3GPP TSG SA WG3 Security — S3#19 **S3-010323**

3 - 6 July, 2001

Newbury, UK

Source: AT&T Wireless

Title: Network Configuration Independence Mechanism

Document for: Approval

1 Introduction

During the last S3 meeting in Phoenix a new work item "Security Aspects of Requirement for Network Configuration Independence" was approved. This contribution addresses the Security needs of Configuration Independence (aka Network Hiding). It includes mechanisms needed to route SIP requests and responses, ensuring that information about the S-CSCF is not provided to those not authorized to receive it. A CR to 23.228 is proposed.

2 Discussion

Network Configuration Independence requirement is stated in TS23.228 as follows:

It is a requirement that it shall be possible to hide the network topology from other operators. It shall be possible to restrict the following information from being passed outside of an operator's network: exact number of S-CSCFs, capabilities of S-CSCFs, or capacity of the network.

The design for Configuration Independence has been discussed in both SA2 and CN1. The mechanism being studied is to encrypt the S-CSCF address in SIP Via, Record-Route, Route, and Path headers at an I-CSCF, and then decrypt them in handling the response to the SIP request. Further, the routing information given to P-CSCF during Registration may contain encrypted information, which would be decrypted by an I-CSCF in handling a SIP request.

Depending on the operator's configuration, the I-CSCF that encrypts the aforementioned headers may or may not be the same I-CSCF that needs to decrypt the information; all I-CSCFs of an operator should have the ability to decrypt each other's data. In the simplest conceivable implementation, all I-CSCFs share a key, which is distributed by whatever provisioning mechanisms already exist for the purposes of setting up security-related information on the CSCFs. This key could also be established by running any number of shared-key generation protocols. This key, which we shall call Kv, will need to be regenerated periodically. When that happens, the previous key is also kept for a small fraction of the key lifetime in case there are still sessions using the old key. With a modern algorithm such as AES, with a 128-bit block and a 256-bit key, there is no real reason to ever rekey during the lifetime of the system, unless, of course, the key gets compromised or otherwise exposed.

The information to be encrypted is appended with a random 128-bit Initialization Vector, and padded to a multiple of 128 bits. The information is encrypted and MAC-protected with a block cipher (e.g., AES), in CBC-MAC mode. One of the proposed new modes for AES is a one-pass integrity-protection and encryption mode, and that should be used once it is standardized by NIST. All this is base-64 encoded and transmitted as a single entry in the header. This information is treated opaquely by the other CSCFs. When an I-CSCF receives this opaque header, it decrypts it with the shared key, verifies the integrity, and reconstructs the headers.

The IV shall be a random number; it cannot be a counter, because multiple CSCFs are using the same key. With a random value and a 128-bit IV, the probability of two CSCFs picking the same IV is roughly 2^{-64}, which is more than adequate. The information does not need to be authenticated, as the threat model does not include malicious tampering of its contents; what is being protected is the identities of all the CSCFs of the home network.

3 Proposal

It is proposed that SA3 endorse the encryption based mechanism as a method of implementing the network configuration independence requirement and that a LS to be sent to S2 with the following CR to TS23.228.

CR-Form-v3

CHANGE REQUEST

⌘ **23.228 CR xx** ⌘ rev ⌘ Current version: **5.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Network Configuration Independence
Source:	⌘	AT&T Wireless
Work item code:	⌘	1515
Date:	⌘	07.07.2001
Category:	⌘	**C**
Release:	⌘	REL-5

Use one of the following categories:
- ***F*** *(essential correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(Addition of feature),*
- ***C*** *(Functional modification of feature)*
- ***D*** *(Editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change:	⌘	The mechanism for Network Configuration Independence was left open in TS23.228. This CR proposes the encryption-based method for Network Configuration Independence, and contains the necessary changes to be applied to the Registration flows in TS23.228.
Summary of change:	⌘	This CR modifies the registration flows to reflect the encryption-based method for Network Configuration Independence requirement.
Consequences if not approved:	⌘	

Clauses affected:	⌘	5.2.2.3 and 5.2.2.4
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

5.2.2.3 Registration information flow – User not registered

The application level registration can be initiated after the registration to the access is performed, and after IP connectivity for the signalling has been gained from the access network. For the purpose of the registration information flows, the subscriber is considered to be always roaming. For subscribers roaming in their home network, the home network shall perform the role of the visited network elements and the home network elements.

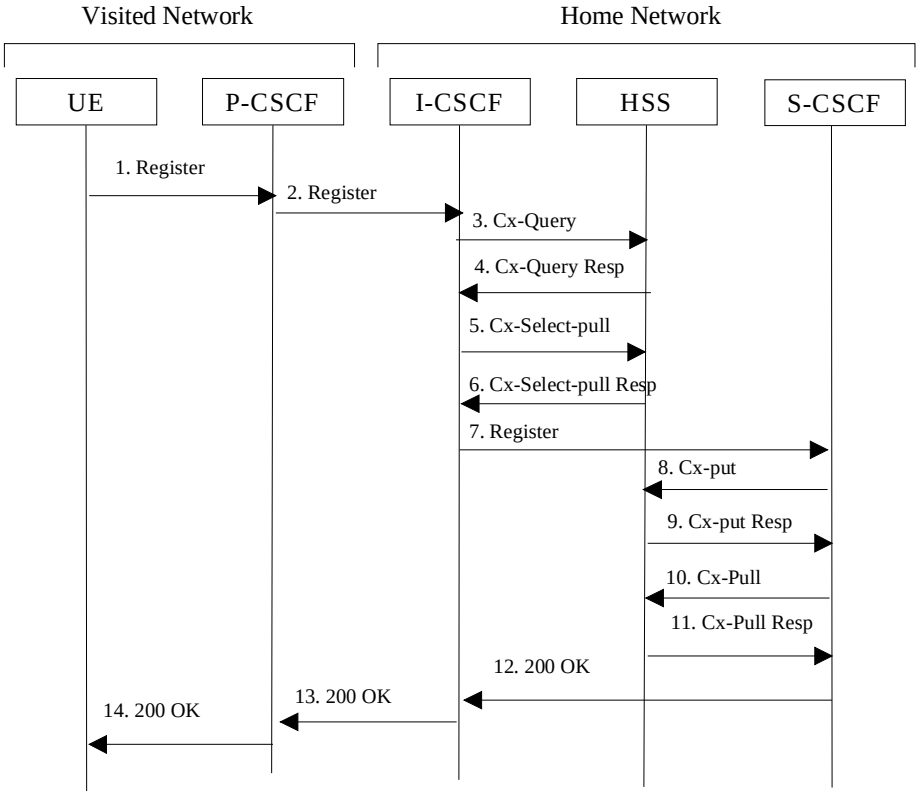

Figure 5.1: Registration – User not registered

1. After the UE has obtained a signalling channel through the access network, it can perform the IM registration. To do so, the UE sends the Register information flow to the proxy (subscriber identity, home networks domain name).

2. Upon receipt of the register information flow, the P-CSCF shall examine the “home domain name” to discover the entry point to the home network (i.e. the I-CSCF). The proxy shall send the Register information flow to the I-CSCF (P-CSCFs name, subscriber identity, visited network contact name).

A name-address resolution mechanism is utilised in order to determine the address of the home network from the home domain name. When the I-CSCF receives the registration information flow from the proxy, it shall examine the subscriber identity and the home domain name, and employ the services of a name-address resolution mechanism, to determine the HSS address to contact.

3. The I-CSCF shall send the Cx-Query information flow to the HSS (subscriber identity, visited domain name). The P-CSCF name is the contact name that the operator wishes to use for future contact to that P- CSCF. The HSS shall check whether the user is registered already. The HSS shall indicate whether the user is allowed to register in that visited network according to the User subscription and operator limitations/restrictions if any.

4. Cx-Query Resp is sent from the HSS to the I-CSCF. If the checking in HSS was not successful the Cx-Query Resp shall reject the registration attempt.

5. At this stage, it is assumed that the authentication of the user has been completed (although it may have been determined at an earlier point in the information flows). The I-CSCF shall send Cx-Select-Pull (subscriber identity) to the HSS to request the information related to the required S-CSCF capabilities which shall be input into the S-CSCF selection function.

6. The HSS shall send Cx-Select-Pull Resp (required S-CSCF capabilities) to the I-CSCF.

7. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism. I-CSCF also determines the name of a suitable home network contact point, possibly based on information received from the HSS. The home network contact point may either be the S-CSCF itself, or a suitable I-CSCF in case network configuration hiding is desired. If an I-CSCF is chosen as the home network contact point, it may be distinct from the I-CSCF that appears in this registration flow, and it will be capable of decrypting the S-CSCF name from the home contact information. I-CSCF shall then send the register information flow (P-CSCFs name, subscriber identity, visited network contact name, home network contact point in case network configuration hiding is desired) to the selected S-CSCF. The home network contact point will be used by the P-CSCF to forward session initiatation signalling to the home network.

8. The S-CSCF shall send Cx-Put (subscriber identity, S-CSCF name) to the HSS. The HSS stores the S-CSCF name for that subscriber.

9. The HSS shall send Cx-Put Resp to the I-CSCF to acknowledge the sending of Cx-Put.

10. On receipt of the Cx-Put Resp information flow, the S-CSCF shall send the Cx-Pull information flow (subscriber identity) to the HSS in order to be able to download the relevant information from the subscriber profile to the S-CSCF. The S-CSCF shall store the P-CSCFs name, as supplied by the visited network. This represents the name that the home network forwards the subsequent terminating session signalling to for the UE.

11. The HSS shall return the information flow Cx-Pull Resp (user information) to the S-CSCF. The user information passed from the HSS to the S-CSCF shall include one or more names/addresses information which can be used to access the platform(s) used for service control while the user is registered at this S-CSCF. The S-CSCF shall store the information for the indicated user. In addition to the names/addresses information, security information may also be sent for use within the S-CSCF.

12. The S-CSCF shall return the 200 OK information flow (serving network contact information) to the I-CSCF. If an I-CSCF is chosen as the home network contact point, the I-CSCF shall encrypt the S-CSCF address in the serving network contact information.

13. The I-CSCF shall send information flow 200 OK (serving network contact information) to the P-CSCF. The I-CSCF shall release all registration information after sending information flow 200 OK.

14. The P-CSCF shall store the serving network contact information, and shall send information flow 200 OK to the UE.

5.2.2.4 Re-Registration information flow – User currently registered

Editor's Note: the definition of re-registration timers requires further study, however it is noted that the timers in the UE are shorter than the registration related timers in the network.

Periodic application level re-registration is initiated by the UE either to refresh an existing registration or in response to a change in the registration status of the UE. Re-registration follows the same process as defined in subclause 5.2.2.3 "Registration Information Flow – User not registered".

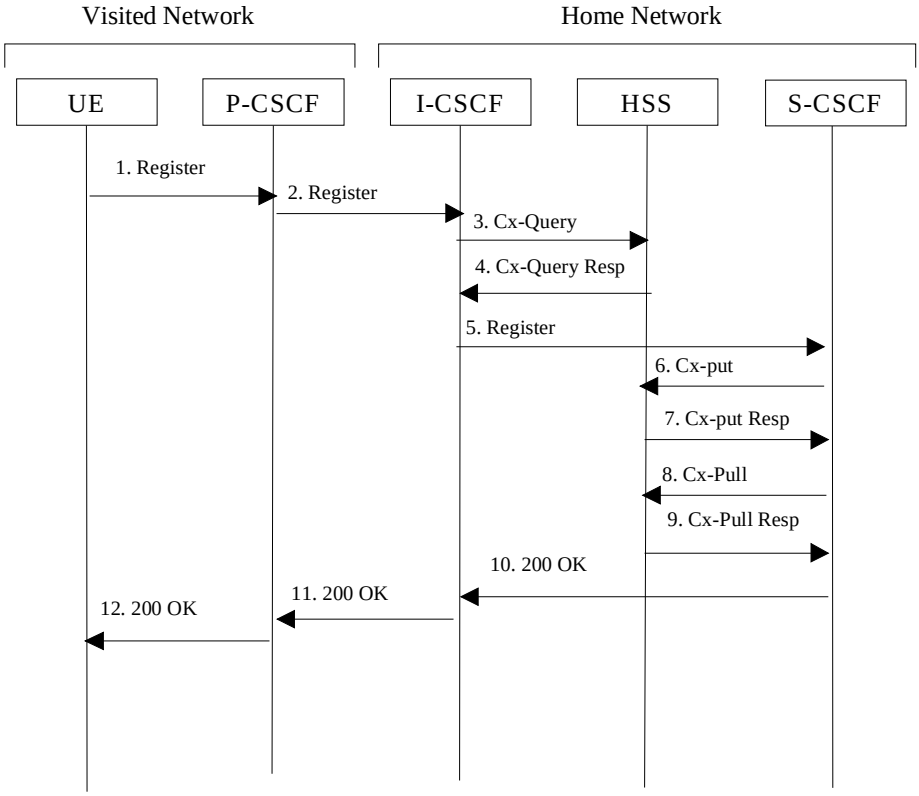

Figure 5.2: Re-registration - user currently registered

1. Prior to expiry of the agreed registration timer, the UE initiates a re-registration. To re-register, the UE sends a new REGISTER request. The UE sends the REGISTER information flow to the proxy (subscriber identity, home networks domain name).

2. Upon receipt of the register information flow, the P-CSCF shall examine the "home domain name" to discover the entry point to the home network (i.e. the I-CSCF). The proxy does not use the entry point cached from prior registrations. The proxy shall send the Register information flow to the I-CSCF (P-CSCFs name, subscriber identity, visited network contact name). A name-address resolution mechanism is utilised in order to determine the address of the home network from the home domain name. When the I-CSCF receives the registration information flow from the proxy, it shall examine the subscriber identity and the home domain name, and employ the services of a name-address resolution mechanism, to determine the HSS address to contact.

3. The I-CSCF shall send the Cx-Query information flow to the HSS (subscriber identity, visited domain name).

4. The HSS shall check whether the user is registered already and return an indication indicating that an S-CSCF is assigned. The Cx-Query Resp (indication of entry contact point, e.g. S-CSCF) is sent from the HSS to the I-CSCF.

5. At this stage, it is assumed that the authentication of the user has been completed (although it may have been determined at an earlier point in the information flows). The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism. I-CSCF also determines the name of a suitable home network contact point, possibly based on information received from the HSS. The home network contact point may either be the S-CSCF itself, or a suitable I-CSCF in case network configuration hiding is desired. If an I-CSCF is chosen as the home network contact point, it may be distinct from the I-CSCF that appears in this registration flow, and it will be capable of decrypting the S-CSCF name from the home contact information. I-CSCF shall then send the register information flow (P-CSCFs name, subscriber identity, visited network contact name, home network contact point in case network configuration hiding is desired) to the selected S-CSCF. The home network contact point will be used by the P-CSCF to forward session initiatation signalling to the home network.

6. The S-CSCF shall send Cx-Put (subscriber identity, S-CSCF name) to the HSS. The HSS stores the S-CSCF name for that subscriber. Note: Optionally as an optimisation, the S-CSCF can detect that this is a re-registration and omit the Cx-Put request.

7. The HSS shall send Cx-Put Resp to the S-CSCF to acknowledge the sending of Cx-Put.

8. On receipt of the Cx-Put Resp information flow, the S-CSCF shall send the Cx-Pull information flow (subscriber identity) to the HSS in order to be able to download the relevant information from the subscriber profile to the S-CSCF. The S-CSCF shall store the P-CSCFs name, as supplied by the visited network. This represents the name that the home network forwards the subsequent terminating session signalling to for the UE. Note: Optionally as an optimisation, the S-CSCF can detect that this a re-registration and omit the Cx-Pull request.

9. The HSS shall return the information flow Cx-Pull-Resp (user information) to the S-CSCF. The S-CSCF shall store the user information for that indicated user.

10. The S-CSCF shall return the 200 OK information flow (serving network contact information) to the I-CSCF. If an I-CSCF is chosen as the home network contact point, the I-CSCF shall encrypt the S-CSCF address in the serving network contact information.

11. The I-CSCF shall send information flow 200 OK (serving network contact information) to the P-CSCF. The I-CSCF shall release all registration information after sending information flow 200 OK.

12. The P-CSCF shall store the serving network contact information, and shall send information flow 200 OK to the UE.