3GPP TR 33.8de V0.0.1 (2012-06)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Security aspects of Public Warning System (PWS);

(Release 12)

Keywords

<keyword[, keyword]>

MCC selects keywords from stock list.

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.

Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

1 Scope

This clause shall start on a new page.

The present document …

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 22.268: "Public Warning System (PWS) requirements".

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

[4] 3GPP TS 23.041: "Technical realization of Cell Broadcast Service (CBS)"

[5] 3GPP TS 48.049: "Base Station Controller - Cell Broadcast Centre (BSC-CBC) interface specification; Cell Broadcast Service Protocol (CBSP)".

[6] 3GPP TS 25.419: "UTRAN Iu-BC interface: Service Area Broadcast Protocol (SABP)".

[7] 3GPP TS 23.251: "Network sharing; Architecture and functional description".

[8] 3GPP TS 22.268: "Public Warning System (PWS) requirements".

3 Definitions, symbols and abbreviations

Delete from the above heading those words which are not applicable.

Clause numbering depends on applicability and should be renumbered accordingly.

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].

Definition format (Normal)

<defined term>: *<definition>.*

example: text used to clarify abstract rules by applying them literally.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Symbol format (EW)

<symbol> <Explanation>

3.3 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].

Abbreviation format (EW)

<ACRONYM> <Explanation>

4 Security requirements of PWS

Editor's Note: This section aims to add the updated security requirements of PWS, including roaming case.

Security requirements for PWS identified by SA1 in section 4.8 of TS 22.268 [2] are as follows:

- PWS shall only broadcast Warning Notifications that come from an authenticated and authorized source.
- The integrity of the Warning Notification shall be ensured.
- The PWS protect against false Warning Notification messages.

NOTE: These requirements are subject to regulatory policies.

- The authentication of the Warning Notification Providers is outside the scope of 3GPP Specifications.

Additional requirements identified by SA3 are as follows:

- For UE that are enabled to receive Warning Notifications from the VPLMN in roaming areas, it shall meet these security requirements listed above.
- The authentication solution should be robust against errors in the key distribution and overload so that genuine (potentially lifesaving) messages do not get rejected due to some error or overload in the network or in the authentication mechanism itself.
- A serving network should periodically send test warning messages on the broadcast channel.
- If the UE has not been configured for PWS message security, PWS warning messages shall always be displayed to the receiving end user.
- Whether the PWS message has been properly authenticated or not should be invisible to the receiving end user except in the case when an authentication failure in a primary notification implies that an already displayed paging notification shall be rejected.
- It shall be possible to configure whether or not primary notifications are displayed.

Additional SA3 working assumptions are as follows:

- The working assumption is that the signing entity is on a national level.

5 System and security architecture of PWS

Editor's Note: This section aims to give an overall description of security aspects of PWS.

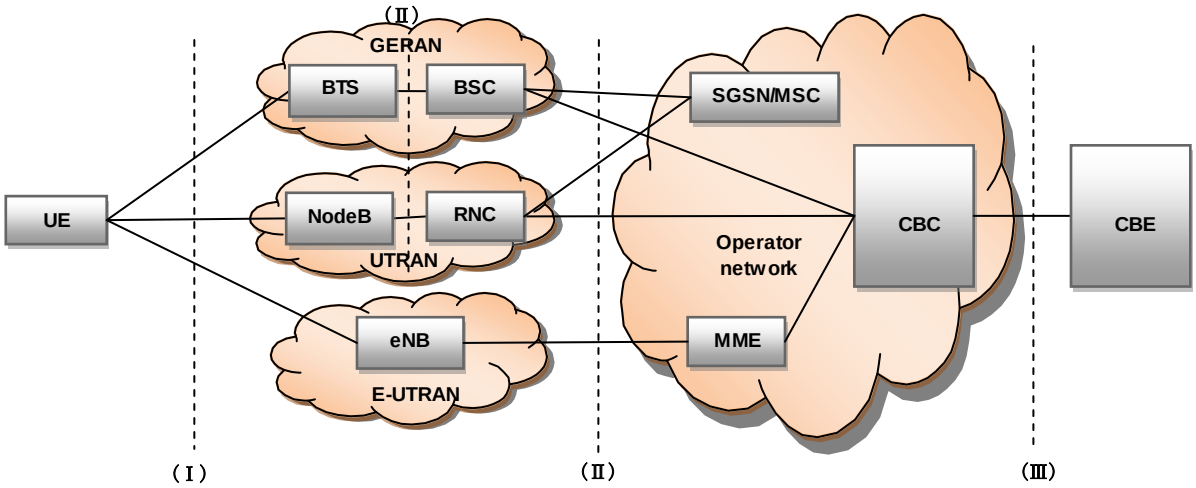


Figure 5.1: PWS system architecture overview

Figure 5.1 gives an overview of the complete security architecture.

- Air interface between UE and access network needs security protection as PWS Warning notification messages are broadcast to UE via SYSTEM INFORMATION.
- CBC is part of the core network and connects to the network node. For GERAN, CBC connects with the access network entity BSC; For UTRAN, CBC connects with the access network entity RNC; For E-UTRAN, CBC connects with the core network entity MME. The protocols between the CBC and these network nodes are defined in 3GPP TS 48.049 [5], TS 25.419 [6] and TS 23.401 [3].
- CBE is outside of the scope of the 3GPP network. It is assumed that the CBE is responsible for all aspects of formatting CBS, including the splitting of a CBS message into a number of pages.
- SGSN or MME can be used to deliver PWS keys to UEs.
- A UE in limited service state is not required to receive, process, and display warning messages.

NOTE: The assumption above has been verified by SA WG1 for the REL-11 timeframe and may have to be reconsidered in later releases.

Editor's Note: It needs to add security architecture of PWS.

Editor's Note: The security solution should minimize the impact to the current mechanism

Editor's Note: SGSN may receive PWS keys from CBC, or PWS keys are configured in SGSN directly. It is for FFS how SGSN gets the PWS keys, and whether the interface between SGSN and CBC should be added.

6 Security features of PWS

Editor's Note: This section aims to give which security features should be done for PWS.

6.1 PWS threats and analysis

6.1.1 General

It needs to protect against attacks that are in the interface between PLMN and the Warning Notification provider. However, it is outside scope of 3GPP. The attacks which are within the wired network can effectively be dealt with NDS methods. So the most crucial threat is the one over air interface.

For PWS Warning Notification messages, the security threats are similar with ETWS. There may be spoofing attacks, e.g. an attacker may forge and issue PWS Warning Notifications maliciously. The messages sent over the air may introduce spoofing attacks. Another threat may be tamper attacks, e.g. an attacker may record and tamper a PWS Warning Notification message over the air interface.

RAN2 has decided to broadcast PWS Warning Notifications to user via SYSTEM INFORMATION over air interface. However, broadcasts of SYSTEM INFORMATION are not protected. If an attacker can imitate the base station behaviour maliciously and broadcast false PWS Warning Notifications or tamper PWS Warning Notifications coming from CBE, it will cause serious panic among the population.

In order to guarantee the authenticity and integrity of the Warning Notifications, the security requirements which specified in 3GPP TS 22.268 [8] are introduced. In order to meet these security requirements, it has been decided that PWS Warning Notifications shall be protected with signature and timestamp that are included in the Warning-Security-Information IE in the WRITE-REPLACE Request message. Moreover, some PWS security features should be considered and defined in details as to solve the remained security issues listed.

6.1.2 Location of node protecting the key delivery in PWS

The placement of the node that protects the delivery of the key is an important consideration in the security for PWS. For E-UTRAN and GERAN PS, it is possible to protect the PWS key delivery from the core network node to the UE using legacy security mechanism, while in UMTS and GERAN CS the protection can only be applied from RAN nodes. These RAN nodes (e.g. collapsed Node Bs or HNB in UMTS) may be deployed in location that are at the edge of the network and hence not be in the most secure locations. As a result of this they are significantly more vulnerable to attack than core network nodes.

Suppose that the node is towards the edge of the network is used to protect the delivery of the PWS key to the mobile. Then the compromise of such a node would allow the attacker to send false keys to all the users that are attached to that node. It would be enough to break the secure tunnel between this node and the operator's network by getting the relevant key out of the compromised node. Then a man-in-the-middle could be inserted between the compromised node and the core network that modifies the signalling to send a known PWS key to the users. It would be then easy to fake a warning message that all the users under that node would believe is genuine. A more sophisticated attack would be to use a compromised network element, for example an open HNB, to get keying material in order to establish to establish a false base station from which to launch an attack. If such attacks are deployed at places where large crowds gather, then it could be possible to make a large number of people incorrectly receive a warning message simultaneously

6.2 Security features of PWS

6.2.1 General

A UE that has the capability to receive PWS message shall support PWS interface as specified in TS 23.401 [3] and TS 23.041 [4]. CBE sends Warning Notifications to the user via core network points and the access network points. When receiving PWS Warning Notifications, the user verifies the signature with the corresponding key and the algorithm. So it is essential that the user shall be notified which key should be for signature verification and algorithm should be used. Otherwise, it will cause verification failure.

As mentioned above, it shall ensure the synchronization of signature key and the signature algorithm between UE and the network. In the current specification, it only states PWS Warning Notifications shall be protected and it has been decided that PWS Warning Notifications are broadcasted to UE via SIB10, SIB11 and SIB12 for ETWS and CMAS. How to verify PWS message has not been specified when PWS Warning Notification messages are integrity protected. Additionally, in the Warning-Security-Information field, the length of signature is only 43 bytes. If PWS uses some popular signature algorithm, e.g. RSA (the length of the message signature is at least 1024 bits) it cannot meet the

maximum length. So it should be considered as the length of signature in particular. In summary, it is essential to ensure that which digital signature algorithms should be used for PWS Warning Notifications protection. So several security features should be considered for PWS security as follows.

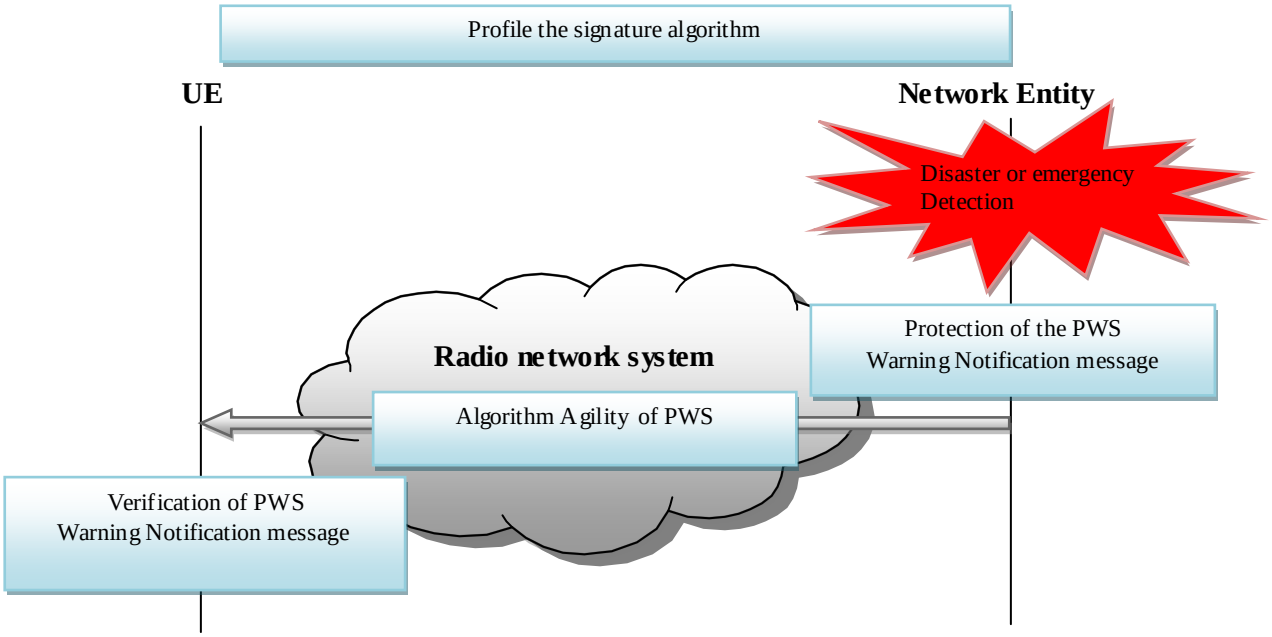


Figure 6.2.1.1: PWS security features

6.2.2 Profile the signature algorithm

It needs to profile the digital signature algorithms. And how to profile digital signature algorithms should be considered and specified as well, i.e., which signature algorithms could be used for PWS and whether same digital signature algorithms shall be used for all the PWS system. And it needs to be settled that how to deal with the length of the signature of PWS message defined in Warning-Security-Information IE of the WRITE-REPLACE Request and how to handle the restriction of the length of the SystemInformationBlockType IE.

Editor's Note: The profiling should take into account the limit of the size of the key (which otherwise may induce too much data sent over the air-interface). It must also take into account the limit on the number of bytes that exist in the protocol fields for the signature today. Further limits may also be identified. The intention is to later ask SAGE for the best algorithm profiling that fulfils these limitations.

6.2.3 Algorithm Agility of PWS

The network should indicate to UE which algorithm to be used. By this way, UE can obtain signature algorithm and know which signature key should be used to verify the signature of PWS Warning Notifications.

Editor's Note: It should avoid negotiation of security information during PWS warning.

An n-bit identifier is allocated to identify the signature algorithm with the following algorithm defined in table 6.2.3.1.

Table 6.2.3.1 Signature algorithms

Value	Signature algorithm
0	128-ECDSA
1	128-DSA
2-2^n	For further use

It has been agreed to limit the number of standardized algorithms to at most the two algorithms listed above. If companies or governments wants to use the “For further use”-range, the registration of new signature algorithms must be handled and approved by 3GPP.

Editor’s Note: The number of bits in the signature algorithm identifier is FFS.

Editor’s Note: It is FFS is the number of standardized algorithms should be narrowed down to only a single algorithm.

6.2.4 Verification of PWS warning notification message

The UE shall support the verification of the signature and a USIM data file with two settings needs to be added to disable the PWS functionality (this only applies from Rel-11 and onwards as required by TS 22.268 [8]).

- HPLMN PWS disable field disables PWS support in HPLMN and PLMNs equivalent to it.
- Unsecured PWS disable field mandates the UE to ignore all PWS warning messages that are received without security protection.

And how to verify PWS Warning Notifications when integrity protected shall be solved. By this way, UE can verify whether the message comes from an authenticated authorized source and whether the messages have been modified maliciously.

If the "unsecured PWS disable" field in the USIM for PWS is set, the UE shall ignore all PWS warning messages that are received without security protection.

If the "unsecured PWS disable" field in the USIM is set, the UE shall verify the "digital signature" and "timestamp" when it receives a warning message with security protection. UE shall silently discard the warning message if the verification of "digital signature" and "timestamp" fails.

Editor’s Note: The impacts of sending more than one signature to the UE and if this solves the overload problem is FFS.

6.2.5 Primary and secondary notifications

To achieve immediate distribution of the highest priority information, ETWS specifies delivery of emergency information in two different notifications:

- The primary notification only contains the most urgent information such as warning type (e.g. Earthquake). When receiving a primary notification the UE sounds an alarm sound and displays a pre-determined warning message on screen.
- The Secondary Notification contains more detailed textual information such as seismic intensity, epicentre, etc. When receiving a secondary notification, the UE simply displays the information on screen.

In case of an earthquake, a UE will typically receive the primary notification several seconds before receiving the secondary notification. When receiving a primary notification, the user has no way of knowing the magnitude of the earthquake, as this information is only included in the secondary notification. And as the magnitude and epicentre is typically not known when sending out the primary notification, users receive primary notifications also for relatively non-serious earthquakes.

An adversary wanting to cause panic might therefore start sending out false notifications. While a false primary notification might only signal "Tsunami", causing people to run to shelter, a false secondary notification might falsify the magnitude of a minor earthquake "Earthquake, Magnitude 9.7" or instruct people to take hazardous or even fatal actions "Drink chlorine bleach to prevent radiation damage". While the above could also be done by e-mail, the impact is likely to be much higher when received through a trusted warning system.

It is therefore important that all notifications carrying warning information are equally protected.

6.2.6 Network Sharing Impact to PWS security

In both GWCN and MOCN configuration for network sharing types, there is no impact to PWS security in GSM, UMTS and EPS when using the current solutions, i.e. NAS messages to distribute public key and CBC to distribute the signature as long as there is no material in the signature specific to any of the operators.

NOTE: It must be ensured that the security constructs in PWS do not cause problems with network sharing, for example, key derivations and signatures should preferably not be dependent on areas, network identities and the like.

6.2.6.1 GWCN configuration

GWCN applies for EPS and UMTS, not for GSM according to TS 23.251 [7] Network Sharing. In EPS and UMTS sharing network, a supporting UE decodes the shared network information and supplies the available core network operator PLMN-ids as candidates to the PLMN selection procedure. The UE performs network selection among available PLMNs. The UE sends an ATTACH REQUEST message to the network entity indicating the chosen core network operator. Then the shared MME/SGSN determines whether the UE is allowed to attach or not and sends the appropriate ACCEPT/REJECT message back to the UE. If successful, a supporting UE has attached to the selected shared network.

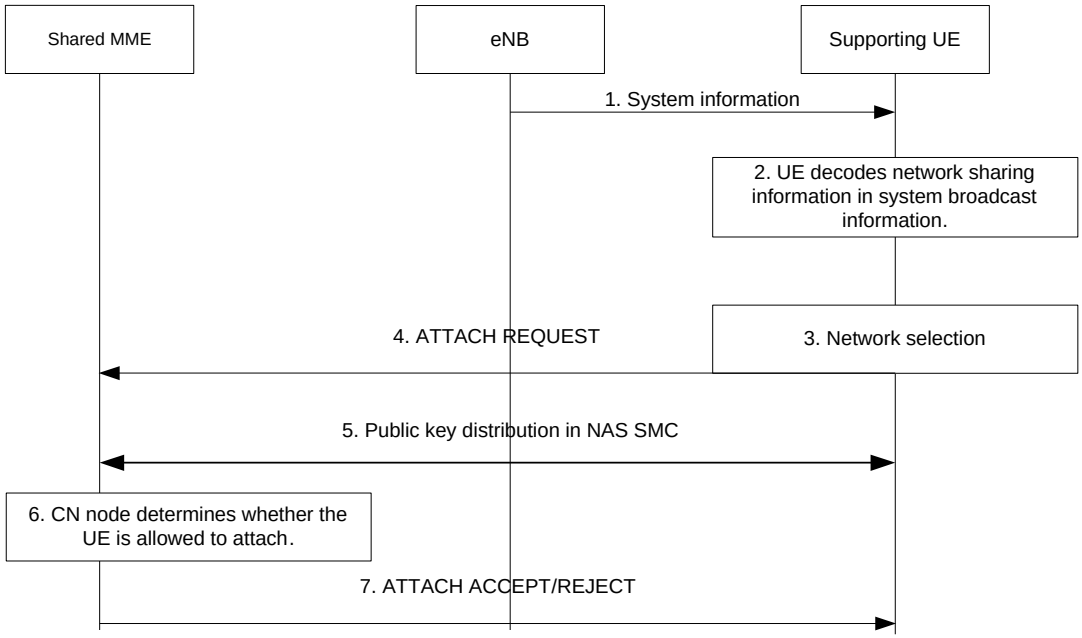


Figure 6.2.6.1.1: An example of Network selection in GWCN configuration for a supporting UE in a shared EPS network for PWS public key distribution

Figure 6.2.6.1.1 shows that network selection procedure in GWCN configuration for network sharing has no impact to public key distribution in NAS SMC for PWS. Moreover, network sharing is an agreement between operators and shall be transparent to the user. This implies that a supporting UE needs to be able to discriminate between core network operators available in a shared radio access network and that these operators can be handled in the same way as operators in non-shared networks. This also means that there is no impact for PWS public key distribution, provided there is no operator-specific material for PWS keys that differentiate the sharing operators.

With regard to PWS signature distribution procedure for GWCN configuration, since the pre-condition defined for network sharing in CBS is using only one single common CBC, CBE always contacts this CBC to broadcast warning messages including signature etc. security information. This single common CBC will use “impacted area” information received from CBE to know which core network entity (EPS) or radio network entity (UMTS) to contact. The following procedure is the same as the normal one in non-shared network. So there is no impact for PWS signature distribution in GWCN configuration, provided there is no operator specific material in the signature.

For GWCN configuration, GSM and UMTS have the same situation like EPS does. So there is also no impact of network sharing for GSM and UMTS PWS services.

6.2.6.2 MOCN configuration

MOCN applies for all the system, i.e. GSM, UMTS and EPS. In sharing network, a supporting UE decodes the shared network information and supplies the available core network operator PLMN-ids as candidates to the PLMN selection procedure. The UE performs network selection among available PLMNs. The UE sends an ATTACH REQUEST message to the network. It also indicates to the radio access node the chosen core network operator. The eNB/RNC/BSC uses the routing information to determine which core network operator the message should be routed to and the ATTACH REQUEST message is sent to the core network operator chosen by the UE. The core network determines whether the UE is allowed to attach to the network. The shared core network node sends the appropriate ACCEPT/REJECT message back to the UE. If successful, a supporting UE has attached to the selected shared network.

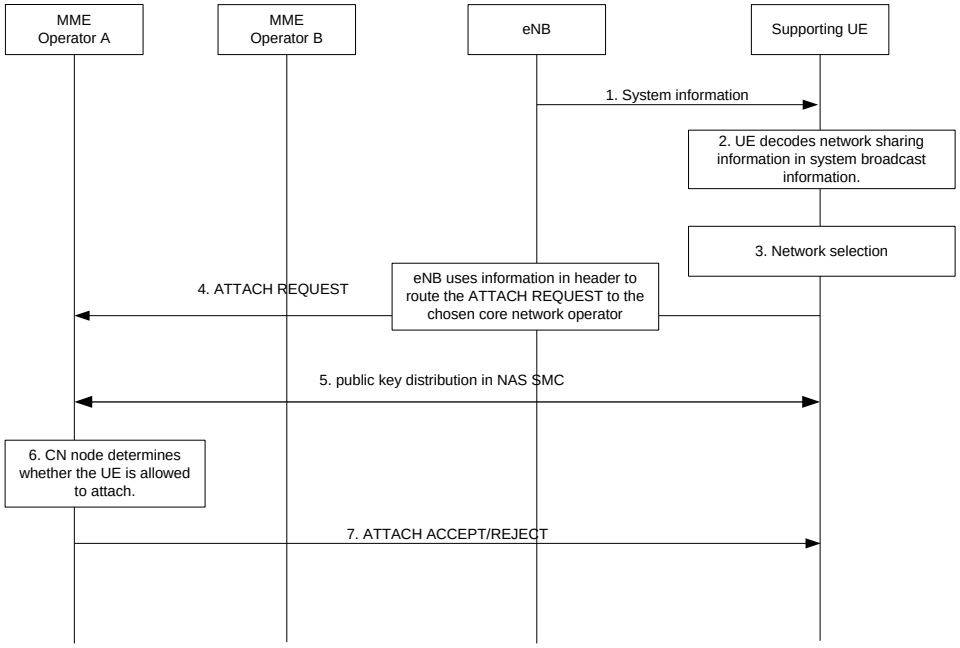


Figure 6.2.6.2.1: An example of Network selection in MOCN configuration for a supporting UE in a shared EPS network for PWS public key distribution

Figure 6.2.6.2.1 shows that network selection procedure in MOCN configuration for network sharing has no impact to public key distribution in NAS SMC for PWS. Similar like the analysis for GWCN case, there is also no impact for PWS public key distribution in MOCN case as long as keying material is not specific to any of the sharing operators.

With regard to PWS signature distribution procedure for MOCN configuration, since the pre-condition defined for network sharing in CBS is using only one single common CBC, CBE always contacts this CBC to broadcast warning messages including its signature which is out of operator control. This single common CBC will use "impacted area" information received from CBE to know which core network entity (EPS) or radio network entity (GSM and UMTS) to contact. The following procedure is the same as the normal one in non-shared network. So there is no impact for PWS signature distribution in MOCN configuration, provided there is no operator specific material in the signature.

For MOCN configuration, GSM and UMTS have the same situation like EPS does. So there is also no impact of network sharing for GSM and UMTS PWS services.

6.2.7 Triggering condition for public key update

There are two scenarios for public key update, i.e. when the signing entity is changed or the signing entity provides new public key to the network. The scenario of triggering public key update could be infrequent.

When the signing entity is changed, the public key is changed and it should be updated. It happens when UE roams to a new cell which belongs to another PLMN with a different CBE. The new PLMN can be associated to the same CBE that the old one is and it can also be the different CBE. If this new PLMN is associated with a different CBE, the UE should use the public key provided by the new CBE to verify PWS signature. In this public key updating scenario, both the PLMN serving the UE and the signing entity-CBE have been changed after UE HO to a new cell.

There can be several reasons for signing entity providing new public key to the network, including end of public key lifetime, compromised public key and replay protection, etc. ECDSA/DSA with 128 bit security level is considered secure enough beyond 2030 according to NIST recommendations. Furthermore, each government will be very careful to send such kind of public warning. So the public keys for PWS signature could be seen as safe for a considerable period of time. However, there remains requirement for PWS public key update for some reasons e.g. private key leakage, key management hole etc.

There may also be policy reasons for changing the key. For example, the key lifetime of the key may expire. The lifetime of the key may be in the order of months or years.

PWS key may be updated after warning notification has been sent.

Editor's Note: Terminology used to identify keys used in the scope of this specification is FFS.

6.2.8 Roaming impact to PWS security

A roaming UE can attach to VPLMN network or perform TAU/RAU/LAU/handover from HPLMN to VPLMN network. Since different PLMN may connect to different CBE/CBC, a roaming UE need to initiate PWS key updating to get latest PWS key of the VPLMN. Then UE can use the latest PWS key to verify Warning Notifications broadcasted by the VPLMN.

- Case1: UE attaches to VPLMN network, PWS key can be distributed to UE via SMC or attach accept message by VPLMN.
- Case 2: UE is in idle state and performs TAU/RAU/LAU to VPLMN network, PWS key can be distributed to UE via TAU/RAU/LAU accept message by VPLMN.
- Case 3: UE is in PS-connected state and performs handover to VPLMN network:
  - When UE handovers to LTE network, UE will initiate TAU just after handover procedure and PWS key can be distributed to UE via TAU accept message by LTE network.
  - When UE handovers to UMTS PS domain, UE will initiate RAU just after handover procedure and PWS key can be distributed to UE via RAU accept message by UMTS network.
  - When UE handovers to GERAN PS domain, UE will initiate RAU just after handover procedure and PWS key can be distributed to UE via RAU accept message by GERAN network.
  - When UE SRVCC handovers to UMTS/GERAN CS domain, then UE has to wait for CS service terminated and then performs LAU at once. Thus UE cannot obtain PWS key in time via LAU accept message since the duration of CS service is uncertain.
- Case 4: UE is in CS-connected state and performs handover to VPLMN network:
  - When UE handovers to UMTS CS domain, then UE has to wait for CS service terminated and then performs LAU at once. Thus UE cannot obtain PWS key in time via LAU accept message since the duration of CS service is uncertain.
  - When UE handovers to GERAN CS domain, then UE has to wait for CS service terminated and then performs LAU at once. Thus UE cannot obtain PWS key in time via LAU accept message since the duration of CS service is uncertain.
  - When UE rSRVCC handovers to LTE/HSPA PS domain, UE will initiate RAU just after handover procedure and PWS key can be distributed to UE via RAU accept message by LTE/HSPA network.

As mentioned above, UE cannot obtain PWS key in time in the following scenarios:

Scenario 1: If UE is in CS-connected state and it handovers to UMTS CS domain, UE has to wait for CS service terminated and then performs LAU at once to update PWS key.

Scenario 2: If UE is in CS-connected state and it handovers to GERAN CS domain, UE has to wait for CS service terminated and then performs LAU at once to update PWS key.

Scenario 3: If UE is in PS-connected state and it SRVCC handovers to UMTS/GERAN CS domain, UE has to wait for CS service terminated and then performs LAU at once to update PWS key.

In above three scenarios, UE cannot obtain PWS key via LAU accept message in time. Since the duration of CS service is uncertain, if UE receives CBS warning message from VPLMN during the duration, it cannot verify the warning message by using latest PWS key.

But in TS 23.041 [4] section 2, the following text and table is described.

'Reception of CBS messages for an MS/UE is not a requirement if it is connected in the CS domain. It should be possible for an MS/UE to receive messages if it is connected in the PS domain and no data is currently transmitted.'

CS-Domain	CS-Connected	CS-Idle	CS-Idle
PS-Domain	-	PS-Idle	PS-Connected
Reception of CBS Message	Not possible	Possible	Depends on RRC mode

When UE is in CS-Connected sate, it is not a requirement for UE to receive SIB message. CBS warning message is broadcasted to UE via SIB message. So it is not possible for a CS-Connected UE to receive CBS warning message. Even if UE has to wait for CS service terminated and then performs LAU at once to update PWS key, there is no impact on PWS key updating and warning message verification.

Based on above analysis, there is no new security requirement on the PS domain needed for PWS key distribution and warning message verification in roaming case.

7 Security solutions of PWS

Editor's Note: This section aims to meet all the requirements and solve all the open issues of PWS.

7.1 Solution 1

Editor's Note: Solutions for GSM and UMTS are needed.

7.1.1 Public key distribution

The solution describes the distribution of the public signature verification key information based on NAS messages. NAS SMC/Attach /TAU ACCEPT message can be used.

1. In the initial attach procedure, UE sends the initial attach request to MME.

NOTE A: If UE has attached the network before, UE sends the public key identifier to MME in Attach request or TAU request.

NOTE B: In the roaming case or in case of network sharing, UE should send PLMN ID to the core network.

2. EPS AKA procedure may take place.

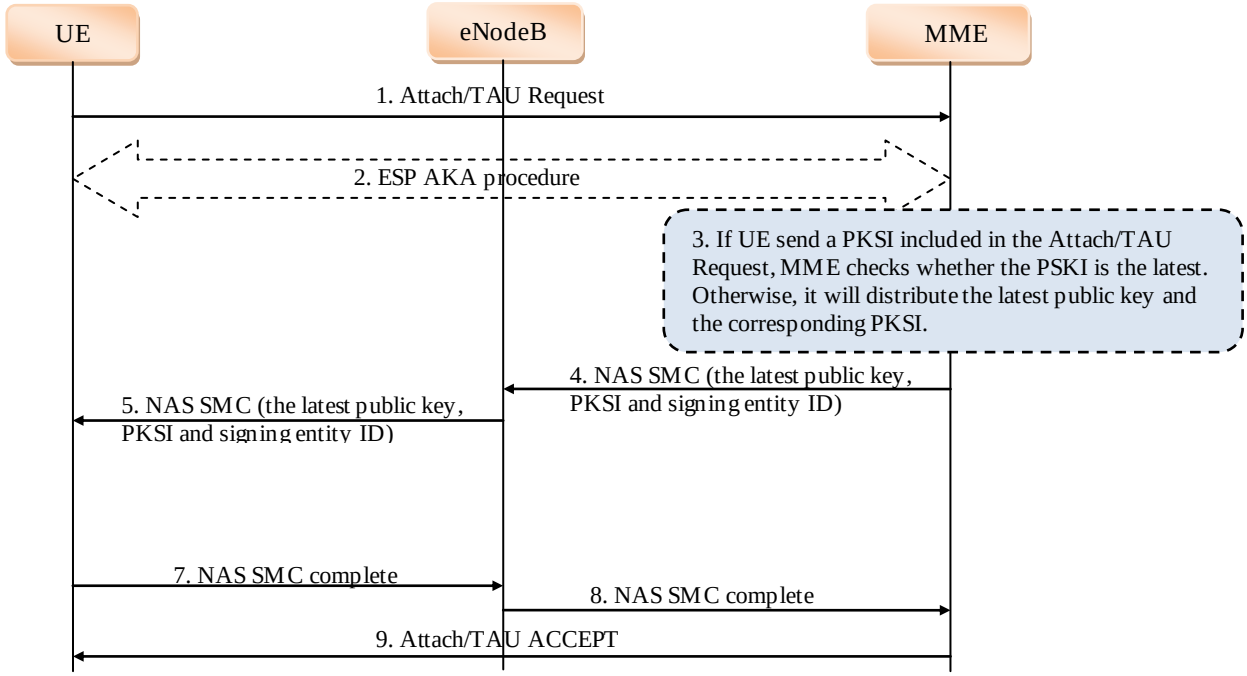
3. When MME receives the initial attach request, MME distributes the latest public key and the identifier of public key and the signing entity identifier in NAS SMC.

NOTE C: In order to validate the PWS warning notification come from different signing entities, UE shall be notified signing entity identifier, to know which signing entity the PWS warning message comes from.

NOTE D: If UE has attached the network before, when MME receives Attach or TAU request, it verifies whether the public key that UE possesses is the latest. Otherwise, MME checks whether the PSKI that UE send is latest. Otherwise, it will distribute the latest public key and the corresponding PKSI.

NOTE E: In the roaming case or in case of network sharing, when core network receives the request message, it will check whether the PLMN ID is same as the PLMN ID that it located in. Otherwise, MME will send the new PLMN ID to UE to avoid the collision of the public key identifier, as the PKSI may not be global unique.

4. At receiving the NAS message, UE receives and saves the public key, PKSI, and the signing entity identifier and the relationship between PWS key, PKSI and the signing entity identifier sent from MME via NAS SMC. UE verifies the signature of PWS Warning Notification message with the public key and signature algorithm.



NOTE F: Only happening in emergency case.

NOTE G: If the UE has several active keys, the UE can send several PKSI in one NAS message and receive several public keys in one NAS message.

Editor's Note: The sizes of NAS messages need to be considered.

The public key distribution mechanism can also be used for public key update in LTE.

7.1.2 Public key distribution in UMTS

The solution describes the distribution of the public signature verification key information based on AS message or NAS messages. SMC /Attach /RAU/LAU ACCEPT message can be used.

1. In the initial attach procedure, UE sends the initial attach request to SGSN.

NOTE A: If UE has attached the network before, UE sends the public key identifier to SGSN in Attach/ RAU/LAU request.

NOTE B: In the roaming case or in case of network sharing, UE should send PLMN ID to the core network.

2. AKA procedure may take place.

3. When SGSN receives the initial attach request, SGSN distributes the latest public key and the identifier of public key in Security Mode Command.

NOTE C: If UE has attached the network before, when SGSN receives Attach/RAU/LAU request, it verifies whether the public key that UE possesses is the latest. Otherwise, SGSN checks whether the PSKI that UE send is latest. Otherwise, it will distribute the latest public key and the corresponding PKSI.

NOTE D: In the roaming case or in case of network sharing, when core network receives the request message, it will check whether the PLMN ID is same as the PLMN ID that it located in. Otherwise, SGSN will send the new PLMN ID to UE to avoid the collision of the public key identifier, as the PKSI may not be global unique.

4. At receiving the Security Mode Command message, RNC transmits this message to UE.

5. When receiving the Security Mode Command message, UE receives and saves the public key sent from RNC via Security Mode Command. UE verifies the signature of PWS Warning Notification message with the public key and signature algorithm.

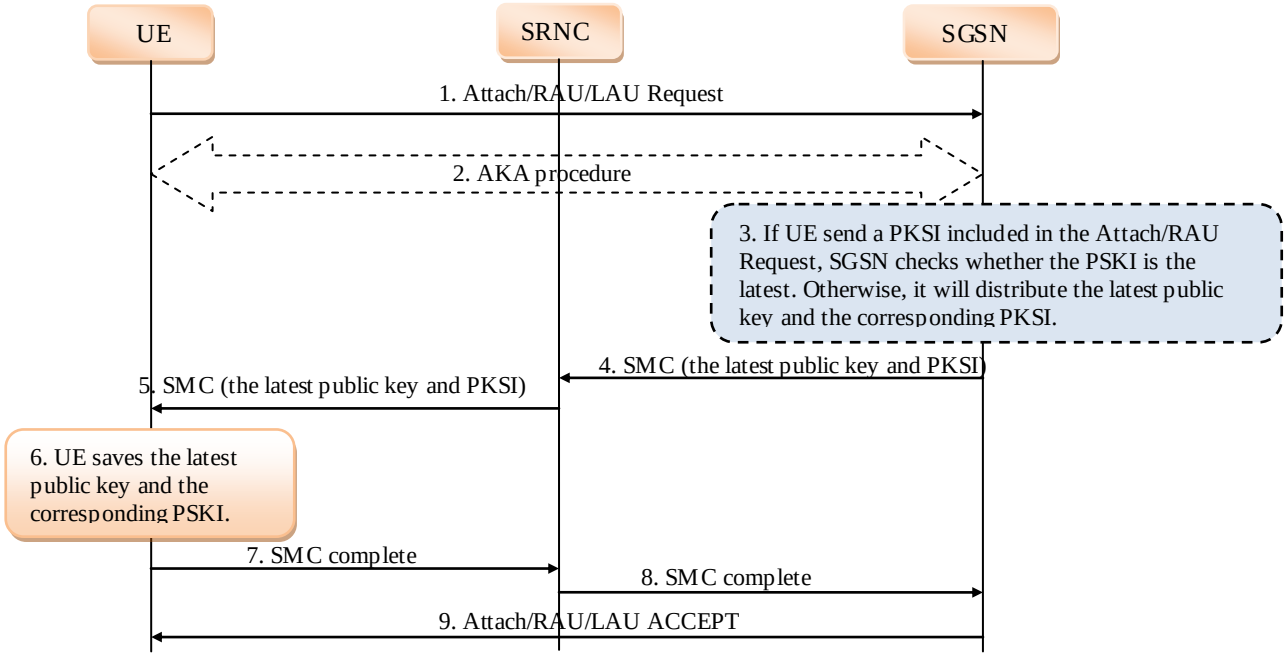


Figure 7.1.2.1 Distribution of public key information in UMTS

Editor's Note: It is FFS whether SMC messages should be used for key distribution.

The public key distribution mechanism can also be used for public key update in UMTS.

7.1.3 Signature algorithm agility

This solution describes the distribution of the signature algorithm identifier based on Warning Notification messages and broadcast message. CBE signs the PWS Warning Notification. Figure 7.1.3.1 gives an example.

NOTE: SAI: Signature Algorithm Identifier

1. In the Emergency Broadcast Request, CBE provides the signature algorithm identifier to CBC.

2. CBC transmits the signature algorithm identifier to MME with Write-Replace Warning Request.

3. The MME sends a Write-Replace Warning Confirm message that indicates to the CBC that MME has started to distribute the warning message to eNB.

4. Upon reception of the Write-Replace Confirm messages from MME, the CBC may confirm to the CBE that the PLMN has started to distribute the warning message.

5. When MME receives this request, it transmits the signature algorithm identifier with Write-Replace Warning Request to eNB.

6. eNB broadcasts the signature algorithm identifier for the network's coverage area to all UEs. And UE verifies the signature of PWS Warning Notification message with the public key and signature algorithm.

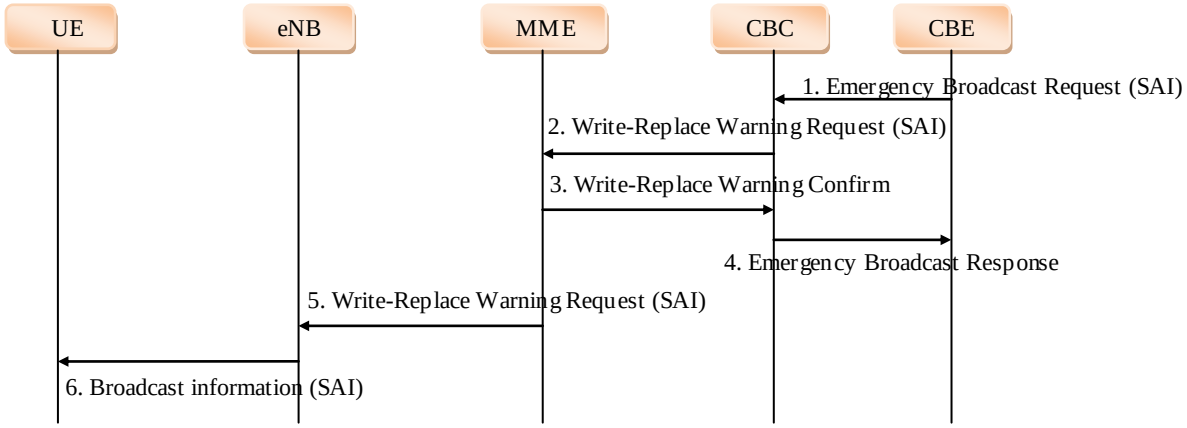


Figure 7.1.3.1: Distribution of signature algorithm identifier

PWS signature algorithm identifier is set in the IE: Warning-Security-Information of PWS Warning Notification.

The signature algorithm identifier can be set in the Warning-Security-Information IE in WRITE-REPLACE Request/Indication. Then the corresponding message over air interface will have no impact. If this approach is introduced, it will not increase the overload for network entity,

Editor's Note: Other mechanisms for signature algorithm identifier distribution need to be studied.

7.1.4 Distribution of signature algorithm identifier in UMTS

This solution describes the distribution of the signature algorithm identifier in the ETWS PRIMARY NOTIFICATION WITH SECURITY or in the Warning Security Information of WRITE-REPLACE Request message.

NOTE: SAI: Signature Algorithm Identifier

1. In the Emergency Broadcast Request, CBE provides the signature algorithm identifier to CBC. CBC transmits the signature algorithm identifier to UTRAN with Write-Replace Warning Request.

2. UTRAN sends a Write-Replace Warning Confirm message that indicates to the CBC that it has started to distribute the warning message to service area.

3. Upon reception of the Write-Replace Confirm messages from CBC, the CBC may confirm to the CBE that the PLMN has started to distribute the warning message.

4. When UTRAN receives this request, it first sends a PAGING TYPE 1 message or a SYSTEM INFORMATION CHANGE INDICATION message, including the IE "ETWS information".

5. After the reception of the IE "ETWS information" in either the PAGING TYPE 1 or the SYSTEM INFORMATION CHANGE INDICATION message. If RRC is configured from upper layers to receive the ETWS primary notification with security, UTRAN shall send SAI included in ETWS PRIMARY NOTIFICATION WITH SECURITY to UEs. And UE verifies the signature of PWS Warning Notification message with the public key and signature algorithm.

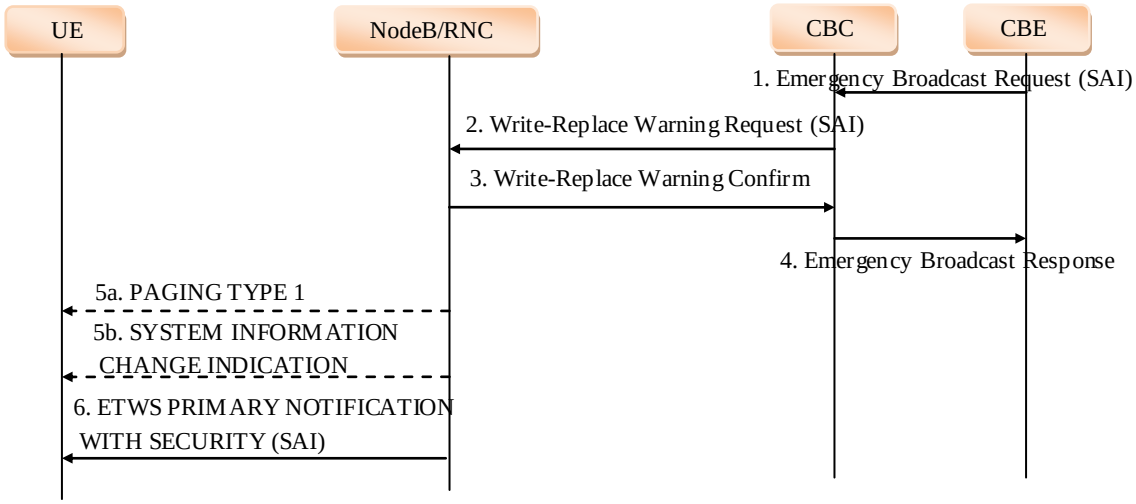


Figure 7.1.4.1: Distribution of signature algorithm identifier in UMTS

7.1.5 Verification of PWS warning notification message

This section describes the solution that UE verifies the signature of PWS Warning Notification message with the saved public signature key and signature algorithm Figure 7.1.5.1 gives an example to show the solution with CBE as the signature entity.

1. CBE sends SAI and the signature included in Emergency Broadcast Request to CBC.
2. CBC sends SAI and the signature in Write-Replace Warning Request to MME.
3. MME sends a Write-Replace Warning Confirm message that indicates to the CBC that MME has started to distribute the warning message to eNB.
4. Upon reception of the Write-Replace Confirm messages from MME, the CBC may confirm to the CBE that the PLMN has started to distribute the warning message.
5. When MME receives this request, it sends SAI and the signature in the Write-Replace Warning Request to eNB.
6. eNB broadcasts SAI and the signature for the network's coverage area to all UEs.
7. At receiving the broadcast information message, UE verifies the signature with the latest public key.

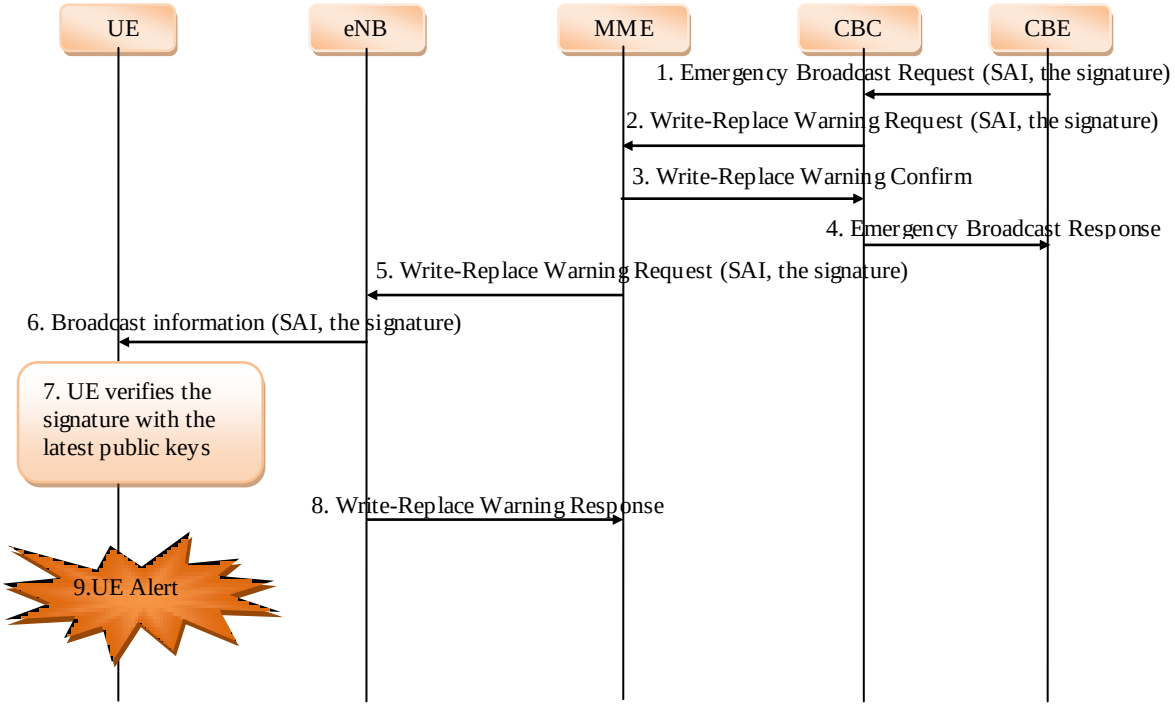


Figure 7.1.5.1: Verification of PWS message

7.2 Solution 2

7.2.1 General

In this solution, a secure point-to-point channel is used to distribute PWS keys to UE registered to the network. Two aspects are included: the one is the network entity (MME/SGSN) distribute PWS key to UE (the blue line as showed in Figure 7.2.1.1 below); the other is network entity (MME/SGSN) get PWS key from CBC/CBE (the red line as showed in Figure 7.2.1.1 below).

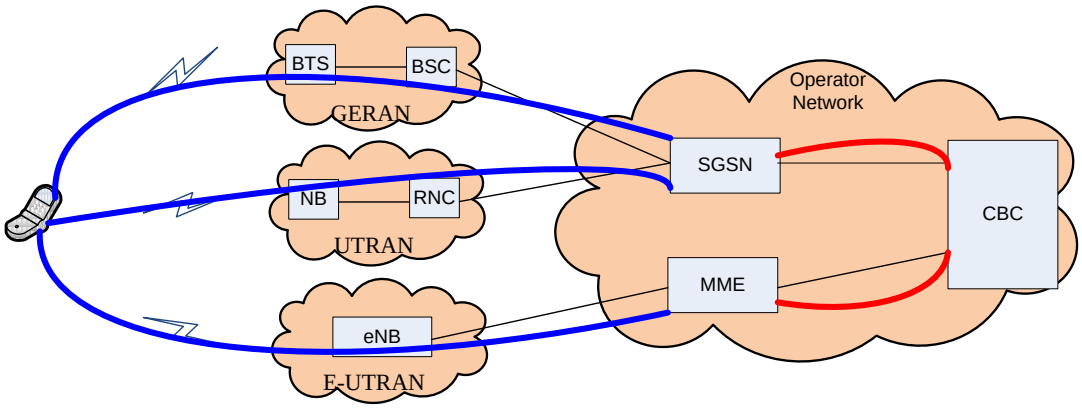


Figure 7.2.1.1: PWS key distribution path

7.2.2 Initial PWS key distribution

Initial PWS keys should be ready just after UE has registered to the network immediately. In this way by anytime there is a PWS warning message sent by the network, UE can verify it with the PWS key it has stored. So a solution is proposed that the initial PWS keys are distributed in attach procedure.

- LTE: Two PWS keys and the corresponding public key identifiers (PKIDs) are sent to UE in Attach Accept message by MME, which is integrity protected.

- UMTS: Two PWS keys and the corresponding PKIDs are sent to UE in Attach Accept message by SGSN, which is integrity protected.

- GSM: Two PWS keys and the corresponding PKIDs are sent to UE in RAU Accept message during attach procedure by SGSN.

NOTE: Whether security enhancement is needed for GSM/GPRS is FFS.

The above two PWS keys are defined to be the current PWS key and the next PWS key. The current PWS key is the currently activated key which is used to sign the PWS notification message. The next PWS key is activated and becomes the current key after the old current one is deactivated.

7.2.3 Network PWS key configuration

Since PWS keys are sent to UE in L3 signallings, the network entity (MME/SGSN) should be configured with the PWS keys when PWS service is determined to be provided to UE by the network. Thus there is a requirement that CBC and MME/SGSN shall have an interface to distribute the PWS keys.

When the network determines to provide PWS service to UEs, CBC shall send PWS keys to MME/SGSN. After PWS keys are configured in MME/SGSN, once there is a UE registered to the network, MME/SGSN should distribute the PWS keys to the UE in the attach procedure.

When CBC/CBE updates the PWS keys of a specified notification area, CBC shall send the updated PWS keys to the network entities (MME/SGSN) which have connections with the affected RAN.

Editor's Note: It is FFS if the working assumption on a national root of trust determines CBC/CBE.

7.2.4 PWS key update

Even if the frequency of PWS key update is rather low, it should also provide a mechanism to permit PWS key to be updated. This solution uses a point-to-point secure channel to update PWS keys.

The network activates and updates PWS keys as follows:

- Two PWS keys are used: the current PWS key and the next PWS key. The current one is the activated one which is used to verify the current PWS notification; the next PWS key is used to verify the PWS notification after it has been activated when the current one is deactivated.

- When CBC determines to change the next PWS key to current PWS keys, it shall also update the next PWS key with a new one. And CBC shall send the updated next PWS key and its identifier to the network entities (MME/SGSN), together with the current PWS key identifier.

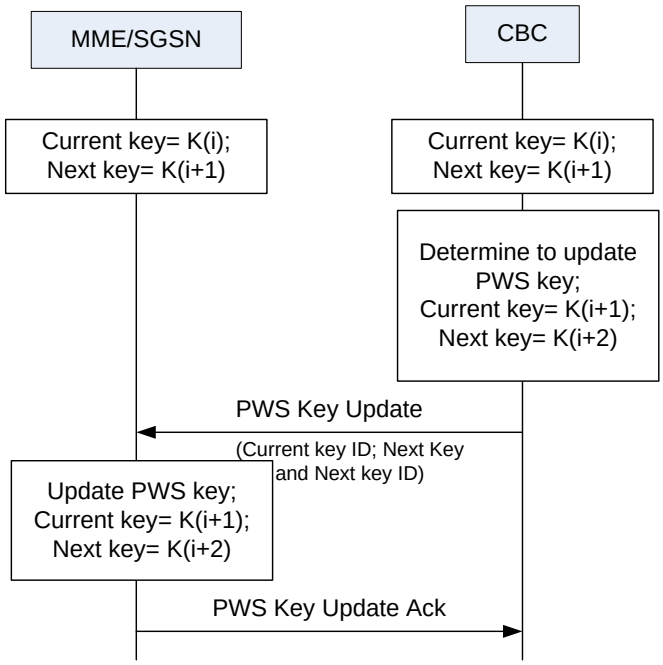


Figure 7.2.4.1: PWS key activates and updates by network side

UE activates and updates PWS keys as follows:

- The serving network always broadcasts the current PWS key identifier and the next PWS key identifier. The network entities notify the corresponding RAN to broadcast the just activated current PWS key identifier and the updated next PWS key identifier.
- UE activates the stored next PWS key to the current key as the serving network indicates.
- Once a UE notices that at least one of the broadcasting PWS key identifiers is different from the one it stores, UE will performs PWS key update till the next normal TA/RA/LA update procedure.
- In response to each successful tracking area, routing area or location area update, the network entity provides the PWS key requested by UE.
- UE stores the received new PWS key as the next one.

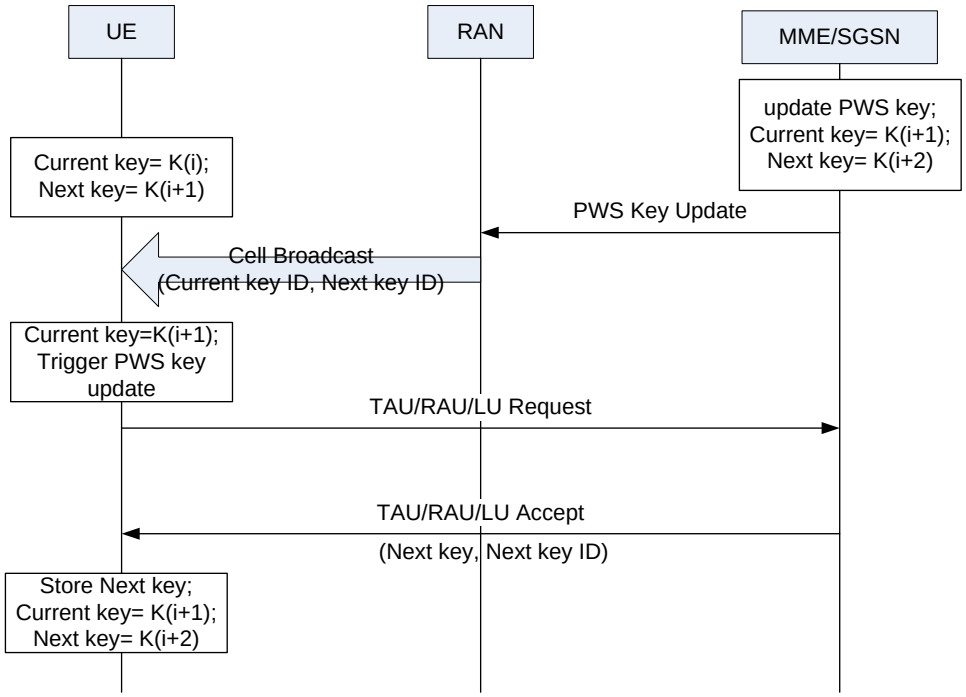


Figure 7.2.4.2: PWS key activates and updates by UE side

Editor's Note: PWS Key Update in Figure 7.2.4.2 needs more detail.

Editor's Note: Lifetime of the key must be longer than the TAU/RAU/LU lifetime.

7.2.5 Delivery of PWS warning notification message

When network nodes distribute PWS Warning Notification message to UE, the public key identifier (PKID) should be included in the message which is identified the public key used to sign the message. This method can avoid UEs trying each public key to verify the signature effectively. Figure 7.2.5.1 gives an example to show the solution used in LTE network.

1. CBC/CBE sends a Write-Replace Warning Request message to MME. The message shall include a"PKID" to identify the public key used to sign the message, as well as the "the signature".
2. MME sends a Write-Replace Warning Confirm message to the CBC/CBE.
3. When MME receives this request, it sends a Write-Replace Warning Request message ("PKID", and "the signature") to eNB.
4. When eNB receives this request, it broadcasts PWS warning message ("PKID", and "the signature") to all UEs in the network's coverage area.
5. At receiving the broadcast information message, UE verifies the signature with the public key identified by PKID which is received in the broadcast message.
6. The eNB sends a Write-Replace Warning response message to MME to confirm the request.
7. The UE alerts the user.

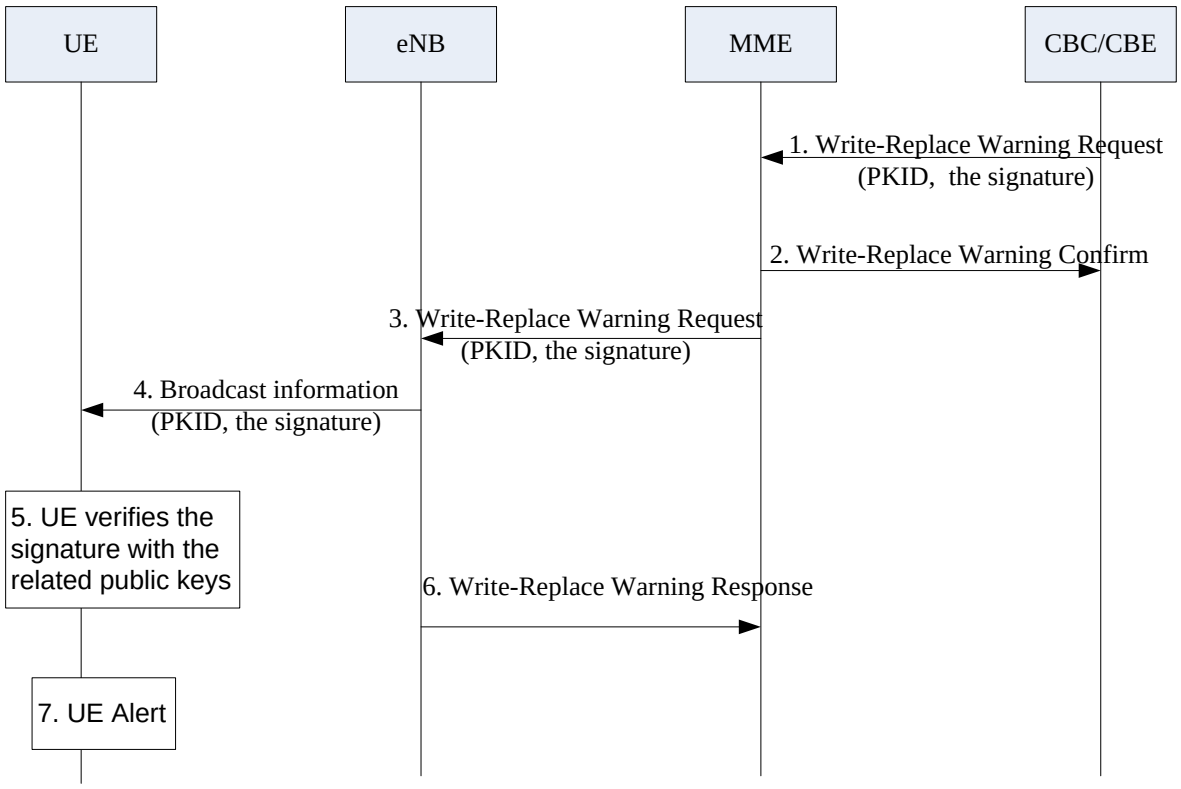


Figure 7.2.5.1: Verification of PWS message

NOTE: Step 6 happens after step 3, otherwise there are no other sequence requirements.

7.3 Solution 3

Editor's NOTE: This is a solution for PWS security which includes solution 1 and 2 and also includes some new points to improve the solution.

With regard to public key distribution procedure, NAS messages, e.g. TAU/RAU/LAU accept can be used to distribute public key which is also in solution 1 and 2 of living doc. From previous meeting discussion, public key update should also be considered. LTE and UMTS can use similar procedures for public key distribution and update. For GSM PWS security solution, it may be different from previous two systems. Current living doc gives some solutions and it depends on the meeting discussions and operators' choice for it. So this doc only discusses LTE and UMTS system solution for PWS security.

7.3.1 PWS public key distribution

7.3.1.1 Initial PWS public key distribution

For LTE system, NAS messages, i.e. NAS SMC/Attach accept/TAU accept are used to distribute public key. Specifically, NAS SMC message is used to distribute PWS public key when UE attaches to a PLMN for the first time. For UMTS system, NAS and AS messages, i.e. SMC/Attach accept/RAU accept are used to distribute public key. Specifically, SMC message is used to distribute PWS public key when UE attaches to a PLMN for the first time. When UE has inter-PLMN handover, TAU accept/RAU accept are used to distribute new PLMN PWS public key.

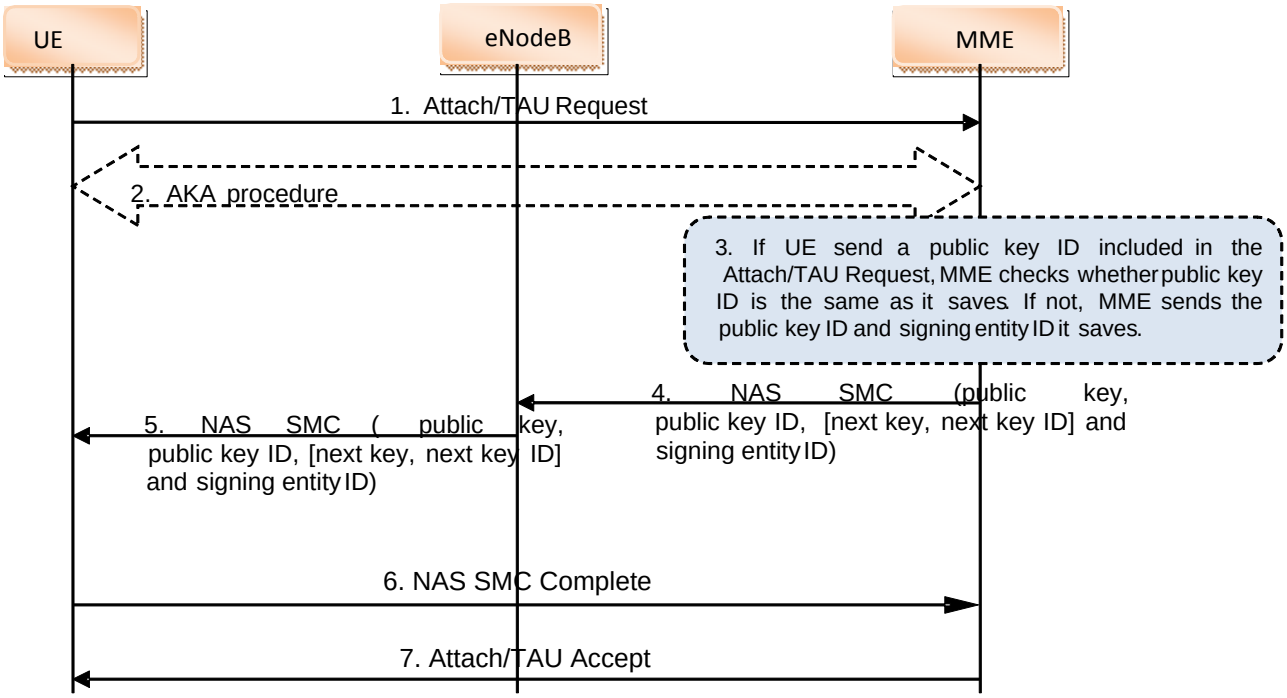


Figure 7.3.1.1.1 Initial distribution of PWS public key in LTE system

When MME receives the initial attach request, MME distributes public key(optional next key)and the corresponding public key ID(s),signing entity ID in NAS SMC messages. UE receives and saves the public key(s), public key ID(s) and signing entity ID and the relationship in all of them. When UE receives warning messages, UE verifies the signature of PWS Warning Notification message with public key and the signature algorithm. If UE failed to verify the signature with current public key, and UE has received the optional next public key and key ID, UE should try to verify the signature with next public key.

If UE has attached the network before, UE sends public key ID(s), signing entity ID in the attach request/TAU request. When MME receives attach request or TAU request, MME checks whether public key ID(s) is the same as it saves. If not, MME sends the public key(s), public key ID(s) and signing entity ID it saves.

NOTE1: [next key, next key ID] means that the next public key and ID is optional to send. It depends on operators' and public key issued entity's policy to use. The procedure of distributing two public keys is the same as distributing one public key.

NOTE2: If the signing entity is CBC, signing entity ID may not need to be sent since there is only one CBC in a PLMN.

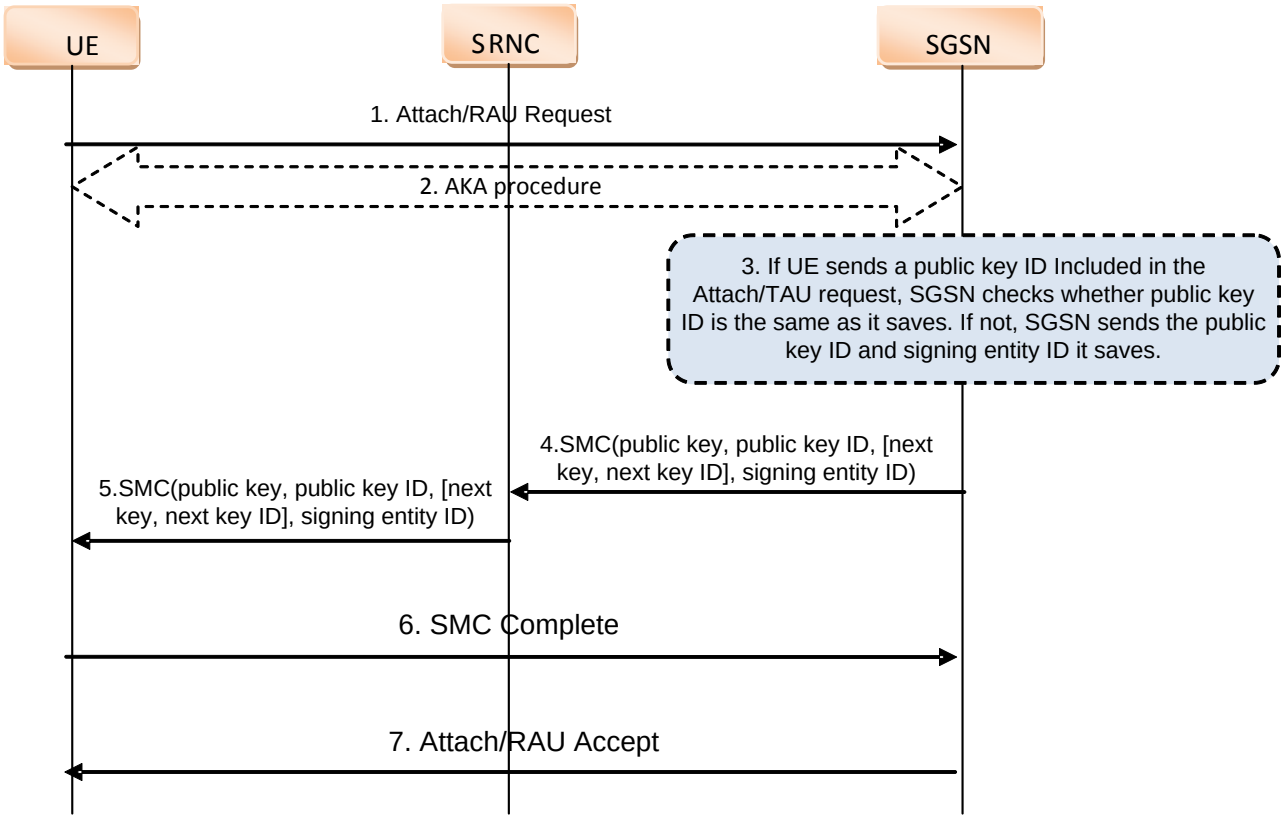


Figure 7.3.1.1.2 Initial distribution of PWS public key in UMTS system

When SGSN receives the initial attach request, SGSN distributes the latest public key(optional next key) and the corresponding public key ID(s) and signing entity ID in SMC messages. UE receives and saves the public key(s), public key ID(s) and signing entity ID and the relationship in all of them. When UE receives warning messages, UE verifies the signature of PWS Warning Notification message with public key and the signature algorithm. If UE failed to verify the signature with current public key, and UE has received the optional next public key and key ID, UE should try to verify the signature with next public key.

If UE has attached the network before, UE sends the saved public key ID(s), signing entity ID and the corresponding PLMN ID in the attach request/RAU request. When SGSN receives attach request or RAU request, SGSN checks whether public key ID(s) is the same as it saves. If not, SGSN sends the public key(s), public key ID(s) and signing entity ID it saves.

Regard how the core network elements get public key and relative ID, for LTE MME can get public key and relative ID by pre-configuration and also can get them through SBc interface from CBC. For UMTS, SGSN can get public key and relative ID by pre-configuration.

NOTE3: [next key, next key ID] means that the next public key and ID is optional to send. It depends on operators' and public key issued entity's policy to use. The procedure of distributing two public keys is the same as distributing one public key.

NOTE4: If the signing entity is CBC, signing entity ID may not need to be sent since there is only one CBC in a PLMN.

Editor's Note: SAI(Signature Algorithm ID) can be included in the Warning-Security-Information IE in WRITE-REPLACE Request/Indication and NAS messages when distributing public key. It needs FFS where to carry this SAI.

7.3.1.2 PWS public key update

When the network updates the public key, it uses the very next TAU/RAU procedure to distribute the update public key for PWS security. This TAU/RAU can be normal procedure that UE moves to trigger and also can be periodic TAU/RAU procedure. The network sends the latest public key, public key ID and signing entity ID in TAU/RAU accept to UE.

There are two cases for UE to get new public key.

1. Signing entity sends periodic warning message "test" which is signed by the latest public key. The warning type of this warning message is "test". Public key ID and CBE-ID should also be included in the test warning message. When UE receives it, UE verifies the signature using the public key it saves . If successful, the public key UE saves is the latest. UE discards the warning test silently. If not, UE sends the public key ID and signing entity ID in the next TAU/RAU request. When MME/SGSN receives them, MME/SGSN checks whether public key ID is the same as it saves. If not, MME/SGSN sends the update public key, public key ID and signing entity ID it saves in TAU/RAU accept message. Especailly, signing entity must send warning message "test" which is signed by the latest public key to let UE knows in time once the signing entity updates the public key.

2. UE sends the public key ID and signing entity ID in the TAU/RAU request. When MME/SGSN receives them, MME/SGSN checks whether public key ID is the same as it saves. If not, MME/SGSN sends the update public key, public key ID and signing entity ID it saves in TAU/RAU accept message.

NOTE: There can be some policy for UE to know when to send public key ID, signing entity ID and the corresponding PLMN-ID in the TAU/RAU request. For example, there can be some pre-configured periodical time for UE to use.

NOTE: Next public key and ID is optional to send. It depends on operators' and public key issued entity's policy to use. The procedure of distributing two public keys is the same as distributing one public key.

7.3.2 PWS warning notification message

For LTE system, CBE/CBC can sign the PWS Warning Notification.

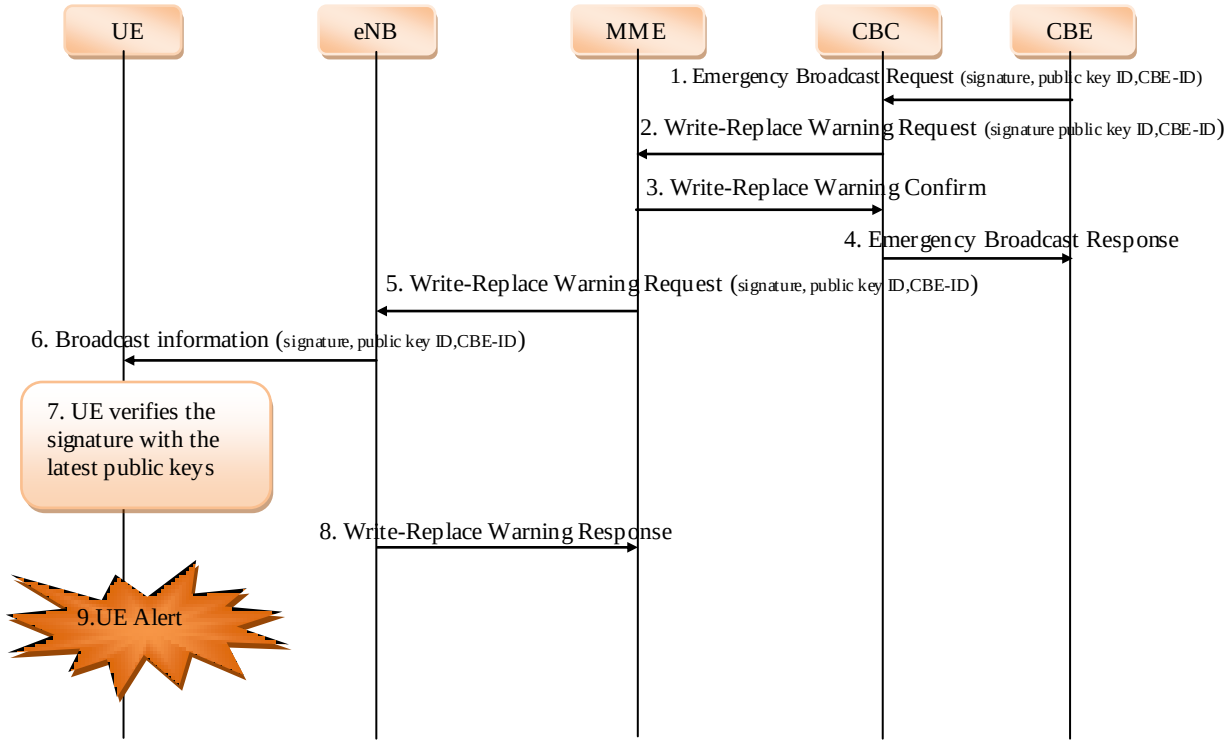


Figure 7.3.2.1 PWS warning notification procedure for LTE system

1. If CBE is the signing entity, CBE sends public key ID and the signature included in Emergency Broadcast Request to CBC.

Editor's Note: SAI(Signature Algorithm ID) can be included in the Warning-Security-Information IE in WRITE-REPLACE Request/Indication and NAS messages when distributing public key. It needs FFS where to carry this SAI.

2. CBC sends public key ID and the signature in Write-Replace Warning Request to MME.

3. MME sends a Write-Replace Warning Confirm message that indicates to the CBC that MME has started to distribute the warning message to eNB.

4. Upon reception of the Write-Replace Confirm messages from MME, the CBC may confirm to the CBE that the PLMN has started to distribute the warning message.

5. When MME receives this request, it sends public key ID and the signature in the Write-Replace Warning Request to eNB.

6. eNB broadcasts public key ID and the signature for the network's coverage area to all UEs.

7. At receiving the broadcast information message, UE verifies the signature with the latest public key and signature algorithm. If UE failed to verify the signature with current public key, and UE has received the optional next public key and key ID, UE should try to verify the signature with next public key.

8. eNB sends Write-Replace Warning Response message to MME to let MME know it has broadcast the warning messages.

9. UE alerts the user what kind of warning will happen.

For UMTS system, CBE/CBC can sign the PWS Warning Notification.

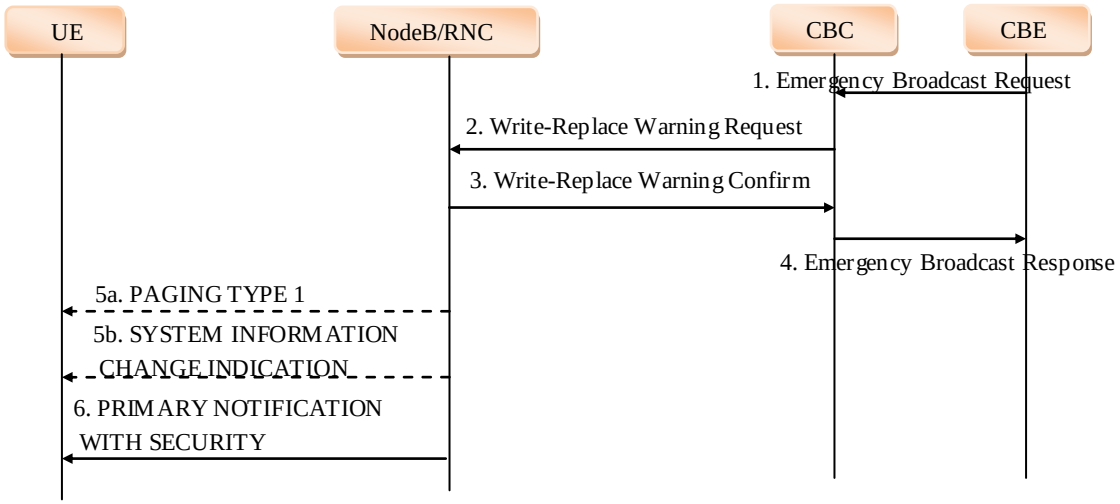


Figure 7.3.2.2 PWS warning notification procedure for UMTS system

1. In the Emergency Broadcast Request, CBE provides public key IDand the signature to CBC. CBC transmits them to UTRAN with Write-Replace Warning Request.

Editor's Note: SAI(Signature Algorithm ID) can be included in the Warning-Security-Information IE in WRITE-REPLACE Request/Indication and NAS messages when distributing public key. It needs FFS where to carry this SAI.

2. UTRAN sends a Write-Replace Warning Confirm message that indicates to the CBC that it has started to distribute the warning message to service area.

3. Upon reception of the Write-Replace Confirm messages from CBC, the CBC may confirm to the CBE that the PLMN has started to distribute the warning message.

4. When UTRAN receives this request, it first sends a PAGING TYPE 1 message or a SYSTEM INFORMATION CHANGE INDICATION message, including the warning type.

5. After the reception of the warning type in either the PAGING TYPE 1 or the SYSTEM INFORMATION CHANGE INDICATION message. If RRC is configured from upper layers to receive primary notification with security, UTRAN shall send public key IDincluded in PRIMARY NOTIFICATION WITH SECURITY and the signature to UEs. And UE verifies the signature of PWS Warning Notification message with the public key and signature algorithm.

Test warning messages:

According to the security requirement in section 2 of this living document,

"A serving network should periodically send test warning messages on the broadcast channel."

Signing entity can send periodic warning message “test” which is signed by the latest public key. The warning type of this warning message is “test”. Public key ID and CBE ID should also be included in the test warning message. When UE receives it, UE verifies the signature using the public key indicated by the public key ID in the “test” message. If successful, the public key UE saves is the current. UE discards the warning test silently. If not, UE sends the saved public key ID and signing entity ID in the next TAU/RAU request. When MME/SGSN receives them, MME/SGSN checks whether the received public key ID is the same as it saves. If not, MME/SGSN sends the public key(optional next key), public key ID, and signing entity ID it saves in TAU/RAU accept message. Especially, signing entity must send warning message "test" which is signed by the latest public key to let UE knows in time once the signing entity updates the public key.

7.4 Solutions to security issues in GSM/GPRS

7.4.1 General

Unlike LTE and UMTS, GSM/GPRS security mechanism does not provide integrity protection on the radio interface. So the proposed PWS public key distribution solution based on integrity protection in AS and NAS messages in UMTS and LTE is infeasible. This section describes solutions on how to distribute the public key and other security information to the UE in GSM/GPRS. Three possible approaches are suggested:

NOTE: This is an exhaustive set of options.

7.4.2 Re-use current GSM/GPRS security mechanism with initiating ciphering

In GSM/GPRS, PWS public key can be ciphered with GSM/GPRS AKA key. The solution that we suggest is distributing public keys based on NAS message. Figure 7.4.2.3.1 shows an example that distributes public key in GSM/GPRS. The RAU/LAU ACCEPT message can also be used.

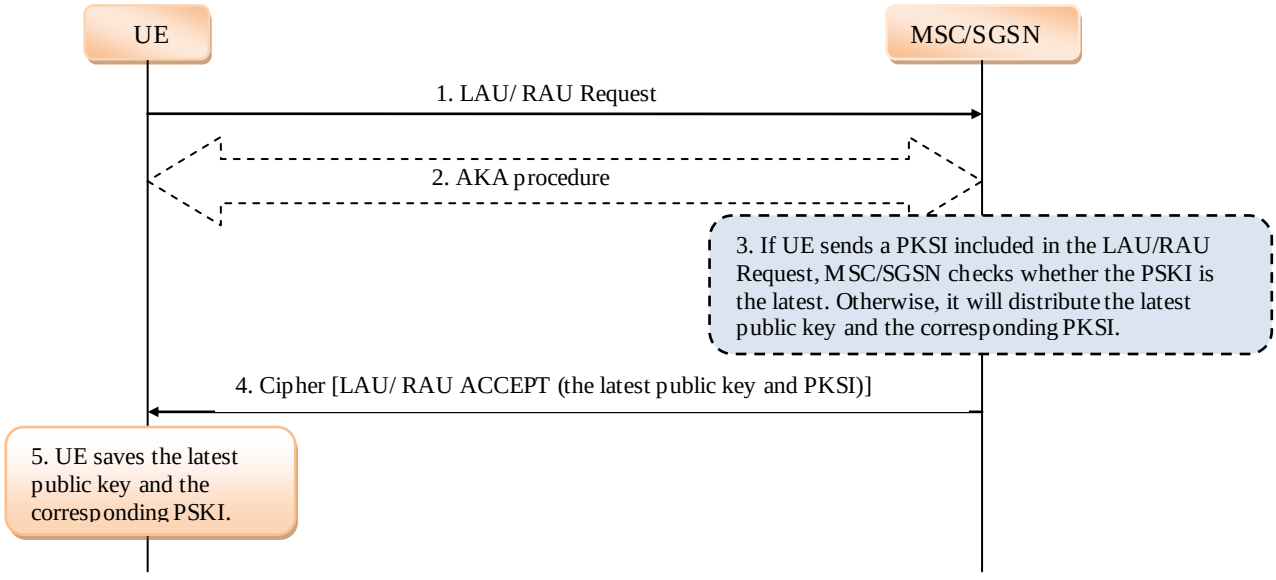


Figure 7.4.2.3.1: Distribution of public key information in GSM/GPRS

In the initial LAU/RAU procedure, UE sends the LAU/RAU request. When MSC/SGSN receives the LAU/RAU request, MSC/SGSN sends LAU/RAU Accept message to UE. In the LAU/RAU Accept, the latest public key and PKSI are included. MSC/SGSN encrypts the LAU/RAU Accept message with Kc. And the PWS public key and PKSI are protected. When UE receives LAU/RAU Accept message, it decrypts the LAU/RAU Accept message to achieve the latest public key and PKSI, saves the latest public key and PKSI.

If UE has attached to the network before, UE can send the public key identifier to the network entity in LAU/RAU. MSC/SGSN checks whether the PSKI is the latest. Otherwise, it will distribute the latest public key and the corresponding PKSI. When UE receives LAU/ RAU ACCEPT, it saves the latest public key and PKSI.

Only cipher LAU/ RAU ACCEPT with UP still remaining unencrypted:

In common views, it cannot only mandate ciphering LAU/RAU one procedure and leave others and UP without ciphering since once ciphering is turned on, it is better not to be turned off for security reasons. If operator does not want to turn on ciphering according to local policy, a possible alternative can be that SGSN/MSC mandates ciphering when performing RAU/LAU procedure for distributing public key. If SGSN/MSC decided to carry PWS public in RAU/LAU accept message, we use the current GSM security to cipher LAU/RAU accept message carrying with PWS public key. Normally, after that, UE will release RRC connection and be in idle mode. In the next session, UE connects to the network and MSC/SGSN sends cipher mode command with turning off ciphering in Cipher Mode Command setting to the UE when local policy is remaining UP unencrypted. Please note that above solution needs some changes in SGSN/MSC. In addition, there may be a possibility that cipher algorithms are disabled in BSS, i.e. BSS does not support any cipher algorithms, if cipher is not allowed by local policies. If it is the case, BSS should also be modified.

Not initiating ciphering in the whole GSM/GPRS system:

In case that operator will not initiate ciphering anyhow in GSM/GPRS, it is suggested to send PWS public key and identifier directly without ciphering in LAU/ RAU ACCEPT message. To some extent, it can also ensure that UE will get public key to verify the signature than without doing any security to PWS in GSM/GPRS.

7.4.3 Enhanced integrity protection mechanism for GSM /GPRS

- Generate the integrity key based on the current GSM security. Kc is the encrypted key which generate from GSM AKA, Kmac is the integrity key used in PWS generated from Kc. Then Kmac can be used to protect PWS public key. Note that in this solution it is not restricted integrity mechanism only for PWS, it can be used in the whole system if operator want to enhance the security in the whole system.
- Key Derivation method directly:
  - Kmac is derived from Kc.It can be generated as follows:
  - Kmac=KDF [Kc, S], S=Fc||P||L, Fc=0x14, P=UE id, L= the length of UE id
- The configuration of the integrity algorithm.
  - Pre- configured the integrity algorithm in MS and network node.
  - Distribution the integrity algorithm to MS from network. When the integrity key is generated, the integrity algorithm or the algorithm identity indication can be distributed with protection.

In GSM, integrity algorithm and PWS public key can be integrity protected with Cipher mode CMD message. The integrity key Kmac is generated with the method discussed above. The procedure is shown in Figure 7.4.3.1.

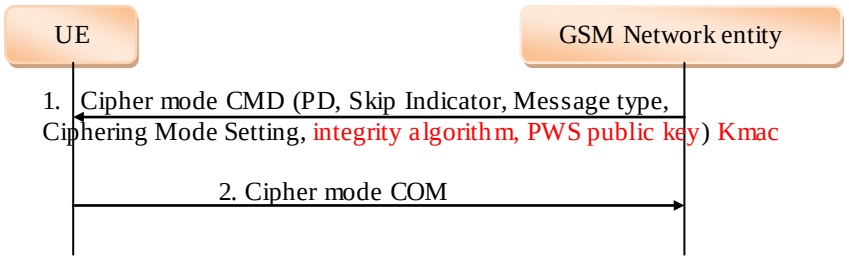


Figure 7.4.3.1: Distribution of public key information in GSM

In GPRS, integrity algorithm and PWS public key can be integrity protected within Authentication and Ciphering Request message. The integrity key Kmac is generated with the method discussed above. The procedure is shown in Figure 7.4.3.2.

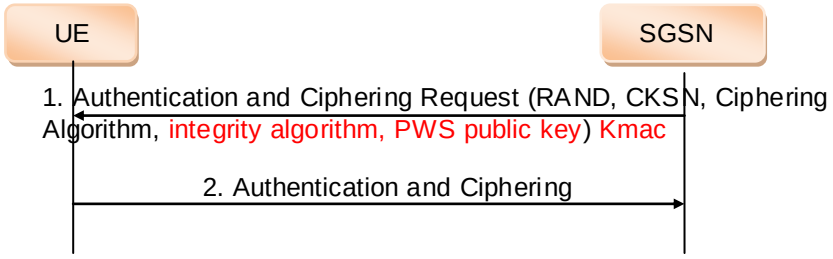


Figure 7.4.3.2: Distribution of public key information in GPRS

7.4.4 Limiting key updates in GSM/GPRS

If the protection of the key distribution in GSM/GPRS has a lower security level (or no security) than the protection of the key distribution in the other accesses, this lower security level might spread to UMTS or LTE capable UEs if they listen for key distribution messages in GSM/GPRS.

The reason being than an UMTS or LTE capable UEs might attach to a GMS network when there is no UMTS or LTE coverage. Even if the UE is configured to discard messages without a valid signature, an adversary could potentially inject false keys and false warning messages in an attempt to cause panic.

- For GSM only UEs, the only solution is to introduce some kind of enhanced GSM/GPRS security context. Making such a large change to existing GSM/GPRS networks seems unjustified just for PWS.
- For UMTS or LTE capable UEs, the problem could be mitigated by only accept key distribution messages in GSM/GPRS is there is no valid key received from UMTS/LTE. If the same signature key is used in all accesses, improved robustness and coverage could still be achieved by listen for warning messages in GSM networks.

As a subscriber with an UMTS or LTE capable UEs could have GSM only coverage for weeks (e.g. when going on vacation), this puts some extra requirements on the key distribution methods. The lifetime of the signature keys would need to be at least as long as the time an subscriber might have GSM only coverage.

Editor's Note: It is FFS if there are regulatory requirements to accept key distribution messages in accesses where the user does not have a subscription.

7.5 Evaluation of different solutions

Solution 1 can support country roaming.

8 Conclusion

Editor's Note: This section aims to give a conclusion of the solution of PWS.

Annex<X>: Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
2012-06					*Initial TR version*	*---*	*0.0.1*