P-CSCF Security Mechanisms

In this section:

Related articles:

- SIP Security Profile - CLI
- SIP Trunk Group - Services - CLI
- SIP Trunk Group - Signaling - CLI
- Show Status Address Context - Zone
- SIP TG - Signaling - Access Class - CLI
- SIP TG - Signaling - NASS IMS Auth - CLI
- Service Profiles - Sip Security Profile (EMA)
- SIP Trunk Group - Services (EMA)
- SIP Trunk Group - Signaling (EMA)

P-CSCF Security Mechanisms

P-CSCF security is established during the Registration process. A security mechanism is chosen based on the Security-Client header information (currently ipsec-3gpp) which is used between UE and P-CSCF.

The following security mechanism options are available:

- IPsec with IMS AKA
- SIP Digest with TLS
- SIP Digest without TLS
- Background
- Authentication Algorithm

The Security Mechanism Criteria table below illustrates the SIP headers and parameter values corresponding to the security mechanisms employed through the P-CSCF. For example, when UE sends a Register request with following parameters, IPsec with AKA is employed:

- Authorization Header indicating Digest with an algorithm of AKA
- Security-Client Header indicating ipsec-3gpp
- Proxy-Require Header indicating sec-agree
- Require Header indicating sec-agree

Table 1: Security Mechanism Criteria

If...				Then PCSCF selects:
Security-Client Hdr contains	**Require and Proxy-Require Hdrs contain**	**Authorization Hdr is present**	**Access Type**	
3gpp-ipsec	sec-agree	✓	-	IMS AKA
tls	sec-agree	✓	-	SIP Digest with TLS
✗	✗	✓	3GPP Access	GIBA
✗	✗	✗	3GPP Access	SIP Digest w/o TLS
✗	✗	✓	-	SIP Digest w/o TLS
✗	✗	✗	-	SIP Digest w/o TLS

Once the Registration process completes and the security associations are established between UE and the SBC, all subsequent messages received from UE must occur over the secure channel if IPsec or TLS is enabled on the received socket. A flag stored in the RCB (Registration Control Block) indicates the Registration is secure. All subsequent messages not received on a secure socket that associate to a secure Registration (except for emergency calls and certain Register requests) are rejected with '488 Not Acceptable Here' message.

The CLI syntax to configure a `sipSecurityProfile` and assign it to a SIP trunk group is shown below:

> **Note**
> When configuring a SIP Security Profile in P-CSCF mode, a Sip Security Mechanism is required.

```
% set profiles services sipSecurityProfile <profile_name>
 forceClientSecurityPref <disabled | enabled>
 rejectSecUnsupportedRequest <disabled | enabled>
 sbxSecMode <sbc-only | sbc-pcscf>
 sipSecurityMechanism <ipsec-3gpp / tls precedence <1-65535>

% set addressContext <addressContext name> zone <zone name> sipTrunkGroup <TG_NAME> services
sipSecurityProfile <profile name>
```

If `forceClientSecurityPref` is enabled, while selecting the Security Mechanism to be applied, precedence is given to the order of occurrence of "mechanism-name" values in the "Security-Client" header.

If `rejectSecUnsupportedRequest` is enabled, the incoming REGISTER is rejected when it does not contain "sec-agree" header value (in Require or Proxy-Require headers) or it does not contain any supported mechanism-name (ipsec-3gpp) in "Security-Client" header. Otherwise, processing continues using "Digest without TLS" security mechanism.

The security mechanism precedence value (range: 1-65535) specifies the precedence to assign a security mechanism. A lower value represents a higher precedence.

IPsec with IMS AKA

IMS AKA (Authentication and Key Agreement) authentication ensures all traffic between UE and P-CSCF during a session is sent on IPsec-protected channels.

The UE starts the AKA session registration process on an unprotected channel. During registration, the AKA mechanism establishes two IPsec protected channels between the UE and the P-CSCF.

Implementing IPsec AKA security involves configuring one or more IMS Security Profiles (maximum of 10), and then assigning the profiles to specific SIP trunk groups. Key features include:

- IMS Security Profiles may be modified or added without affecting services.
- An IMS Security Profile object may be deleted as long as it is not referenced by any SIP Trunk Group.
- The precedence object can be configured to prioritize the application of security-mechanism when more than one option is available.

Example CLI commands:

```
% set profiles services sipSecurityProfile S-PROFILE1 forceClientSecurityPref enabled
rejectSecUnsupportedRequest enabled sipSecurityMechanism ipsec-3gpp precedence 1

% set addressContext default zone MYZONE sipTrunkGroup STG-1 services sipSecurityProfile S-PROFILE1
```

Table 2: Maximum Number of Registered Subscribers on IMS AKA

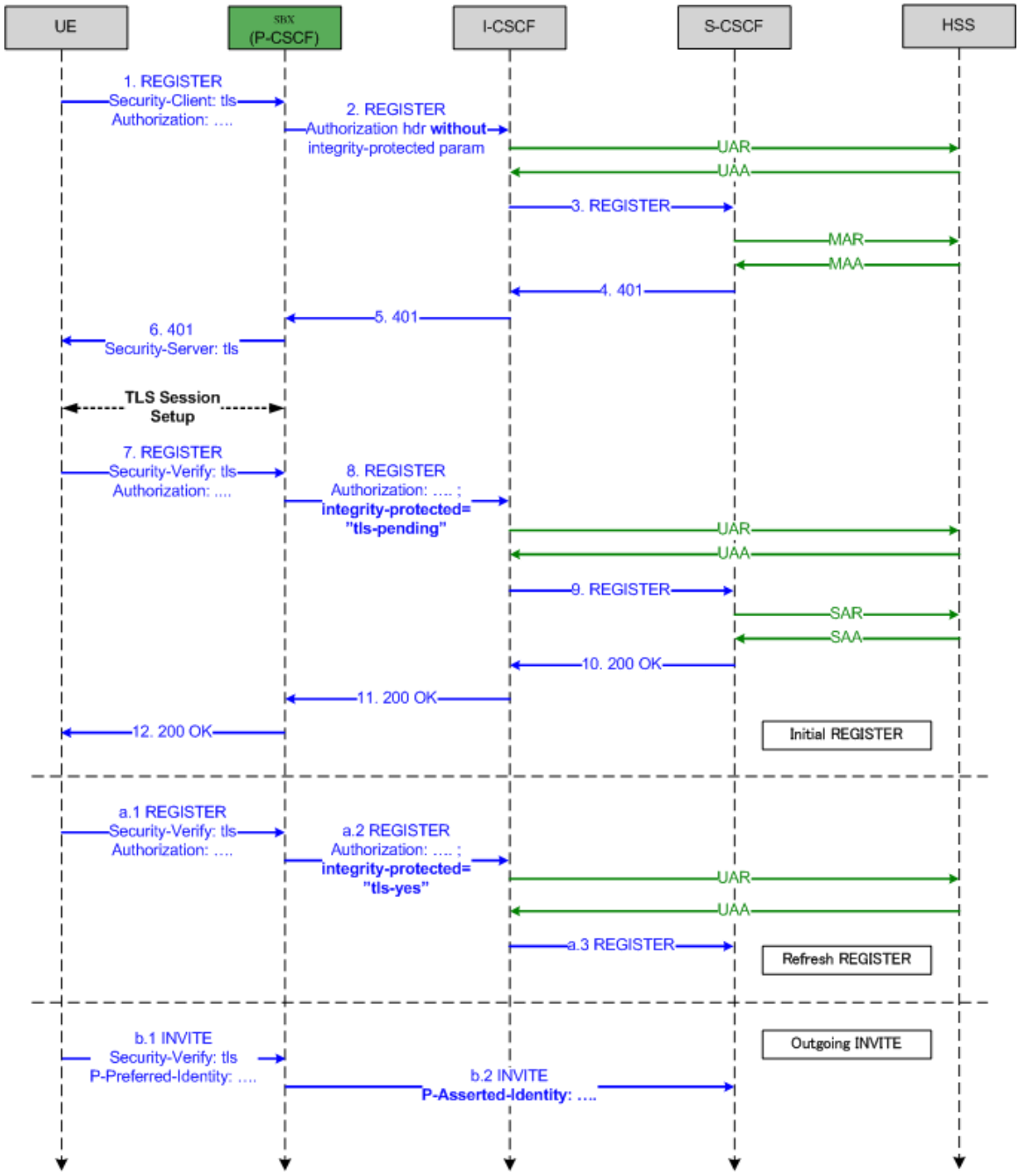
Platform	Max Number Registered Subscribers
SBC 51x0	100,000
SBC 52x0	256,000
SBC 7000	1 million
SBC SWe	100,000

SIP Digest with TLS

The SBC as P-CSCF supports TLS over TCP as a transport towards IMS UE as per 3GPP TS 33.203. Whether to use IPsec or TLS towards the IMS UE is negotiated at the time of registration.

A typical call flow when using "tls" as the security mechanism is show below with a brief explanation following the table.

Figure 1: SIP Digest with TLS



Call Flow Summary:
• UE determines to use TLS for registration and proposes a security-mechanism of "tls" in the Security-Client header in the initial REGISTER. This is sent unprotected towards the P-CSCF. UE includes all the other standard SIP/IMS headers including Authorization header as described in 3GPP TS 24.229. • P-CSCF forwards the same to S-CSCF with no "integrity-protected" parameter in Authorization header. • S-CSCF challenges the UE and P-CSCF forwards the 401 response towards UE. P-CSCF adds Security-Server header with security-mechanism as "tls". This is an indication to UE that P-CSCF supports TLS. • UE proceeds to establish TLS connection towards P-CSCF. It validates the TLS certificate of the network in this process. If the certificate presented by the P-CSCF is found acceptable to the UE, it sends REGISTER with credentials over the established TLS session. • P-CSCF forwards the REGISTER request with credentials to S-CSCF with “integrity-protected” parameter as "tls-pending" in Authorization header. • S-CSCF validates the credentials and sends 200 OK towards the P-CSCF, which in turn forwards 200 OK towards the UE over the established TLS session. • Any subsequent registrations (like refresh registrations) are received over TLS and P-CSCF inserts “integrity-protected” parameter as "tls-yes" in Authorization header in the forwarded REGISTER message.

P-CSCF receives only the initial REGISTER on the unprotected connection when TLS is employed. The REGISTER with credentials and all the subsequent messages are received only on the protected connection. Otherwise, P-CSCF ignores the messages.

SIP Digest without TLS

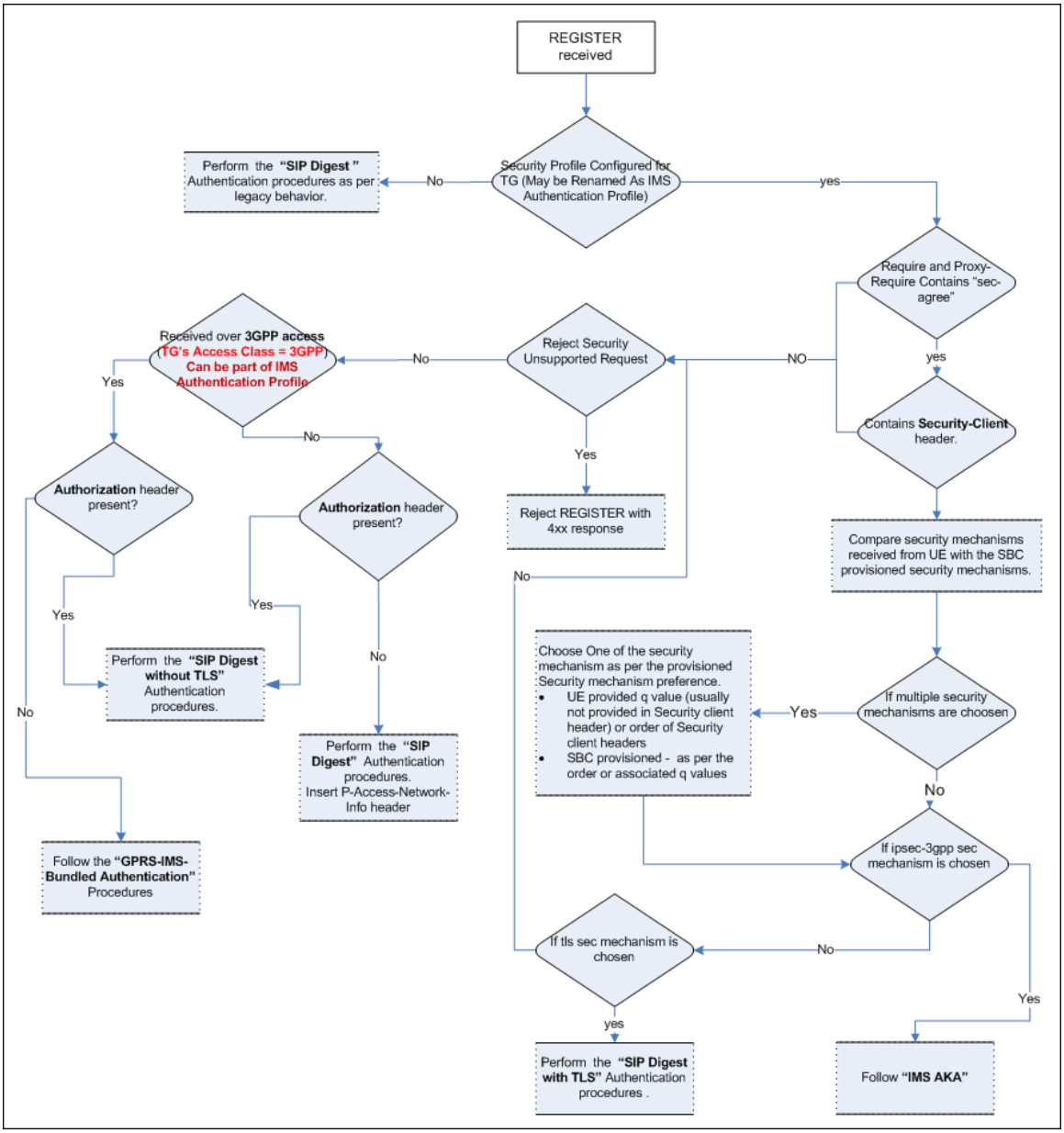
The SBC acting as a P-CSCF applies the following procedures once it infers SIP Digest without TLS is employed. When it receives a REGISTER request from the UE, the P-CSCF applies the “integrity-protected” header field parameter according to the following criteria:

- If the REGISTER request does not map to an existing IP association and does not contain a challenge response, P-CSCF does not include the "integrity-protected" header field parameter.
- If the REGISTER request does not map to an existing IP association and does contain a challenge response, P-CSCF includes the "integrity-protected" header field parameter with the value set to "ip-assoc-pending".
- If the REGISTER request maps to an existing IP association, P-CSCF includes the "integrity-protected" header field parameter with the value set to "ip-assoc-yes" in order to refresh and de-register messages.

P-CSCF Authentication Procedure

The following flow diagram provides a high-level view of the P-CSCF authentication procedure.

Figure 2: P-CSCF Authentication Flow Diagram



GPRS-IMS-Bundled-Authentication (GIBA) Security

3GPP standards ensure that simple, yet adequately secure mechanisms are in place to protect against the most significant security threats that will exist in early IMS implementations. These mechanisms are described under the heading of “GPRS-IMS-Bundled-Authentication” (GIBA) in the standards. For security reasons, these provisions only apply to IMS procedures used over the 3GPP PS domain. That is, these procedures are NOT recommended to be used for IP access networks other than 3GPP access.

The GIBA security solution works by creating a secure binding in the HSS between the public/private user identity (SIP-level identity) and the IP address currently allocated to the user at the GPRS level (bearer/network level identity). Therefore, IMS level signaling, and especially the IMS identities claimed by a user, can be connected securely to the PS domain bearer level security context.

The GGSN terminates each user's PDP context and has assurance that the IMSI used within this PDP context is authenticated. The GGSN shall provide the user's IP address, IMSI and MSISDN to a RADIUS server in the HSS when a PDP context is activated towards the IMS system. The HSS has a binding between the IMSI and/or MSISDN and the IMPI and IMPU(s), and is therefore able to store the currently assigned IP address from the GGSN against the user's IMPI and/or IMPU(s). The GGSN informs the HSS when the PDP context is deactivated / modified so that the stored IP address can be updated in the HSS.

When S-CSCF receives a SIP registration request or any subsequent requests for a given IMPU (public user identity), it checks that the IP

address in the SIP header (verified by the network) matches the IP address that was stored against that subscriber's IMPU in the HSS.

The GIBA mechanism relies on several assumptions and restrictions to provide the desired level of security. The two most notable assumptions are:

- GGSN does not allow a UE to successfully transmit an IP packet with a source IP address that is different to the one assigned during PDP context activation. In other words, the GGSN must prevent "source IP spoofing".
- The SBC acting as P-CSCF checks that the source IP address in the SIP header is the same as the source IP address in the IP header received from the UE (assumiing no NAT is present between the GGSN and the P-CSCF).

For an SBC acting as P-CSCF to implement GIBA security, user must set accessClass parameter to "3GPP" for Trunk Groups facing the UE. The following behavior applies to this feature:

- If a REGISTER message is received without specific security headers and accessClass is set to “3GPP”, the SBC selects GIBA as the security mechanism.
- The SBC defaults to SIP Digest without TLS authentication if accessClass is set to "None" (default behavior).
- If REGISTER message is received with "sec-agree" in Proxy-Require header along with Auth headers, and no IP Sec profile is configured, the SBC rejects the message with "4xx Bad Extension" error response irrespective of the accessClass parameter value.
- When GIBA security mechanism is selected, the SBC validates Source IP Address against Via header IP Address and transparently passes UEs Via header in egress messages towards network entities.
- When GIBA security mechanism is selected and Via header is configured to pass transparently to egress leg, the SBC inserts a “received” parameter with the source IP address of the PDU if the host portion of the UE’s Via header does not equate to the source IP address seen by the SBC.

The CLI syntax to enable 3GPP security is shown below:

```
% set addressContext <address context name> zone <zone name> sipTrunkGroup <TG name> signaling
accessClass <3GPP | none>
```

NULL Encryption Algorithm for IPSec/IMS AKA

The SBC Core supports the NULL algorithm for IP Multimedia Subsystem Authentication and Key Agreement (IMS AKA) registration request processing when it is offered by a UE. Previously, the SBC could not force a UE to use the NULL encryption algorithm. The SBC is enhanced with the SIP Security Profile parameter `encryptionPreference` to either enforce the NULL encryption algorithm irrespective of what encryption algorithm is offered by the UE or enforce non-NULL encryption algorithm by rejecting the registration request if the UE offers a NULL encryption algorithm.

The `encryptionPreference` options are:

- `always-encrypt`
- `none`
- `null-forced`

NASS-IMS-Bundled Authentication Support

NASS-IMS-Bundled-Authentication (NBA) is used to provide access to the IMS network for legacy equipment that cannot support IMS AKA. The authentication algorithm is enhanced to include and select NBA authentication.

The primary objective of the NBA is to gain access to the IMS network, based on successful access level authentication. This is achieved by associating an IMS identity with a fixed specific location from where it is authorized to access from. The SBC Core infers an authentication scheme applicable to the user based on response from S-CSCF for initial REGISTER request. If S-CSCF selects NBA, it either sends 200 OK or 403 response. The SBC infers an NBA authentication scheme on receipt of 200 OK and follows procedures associated with NBA. So, P-CSCF switches to either NBA or SIP Digest w/o TLS based on S-CSCF's response. When NBA is in use, receiving a 401 (Unauthorized) response to the REGISTER request is not expected.

The SBC performs NBA authentication procedures followed by SIP Digest w/o TLS authentication for the REGISTER request received over TISPAN NASS access.

The SBC continues to use the authentication mechanism selected during processing of initial registration message for a "subsequent" registration.

Note
The steps required for SIP Digest and for NBA are not in contradiction. Rather, for NBA, P-CSCF needs to perform additional steps, namely an exchange with TISPAN NASS and an inclusion of NASS location information in REGISTER request, on top of the steps required for SIP Digest.

When P-CSCF receives a REGISTER from the UE, and once NBA is selected as the authentication scheme, P-CSCF contacts CLF over the e2 interface. P-CSCF performs a"Location Information Query" towards CLF using the E2 interface User-Data-Request and User-Data-Answer message exchange to learn the location information. CLF sends the response to P-CSCF including location information of UE using the given IP address / User-Name. Upon getting a response from CLF, P-CSCF inserts PANI header, appends NASS location information to SIP REGISTER message, and forwards REGISTER message towards IMS core, in order to authenticate UE.

Background

When registering to an IMS subsystem, the location where UE is accessing from is verified by the Network Attachment Subsystem (NASS). If the NASS location is equal to the provisioned location, then the UE is authorized to access IMS.

The UE gets network attachment after authentication at the NASS level. The Connectivity session Location and repository Function (CLF) in the NASS is a database that holds a binding between the IP address and location information. The interface between CLF and P-CSCF is known as the e2 interface.

The SBC supports various IMS authentication schemes like IMS AKA, SIP digest w/o TLS, GIBA, and now NBA. When a UE sends a register request, P-CSCF selects one of the authentication schemes based on the algorithm.

Authentication Algorithm

If a REGISTER request from UE does not contain a Security-Client header field, and instead contains a Security-Client header field and Require, and if the Proxy-Require header fields do not contain "sec-agree", then P-CSCF behaves as follows using the authentication algorithm:

- If REGISTER request does NOT contain an Authorization header field and is received over TISPAN NASS access, and P-CSCF supports both SIP digest and NBA, then P-CSCF performs NBA as well as steps required for SIP digest w/o TLS
- If REGISTER request contains an Authorization header field and was received over TISPAN NASS access, and P-CSCF supports both SIP digest and NBA, then P-CSCF performs NBA as well as steps required for SIP digest w/o TLS.