



# Gigaset IP and IP-PRO Phones Provisioning / Remote Management

last modifications by J. Stahl,  
Bocholt, January the 18<sup>th</sup> 2011

# ■ Agenda

## Provisioning / Remote Management for Gigaset IP phones

- [Introduction](#)
- [Autoprovisioning for Gigaset IP phones](#)
- [Autoprovisioning Message Flow](#)
- [MAC based autoprovisioning for retail devices](#)
- [Autoprovisioning with a customized provisioning server](#)
- [Remote management via TR069](#)
- [Contacts](#)



# Gigaset

## Introduction



## Introduction: Provisioning for Gigaset IP phones

### **Installing a VoIP-Phone**

What the end customer expects is a “plug & play” device as it is usual for an “analogue” phone.

For reaching this aim with a Gigaset / Gigaset-PRO VoIP phone there are different provisioning methods supported depending on the prevailing infrastructure.

### **Provisioning via Profiles**

A “Profile” is a configuration file containing Gigaset VoIP-phone specific settings. A VoIP-Profile can be loaded via the Ethernet interface.

### **Gigaset Provisioning**

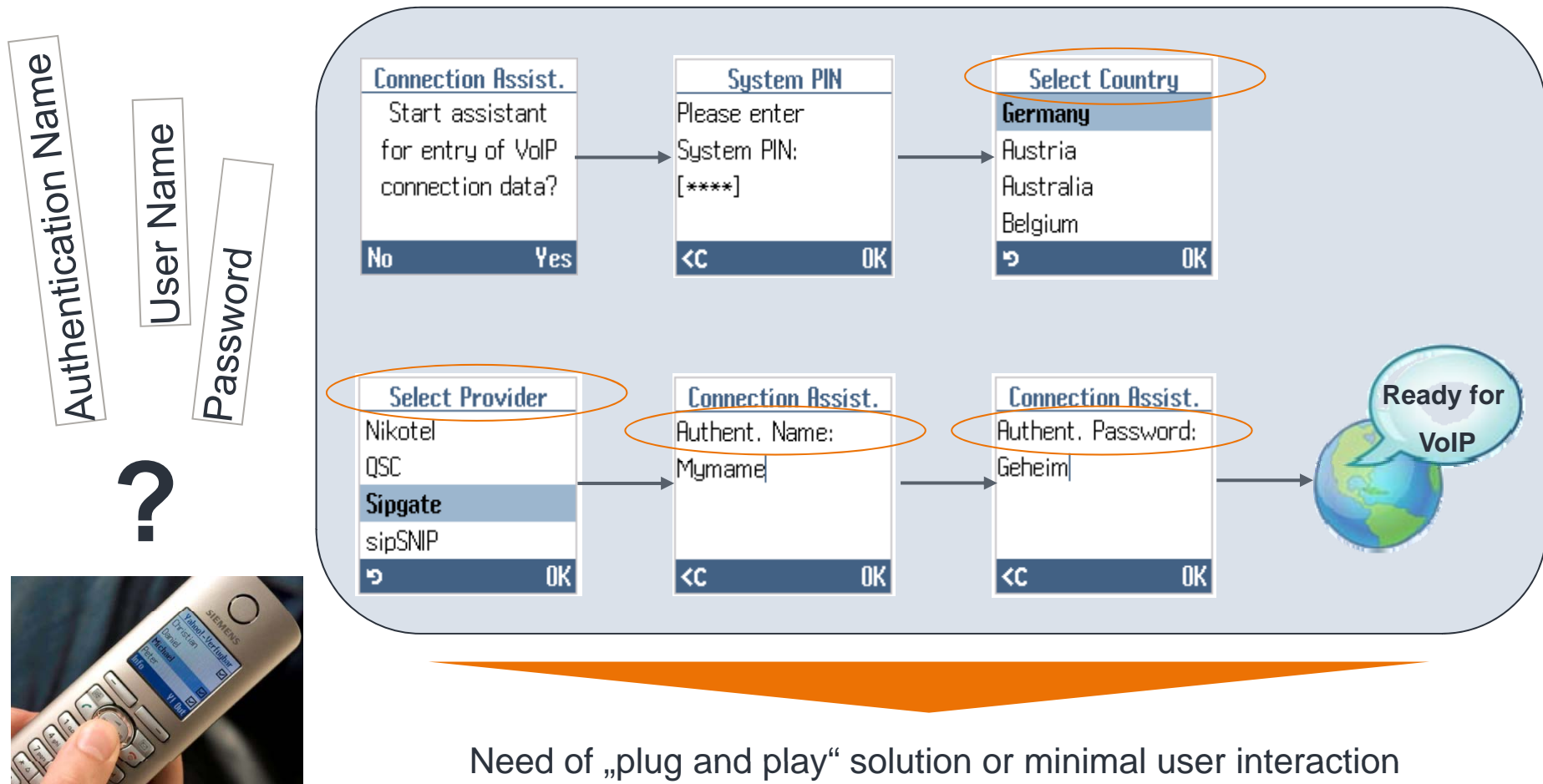
The standard Gigaset provisioning allows the user to load a VoIP-Profile containing VoIP-Provider / ISP specific data via the Ethernet interface. The user has only to enter manually the user specific data (ID('s) and password).

→ please see following pages

- Gigaset IP Phones do not require the use of a PC
- Easy Set-up behind router



- Login parameters are required to set-up VoIP provider
- Principle of manually configuration of VoIP connection data:



## Terms

### Remote Management

The term "Remote Management" is the synonym for three different methods supported by Gigaset VoIP-phones:

- For the **<auto-provisioning with an Activation Code>** are VoIP-Profiles used which can also contain user specific content. For loading such a VoIP-Profile the user has only to enter manually the activation code.
- For loading user specific Profiles without any user interaction the **<MAC based auto-provisioning>** can be used. The database containing the user specific data can be hosted on a Gigaset server or on a Provider / PBX related server.
- Some Gigaset phones are additionally supporting the remote management based on **<TR069>**. This method is especially used for Provider specific product variants.

Part of the "Remote Management" are also the methods for sending the URL / address of the provisioning server to the VoIP-phone. This can be done via:

- factory setting, or
- DHCP option, or
- the SIP Multicast mechanism (currently supported by T300 and T500), or
- manually in the WEB configurator.

# Gigaset

## Autoprovisioning for Gigaset IP phones





# Autoprovisioning for Gigaset IP phones

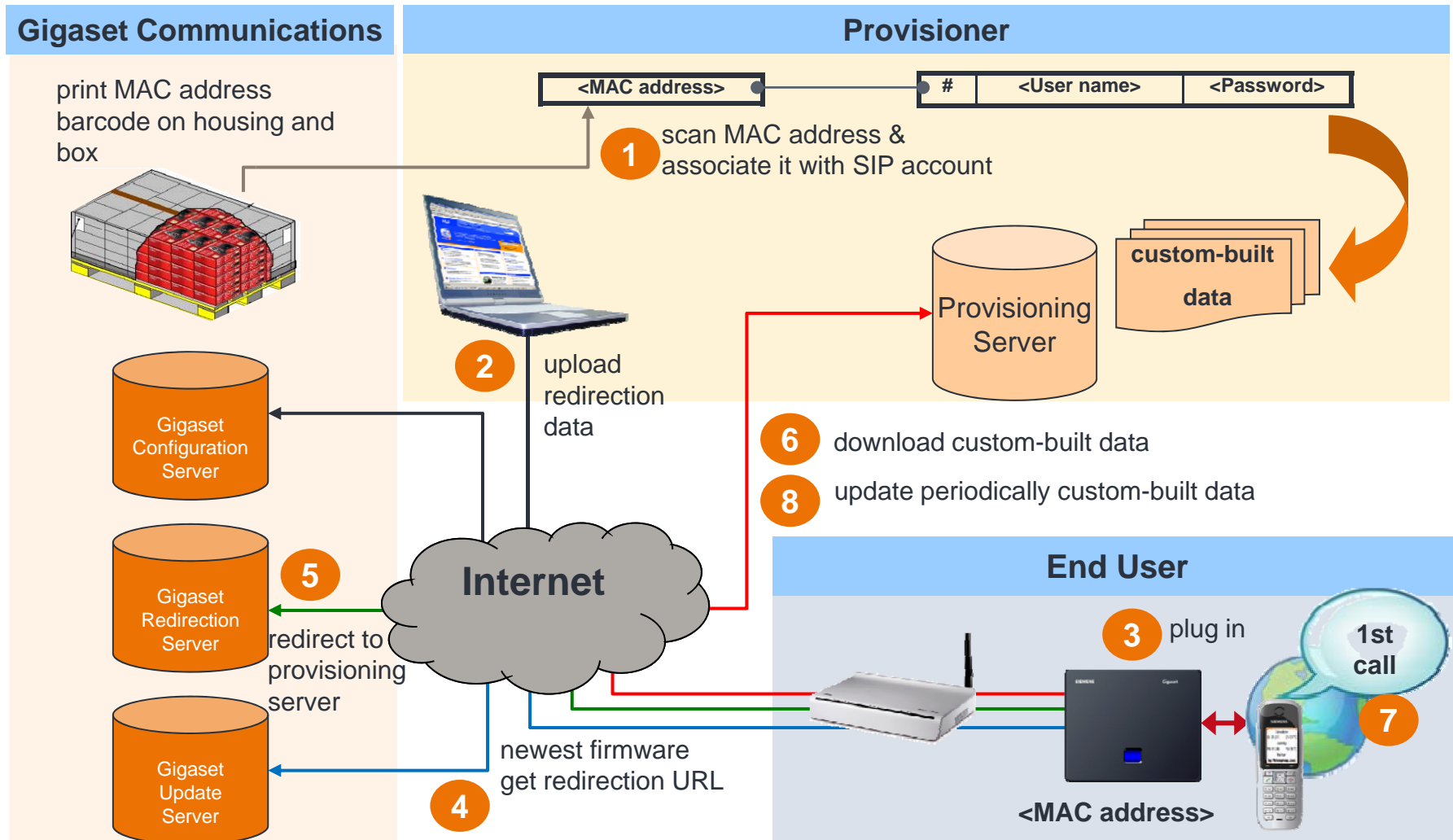
## How to tackle the set up...

Autoprovisioning variants offered	MAC based	Activation code	One shot	TR069 / TR104 / TR106 / TR111
<b>Principle</b>	MAC address used to identify and provide access	Code used to identify and provide access	Code used to identify and provide access	Remote configuration system
<b>Target audience</b>	Operator and Retail	Operator and Retail	Retail	Operator
<b>Customer to do</b>	Connect only, nothing to enter	enter activation code	enter activation code	connect only, nothing to enter )*
<b>Operator to do</b>	Scan MAC addresses and link to customer record (tooling available). Provide access if MAC registers	Codes are linked to customer record and sent to customer. Provide access when code entered	Codes are linked to customer record and sent to customer. Provide access when code entered.	Setup and run TR069 system. Remote configuration of phone.
<b>Advantage</b>	low invest, compared to TR069; integration into TR069 system possible;	easy handling, no MAC scanning needed; low invest, integration into TR069 system possible;	add convenience for retail variant. low invest	Use existing TR069 system; Update configuration later;
<b>Locked variant</b> (configuration partly blocked)	yes (optional for operator variants)	yes (optional for operator variants)	no	Yes (optional)
<b>Availability</b>	TODAY	TODAY	TODAY	TODAY

)\* if appropriate credential management installed

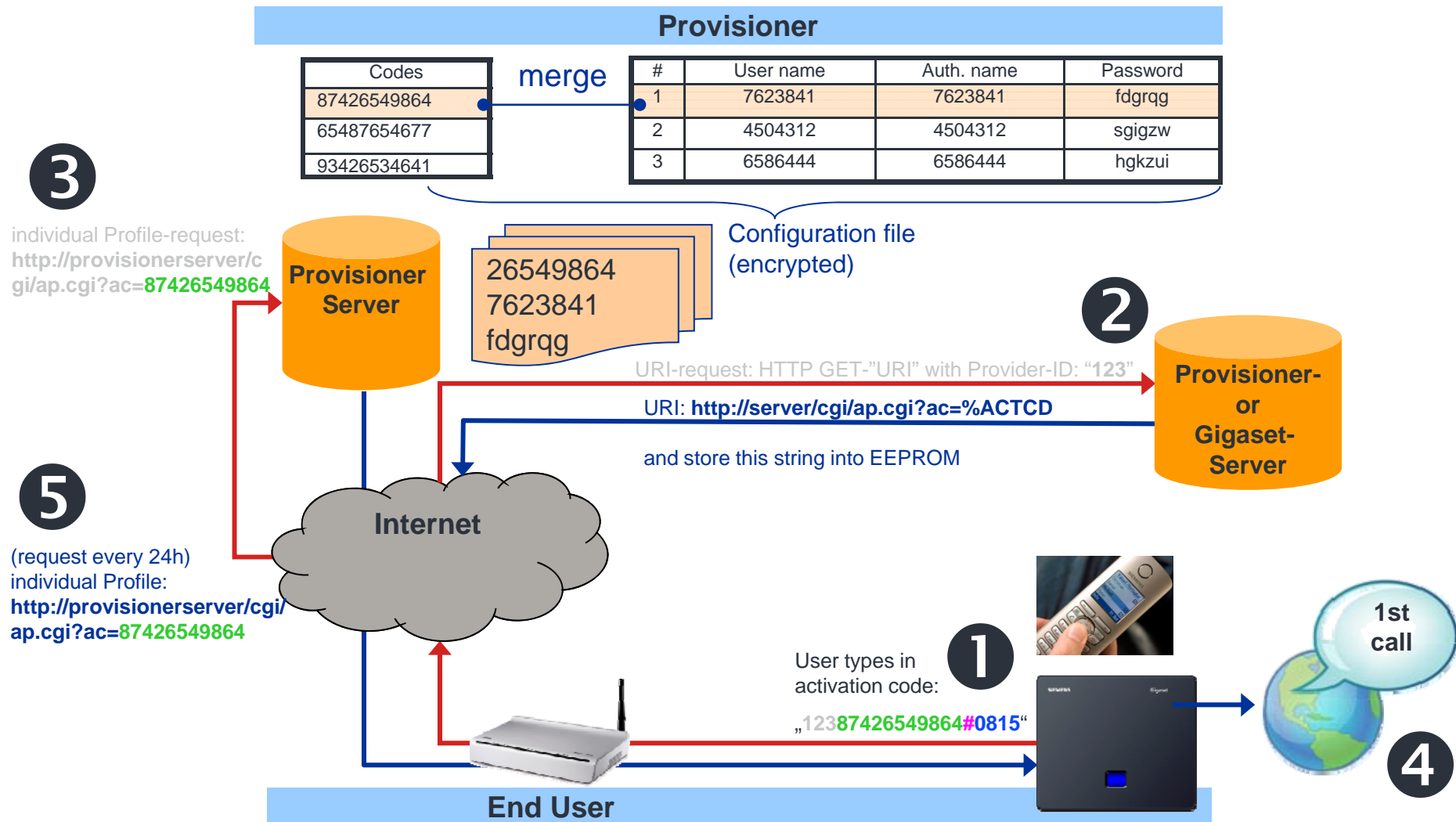
# Autoprovisioning for Gigaset IP phones

## the MAC based approach



# Autoprovisioning for Gigaset IP Phones

## Activation Code based approach



# Autoprovisioning for Gigaset IP Phones

■ further informations ...

List of the supported Provider and used VoIP-parameter :



(26.05.2010)

master\_providers.xml

List of the usable parameter in a Profile / configuration file for the Gigaset VoIP-phones:



(09.12.2010)

Adobe  
Acrobat-Dokument

# Gigaset

## Autoprovisioning Message Flow

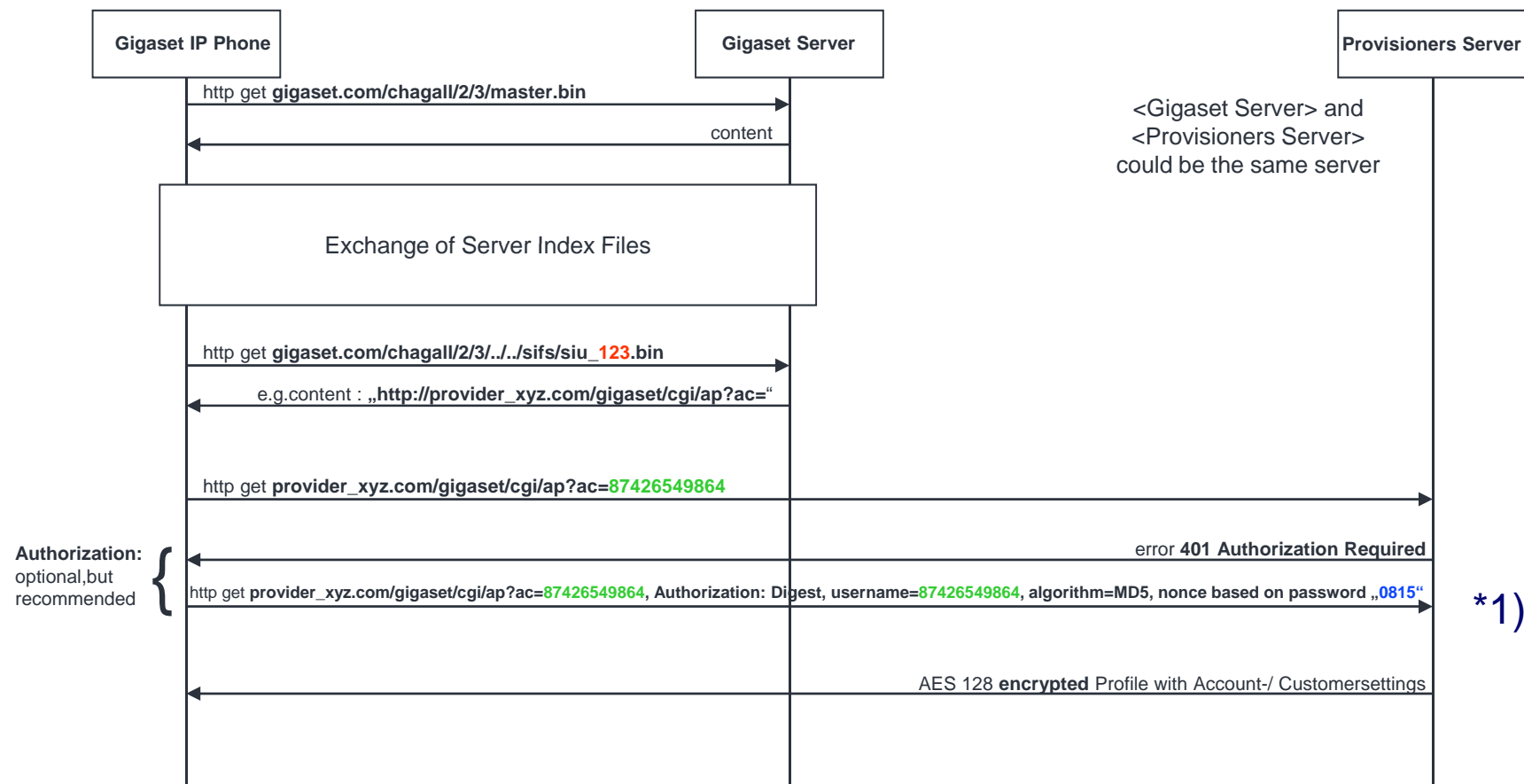


# Message Sequenz Chart (MSC)

## Autoprovisioning with Activation Code

The following diagram shows in principle the message flow between a Gigaset IP Phone and the involved servers from Autoprovisioning point of view.

Use Case: The IP Phone is prepared for Autoprovisioning with activation code (locked or non locked (One Shot)) and the Customer feeds in the Activation Code **12387426549864#0815** in the Handset- or WEB-UI.

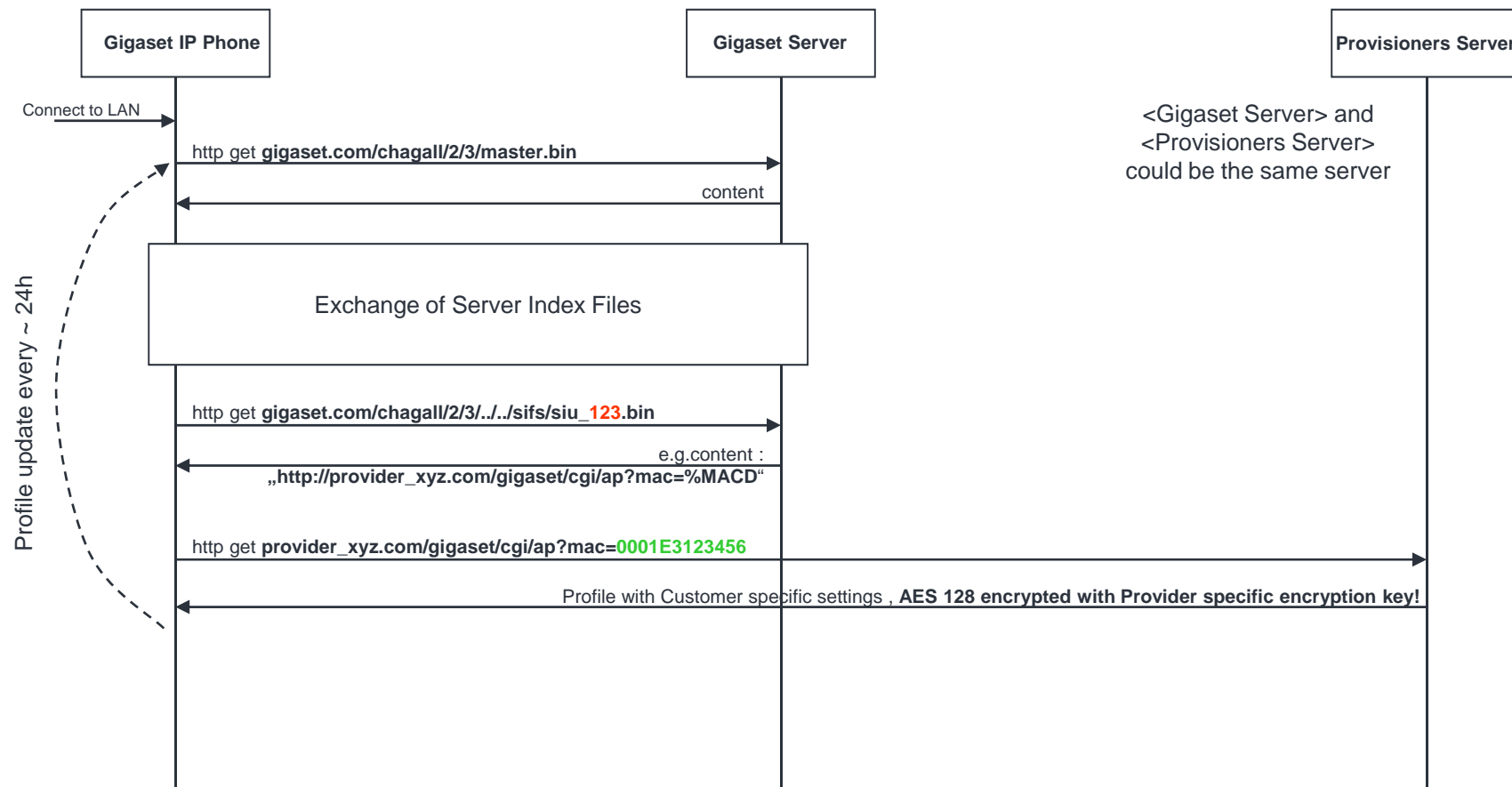


# Message Sequenz Chart (MSC)

## MAC based autoprovisioning

The following diagram shows in principle the message flow between a Gigaset IP Phone and the involved servers from Autoprovisioning point of view.

Use Case: The IP Phone is prepared for MAC-Autoprovisioning (UI partly locked) and connected to the Internet.



# Message Sequenz Chart (MSC)

## Remarks

- \*1)** Additionally the MAC address will be send. The provisioner can use the MAC address for different security enhancements. E.g.:
- He can store the MAC address during the first registration and allow for future registration only this MAC address.
  - He can compare the MAC address with his own MAC address data base for making sure, that no foreign phone uses this account data.

### Security aspects:

- Use of HTTP digest for authentication (for Autoprovisioning with Activation Code).
- The Profile is encrypted with AES 128 using a Provider specific encryption key!
- The activation code string (e.g.: 12387426549864#0815) can include up to 32 characters. The string contains the provider identification (3 chars fix), the activation code and an optional password, separated by a #.
- Additional TLS is supported with some Gigaset VoIP phones.




# Gigaset

**Autoprovisioning with a  
customized provisioning server**



## ■ Autoprovisioning with a customized provisioning server

### General Aspects:

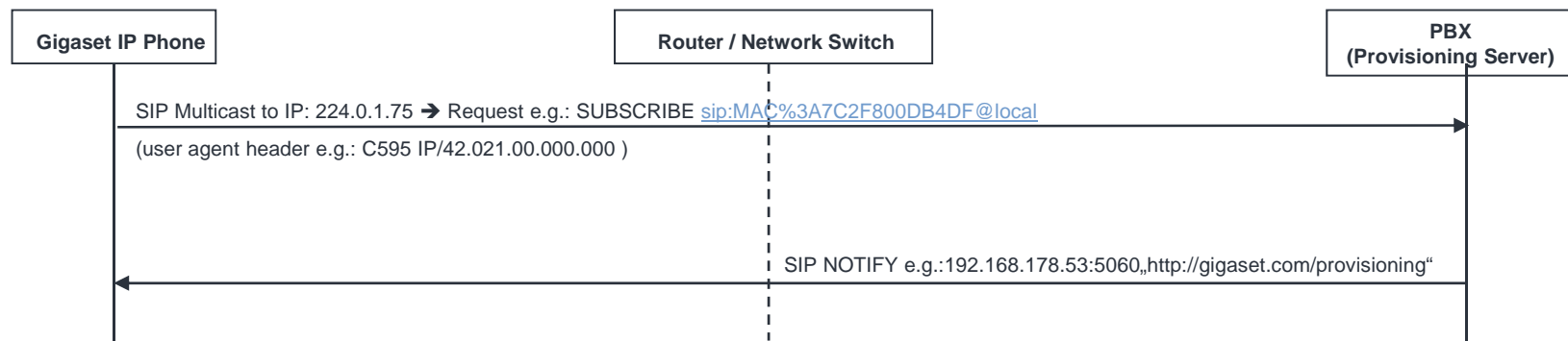
- Reasons for using an other provisioning server than the Gigaset provisioning server are varied. It could be, that the VoIP-phone is located in a closed Network with no possibility to reach the Gigaset provisioning server via the WWW (ere no HTTP proxy is available for connecting the Gigaset provisioning server via the WWW. Or may be the VoIP phone is used behind a VoIP-PBX and the provisioning has to be independent from the LAN/WAN infrastructure.
- First off all the VoIP-Phone has to find the new URL of the provisioning server (default = profile.gigaset.net/device). Depending on the Network infrastructure this can occur in different ways:
  - manually per WEB server, or
  - via DHCP option (product dependent), or
  - via the SIP-Multicast mechanism (please see details on next page), or
  - as factory default (only for product variants!).
- The VoIP-Provider / VoIP-PBX has to provide a „Linux“ server, where the specific Gigaset SW package can be installed. A SW package is including all the necessary files, scripts, tools and the manual (  ) for setting up a provisioning server. The provider only has to create a connection between the provisioning script and his data base containing the user specific account data.

## ■ SIP-Multicast mechanism

The SIP-Multicast mechanism is supported by most of the Gigaset VoIP phones and by the Gigaset PBX T300 and T500 (also supported by some products from other companies).

The mechanism is mainly designed for VoIP PBXs which are offering an own provisioning server for the configuration of connected VoIP phones.

The following example flow chart shows the principle of this mechanism:



# Gigaset

**MAC based autoprovisioning for  
retail devices**



# MAC based autoprovisioning for retail devices

## general

A VoIP-phone can be identified by its e.g. MAC address or another clear phone specific number. For the Gigaset VoIP phones the MAC address inclusive a checksum is used for identification. This „ID“ is printed on the housing and on the packaging. Additionally the phones (depends on the product) are containing a RFID chip with the same information.

The auto-provisioning of a retail VoIP phone is working as follows:

- Customer is connecting the phone to the Network and the phone is sending a provisioning request to the Gigaset provisioning server (default URL).
- The provisioning server is checking the variant ID (444 for a retail device) and the MAC address.
- If the phone is available in the Gigaset provisioning database the server sends a redirect URL to the phone.
- The phone now can start the provisioning using the new URL!

This provisioning procedure only will have success, if the Gigaset provisioning database is containing the MAC addresses of the phone for which the provisioning has to be done and the URL for the redirection!

A distributor or VoIP-Provider can enter the phone ID's via the WEB portal: <http://prov.gigaset.net>. There is also a XML-RPC Interface available (<http://prov.gigaset.net/apxml/rpc.do>).

Before the WEB portal can be used the Provider or distributor needs an account to the Gigaset provisioning server (ID and password). If there is a new Provider, please send a short information about the Provider/Provisioner (company, contact, address, etc.) to Gigaset System-Engineering. Creating a corresponding account it is also important if the customer will use HTTPS and/or Digest Authentication.

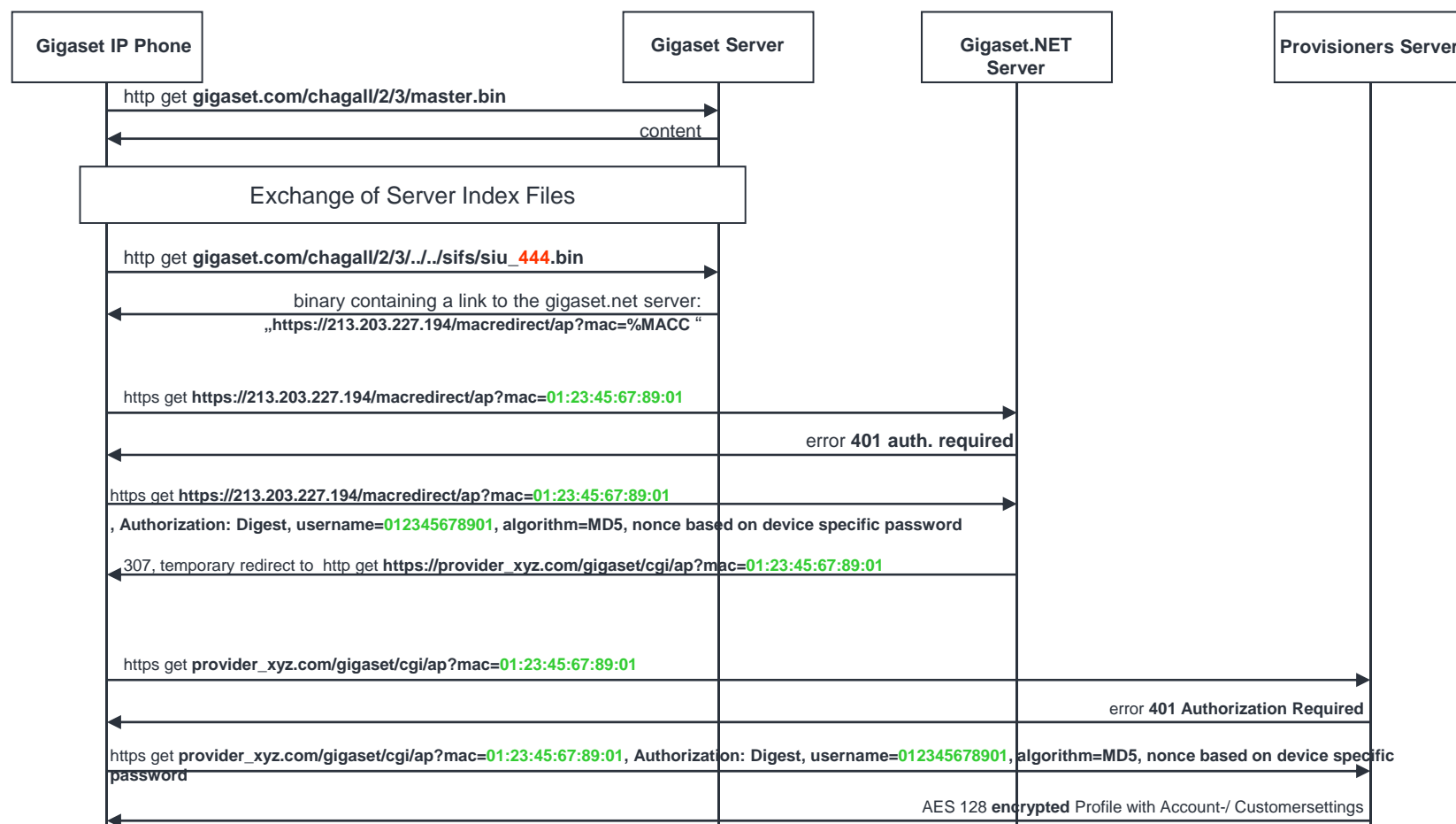
The actual specification:



# MAC based autoprovisioning for retail devices

## Message Sequenz Chart (MSC)

The following diagram shows in principle the message flow between a Gigaset IP Phone and the involved servers from Autoprovisioning point of view.



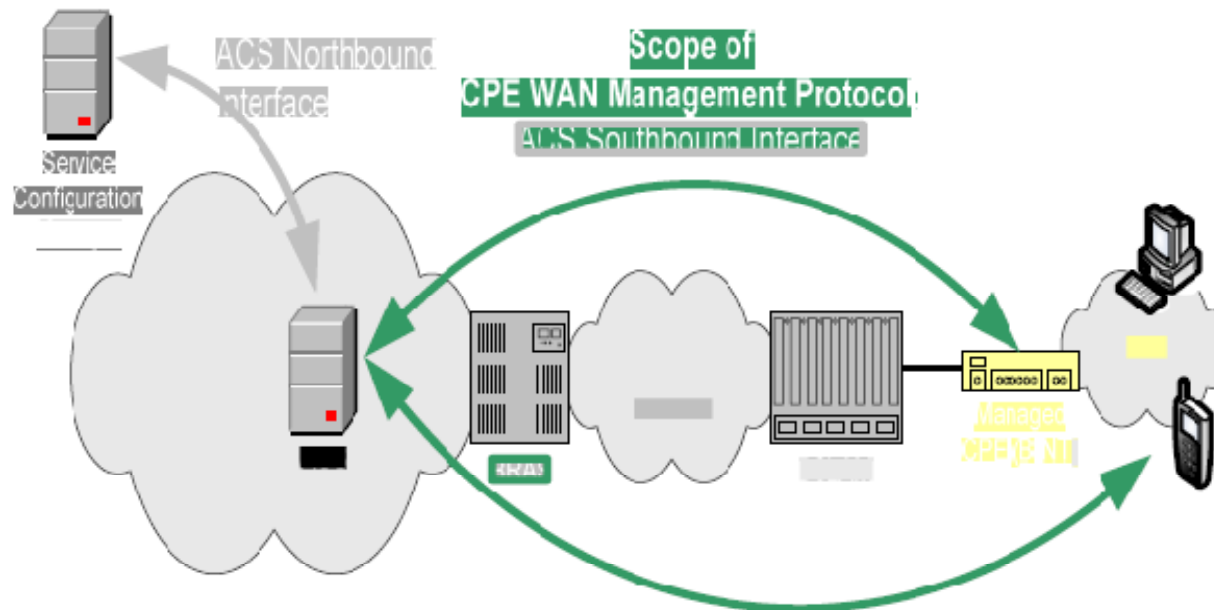
# Gigaset

## Remote management via TR069



## Remote management via TR069 Architecture and Functionality

The TR-069 is defined by the DSLHome Technical Working Group of the DSL Forum. It specifies the CPE WAN Management Protocol (CWMP) for the communication between a Customer Premises Equipment (CPE) and an Auto-Configuration Server (ACS). The ACS is a server within the provider's network that manages CPEs using TR-069. The diagram below illustrates the positions of the ACS and CPE within the DSL network.





# ■ Remote management via TR069

## Main topics ...

### Main topics which are agreed for the TR-069 implementation at Gigaset IP phones:

- all RPC methods as defined in TR-069 with relevance for Gigaset IP-phones are supported;  
[\(details on next pages\)](#)
- all VoIP-parameter of a Gigaset IP phone are supported within a data model based on TR-106 and TR-104;
- ACS initiated connection: support of TR-111 Part 1 (Device-Gateway Association);
- Security: A proprietary AES-128 solution will be used in order to offer at least a payload encryption for SW-release 7; SSL/TLS support will be implemented for SW-release 8;
- remote Firmware download using RPC Methods is implemented;
- a periodical initialization of sessions is also supported;

The features related are:

- TR104
- TR106
- TR111 / part1
- TR069
- SW-Update
- ACS initiated Connection

## Remote management via TR069

### Protocol Stack: overview

The protocol stack used by the CWMP is shown in a figure below:

<b>CPE / ACS Management Applications</b>	The TR-069 client and ACS use CWMP. The application is locally defined and not specified as part of the CWMP.
<b>RPC Methods</b>	The specific RPC methods that are defined by the CWMP.
<b>AES-128 (optional)</b>	The Advanced Encryption Standard (AES) is an encryption algorithm using block encryption of 128 bits in size.
<b>SOAP (XML)</b>	A standard XML-based syntax used to encode RPC's as specified in SOAP 1.1.
<b>HTTP</b>	Hypertext Transfer Protocol (RFC 2616 and RFC 2617).
<b>SSL / TLS</b>	The standard Internet transport layer security protocols.
<b>TCP / IP</b>	Standard TCP / IP.

## ■ Remote management via TR069

### Protocol Stack: HTTP

#### **Client / Server**

SOAP messages are carried between a CPE and an ACS using HTTP 1.1 where the CPE acts as the HTTP client and the ACS acts as the HTTP server. In case of Connection Requests, the ACS acts as the HTTP client and the CPE acts as the HTTP server.

#### **File Transfers**

Initiated by the ACS, the CPE is provided with the location of the file to be transferred, using HTTP as the transport protocol. The CPE then performs the transfer, and notifies the ACS of the success or failure. Chagall doesn't support the file upload which acc. to CWMP may be optionally initiated by a CPE.

The digest authentication must be used for file transfer. HTTP digest / md5 is supported in the current Gigaset IP phone.

#### **Use of Cookies**

To ensure that an ACS can make use of a session cookie, a CPE MUST support the use of cookies as defined in RFC 2965 including the return of the cookie value in each subsequent HTTP POST. Please note that a CPE need not to maintain a cookie beyond the duration of the session. The ACS might send old-style, new-style, or a mixture of both of these cookies, therefore the CPE MUST support the compatibility requirements of section 9.1 of RFC 2965.

CPE establishes a TCP connection and sends an HTTP request with *Inform* message. The CPE messages to the ACS do not contain any session cookies. During HTTP authentication stage or as a part of the *InformResponse*, the ACS sets an HTTP cookie in HTTP response. After the cookie has been set, the CPE resends the cookie in all subsequent HTTP requests within the same session, including any final empty posts used when indicating session termination.

#### **SOAP over HTTP**

The encoding of SOAP over HTTP extends the HTTP binding for SOAP. The 30 maximum number of SOAP envelopes supported is currently fixed to 1.

## Remote management via TR069

### RPC Methods

The table provides a summary of all RPC methods indicating the support in the Gigaset IP phones (e.g. Chagall) implementation.

**CPE Methods** listed are defined to be supported on a CPE. Only an ACS can call these methods.

**ACS Methods** listed are defined to be supported on an ACS. Only a CPE can call these methods.

**Optional RPC Methods** listed MAY optionally be supported on a Gigaset IP phone Rel7 or on an ACS. Currently, the only required optional method is *FactoryReset* (planned for a later SW release).

For CPE required and supported for SW Release 7.

For CPE required but not possible with a Gigaset IP phone.

CPE support planned for SW release 8.

For CPE optional and currently not supported.

Method name	CPE requirement	ACS requirement	Support for Swisscom
<b>CPE Methods</b>	<b>Responding</b>	<b>Calling</b>	
GetRPCMethods 1	REQUIRED	OPTIONAL	YES
SetParameterValues 1	REQUIRED	REQUIRED	YES
GetParameterValues 1	REQUIRED	REQUIRED	YES
GetParameterNames 1	REQUIRED	REQUIRED	YES
SetParameterAttributes 2	REQUIRED	OPTIONAL	NO
GetParameterAttributes 2	REQUIRED	OPTIONAL	NO
AddObject 2	REQUIRED	OPTIONAL	NO
DeleteObject 2	REQUIRED	OPTIONAL	NO
Reboot 3	REQUIRED	OPTIONAL	YES
Download 1	REQUIRED	REQUIRED	YES
Upload 4	OPTIONAL	OPTIONAL	NO
FactoryReset 3	OPTIONAL	OPTIONAL	YES
GetQueuedTransfers 4	OPTIONAL	OPTIONAL	NO
ScheduleInform 4	OPTIONAL	OPTIONAL	NO
SetVouchers 4	OPTIONAL	OPTIONAL	NO
GetOptions 4	OPTIONAL	OPTIONAL	NO
<b>ACS Methods</b>	<b>Calling</b>	<b>Responding</b>	
GetRPCMethods 4	OPTIONAL	REQUIRED	NO
Inform 1	REQUIRED	REQUIRED	YES
TransferComplete 1	REQUIRED	REQUIRED	YES
RequestDownload 4	OPTIONAL	OPTIONAL	NO
Kicked 4	OPTIONAL	OPTIONAL	NO

## ■ Remote management via TR069 additional planned RPC methods:

.... (working)

## ■ Remote management via TR069

### Security: TLS / SSL

**Main topics implemented for the “transport layer security” (TLS) at the Gigaset IP phones (depends on project, e.g. within the SW release 8 for “Chagall”):**

- TLS is implemented conform to RFC5246;
- HTTP over TLS is implemented conform to RFC2818;
- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC3647) is supported with a limited list of Server Root Certificates;
- the following cipher suites is supported:
  - SSL\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA
  - SSL\_RSA\_WITH\_RC4\_128\_SHA
  - SSL\_RSA\_WITH\_RC4\_128\_MD5
- as operational mode the “client mode” is used;
- root certificates can be entered via WEB-server and will be checked against target certificates;
- server authentication will be supported;
- secure channels: use of parallel running applications with parallel use of secured channels by each application at a time is supported;
- deriving further secure channels from existing secure channel is supported;

## ■ Remote management via TR069 further informations ...

Overview about used standards:



Microsoft  
PowerPoint Presentati

Detailed TR069 concept:



Adobe Acrobat  
Document

List of supported parameter:

(also included in "detailed TR069 concept")



Adobe Acrobat  
Document