
3GPP TSG SA WG3 Security — S3#17

S3-010034

27 February - 02 March, 2001

Gothenburg, Sweden

3GPP TSG CN1/SA2 Joint meeting
13-15 February, 2001
New Jersey/USA

Tdoc N1-010268

Title: LS on Security implications of supporting "hiding"

Source: TSG-CN1/SA2 SIP ad hoc

TO ⁽¹⁾: TSG-SA2, TSG-SA3

WI: SIP Call Control Protocol for the IM Subsystem

Contact Person:

Name: Sonia Garapaty, Nortel Networks

E-mail Address: sonia.garapaty@nortelnetworks.com

Attachments: N1-010267

(Please list documents numbers to be attached)

Date: 15 February 2001

TSG-CN1 has agreed the principles in the attached document N1-010267, which describes the usage of a new SIP Path header and a token mechanism to support "hiding" or "network configuration independence".

TSG-CN1 ask TSG-SA2 and SA3 to look into the security implications for supporting such a mechanism.

If the proposal is agreed then SA2 and SA3 are invited to study the impact on their documents under its control (changes on 23.228 are expected).

¹ Please write any action required from the groups in a clear way.

Agenda Item: 5.2

WI / Topic: SIP Call Control Protocol for the IM Subsystem

Source: Nokia, AT&T, Lucent, Nortel Networks

Title: The usage of Path Header

Effected Specifications / Releases: 23.228 / 24.228

Document for: Discussion/Approval

Date: 14 February 2001

1. Introduction

This contribution is a revised contribution of Tdoc N1-010089 agreed to be put in the annex in the N1 Beijing meeting, and Tdoc N1-010261 agreed in S2/N1 joint meeting, New Jersey.

This contribution makes the following changes to the N1-010089 document:

- It defines a token concept.
- It updates the usage of the Path header, which will be inserted in the Register message by the Proxy CSCF (instead of the I-CSCF as proposed earlier). Proxy CSCF will add its own contact point name to this header and based on the requirements for network hiding of the operator, the I-CSCF may or may not add its or another suitable I-CSCF contact point name to the Path header.
- S-CSCF will store the Call path information from the Path header and will use it to route the subsequent terminating requests successfully to the Proxy CSCF. This makes unnecessary for the proxy to modify the contact header in register messages.

2. Proposal

It is proposed to introduce a new SIP header for conveying serving network information to the P-CSCF during registration phase. The P-CSCF shall then use this serving network information when routing the originating session initiation requests to S-CSCF.

The S-CSCF shall store the path information from the Path header and use when routing the terminating requests to the P-CSCF.

Furthermore, it is proposed to use a simpler and flexible token concept, which only has significance to the home network that supplies the token. The token could be used to transport an encrypted S-CSCF name, another representation of the S-CSCF name, or simply a pointer to where the S-CSCF name can be found to hide the serving network configuration. To conform to SIP message encoding, this token is a cryptographically random alphanumeric representation.

3. Discussion

According to 3G TS 23.228 it shall be possible for a network operator to hide its serving network configuration, and maintain only a few contact points for outside networks. This possibility is given by optionally having an I-CSCF as the contact point for all incoming requests in the serving network.

During registration the S-CSCF name is to be conveyed to the P-CSCF, at the same time the serving network operator may want to hide the S-CSCF name from the visited network operator. The solution proposed here is to have the I-CSCF of the serving network translate the S-CSCF name into a token, and provide this token along

with the I-CSCF name to the P-CSCF. P-CSCF shall then store both of these network element names, and associate it with the subscriber under registration. This information will then be used to route this subscriber's subsequent originating requests successfully to the S-CSCF.

The serving network information (S-CSCF name, and possible I-CSCF name) is proposed to be conveyed in a new SIP header of the REGISTER transaction. This new header is called the Path header (as introduced by Tdoc N1-001243) which is to be filled during the REGISTER request in similar fashion as the Record-Route header of an INVITE. If the serving network configuration is to be hidden, then

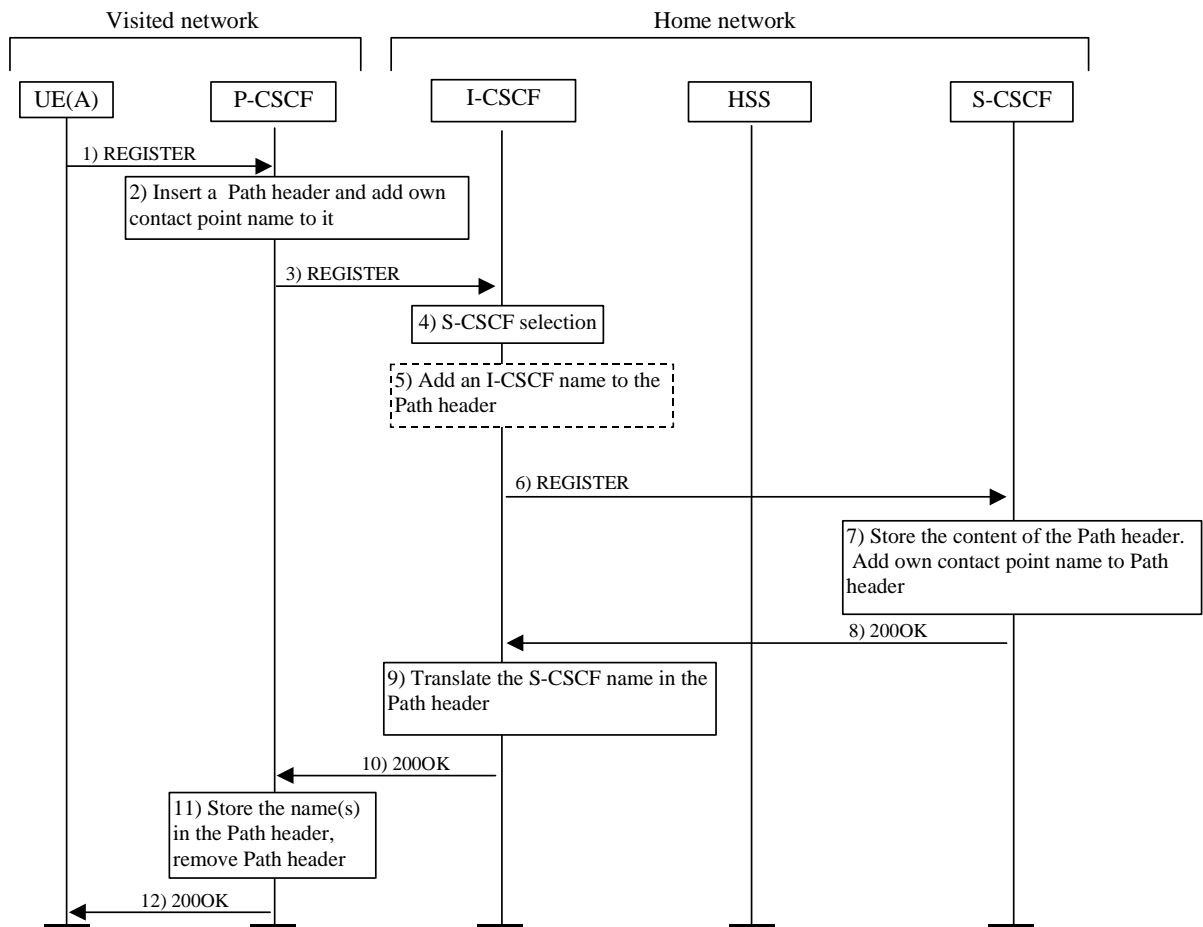
- a.) the I-CSCF should add its name or the name of a suitable I-CSCF to the Path header of the REGISTER request, and
- b.) the S-CSCF name in the Path header of the 200OK response should be translated by the I-CSCF into a token.

The token concept has the following benefits:

- Removes the need to standardise security algorithms and key exchange mechanisms
- Removes the need to perform encryption/decryption at the I-CSCF, which may result in additional call processing delay (depending on the strength of the encryption).
- Allows the option for innovative solutions to meet the hiding requirement.

The proposed mechanism is explained in the example below, inclusive hiding of the serving network configuration:

Annex A



1) UE(A) initiates registration procedure:

```

REGISTER      home_a.com SIP/2.0
Via:          SIP/2.0/UDP 12.34.56::EF:5060
From:         User_A <sip:ue_a@home_a.com>
To:          User_A <sip:ue_a@home_a.com>
Call-Id:     12345@ue_a.home_a.com
Cseq:        1 REGISTER
Contact:     User_A <sip:ue_a@12.34.56::EF:5060>
  
```

2) The P-CSCF inserts a Path header, adds own name to it.

3) P-CSCF forwards the registration request to the contact point of the home network:

```

REGISTER      home_a.com SIP/2.0
Via:          SIP/2.0/UDP p_cscf.visited_a.com
Via:          SIP/2.0/UDP 12.34.56::EF:5060
Path:         <sip:p_cscf.visited_a.com>
From:         User_A <sip:ue_a@home_a.com>
To:          User_A <sip:ue_a@home_a.com>
Call-Id:     12345@ue_a.home_a.com
Cseq:        1 REGISTER
Contact:     Visited network contact name
  
```

4) The I-CSCF selects a suitable S-CSCF for the subscriber.

5) Based on the requirements for network hiding of the operator, the I-CSCF may or may not add its or other suitable I-CSCF contact point name to the Path header.

6) I-CSCF forwards the registration request to the selected S-CSCF:

```
REGISTER           home_a.com SIP/2.0
Via:                SIP/2.0/UDP i_cscf.home_a.com
Via:                SIP/2.0/UDP p_cscf.visited_a.com
Via:                SIP/2.0/UDP 12.34.56::EF:5060
Path:               <sip:i_cscf.home_a.com>
Path:               <sip: p_cscf.visited_a.com >
From:               User_A <sip:ue_a@home_a.com>
To:                 User_A <sip:ue_a@home_a.com>
Call-Id:            12345@ue_a.home_a.com
Cseq:               1 REGISTER
Contact:            Visited network contact name
```

7) S-CSCF stores the information in the Path header, then adds its own name to it.

8) S-CSCF sends a 200 OK response to the registration request to I-CSCF:
Note: When network hiding is not required I-CSCF will not add own name to the Path header in step 5, thus this message will be forwarded directly to P-CSCF.

```
SIP/2.0 200OK
Via:                SIP/2.0/UDP i_cscf.home_a.com
Via:                SIP/2.0/UDP p_cscf.visited_a.com
Via:                SIP/2.0/UDP 12.34.56::EF:5060
Path:               <sip:s_cscf.home_a.com>
Path:               <sip:i_cscf.home_a.com>
Path:               <sip: p_cscf.visited_a.com >
From:               User_A <sip:ue_a@home_a.com>
To:                 User_A <sip:ue_a@home_a.com>
Call-Id:            12345@ue_a.home_a.com
Cseq:               1 REGISTER
```

9) To achieve network configuration hiding, the I-CSCF translates the S-CSCF name (the topmost path header) into a token.

10) I-CSCF forwards the 200OK response to the P-CSCF:

```
SIP/2.0 200OK
Via:                SIP/2.0/UDP p_cscf.visited_a.com
Via:                SIP/2.0/UDP 12.34.56::EF:5060
Path:               <sip:token(s_cscf.home_a.com)>
Path:               <sip:i_cscf.home_a.com>
Path:               <sip: p_cscf.visited_a.com >
From:               User_A <sip:ue_a@home_a.com>
To:                 User_A <sip:ue_a@home_a.com>
Call-Id:            12345@ue_a.home_a.com
Cseq:               1 REGISTER
```

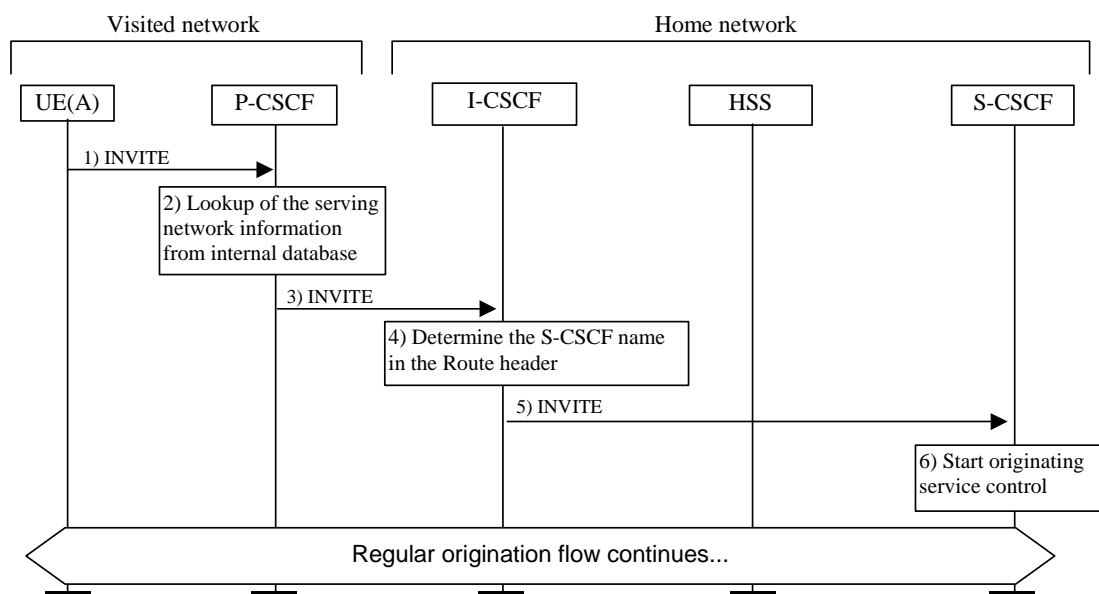
11) P-CSCF stores the names from the Path header (except the last one) and associates it with UE(A).

12) P-CSCF removes the Path header from the 200OK response, and forwards the response to UE(A):

```
SIP/2.0 200OK
Via:                SIP/2.0/UDP 12.34.56::EF:5060
```

From: User_A <sip:ue_a@home_a.com>
To: User_A <sip:ue_a@home_a.com>
Call-Id: 12345@ue_a.home_a.com
Cseq: 1 REGISTER

An example origination flow with network hiding enabled is shown below:



- 1) UE(A) initiates the establishment of a new session, accordingly sends an INVITE request to P-CSCF:

```

INVITE          ue_b@home_b.com SIP/2.0
Via:            SIP/2.0/UDP 12.34.56::EF:5060
From:           User_A <sip:ue_a@home_a.com>
To:             User_B <sip:ue_b@home_b.com>
Call-Id:        12345@ue_a.home_a.com
Cseq:           1 INVITE
  
```

- 2) P-CSCF looks up the serving network information for the subscriber that was stored during registration. A Route header is inserted into the INVITE request, its content is generated based on the stored serving network information.

- 3) P-CSCF forwards the session initiation request to the element specified in the stored serving network information. Accordingly, the request is forwarded to the I-CSCF, and the token is inserted as a Route header into the request:

```

INVITE          ue_b@home_b.com SIP/2.0
Via:            SIP/2.0/UDP p_cscf.visited_a.com
Via:            SIP/2.0/UDP 12.34.56::EF:5060
Route:          <sip: token(s_cscf.home_a.com)>, <called party name>
From:           User_A <sip:ue_a@home_a.com>
To:             User_B <sip:ue_b@home_b.com>
Call-Id:        12345@ue_a.home_a.com
Cseq:           1 INVITE
  
```

- 4) I-CSCF determines the S-CSCF name using the token in the Route header field to retrieve the routing information.

- 5) I-CSCF forwards the session initiation request to S-CSCF:

INVITE s_cscf.home_a.com SIP/2.0
Via: SIP/2.0/UDP i_cscf.home_a.com
Via: SIP/2.0/UDP p_cscf.visited_a.com
Via: SIP/2.0/UDP 12.34.56::EF:5060
Route: <sip:called party name>
From: User_A <sip:ue_a@home_a.com>
To: User_B <sip:ue_b@home_b.com>
Call-Id: 12345@ue_a.home_a.com
Cseq: 1 INVITE

- 6) S-CSCF starts originating service control for UE(A), and the call will proceed according to regular procedures.