{SDT} = KDF(K_{ASME}, other parameter(s))

Other parameters in the key derivation can include e.g. parameters to ensure freshness of K_{SDT} .

The MME provides K_{SDT} to the S-GW using (modified) EPS bearer establishment and modification procedures whenever needed. K_{SDT} is the basis of small data transfer security context which is used for the protection of the small data between the UE and S-GW.

The K_{SDT} is stored in the S-GW and it could be changed as often as the K_{ASME} is changed (for example, the MME could send a new K_{SDT} to the S-GW whenever the K_{ASME} is changed). In this way, there would always be a K_{SDT} corresponding to a K_{ASME}. A good thing with changing the small data transfer security context as often as the K_{ASME}, is that the UE and the MME are synchronized on the K_{ASME} and hence there would be an implicit synchronization of the K_{SDT}. Additional synchronization is achieved by comprising the Key Set Identifier (KSI) of the currently active K_{ASME} also in the traffic between the UE and the S-GW. This KSI would then also indicate which K_{SDT} should be used for the packet in question. The MME would have to provide the S-GW with the KSI that corresponds to the K_{SDT}.

The S-GW can further derive encryption (K_{SDT_enc}) and integrity keys (K_{SDT_int}) from K_{SDT}, which can be used for encryption and integrity protection of small data.

K_{SDT_enc} = KDF(K_{SDT}, "SDT_ENC", Algorithm identifier, ...)

K_{SDT_int} = KDF(K_{SDT}, "SDT_INT", Algorithm identifier, ...)

The UE and S-GW also need to share the same encryption and integrity algorithms for small data protection. One possibility is that the same algorithms that are used for NAS security are also used for small data transfer security. . But as this restricts the algorithm choice to the subset of algorithms supported by both MME and S-GW it is better to negotiate the small data separately.

The algorithms can be negotiated between the UE and MME at the same time when NAS security algorithms are negotiated and the MME can indicate them to the S-GW. This means that the MME may have to know which algorithms are supported by the S-GW.

Editor's Note: It is FFS whether the MME should be configured with the knowledge of which algorithms are supported by the S-GW or whether a protocol based solution would be preferable.

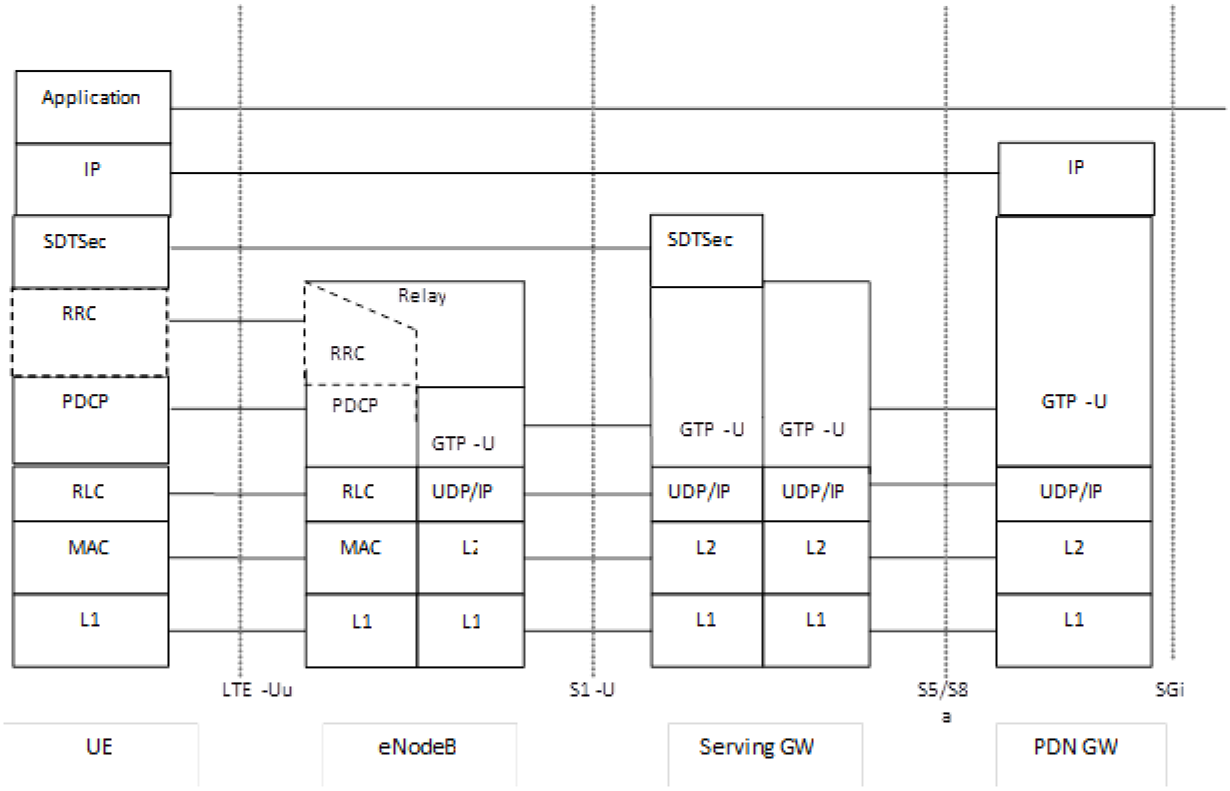
Since the UE also has the K_{ASME}, the UE can derive the same K_{SDT} and further keys similarly as the S-GW.

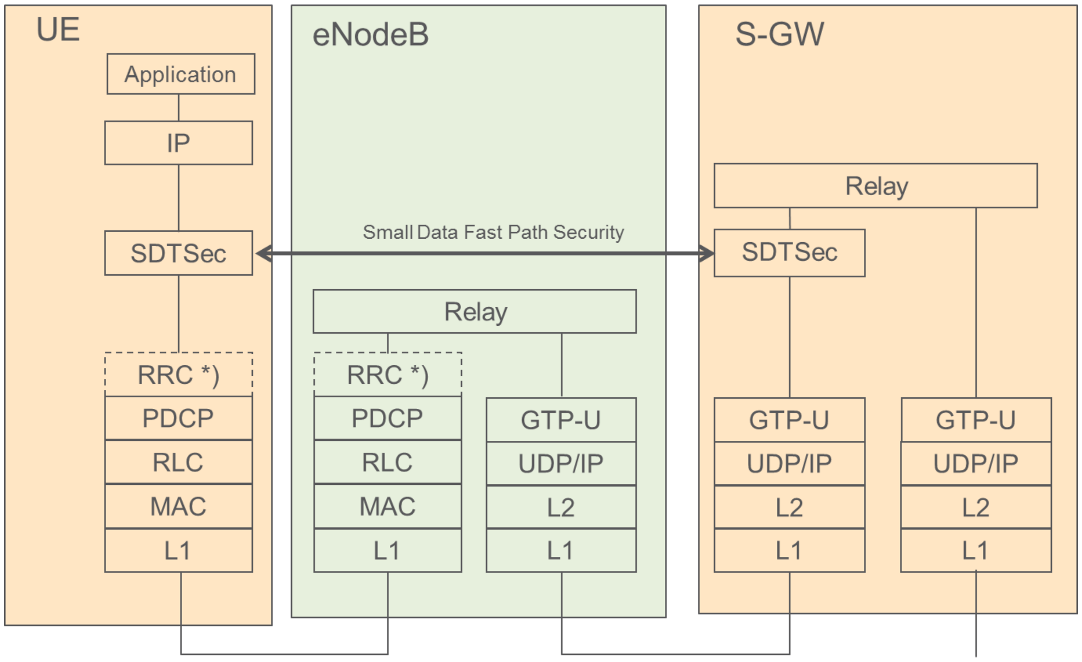
Editor's Note: It is proposed in TR23.887 v.080 [26] that the small data transfer security context is kept after creation in the UE and the S-GW regardless if the fast path is active or not. The security information is not removed when the fast path is deactivated after timeout or at transition from ECM-idle to ECM-connected. It needs to be studied when is the proper time to remove the small data transfer security context from the UE and the S-GW(s), with which the UE shares a context, and how. This is dependent on how SA2 decides how to handle the UE context in the S-GW in case of small data, since the security context is supposed to be a subset of the UE context.

Editor's Note: How to define the input for key derivation and how the UE gets it is ffs.

Editor's Note: It needs to be studied how a change of security contexts can be synchronised between UE and S-GW when triggered by a K_{ASME} change, in particular when small data are being transferred while a new K_{ASME} is established via AKA and NAS SMC.

5.7.4.2.3A Small data transfer security protocol





*) RRC used depending if CP or UP is used for small data

Figure 5.7.4.2.3A-1: Protocol stack for small data fast path

Figure above shows the protocol architecture for small data fast path between the UE, eNB and S-GW. A security protocol to implement SDTSec needs to provide support for encryption and probably also for integrity and replay protection.

Today AS security is implemented in the RRC for key handling and security control and in the PDCP for user plane and control plane ciphering and integrity protection, and NAS security is implemented in the NAS protocol. Small data fast path security is terminated in the S-GW and therefore the existing protocols cannot be used. A new security protocol called small data transfer security protocol (SDTSec) is introduced between the UE and S-GW.

As most other security protocols are tightly coupled to a specific key management or transport protocol, the SDTSec protocol is based on PDCP (TS 36.323) and uses the same ciphering and integrity algorithms. Processing for replay protection etc. can also be re-used from TS 36.323. The packet format is shown in Figure 5.7.4.2.3A-2.

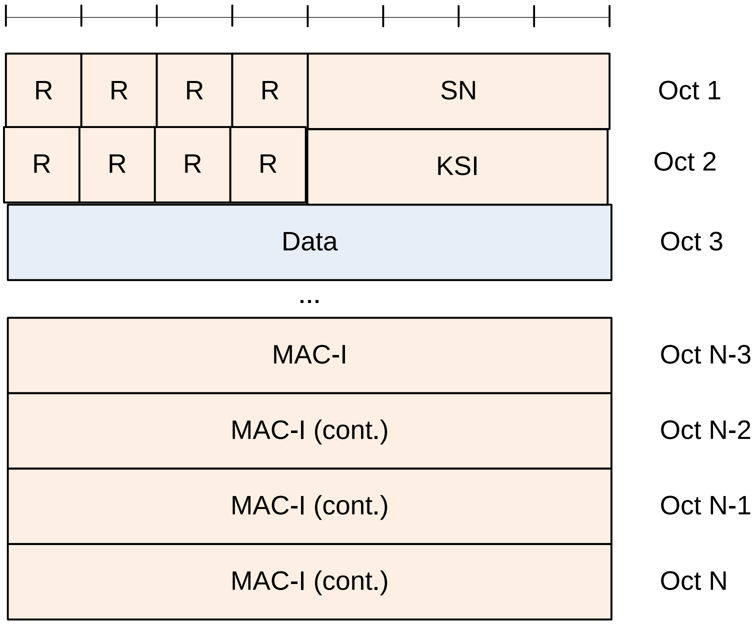


Figure 5.7.4.2.3A-2: SDTSec data format. The exact format can be left to stage 3 groups to decide. The figure shows the information needed and an example format.

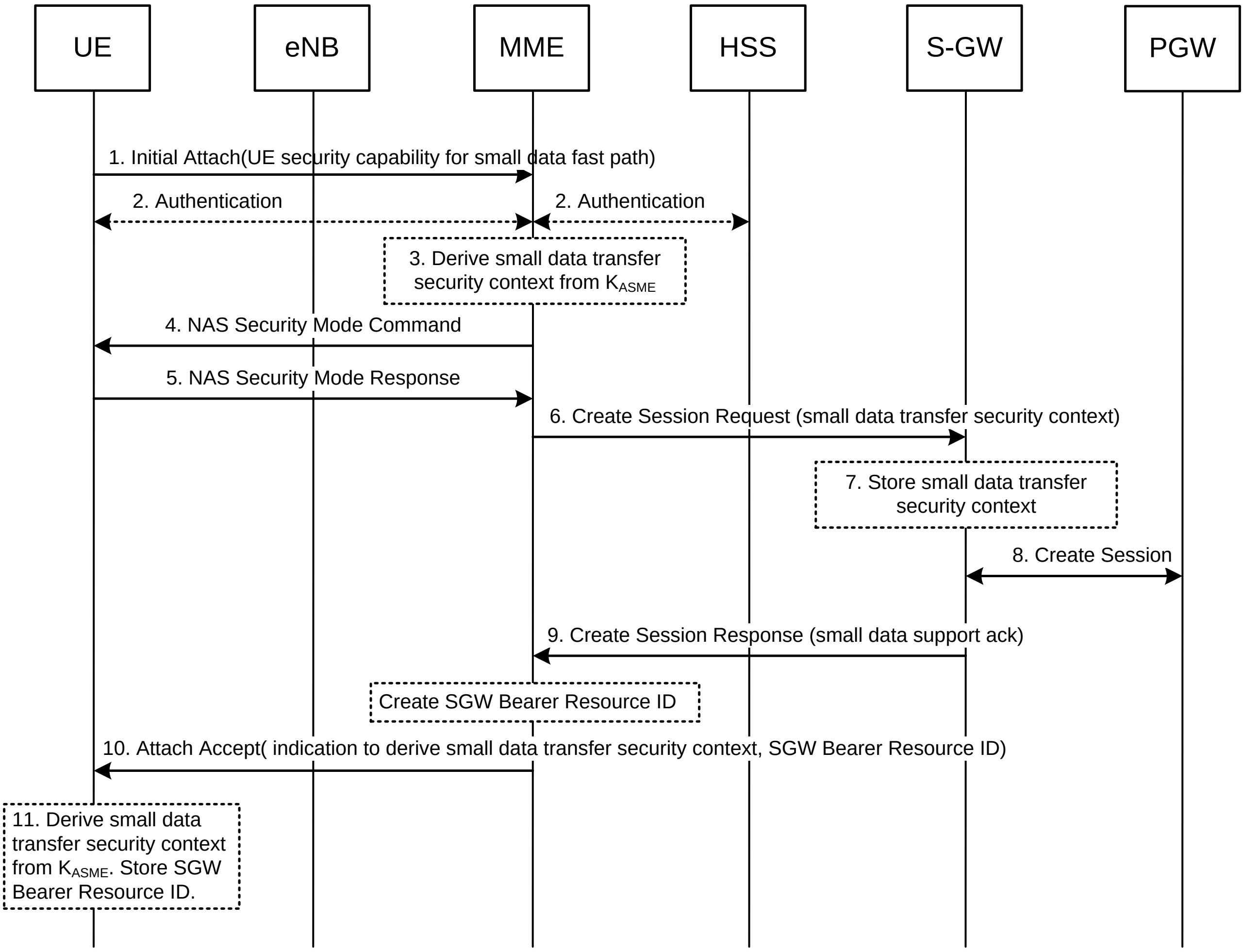
Even without security the S-GW must be able to identify the subscriber (otherwise it cannot do charging). With the SDTSec sequence number (SN) the normal encryption sync and replay protection is provided. The KSI, a field not currently present in the LTE PDCP protocol, the UE and S-GW can identify the correct small data transfer security context.

It will be under the remit of RAN to decide if and how Uu will be developed to support small data, e.g. whether user plane or control plane will be used to carry small data over the Uu. If user plane is chosen, the user plane PDCP encryption does not need be activated when small data fast path is used.

Editor's Note: Interaction between fast path and normal mode switching need further study and also depends on the SA2 decision.

5.7.4.2.4 Small data transfer security context establishment at Attach procedure

EPS bearers are enabled for small data fast path during MM and SM procedures (see TR 23.887 clause 5.1.1.3.6.2 [26] for more non-security details). Figure 5.7.4.2.4-1 shows how an existing signalling message sequence for Attach Procedure is updated for small data fast path.


UE
eNB
MME
HSS
S-GW
PGW
1. Initial Attach(UE security capability for small data fast path)
2. Authentication
2. Authentication
3. Derive small data transfer security context from K_{ASME}
4. NAS Security Mode Command
5. NAS Security Mode Response
6. Create Session Request (small data transfer security context)
7. Store small data transfer security context
8. Create Session
9. Create Session Response (small data support ack)
Create SGW Bearer Resource ID
10. Attach Accept(indication to derive small data transfer security context, SGW Bearer Resource ID)
11. Derive small data transfer security context from K_{ASME}. Store SGW Bearer Resource ID.

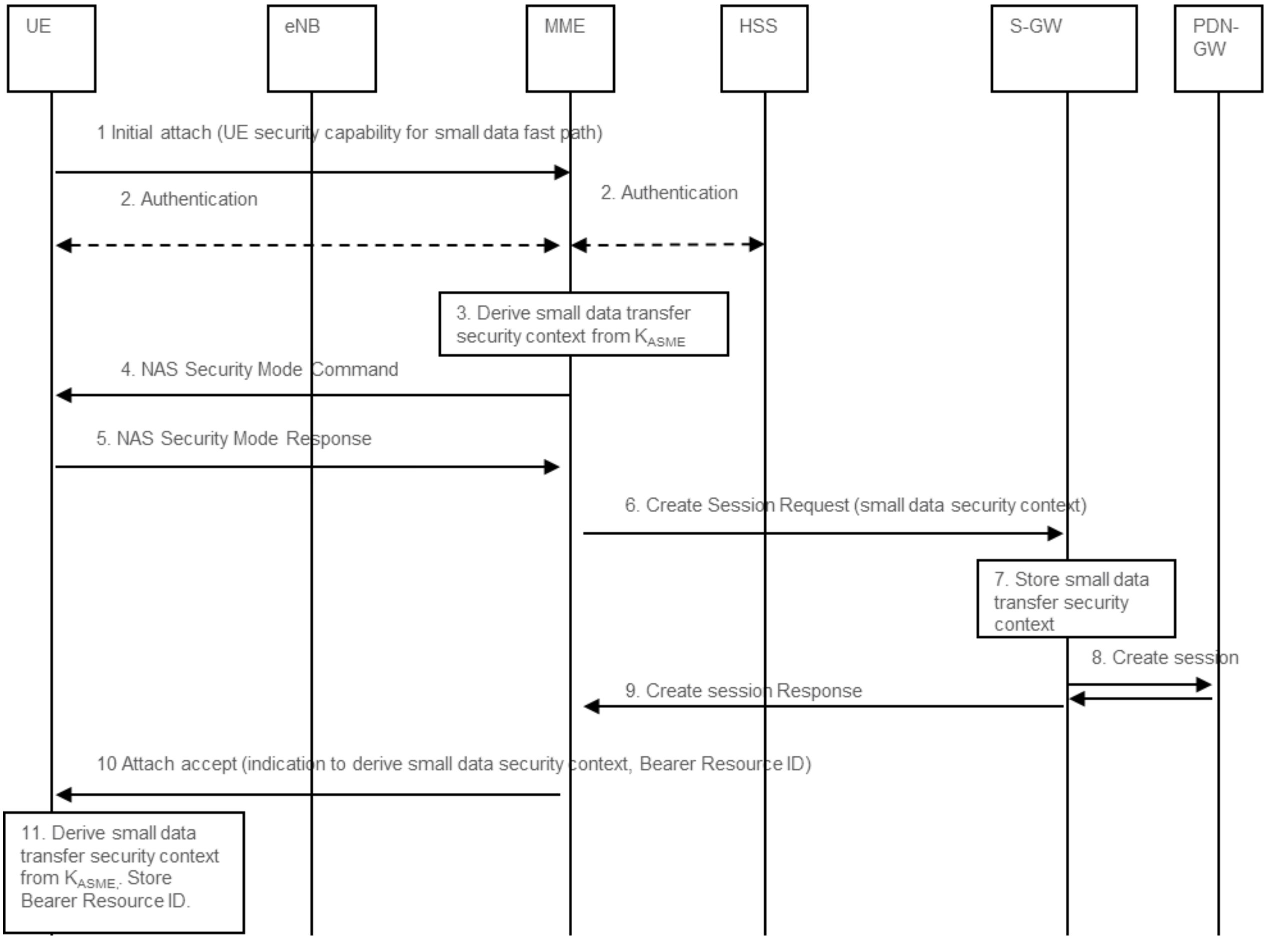

UE
eNB
MME
HSS
S-GW
PDN-GW
1 Initial attach (UE security capability for small data fast path)
2. Authentication
2. Authentication
3. Derive small data transfer security context from K_{ASME}
4. NAS Security Mode Command
5. NAS Security Mode Response
6. Create Session Request (small data security context)
7. Store small data transfer security context
8. Create session
9. Create session Response
10 Attach accept (indication to derive small data security context, Bearer Resource ID)
11. Derive small data transfer security context from K_{ASME}. Store Bearer Resource ID.

Figure 5.7.4.2.4-1: Initial Attach procedure for small data fast path

Editor's Note: It is FFS whether and how the confidentiality of the radio bearer identity associated with the UE when the SGW Bearer Resource ID is sent from the UE to the eNB during small data radio bearer establishment is ensured. C.f. long ed-note in 5.7.2.2.

Editor's Note: It is FFS how the S-GW can ensure that the COUNT values do not wrap around.

The following steps are performed as described in the signalling flow above:

1. The UE initiates an attach procedure with an MME and provides its 'UE security capability for small data fast path' to the MME (indicating support of small data fast path, support of ciphering and integrity algorithms).

2. The MME optionally authenticates the UE and a K_{ASME} is established.

3. The MME derives K_{SDT} from the K_{ASME}, decides which cryptographic algorithms are to be used with small data transfer security, and creates the small data transfer security context.

4. The MME initiates NAS Security Mode Command procedure with UE in order to establish NAS security. In the same message the MME indicates which cryptographic algorithms are to be used with small data transfer security. This implies additional fields in the NAS SMC. The MME indicates also the identifiers of the keys for small data (KSI) and replays the 'UE security capability for small data fast path', to the UE in NAS SMC or some other appropriate NAS message.

5. The UE responds with a NAS Security Mode Response to the MME.

6. The MME sends a Create Session Request to the selected SGW together with the small data transfer security context (including K_{SDT}, identifiers of security keys for small data (KSI), and selected cryptographic

algorithms). The S-GW derives K_{SDT_enc} and K_{SDT_int} from the K_{SDT} key and the cryptographic algorithm identifiers received from the MME.

7. When the Create Session Request is received by the S-GW, the S-GW enables the EPS bearer for small data fast path and stores the small data transfer security context for the session.

8. The new EPS bearer is established towards the PGW.

9. The S-GW sends a Create Session Response and acknowledges that it supports small data fast path and will use it for the established EPS bearer.

10. The MME creates a SGW Bearer Resource ID. The SGW Bearer Resource ID enables the eNB to derive the SGW S1-U F-TEID, i.e. the UL GTP-U TEID and S-GW IP address. The MME sends an Attach Accept together with an indication which requests the UE to create a new small data transfer security context, and includes also the SGW Bearer Resource ID to the UE.

11. The UE creates small data transfer security context, it derives K_{SDT} from the K_{ASME} , and stores SGW Bearer Resource ID. The UE also derives K_{SDT_enc} and K_{SDT_int} from the K_{SDT} key and the selected cryptographic algorithms identifiers received from the MME in step 4 above.

5.7.4.2.5 UE initiated uplink (UL) small data

Figure 5.7.4.2.5-1 shows how mobile originated small data packet is passed uplink (UL) and how a subsequent small data IP packet is passed back to the UE in downlink (DL).

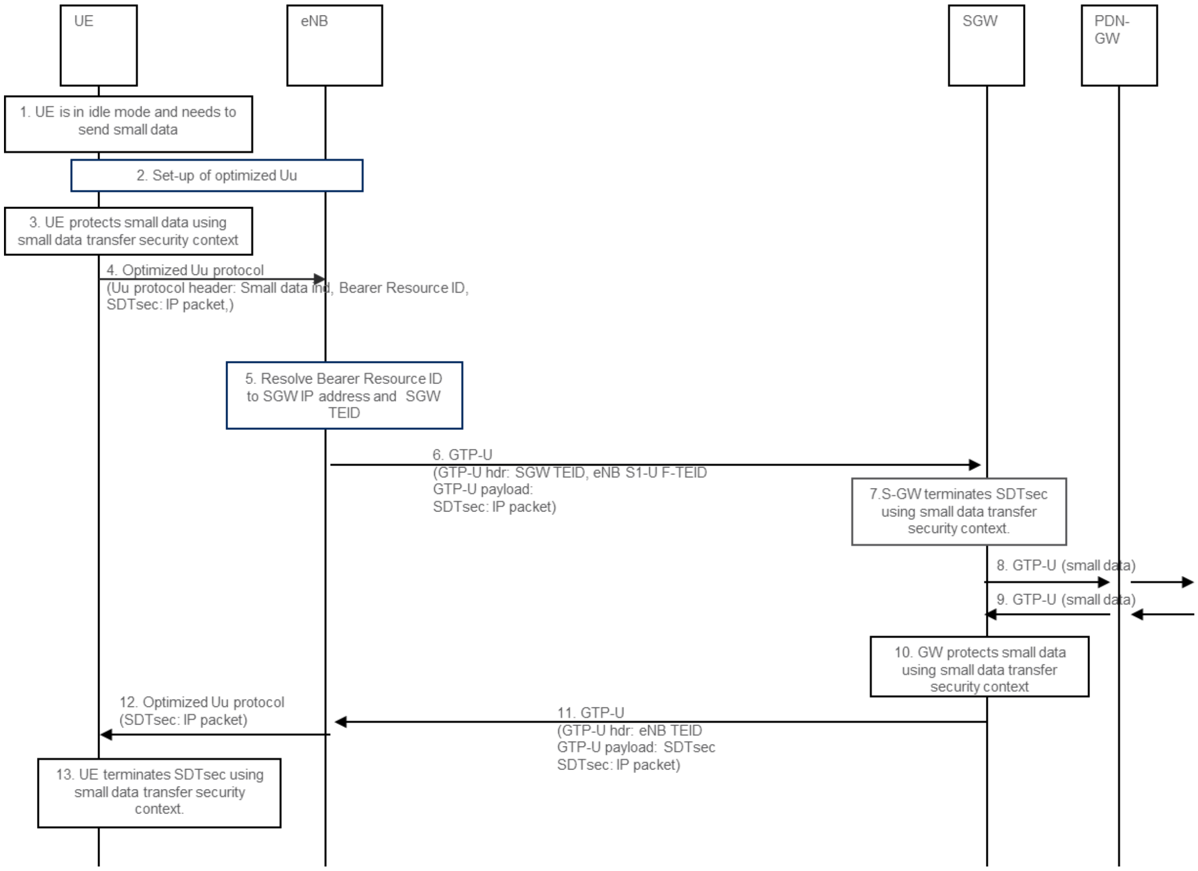

UE
eNB
SGW
PDN-GW
1. UE is in idle mode and needs to send small data
2. Set-up of optimized Uu
3. UE protects small data using small data transfer security context
4. Optimized Uu protocol
(Uu protocol header: Small data ind, Bearer Resource ID,
SDTsec: IP packet,)
5. Resolve Bearer Resource ID to SGW IP address and SGW TEID
6. GTP-U
(GTP-U hdr: SGW TEID, eNB S1-U F-TEID
GTP-U payload:
SDTsec: IP packet)
7.S-GW terminates SDTsec using small data transfer security context.
8. GTP-U (small data)
9. GTP-U (small data)
10. GW protects small data using small data transfer security context
11. GTP-U
(GTP-U hdr: eNB TEID
GTP-U payload: SDTsec
SDTsec: IP packet)
12. Optimized Uu protocol
(SDTsec: IP packet)
13. UE terminates SDTsec using small data transfer security context.

Figure 5.7.4.2.5-1: UE initiated uplink small data

The following steps describe the signalling flow above:

1. The UE wants to send an UL IP packet for an idle mode bearer enabled for small data fast path and

2. The UE sets up the optimized Uu for small data.

3. The UE performs protection (integrity and/or encryption) of the small data using the security protocol called SDTSec and the small data transfer security context.

4. The UE sends the protected small data to the eNB over optimized Uu protocol. The Bearer Resource ID is included in a Uu protocol header or IE. This is needed since the eNB needs to be able to interpret the Bearer Resource ID and therefore it cannot be within the security protocol or be encrypted.

5. The eNB resolves the Bearer Resource ID to S-GW UL TEID and S-GW IP address, and assembles a GTP-U PDU using information received with small data.

6. The eNB forwards the GTP-U PDU to the S-GW.

7. The S-GW receives the GTP-U PDU including the protected small data and terminates SDTSec (integrity check and/or decryption) using the small data transfer security context.

8. The S-GW forwards the GTP-U PDU to the PGW.

9. The S-GW receives a DL GTP-U PDU on an EPS bearer that has an active fast path.

10. The S-GW performs protection (e.g. integrity and/or encryption) of the small data in the GTP-U PDU using SDTSec and the small data transfer security context.

11. The S-GW forwards the GTP-U PDU with the protected small data to the eNB.

12. The eNB forwards the protected small data to the UE over optimized Uu.

13. The UE terminates SDTSec (integrity check and/or decryption) of the small data using the small data transfer security context.

5.7.4.2.6 Network initiated downlink (DL) small data

Figure 5.7.4.2.6-1 shows small data initiated DL, that is, DL data received in the S-GW on an EPS bearer where fast path is enabled but not active, is handled as described in the figure below. It should be noted that compared to when small data is initiated UL, an additional paging of the UE is required.

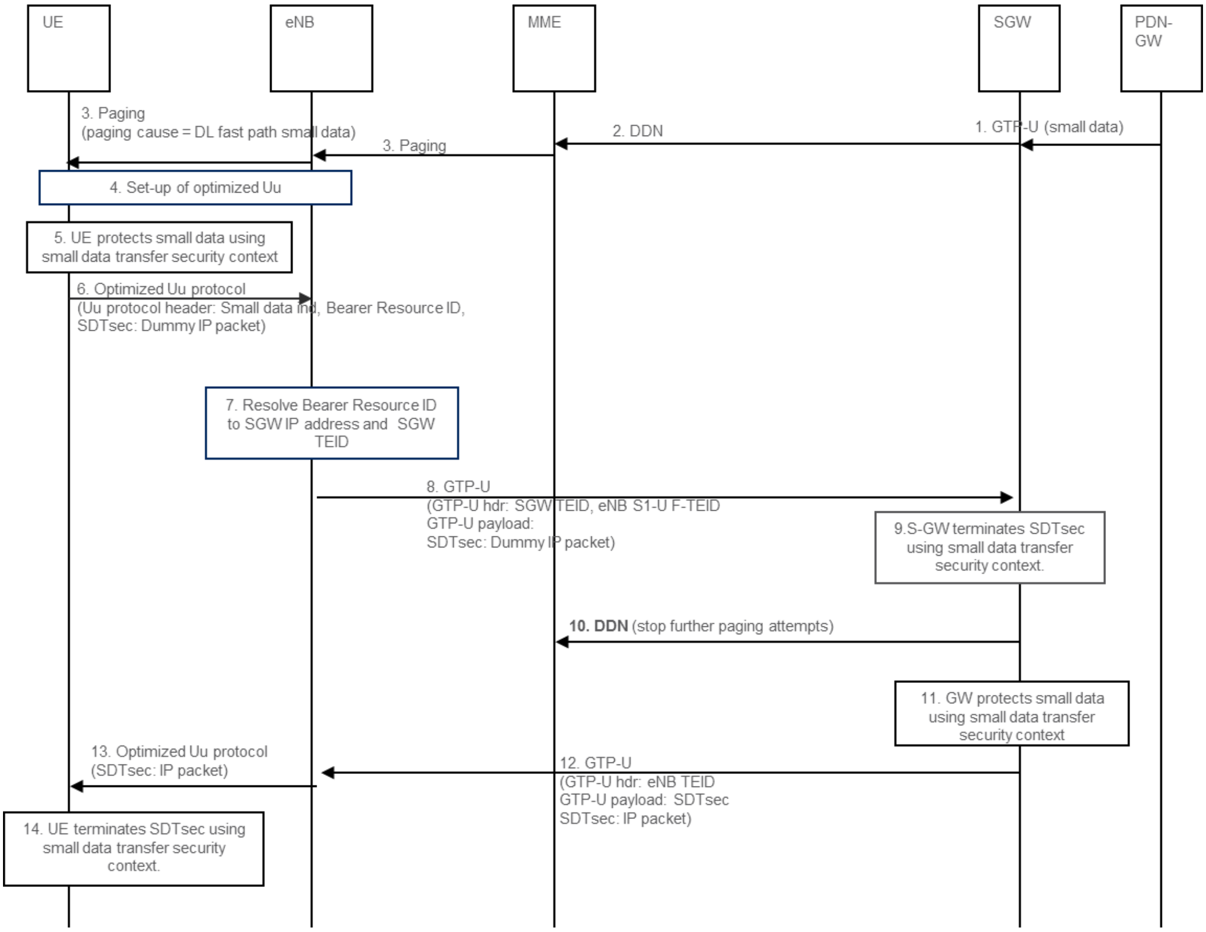

UE
eNB
MME
SGW
PDN-GW
1. GTP-U (small data)
2. DDN
3. Paging
3. Paging
(paging cause = DL fast path small data)
4. Set-up of optimized Uu
5. UE protects small data using small data transfer security context
6. Optimized Uu protocol
(Uu protocol header: Small data ind, Bearer Resource ID,
SDTsec: Dummy IP packet)
7. Resolve Bearer Resource ID to SGW IP address and SGW TEID
8. GTP-U
(GTP-U hdr: SGW TEID, eNB S1-U F-TEID
GTP-U payload:
SDTsec: Dummy IP packet)
9.S-GW terminates SDTsec using small data transfer security context.
10. DDN (stop further paging attempts)
11. GW protects small data using small data transfer security context
12. GTP-U
(GTP-U hdr: eNB TEID
GTP-U payload: SDTsec
SDTsec: IP packet)
13. Optimized Uu protocol
(SDTsec: IP packet)
14. UE terminates SDTsec using small data transfer security context.

Figure 5.7.4.2.6-1: Network initiated downlink data

The following steps describe the signalling flow above:

1. The S-GW receives a GTP-U PDU from the P-GW.

2. If the EPS bearer is idle and fast path enabled but not active, then the S-GW indicates to the MME to start paging the UE.

3. The MME pages the UE indicating ‘DL fast path small data’ as paging cause.

4. The UE sets up the optimized Uu for small data.

5. Protection of the dummy IP packet corresponds to step 3 in clause 5.7.4.2.5.

6. The UE sends the protected dummy IP packet.

> Editor’s Note: according to an Editor’s note in TR 23.887 [26], whether the dummy IP packet is generated in the UE or the eNB is for further study by RAN. Therefore, whether the dummy IP packet can be integrity protected and optionally encrypted by the small data transfer security context depends on the study outcome of RAN WGs.

7. This corresponds to step 5 in clause 5.7.4.2.5.

8. This corresponds to step 6 in clause 5.7.4.2.5.

9. This corresponds to step 7 in clause 5.7.4.2.5.

10. The S-GW requests the MME to stop further paging attempts.

11. This corresponds to step 10 in clause 5.7.4.2.5.

12. This corresponds to step 11 in clause 5.7.4.2.5.

13. This corresponds to step 12 in clause 5.7.4.2.5.

14. This corresponds to step 13 in clause 5.7.4.2.5.

.

5.7.4.2.7 S-GW relocation

It may be possible that more than one small data transfer security context is derived from the same base key i.e. the K_{ASME}, and these small data transfer security contexts are sent to different S-GW's. An example where this can occur is if the UE is first sharing a small data transfer security context with one S-GW and then later there is a change of S-GW. To ensure that the first S-GW cannot deduce any information about the small data transfer security context used in the second S-GW and vice versa, the key derivation function calculating the small data transfer security context should use some unique input that is unique for each S-GW. Another option is that the same small data transfer security context is used with all S-GWs.

X2 handover, S1 handover, and TAU may result in SGW relocation, if different SGWs use different SDT security contexts, new security context need to be established and synchronizes between UE and the new SGW. Thus UE and SGW need to exchange security parameters which used to generate new SDT security context during these three procedures.

- For TAU, MME can generate new SDT security context and deliver it to target SGW through message “create session request”, and MME can also send its security parameters to UE through message “TAU accept”. However, UE can not report its security parameters to MME through message “TAU Request”, because the SGW relocation is determined by MME, so UE can not know whether SGW shall relocate before sending “TAU Request”. If the generation of new SDT security context needs parameters from UE, there is the problem that UE can not report its necessary security parameters to MME. And the security parameters like “uplink NAS count” and “downlink NAS count” have been used already, thus they cannot be used to generate SDT security context. So SDT security context may not be synchronized in TAU with SGW relocation.

- For S1/X2 handover, the UE and the network is not expected to maintain the radio bearer during the handover. UE will release the radio bearer and reconnect once the S1/X2 handover is completed at which time a new SDT security context will be established

5.7.4.2.8 Switching between small data fast path and regular UP

If the UE or network realizes that it is more beneficial to switch to normal user plane traffic than using the small data transfer path (or vice versa), they may switch.

Since the UE and eNB transmits the two traffic types on two different bearers, there is no ambiguity whether it is a small data transfer or a regular user plane connection. Therefore the UE can use the normal LTE AS security to protect any data sent over the normal user plane data radio bearer and only apply the new small data transfer protection if the small data is transmitted over the (otherwise unprotected) data radio bearer used for small data transfer.

When the switches appear, there needs to be an indication sent to the UE from the network, so that the UE will know to re-configure itself for the new data radio bearer and switch to the other security context.

When the switches appear, there needs to be an indication sent from the MME to the S-GW, so that the S-GW will know to re-configure itself when to apply small data security to the small data traffic.

5.7.4.3 Connectionless Data Transmission solution

5.7.4.3.0 General

SA2 solution currently considered in SA2 TR 23.887 v0.8.0 Sec.5.1.1.3.6.3 [26] (Connectionless data transmission, Alternative B) is based on the principle that small occasional data bursts are sent while the UE is in the Idle mode. The RRC connection is established for this transmission, but the S1 MME connection is not. Also, the connections over S1-U/S12 tunnels are predefined at bearer set up time, and maintained via Mobility management procedures (i.e. when SGW relocation happens). The S1-U/S12 UL tunnels are unique per UE and bearer for a given SGW. This eliminates the need to re-establish these tunnels per UE for each short data transmission in the idle mode. This mode of operation is called here the Connectionless mode.

The intention with the Connectionless data transmission solution is that small data can be sent in user plane when the UE is in idle mode without requiring the normal transition to connected mode in AS-layer in LTE systems. As stated in SA2 TR 23.887 Sec.5.1.1.3.6.3.1 [26], the mobility is not required in connectionless mode. Conventionally, this data would be sent either without any AS security, or full AS security re-configuration needs to be executed, including NAS signalling, in order to re-establish AS security. Former would result in vulnerability of small data to eavesdropping, injection, and interception, while latter would be prohibitively complex.

Efficient solution is hence needed to re-establish the AS security protection of the small data traffic with reduced signalling overhead, e.g. without the need for a NAS signaling with the MME/SGSN at every re-connection.

The security solution described below re-uses cached security context at the UE and the eNB/RNC rather than re-creating it at every RRC connection instance. Solution involves the usage of a ‘Token’ for the fast identification of the UE context.

5.7.4.3.1 UE Initial Access and Token Allocation

When the ‘MTC Connectionless’ device uses an eNB/RNC area for the first time to send or receive data on a connectionless bearer, it issues a service request with an indication it is for connectionless service. Security procedures run as defined in Rel.11 (involving the MME, the ENB and the UE per Rel11 33.401 [13], e.g. the MME determines a K_{eNB} and communicates it to the serving eNB via S1-AP, involving the SGSN, the RNC and the UE per Rel11 33.102 [12]) with the addition of following mechanisms:

- The MME returns to the eNB a UE-specific cookie that is uniquely associated with the permanent UE Identity (IMSI) along with the K_{eNB}. This cookie allows the eNB to recognize the potential duplicate cached context for the same UE. The cookie must be unique within the network without revealing the true UE identity.
- The new eNB/RNC allocates a ‘Token’ to indicate the UE security context associated with that eNB. The Token is integrity protected by the established security association. The security context is cached in both the eNB/RNC and UE, while the Token acts as an index to this context. The Token is considered valid for the duration of its life time assigned by the eNB/RNC. The Token, its assigned lifetime, and its associated context have significance within the eNB/RNC that assigns it.
- The UE is expected to retain a context and associated Token for each eNB/RNC it visits and communicates with during the lifetime of the Token.
- The eNB/RNC is expected to retain a context and associated Token for each UE that visits it and communicates with it during the lifetime of the Token assigned by this eNB/RNC.
- When the UE moves to a new eNB/RNC where the UE and eNB/RNC do not have context cached, the new eNB/RNC allocates a new ‘Token’ to indicate the UE security context associated with the new eNB/RNC.

The process of Token Allocation during the initial access is shown on Fig.5.7.4.3.1-1.

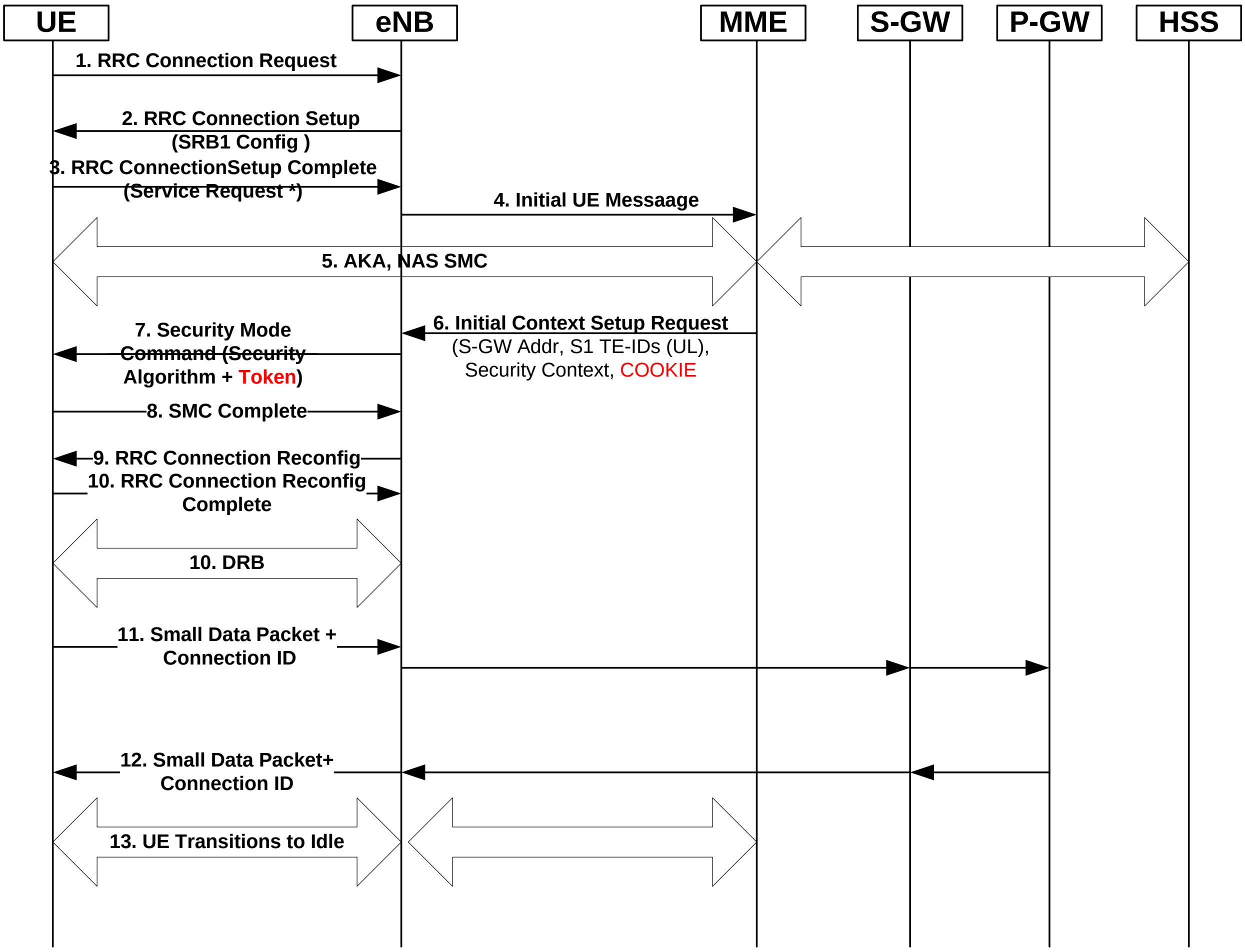

UE
eNB
MME
S-GW
P-GW
HSS
1. RRC Connection Request
2. RRC Connection Setup (SRB1 Config)
3. RRC ConnectionSetup Complete (Service Request *)
4. Initial UE Messaage
5. AKA, NAS SMC
6. Initial Context Setup Request (S-GW Addr, S1 TE-IDs (UL), Security Context, COOKIE
7. Security Mode Command (Security Algorithm + Token)
8. SMC Complete
9. RRC Connection Reconfig
10. RRC Connection Reconfig Complete
10. DRB
11. Small Data Packet + Connection ID
12. Small Data Packet+ Connection ID
13. UE Transitions to Idle

Fig.5.7.4.3.1-1. Initial Access and Token Allocation

Insteps 1-6,the UE initially accesses the new eNB. This is a regular access call flow using the NAS Service Request procedure. In step 5, HSS gives subscription information of UE which includes Connectionless capability to MME. In step 6, Along with security context, the MME also delivers the cookie to the eNB and Token lifetime indication. In step 7 the eNB allocates the Token for the established security context and delivers it to the UE In the RRC Security Mode Command. Steps 7-9, and all subsequent interactions are protected by AS security in Connected state, until UE transitions to Idle state. Transition to Idle state happens after the data transmission is completed.

The Fig. 5.7.4.3.1-2 shows subsequent access to a new eNB when security context already exists at the MME, and AKA authentication is skipped.

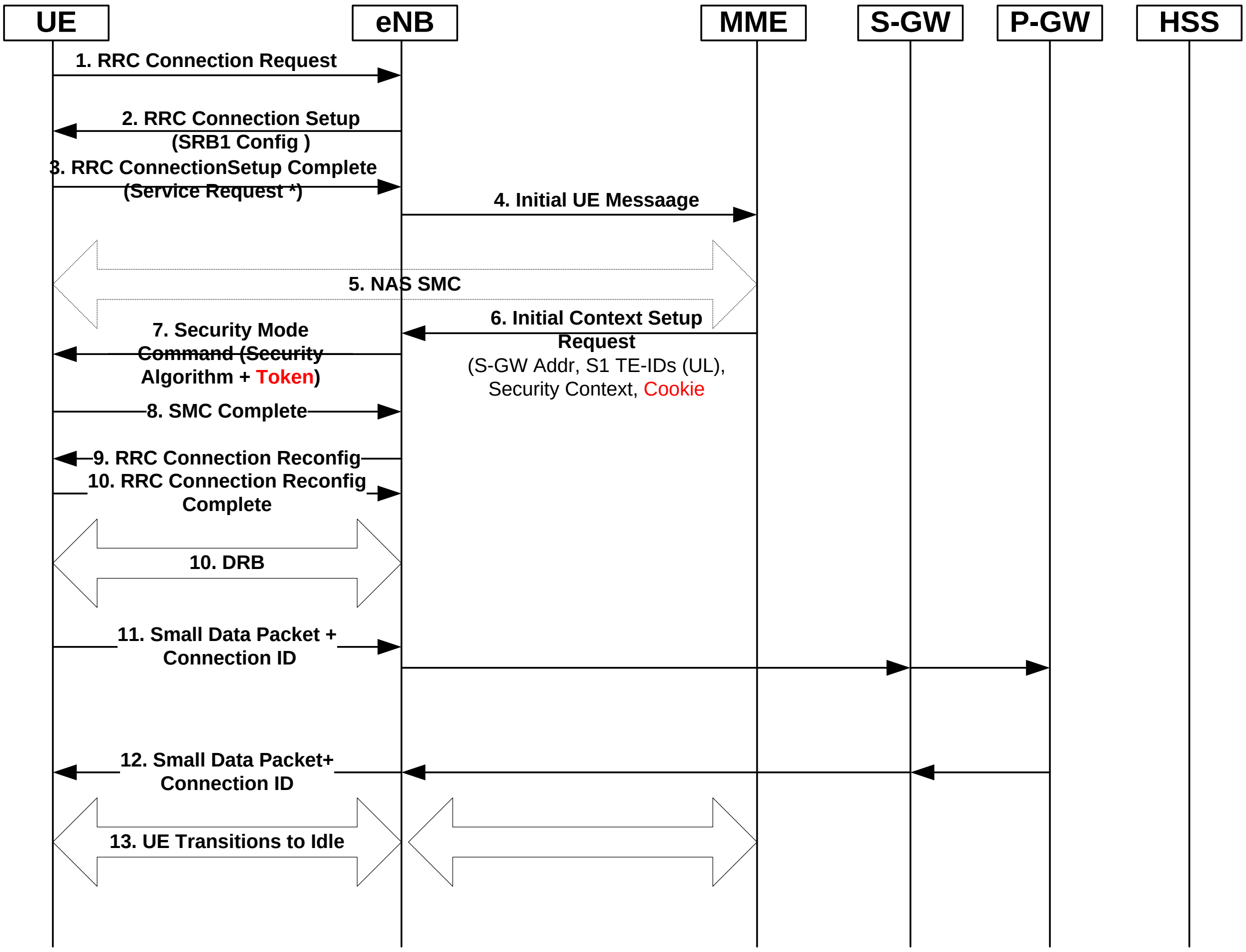

UE
eNB
MME
S-GW
P-GW
HSS
1. RRC Connection Request
2. RRC Connection Setup (SRB1 Config)
3. RRC ConnectionSetup Complete (Service Request *)
4. Initial UE Messaage
5. NAS SMC
6. Initial Context Setup Request (S-GW Addr, S1 TE-IDs (UL), Security Context, Cookie
7. Security Mode Command (Security Algorithm + Token)
8. SMC Complete
9. RRC Connection Reconfig
10. RRC Connection Reconfig Complete
10. DRB
11. Small Data Packet + Connection ID
12. Small Data Packet+ Connection ID
13. UE Transitions to Idle

Fig.5.7.4.3.1-2. UE Subsequent Access to MME with K_{ASME} (no AKA)

Similarly to the process shown in Fig.5.7.4.3.1-1, in step 6 the MME returns the security context as well as the cookie, and in step 7 the eNB allocates the Token to this security context.

5.7.4.3.2 Use of a Token for Subsequent Network Access

For subsequent access in connectionless mode to the eNB/RNC with which the UE has a cached context and a valid Token, once the UE recognizes the eNB/RNC from the id it broadcasts, the UE uses this Token to re-initiate the security context.

The unique eNB identity within PLMN is explicitly included in the E-UTRAN broadcast (CI in the SIB1).

In UTRAN the RNC identity is not explicit, and as imbedded in the 28-bit CellID, may be between 12 and 16 bits. In a simplified case, the Token will be assigned per CellID resulting in multiple Tokens leading to the same context. Optimizations are possible if the UE can better identify specific RNC that holds the context.

UE continues PDCP Counters used for ciphering and integrity protection as per the Token context applicable to the eNB/RNC.

UE sends the Token to eNB/RNC in the RRC Connection Request procedure to do a fast establishment of the DRBs and SRBs needed for the intended service. From the eNB/RNC viewpoint, once the context is found, the session is restored as if the UE never left this eNB/RNC.

The Token included in the Connection Request procedure is integrity protected using the respective RRC security association (Integrity Protected using K_{RRCInt}), to allow one step validation and replay protection.

When the ENB/RNC has validated the Token and retrieved the corresponding context, the ENB/RNC does not need to contact the MME/SGSN to provide service to the UE.

An UE that wants to exchange NAS signalling (e.g. to activate a PDN connection) uses normal connected mode operation, not connectionless mode operation. The process of Token use for subsequent accesses is shown on Fig.5.7.4.3.3-1.

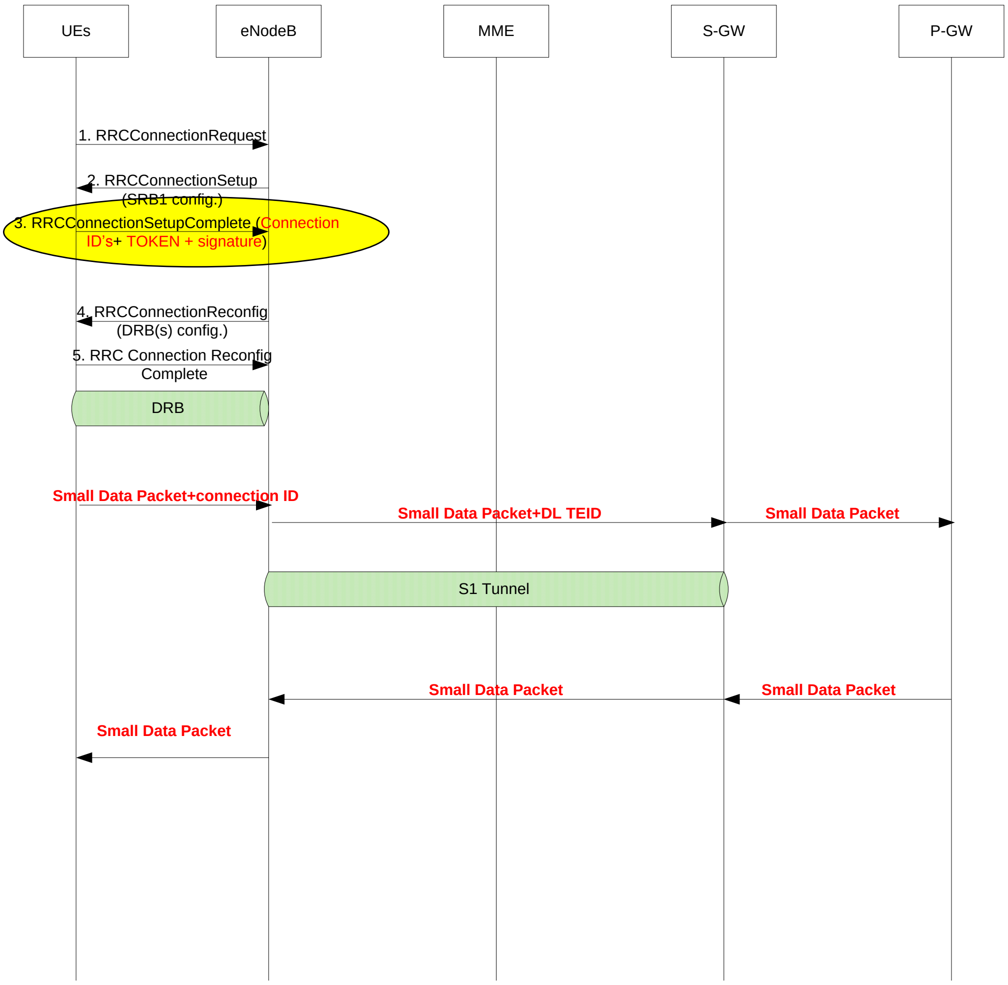

UEs
eNodeB
MME
S-GW
P-GW
1. RRCConnectionRequest
2. RRCConnectionSetup (SRB1 config.)
3. RRCConnectionSetupComplete (Connection ID's+ TOKEN + signature)
4. RRCConnectionReconfig (DRB(s) config.)
5. RRC Connection Reconfig Complete
DRB
Small Data Packet+connection ID
Small Data Packet+DL TEID
Small Data Packet
S1 Tunnel
Small Data Packet
Small Data Packet
Small Data Packet

Fig.5.7.4.3.2-1 Use of Token for subsequent access.

In message 3 "Connection Setup Complete" UE includes the Connection ID allocated for small data, and the Token associated with the security context established during initial attach. This and all subsequent messages and data are protected by AS security associated with the Token.

5.7.4.3.2.1 AS security context separation and coexistence.

Connection-oriented and connectionless sessions will not run simultaneously.

If during the regular data session in connected state the application needs to send a small data, it will be sent through a normal data channel on already allocated bearer. Conventional AS security created for the connection-oriented session will be used to secure the short data. Additionally, per 5.7.4.3.1 UE Initial Access and Token Allocation, the eNB will cache the security context and generate a Token for future connectionless mode sessions. If during the connection state a handover is performed to a eNB with a cached security context, the cached security context (if exists) is left untouched and unused in connected state.

Similarly, if the connectionless mode is established for sending the small data, then regular data session will not be established concurrently.

Transitions from connectionless to a connection-oriented mode or vice versa during the data transmission session are not expected.

5.7.4.3.2.2 Duplicate Cached Context Recognition

The eNB may recognize during connection-oriented session establishment that there is already a valid security context and a Token cached for this UE. The recognition would be possible because the cached context is linked to the UE-specific cookie returned by the MME during the session establishment.

Recognition of a duplicate cached context is achieved as follows:

When the AS security context is received from the MME, the eNB will search its cache for a stored context associated with the cookie for the UE, and if found, the eNB can declare the duplicate context.

Once the duplicate context is declared, the eNB replaces the existing cached context with the new one, and assigns a new Token to it. The old context and Token are purged.

5.7.4.3.3 Cached Context Invalidation and Deletion

The contexts and the Tokens in the UE get deleted in the UE when it detaches from the network.

The contexts and the Tokens are also deleted due to aging, when associated lifetime expires.

The context and the Token are deleted in the UE when the value of PDCP Counter approaches locally preset maximum limit, to avoid roll over. Subsequent access to the same eNB/RNC will proceed without Token, and new context will be derived.

If new AKA authentication is executed, and new K_{ASME} (or CK/IK) is derived, all existing cached Tokens and contexts in the UE are deleted. The new Token is assigned for the current new context.

If UE returns to the eNB/RNC with no Token indication, even if eNB/RNC has the valid cached context and valid Token with this UE, the eNB/RNC will delete existing Token for this UE, treat the access as an initial entry, and assign the new Token.

If the eNB receives the security context from the MME to be used for connectionless mode for the UE, and eNB finds already cached valid context for this UE/cookie, the eNB invalidates the old security context and Token, replaces it with the new security context, and assigns the new Token.

If UE returns to the eNB/RNC with a Token but the eNB/RNC has no valid cached context associated with this valid Token, the eNB/RNC will reject the access attempt and require the UE to execute a full service request procedure as if this was a new eNB/RNC for the UE.

5.7.4.3.4 Token Lifetime Management.

Different MTC applications may have different activity times and hence the Token Lifetime needed for the devices may differ from device to device.

A uniform allocation of the Token Lifetime for all MTC devices is a simple option for eNB implementation. However, if the Token runs out too soon compared to the MTC device activity, it would need to go through the initial access procedure every time, which is not optimal. Similarly, if the Token Lifetime is too long, storage resources in the UE and eNB may become overloaded for no reason, which is not optimal either.

Another option could be an allocation based on the subscription details coming from HSS to MME/SGSN and to eNB/RNC. At the initial access, the IMSI of the device may be correlated with requirements of its subscription applications, and Token lifetime allocation may correspond to these application requirements. This option will need standardization effort.

Some intelligent eNB/RNC implementations may adapt the Token Lifetime allocation to the observed periodicity of UE activity.

Hence there are different considerations for Token lifetime allocation.
Token lifetime allocation need to be sensitive to the nature of MTCe device application and the frequency of data exchange.

For example for once a month metering device where one or two packets of meter reading data are sent by the device it may not make sense to keep a cached context in the eNB. Conventional connected mode operation may be sufficient.

Whereas for an MTCe device which sends a sensor data once an hour it might make sense to keep its context cached in the eNB for at least a couple of hours, and allow a Connectionless transmission protected with a cached context.

Hence for Connectionless devices, the application-specific frequency of transmission correlated with practical Token lifetime may be a part of the subscription information transferred to MME to fine tune the Token allocation and context retention.

Token life time indication is send from MME to eNB as part of the Initial Context setup message. MME makes this determination based on the subscription data.

5.7.4.3.5 Threat scenarios

5.7.4.3.5.1 A “Stolen Token” scenario:

Since Token is sent by the UE in the clear, it could be eavesdropped on by the attacker. Subsequently, the attacker may try to replay the same Token in its own access. However, because the attacker will not have a security context associated with the Token, he will not be able to apply a proper integrity protection to the Token. Integrity Validation of the Token will fail at the eNB, presented value of the Token will be ignored, connectionless access request will be rejected. Therefore, there is no benefit to the attacker to steal the Token.

5.7.4.3.5.2 eNB Resource exhaustion attack by a malicious UE

To explore resource exhaustion (i.e., cached context), the malicious UE may continually access the eNB with the connectionless indication but without the Token, even though the eNB already cached a valid context and Token for this UE. The potential resource exhaustion on eNB is addressed by identifying the duplicate context for the same UE. This is accomplished by sending the UE -specific cookie by the MME to the eNB. The cookie is cached along with the context, and when the new context is received from the MME, the eNB can search for the duplicate context associated with the same UE/cookie. The old duplicate context will be replaced with the new context and a new Token will be assigned. As this request can be entertained only if the UE issuing it properly authenticates, the malicious UE will not be able to invalidate the context associated with any other UE. Therefore there is no benefit to the attacker to plant the resource exhaustion attack.

In other way to explore resource exhaustion, the malicious UE may access multiple eNBs with the connectionless indication but without the Token, thus leading each eNB to creating the cached security context with the Token that will not be used. This created in vain security context will be purged upon its lifetime expiration, and will present a small fraction of overhead in utilization of memory resources for the eNB, as allocated to a single memory cache for a single malicious UE.

5.7.4.3.5.3 Forging of small data transmission by obtaining cached security context from a compromised eNB while the cached security context is still valid.

The compromised eNB will receive from the MME a necessary security association – the K_{eNB} – that will enable it to forge data transmission for all sessions - connectionless and connection-oriented. There is no benefit to target only cached context, if a fresh context can be simply received for every session. Moreover, the forged small data can be delivered into the S1U without regard to any AS security, whether cached or not. Therefore, danger of eNB compromise remains critical for small data as well as normal data sessions, and is not different from that addressed in a current security framework.

5.7.4.3.5.4 Retroactive decryption of past data by obtaining the cached security context from a compromised eNB while the cached security context is still valid.

The attacker may gain access to the eNB during the off-hours, when eNB is not monitored for an unauthorized access and therefore is more vulnerable. Proper Token lifetime management policies can ensure that cached context is deleted during these hours of higher vulnerability. The context used for protecting the short data during hours of higher vulnerability should be time-limited, possibly limited to individual short data transmission session or few sessions, and should be deleted after these set limits are over. During the normal business hours, when access to the eNB is normally monitored, the connectionless context lifetime management can be restored again to its normal policy values. Re-establishing the connectionless context in such a scenario may have additional processing if large number of UEs are involved.

If an eNB is permanently vulnerable to a compromise, the Connectionless feature could be disabled from such an eNB.

5.7.4.3.5.5 Potentially increased risk of key compromise in the eNB due to retaining the AS security context.

Retained AS security context can be used over extensive period of time for securing a large number of small data transmissions. However, it does not present a different potential for cryptanalysis than when the same AS security context is used for securing a large data transmission over the single session for a comparable amount of data. The validity of security context is currently limited by the size of the PDCP counter, which is used as the crypto-sync. The same limitation is observed for the connectionless mode to limit the amount of data exchanged during a validity period of the cached security context. Therefore, there is no additional risk of key compromise in the eNB due to retaining the AS security context.

Key vulnerability due to caching: The cached AS security context is available in the eNB. This increases the time an attacker can spend on cryptanalyzing traffic sent between the UE and the eNB, resulting in that the attacker gets they encryption key. The attacker can then decrypt new traffic sent at a later time using the cached AS security context. However, there is no reason to believe that it is feasible to break the currently used security algorithms.

Moreover as discussed in 5.7.4.3.4 context caching need to be sensitive to the nature of MTCe application and the frequency of data exchange. The application sensitive context caching at eNB, helps eNB to fine tune the caching specific to individual UEs. This means that it is possible to have some control over how long time the AS security context is available in the eNB. Further periodic refresh of cached context at eNB can be implemented as a policy to re-fresh of context oblivious to UE procedures.

5.7.4.3.5.6 Potentially increased risk to UE Identity Confidentiality in eNB.

Unlike in current operation, when the eNB does not recognize identity of the UE, the connectionless security scheme proposes to send the UE-specific cookie from the MME to the eNB to assist in recognizing duplicate cached context. Identity Confidentiality is preserved since a cookie is generated instead of sending the UE identity to the eNB.

5.7.4.4 MTC-IWF based Secure Solution for Small data transmission

5.7.4.4.1 Background and requirements

In SA3, we are studying small data transmission (SDT) security where the issue of concern is in-frequent transmission of SD while UE is in RRC-IDLE state because that is when AS security context does not exist. This is also visible in SA2 solutions [TS 23.887 sections 5.1.1.3.1 and 5.1.1.3.2 [26]]. As many such UEs can exist, establishment of AS and/or NAS security will increase signalling and have negative impact on network as well as UE resources. Therefore it is required to minimize signalling traffic [TS 22.368 [9] section 7.2.5 and TS 23.887 section 5.1.1.2 [26]].

5.7.4.4.2 Potential solutions

As AS security is out of question to secure SDT the security in core network can end at (i) MME with NAS security, (ii) MTC-IWF or (iii) some other network element like SGW. Any solution should provide adequate security while having minimal impact on the current system architecture; this valid for both SDT and DT.

So as to minimize impact on network, reduce resource usage and minimize system architecture impact we propose a solution with MTC-IWF as the end-point for security in the network. With MTC-IWF as security end-point in the network, security of SD and DT communication can be provided even when AS and/or NAS security context are not available.

5.7.4.4.3 Solution overview

The solution consists of 1) Authentication and Key Agreement (AKA). During this procedure, HSS derives a master key K_iwf and sends it to MTC-IWF. 2) keys negotiation and establishment using a new Security Mode Command (SMC) procedure carried between UE and MTC-IWF – this new procedure can ride on NAS SMC. As a result of this procedure, UE and MTC-IWF share the same K_iwf and subkeys for confidentiality and integrity protection. 3) SD (both mobile originated, MO, and mobile terminated, MT) and trigger transmission: the transmission can ride on packets that do not need NAS security as per current specification, with recognition of such data is being carried, NAS security can be omitted. In the following section we propose the detailed solution.

Editor's Note: The impact to MME is FFS when terminating the security in the IWF and MME receives unprotected NAS message carrying small data.

Editor's Note: Details including confidentiality and integrity protection of the security protocols between the UE and the MTC-IWF should be given.

5.7.4.4.4 Detailed Solution

5.7.4.4.4.0 General

In this section we discuss solution detail covering key derivation and negotiation, security mode command, and small data transmission and delivery. Solution evaluation is given at the end of the section.

5.7.4.4.4.1 Key Derivation and negotiation

We propose a new key hierarchy shared between UE and MTC-IWF. This new key hierarchy contains a master key K_iwf, and a pair of subkeys (for confidentiality and integrity protection separately) derived from K_iwf. The message sequence of how the K_iwf and subkeys are derived in network during Attach procedure is depicted in Figure 1 and discussed below.

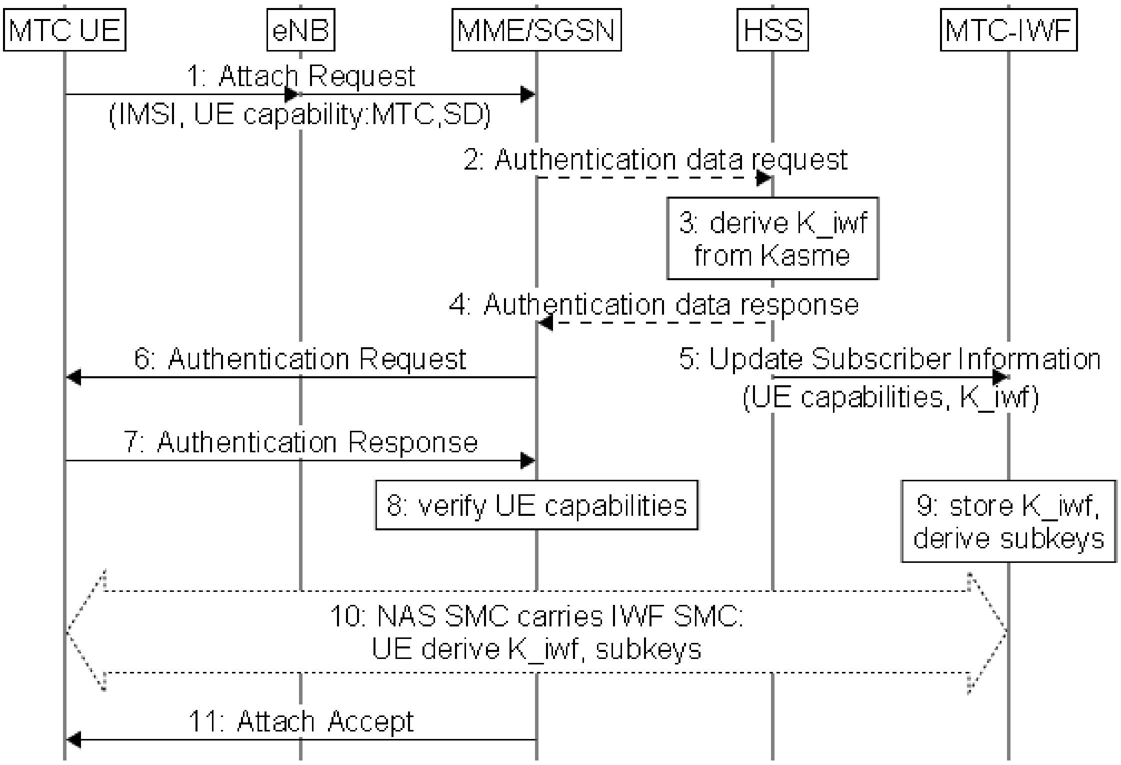

MTC UE
eNB
MME/SGSN
HSS
MTC-IWF
1: Attach Request
(IMSI, UE capability:MTC,SD)
2: Authentication data request
3: derive K_iwf from Kasme
4: Authentication data response
6: Authentication Request
5: Update Subscriber Information
(UE capabilities, K_iwf)
7: Authentication Response
8: verify UE capabilities
9: store K_iwf, derive subkeys
10: NAS SMC carries IWF SMC:
UE derive K_iwf, subkeys
11: Attach Accept

Figure 1. Key derivation in Attach Procedure

1. UE sends Attach Request, contains IMSI and UE capability of MTC communication and sending/receiving Small Data.
2. MME sends Authentication data request to HSS.
3. HSS derives K_iwf from Kasme (in case of E-UTRAN).
4. HSS sends Authentication data response to MME
5. HSS sends MTC-IWF the UE capabilities and K_iwf in a new message for example Update Subscriber Information
6. MME sends Authentication Request to UE
7. UE sends MME the Authentication Response.

Note: Step 2, 3, 5, and 6 follow the normal Authentication procedure.

8. MME verifies whether UE is a MTC device and is allowed to send/receive Small Data, according to the information it retrieved from HSS.
9. At MTC-IWF, K_iwf is stored and subkeyes are derived.
10. We propose a new IWF SMC procedure, which is carried in NAS SMC. After the procedure, UE shares the same K_iwf and subkeys with MTC-IWF. The detail of IWF SMC procedure is depicted in Figure 2.
11. MME sends Attach Accept to UE.

5.7.4.4.4.2 Security Mode Command

In this section, Step 9 in Figure 1 of IWF SMC carried in NAS SMC procedure is discussed. During the procedure, MTC-IWF can inform UE the algorithm for key derivation. UE and MTC-IWF can perform integrity check with the integrity subkey. After IWF SMC procedure, UE and MTC-IWF will share the K_iwf and subkeys. The details are given in Figure 2.

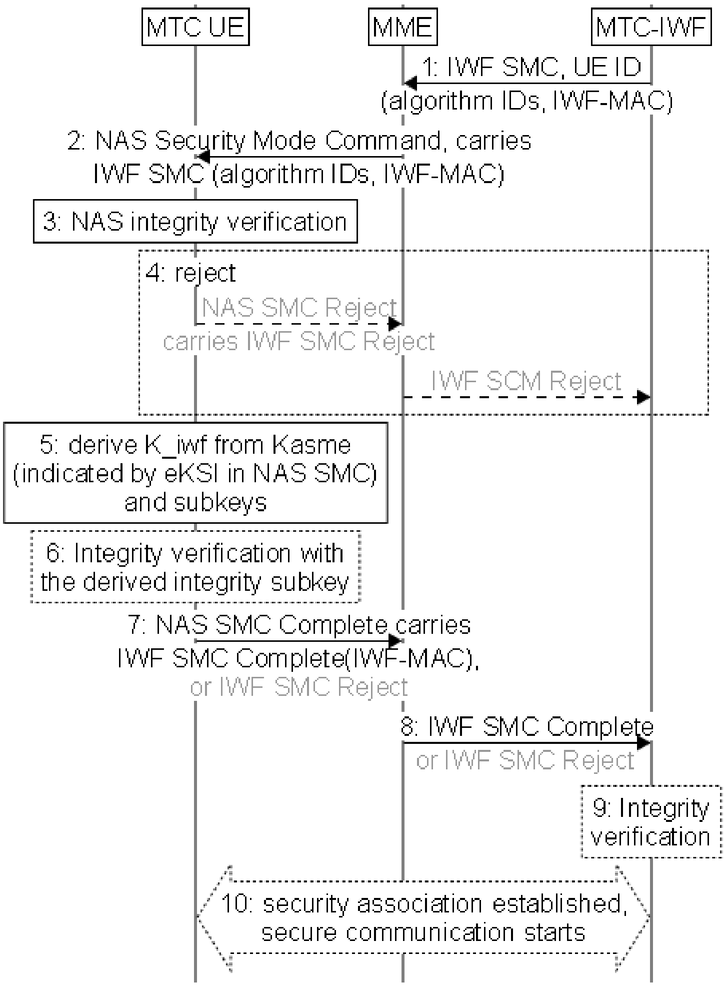

MTC UE
MME
MTC-IWF
1: IWF SMC, UE ID
(algorithm IDs, IWF-MAC)
2: NAS Security Mode Command, carries
IWF SMC (algorithm IDs, IWF-MAC)
3: NAS integrity verification
4: reject
NAS SMC Reject
carries IWF SMC Reject
IWF SCM Reject
5: derive K_iwf from Kasme
(indicated by eKSI in NAS SMC)
and subkeys
6: Integrity verification with
the derived integrity subkey
7: NAS SMC Complete carries
IWF SMC Complete(IWF-MAC),
or IWF SMC Reject
8: IWF SMC Complete
or IWF SMC Reject
9: Integrity
verification
10: security association established,
secure communication starts

Figure 2. IWF SMC procedure carried in NAS SMC

1. MTC-IWF sends integrity protected IWF SMC message or the necessary parameters for UE to perform key derivation, with UE ID to MME.
2. MME carries the IWF SMC message with NAS Security Mode Command message and sends it to UE.
3. UE performs NAS integrity verification.
4. If NAS integrity verification fails, UE sends NAS SMC Reject message carrying IWF SMC Reject message to MME, MME forwards the IWF SMC Reject message to MTC-IWF.
5. If NAS integrity verification is successful, UE derives K_iwf and subkeys. UE uses the Kasme indicated by the eKSI in NAS Security Mode Command.
6. UE performs integrity verification on the IWF SMC, using the integrity subkey derived by UE.
7. UE sends the NAS SMC Complete carrying IWF SMC Complete to MME, IWF SMC Complete message can be integrity protected.
8. Or UE sends IWF SMC Reject message carried in NAS SMC Complete, if the verification in Step 6 fails.

Or MME forwards the IWF SMC Complete or IWF SMC Reject message to MTC-IWF.

9. MTC-IWF can perform integrity verification on the IWF SMC Complete message.
10. Security association is established between UE and MTC-IWF and they can start secure communication. If MTC-IWF received IWF SMC Complete, and integrity verification is passed at Step 9 (when it is carried).

If a NAS SMC procedure is carried following a normal AKA in initial procedures, MME can know that whether UE already has Kasme, whether UE Capability allows itself to derive K_iwf (for example, if UE subscribes MTC service, if UE subscribes SDT service). A timer can be set in MME to wait for IWF SMC from MTC-IWF.

(1) Before the timer expires, MME waits for the IWF SMC to start NAS SMC procedure.
(2) If MME does not receive IWF SMC from MTC-IWF, and the timer is expired, MME will perform a normal NAS SMC to UE.
(3) If MME receives IWF SMC from MTC-IWF when the timer is already expired, MME can run an empty NAS SMC only for carrying the IWF SMC procedure.
(4) When MTC-IWF decides to update K_iwf and sends MME the IWF SMC, MME will perform an empty NAS SMC to carry the IWF SMC.
(5) The timer: the timer can be started when MME received Authentication Response from UE. The timer can be stopped when it is expired or when IWF SMC is received from MTC-IWF.
(6) The IWF-SMC procedure: it is independent from other NAS procedures. MTC-IWF can decide when to send it. During initial procedure, if MTC-IWF sends the IWF SMC before timer in MME expired, the IWF SMC and NAS SMC can be combined; if not, they can be separated.

5.7.4.4.4.3 Small data and device trigger communication

5.7.4.4.4.3.0 General

We consider the procedure can be the same for MTC device trigger and Small Data MT transmission. It is assumed that MTC-IWF has UE serving node information. If not, it can retrieve the information upon receiving Device Trigger/Small Data Submission Request, by sending Subscriber Information Request to HSS, and receives a Subscriber Information Response from HSS that contains the serving node information.

Note: As per the current document small data should be integrity protected and maybe confidentiality protected.

5.7.4.4.4.3.1 MT small data when UE is IDLE

This section presents secure MT small data transmission when UE is idle. It can also apply to device trigger. MTC-IWF upon receiving the small data or trigger will perform SCS authorization and submit it to MME. Paging procedure is used for the SD or DT delivery. The detail is depicted in Figure 3 given below.

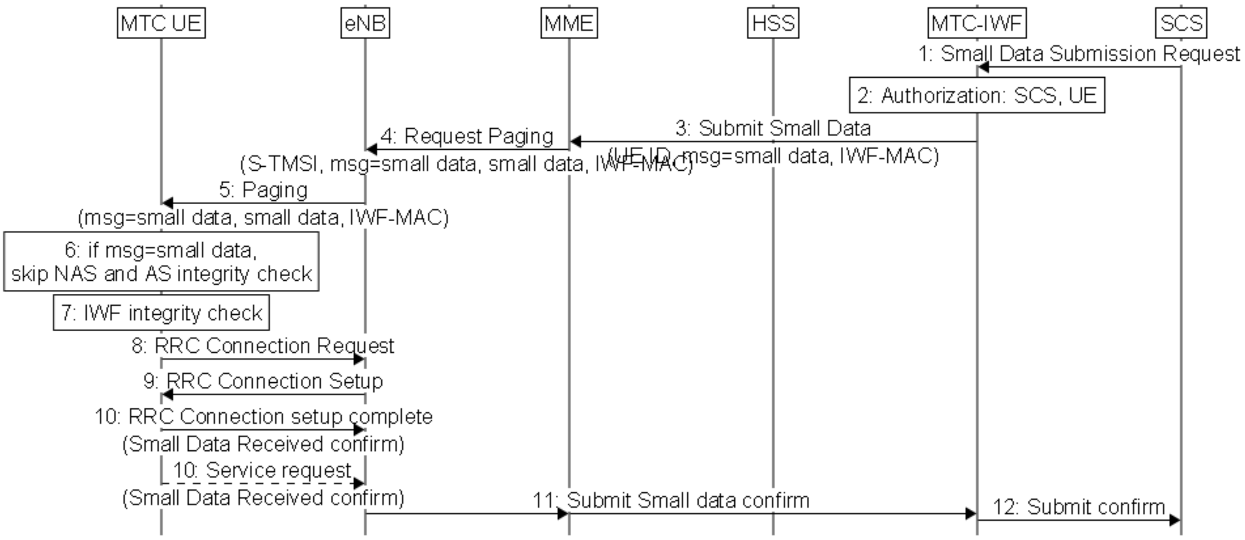

MTC UE
eNB
MME
HSS
MTC-IWF
SCS
1: Small Data Submission Request
2: Authorization: SCS, UE
3: Submit Small Data
(UE ID, msg=small data, IWF-MAC)
4: Request Paging
(S-TMSI, msg=small data, small data, IWF-MAC)
5: Paging
(msg=small data, small data, IWF-MAC)
6: if msg=small data,
skip NAS and AS integrity check
7: IWF integrity check
8: RRC Connection Request
9: RRC Connection Setup
10: RRC Connection setup complete
(Small Data Received confirm)
10: Service request
(Small Data Received confirm)
11: Submit Small data confirm
12: Submit confirm

Figure 3. MT Small Data Transmission

1. SCS sends Small Data Submission Request to MTC-IWF.
2. MTC-IWF performs SCS and UE authorization, to see if SCS can send Small Data and if UE can receive Small Data.
3. MTC-IWF submits the Small Data to MME, with UE ID, message type as small data, integrity protection with integrity subkey (IWF-MAC), and confidentiality protection with confidentiality subkey if needed.
4. MME sends to eNB the Small Data in Request Paging message, contains S-TMSI, message type as small data, and IWF-MAC.
5. eNB sends to UE the Small Data in Paging message.
6. Upon receiving, UE can skip NAS and AS integrity check, if the message type is small data.
7. UE performs IWF integrity check, with the integrity subkey.
8. Normal RRC Connection Request is sent from UE to eNB.
9. Normal RRC Connection Setup is sent from eNB to UE.
10. The Small Data Receive confirm can be sent in RRC Connection setup complete or sent in Service Request to eNB.
11. Submit Small data confirm can be sent from eNB→MME→MTC-IWF.

5.7.4.4.4.3.2 MO small data when UE is IDLE

This section presents secure MO small data transmission when UE is idle. It requires MME to store the routing information for UE, such that UE does not need to contain MTC-IWF identifier in the Small Data. The detail is depicted in Figure 4 given below

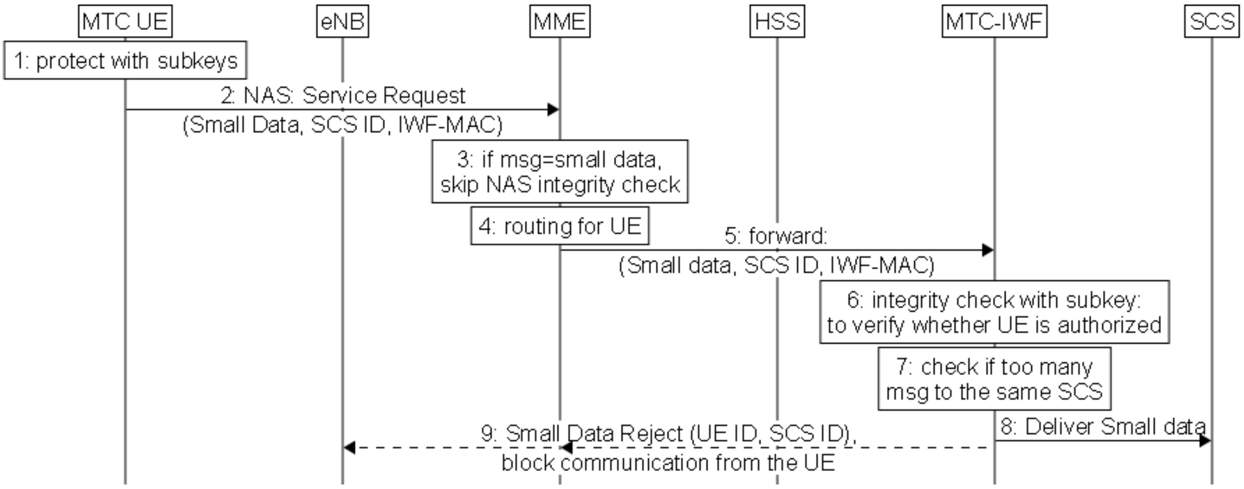

MTC UE
eNB
MME
HSS
MTC-IWF
SCS
1: protect with subkeys
2: NAS: Service Request
(Small Data, SCS ID, IWF-MAC)
3: if msg=small data, skip NAS integrity check
4: routing for UE
5: forward:
(Small data, SCS ID, IWF-MAC)
6: integrity check with subkey: to verify whether UE is authorized
7: check if too many msg to the same SCS
8: Deliver Small data
9: Small Data Reject (UE ID, SCS ID), block communication from the UE

Figure 4. MO Small Data Transmission

1. UE uses the subkeys to integrity and confidentiality (if necessary) protect the Small Data.
2. UE sends Small Data in Service Request to MME, with SCS ID.
3. MME can skip NAS integrity check, if the message type is small data.
4. MME retrieves the routing for UE and finds out to which MTC-IWF the Small Data should be sent.
5. MME forwards the Small Data to MTC-IWF.
6. MTC-IWF performs integrity check with its subkey and performs UE authorization, to see if the UE is allowed to send Small Data towards the given SCS.
7. MTC-IWF can also detect if there are too many small data being sent to the same SCS.
8. If the verifications in Step 6 and 7 are successful, MTC-IWF delivers the Small Data to SCS.
9. If the verifications in Step 6 and 7 failed, MTC-IWF can inform MME/eNB by sending Small Data Reject message, such that eNB and MME can block communication from the given UE and/or to the given SCS.

5.7.4.4.4.3.3 Small data and device trigger when UE is CONNECTED

We consider the procedure can be the same for MTC device trigger and Small Data MT transmission when UE is CONNECTED. The SD or DT can be protected with subkeys and carried in NAS message of DOWNLINK GENERIC NAS TRANSPORT. This is to show that the proposed solution can be applied to UE in CONNECTED. The details are depicted in Figure 5 given below.

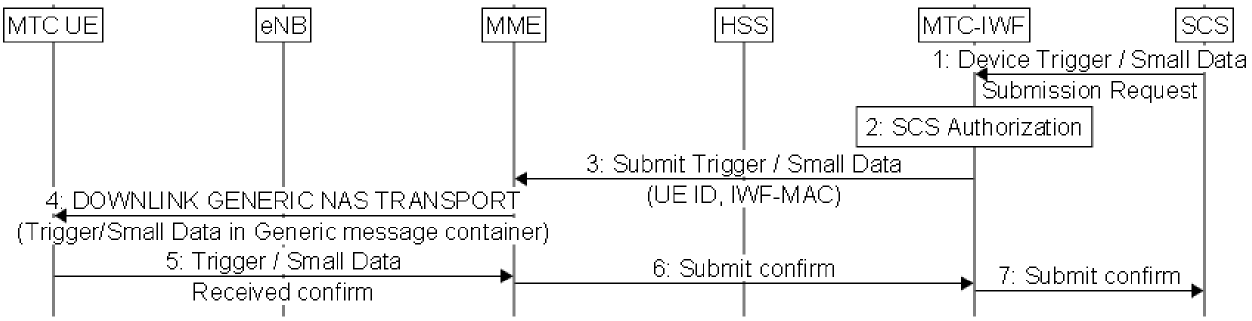

MTC UE
eNB
MME
HSS
MTC-IWF
SCS
1: Device Trigger / Small Data Submission Request
2: SCS Authorization
3: Submit Trigger / Small Data (UE ID, IWF-MAC)
4: DOWNLINK GENERIC NAS TRANSPORT (Trigger/Small Data in Generic message container)
5: Trigger / Small Data Received confirm
6: Submit confirm
7: Submit confirm

Figure 5. Trigger and Small Data Transmission

1. SCS sends Device Trigger or Small Data Submission Request to MTC-IWF.
2. MTC-IWF performs SCS authorization.
3. MTC-IWF submits the Trigger or Small Data to MME, with UE ID and also integrity protection with integrity subkey, and confidentiality protection with confidentiality subkey if needed.
4. MME carries the Trigger/Small Data in Generic message container of DOWNLINK GENERIC NAS TRANSPORT message.
5. Upon receiving, UE sends Trigger/ Small Data Received confirm to MME.
6. MME sends to MTC-IWF the Submit confirm.
7. MTC-IWF sends the Submit confirm to SCS.

5.7.4.4.4.4 Protocol between UE and MTC-IWF

The IWF protocol is between NAS and application layer protocol for MTC, it spans between UE and MTC-IWF and can be transparent to MME/SGSN/MSC. For the protocol between MME and MTC-IWF, the T5-AP defined in clause 5.1.1.3.3 TR 23.887 [26] can be used.

The figure below illustrates the protocol stack.

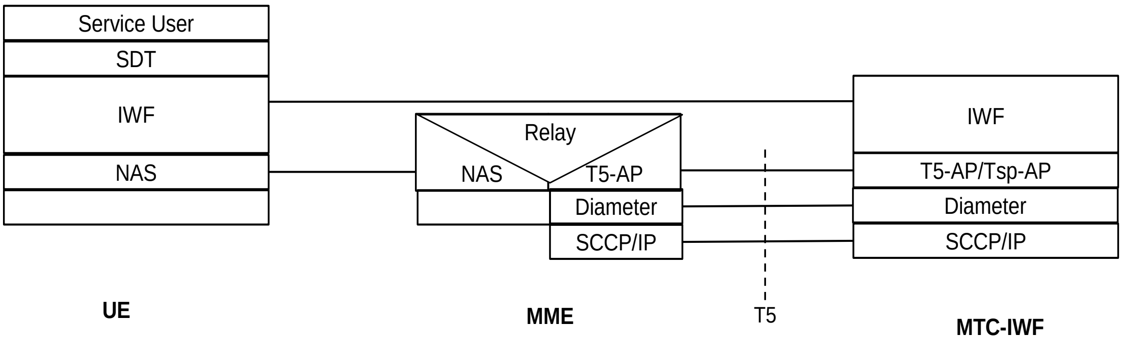


Figure 6. Protocol stack between UE and MTC-IWF

5.7.4.4.4.5 Normal small data consideration

We assume that:

a. Normal data can be sent through MTC-IWF or SGW, and this section only presents the case when it is sent through MTC-IWF.

b. Normal procedures means the data is not small data

c. Normal data can only be sent when UE is CONNECTED and the NAS and AS security are activated.

(1) In case of MTC-IWF, our solution can be used with improvement.

For Downlink, MTC-IWF receives normal Data Submission Request from SCS, it performs data size check, authorization and protection. Normal data should not be delivered to UE in idle. NAS and AS security can be optional or mandatory depends on the agreement between UE and network.

For Uplink, when UE sends normal data, MME can perform normal/small data check. There should be requirements on when and how normal data can be sent. For example: normal data can only be sent when UE is connected. NAS and AS security can be optional or mandatory depends on the agreement between UE and network.

(2) In case of SGW, current procedure is followed.

5.7.4.5 Connectionless Data Transmission Solution Using Separate Security Context

5.7.4.5.1 General

In order to achieve acceptable level of security and low complexity in handling the security context, a separate security key to be used for connectionless data transmission. The reasons being:

➢ Effective PDCP COUNT handling

  – Current specification resets the PDCP COUNT, during state transitions. With the solution under study (cf. secition5.7.4.3), PDCP COUNT to be maintained along with the AS security context and it is continued even when the UE comes back to the same cell and also when the UE moves from connection oriented mode to connectionless mode of operation. This will lead to HFN de-synchronization issues and complex PDCP COUNT handling in the UE and also in the eNB.

❖ To be in line with the existing PDCP COUNT handling mechanisms and to reduce complexity, a separate security key to be used for connectionless data transmission, so that PDCP COUNT can be reset to “0” during state transitions.

➢ Potentially increased risk of key compromise in the eNB due to retaining the AS security context for long time.

  – Solution under study (cf. section 5.7.4.3) uses the same AS security context for both connection oriented and connectionless mode of operations, the risk from key compromise is high since the same keys are cached and used for long time for both modes. Also if the key is compromised, then the attack duration is long. We assume that the key compromise happens over the air interface.

❖ Whereas in case of separate security key for connectionless data transmission, since different keys are used, life time/usage of the key is less (key refresh happens whenever there is state transition and also whenever there is cell change), so the risk is minimized. The proposed solution refreshes the key without performing the service request procedure.

➢ Resource exhaustion attack on eNBs

  – As the MME is not aware of whether the key will be used for connectionless or connection oriented transmission, there is possibility of resource exhaustion attack on eNBs by a malicious UE creating security contexts in several eNBs.

❖ If the MME is involved in the connectionless data transmission key derivation, then the MME can control the number of keys established for the UE for the connectionless transmission and may also delete the security context in the eNB, if the MME identifies UE’s cell change or make UE to move to connection oriented mode as UE request key frequently for connectionless operation or reduce the lifetime of the key, as key request for connectionless operation is frequent.

➢ Preventing the attacks being carried out between Idle and Connected modes

  – If the connected mode operation key is compromised, then this should not lead to continue the attack in the connectionless operation.

❖ To be in line with the compartmentalization security principle, the key used for connectionless data transmission to be cryptographically different with the key used in connected mode. This is achieved using separate key for connectionless transmission.

➢ Support for cell change without performing service request procedure

❖ It would be advantages to get the security context in place for the connectionless without performing the complete service request procedure.

➢ No concurrent Connectionless and Connection oriented mode of operation at any one time

- As SA2 decided that *"Multiple PDN connections can be supported concurrently. However all PDN connections are handled in Connectionless or Connection oriented mode at any one time."*. This is in favour of using separate security context for connectionless mode to enhance the level of security.

5.7.4.5.2 Separate Security Context Mechanism

The security solution described below use separate key K_{CLT} at the UE and the eNB for connectionless transmission rather than caching and using the keys used in connected mode. In case of LTE, the protection is be provided by the PDCP layer between UE and eNB. The UE and the MME derives the key K_{CLT} . When requested by eNB, MME derives and passes the K_{CLT} for the AS security protection (especially user traffic protection). The separate AS security protection of the small data traffic is established for the first small data packet, when the UE is in idle mode and use the established context for the rest small data transmission in the same cell and till the life time of the key. When the UE moves to connected mode, the security context established for the small data traffic is deleted and the UE follow the existing procedure for establishing the AS security context. The small data packets are secured by the UE and the eNB by encrypting the data packets and/or applying the integrity protection with keys derived fro m the key K_{CLT} and using the selected cryptographic algorithms for the connectionless data transmission. The cryptographic algorithms selected during AS SMC procedure for connected mode protection can be used for connectionless data protection. When there is a cell change or state transition to idle, PDCP COUNT for s mall data are reset to 0 and the key K_{CTL} is refreshed.

5.7.4.5.3 Key Derivation

The MME and the UE derives the new security key K_{CLT} using MME nonce and the K_{ASME} for connectionless transmission mode. The K_{CLT} derivation using MME nonce is given below:

$$K_{CLT} = KDF \{K_{ASME}, NONCE_{MME\text{-}CLT}\}$$

MME nonce is used to generate unique key per request. $K_{CLT\text{-}int}$ and $K_{CLT\text{-}enc}$ are derived in the UE and in the eNB.

The derivation of $K_{CLT\text{-}int}$ and $K_{CLT\text{-}enc}$ are as follows:

$$K_{CLT\text{-}int} = KDF \{K_{CLT}, \text{Int Alg-ID, CLT-int-alg}\}$$

$$K_{CLT\text{-}enc} = KDF \{K_{CLT}, \text{Enc Alg-ID, CLT-enc-alg}\}$$

5.7.4.5.4 Security Procedure:

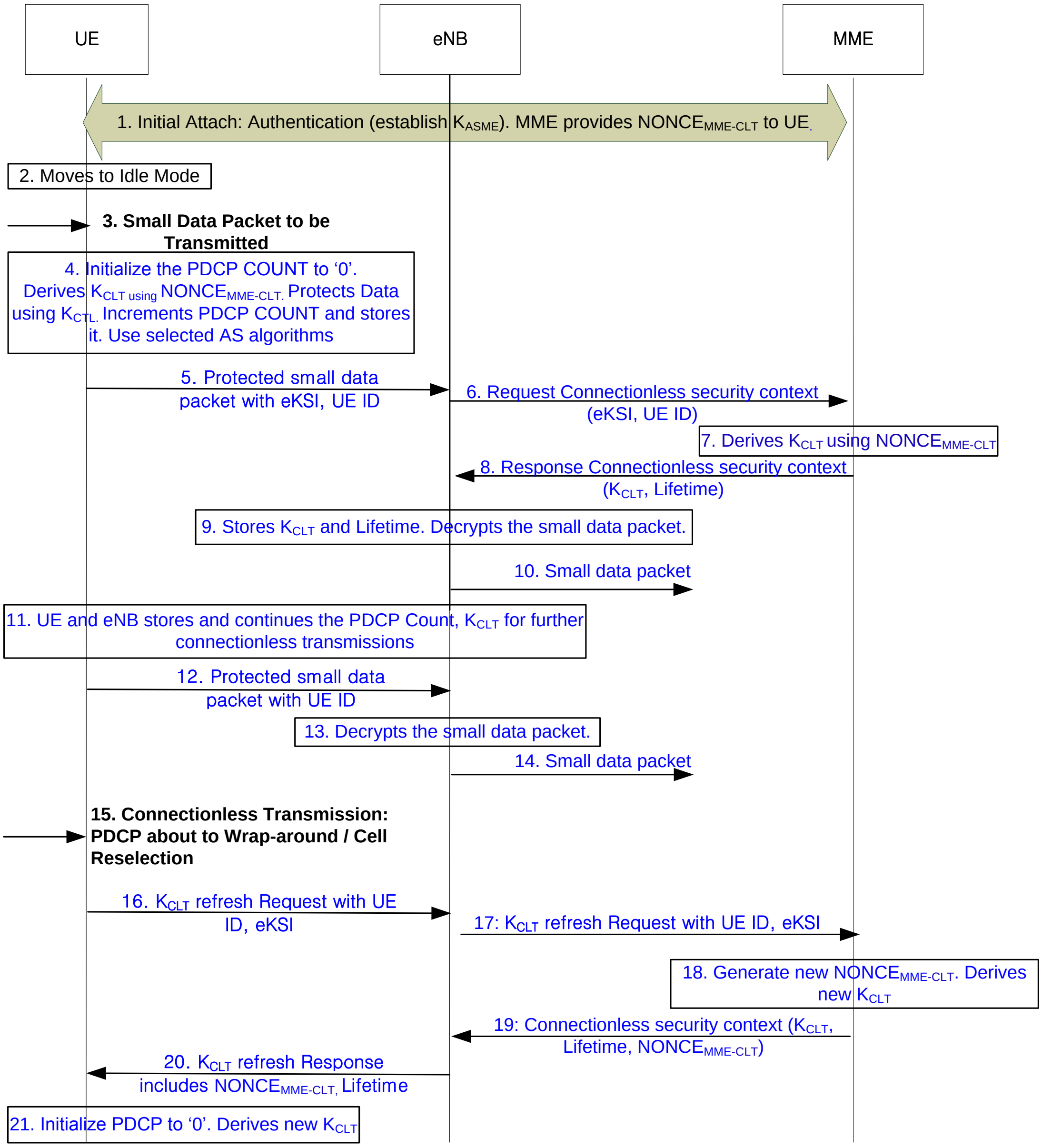

UE
eNB
MME
1. Initial Attach: Authentication (establish K_{ASME}). MME provides $NONCE_{MME-CLT}$ to UE.
2. Moves to Idle Mode
3. Small Data Packet to be Transmitted
4. Initialize the PDCP COUNT to '0'. Derives $K_{CLT\ using}$ $NONCE_{MME-CLT.}$ Protects Data using $K_{CTL.}$ Increments PDCP COUNT and stores it. Use selected AS algorithms
5. Protected small data packet with eKSI, UE ID
6. Request Connectionless security context (eKSI, UE ID)
7. Derives K_{CLT} using $NONCE_{MME-CLT}$
8. Response Connectionless security context (K_{CLT}, Lifetime)
9. Stores K_{CLT} and Lifetime. Decrypts the small data packet.
10. Small data packet
11. UE and eNB stores and continues the PDCP Count, K_{CLT} for further connectionless transmissions
12. Protected small data packet with UE ID
13. Decrypts the small data packet.
14. Small data packet
15. Connectionless Transmission: PDCP about to Wrap-around / Cell Reselection
16. K_{CLT} refresh Request with UE ID, eKSI
17: K_{CLT} refresh Request with UE ID, eKSI
18. Generate new $NONCE_{MME-CLT}$. Derives new K_{CLT}
19: Connectionless security context (K_{CLT}, Lifetime, $NONCE_{MME-CLT}$)
20. K_{CLT} refresh Response includes $NONCE_{MME-CLT,}$ Lifetime
21. Initialize PDCP to '0'. Derives new K_{CLT}

Fig.5.7.4.5.4-1 Connectionless Data Transmission Solution Using Separate Security Context

The following steps are performed as described in the signalling flow above:

1. The UE initiates an attach procedure with an MME and provides its security capability for connectionless data transmission protection to the MME. The MME optionally authenticates the UE and a K_{ASME} is established. The MME generates the $NONCE_{MME-CLT}$ and pass it to the UE. The $NONCE_{MME-CLT}$ and its lifetime is passed to the UE through the AS SMC procedure. The MME stores the $NONCE_{MME-CLT.}$

The MME use the $NONCE_{MME-CLT}$ only once and for every further request for $K_{CLT,}$ it will generate new $NONCE_{MME-CLT}$ to make K_{CLT} unique per request.

2. If there is no data to transmit, the UE moves in to idle mode.

3. When the UE is in idle, small data to be transmitted using connectionless data transmission, the following procedure is followed;

4. The UE derives the K_{CLT} using the $NONCE_{MME-CLT}$ and further keys for protecting the small data (as detailed in the above section 2.2.1). The UE sets the PDCP COUNT to '0" and protects the small data (encrypted and/or Integrity

protected). Small data protection is be provided by the PDCP layer. The cryptographic algorithms to be used with small data protection are the same, selected during AS SMC procedure initially.

5. After applying security, the UE transmits the protected (encrypted and/or Integrity protected) packet to the eNB. The first small data packet to the eNB carries eKSI as to ensure the key to be used are same. The small data packet includes UE-ID (S-TMSI).

6. If there is no valid keys for the UE in the eNB, the eNB request the MME for the key $K_{CLT.}$ The eNB includes the eKSI and the UE ID along with the request.

7. After receiving the request, the MME derives the Key K_{CLT}, as detailed in the above section 2.2.1.

8. The MME responds with the key K_{CLT} and its lifetime to the eNB.

9. The eNB stores the key $K_{CLT,}$ its life time and starts the timer. The eNB derives further keys to perform the security check (integrity check and/or decryption). The eNB remembers the cryptographic algorithms selected during AS SMC procedure initially. If needed eNB performs AS SMC procedure for the connectionless security context establishment.

10. After successful integrity verification and/or decryption, the eNB process the small data packet as detailed in the TR 23.887 (section 5.1.1.3.6.3) [26].

11 - 14. The UE and the eNB maintain the key K_{CLT} till its life time and continue the PDCP COUNT for small data transmissions.

15. If PDCP COUNT wrap-around about to happen or the UE performs cell reselection, the following procedure will be performed;

16. The UE request for K_{CLT} refresh. The refresh request includes the UE ID and eKSI.

17. After receiving the K_{CLT} refresh request, the eNB request the MME to refresh the keys.

18. The MME generates new $NONCE_{MME-CLT}$ and derives new $K_{CLT.}$

19. The MME passes the new $K_{CLT,}$ the $NONCE_{MME-CLT}$ and lifetime to the eNB.

20. The eNB stores the new key from the MME with validity time and further keys for protecting the small data. The eNB sends the $NONCE_{MME-CLT}$ to the UE. If needed eNB performs AS SMC procedure for the connectionless security context establishment.

21. After receiving the $NONCE_{MME-CLT}$, the UE derives the K_{CLT} and further keys for protecting the small data. The UE sets the PDCP COUNT to '0"

5.7.4.5.5 Switching from Connectionless to Connected mode

As described in section 5.7.4.2.7, the procedure is very similar to this solution also. The UE use the normal LTE AS security to protect any data sent over the normal user plane data radio bearer and only apply the new small data transfer protection if the small data is transmitted over the (otherwise unprotected) data radio bearer used for small data transfer.

When the switches appear (either decided by the UE or by the network), there needs to be an indication sent to the UE from the network or to the network from the UE, so that the UE, the eNB and the MME will know to re-configure itself for the new data radio bearer and switch to the other security context. Whenever the UE and the eNB switches, it will delete the existing keys.

5.7.6 Evaluation

5.7.6.1 General

Solution 3 "Standalone Small Data Service with T5/Tsp and generic NAS transport", solution 4 "Stateless Gateway for cost efficient transmission of infrequent or frequent small data", and solution 8 "Optimized Service Request procedure for UEs with a single bearer" in SA2 TR 23.887 [26] don't have security impact.

5.7.6.2 Connectionless Data Transmission Solution

For improved messaging efficiency the Connectionless data solution proposes the following changes in UE eNB and MME requirements.

Additional UE requirements:

- UE capable of operating in the Connectionless mode should be able to cache the security context with associated Token for each eNB/RNC with which it established security context since last AS authentication, and for which the Token is assigned. UE should also caches the Cell ID /RNC ID of the cell/RNC with which it has the connectionless context.
- UE should also be able to maintain validity of the cached context and its associated Token, including its lifetime for expiration and purging. The cached context should be maintained independent of the normal AS security context associated with the connection-oriented mode.
- Separation between AS security contexts for connectionless mode and connection oriented mode, and between multiple cached AS security contexts shared with different eNBs.

Additional eNB/RNC requirements:

- eNB/RNC capable of supporting Connectionless mode should be able to cache security context for each connectionless UE with which it established security context since last AS authentication.
- eNB/RNC should be able to assign and maintain a locally unique Token for each cached security context, and manage its validity including lifetime for expiration and purging.
- eNB/RNC should be able to recognize that the cached context already exists for the UE when UE requests the new context for the connectionless mode of operation.

Additional MME requirements:

- The MME should be able to deliver to the eNB the cookie representing the UE Identifier and a Token life time indicator when delivering the session-related AS security context to the eNB, in order to assist the eNB in recognition of the duplicate cached context, and deliver a subscription based indication for the eNB to allocate an application-specific Token lifetime.

To summarize, increased complexity of the UE, the eNB and the MME are expected. Caching of Connectionless contexts will consume memory resources at UE and eNB to provide current level of AS and NAS security. Token lifetime allocation sensitive to the application needs conserves any disproportionate consumption of resources.

5.7.6.3 MTC-IWF based Secure Solution for Small data transmission

5.7.6.3.0 General

The solution can be used for MT and MO small data transmission and trigger delivery. This section gives the solution benefits and impacts to existing system.

5.7.6.3.1 Benefits

The solution can provide security for SD and DT communication, even when there is no AS and NAS security context, meanwhile it can reduce the network signalling and offload NAS protocol.

This solution fulfils the following security requirements.

1. Small data and trigger protection: authentication, integrity and confidentiality
2. Small data and trigger protection in case AS and/or NAS security is not available

The MTC-IWF based solution has the following benefits compared to NAS security based solution.

- Prevent attacks from UE or SCS

The MME, when it comes to NAS security based small data transmission, does not have information about SCS, such that it cannot perform authorization on SCS and the SDs sent from SCS. For the same reason, MME has no knowledge whether the UE(s) are allowed to send SD to a given SCS, and may blindly forward the SD and waste network resource.

MTC-IWF based solution (5.7.4.4) performs authorization on both UE and SCS for SDT that can verify: 1) whether SCS is allowed to send SDT to the given UE; 2) whether the UE is allowed to send SDT to the given SCS; 3) whether there is a large number of SDT being sent by a UE or several UEs to a given SCS, this information can be used by MTC-IWF to inform MME or eNB to block the communication.

- Security when there is no pre-established NAS security

When there is no pre-established NAS security available, MME may discard or reject the SD or initiate establishment of NAS security. If MME discards or rejects the SD, the SD cannot be delivered to UE or SCS and affect the availability of MTC. To generate and negotiate NAS security will create more signaling and overload NAS protocol for only one SDT.

The MTC-IWF based solution can provide security protection for SD with the keys shared between UE and MTC-IWF, such that the SD can be transmitted securely in time, without invoke extra procedure and signalling.

- Reduce load to MME

MME and NAS protocol are not designed for MTC communication and service but the NAS security based solution requires MME to perform encryption, decryption, integrity protection and integrity check each time a SDT happens. Considering high traffic needs from SDT sending to and from MTC UEs, the load to MME and NAS protocol is heavy.

MTC-based solution is independent from NAS security protection thus it can reduce the processing load due to security on MME. The MME should only forward the SDT to and from MTC-IWF.

In exception case when IWF SMC is carried in the empty NAS SMC the NAS signalling will increase by one round-trip (SMC messages).

When terminating the security in the IWF without protecting and verification by the MME:

The security association established between UE and MTC-IWF is sufficient to protect the SDT, if UE can verify whether the MTC-IWF is a network trusted entity. Only the network authorized MTC-IWF can have the same Kasme that UE has, and can derive the same K_iwf and subkeys. Thus UE can verify that whether MTC-IWF is an authorized network element.

In MTC-IWF based solution, the MTC-IWF keys protected SDs are carried in NAS messages. MME has the information of whether the traffic is from/to a proper MTC-IWF: 1) MME has the mapping of UE and MTC-IWF, such that MME can ensure that the MTC communication does not go to an unexpected MTC-IWF. 2) MME carries IWF SMC in NAS SMC procedure, it can know whether IWF SMC is successful or not. This can prevent MME from forwarding SD without any protection, when NAS security is not available. When the NAS security context is activated, MME can perform protection and verification as in normal NAS security. Overload attack on MME is prevented as given in discussion of the first Editor's Note.

5.7.6.3.2 Impacts to existing system

The proposed solution requires support from HSS, MTC-IWF and UE It has the following impacts:

- New keys derivation at UE and HSS, new keys handling in UE and MTC-IWF.
- Needs an indicator of small data / trigger transmission to provide message type.
- Change to NAS protocol messages for AKA and SMC.

5.7.6.3.3 Open issues

The following issues are still open and should be studied in SA3.

- Details of key handling.

- Key management in UE mobility.

5.7.6.4 Security Solutions of Small Data Transfer in NAS PDU

- The security solution 1 provides necessary integrity and confidentiality protection for small data transfer in NAS PDU, and make optimization on signalling simultaneously.

- Lack of security context: Solution 1 can address this issue.

- When the solutions are applied, the consumption of NAS COUNT will be increased. But NAS security counter wraparound is not a problem because the normal NAS COUNT range is about [0, 2^{24}-1] mentioned in TS 33.401, section 9.2.2.2 [13].

Both solution 1 and solution 2 reuse the existing NAS layer security for protecting uplink small data packets in NAS PDU. For small data encryption, the additional requirement is the partial ciphering of the initial L3 message which is currently only integrity protected without encryption. Such partial ciphering solution has the following impacts on the UE and the MME.

Additional UE requirements:

- Set new value for “Security header type” IE and partially cipher initial L3 message

Additional MME requirements:

- Be able to identify whether the initial L3 message is ciphered or not, and partially decipher the initial L3 message

5.7.6.5 Security Solution of Small Data Fast Path in User Plane

- Security termination point issue (eNB vs S-GW): From security point of view, the terminating point can be in the eNB or in the S-GW.

- Additional threat: without RRC security, the threats (eavesdropping attack and modification attack) to the unprotected radio link identity and SGW Bearer Resource ID sent to the eNB are FFS.

- Additional UE requirements:

    - Support new security capability for small data fast path. This includes maintaining a small data security context for the lifetime of the fast path bearer that needs to be kept separate from any other security context.

    - Support new security protocol for small data fast path

- Additional SGW requirements:

    - Support security capability for small data fast path. This includes maintaining a small data security context for the lifetime of the fast path bearer in addition to the UE context that the S-GW needs to keep for the UE.

    - Support security protocol for small data fast path

- Additional MME requirements:

    - Negotiate with the UE the cryptographic algorithms to be used by the SGW

    - Derive small data security key(s) and send to the SGW together with the selected algorithms

    - Indicate the UE to derive small data security keys to be shared with the SGW

    - Refresh small data security key(s) for the SGW upon Kasme change

    - All the above MME-UE signalling can be piggy-backed on the corresponding NAS signalling for K_{ASME} management. The above MME-SGW signalling can be piggy-backed on existing GTPv2-C. Potentially new procedures need to be added to GTPv2-C.

The above can be summarized in the following bullets:

1. As already identified above, solution 6a adds a new security protocol which requires handling of new security functions in the UE and the SGW. Compared to a system without small data fast path (i.e., a pre-rel-12 system) this is an increase in complexity of security mechanisms. The complexity also includes the new interactions for changing between modes.

2. One example of the interaction scenarios is as such: If a UE with an enabled fast path bearer is firstly camped on a legacy eNB, the small data will have to be transferred in connected mode in a normal bearer, i.e. the small data is protected with normal AS security context. When the UE is handed over to a fast-path-enabled eNB, it is not clarified in TR 23.887 [26] whether the UE should keep transmitting small data in the existing normal bearer or the UE should activate the fast path bearer. Hence the un-clarity whether the normal AS security context or the fast path security context should be used. Once this is clarified in SA2, SA3 may make further analysis. The solution for small data defined in TR 23.887 [26] prescribes that small data PDN contexts are kept after creation during Attach procedure in the SGW and the UE as long as the fast path remains enabled. The PDN context contains a security context as a subset. Therefore the PDN context will become larger when security is added to the solution. It is under discussion whether that is a significant increase in size of the PDN context or not. Regardless if the fast path is active or not, this situation may result in unnecessary resource consumption in the SGW and the UE in the following two cases:

   - The procedure of "EPS bearers enabling for small data fast path" is actually transparent to the eNB. I.e. the HSS, the MME, the SGW and the UE need to have the supporting capability in order to enable the fast path bearer, but the capability of the eNB is not taken into account. It's further described in TR23.887 [26] that "*when bearers have been enabled for small data fast path in the UE, MME and SGW, and the current eNB does not support small data fast path, a fast path is never activated*". Therefore, in case where the UE is camped on a legacy eNB, the PDN contexts in the SGW and the UE which are already created at fast path enabling procedure will never be used because the fast path is never activated. Such resource consumption is particularly unnecessary for low mobility or stationary UEs camped on legacy eNBs which hardly get the chance to move to eNBs supporting fast path activation. A mechanism is needed for the network to avoid unnecessary resource consumption for security context.

   - Also the current solution described in TR 23.887 [26] provides no clear mechanism to disable the fast path bearer once enabled. I.e. there's no clear indication when to delete the security contexts in the SGW and the UE for fast path bearer. Although it can be assumed that fast path bearer can be implicitly disabled due to SGW relocation (e.g. new SGW Bearer Resource ID overwrites the old SGW Bearer Resource ID in the UE), such implicit disabling is hardly applicable to fast path bearers in low mobility or stationary UEs. The small data PDN contexts may unnecessarily occupy the resources in the UE and the SGW for a long time only for infrequent communication. The trade-off between saving the S1AP signalling between MME and eNB for setting up the UE context in the eNB at IDLE-CONNECTED transition, and storing PDN contexts in the SGW that may not be used, is under discussion.

5.7.6.6 Security Evaluation on Different Solutions of Small Data Optimization

Now both (5.7.6.4 and 5.7.6.5) types of security solutions can provide the integrity and confidentiality protection small data transmission.

However, the protection through fast path in user plane will have impact on security architecture and key hierarchy.

5.7.6.7 Overall Evaluation

In this section all different solutions for Small Data Transmission are compared from a security perspective. For convenience, the SA2 solutions are divided into three different groups.

All solutions that include small amounts of data sent using control plane NAS messages belong to the category "CP":

1: Small Data Transfer starting from RRC IDLE (E-UTRAN): Use of pre-established NAS security context to transfer the IP packet as NAS signalling without establishing RRC security

2:Optimised handling of C-plane connection for Small Data and Device Trigger

3:Standalone Small Data Service with T5/Tsp and generic NAS transport. MTC-IWF based Secure Solution for Small data transmission (clause 5.7.4.4) is a potential security solution for 3 being discussed in SA3.

Solutions proposing user plane transport in connectionless mode are combined in the "UP" category:

4: Stateless Gateway for cost efficient transmission of infrequent or frequent small data

6a: Small Data Fast Path

6b: Connectionless

Optimizations like data piggy-backing, combining of messages or re-using of existing security context are combined in the category "OPT":

5: Downlink small data transfer using RRC message

7: Service Request signalling reduction by RRC message combining

8: Optimized Service Request procedure for UEs with a single bearer

9: Lean Service Request Procedure

Note: SA2 informed (S3-130618/ S2-132327) that solutions 4, 5, 7 and 9 are dropped by SA2 from Rel-12.

Note: Solution 8 has been concluded with no security impact. Therefore, evaluation on category "OPT" is skipped.

Criteria for an overall evaluation contain the impact to existing elements (eNB, MME, SGW, and UE) from security point of view. Additional criterias are implications to service aspects like Lawful Interception (LI), Mobility aspects, restrictions on the usage (e.g. one radio bearer only), charging aspects, and the efficiency of the optimization. Although the evaluation in this TR is security related in general, important criterias for evaluation are the magnitude of chances to the existing security framework, security protocols, and key hierarchy.

Among solutions in category "CP", both solution 1 and solution 2 have security impacts on the UE and the MME for supporting the partly ciphering of initial L3 message. Also, the issue of whether or not the partial ciphering may violate the current NAS protocol layer security concepts is still un-clarified for solutions 1 and 2. Solution 3 has no new security function but may impose higher load on existing security functions.

Among solutions in category "UP", solution 4 has been dropped from Rel-12 as decided by SA2.

- Solution 6a as analyzed in 5.7.6.5 introduces new security functions in the UE, the SGW, the MME, and the eNB, and modifies the existing security framework (incl. deviation from the current EPS security architecture, new security protocol). It may also introduce the new threats leading to small data reaching the wrong destination.

- Solution 6b as analyzed in 5.7.6.2, comes at the expense of increased complexity in the UE, the eNB and the MME, as well as increased resource consumption due to the caching of AS security contexts and related tokens in UE and eNB.

6 General Security Requirement

Editor's note: Contributions to this section should be aligned with agreements achieved in the security requirements sub-clauses of individual Key Issues.

Network should be able to perform access control for UE accessing network, e.g., based on MTC feature and/or subscription type.

Editor's Note: The meaning of "access control" (only authorization or authentication and authorization) need to be clarified.

7 Conclusions

Editor's Note:This section is intended to list conclusions that have been agreed during the course of the work item activities.

7.1 Rel-11 Conclusions

In the SA3#67 meeting, SA3 agreed on the following security aspects for Rel-11 and the normative text for Rel-11 SIMTC features were included in the SA2 TS 23.682 [23]:

- Security requirements for Tsp Reference Point and MTC-IWF (section 4.8 in TS 23.682 [23])
- Security procedures for Tsp Interface Security and Network based solution for filtering SMS-delivered device trigger messages (section 5.4 in TS 23.682 [23]).

8 Impacts to normative specifications

Editor's Note:This section is intended to capture the impacts to normative specifications within the responsibility of SA3. It can be used as a placeholder to document agreements until a set of normative CRs can be generated for the selected solutions(s).

8.1 General

Annex A: Key Issues and Solutions deferred from Rel-12

A.1 Time controlled

A.1.1 Issue Details

Time controlled is one of the MTC features. The point of this feature aims at how to restrict UE’s access to the network and avoid unnecessary network load outside these pre-defined time periods. Three terminologies are used in this feature, i.e. grant time interval, forbidden time interval, communication window. The home network operator may restrict altering the time period e.g. to avoid traffic when the MTC server is in maintenance by means of a 'forbidden time interval'. Typically, an MTC User agrees with an operator on a predefined time period for a group of UEs. The time in which access is permitted is termed a 'grant time interval.' For many applications, individual UEs do not need the total duration of this predefined time period to communicate with the MTC Server. Typically a 5-10 minutes 'communication window' is sufficient for an individual UE.

A.1.2 Threats

There are several solutions in TR 23.888 [10] to handle this feature. These so-called time interval and time window can be defined/randomized by both UE and MTC server in TR 23.888 [10] solutions. There exist security threats if the intervals and time window are sent to UE without any protection. The attackers can change time interval/window to limit or extend the time. UE will not have enough time to finish the job when time interval/window is limited. The UE will extend online time to do its job repeatedly and waste its power and thus it will cause network congestion when time interval/window is tampered to extend. Moreover, MTC users may be charged more according to TR 23.888 [10] when UE exchanges signalling or sends and receives data outside of defined time intervals.

A.1.3 Security requirements

Time interval and communication window should be integrity-protected when sent to UE.

Editor's Note: It is ffs if other protection (e.g. confidentiality) is required.

A.1.4 Solutions

With regard to different scenarios of inform messages in solutions of TR 23.888 [10], current mechanisms can be used to solve the issue:

NAS protection

Time interval and communication window can be sent in the NAS to inform the UE of the length of interval/window. After NAS SMC, security is setup for protection. All NAS signalling messages should be integrity-protected according to TS 33.401 [13], and therefore current LTE mechanisms ensure that the time interval/window can not be tampered. For GSM and UMTS, SA2 has not defined any solutions yet. But the time interval/window should be protected in this case as well.

Editor's Note: It is FFS how to protect time interval/window in GSM/UMTS when SA2 figures out GSM/UMTS solutions for time controlled feature.

Application level protection

Another potential solution is that time interval/window is sent by MTC server via application level data. Current mechanism, e.g. GBA push which is defined in TS 33.223 [22], can be used to protect the data sent from MTC server. Or some application security mechanism can also be used. However, these solutions are out of 3GPP scope.

Editor's Note: It is FFS whether there is any other solution for this feature- time controlled.

A.1.5 Evaluation

Editor's note: This section contains evaluation (possibly including cost and benefit trade-off analysis) of candidate solutions enumerated in the preceding General Description subsections.

A.2 Low Mobility

A.2.1 Issue Details

Low mobility UEs do not move, move infrequently, or move only within a certain region as defined in TS 22.368 [9] and TR 23.888 [10].

Service requirements of low mobility UEs are described in clause 7.2.1 of TS 22.368 [9] as follows:

"- The home network operator should be able to change the frequency of mobility management procedures or simplify mobility management per MTC Devices.

- The network operator should be able to define the frequency of location updates performed by the MTC Device."

When the UE moves, there is a solution in TR 23.888 [10] that "the SGSN/MME detects the moving and pages within the new area which is reported by RAN or by the MTC Device explicitly."

A.2.2 Threats

Threat 1: There can be security risks if the incorrect location information is reported to the network.

A.3 Security of UE Configuration

A.3.1 Issues Details

Different UEs configuration options were introduced in stage 2 to avoid/alleviate congestion and overload in the network, in particular to control the network access from low priority UEs (i.e. delay tolerant).

There are two potential approaches for delivering the configuration commands to the UEs.

One approach is using OMA device management (OMA DM) and the other is using UICC OTA (as specified in ETSI TS 102 225 [17] / TS 102 226 [18] and 3GPP TS 31.115 [19] / TS 31.116 [20]). The OMA DM approach only applies to the terminal part of the UE (ME). Respectively, UICC OTA is applied to UICC part of the UE.

A.3.2 Threats

Editor's Note: Further contributions are needed to identify the threats.

Without security protection, the configuration options will face MitM attack when it's provisioned to the UEs.

A.3.3 Security Requirements

OMA DM case

TS 24.368 (V1.0.1) [5] has defined the Management Object (MO) and possible leaf objects to represent the UEs configuration options. They should be stored securely in the UEs. In case of configuration options stored in the MTC ME:

The DM server should be authenticated by the MEs.

The MEs may be authenticated by the DM server.

OMA DM messages should be integrity-protected.

UICC OTA case

There are different security levels for OTA message protection. In the scope of the configuration of UICC in UE:

- The OTA server should be authenticated by the UICC.
- The UICC may be authenticated by the OTA server.
- UICC OTA messages should be integrity-protected.
- UICC OTA messages should be confidentiality -protected.

Editor's Note: It is FFS whether secure channel is needed to convey configuration info from UICC to the MTC ME.

A.3.4 Solutions

Editor's Note: Further contributions are needed.

A.3.4.1 ME Configuration

OMA DM security, as specified in [7] and [8], contains a number of options, where some are not needed for the purposes of this document and others are required. OMA DM security is therefore profiled in this clause as:

- The UEs should have a root certificate to authenticate the DM server.
- The root certificate needs to be provided to the UEs in a secure manner.
- The root certificate should be securely stored.

Editor's Note: It is FFS how to securely store the certificate

- The DM server and the UEs should support and use TLS according to the profile specified in Annex E of TS 33.310 [6].

To verify the validation of the DM service certificate one can consider either OCSP or the use of a secure real time clock in the UE for expiry checking of the DM server certificate. The choice of which one to be used by the UE may depend on the usage characteristics (e.g. how often checking occurs). If a secure real time clock in the UE is used, then the DM server certificate shall have a short validity time in order to be refreshed in time. If the DM server certificate has expired but has not been revoked, the OCSP server will not reply with certificate verification failure. Possible ways to overcome this are that expired DM server certificates are also revoked or that the UE sends a nonce to the OCSP server who then replies with correct time and the UE can make the certificate verification itself.

Note: For devices identified as requiring additional security, the use of secure real time clock may be provided by means of a secured environment logically defined within the UE. Such a secured environment should protect the real time clock from external attacks and tampering, and may additionally be utilized for secure storage of the DM server certificate.

Editor’s Note: The cost of implementing secure environment should be considered

Editor’s Note: The secure real time clock is FFS.

Editor’s Note: it is FFS how short is sufficiently short for the DM certificate validity duration.

A.3.4.2 UICC Configuration

UICC OTA is specified in ETSI TS 102 225 [17] / TS 102 226 [18] and 3GPP TS 31.115 [19] / TS 31.116 [20].

In the scope of MTC configuration the security requirements are met using SPI configuration for secured packets transmission, as described in 3GPP TS 31.115 [19] referencing ETSI 102 225 [17], or using PSK-TLS as described in 3GPP TS 31.116 [20] referencing ETSI 102 225 [17] for secured messages based on HTTPS.

A.3.5 Evaluation

Editor's note: This section contains evaluation (possibly including cost and benefit trade-off analysis) of candidate solutions enumerated in the preceding General Description subsections.

A.4 Reject message without integrity protection

A.4.1 Issue Details

In the overload situation, the MM/GMM/EMM reject cause values such as "IMSI unknown in HLR"; "illegal ME"; and "PLMN not allowed" could be wrongly sent "in panic" by an overloaded (V)PLMN.

It's unrealistic for SGSN/MME to get authentication vector from the HSS, perform a successful AKA with the UE, then perform the security mode command procedure for integrity protection and encryption. So the MM/GMM/EMM Reject message will be sent to the UE without with integrity protection.

A.4.2 Threats

If the Reject message is sent without integrity protected, any false base station can fake the MM/GMM/EMM reject cause values such as "IMSI unknown in HLR", "illegal ME", or "PLMN not allowed" in the Reject message as a denial of service attack to the UEs and the network.

A.4.3 Security Requirements

A security mechanism is needed to prevent the DoS attack.

A.5 Congestion Control

A.5.1 Issue Details

In order to combat signalling congestion, network nodes should be able to reject or prevent attach or connection requests. The challenge is to block the traffic of the particular UE(s) used for MTC that is causing the congestion, without restricting non-MTC traffic or traffic from other UEs that are not causing a problem. SA2 has designed several solutions for it. The aim of these solutions is when the network finds that the UE used for MTC that will cause congestion or the UE is a low priority UE, it will reject the connection request. So the UE can use e.g. a low access priority indicator or delay tolerant access.

A.5.2 Threats

When requesting access to the mobile network, a UE should provide its currently enabled indicators to the network. There exist security threats if the indicators are sent without any protection. The attackers can tamper with the low access priority indicators or delay tolerant access to the normal state to let many UEs connect when the network setup congestion control mechanism. The problem is serious since nowadays congestion is the most urgent issue that operators face. Vice versa, if an attacker adds a fake low access priority indicator or delay tolerant access in the request sent by normal UEs, the service of normal UEs (esp. some VIP users) will be maliciously degraded.

A.5.3 Security requirements

The low access priority indicator should be integrity-protected according to the rules in TS 33.102 [12], TS 33.401 [13], TS 23.060[3] and TS 23.401[4].

A.5.4 Solutions

CN mechanism for congestion control:

If the UE has valid security context, then the Attach Request and LAU/RAU/TAU request should be integrity protected.

However, attach request and TAU request can not be protected, when the UE does not have a valid security context, e.g. when UE connects to the network for the first time.

In UMTS case, initial L3 messages could not be integrity protected since they are sent before security on air interface is activated. Attach Request and LAU/RAU request could not be integrity protected if they are sent as initial L3 messages.

In GSM/GPRS case, integrity protection is not provided. Attach Request and LAU/RAU request could not be integrity protected. In addition, Attach Request and LAU/RAU request could not be ciphered either if they are sent as initial L3 messages.

Editor’s Note: In case that Attach Request and LAU/RAU/TAU request could not be protected by the current mechanism, security solutions for congestion control are FFS.

RAN mechanism for congestion control:

In UMTS/LTE case, RRC connection request is sent via SRB0 before security activated. Neither integrity protection nor ciphering applies for SRB0. In GSM/GPRS case, integrity protection is not provided. The “delay tolerant access” in the RRC connection request can not be integrity protected.

Also when the network rejects the RRC connection request (due to overload condition), the RRC connection reject message which carries extended wait timer is neither integrity protection nor ciphered.

A.5.5 Evaluation

Editor's note: This section contains evaluation (possibly including cost and benefit trade-off analysis) of candidate solutions enumerated in the preceding General Description subsections.

A.6 Group Based Feature

A.6.1 Issue Details

SA2 is currently working on group based feature which includes the following key issues: Group based Messaging, Group based Charging Optimizations, Group based Policy Control and Group based Addressing and Identifiers. SA2 is currently considering mechanism to distribute a group message from an SCS to those members of an MTC group located in a particular geographic area [26]. According to the current architecture and solutions, MTC-IWF receives a group message from SCS and forwards it to the target group of UEs.

As group based messaging can significantly reduce the overhead of network resource, it may be required to protect the group messages.

For the UEs in one group, each may need to communicate with the network individually so an independent session key for each device may be needed.

Editor's Note: Individual session key establishment per UE in the group need to be considered and studied further.

For the UEs in one group, the network may need to distribute the same message (e.g. a trigger request) to those members of one MTC group so a same group session key may be needed.

Editor’s Note: The same MTC group session key establishment for all UEs in the group need to be considered and studied further.

A.6.2 Threats

If the broadcast message for a particular group is not protected, then private information related to particular group are revealed. Therefore a mechanism should be provided to protect the confidentiality of the group message broadcasted for a particular group. However confidentiality protection is subject to regional regulatory requirements.

Group based messaging would be more prone to tampering and fake triggering attacks, if there is no integrity and replay protection provided by the core network or by the SCS.

With a group message multiple UEs can be triggered. Therefore an unauthorized group message may cause much more severe problem compared to what a trigger to a single UE can cause. Other threats like MitM attack which were considered for non-group message also apply here with amplified effect.

A.6.3 Security Requirements

A MTC Group is a group of UEs that can be in the same area and/or have the same MTC Features attributed and/or belong to the same MTC user. MTC Group should be identified uniquely across 3GPP networks.

> Editor Notes: It should be studied further, to what extent group based protection and management can be used to save network resource and improve efficiency.

There should be a mechanism by which an UE can be verified as a legitimate member of an MTC Group.

Requirements on group based messaging

- MTC-IWF should verify if the SCS is authorized to send group message to a given MTC group.
- Network should be able to distinguish group message from other messages.
- Group message that are distributed to the group of UEs should be integrity protected, replay protected and may be confidentiality protected.
- Local Group ID should not to be exposed to an entity that is located outside of 3GPP network. This includes the SCS which is outside of 3GPP network as well.

A.6.4 Solutions

A.6.4.1 Solution 1: Application layer based protection

Security protection applied at MTC application layer is a straightforward solution. However, the network should trust the SCS and assure/ensure that SCS protects the group message and MTC application in the UE verifies it. In case, if the security is not applied in the application layer, then there can be attacks on the network.

SCS should apply encryption, signature and replay protection to the group message. The MTC application on the UE should verify the source of the group message and ensure the integrity of the received group message. The mechanism to verify the integrity of the group message, encryption/decryption and replay protection by the MTC application layer is out of scope of this specification.

The UE should discard the group message if it is not signed and replay protected by the SCS.

> Editor’s Note: It is ffs, whether key management for application layer based protection is within scope of 3GPP.

A.6.4.2 Solution 2: Network based protection for cell broadcast

In network based protection, MTC-IWF generates the keys for group message protection and protects the group message. The figure below shows the message sequence and describes the mechanism for EPS.

> Editor's Note: The below solution is intended for LTE, it is FFS on applicability of this solution in GSM/UMTS.

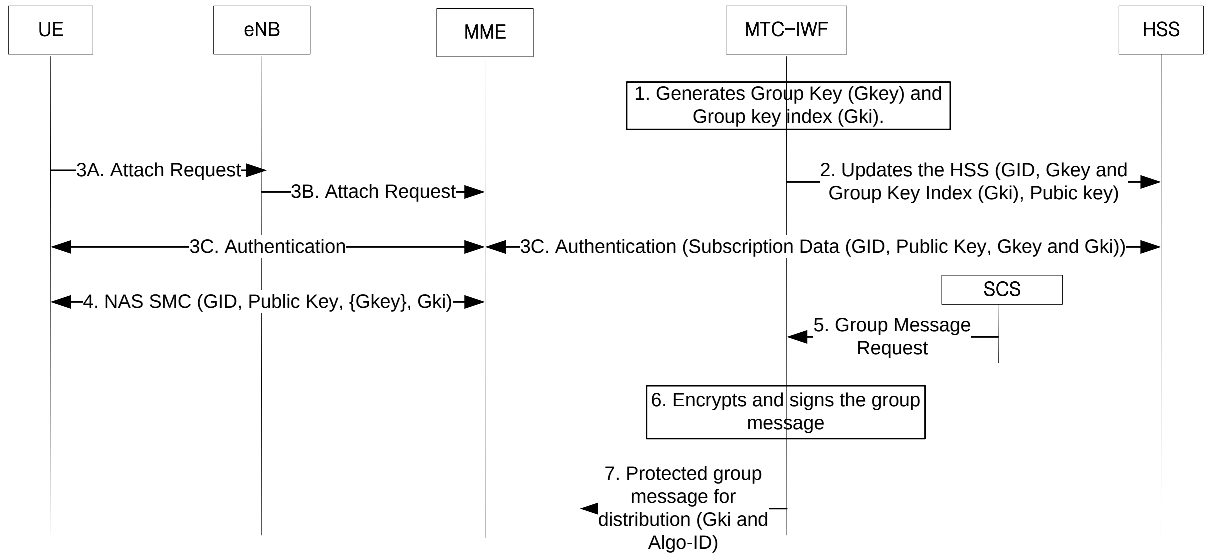

UE
eNB
MME
MTC-IWF
HSS
1. Generates Group Key (Gkey) and Group key index (Gki).
3A. Attach Request
3B. Attach Request
2. Updates the HSS (GID, Gkey and Group Key Index (Gki), Pubic key)
3C. Authentication
3C. Authentication (Subscription Data (GID, Public Key, Gkey and Gki))
SCS
4. NAS SMC (GID, Public Key, {Gkey}, Gki)
5. Group Message Request
6. Encrypts and signs the group message
7. Protected group message for distribution (Gki and Algo-ID)

Fig. 5.7.4.2-1: Network based protection for cell broadcast

1. The MTC-IWF creates the group and generates the group encryption key for encrypting the group message. MTC-IWF uses the PKI infrastructure for signing the group message and symmetric key (Gkey) is used for encryption/decryption of the group messages.

Editor’s Note: Need to check with SA2 for the specific node in the 3GPP network responsible for group formation. Based on the SA2 decisions, other suitable network elements for group key generation and key management are FFS.

2. The MTC-IWF updates the HSS with the public key and the encryption key for a particular group with the Group ID. The HSS maintain/maps the group based feature subscription details along with the UE subscription data.

3. During individual authentication, the MME fetches subscription data from the HSS. If the UE is subscribed for group based feature, then the subscription data contains the group based feature information (GID, encryption key, public key and the key index).

4. After successful authentication, the MME passes the group keys to the UE. The MME protects the keys using the NAS security context.

Editor’s Note: Further study may be required on the possibility of using dedicated NAS message for group key distribution. Also further study is required on whether the NAS message carrying the group key requires partial encryption for protecting the group keys.

5. When the SCS wants to send the group message, it provides the group message over Tsp interface.

6. The MTC-IWF protects the group message based on the Group ID received from SCS or from the HSS.

7. The MTC-IWF sends the protected group messages to the selected CBC. The protected group message includes the key ID and also algorithm ID used for protection.

Editor’s Note： Mechanisms for signature algorithm selection is FFS.

A.6.4.3 Solution 3: MBMS based method

MBMS security can provide shared key for data transferring. So it can be used to protect the group message transferred from one MTC application server/MTC SCS to multiple UEs in the group when the UEs use shared secret keys for transferring.

Otherwise, when all UEs in one group need to be authenticated together, or UE wants to communicate with MTC application server/MTC SCS/network individually, or UEs wants to send uplink data, the current MBMS security solution can’t be applied.

A.6.4.4 Solution 4: Authentication of UEs of a group

There are two options to authenticate UEs of a group. One option is that network performs two steps authentication: the first is to identify the individual UE and the second is to associate this UE as a member of MTC group. The other option is that network authenticates all related UE in a group together at the same time, by which the authentication solution can be called as group authentication. If such group authentication is used, it can save network resource to combine the two steps into one step.

Editor Note: whether or not group authentication can save network resource is ffs.

A.6.5 Evaluation

Editor Note: it is ffs to see if there are any security threats on the group authentication.

Editor Note: How to achieve a balance between network resource saving and solution complexity is FFS.

A.7 Monitoring

A.7.1 Issue Details

As discussed in TR 23.888 (clause 5.10.1) [10], UEs may be deployed in locations with high risk, e.g. possibility of theft of the communication module. There are UEs that should not move from an authorized location, or should only move in an authorized area. For those UEs, it is desirable that the network detects and reports events (including location) caused by those devices that may result, for example, from theft of the communication module. If such an event is detected, the network might be configured to perform special actions. There are UEs that can move in a widely open area without restriction (e.g. UEs that are used to track cargo, animals, vehicle, etc.).

A.7.2 Threats

In the case of an MTC application where the UE should not move from an authorized location, or should only move in an authorized area (e.g. within a home), there could be security risks if the device is operated from an unauthorized location (e.g. as a result of theft of the communication module). For example, a water metering used in user A's home to record user A's water usage should be fixed in user A's home. If it is moved to another place like B's home without permission, it could potentially be used to report user B's water usage against user A's account. The primary method to mitigate this attack should be to bind the identity and authentication of the UE to the specific user's water meter. Detecting or preventing a change in location of the UE could be a useful secondary security mechanism.

Another example is fire monitor in the building. When a fire monitor is moved to another place, wrong location information will be sent to the fire monitoring server if there is a fire. In this case detecting change of the location of the UE would be a useful feature.

For mobile UEs used for tracking purposes, the mobile area is not limited for mobile UEs, the network can not verify if the UE is stolen or controlled by attackers just by comparing the location identifier of UE and the pre-defined location identifier stored in the network. As a result, the stolen vehicle monitor of A may be used for B, or attackers with stolen UE can report a wrong location identifier to the network, or attackers can use UE to trace other peoples ' positions, etc.

For those UEs that can be linked to an individual, MTC Monitoring could cause an invasion of privacy. In particularly, if MTC Monitoring is applied to UEs that should not be monitored.

A.7.3 Security Requirements

It is required for the network to provide a location management mechanism for UEs that should not move from an authorized location, or should only move in an authorized area to detect if the device has been moved to an unauthorized location.

The network should be able to distinguish between UEs that have restriction in movement and those that do not have restriction and manage their mobility accordingly, i.e., where they can be used and cannot be used.

The network should be able to prevent MTC monitoring to be activated for those devices that should or are not monitored by the network.

A.7.4 Solutions

A.7.4.1 Location Management

A.7.4.1.0 General

The requirement mentioned in clause 5.6.3 of this document, can be met as follows.

UE reports the location identifiers. Network entity (e.g. SGSN/MME) should store the pre-defined location identifier and be able to verify the location identifier by comparing these two identifiers.

When the UE moves; a network entity (e.g. MSC/SGSN/MME) receives new location information which is reported by RAN or by the UE explicitly and detects if it is different from pre-configured location information. Then the network entity can confirm that the UE has moved to other area and will send a warning message to the MTC server, which can then take further action.

Editor's Note: Multiple solutions are being considered in SA2 about which network entity detects and reports unauthorized movements.

Editor's Note: Granularity of above mentioned location identifiers and the resulting impact on the ability of the solutions to meet the requirements, as well as possible other solutions (e.g., solutions relying on network reporting) are ffs.

A.7.4.1.1 Impacts on existing nodes or functionality

A network entity should be able to store the pre-configured location information of UE with low mobility feature.

A network entity should be able to send warning to MTC server that UE is not in the authorized location/area.

A.7.5 Evaluation

Editor's note: This section contains evaluation (possibly including cost and benefit trade-off analysis) of candidate solutions enumerated in the preceding General Description subsections.

Annex <X>: Change history

It is usual to include an annex (usually the final annex of the document) for reports under TSG change control which details the change history of the report using a table as follows:

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2010-11					*Converted from living document (S3-101398)*	*-*	*0.1.0*
2011-01					*Addition of S3-110150, S3-110057, S3-110110, S3-110200, S3-110151 with the changed discussed during SA3#62*	*0.1.0*	*0.2.0*
2011-04					*Addition of contributions agreed in SA3#63 meeting*	*0.2.0*	*0.3.0*
2011-05					*General clean-up done by MCC editing department*	*0.3.0*	*0.3.1*
2011-07					*Restructured the TR based on Rel-11 Building Blocks (SP-110218/S3-110343). Incorporated suggestions from MCC editing department. Introduced Annex – A.*	*0.3.1*	*0.4.0*
2011-07					*Addition of contributions agreed in SA3#64 meeting*	*0.4.0*	*0.5.0*
2011-11					*Addition of contributions agreed in SA3#65 meeting*	*0.5.0*	*0.6.0*
2012-02					*Addition of contributions agreed in SA3#66 meeting*	*0.6.0*	*0.7.0*
2012-05					*Addition of contributions agreed in SA3#67 meeting*	*0.7.0*	*0.8.0*
2012-07					*Addition of contributions agreed in SA3#68 meeting*	*0.8.0*	*0.9.0*

2012-08					*Structural Changes. Changed “MTC device” to “UE” in appropriate places*	*0.9.0*	*0.10.0*
2012-11					*Addition of contributions agreed in SA3#69 meeting*	*0.10.0*	*0.11.0*
2013-01					*Addition of contributions agreed in SA3#70 meeting*	*0.11.0*	*0.12.0*
2013-04					*Addition of contributions agreed in SA3#71 meeting*	*0.12.0*	*0.13.0*
2013-07					*Addition of contributions agreed in SA3#72 meeting*	*0.13.0*	*0.14.0*
2013-09					*Inclusion of contents based on S3-130740 and S3-130749 (e-mail approval)*	*0.14.0*	*0.15.0*