
S60 3rd Edition: SIP Settings Configuration Guide

Version 1.0
November 9, 2007

S60 platform

Legal notice

Copyright © 2007 Nokia Corporation. All rights reserved.

Nokia and Nokia Connecting People are registered trademarks of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

Disclaimer

The information in this document is provided “as is,” with no warranties whatsoever, including any warranty of merchantability, fitness for any particular purpose, or any warranty otherwise arising out of any proposal, specification, or sample. This document is provided for informational purposes only.

Nokia Corporation disclaims all liability, including liability for infringement of any proprietary rights, relating to implementation of information presented in this document. Nokia Corporation does not warrant or represent that such use will not infringe such rights.

Nokia Corporation retains the right to make changes to this document at any time, without notice.

License

A license is hereby granted to download and print a copy of this document for personal use only. No other license to any other intellectual property rights is granted herein.

Contents

1.	Introduction	5
2.	SIP profiles.....	6
2.1	Tools and terminology.....	6
2.2	Supported profile types	7
2.3	Default profile	7
2.4	Security negotiation.....	8
2.5	Signaling compression	8
2.6	Registration mode	8
2.7	Profile lock.....	9
2.8	Internet access point (IAP).....	9
2.9	Address, port, and transport of the outbound proxy (or P-CSCF)	9
2.10	Loose routing	10
2.11	Address, port, and transport of the registrar server (or S-CSCF).....	10
2.12	Authentication parameters	11
2.12.1	IMS network supporting IMS AKA authentication	11
2.12.2	IMS network supporting Early IMS authentication	11
2.12.3	IMS network supporting HTTP Digest authentication	12
2.12.4	Internet-style network supporting HTTP Digest.....	12
2.13	Limitations	12
3.	Examples.....	13
3.1	IMS network supporting IMS AKA authentication and 3gpp-ipsec	13
3.2	IMS network supporting Early IMS authentication	13
3.3	Pre-standard IMS network supporting HTTP Digest authentication	13
3.4	Internet-style WLAN VoIP network with a separate proxy and registrar.....	14
3.5	Internet-style WLAN VoIP network with co-located proxy and registrar	14
4.	Terms and abbreviations.....	15
5.	References	16
6.	Evaluate this resource	17

Change history

November 9, 2007	Version 1.0	Initial document release

1. Introduction

This document gives an overview of how to configure S60 3rd Edition and 3rd Edition, Feature Pack 1 SIP settings parameters (that is, SIP profiles) for different types of SIP network deployments. SIP profiles take care of registering the device for one or multiple SIP/IMS (IP multimedia subsystem) service providers.

This document is a generic guideline document for SIP settings configuration in S60 devices. It is mainly targeted for mobile operators for setting up the SIP profile to enable SIP applications to work correctly.

2. SIP profiles

This chapter describes how to configure the SIP settings parameters for different types of SIP network deployments.

2.1 Tools and terminology

SIP settings can be managed with a number of tools:

- OMA Device Management (DM): For DM, a Nokia proprietary MO structure is supported.
- OMA Client Provisioning (CP): For CP, a Nokia proprietary MO structure is supported for SIP, just like for DM.
- SIP Settings UI

Unfortunately, each of these tools and structures use different names for the same parameters. Table 1 provides a mapping for the terms and gives links to the appropriate sections of this document.

Table 1: Terminology used in the different tools

Settings UI	Nokia DM	Nokia CP	IMS	IETF
Profile name	Name	PROVIDER-ID		
Service profile	ProfileType	PTYPE	2.2	2.2
Public username	AddressOfRecord	PUID	2.12	2.12.4
Default profile	Default	n/a	2.3	2.3
Security negotiation	EnableSecurity Negotiation	SECNEG	2.4	2.4
Use compression	EnableSignal Compression	SIGNALCMPR	2.5	2.5
Registration mode	EnableAuto Registration	APPADDR/ AUTOREG	2.6	2.6
n/a	ProfileLock	APPADDR/ LOCK	2.7	2.7
Access point	PrefConRef	TO-NAPID	2.8	2.8
Proxy address	Host	APPADDR/ ADDR	2.9	2.9
Port	Port	APPADDR/ PORT/ PORTNBR	2.9	2.9
Transport protocol	Transport	APROTOCOL	2.9	2.9
Username	Username	APPAUTH/ AAUTHNAME	2.12	2.12.4

Settings UI	Nokia DM	Nokia CP	IMS	IETF
Password	Passwd	APPAUTH/ AAUTHSECRET	2.12	2.12.4
Realm	Realm	APPAUTH/ AAUTHDATA	2.12	2.12.4
Loose routing	LooseRouting	APPADDR/LR	2.10	2.10
Registrar address	Host	RESOURCE/URI	2.11	2.11
Port	Port		2.11	2.11
Transport protocol	Transport		2.11	2.11
Username	Username	RESOURCE/ AAUTHNAME	n/a	2.12.4
	PrivateIdentity		2.12	n/a
Password	Passwd	RESOURCE/ AAUTHSECRET	2.12	2.12.4
Realm	Realm	RESOURCE/ AAUTHDATA	2.12	2.12.4

If a profile is in a "Registered" status, updating the values of the parameters most often causes the profile to be deregistered and thereafter registered again. Deregistration is, however, not done for updating HTTP Digest authentication parameters or profile name.

2.2 Supported profile types

S60 SIP software supports two different types of SIP profiles:

- IMS profiles which can be used for networks that support 3GPP IMS Rel-5 (and any later 3GPP IMS release) or pre-standard IMS networks that support 3GPP Early IMS authentication or HTTP Digest authentication.
- IETF profiles which can be used for networks that support Internet-style SIP. Most common deployments of this type are provided by VoIP service providers who use SIP. They usually support HTTP Digest authentication.

Note that S60 devices support multiple parallel SIP profiles for the following use case:

- The user of the mobile device uses SIP-based services from multiple service providers, for instance IMS services from a mobile operator and VoIP services from an Internet VoIP service provider.

2.3 Default profile

When the profile is set as the default profile, it will be used if a SIP-based application initiates registration without indicating any specific profile to be used. Note that a mobile device with the default factory settings does not contain any pre-provisioned profiles. All the profiles must be created by the OTA tools or SIP Settings UI, unless operator-specific factory settings also contain SIP profiles.

2.4 Security negotiation

Security negotiation means the process described in IETF RFC 3329 [9].

For the IMS profile, security negotiation is enabled by default since it is needed for setting up the ipsec-3gpp security associations as described in 3GPP TS 24.229 [2]. If the IMS network supports IMS AKA (authentication and key agreement) but does not support ipsec-3gpp, security negotiation shall be disabled.

For the IETF profile, security negotiation is disabled by default since most Internet-style SIP providers do not support the mechanism. If needed, negotiation can be enabled.

2.5 Signaling compression

Security negotiation means the process described in IETF RFC 3329 [9].

For the IMS profile, security negotiation is enabled by default since it is needed for setting up the ipsec-3gpp security associations as described in 3GPP TS 24.229 [2]. For the IMS profile, the security algorithm announced in the Security-Client header depends on how the authentication parameters are configured within the profile. If the authentication parameters are left empty, Security-Client will contain all the information needed for ipsec-3gpp. However, if the profile has been configured for HTTP Digest authentication, the Security-Client header only suggests using digest.

If the IMS network supports IMS AKA but does not support ipsec-3gpp, security negotiation shall be disabled. When security negotiation is disabled, the Security-Client header will not be sent.



Note: Leaving the authentication parameters empty and disabling security negotiation also makes it possible to use Early IMS authentication procedures where the network will respond to the initial REGISTER request with a 200 OK response. However, in this case there is one small difference to the Early IMS procedures as specified in TR 33.978 [4]: the initial REGISTER request contains an Authorization header. The reason for this is that the Authorization header is needed for cases where the network supports IMS AKA without ipsec-3gpp.

For the IETF profile, security negotiation is disabled by default since most Internet-style SIP providers do not support the mechanism. If needed, negotiation can be enabled. When enabled for the IETF profile, the only supported algorithm announced in the Security-Client header is digest.

2.6 Registration mode

The registration mode parameter is used to control when the device performs the registration for the corresponding SIP/IMS service provider. The parameter can be configured to one of the following values:

- Always On: The device registers the profile when switched on. The device tries to keep the profile registered whenever it is in the coverage of any packet network corresponding to the IAP used by the profile.
- When needed: Registration is done only when a SIP-based application explicitly asks the device to perform the registration and the device is in the coverage of a packet network corresponding to the IAP within the profile that the application is using.

2.7 Profile lock

The profile lock parameter can be used from DM and CP to disable the modifying or deleting of this profile with the SIP Settings UI, that is, to protect the profile from being modified by the end user.

2.8 Internet access point (IAP)

The IAP parameter refers to an access point name (APN) that identifies the GPRS or WLAN access point to be used for SIP connectivity for the profile. IMS profiles support only GPRS access whereas IETF profiles can be used with both access methods.

The SIP profile settings must explicitly indicate the access point to be used for SIP. SIP is **not** aware of the default IAP configured to the mobile device so that it would be used if no explicit IAP was defined for SIP.

If the operator creates new SIP settings to the device with OMA Device Management and aims to refer to some access points already configured to the device, the DM can at first query the existing access point settings from the device. The OTA message sent after that by OMA DM for SIP can refer to the IAP settings retrieved from the device.

If the operator creates new SIP settings to the device with OMA Client Provisioning, the OTA message must also contain a command to create the related access point to the device. With OMA CP, there is no mechanism available for how the SIP settings sent over-the-air could refer to a predefined access point already existing in the device.

2.9 Address, port, and transport of the outbound proxy (or P-CSCF)

For the address of the outbound proxy (called P-CSCF in the IMS networks), the following configuration options are available:

- Leave the parameter empty in the IETF profile if the outbound proxy is co-located with registrar and it does not accept its own address within a Route header when the outbound request comes from the User Agent. In the IMS profile, an empty value causes automatic P-CSCF discovery (that is, the same behavior as with IP address 0.0.0.0 as described below) since IMS networks will always have P-CSCF as outbound proxy.
- Configure the IP address to be 0.0.0.0. This means that the SIP stack discovers the outbound proxy automatically, by using GPRS or DHCP procedures.
- Configure the IPv4/v6 address, SIP URI, or the fully qualified domain name of the outbound proxy to SIP settings. The domain name will be resolved to the IP address by using DNS. In many cases the proxy address is the SIP domain, that is, the hostname part of the public SIP URI (AOR, address-of-record).

For discovering and/or resolving the IP address, transport, and port of the proxy, the S60 SIP stack uses the following procedures:

- If the address of the outbound proxy is supplied as 0.0.0.0, the real address of the proxy is discovered using the DHCP SIP server option. If the server returns the address as a domain name, the rules specified in the following bullets will be used to resolve the IP address, transport, and port by DNS.
- If the address is supplied as a SIP URI or domain name without port and transport parameters, the S60 SIP stack tries to resolve the IP address, port,

and transport using the DNS NAPTR, SRV, and finally the A and AAAA queries.

- If the address is supplied as a SIP URI or domain name without the port but with the transport parameter, the S60 SIP stack tries to resolve the IP address and port for the specified transport using the DNS SRV and finally the A and AAAA queries.
- If the address is supplied as a SIP URI or domain name with the port parameter, the terminal tries to resolve it using only the A and AAAA queries. If no explicit transport parameter is given, transport will be selected dynamically based on the size of the SIP request sent.

For further information about these procedures, check the following documents:

- RFC 3263 [7] specifies the usage of DNS NAPTR, SRV, A, and AAAA procedures for resolving the address of a SIP server.
- RFC 3319 [8] specifies a DHCPv6 option for discovering the local SIP server.
- RFC 3361 [10] specifies a DHCPv4 option for discovering the local SIP server.

The transport setting affects all initial requests. A possible transport parameter on the next hop in the Record-Route or Contact overrides this setting. The setting can have one of the following values:

- UDP – Transport selected according to RFC 3261 [6], that is, UDP is used for initial requests that are smaller or equal to 1300 bytes, and TCP is used for initial requests that are larger than 1300 bytes.
- TCP – TCP transport forced to be used. Set, for instance, if a persistent TCP is used for NAT traversal.

2.10 Loose routing

Loose routing is enabled by default. It shall be disabled only for old proxies based on the obsolete SIP RFC 2543.

2.11 Address, port, and transport of the registrar server (or S-CSCF)

Values for address, port, and transport should only be provided when the registrar uses HTTP Digest authentication. The following cases need to be considered:

- Outbound proxy and registrar server have different addresses. In this case the device will use the outbound proxy as the next hop when sending the REGISTER request. The address of the registrar server should typically be the host part of the AOR and it will be used as R-URI of the REGISTER request. There is usually no need to configure port or transport because the R-URI of the REGISTER request typically does not need port or transport parameters.
- Outbound proxy and registrar server are co-located and thus have the same address. If the address of the outbound proxy is not left empty or supplied as 0.0.0.0, the address configured for the registrar should match the address of the outbound proxy. In that case the port and transport parameters can be omitted from the registrar server since the values configured for the outbound proxy will be used for the next hop. However, when the address of the proxy is left empty (to avoid it appearing in a Route header within the

REGISTER request), the values of port and transport of the registrar server will be used when sending requests to the next hop, as defined in Section 2.9.

2.12 Authentication parameters

The S60 software natively supports the following authentication methods for SIP:

- HTTP Digest authentication as specified in RFC 2617 [5] and 3261 [6].
- IMS AKA authentication as specified in 3GPP TS 24.229 [2] and 33.203 [3].
- Early IMS authentication as specified in 3GPP TR 33.978 [4]

This section describes the parameters needed to configure a SIP profile for any supported authentication method for IMS or Internet-style networks.

2.12.1 IMS network supporting IMS AKA authentication

For the IMS AKA authentication, the device must be equipped with an UICC containing at least the USIM application (but possibly also the ISIM application). The device reads the IMS home domain name, private user identity, and public user identity from the ISIM application or derives them from the IMSI parameter read from USIM as specified in 3GPP TS 23.003 [1], when the UICC does not contain the ISIM application.



Note: When using IMS AKA, the S60 platform does not support configuring any of the authentication-related parameters (home domain name, i.e., the registrar address, realm, private and public user identity) to SIP settings. However, S60 supports the standard mechanism as specified in 3GPP TS 24.229 [2] so that the realm parameter of the initial REGISTER is populated with the home domain name, as read from ISIM/USIM, but for any subsequent REGISTER the realm parameter is populated with the value that the network returns in the WWW-Authenticate header of the 401 response.

2.12.2 IMS network supporting Early IMS authentication

There are two different options for how to get the S60 SIP stack to use Early IMS authentication. In both options the IMS profile shall be configured exactly as for IMS AKA authentication.

1. The first option is to equip the device with a UICC containing a USIM application and keep security negotiation enabled. This option can be used if the network is able to reject the initial REGISTER with `Require: sec-agree` with a 420 response containing the `Unsupported: sec-agree` header. As a fallback, the SIP stack will send the initial REGISTER again without the Authorization header and security negotiation procedures, as specified in 3GPP TR 33.978 [4].
2. The second option is to equip the device with a GSM-type SIM. In this case the SIP stack immediately sends the initial REGISTER without the Authorization header or security negotiation procedures, as specified in 3GPP TR 33.978 [4]. For this option, the configured value of security negotiation parameter does not matter.

2.12.3 IMS network supporting HTTP Digest authentication

In an IMS network which supports HTTP Digest authentication, all the SIP identity and authentication details shall be configured to the SIP profile and none of them will be read from a SIM or UICC card.

The IMS profile shall be configured with the public user ID, private user ID (user name used for authentication), password, and realm for S-CSCF (registrar). Private user ID, password, and realm should be configured for P-CSCF (proxy) only in the rare case where P-CSCF uses a different realm than S-CSCF. Note that, when supplied, the realm must be exactly the same string as returned by the CSCF within the realm parameter of the 401 or 407 response.

In these kinds of deployments the security negotiation is typically disabled but can be enabled if needed. If enabled, the S60 SIP stack indicates the support for the digest method within the Security-Client header.

2.12.4 Internet-style network supporting HTTP Digest

Public user name shall contain the SIP or SIPs AOR of the user.

For HTTP Digest, the IETF profile shall be supplied with the address, user name, password, and realm for the registrar whenever proxy and registrar use the same realm string. Configuring those parameters for proxy is done only when the realm of proxy is different than the realm of registrar.

Note that the stack supports only one single user name and password per one realm string, across all the profiles configured to the device. This means that if one realm string is used within multiple profiles (or for both registrar and proxy of a single profile), the user name and password must be identical for all those profiles and servers using the same realm.

The address of the registrar is typically the host part of the user's SIP AOR.

Note that, when supplied, the realm must be exactly the same (case-sensitive) string as returned by the registrar or proxy within the realm parameter of the 401 or 407 response.

2.13 Limitations

SIP settings do not support modifying the values of the following parameters:

- Expiration time sent within a REGISTER request. For the IMS profile, the value is always 600000 seconds (one week) and for the IETF profile 3600 seconds (one hour). However, the SIP stack will use the expiration time which the registrar tells within its 200 OK response for the REGISTER request (or within a registration state event for the IMS profile)
- Values of the SIP timers. The default values for the timers are as follows: T1=3 sec, T2=16 sec, and T4= 17 sec. These timers can have operator-specific values if preconfigured in the factory. There is only one set of timer values in the device, which means the same timer values will be used for every profile regardless of the type of radio access method (GPRS or WLAN).

Another limitation is that the stack supports only one single HTTP Digest user name and password per one realm string, across all the profiles configured to the device. This means that if one realm string is used within multiple profiles (or for both registrar and proxy of a single profile), the user name and password must be identical for all those profiles and servers using the same realm.

3. Examples

The examples in this chapter indicate only those parameters where the values must be explicitly given. For the rest of the parameters, the default values are sufficient and will be used.

Note that the actual value of the Profile Type is specific to the tool (OMA DM, CP, or SIP Settings UI) and even for the device model. For instance, the Profile Type IMS is shown on the UI of some devices as "Nokia 3GPP" and IETF as "Internet".

3.1 IMS network supporting IMS AKA authentication and 3gpp-ipsec

If the network supports IMS AKA authentication, the profile has to be configured with one single mandatory parameter only, namely the Internet access point (IAP). Other parameters can be left to their default values, assuming that the network also provides automatic P-CSCF discovery (via GPRS or DHCP).

Profile name: My IMS operator
 Profile type: IMS
 Internet access point: operator-IMS-AP

3.2 IMS network supporting Early IMS authentication

In this example the IMS network supports Early IMS authentication but does not support automatic P-CSCF discovery. Thus the address of P-CSCF is configured to SIP settings.

Profile name: My Early IMS operator
 Profile type: IMS
 Internet access point: operator-IMS-AP
 Outbound proxy
 - Proxy address: pcscf.operator.com

3.3 Pre-standard IMS network supporting HTTP Digest authentication

In this example the IMS network uses HTTP Digest but supports automatic P-CSCF discovery. The address of S-CSCF has to be configured to the device. The pre-standard network does not support security negotiation or signaling compression; they are, therefore, disabled. In this example the operator uses its domain name as the realm string to be returned within 401 and 407 responses. Since identical realm, user name, and password are used for both the proxy and registrar, those parameters should only be configured for registrar. Defining them twice (that is, also for proxy) is possible, but redundant and should not be done to avoid mistakes.

Profile name: My digest IMS operator
 Profile type: IMS
 Public username (AOR): sip:user@operator.com
 Security negotiation: disabled
 Signaling compression: disabled
 Internet access point: operator-IMS-AP

Outbound proxy
 - Proxy address: 0.0.0.0

Registrar server
 - Registrar address: operator.com

- Username: my_private_user_id
- Password: asdfjkl
- Realm: operator.com

3.4 Internet-style WLAN VoIP network with a separate proxy and registrar

In this example the IETF profile is configured with different addresses for outbound proxy and registrar server. The proxy only supports UDP, and transport is, therefore, explicitly selected, in order to force UDP regardless of the message size. Because the proxy and registrar in this example use different realm strings, it is necessary to define all the authentication parameters (`realm`, `username`, and `password`) separately for proxy and registrar (regardless of whether the user name and password are the same or different for these two realms).

Profile name: My VoIP provider
 Profile type: IETF
 Public username (AOR): sip:user@provider.com
 Internet access point: home-WLAN-AP

Outbound proxy

- Proxy address: proxy.provider.com
- Transport protocol: UDP
- Username: user@provider.com
- Password: asdfqwer
- Realm: realm_proxy_operator_com

Registrar server

- Registrar address: provider.com
- Username: user@provider.com
- Password: asdfqwer
- Realm: realm_operator_com

Note that SIP settings are not sufficient to enable VoIP service for an S60 device. The device also has to be configured with VoIP and NAT traversal settings, which are out of the scope of this document.

3.5 Internet-style WLAN VoIP network with co-located proxy and registrar

In this example the outbound does not accept its own address in the Route header when the device sends a request via the proxy. The proxy is configured to receive SIP requests in port 12345. When the same realm, user name, and password are used for both proxy and registrar, they should only be configured for the registrar.

Profile name: My VoIP provider
 Profile type: IETF
 Public username (AOR): sip:user@provider.com
 Internet access point: home-WLAN-AP

Registrar server

- Registrar address: sip:provider.com
- Port: 12345
- Username: user@provider.com
- Password: asdfqwer
- Realm: realm_operator_com

Note that SIP settings are not sufficient to enable VoIP service for an S60 device. The device also has to be configured with VoIP and NAT traversal settings, which are out of the scope of this document.

4. Terms and abbreviations

Term or abbreviation	Meaning
AKA	Authentication and key agreement
AOR	Address-of-record
AP	Access point
APN	Access point name
CP	Client Provisioning
DM	Device Management
GPRS	General packet radio service
IAP	Internet access point
IETF	Internet Engineering Task Force
IMS	IP multimedia subsystem
IMSI	International mobile subscriber identity
IPv4/6	Internet Protocol version 4/6
ISIM	IM services identity module
OMA	Open Mobile Alliance
OTA	Over the air
P-CSCF	Proxy call state control function (analogous to outbound proxy)
S-CSCF	Serving call state control function (analogous to registrar proxy)
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UICC	Universal integrated circuit card
URI	Uniform resource identifier
USIM	Universal subscriber identity module
VoIP	Voice over IP

5. References

- [1] 3GPP TS 23.003, "Numbering, addressing and identification," <http://www.3gpp.org/>
- [2] 3GPP TS 24.229, "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3," <http://www.3gpp.org/>
- [3] 3GPP TS 33.203, "3G security; Access security for IP-based services," <http://www.3gpp.org/>
- [4] 3GPP TR 33.978, "Security aspects of early IP Multimedia Subsystem (IMS)," <http://www.3gpp.org/>
- [5] IETF RFC 2617, "HTTP Authentication: Basic and Digest Access Authentication," <http://www.ietf.org/>
- [6] IETF RFC 3261, "SIP: Session Initiation Protocol," <http://www.ietf.org/>
- [7] IETF RFC 3263, "Session Initiation Protocol (SIP): Locating SIP Servers," <http://www.ietf.org/>
- [8] IETF RFC 3319, "Dynamic Host Configuration Protocol (DHCPv6) Options for Session Initiation Protocol (SIP) Servers," <http://www.ietf.org/>
- [9] IETF RFC 3329, "Security Mechanism Agreement for the Session Initiation Protocol (SIP)," <http://www.ietf.org/>
- [10] IETF RFC 3361, "Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers," <http://www.ietf.org/>

6. Evaluate this resource

Please spare a moment to help us improve documentation quality and recognize the resources you find most valuable, by [rating this resource](#).