OpenStage / OpenScape Desk Phone IP Provisioning Interface

Developer's Guide

A31003-S2000-R102-16-7620

Our Quality and Environmental Management Systems are implemented according to the requirements of the ISO9001 and ISO14001 standards and are certified by an external certification company.

unify.com

1 Getting Started

1.1 Overview

OpenStage SIP phones and OpenScape Desk Phones IP support the SIP protocol according to RFC 3261 and therefore can operate at any standard-compliant SIP server.

Moreover, a multitude of interfaces for control, configuration, and provisioning is available:

- Local user interface, graphical or text based: Allows for control and configuration both by the user and the administrator.

- Web-based interface: The phone has a built-in web server enabling both the user and the administrator to control and configure the phone via a standard web browser.

- Phone manager: A phone management tool for the user which allows for e. g. editing the local phonebook and synchronizing it with MS Outlook contact data. The software, which communicates over IP, is installed on the user's PC (Windows 2000, Windows XP, or Windows 7/8)

- **Provisioning interface**: The phone is controlled and configured by messages in XML format which are transmitted by HTTPS. In turn, the phone provides configuration and status information over the same interface. Moreover, when local changes have been executed on the phone, it informs the provisioning service automatically. Any kind of administration task is supported, such as updating the firmware on a selection of phones. Hence, mass deployment can be accomplished conveniently. Unlike many other VoIP phones, which are limited to prefabricated configuration files to be downloaded at startup, OpenStage phones can be deployed and provisioned by an interactive service at virtually any time.
  The interface supports two different Security Modes:
  - Default Mode: The devices cannot directly validate the authenticity of the provisioning server, but must rely on appropriate IP address / DHCP configuration only.
  - Secure Mode: Mutual authentication based on individual digital signatures is enforced, in accordance with the TLS standard. This allows the devices to check the server's authenticity directly. The required certificates and private keys are generated, managed and distributed by provisioning service.

This document contains information about the required infrastructure and describes the provisioning interface in detail.

1.2　　　Prerequisites

For developing and operating a provisioning service for OpenStage phones, please ensure that you have the following prerequisites.

1. OpenStage phone or OpenScape Desk Phone IP with appropriate firmware version.

2. Infrastructure:

   • Connection to an IP network.

   • (Recommended:) DHCP server to communicate the IP address of the provisioning server to the phone.

   • Web browser to configure the application on the phone using the Web Based Management. Alternatively, the phone's local menu can be used.

   • FTP or HTTPS server for file and software deployment.

   • SIP server

1.3 Basic Network Infrastructure

1.3.1 Standard Network Structure

All components are connected via LAN. The OpenStage IP phones and OpenScape Desk Phones IP receive their basic network configuration from the DHCP server and/or from LLDP-MED. This may include a VLAN ID, if a VLAN infrastructure is required. Further configuration is done via the provisioning service. Additionally, many configuration and deployment tasks can be accomplished via the phone's web interface. For uploading files, such as ringtones, screen-saver images, or firmware, to the phone, a file server is required (FTP or HTTPS). To enable telephony, the phones are registered at a SIP server.
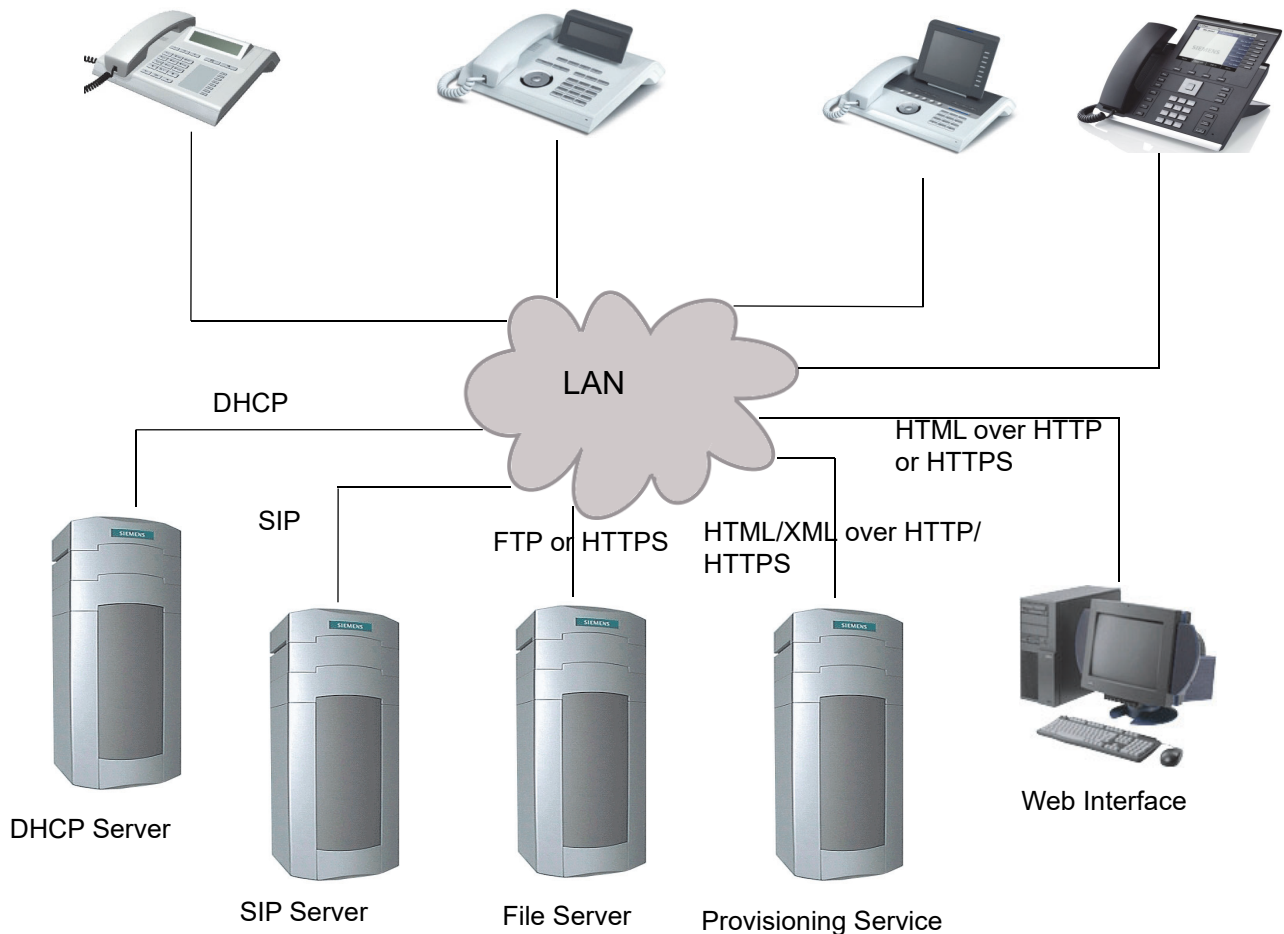
1.3.2 Firewall and NAT

If the phones and the provisioning service reside in different networks or subnets, which are separated by a firewall and/or NAT, it may be impossible for the provisioning service to establish a connection with the phones. In this case, provisioning service driven interactions may not be possible (for details about provisioning service driven interactions, please refer to Section 1.4.4.2, "Contact-me Messages" and Section 3.1.2, "Provisioning Service Driven Interaction").

To enable a solution for this problem, the phone can be configured to periodically poll the provisioning service, or a special proxy, for new messages. Thus, provisioning service driven interactions are possible even when the provisioning service is located behind a firewall, or in a DMZ. For further information, please refer to Section 1.4.4.3, "Polling Request To Bridge A Firewall" and Section 3.1.2.2, "Provisioning Service Located Behind A Firewall".

Firewall

Periodic poll over HTTP

XML messages over
HTTP/HTTPS

Provisioning Service,
possibly in combina-
tion with a proxy
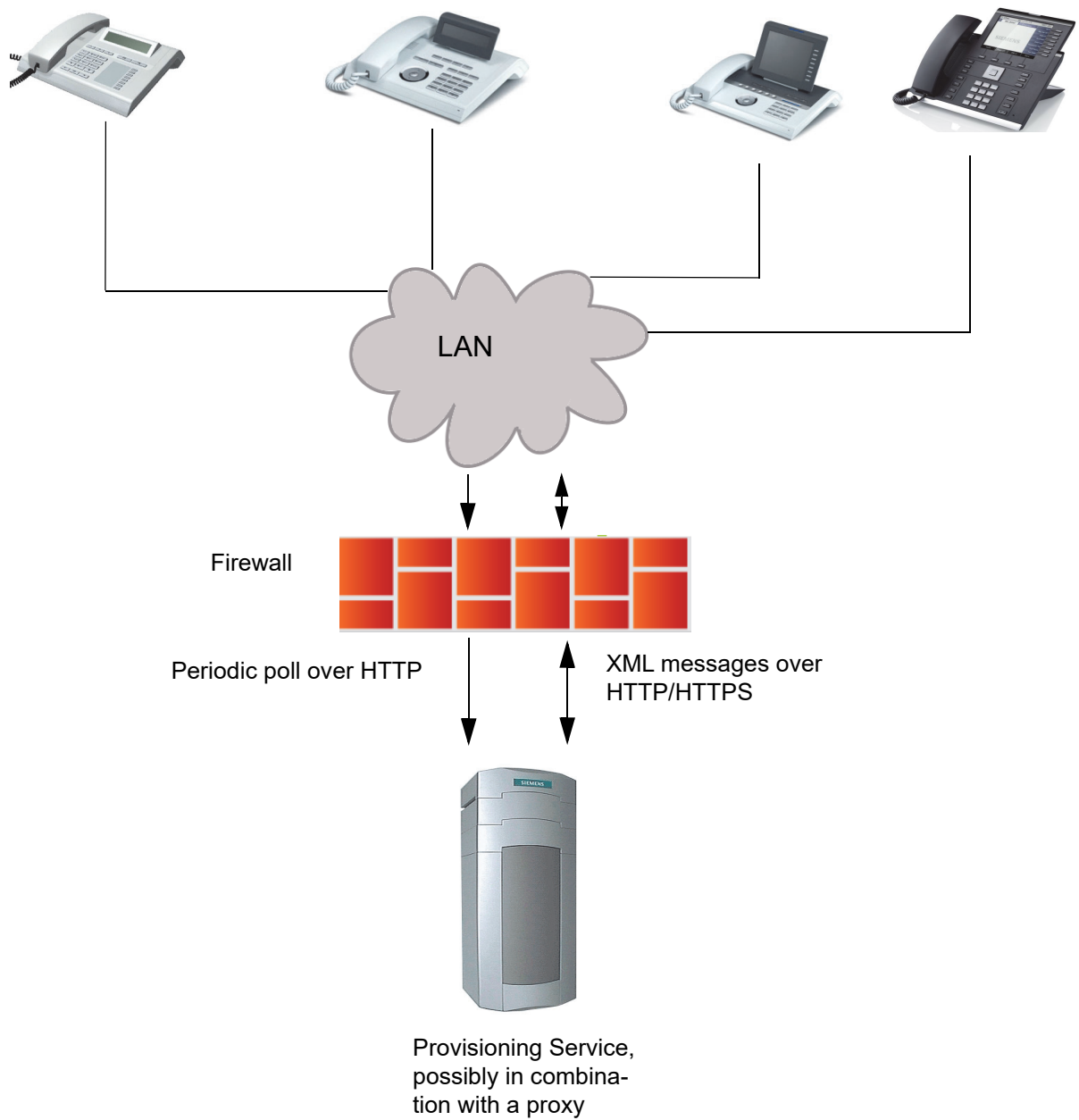
1.4 Network Communication

This chapter contains the elementary HTTP/HTTPS communication required for interaction between the phone and the provisioning service. For a high-level description of the possible interactions, please refer to Section 3, "Basic Communication Procedures".

> To prevent communication problems in the HTTP layer, please consider the following:
> - The keep-alive timeout in the provisioning server should be set to 10.
> - The provisioning server must be set to use HTTP 1.1.
> - With phone firmware V2R2 and lower, the provisioning server must not use HTTP chunked encoding. This problem is solved with firmware version V3.

1.4.1 Protocols

When the provisioning service wants to start communicating with a phone, it has to send a special contact-me message. This message, as well as the response from the phone, is transmitted via HTTP (clear text, not encrypted).

All further communication between the provisioning service and the phone consists of messages in XML format, which are transmitted using HTTP v1.1 over TLS (HTTPS).

> OpenStage phones and OpenScape Desk Phone IP expect the interface on port 18443 to be TLS-encrypted (HTTPS). Therefore, the provisioning server needs to configure SSL/TLS on this listener port. In Default Mode OpenStage phones and OpenScape Desk Phone IP do not authenticate the server, any certificate is suitable. In Secure Mode OpenStage phones and OpenScape Desk Phone IP requires certificates supported by provisioning service. All further requests of this device are performed on port 18444. For information on importing or creating a suitable TLS web server certificate, please refer the relevant documentation for your web server.

1.4.2 Ports

On the phone side, the destination port for messages to the provisioning server can be freely chosen. The address and port number of the provisioning service are defined under **Network > Update service** in the phone's web interface or provided by DHCP (see Section 2.2, "Extended Configuration").

For sending contact-me messages to the phone in order to initiate an interaction, the provisioning service must use port 8085 as destination port.

1.4.3   HTTP Sessions

As some interactions may consist of several subsequent HTTPS request/response messages, it must be possible to establish HTTP sessions. For this purpose, OpenStage phones and OpenScape Desk Phone IP support HTTP cookies.

To end a session, the provisioning server sends a special clean-up message to the phone. In some error cases, e. g. when the received XML is invalid, the phone will send a clean-up message on its part.

1.4.4 HTTP/HTTPS Messages

Generally, two types of HTTP/HTTPS messages are used by the provisioning interface: XML messages for phone control and data exchange, and HTML messages for initiating an interaction by the provisioning service.

> The content-length of HTTPS responses should be set to the length of the XML message content.

1.4.4.1 XML Messages For Data Exchange

Regular XML messages used for interactions between phone and provisioning service are transmitted via HTTPS. The HTTP method is `POST`, and the `Content-type` is `text/xml`. The structure of the XML messages is described in Section 3, "Basic Communication Procedures".

This is the structure of a URI for a request sent by the phone to the provisioning server:

`https://<host>:<port>/<path to provisioning service>`

Example: `https://192.168.1.103:18443/provisioningService`

1.4.4.2 Contact-me Messages

With this type of message, the provisioning service announces to the phone that it has a new message for the phone.

Initial contact-me messages from the provisioning service are transmitted via non-encrypted HTTP. The `POST` method is used. The HTTP `Content-type` is `application/x-www-form-urlencoded`. The following parameters must/can be sent to the phone:

*   `ContactMe` (required): Set to true if a response from the phone is expected.

*   `dls_ip_addr` (optional): Target IP address for the response from the phone.

*   `dls_ip_port` (optional): Port associated with the IP address provided with `dls_ip_addr`.

The parameters described above enable the provisioning service to scan a certain range of IP addresses for phones simply by sending contact-me requests to each address consecutively.

The complete URI for contact-me messages has the following structure:

`http://<IP address>:8085/contact_dls.html/ContactDLS`

Example: `http://192.168.1.4:8085/contact_dls.html/ContactDLS`

The following examples show the HTTP communication initiated by a contact-me message.

Contact-me Message Example

```
POST /contact_dls.html/ContactDLS HTTP/1.1
Content-type: application/x-www-form-urlencoded; charset=utf-8
User-Agent: Jakarta Commons-HttpClient/2.0final
Host: 192.168.1.103:8088
Content-Length: 14

ContactMe=true
```

Phone Response to Contact-me Example

The phone sends a corresponding HTTP response. The HTTP status is `204` (no content). The HTTP `Content-type` is `text/html`.

```
HTTP/1.1 204 No Content
Server: DlsClient
Content-Length: 0
Content-type: text/html
```

1.4.4.3   Polling Request To Bridge A Firewall

When the provisioning service is located behind a firewall, or in a DMZ, it may have no possibility to send a contact-me message to the phone. To enable provisioning service driven interactions despite this limitation, the phone can be configured to periodically poll the provisioning service, or a special proxy, for new messages. This configuration is done by the provisioning service, for instance, at phone startup; for the relevant data items, see Section 6.1, "Provisioning Service Related".

The polling request is an HTTP GET request which contains a particular key/value pair to identify the phone. The key is `device-id`, and the value is the phone's MAC address as a parameter. The structure is as follows:

```
http://<target address>/dcmp/contact-me?device-id=<MAC address>
```

Example:

```
http://provisioning.mycompany.com/dcmp/contact-me?device-
id=12:34:56:78:9a:bc
```

2 DHCP

The use of DHCP for network configuration is highly recommended. To enable an OpenStage phone or OpenScape Desk Phone IP to contact the provisioning service immediately on start-up, the appropriate contact address must be provided beforehand. This can be done by DHCP. Moreover, this method prevents faking a provisioning service with malicious intentions, as the phone will only contact the provisioning service whose address it has learned from the DHCP server.

> Please ensure that the phone's DHCP client is enabled. For configuration instructions, see the OpenStage or OpenScape Desk Phone IP Administration Manual.

> Parameters that have been set by DHCP cannot be modified afterwards, regardless of the interface in use (local menu, web interface, provisioning interface).

2.1 Basic Network Configuration

For basic networking functionality, DHCP must provide the following parameters:
- **IP Address**: IP address for the phone.
- **Subnet Mask (option #1 "Subnet Mask")**: Subnet mask of the phone.
- **Default Route (option #3 "Router")**: IP address of the default gateway which is used for connections beyond the subnet.
- **DNS IP Addresses (option #6 "Domain Server")**: IP addresses of the primary and secondary DNS servers.

2.2 Extended Configuration

Additionally, it is possible to provide these parameters by DHCP, as an alternative to setting them manually, or via provisioning service.

- **SNTP IP Address (option #42 "NTP Servers")**: IP address or hostname of the SNTP server to be used by the phone.

- **Timezone offset (option #2 "Time Offset")**: Offset in seconds in relationship to the UTC time provided by the SNTP server.

- **SIP server (option #120 "SIP Servers DHCP Option")**: The SIP server to be used by the phone.

- **Domain name (option #15 "Domain Name")**: The name of the DNS domain wherein the phone is residing.

- **VLAN ID**: Necessary if the phone operates in a VLAN (Virtual LAN). This parameter can be provided by means of a "vendor-encapsulated-options" option.

- **Provisioning service contact address**: Enables the phone to contact the provisioning service immediately on startup. This parameter can be provided by means of a `vendor-encapsulated-options` option.

2.3 Example DHCP server configuration

The following description demonstrates by example how a ISC DHCP server can be configured in order to build up a working infrastructure for OpenStage phones or OpenScape Desk Phone IP.

The configuration example has been tested with ISC DHCP server version 3 running on Debian Linux (package: dhcp3-server).

On startup, the OpenStage phone or OpenScape Desk Phone IP sends a DHCP discovery message which contains the `vendor-class-identifier` option. The fixed value is `OptiIpPhone`. This identifier is used by the DHCP server to send a specified set of sub-options to each OpenStage phone or OpenScape Desk Phone IP by means of vendor encapsulated options. The `vendor-encapsulated-options` option allows for defining custom-made options in either a single series of bytes or a sequence of parameters which is constructed from:

1. the single-byte vendor-specific option code;

2. the single-byte length indication for the option data (the length does not include itself or the option code);

3. the data itself in as many bytes of data as are specified in the length indication.

The value of the `vendor-encapsulated-options` option can either be set directly by coding the bytes in hexadecimal notation, or, preferably, by using the `option space` statement. This statement is available with ISC DHCP 3.0 onwards.

To assign the specific `vendor-encapsulated-options` to the appropriate devices, the use of classes is recommended. In the example, the `vendor-classes` class is divided into sub-classes automatically for each `vendor-class-identifier` option that is received from the clients. As OpenStage phones or OpenScape Desk Phone IP send the value `OptiIpPhone`, the specifications for these phones are defined in the corresponding sub-class.

Example dhcpd.conf

```
# General configuration for all clients in the subnet
subnet 192.168.2.0 netmask 255.255.255.0 {
    option domain-name-servers 192.168.2.2;
    option broadcast-address 192.168.2.255;
    option routers 192.168.2.251;
    option subnet-mask 255.255.255.0;
    option domain-name "phones.intranet";
    option ntp-servers 192.43.244.18;
    option time-offset 3600;
    default-lease-time 864000;
    max-lease-time 8640000;
}

# Set up an option space to contain the vendor-encapsulated options
option space OpenStage;
option OpenStage.vendor code 1 = string;
option OpenStage.vlanid code 2 = unsigned integer 32;
option OpenStage.dls code 3 = string;

# Each vendor-class-identifier will constitute a class
class "vendor-classes" {
    match option vendor-class-identifier;
}

# Specifications for OpenStage phones
subclass "vendor-classes" "OptiIpPhone" {
    vendor-option-space OpenStage;
    option OpenStage.vendor "Siemens";
    option OpenStage.vlanid 4;
    option OpenStage.dls "sdlp://192.168.2.103:18443";
    option sip-server 192.168.2.117;
}
```

3 Basic Communication Procedures

This chapter describes the interaction between the phone and the provisioning server in detail. Depending on the situation and the intended task, the interaction will be started by the phone or by the provisioning service. First, we will explain the basic message flow.

> Depending on the amount of configuration data, the XML messages might become quite long. In order to prevent overflow problems, longer messages can be split into fragments. For details, see Section 3.7, "Message Fragmentation".

3.1 Basic Message Flow

3.1.1 Phone Driven Interaction

A typical reason for contacting the provisioning service is a configuration change on the phone. The message flow might proceed as follows: In an initial HTTPS request, the phone tells the provisioning service that it is ready for operation. In its response, the provisioning service asks for all current settings (data items). Hence, the phone sends a complete list of settings, allowing the provisioning service to update its database. At this point, the provisioning service may decide whether the phone's configuration needs to be changed or not. If not, the provisioning service should send a CleanUp message, telling the phone not to expect any further messages. This will also end the HTTPS session.

Phone

Provisioning Service

HTTPS Request
Initial message, declaring
the reason for contact,
which is one of the follow-
ing:

– Startup (=registration
  with the provisioning
  service)

– Configuration changes

– Hardware connected/
  disconnected

– Indicate file deploy-
  ment status

HTTPS Response
Provisioning service re-
quests all data items from
the phone

HTTPS Request
Phone sends all available
data items

HTTPS Response
CleanUp message tells
the phone that the interac-
tion is finished

3.1.2 Provisioning Service Driven Interaction

3.1.2.1 No Firewall

A typical reason for contacting the phone is the modification of one or more configuration settings. The message flow might proceed as follows:

In an initial HTTP request, the provisioning service sends a contact-me message to the phone. The phone responds to this request, and afterwards transmits a basic set of data items containing configuration settings to the provisioning service.

Now, the provisioning service sends a list of data items that have to be changed. If the phone is ready, it will confirm the action and execute the commands or configuration changes. If the phone is busy, it will send an appropriate message to the provisioning service (see Section 3.3.4, "Reason for Contact"). Starting with V3R3 the provisioning service sends a CleanUp with a 'send-solicited' item. The phones reaction will be to schedule an automatic solicited connection to the provisioning service when the busy condition is cleared.

If the phone is downgraded then any receipt of a Send-solicited item in a CleanUp action from the provisioning service will result in the pre-existing behaviour. If the provisioning service has been upgraded to expect the 'Send-solicited'-feature is supported then it is the responsibility of the provisioning service to ensure that the use of 'send-solicited' is restricted to the defined DCMP use when a phone with an prior bind is involved.

In order to make sure that the desired changes have been made, the provisioning service should send a read request for the modified data. Hereupon, the phone sends back the modified items. Finally, the provisioning service terminates the interaction with a CleanUp message.

Phone

Provisioning Service
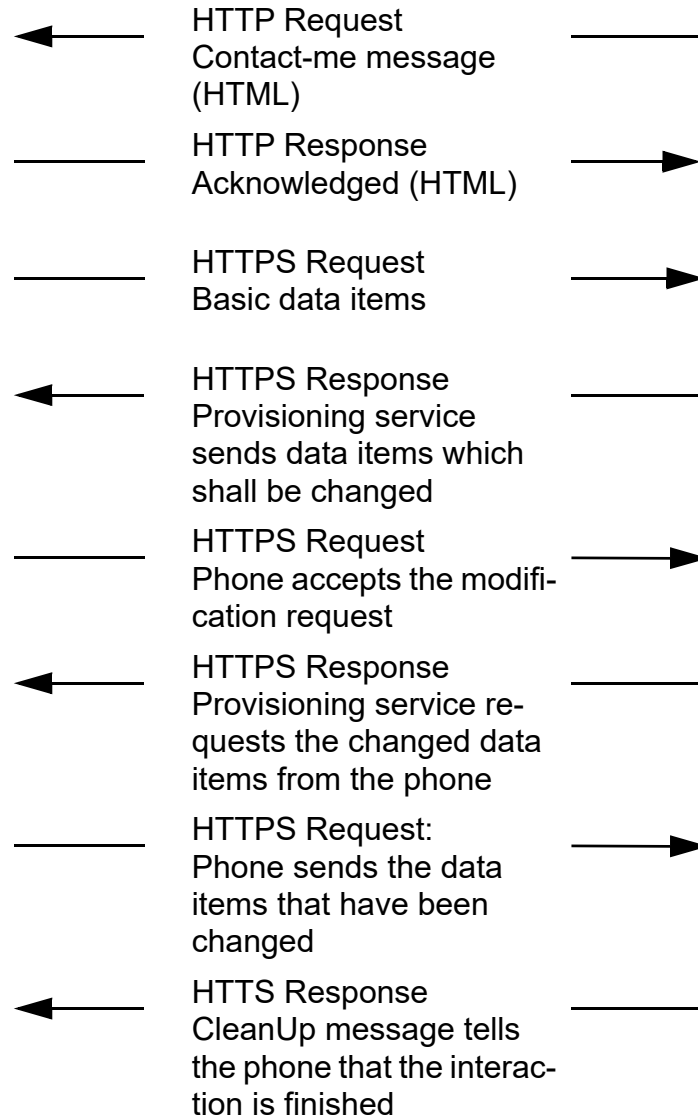
HTTP Request
Contact-me message
(HTML)

HTTP Response
Acknowledged (HTML)

HTTPS Request
Basic data items

HTTPS Response
Provisioning service
sends data items which
shall be changed

HTTPS Request
Phone accepts the modifi-
cation request

HTTPS Response
Provisioning service re-
quests the changed data
items from the phone

HTTPS Request:
Phone sends the data
items that have been
changed

HTTS Response
CleanUp message tells
the phone that the interac-
tion is finished

3.1.2.2 Provisioning Service Located Behind A Firewall

When the provisioning service is located behind a firewall, or in a DMZ, it may have no possibility to send a contact-me message to the phone. To enable provisioning service driven interactions despite this limitation, the phone can be configured so that it periodically polls the provisioning service, or a special proxy, for new messages. The procedure is as follows:

1. On startup, the phone receives the address and port of the provisioning service from the DHCP server.

2. During the startup procedure, the phone contacts the provisioning service (see Section 3.5.1, "An Exemplary Startup Interaction").

3. The provisioning service instructs the phone to poll the provisioning service, or a proxy, along with the target URL for the polling messages, and the polling interval (see Section 6.1, "Provisioning Service Related").

4. From now on, the phone will periodically poll the provisioning service, or proxy, according to the configured polling interval.

In the following message flow, the phone polls the provisioning service or proxy, and the provisioning service resp. proxy has no new message for the phone:

Phone

HTTP Request
Polling the provisioning
service or proxy

HTTP Response
Status=200 OK

Provisioning Service / proxy
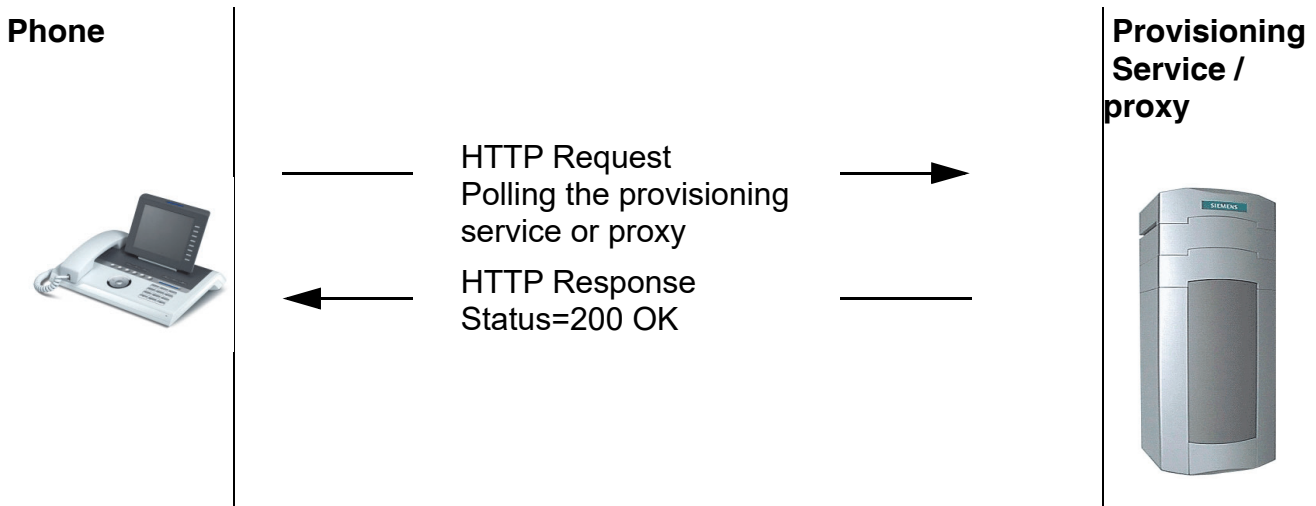
In this message flow, the phone polls the provisioning service or proxy, and the provisioning service resp. proxy has a new message for the phone:

Phone

Provisioning Service / proxy

HTTP Request
Polls the provisioning service or proxy for new messages

HTTP Response
Status=202 Accepted

HTTP Request
Reason for contact:
solicited
<Basic data items>

HTTPS Response
Provisioning service
sends data items which
shall be changed

HTTPS Request
Phone accepts the modification request

HTTS Response
CleanUp message tells
the phone that the interaction is finished

3.2   Configuration Data

Configuration and control data is communicated in data items which act as containers for the parameters proper. Most of the simpler items are defined by the `name` attribute and the content of the element.

The attributes `name` and `index` are used in messages sent by the phone, and in messages sent by the provisioning service. The `status` attribute only exists in responses from the phone.

The `item` element can have the following attributes:

Attribute	Value	Description
`name` (mandatory)	Enumerated: Tag name	Identifier for the item. However, more than one `item` element may appear within one message (See `index` underneath).
`index` (optional)	Number	Enables multiple instances of one item. It represents the sequential number of a particular instance of an item.
`type` (optional)	String	An arbitrary value may be associated with the item. Currently, this attribute is not used.
`status` (optional)	`failed`	The phone did not accept the value of this item.
	`unknown item`	An item with this name is not known.
	`read only`	The value of the item cannot be modified.
	`invalid index`	The index of this item is out of the range or does not make sense in this context.
	`unexpected item`	This item was not expected by the phone, or within this context.
	`not supported`	This item is not implemented yet in the phone.
	`invalid data`	The phone does not accept the value of this item.
	`undefined status`	Some other problem has occurred.

Examples

`<Item name="e164">49897223290</Item>` - E.164 number of the phone

`<Item name="device-type">OpenStage 60</Item>` - type of phone

`<Item index="1" name="ldap-server-address">ldap.mycompany.com</Item>` - DNS name (or IP address) of the first LDAP server to be queried

`<Item name="reg-addr">192.168.1.117</Item>` - IP address of the SIP server (registrar) at which the phone is registered or shall be registrated

3.3 Phone Message Structure

3.3.1 Initial Message From the Phone

When the phone initiates an interaction with the provisioning service, it will include at least the following data items in its message:

Item	Description
`contact-me-uri`	The provisioning service must send its contact-me messages to this fully qualified URI in order to start an interaction with the phone.
`mac-addr`	Contains the phone's MAC address, which is eligible as a unique identifier for the phone.
`e164`	This is the E.164 number of the phone. It can be used as additional or alternative identifier in case an identification by the `mac-addr` alone should fail. The `E.164` item can be rewritten by the provisioning service. If so, the new value will be used by the phone for subsequent interactions.

Table 3-1

3.3.2 Root Element

The root element of any message from the phone to the provisioning service is `WorkpointMessage`. For the corresponding XML schema, please refer to Section 3.5.1.2, "XML Data Exchange".

3.3.3 Message Element

The root element contains another container element, `Message`. It has a mandatory attribute named `nonce`; its task is to prevent replay attacks. Any reply by the provisioning service contains this attribute. With the optional attribute `maxItems`, the phone can define the maximum number of items allowed in one single message document from the provisioning service. If the reply requires a greater number of items, it must be fragmented (see Section 3.7, "Message Fragmentation").If `maxItems` is set to -1, there is no limitation.

3.3.4 Reason for Contact

The `ReasonForContact` element indicates the motivation for sending a message to the provisioning service. See the following table for possible values:

Content Value	Description
start-up	On each startup or reset, the phone sends a message to the provisioning service with `reason` set to this value. This can be viewed as a registration with the provisioning service.
local-changes	Some configuration changes have been made locally, that is, by the local phone menu or by the phone's web interface.
inventory-changes	Some inventory-related items have changed, due to a new side-car or adaptor that has been connected.
status	The phone communicates the status of a file transfer initiated earlier by the provisioning service (see Section 3.6.7, "File Provisioning").
solicited	The phone has received a contact-me message from the provisioning service and is calling back for further actions.
reply-to	This message is a reply to a particular message from the provisioning service. As it is part of a complex interaction between phone and provisioning service, it is recommended to establish an HTTP session by using cookies. If so, OpenStage phones will present a valid session-cookie along with this message. Further specifications can be given via the attributes `action` and `status`, and, if applicable, via `fragment` (see next table).
clean-up	If the phone recognizes any problem, either due to its internal state or due to a corrupted reply from the provisioning service, it will end the interaction deliberately by sending this value. Further specifications can be given via the ItemList, e.g. `<Item name="cleanup-reason"> password retries exceeded</Item>` when number of retries for PIN entry at the device in Secure Mode has exceeded.

Furthermore, the `ReasonForContact` element has additional attributes, which are relevant if the reason is `reply-to`:

Attribute	Value	Description
`action`	action name	Contains the action name of the message from the provisioning service to which this message is a reply. For details, see Section 3.4.2, "Action Type".
`status`	`accepted`	The action in question is accepted.
	`failed`	The action is not accepted or is unsupported.
	`busy`	The phone is busy and therefore cannot accept the action.
`fragment`	`next`	This attribute is needed only if the list of items has to be fractioned because of its length. If one or more message containing further fragments is expected, this value is used.
	`final`	If the list of items is fractioned, and the current message contains the last fragment, this value is used.

For examples, see Section 3.5.1.2, "XML Data Exchange" and Section 3.5.2.2, "XML Data Exchange (up to OpenStage V2R1)".

3.4   Provisioning Service Message Structure

3.4.1   Initiation

Before issuing XML messages to the phone, the provisioning service must announce to the phone that it desires an interaction with it. For details, see Section 1.4.4.2, "Contact-me Messages".

> ⓘ In case a firewall/DMZ should prevent the provisioning service from initiating an interaction with the phone, please refer to Section 3.1.2.2, "Provisioning Service Located Behind A Firewall".

> ⓘ The character encoding of the XML data sent to the phone should be UTF-8 in order to allow for special characters, such as german umlaut.

3.4.2   Action Type

Any message from the provisioning service must contain the Action element. It determines the activity the phone should perform. The possible actions are listed in the following table:

Content Value	Description
ReadAllItems	The phone will deliver its whole set of items. However, this does not include certificates.
WriteItems	The phone is requested to modify its current settings for those items which are contained in the message. Please note that this request will be denied when the phone is in a call (for details, please see Section 3.6.4, "Modify Phone Settings").
ReadItems	The provisioning service asks the phone to deliver the values of a certain subset of items.
Restart	The provisioning service asks the phone to restart.
FileDeployment	The phone is requested to download a file from an FTP or HTTPS server denoted by the items contained in the message.
SoftwareDeployment	The phone is requested to download a firmware image from a FTP or HTTPS Server denoted by the items contained in the message.

Content Value	Description
`CleanUp`	In complex interactions, this is the final message indicating the termination of the whole interaction cycle. It indicates to the phone that the TLS connection can be cleared. The HTTPS session will also be closed. Further specifications can be given via the ItemList. E.g. <Item name="cleanup-reason">wrong TAN from device</Item>, if the device doesn't send the required TAN. If the 'send-solicited' is set in ItemList (>=V3R3) the phone scedules an automatic solicited connection to the provisioning service when the busy condition is cleared.
`GetNextFragment`	In case the phone indicates that the current message contains only a fraction of the items requested, the provisioning service uses this action to request the next fragment.

3.5 Phone Driven Interactions

Three different kinds of activities initiated by phones can be distinguished:

1. Register with the provisioning service after startup, either initial startup, subsequent resets or a factory reset.

> Please ensure to provide the phone with the contact address of the provisioning service (see Section 2.2, "Extended Configuration"). Otherwise, it will not be able to register with the provisioning service after a factory reset.

2. Inform the provisioning service about local configuration changes, even in case of a factory reset.

> Please ensure to provide the phone with the contact address of the provisioning service (see Section 2.2, "Extended Configuration"). Otherwise, it will not be able to register with the provisioning service after a factory reset.

3. Inform the provisioning service about the status of a software or file deployment.

3.5.1 An Exemplary Startup Interaction

3.5.1.1 Message Flow

On startup, the phone informs the provisioning service about its existence. The following diagram shows an example message flow which might occur on phone startup:

	Phone		**Provisioning Service**
1	⎯⎯	HTTPS Request Reason for contact: start-up <Basic data items>	⟶
2	⟵	HTTPS Response Action: ReadAllItems	⎯⎯
3	⎯⎯	HTTPS Request Reason for contact: reply-to <All data items>	⟶
4	⟵	HTTPS Response CleanUp	⎯⎯
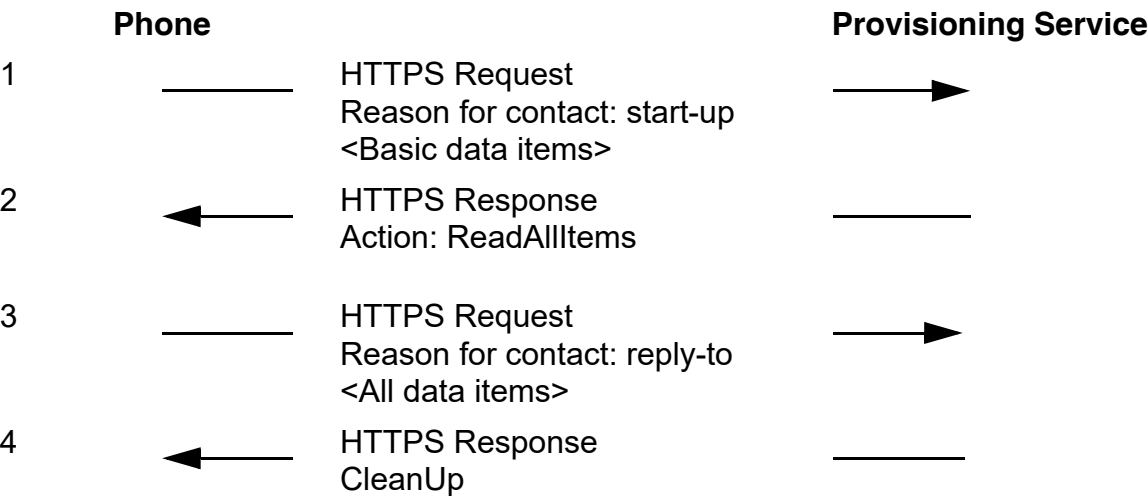
> ⓘ A new message flow starts as soon as a new connection to the provisioning service is established.

3.5.1.2 XML Data Exchange

1. At startup, the phone sends a set of data to the provisioning service. See the following example:

```
<WorkpointMessage
    xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="ab15234de14f15a667c6f8d">
        <ReasonForContact>start-up</ReasonForContact>
        <ItemList>
            <Item name="device-type">OpenStage 60</Item>
            <Item name="related-device-type">OpenStage 60</Item>
            <Item name="software-type">Siemens SIP</Item>
            <Item name="related-software-type">Siemens SIP</Item>
            <Item name="contact-me-uri">
                http://192.168.3.33:8085/contact_dls.html/ContactDLS
            </Item>
            <Item name="mac-addr">00:01:E3:00:A9:F3</Item>
            <Item name="configuration-changed-flag">false</Item>
            <Item name="part-number">S30817-S7403-A101-015</Item>
            <Item name="sip-mobility-state">0</Item>
            <Item name="e164">49897223290</Item>
            <Item name="user-pwd">123456</Item>
            <Item status="failed" name="user-pwd-unicode"/>
            <Item name="basic-e164">49897223290</Item>
            <Item name="mobility-enabled">false</Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

2. When the provisioning service has received the message from the phone, it sends an appropriate response, including the nonce value received by the phone, and a session cookie. The nonce value will be the same for all subsequent messages within this message flow. In this response, the provisioning service may request all items from the phone in order to gain comprehensive knowledge about its settings. However, if the phone is already known to the provisioning service, it will be sufficient to look at the `configuration-changed-flag` item. By setting it to `false`, the phone indicates that the configuration is still the same as with the last data exchange. See the following example:

```
<DLSMessage
    xsi:schemaLocation="http://mydomain/provisioning"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://mydomain/provisioning">
    <Message nonce="ab15234de14f15a667c6f8d">
        <Action>ReadAllItems</Action>
    </Message>
</DLSMessage>
```

3. Next, the phone sends the desired data. Note the content of `ReasonForContact` and the `action` attribute:

```
<WorkpointMessage
    xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="ab15234de14f15a667c6f8d">
        <ReasonForContact action="ReadAllItems"
            status="accepted">reply-to
        </ReasonForContact>
        <ItemList>
            <Item name="...">...</Item>
            <Item name="...">...</Item>
            ...
        </ItemList>
    </Message>
</WorkpointMessage>
```

4. The interaction, as well as the HTTPS session, is closed by the provisioning service, which is sending a CleanUp message:

```
<DLSMessage
    xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="ab15234de14f15a667c6f8d">
        <Action>CleanUp</Action>
    </Message>
</DLSMessage>
```

3.5.1.3   Items Sent On Startup and Configuration Change

The following table describes the items typically sent by an OpenStage SIP phone or Open-Scape Desk Phone IP on startup, or when the configuration has changed:

Item Name	Values	Description
device-type	OpenStage 15 OpenStage 20E OpenStage 20 OpenStage 40 OpenStage 60 OpenStage 80	Phone variant. This value is displayed in the banner of the web interface.
related-device-type	OpenStage 15 OpenStage 20E OpenStage 20 OpenStage 40 OpenStage 60 OpenStage 80	Phone variant. This represents the hardware type.
software-type	Siemens SIP	Firmware type used by the phone. For OpenStage SIP phones, this value is as indicated here.
related-software-type	Siemens SIP	Firmware type used by the phone. For OpenStage SIP phones, this value is as indicated here.
contact-me-uri	String Max. 255 characters	This is the URI to be used by the provisioning service in order to send messages to the phone. It is based on the phone's IP address.
mac-addr	MAC address	The unique MAC address of the phone can be used as an identifier for the device.

Item Name	Values	Description
`configuration-changed-flag`	`true` `false`	Indicates whether any configuration parameter has been changed since the last data exchange between phone and provisioning service. If set to true, the provisioning service should update its database.
`part-number`	String Max. 25 characters	Part number of the phone. Example: `S30817-S7403-A103`.
`e164`	String Max. 64 characters	The actual E.164 number of the phone.
`user-pwd`	String 6 -24 ASCII characters	Password for access to the phone's user menu via local menu or WBM.

3.5.2 Local Changes in Phone Configuration

A short while after the user or administrator has changed the configuration, the phone will send an appropriate message to the provisioning service in order to keep it up-to-date. Accordingly, the `ReasonForContact` is now set to `local-changes`.

For OpenStage phones with firmware version V2R2 onwards, the message flow is simpler, as the phone includes the changed data in its first message.

3.5.2.1 Message Flow (up to OpenStage V2R1)
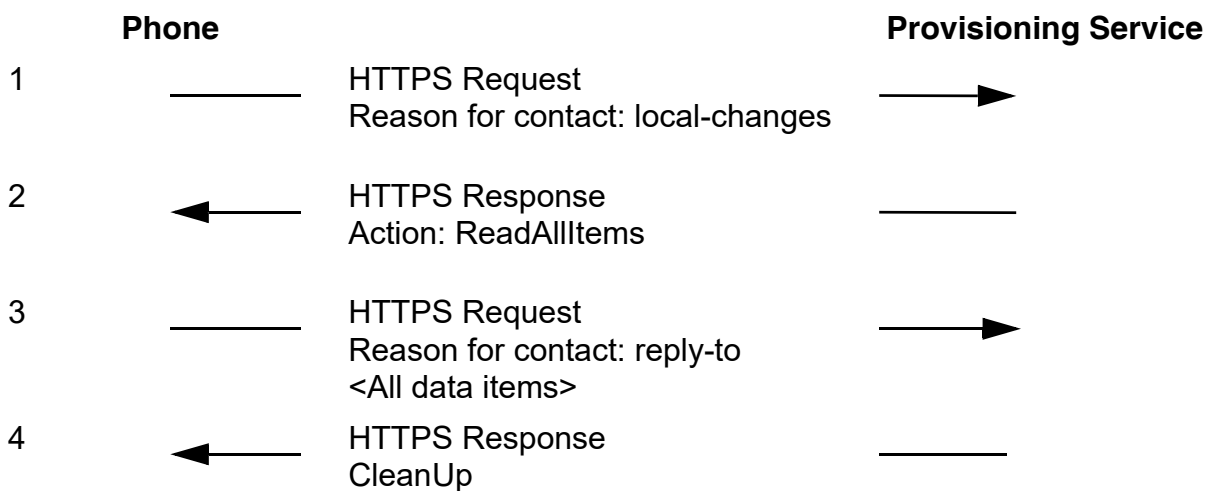
	Phone		**Provisioning Service**
1	————	HTTPS Request Reason for contact: local-changes	———▶
2	◀————	HTTPS Response Action: ReadAllItems	————
3	————	HTTPS Request Reason for contact: reply-to <All data items>	———▶
4	◀————	HTTPS Response CleanUp	————

3.5.2.2   XML Data Exchange (up to OpenStage V2R1)

1. The following example shows XML data sent from a phone to the provisioning service after a local configuration change. Note the value of `configuration-changed-flag`:

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message maxItems="-1"
    nonce="BD9438C65D42D90F566E2D03D6083602">
        <ReasonForContact>local-changes</ReasonForContact>
        <ItemList>
            <Item name="device-type">OpenStage 60</Item>
            <Item name="related-device-type">OpenStage 60</Item>
            <Item status="failed" name="gigabit-ethernet"/>
            <Item name="software-type">Siemens SIP</Item>
            <Item name="related-software-type">Siemens SIP</Item>
            <Item name="software-version">V1 R4.9.0</Item>
            <Item name="related-software-version">V1 R4.9.0</Item>
            <Item name="contact-me-uri">
                http://192.168.1.4:8085/contact_dls.html/ContactDLS
            </Item>
            <Item name="mac-addr">00:01:E3:25:EA:13</Item>
            <Item name="configuration-changed-flag">true</Item>
            <Item name="part-number">S30817-S7403-A101-015</Item>
            <Item name="sip-mobility-state">0</Item>
            <Item name="e164">49897223290</Item>
            <Item name="user-pwd">123456</Item>
            <Item status="failed" name="user-pwd-unicode"/>
            <Item name="basic-e164">49897223290</Item>
            <Item name="mobility-enabled">false</Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

2. The rest of the interaction is analogical to the startup case, as described in Section 3.5.1, "An Exemplary Startup Interaction".

3.5.2.3   Message Flow

Phone   **Provisioning Service**

1   ———   HTTPS Request   ———▶
                                    Reason for contact: local-changes
                                    <Changed data items>

2   ◀———   HTTPS Response   ———
                                    CleanUp
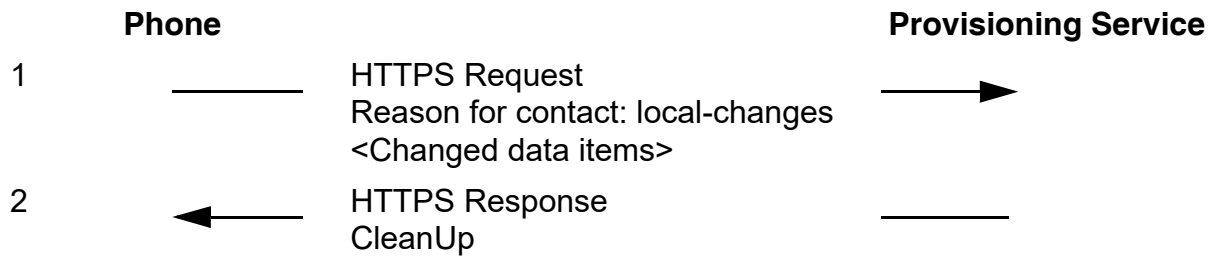
3.5.2.4 XML Data Exchange (OpenStage V2R2 onwards)

1. The following example shows XML data sent from a phone with to the provisioning service after a local configuration change. Note the values of `configuration-changed-flag`, `configuration-attached-flag`, and `configuration-attached-number`:

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message maxItems="-1"
    nonce="BD9438C65D42D90F566E2D03D6083602">
        <ReasonForContact>local-changes</ReasonForContact>
        <ItemList>
            <Item name="device-type">OpenStage 60</Item>
            <Item name="related-device-type">OpenStage 60</Item>
            <Item name="gigabit-ethernet-enabled">false</Item>
            <Item name="software-type">Siemens SIP</Item>
            <Item name="related-software-type">Siemens SIP</Item>
            <Item name="software-version">V2 R2.30.0</Item>
            <Item name="related-software-version">V2 R2.30.0</Item>
            <Item name="contact-me-uri">
                http://192.168.1.243:8085/contact_dls.html/ContactDLS
            </Item>
            <Item name="mac-addr">00:01:E3:25:E4:54</Item>
            <Item name="configuration-changed-flag">true</Item>
            <Item name="configuration-attached-flag">true</Item>
            <Item name="configuration-attached-number">2</Item>
            <Item name="part-number">S30817-S7403-A108-006</Item>
            <Item name="backlight-type">1</Item>
            <Item name="sip-mobility-state">0</Item>
            <Item name="e164">49897223337</Item>
            <Item name="user-pwd">123456</Item>
            <Item name="mobility-enabled">false</Item>
            <Item name="basic-e164">49897223337</Item>
            <Item name="dhcp">false</Item>
            <Item name="dls-addr">192.168.1.151</Item>
            <Item name="lldp-enabled">false</Item>
            <Item name="vlan-method">0</Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

The rest of the interaction is analogical to the startup case, as described in Section 3.5.1, "An Exemplary Startup Interaction"

3.6 Provisioning Service Driven Interaction

To initiate an interaction with the phone, the provisioning service must send an HTML-based contact-me message to the phone's contact-me URI. In turn the phone will send a response with `solicited` as a `ReasonForContact`. For the corresponding XML schema, please refer to Section 3.6.3.2, "XML Data Exchange".

3.6.1 Start an Interaction: Contact-me

The main purpose of the contact-me message is to allow the phone to decide when to send a response. If the provisioning service is acting as a web server, this initial message is required, as the service must be contacted by the phone, which acts as a web client. For details about the structure of a contact-me message, see Section 1.4.4.2, "Contact-me Messages".

If the phones and the provisioning service reside in different networks or subnets, which are separated by a firewall and/or NAT, it may be impossible for the provisioning service to send a contact-me message. To solve this problem, the phone can be configured so that it periodically polls the provisioning service, or a special proxy, for new messages. For further information, please refer to Section 1.4.4.3, "Polling Request To Bridge A Firewall" and Section 3.1.2.2, "Provisioning Service Located Behind A Firewall".

3.6.2 End an Interaction: CleanUp

An interaction is terminated when the phone receives a CleanUp message from the provisioning service. Together with the CleanUp message, the provisioning service should also invalidate the HTTPS session. See the following example:

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="9A6439F4E323CDB19283E40459828B56">
        <Action>CleanUp</Action>
    </Message>
</DLSMessage>
```

When sending a 'send-solicited' with the CleanUp message as response to a 'busy' state message of the phone, the phone is forced to contact automatically the provisioning service when it switches to 'idle' state. See also Section 3.7.3, "Contact-Me during Busy State".

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="9A6439F4E323CDB19283E40459828B56">
        <Action>CleanUp</Action>
        <ItemList>
            <Item name="send-solicited">true</Item>
```

```
        </ItemList>
    </Message>
</DLSMessage>
```

3.6.3   Read Phone Settings

Besides the `ReadAllItems` option, it is also possible to request a particular set of data items from the phone. For this purpose, the provisioning service sends a message with `Action` set to `ReadItems`.

3.6.3.1   Message Flow

	Phone		**Provisioning Service**
1	⬅———	HTTP Request Contact-me (HTML)	———
2	———	HTTP Response Acknowledged (HTML)	———➤
3	———	HTTPS Request Reason for contact: solicited <Basic data items>	———➤
4	⬅———	HTTPS Response Action: ReadItems <data items to read>	———
5	———	HTTPS Request Reason for contact: reply-to <Requested data items>	———➤
6	⬅———	HTTPS Response CleanUp	———

3.6.3.2   XML Data Exchange

The provisioning service must send a list containing the relevant item names to specify the desired data items.

1. The provisioning service sends a contact-me request to the phone (see Section 3.6.1, "Start an Interaction: Contact-me").

2. The phone responds to the contact-me request (see Section 1.4.4.2, "Contact-me Messages").

3. The phone sends basic configuration items.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.siemens.com/DLS">
    <Message nonce="2253A404241C11D774122654989181BC"
maxItems="-1">
        <ReasonForContact>solicited</ReasonForContact>
        <ItemList>
            <Item name="device-type">OpenStage 80</Item>
            <Item name="related-device-type">OpenStage 80</Item>
            <Item status="failed" name="gigabit-ethernet"></Item>
            <Item name="software-type">Siemens SIP</Item>
            <Item name="related-software-type">Siemens SIP</Item>
            <Item name="software-version">V1 R5.6.53</Item>
            <Item name="related-software-version">V1 R5.6.53</Item>
            <Item name="contact-me-uri">
http://192.168.233.195:8085/contact_dls.html/ContactDLS</Item>
            <Item name="mac-addr">00:01:E3:25:E1:CB</Item>
            <Item name="configuration-changed-flag">false</Item>
            <Item name="part-number">Unknown</Item>
            <Item name="sip-mobility-state">1</Item>
            <Item name="e164">5419431261</Item>
            <Item name="user-pwd">111111</Item>
            <Item status="failed" name="user-pwd-unicode"></Item>
            <Item name="basic-e164">5419431261</Item>
            <Item name="mobility-enabled">true</Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

4. The provisioning service sends a list of the desired data items.

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="2253A404241C11D7741122654989181BC">
        <Action>ReadItems</Action>
        <ItemList>
            <Item name="device-type"/>
            <Item name="related-device-type"/>
            <Item name="software-type"/>
            <Item name="software-version"/>
            <Item name="contact-me-uri"/>
            <Item name="mac-addr"/>
            <Item name="e164"/>
            <Item name="ipaddress"/>
            <Item name="reg-addr"/>
            <Item name="reg-port"/>
            <Item name="reg-ttl"/>
            <Item name="register-by-name"/>
            <Item name="registrar-addr"/>
            <Item name="registrar-port"/>
            <Item name="rtp-base-port"/>
            <Item name="server-type"/>
        </ItemList>
    </Message>
</DLSMessage>
```

5. In the response, the phone returns the requested data items.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message fragment="final" maxItems="-1"
        nonce="EB2C4CDF45D86E548CCD6F6612B26112">
        <ReasonForContact status="accepted" action="ReadItems">
            reply-to
        </ReasonForContact>
        <ItemList>
            <Item name="device-type">OpenStage 60</Item>
            <Item name="related-device-type">OpenStage 60</Item>
            <Item name="software-type">Siemens SIP</Item>
            <Item name="software-version">V1 R4.7.0</Item>
            <Item name="contact-me-uri">http://192.168.1.4:8085/
                contact_dls.html/ContactDLS</Item>
            <Item name="mac-addr">00:01:E3:25:EA:13</Item>
            <Item name="e164">49897223290</Item>
            <Item name="ipaddress">192.168.1.4</Item>
            <Item name="reg-addr">192.168.1.117</Item>
            <Item name="reg-port">5060</Item>
            <Item name="reg-ttl">3600</Item>
            <Item name="register-by-name">false</Item>
            <Item name="registrar-addr">192.168.1.117</Item>
            <Item name="registrar-port">5060</Item>
            <Item name="rtp-base-port">5010</Item>
            <Item name="server-type">0</Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```
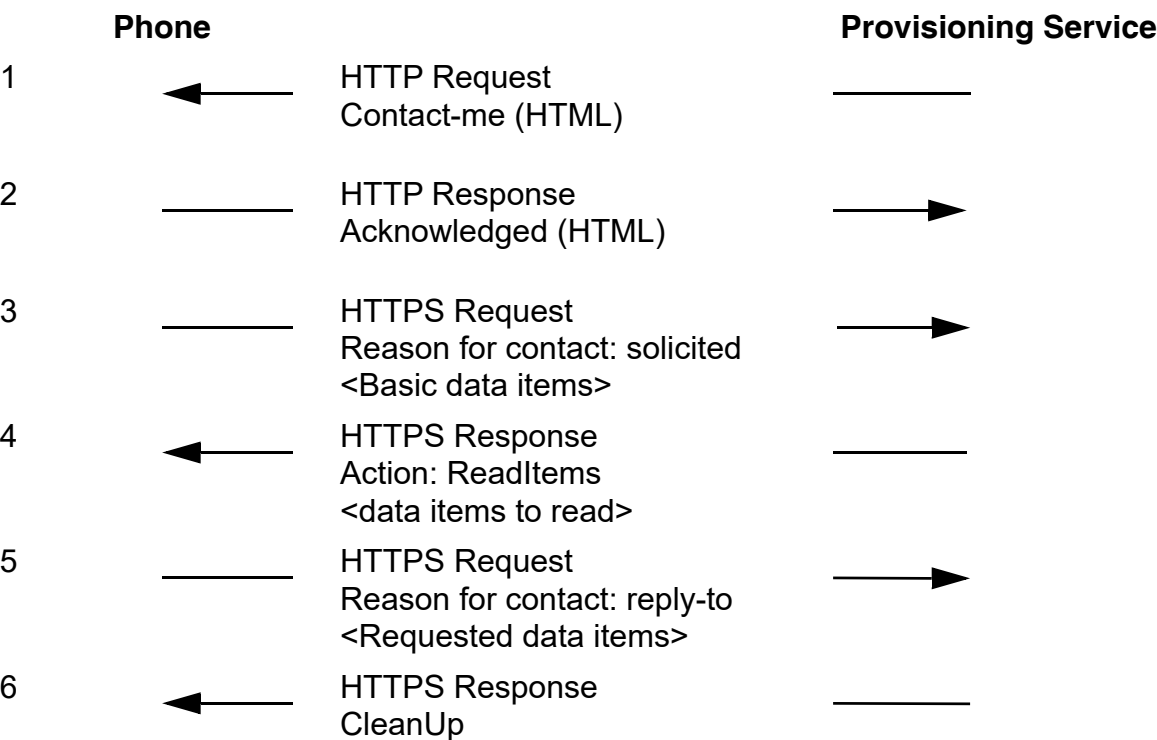
6. The provisioning service sends a CleanUp message.

```
<DLSMessage xmlns="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.siemens.com/DLS">
    <Message nonce="EB2C4CDF45D86E548CCD6F6612B26112">
        <Action>CleanUp</Action>
    </Message>
</DLSMessage>
```

3.6.4   Modify Phone Settings

To modify settings on the phone, that is, to write data items to the phone, the provisioning service sends a message with `Action` set to `WriteItems`. The items in question are sent to the phone in a similar fashion as described for reading data items (see Section 3.6.3.2, "XML Data Exchange").

> When the phone is in a call, it will not accept a `WriteItems` action. Instead, it will reply with a message stating it is in `busy` status. Example:
> ```
> <WorkpointMessage xsi:schemaLocation="http://www.siemens.com/
> DLS" xmlns="http://www.siemens.com/DLS" xmlns:xsi="http://
> www.w3.org/2001/XMLSchema-instance">
>     <Message nonce="957AE6C2E40C0E916B7CD5636480F171" max-
> Items="-1" fragment="final">
>         <ReasonForContact status="busy"
> action="WriteItems">reply-to</ReasonForContact>
>     </Message>
> </WorkpointMessage>
> ```
>
> When the provisioning service sends a CleanUp with a 'send-solicited' item, the phones reaction will be to schedule an automatic solicited connection to the provisioning service when the busy condition is cleared (>=V3R3). See also Section 3.7.3, "Contact-Me during Busy State".
> When sending a CleanUp without a 'send-solicited' item, the phone will not inform the provisioning service when it has returned to idle state, so the provisioning service will have to resend the request periodically.

3.6.4.1   Message Flow

Please note that step 6 and 7 are optional.

Phone		**Provisioning Service**
1	← HTTP Request Contact-me (HTML)	──
2	── HTTP Response Acknowledged (HTML)	→
3	── HTTPS Request: Reason for contact: solicited <Basic data items>	→

Phone   **Provisioning Service**

4   ◄———   HTTPS Response   ———
                   Action: WriteItems
                   <data items to write>

5   ———   HTTPS Request   ———►
                   Reason for contact: reply-to
                   Status: Accepted

6   ◄———   HTTPS Response   ———
                   Action: ReadItems
                   <data items to read (without val-
                   ues)>

7   ———   HTTPS Request   ———►
                   Reason for contact: reply-to
                   <data items from the ReadItems
                   list with current values>

8   ◄———   HTTPS Response   ———
                   CleanUp

3.6.4.2   XML Data Exchange

As steps 1-3 are described already in Section 3.6.3, "Read Phone Settings", only the subsequent steps are demonstrated here.

4.   The provisioning service sends a list of the desired data items.

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="58D4EE11C844865CAF0E9AA11ED2856F">
        <Action>WriteItems</Action>
        <ItemList>
            <Item name="sntp-tz-offset">60</Item>
            <Item name="auto-daylight-save">true</Item>
            <Item name="sntp-addr">time.nist.gov</Item>
            <Item name="daylight-save">true</Item>
            <Item name="daylight-save-zone-id">9</Item>
        </ItemList>
    </Message>
</DLSMessage>
```

5.   In its reply, the phone confirms that the action has been accepted.
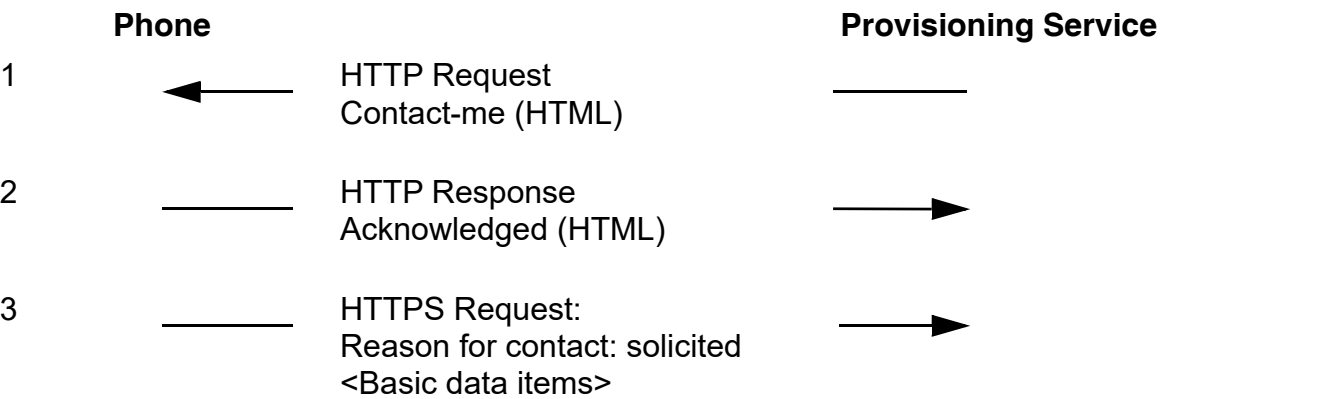
```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message fragment="final" maxItems="-1"
        nonce="0A8D39A3253E92715EFA5F5F63C25FFB">
        <ReasonForContact status="accepted" action="WriteItems">
            reply-to
        </ReasonForContact>
        <ItemList/>
    </Message>
</WorkpointMessage>
```

6. The provisioning service requests the data items to be modified in order to check whether they have been set correctly.

```xml
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="0A8D39A3253E92715EFA5F5F63C25FFB">
        <Action>ReadItems</Action>
        <ItemList>
            <Item name="daylight-save"/>
            <Item name="auto-daylight-save"/>
            <Item name="sntp-addr"/>
            <Item name="daylight-save-zone-id"/>
            <Item name="sntp-tz-offset"/>
        </ItemList>
    </Message>
</DLSMessage>
```

7. The phone sends the updated data items.

```xml
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message fragment="final" maxItems="-1"
    nonce="9A6439F4E323CDB19283E40459828B56">
        <ReasonForContact status="accepted" action="ReadItems">
            reply-to
        </ReasonForContact>
        <ItemList>
            <Item name="daylight-save">true</Item>
            <Item name="auto-daylight-save">true</Item>
            <Item name="daylight-save-zone-id">9</Item>
            <Item name="sntp-addr">time.nist.gov</Item>
            <Item name="sntp-tz-offset">60</Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

8. The provisioning service sends a CleanUp message.

3.6.5   Restart Phone

OpenStage phones and OpenScape Desk Phones IP can be rebooted via the provisioning interface.

3.6.5.1   Message Flow

Phone		Provisioning Service

1   ⟵   HTTP Request
Contact-me (HTML)

2   ⟶   HTTP Response
Acknowledged (HTML)

3   ⟶   HTTPS Request
Reason for contact: solicited
<Basic data items>

4   ⟵   HTTPS Response
Restart

3.6.5.2 XML Data Exchange

As the other elements of the message flow are already described in Section 3.6.3, "Read Phone Settings", only the relevant section (step 4) is illustrated by an example.

```
<DLSMessage
    xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="ab15234de14f15a667c6f8d">
        <Action>Restart</Action>
    </Message>
</DLSMessage>
```
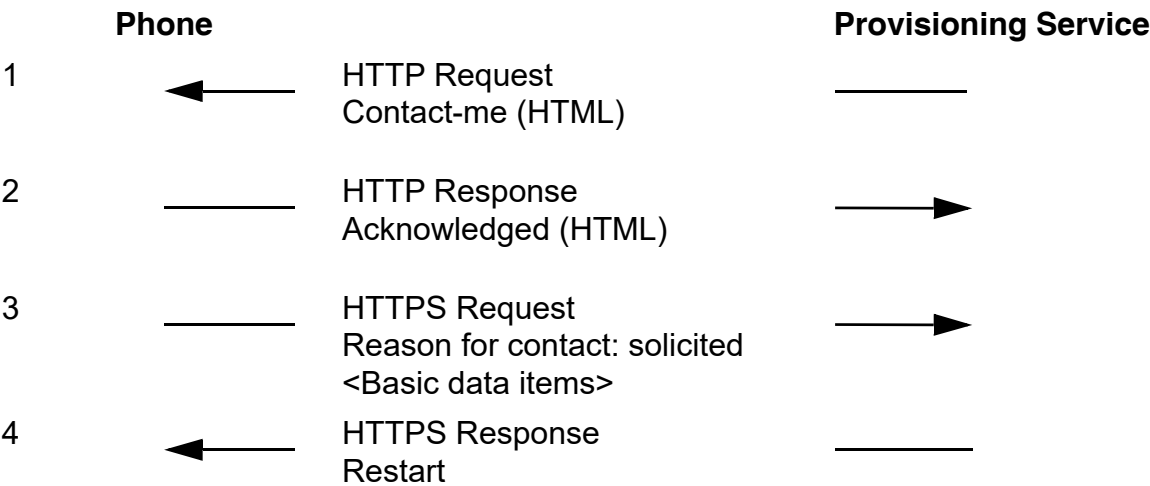
3.6.6 Factory Reset

The factory reset, that is, the complete recovery of the delivery status, can be triggered by the provisioning service. This includes a phone reboot.

As this is a variant of the phone restart, the message flow is as described in Section 3.4.5, "Restart Phone".

Two additional parameters are needed to initiate a factory reset:

- `restart-password`: For executing a factory reset, OpenStage phones and OpenScape Desk Phone IP require a special password, whatever interface is used. The value is `124816`.

- `restart-type`: For a factory reset, this must be set to `FactoryReset`.

3.6.6.1 XML Data Exchange

The additional parameters indicating the factory reset are transmitted as data items:

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="7D49388DE3E95AE2450BD64FEB8A2079">
        <Action>Restart</Action>
        <ItemList>
            <Item name="restart-password">124816</Item>
            <Item name="restart-type">FactoryReset</Item>
        </ItemList>
    </Message>
</DLSMessage>
```
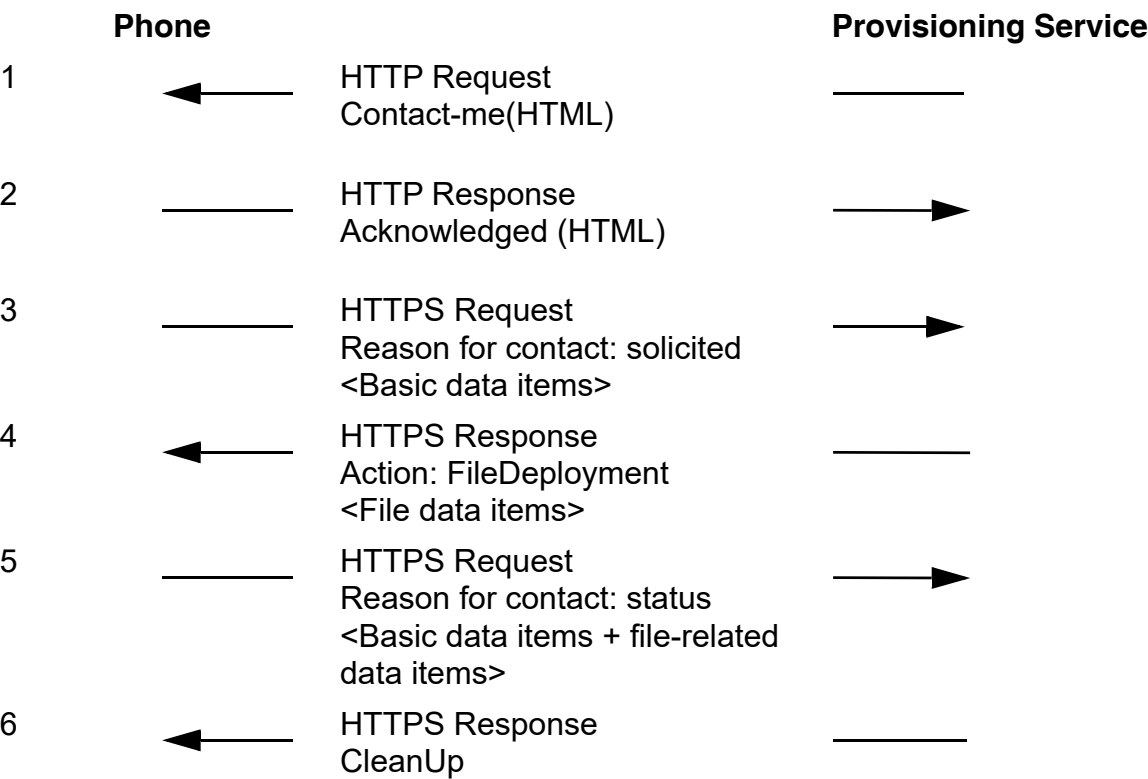
3.6.7 File Provisioning

The provisioning interface allows for deploying all kinds of files supported by the phone in question, such as ringtones, music on hold, or LDAP templates.

While the provisioning service initiates the transfer of files to the phone, the phone obtains the data from an FTP server or an HTTPS server. The necessary access parameters for the file server are provided by the provisioning service.

Unlike the phone's web interface, the provisioning interface also enables deploying more than one file at the same time.

3.6.7.1 Message Flow

	Phone		**Provisioning Service**
1	←	HTTP Request Contact-me(HTML)	——
2	——	HTTP Response Acknowledged (HTML)	→
3	——	HTTPS Request Reason for contact: solicited <Basic data items>	→
4	←	HTTPS Response Action: FileDeployment <File data items>	——
5	——	HTTPS Request Reason for contact: status <Basic data items + file-related data items>	→
6	←	HTTPS Response CleanUp	——

3.6.7.2   XML Data Exchange For Single File Deployment

As the other elements of the message flow are already described in Section 3.6.3, "Read Phone Settings", only the relevant sections (step 4 and 5) are illustrated by an example.

4.   In the following example, the phone is provided with a new ringtone, which is available as .wav file. The file is residing on an FTP server:

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="93D295F38327460697324D39D9824FDB">
        <Action>FileDeployment</Action>
        <ItemList>
            <Item name="file-server">192.168.1.150</Item>
            <Item name="file-pwd">dlsftp5</Item>
            <Item name="file-path">/media</Item>
            <Item name="file-name">ringtone-phone.wav</Item>
            <Item name="file-type">RINGTONE</Item>
            <Item name="file-username">dls</Item>
            <Item name="file-port">21</Item>
        </ItemList>
    </Message>
</DLSMessage>
```

In the second example, the ringtone is residing on an HTTPS server:

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="93D295F38327460697324D39D9824FDB">
        <Action>FileDeployment</Action>
        <ItemList>
            <Item name="file-type">RINGTONE</Item>
            <Item name="file-username">dls</Item>
            <Item name="file-https-base-url">
                https://192.168.1.150/media/ringtone-phone.wav
            </Item>
        </ItemList>
    </Message>
</DLSMessage>
```

5. The response from the phone may look like the following:

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
<Message maxItems="-1"
    nonce="4F6A1034A46B463F8D008DA09314040A">
    <ReasonForContact>status</ReasonForContact>
    <ItemList>
        <Item name="device-type">OpenStage 60</Item>
        <Item name="related-device-type">OpenStage 60</Item>
        <Item status="failed" name="gigabit-ethernet"/>
        <Item name="software-type">Siemens SIP</Item>
        <Item name="related-software-type">Siemens SIP</Item>
        <Item name="software-version">V1 R4.9.0</Item>
        <Item name="related-software-version">V1 R4.9.0</Item>
        <Item name="contact-me-uri">
            http://192.168.1.4:8085/contact_dls.html/ContactDLS
        </Item>
        <Item name="mac-addr">00:01:E3:25:EA:13</Item>
        <Item name="configuration-changed-flag">false</Item>
        <Item name="part-number">S30817-S7403-A101-015</Item>
        <Item name="sip-mobility-state">0</Item>
        <Item name="e164">49897223290</Item>
        <Item name="user-pwd">123456</Item>
        <Item status="failed" name="user-pwd-unicode"/>
        <Item name="basic-e164">49897223290</Item>
        <Item name="mobility-enabled">false</Item>
        <Item name="file-deployment-date">10:06:2008</Item>
        <Item name="file-deployment-time">15:35:52</Item>
        <Item name="file-deployment-name">
            ringtone-phone.wav
        </Item>
        <Item name="file-deployment-type">RINGTONE</Item>
        <Item name="file-deployment-status">ok</Item>
    </ItemList>
</Message>
</WorkpointMessage>
```

3.6.7.3 XML Data Exchange For Multiple File Deployment

With multiple file deployment, the message exchange is similar to single file deployment, but the data items are indexed. These indexed items enable deploying a set of files of various types with a singular message. Additionally, it is possible to delete files on the phone. A single action can include both deployment and deletion commands. A specific file and the action to be executed with it (`file-action`) are assigned to each other by a common index number.

The selective deletion of files is possible because the combination of `file-name` and `file-type` is unique on the phone.

As the phone will not send status information on multiple file deployment or file deletion, the provisioning server should check the result by requesting a ReadAllItems.

The following example shows a multiple file deployment request; in the message flow, it corresponds to the XML message described in Section 3.6.7.2, "XML Data Exchange For Single File Deployment".

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="E5BFC5E2FBCE6CD3D20DC9AD975C0355">
        <Action>FileDeployment</Action>
        <ItemList>
            <Item name="file-server" index="1">192.168.1.150</Item>
            <Item name="file-path" index="1">/media/</Item>
            <Item name="file-name" index="1">
                Logo for OpenStage 80.png
            </Item>
            <Item name="file-type" index="1">LOGO</Item>
            <Item name="file-pwd" index="1">dlsftp5</Item>
            <Item name="file-port" index="1">21</Item>
            <Item name="file-username" index="1">dls</Item>
            <Item name="file-action" index="1">deploy</Item>
            <Item name="file-server" index="2">192.168.1.150</Item>
            <Item name="file-path" index="2">/media/</Item>
            <Item name="file-name" index="2">ringtone-ringin.wav</Item>
            <Item name="file-type" index="2">RINGTONE</Item>
            <Item name="file-pwd" index="2">dlsftp5</Item>
            <Item name="file-port" index="2">21</Item>
            <Item name="file-username" index="2">dls</Item>
            <Item name="file-action" index="2">deploy</Item>
        </ItemList>
    </Message>
</DLSMessage>
```
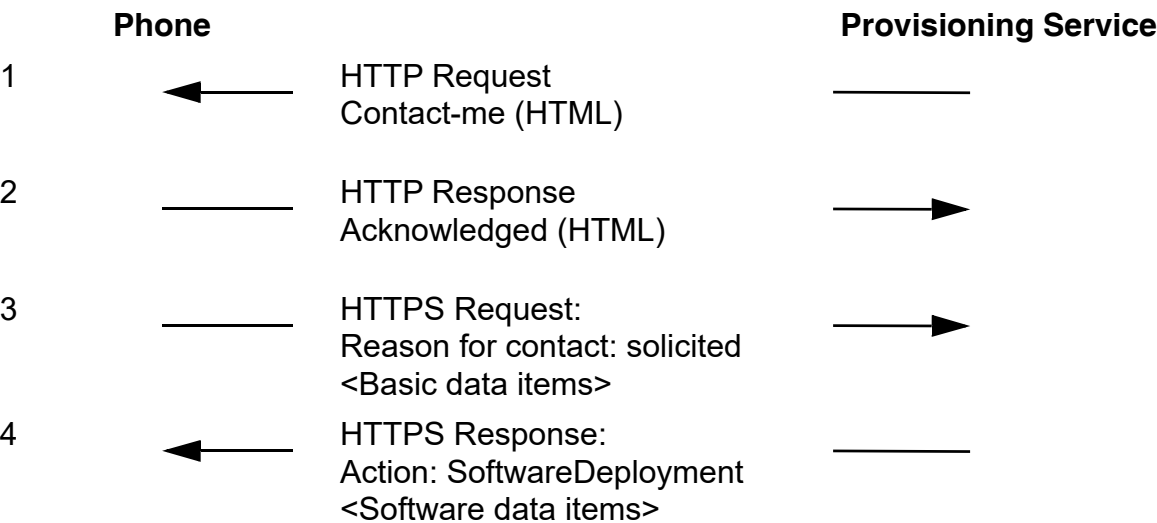
3.6.8   Firmware Deployment

The deployment of firmware for the phone is very similar to the regular file deployment, as described in Section 3.6.7, "File Provisioning". The type of `Action` is different, the item is named `file-sw-type` is used instead of `file-type`, and the items `file-sw-version` and `file-priority` are added.

> If a call is in progress and the `file-priority` has not been set to `immediate`, the deployment will be rejected.

When the phone has received the software file, it will reboot, thereby loading the new software. Like with every startup, the phone will send a startup message (see Section 3.5.1, "An Exemplary Startup Interaction"). By issuing a `ReadItems` or `ReadAllItems` message, the provisioning service can determine whether the phone has the intended software version now.

3.6.8.1   Message Flow

Phone   **Provisioning Service**

1   ⟵ ⎯⎯⎯   HTTP Request
                         Contact-me (HTML)   ⎯⎯⎯

2   ⎯⎯⎯   HTTP Response
                         Acknowledged (HTML)   ⎯⎯⎯⟶

3   ⎯⎯⎯   HTTPS Request:
                         Reason for contact: solicited   ⎯⎯⎯⟶
                         <Basic data items>

4   ⟵ ⎯⎯⎯   HTTPS Response:
                         Action: SoftwareDeployment   ⎯⎯⎯
                         <Software data items>

3.6.8.2   XML Data Exchange

As the other elements of the message flow are already described in Section 3.6.3, "Read Phone Settings", only the relevant section (step 4) is illustrated by an example. In the example, FTP is used; it can also be done by HTTPS.

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="BDB60C70FE707FD023E09F0A9363DD8D">
        <Action>SoftwareDeployment</Action>
        <ItemList>
            <Item name="file-server">192.168.1.150</Item>
            <Item name="file-pwd">dlsftp5</Item>
            <Item name="file-path">/OS/SIP/HI</Item>
            <Item name="file-name">OS_80_SIP_V1_R4_9_0.img</Item>
            <Item name="file-type">APP</Item>
            <Item name="file-username">dls</Item>
            <Item name="file-port">21</Item>
            <Item name="file-sw-type">Siemens SIP</Item>
            <Item name="file-sw-version">1.4.9.0</Item>
            <Item name="file-priority">normal</Item>
        </ItemList>
    </Message>
</DLSMessage>
```

3.6.9 Certificate Deployment

To enable secure connections and data transmission, OpenStage phones and OpenScape Desk Phone IP need appropriate certificates. These can be deployed using the provisioning service. Certificates can be used for the following functional areas:

- XML applications (see Section 4.1.1, "XML applications")

- WBM (Web Based Management)

- SIP server

- IEEE 802.1x / RADIUS server

- Send URL (see Section 4.4.5.3, "Send URL")

For detailed information about the required items, see Section 6.13, "Certificates". For deployment on the phone, the credentials must be prepared as follows:

- PKCS#12 format, except RADIUS certificates, which are in .pem format

- The PKCS#12 data is packaged and encrypted with this shared secret: `cum-sek-ewa-bss`

- For transfer via WPI, the PKCS#12 data is encoded in base64 format.

3.6.9.1 Message Flow

Phone   **Provisioning Service**

1   ⬅———   HTTP Request
                     Contact-me (HTML)   ———

2   ———   HTTP Response
                     Acknowledged (HTML)   ———➤

3   ———   HTTPS Request:
                     Reason for contact: solicited   ———➤
                     <Basic data items>

4   ⬅———   HTTPS Response:
                     Action: WriteItems   ———
                     <Certificate>

5   ———   HTTPS Request:
                     Reason for contact: status   ———➤

6   ⬅———   HTTPS Response:
                     Action: ReadItems   ———
                     <Certificate info>

7   ———   HTTPS Request:
                     Reason for contact: status   ———➤
                     <Certificate info>

6   ⬅———   HTTPS Response
                     CleanUp   ———
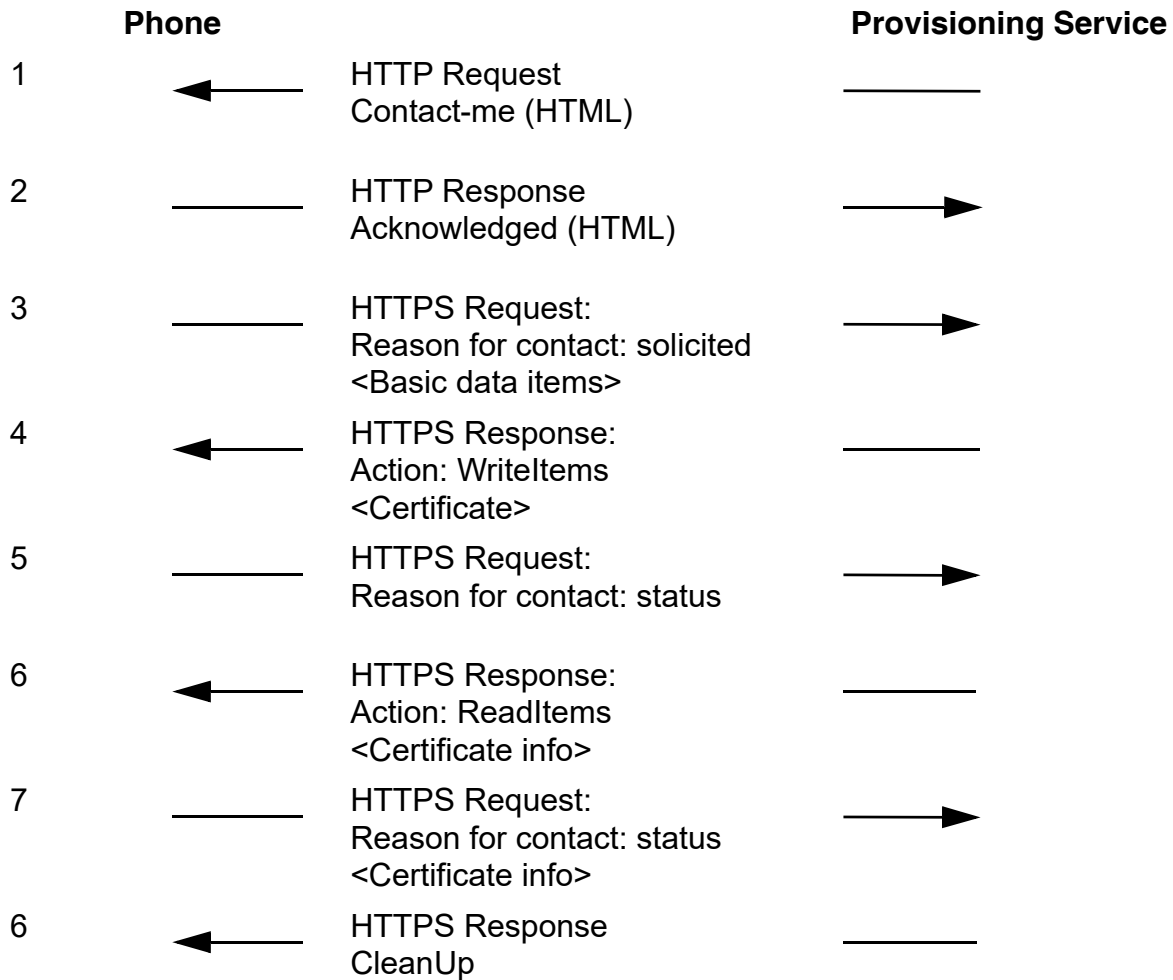
3.6.9.2 XML Data Exchange

The following example shows the deployment of a WBM server certificate, which is needed for secure communication between the phone's web server and a web browser. As steps 1 to 3 are already described in Section 3.6.3, "Read Phone Settings", only the specific steps are shown.

1. The provisioning service send the base64-encoded certificate data.

```
<DLSMessage xmlns="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.siemens.com/DLS">
    <Message nonce="BB0DBC18D7B8A34BA3DB8295BD5B29D3">
        <Action>WriteItems</Action>
            <ItemList>
                <Item name="wbm-server-certificate">[PKCS#12 data,
base64 encoded]</Item>
            </ItemList>
    </Message>
</DLSMessage></Object>
```

2. The phone informs the provisioning service that it has accepted the action.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <Message nonce="43C308AE8D03F14392F565075A9922FB" maxItems="-1"
    fragment="final">
        <ReasonForContact status="accepted" action="WriteItems">
            reply-to</ReasonForContact>
            <ItemList/>
    </Message>
</WorkpointMessage>
```
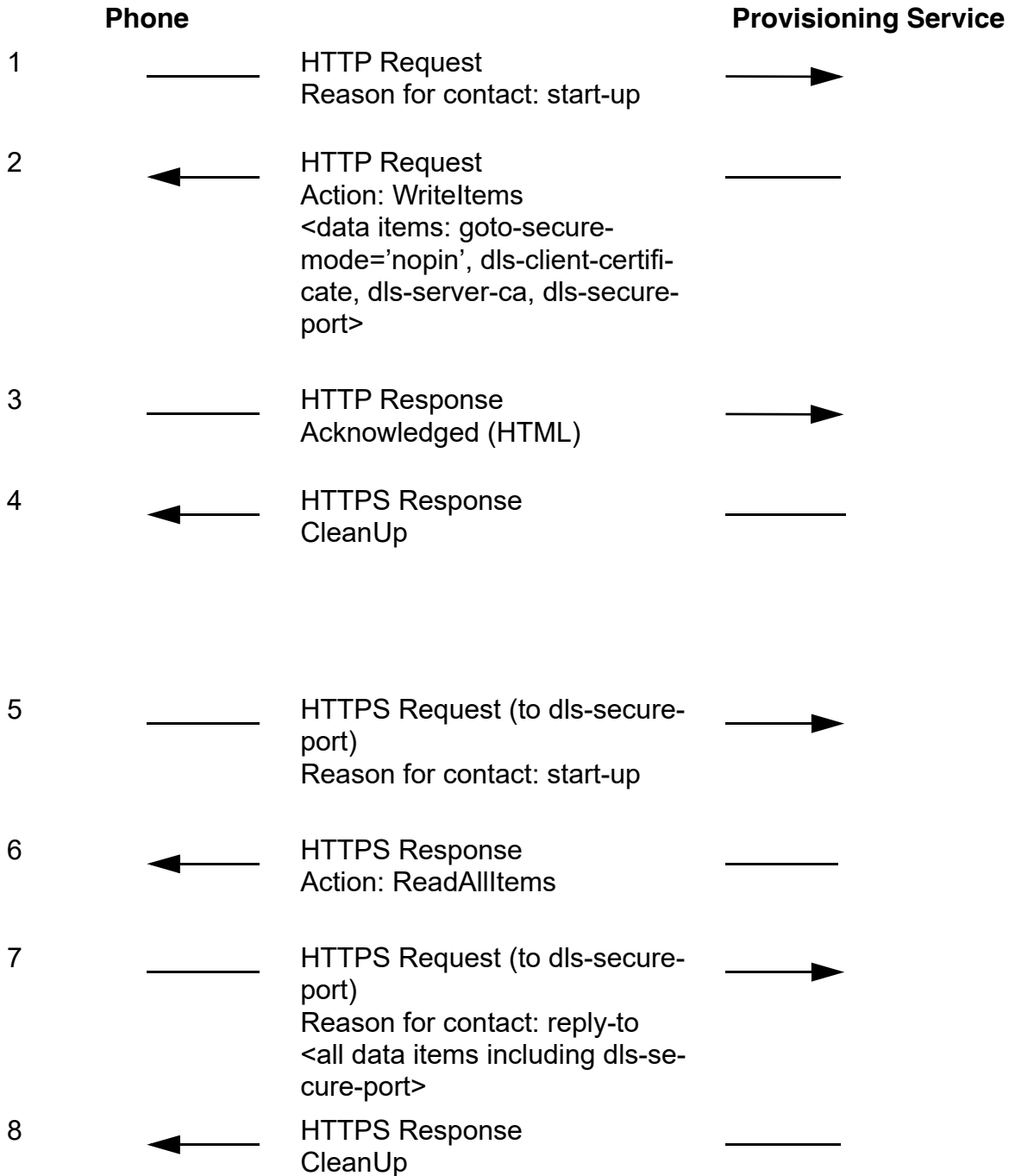
3. To verify if the certificate had been deployed correctly, the provisioning service requests the `wbm-server-certificate-info` item.

```
<DLSMessage xmlns="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://www.siemens.com/DLS">
    <Message nonce="43C308AE8D03F14392F565075A9922FB">
        <Action>ReadItems</Action>
            <ItemList>
                <Item name="wbm-server-certificate-info"></Item>
            </ItemList>
    </Message>
</DLSMessage>
```

4. The phone sends the certificate it has extracted from the PKCS#12 data, without the private key and the optional CA certificate.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
   xmlns="http://www.siemens.com/DLS"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <Message nonce="C9E1C9A2BAA1644559FF110C7299BBC6" maxItems="-1"
      fragment="final">
      <ReasonForContact status="accepted" action="ReadItems">
         reply-to</ReasonForContact>
      <ItemList>
         <Item name="wbm-server-certificate-info">
            [certificate, base64 encoded]</Item>
      </ItemList>
   </Message>
</WorkpointMessage>
```

5. The provisioning service sends a CleanUp message.

3.6.10   Secure Mode and Bootstrapping

Workpoint Interface supports Secure Mode, where mutual authentication based on individual digital signatures takes place. The mode without mutual authentication is called Default Mode.

Bootstrapping means the interface security between device and provisioning service is raised from Default Mode to Secure Mode. The bootstrapping process is initiated by the provisioning service with sending the writeItems message containing the XML item 'goto-secure-mode'. There is no other message exchanged between provisioning service and device that contains this item.

There are two alternatives defined for bootstrapping, with PIN and without PIN.

For bootstrapping the provisioning service has to provide

– its individual client certificate, including private key

– the CA certificate(s), the provisioning server is signed with

– the port number where to contact provisioning service in Secure Mode

– the PIN which the user has to enter at the device in case the bootstrapping is protected by PIN

In case of bootstrapping with PIN the data above are packed, encrypted and Base64-encoded. To decrypt the data the device has to prompt the user to enter a PIN.

When the phone is in a call, it will not accept a `WriteItems` action. Instead, it will reply with a message stating it is in `busy` status. Example:

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/
DLS" xmlns="http://www.siemens.com/DLS" xmlns:xsi="http://
www.w3.org/2001/XMLSchema-instance">
    <Message nonce="957AE6C2E40C0E916B7CD5636480F171" max-
Items="-1" fragment="final">
        <ReasonForContact status="busy" action="WriteItems">
reply-to</ReasonForContact>
    </Message>
</WorkpointMessage>
```

When the provisioning service sends a CleanUp with a 'send-solicited' item, the phones reaction will be to schedule an automatic solicited connection to the provisioning service when the busy condition is cleared (>=V3R3). See also Section 3.7.3, "Contact-Me during Busy State"

When sending a CleanUp without a 'send-solicited' item, the phone will not inform the provisioning service when it has returned to idle state, so the provisioning service will have to resend the request periodically.

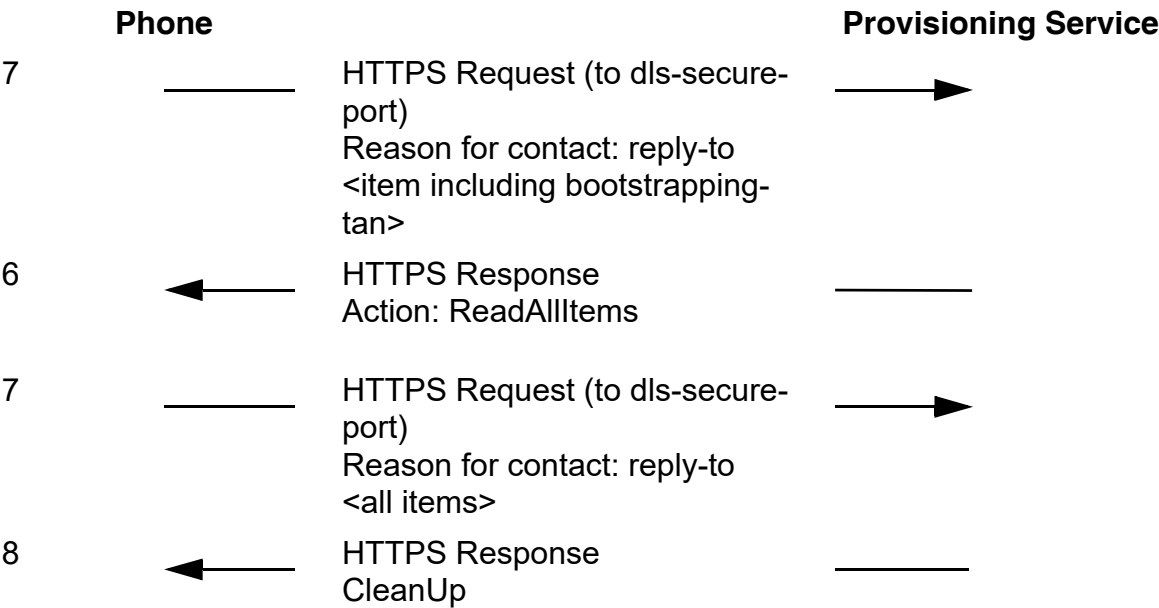### 3.6.10.1 Message Flow: Secure Mode, No PIN

The preconditions are:

– Device is not registered, but configured in provisioning service as Secure Mode with no PIN required

Phone		**Provisioning Service**

1   ———   HTTP Request
Reason for contact: start-up   ——▶

2   ◀———   HTTP Request
Action: WriteItems
<data items: goto-secure-mode='nopin', dls-client-certificate, dls-server-ca, dls-secure-port>   ———

3   ———   HTTP Response
Acknowledged (HTML)   ——▶

4   ◀———   HTTPS Response
CleanUp   ———

5   ———   HTTPS Request (to dls-secure-port)
Reason for contact: start-up   ——▶

6   ◀———   HTTPS Response
Action: ReadAllItems   ———

7   ———   HTTPS Request (to dls-secure-port)
Reason for contact: reply-to
<all data items including dls-secure-port>   ——▶

8   ◀———   HTTPS Response
CleanUp   ———

3.6.10.2 XML Data Exchange: Secure Mode, No PIN

1. As step 1 start-up is described already in Section 3.5.1.2, "XML Data Exchange", only the subsequent steps are demonstrated here.

2. As the device is configured to Secure Mode without PIN, the provisioning service sends a request to switch to Secure Mode (bootstrapping) including certificates and secure-port number.

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="58D4EE11C844865CAF0E9AA11ED2856F">
        <Action>WriteItems</Action>
        <ItemList>
            <Item name="goto-secure-mode">nopin</Item>
            <Item name="dls-client-certificate">.....</Item>
            <Item name="dls-server-ca" index="0">-----BEGIN
             CERTIFICATE-----.....</Item>
            <Item name="dls-server-ca" index="1"></Item>
            <Item name="dls-secure-port">18444</Item>
        </ItemList>
    </Message>
</DLSMessage>
```

3. Device responses to default provisioning server port and confirms that the action has been accepted.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message fragment="final" maxItems="-1"
        nonce="58D4EE11C844865CAF0E9AA11ED2856F">
        <ReasonForContact status="accepted" action="WriteItems">
            reply-to
        </ReasonForContact>
        <ItemList/>
    </Message>
</WorkpointMessage>
```

4. The provisioning service sends a CleanUp message.

5. Device sends start-up request to secure port (18444) of provisioning service using the client certificate received with bootstrapping message (2).

6. The provisioning service verifies the client certificate and proceeds with standard message flow, here responds with action `ReadAllItems`.

7. Individual client certificate and provisioning server CA certificate(s) have been stored, all further requests from this device perform mutual authentication on port 18444.

8. When bootstrapping process has finished with success, requests from device via Default Mode port (18443) are blocked now.
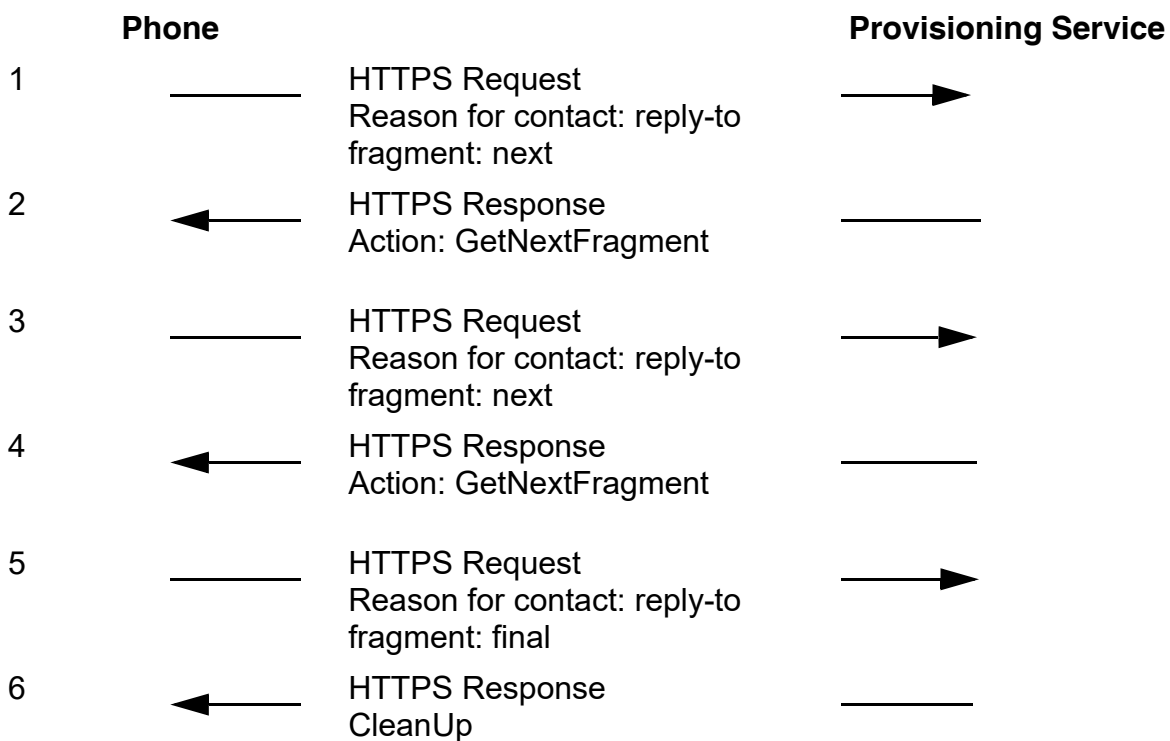
3.6.10.3   Message Flow: Secure Mode, With PIN

The preconditions are:

– Device is not registered, but configured in provisioning service as Secure Mode with PIN required

– A PIN is configured for this device
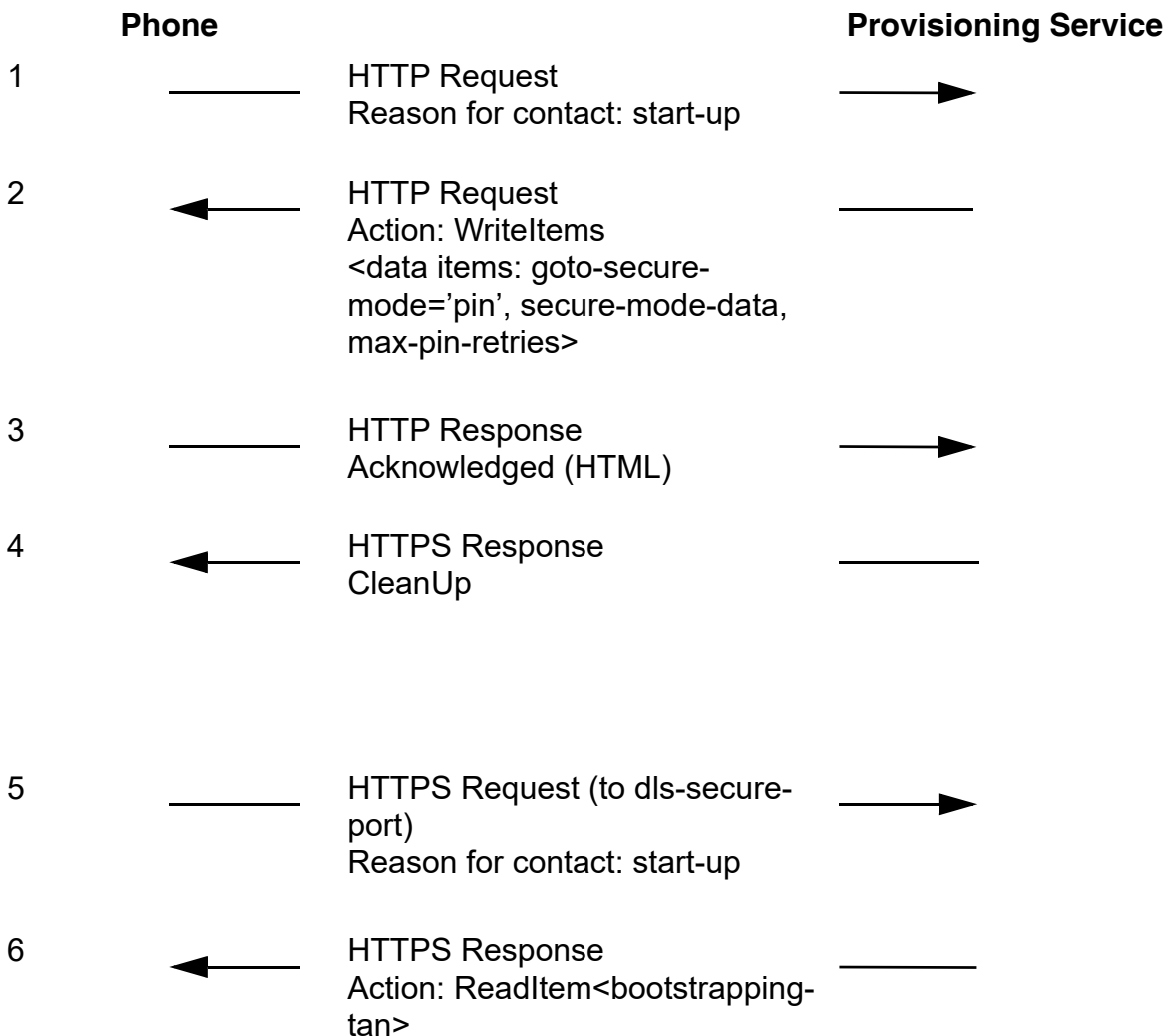
	Phone		**Provisioning Service**
1	⎯⎯⎯	HTTP Request Reason for contact: start-up	⟶
2	⟵	HTTP Request Action: WriteItems <data items: goto-secure-mode='pin', secure-mode-data, max-pin-retries>	⎯⎯⎯
3	⎯⎯⎯	HTTP Response Acknowledged (HTML)	⟶
4	⟵	HTTPS Response CleanUp	⎯⎯⎯
5	⎯⎯⎯	HTTPS Request (to dls-secure-port) Reason for contact: start-up	⟶
6	⟵	HTTPS Response Action: ReadItem<bootstrapping-tan>	⎯⎯⎯

Phone		**Provisioning Service**
7	HTTPS Request (to dls-secure-port) Reason for contact: reply-to <item including bootstrapping-tan>	
6	HTTPS Response Action: ReadAllItems	
7	HTTPS Request (to dls-secure-port) Reason for contact: reply-to <all items>	
8	HTTPS Response CleanUp	

3.6.10.4   XML Data Exchange: Secure Mode, With PIN

1. As step 1 start-up is described already in Section 3.5.1.2, "XML Data Exchange", only the subsequent steps are demonstrated here.

2. As the device is configured to Secure Mode with PIN, the provisioning service sends a request to switch to Secure Mode (bootstrapping) including all items needed packed, encrypted and Base64-encoded into the single data item 'secure-mode-data'.

3.
```xml
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="58D4EE11C844865CAF0E9AA11ED2856F">
        <Action>WriteItems</Action>
        <ItemList>
            <Item name="goto-secure-mode">pin</Item>
            <Item name="secure-mode-data"><packed-encrypted-
base64encoded-data></Item>
            <Item name="max-pin-retries">3</Item>
        </ItemList>
    </Message>
</DLSMessage>
```
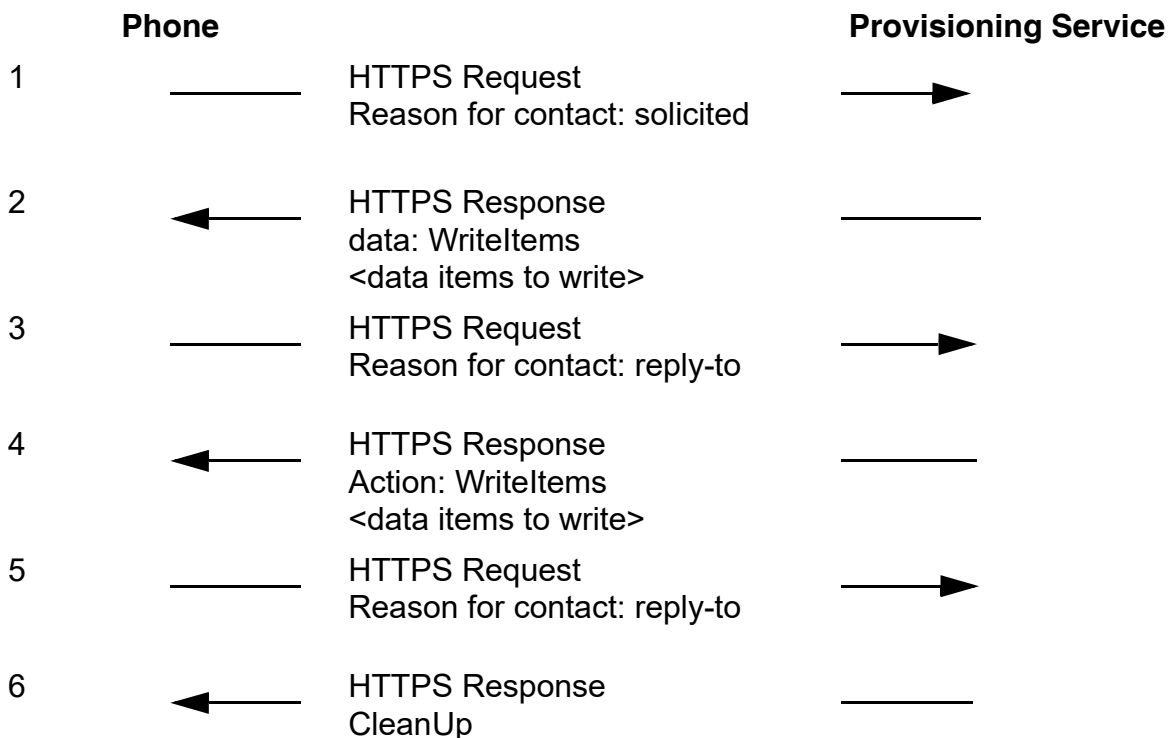
4. Device responses to default provisioning server port and confirms that the action has been accepted.

```xml
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message fragment="final" maxItems="-1"
        nonce="58D4EE11C844865CAF0E9AA11ED2856F">
        <ReasonForContact status="accepted" action="WriteItems">
            reply-to
        </ReasonForContact>
        <ItemList/>
    </Message>
</WorkpointMessage>
```

5. The provisioning service sends a CleanUp message.

6. Device needs to display the PIN dialog to the user, to get the PIN for decrypting the secure-mode-data.

7. The device has decrypted secure-mode-data successfully by using of entered PIN (except last 3 characters) as password and contacts the provisioning service via Secure Mode port using the client certificate.

8. With the next contact of device, the provisioning service verifies the client certificate and because of the PIN a readItems for getting the bootstrapping TAN is sent to the device.

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="58D4EE11C844865CAF0E9AA11ED2856F">
        <Action>ReadItems</Action>
        <ItemList>
            <Item name="bootstrapping-tan"></Item>
        </ItemList>
    </Message>
</DLSMessage>
```

9. The device responds with accepted including the TAN (last 3 characters of the PIN)

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message fragment="final" maxItems="-1"
        nonce="58D4EE11C844865CAF0E9AA11ED2856F">
        <ReasonForContact status="accepted" action="ReadItems">
            reply-to
        </ReasonForContact>
        <ItemList>
            <Item name="bootstrapping-tan">321</Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

10. The TAN has been accepted and the provisioning service continues with normal message flow.

11. Individual client certificate and provisioning server CA certificate(s) have been stored, all further requests from this device perform mutual authentication on port 18444.

12. When bootstrapping process has finished with success, requests from device via Default Mode port (18443) are blocked now.

3.7   Message Fragmentation

Messages are limited to a length of 50 kB. Larger messages will be split into fragments. On the phone side, the threshold is defined by the `maxItems` attribute of the `Message` element. When the number of data items to be contained in a message exceeds the number given here, or the message reaches the 50 kB limit, the message is split up. Alternatively, the provisioning service can decide to construct a message as multiple messages.

3.7.1   Fragmentation of Phone Messages

3.7.1.1   Message Flow

In the following message flow example, the phone sends data which is divided into 3 fractions. Please note that this is not a full interaction, but only the relevant section of an interaction that could have been driven both by the phone or by the provisioning service.

Phone		**Provisioning Service**
1	HTTPS Request Reason for contact: reply-to fragment: next	→
2	HTTPS Response Action: GetNextFragment	←
3	HTTPS Request Reason for contact: reply-to fragment: next	→
4	HTTPS Response Action: GetNextFragment	←
5	HTTPS Request Reason for contact: reply-to fragment: final	→
6	HTTPS Response CleanUp	←

3.7.1.2 XML Data Exchange

Step 1 and 2 of the example interaction are presented here.

1. The phone sends its first fragment. The `ItemList` provided in the example is not real-life, as it represents a very long list.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message maxItems="-1" nonce="B0151B36FE9CEEA0F667FF3A208AC994"
    fragment="next">
        <ReasonForContact action="ReadItems" status="accepted">
            reply-to
        </ReasonForContact>
        <ItemList>
            <Item name="device-type">OpenStage 60</Item>
            <Item name="related-device-type">OpenStage 60</Item>
            ...
        </ItemList>
    </Message>
</WorkpointMessage>
```

2. The provisioning service requests the next fraction of data from the phone.

```
<DLSMessage xsi:schemaLocation="http://www.siemens.com/DLS"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="http://www.siemens.com/DLS">
    <Message nonce="B0151B36FE9CEEA0F667FF3A208AC994">
        <Action>GetNextFragment</Action>
    </Message>
</DLSMessage>
```

3.7.2 Fragmentation of Provisioning Service Messages

3.7.2.1 Message Flow

In the following message flow example, the provisioning service sends data which is divided up in 2 fractions. Please note that this is not a full interaction, but only the relevant section of an interaction driven by the provisioning service.

> All related data items must be sent in a single message.

	Phone		**Provisioning Service**

1   ————   HTTPS Request
Reason for contact: solicited   ————▶

2   ◀————   HTTPS Response
data: WriteItems
\<data items to write>   ————

3   ————   HTTPS Request
Reason for contact: reply-to   ————▶

4   ◀————   HTTPS Response
Action: WriteItems
\<data items to write>   ————

5   ————   HTTPS Request
Reason for contact: reply-to   ————▶

6   ◀————   HTTPS Response
CleanUp   ————

3.7.2.2 XML Data Exchange

The XML messages in a fragmented message flow from the provisioning service have the same structure as regular messages for phone configuration. For details, see Section 3.6.4, "Modify Phone Settings".

3.7.3 Contact-Me during Busy State

3.7.3.1 Message Flow

When the phone is asked by the provisioning service to write a data item whilst the phone is busy in a call, the phone rejects the WriteItems with a 'Busy' status response but supports the use of the 'send-solicited' item in the CleanUp message to reconnect automatically to the provisioning service when the call ends. The phone caches the indication for reconnection, but it makes no assumptions about why it reconnects, it is expected that the provisioning service will remember that it still has a data item that it needs to set on the phone.

When the CleanUp message does not include a 'send-solicited' item, the phone does not attempt to reconnect to the provisioning service when it is idle.

For multiple provisioning service jobs cached on a phone, the provisioning service has to send a CleanUp message with 'send-solicited' until the last job, which is closed with an plain CleanUp message. See also Section 3.7.3.1, "Multiple provisioning service jobs". The provisioning service is expected to remember and re-request the previously failed WriteItems since the phone will only establish a single solicited connection even if multiple send-solicited CleanUps are received by the phone.

Any cached indication of the need to initiate a solicited connection to the provisiong service when no longer busy will be cleared when the phone restarts (e.g. due to a restart, factory reset, or new bind), i.e. the cached indication is not persisted. If the phone is unable to establish a solicited connection when no longer busy then the cached indication is retained after the existing process to connect to the provisioning service has failed.

The 'send-solicited' item is applicable to provisioning service Secure mode and Default mode.

> Available with V3R3.

Single provisioning service job

	Phone		Provisioning Service
1	⟵	HTTP Request Contact-me (HTML)	
2	—	HTTP Response Acknowledged (HTML)	⟶

Phone		Provisioning Service

3 ——— HTTPS Request:
Reason for contact: solicited
<Basic data items> ——▶

4 ◀—— HTTPS Response
Action: WriteItems
<data items to write> ———

5 ——— HTTPS Request
Reason for contact: reply-to
Status: Busy ——▶

6 ◀—— HTTPS Response
CleanUp
Item: send-solicited ———

Time passes. Phone switches
from 'busy' to 'idle'-state.

7 ——— HTTPS Request:
Reason for contact: solicited
<Basic data items> ——▶

8 ◀—— HTTPS Response
Action: WriteItems
<data items to write> ———

9 ——— HTTPS Request
Reason for contact: reply-to
Status: Accepted ——▶

10 ◀—— HTTPS Response
CleanUp ———

Multiple provisioning service jobs

Phone		Provisioning Service

1 ◀—— HTTP Request 1
Contact-me (HTML) ———

2 ——— HTTP Response 1
Acknowledged (HTML) ——▶

Phone		Provisioning Service

3   ———   HTTPS Request 1:   ⟶
Reason for contact: solicited
<Basic data items>

4   ⟵———   HTTPS Response 1   ———
Action: WriteItems
<data items to write>

5   ———   HTTPS Request 1   ⟶
Reason for contact: reply-to
Status: Busy

6   ⟵———   HTTPS Response 1   ———
CleanUp
Item: send-solicited

7   ⟵———   HTTP Request 2   ———
Contact-me (HTML)

8   ———   HTTP Response 2   ⟶
Acknowledged (HTML)

9   ———   HTTPS Request 2:   ⟶
Reason for contact: solicited
<Basic data items>

10   ⟵———   HTTPS Response 2   ———
CleanUp

11   ⟵———   HTTP Request 3   ———
Contact-me (HTML)

12   ———   HTTP Response 3   ⟶
Acknowledged (HTML)

13   ———   HTTPS Request 3:   ⟶
Reason for contact: solicited
<Basic data items>

14   ⟵———   HTTPS Response 3   ———
Action: WriteItems
<data items to write>

15   ———   HTTPS Request 3   ⟶
Reason for contact: reply-to
Status: Busy

Phone **Provisioning Service**

16 ← HTTPS Response 3
CleaUp
Item: send-solicited

Time passes. Phone switches
from 'busy' to 'idle'-state.

17 → HTTPS Request:
Reason for contact: solicited
<Basic data items>

18 ← HTTPS Response 1
Action: WriteItems
<data items to write>

19 → HTTPS Request 1
Reason for contact: reply-to
Status: Accepted

20 ← HTTPS Response 1
CleanUp
Item: send-solicited

21 → HTTPS Request:
Reason for contact: solicited
<Basic data items>

22 ← HTTPS Response 3
Action: WriteItems
<data items to write>

23 → HTTPS Request 3
Reason for contact: reply-to
Status: Accepted

24 ← HTTPS Response 3
CleanUp

ad 10: The 2nd job does not include a WriteItems, so it is terminated by a normal CleanUp
ad 17: The phone responds the send-solicited request in 6 and 16 with a single solicited con-
nection
ad 18: The provisioning service allocates the 1st waiting job to the connection.
ad 20: The job succeeds but the provisioning service adds a 'send-solicited' item due to another
waiting job.
ad 21: Since the phone is idle it connects immediately.
ad 22: The provisioning servic allocates the 2nd waiting job to the connection.
ad 23: The job succeeds and the provisioning service sends a normal CleanUp since there are
no other waiting jobs.

3.7.3.2 XML Data Exchange

For details, see Section 3.6.4, "Modify Phone Settings".

1. The phone sends a response with 'busy' state.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
xmlns="http://www.siemens.com/DLS" xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">
    <Message nonce="957AE6C2E40C0E916B7CD5636480F171" maxItems="-1"
fragment="final">
        <ReasonForContact status="busy" action="WriteItems">

reply-to</ReasonForContact>
    </Message>

</WorkpointMessage>
```

2. The provisioning service sends a CleanUp message with 'send-solicited' item.

```
<DLSMessage xmlns="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.siemens.com/DLS">
    <Message nonce="EB2C4CDF45D86E548CCD6F6612B26112">
        <Action>CleanUp</Action>
        <ItemList>
            <Item name="send-solicited">true</Item>
        </ItemList>
    </Message>
</DLSMessage>
```

3.8 Error Handling

In case the provisioning service should send erroneous write actions, the phone will answer with appropriate error messages.

In this section, the error-handling by the phone is illustrated by three interaction examples. Please note that the sequences of messages shown here start with the phone sending a message to the provisioning service with `ReasonForContact` set to `solicited`. The contact-me message from the provisioning server is omitted for brevity.

3.8.1 Example 1: Item is Unknown at Phone

1. The phone initiates a connection to the provisioning service.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.siemens.com/DLS">
    <Message nonce="104EBC8C863E0C5CA384D4D924C4B220"
maxItems="-1">
        <ReasonForContact>solicited</ReasonForContact>
        <ItemList>
            <Item name="device-type">OpenStage 80</Item>
            <Item name="related-device-type">OpenStage 80</Item>
            <Item status="failed" name="gigabit-ethernet"></Item>
            <Item name="software-type">Siemens SIP</Item>
            <Item name="related-software-type">Siemens SIP</Item>
            <Item name="software-version">V1 R5.6.53</Item>
            <Item name="related-software-version">V1 R5.6.53</Item>
            <Item name="contact-me-uri">
http://192.168.233.195:8085/contact_dls.html/ContactDLS</Item>
            <Item name="mac-addr">00:01:E3:25:E1:CB</Item>
            <Item name="configuration-changed-flag">false</Item>
            <Item name="part-number">Unknown</Item>
            <Item name="sip-mobility-state">1</Item>
            <Item name="e164">5419431261</Item>
            <Item name="user-pwd">111111</Item>
            <Item status="failed" name="user-pwd-unicode"></Item>
            <Item name="basic-e164">5419431261</Item>
            <Item name="mobility-enabled">true</Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

2. The provisioning service attempts to write an item that is unknown at the phone.

```
<DLSMessage xmlns="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.siemens.com/DLS">
    <Message nonce="7FAA6353A4887BBFA14B78370FE99144">
        <Action>WriteItems</Action>
        <ItemList>
            <Item name="socketed-headset-mode">0</Item>
        </ItemList>
    </Message>
</DLSMessage>
```

3. The phone responds with the status item indicating the unknown item.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.siemens.com/DLS">
    <Message nonce="9DD3EB02AA6A93A00CA63EE07B25ABF3" maxItems="-1"
fragment="final">
        <ReasonForContact status="accepted" action="WriteItems">
reply-to</ReasonForContact>
        <ItemList>
            <Item status="unknown item"
name="socketed-headset-mode"></Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

4. The provisioning service terminates the interaction with a CleanUp.

```
<DLSMessage xmlns="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.siemens.com/DLS">
    <Message nonce="CF8CDC3C82D1FC7966B6318537C6E0F6">
        <Action>CleanUp</Action>
    </Message>
</DLSMessage>
```

3.8.2 Example 2: Configuration Items Failed to be Set at Phone

1. The phone initiates a connection to the provisioning service.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.siemens.com/DLS">
    <Message nonce="104EBC8C863E0C5CA384D4D924C4B220"
maxItems="-1">
        <ReasonForContact>solicited</ReasonForContact>
        <ItemList>
            <Item name="device-type">OpenStage 80</Item>
            <Item name="related-device-type">OpenStage 80</Item>
            <Item status="failed" name="gigabit-ethernet"></Item>
            <Item name="software-type">Siemens SIP</Item>
            <Item name="related-software-type">Siemens SIP</Item>
            <Item name="software-version">V1 R5.6.53</Item>
            <Item name="related-software-version">V1 R5.6.53</Item>
            <Item name="contact-me-uri">http://192.168.233.195:8085/
contact_dls.html/ContactDLS</Item>
            <Item name="mac-addr">00:01:E3:25:E1:CB</Item>
            <Item name="configuration-changed-flag">false</Item>
            <Item name="part-number">Unknown</Item>
            <Item name="sip-mobility-state">1</Item>
            <Item name="e164">5419431261</Item>
            <Item name="user-pwd">111111</Item>
            <Item status="failed" name="user-pwd-unicode"></Item>
            <Item name="basic-e164">5419431261</Item>
            <Item name="mobility-enabled">true</Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

2. The provisioning service attempts to write several settings.

```
<DLSMessage xmlns="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.siemens.com/DLS">
    <Message nonce="104EBC8C863E0C5CA384D4D924C4B220">
        <Action>WriteItems</Action>
        <ItemList>
            <Item name="Canonical-dialing-international-prefix">0
</Item>
            <Item name="Canonical-dialing-operator-code">0</Item>
            <Item
name="Canonical-dialing-emergency-number">999,555</Item>
            <Item name="Canonical-dialing-local-country-code">44
</Item>
            <Item
name="Canonical-dialing-extension-initial-digits">1</Item>
            <Item name="Canonical-dialing-external-access">9</Item>
            <Item name="Canonical-dialing-local-node">943</Item>
            <Item
name="Canonical-dialing-min-local-number-length">4</Item>
            <Item name="Canonical-dialing-local-area-code">541
</Item>
            <Item name="Canonical-dialing-national-prefix">0</Item>
            <Item index="1"
name="Canonical-lookup-international-code">+44541</Item>
            <Item index="1" name="Canonical-lookup-local-code">541</
Item>
            <Item index="2"
name="Canonical-lookup-international-code">+44551</Item>
            <Item index="2" name="Canonical-lookup-local-code">551
</Item>
            <Item index="3"
name="Canonical-lookup-international-code">+44511</Item>
            <Item index="3" name="Canonical-lookup-local-code">511
</Item>
            <Item index="4" name="Canonical-lookup-international-
code">+44521</Item>
            <Item index="4" name="Canonical-lookup-local-code">521
</Item>
            <Item index="5"
name="Canonical-lookup-international-code">+44531</Item>
            <Item index="5" name="Canonical-lookup-local-code">531
</Item>
            <Item index="6"
```

```
name="Canonical-lookup-international-code">+44561</Item>
        <Item index="6" name="Canonical-lookup-local-code">561
</Item>
      </ItemList>
    </Message>
</DLSMessage>
```

3. The phone responds with item status "failed" for any items it could not save.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.siemens.com/DLS">
    <Message nonce="BFBD54B05B45E13F9E7E773F65CE3956" maxItems="-1"
fragment="final">
      <ReasonForContact status="accepted" action="WriteItems">
reply-to</ReasonForContact>
      <ItemList>
        <Item status="failed"
name="Canonical-lookup-international-code" index="6"></Item>
        <Item status="failed" name="Canonical-lookup-local-code"
index="6"></Item>
      </ItemList>
    </Message>
</WorkpointMessage>
```

4. The provisioning service terminates the interaction with a CleanUp.

```
<DLSMessage xmlns="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.siemens.com/DLS">
    <Message nonce="C528BD461ABF3247D545E8BBF5A6D809">
      <Action>CleanUp</Action>
    </Message>
</DLSMessage>
```

3.8.3 Example 3: Item is Read Only

1. The phone initiates a connection to the provisioning service.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.siemens.com/DLS">
    <Message nonce="71E7F7FF699CE4467956071307E7478F"
maxItems="-1">
        <ReasonForContact>solicited</ReasonForContact>
        <ItemList>
            <Item name="device-type">OpenStage 80</Item>
            <Item name="related-device-type">OpenStage 80</Item>
            <Item status="failed" name="gigabit-ethernet"></Item>
            <Item name="software-type">Siemens SIP</Item>
            <Item name="related-software-type">Siemens SIP</Item>
            <Item name="software-version">V1 R5.6.53</Item>
            <Item name="related-software-version">V1 R5.6.53</Item>
            <Item name="contact-me-uri">
http://192.168.233.195:8085/contact_dls.html/ContactDLS</Item>
            <Item name="mac-addr">00:01:E3:25:E1:CB</Item>
            <Item name="configuration-changed-flag">false</Item>
            <Item name="part-number">Unknown</Item>
            <Item name="sip-mobility-state">1</Item>
            <Item name="e164">5419431261</Item>
            <Item name="user-pwd">111111</Item>
            <Item status="failed" name="user-pwd-unicode"></Item>
            <Item name="basic-e164">5419431261</Item>
            <Item name="mobility-enabled">true</Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

2. The provisioning service attempts to write a data item that is read-only at the phone.

```
<DLSMessage xmlns="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.siemens.com/DLS">
    <Message nonce="71E7F7FF699CE4467956071307E7478F">
        <Action>WriteItems</Action>
        <ItemList>
            <Item name="device-type">OpenStage 75</Item>
        </ItemList>
    </Message>
</DLSMessage>
```

3. The phone responds with item status "read-only".

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.siemens.com/DLS">
    <Message nonce="930873879B353894AAB792E175847F39" maxItems="-1"
fragment="final">
        <ReasonForContact status="accepted" action="WriteItems">
reply-to</ReasonForContact>
        <ItemList>
            <Item status="read only" name="device-type"></Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

4. Provisioning service terminates interaction with a CleanUp.

```
<DLSMessage xmlns="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.siemens.com/DLS">
    <Message nonce="34459A26CEBCF29550D72BE0ECB655C3">
        <Action>CleanUp</Action>
    </Message>
</DLSMessage>
```

3.8.4 Example 4: PIN entry exceeds max. retries

1. The provisioning service has requested the "bootstrapping-tan". The user has to enter the PIN at the phone, where the phone has to check if the maximum number PIN entry is exceeded. The phone responds with RFC 'clean-up'.

```
<WorkpointMessage xsi:schemaLocation="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns="http://www.siemens.com/DLS">
    <Message nonce="930873879B353894AAB792E175847F39" maxItems="-1"
fragment="final">
        <ReasonForContact>clean-up</ReasonForContact>
        <ItemList>
            <Item name="cleanup-reason">password retries exceeded</
Item>
        </ItemList>
    </Message>
</WorkpointMessage>
```

2. Provisioning service terminates interaction with a CleanUp. The session is not aborted by the phones CleanUp message; this is done by the CleanUp message from the provisioning service.

```
<DLSMessage xmlns="http://www.siemens.com/DLS"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.siemens.com/DLS">
    <Message nonce="34459A26CEBCF29550D72BE0ECB655C3">
        <Action>CleanUp</Action>
    </Message>
</DLSMessage>
```

3.9 Tracing and Debugging

Besides the error handling capabilities described above, the phone provides detailed tracing information about the communication between phone and provisioning service. To enable this functionality via the WBM, proceed as follows:

- Open the WBM in your browser, log in to the "Administrator Pages", and navigate to "Diagnostics" > "Fault trace configuration".

- Under "Trace levels for components", set the trace level for "DLS client management", e.g. "DEBUG", and set all other trace levels to "OFF".

- Confirm the changes by clicking "Submit".

- When the processes to be traced are finished, you can view the tracing data by clicking on the link "Download trace file" under "Diagnostics" > "Fault trace configuration".

The tracing facility can also be configured and controlled by the provisioning service; see Section 4.13.3, "Fault trace configuration".

4 Phone Parameters - Administration

This section provides a comprehensive survey of the configuration and control parameters in the administration area. The structure and order in which the data are presented corresponds to the web interface of the OpenStage phones and OpenScape Desk Phone IP. For example, Section 4.4.1, "System Identity" is located under Section 4.4, "System", which represents the navigation path "**System** > **System identity**" in the web interface. However, deviations are possible due to changes between firmware versions.

Additionally, there are parameters which are only accessible via the provisioning service. These will be added according to the functional area they belong to. Those parameters which are neither configurable via local/web interface nor associated with parameters configurable via local/web interface are listed in Section 6, "Phone Parameters - Provisioning".

If not otherwise stated, the Items are available on all phone variants, that is, OpenStage 15/20/40/60/80 and OpenScape Desk Phone IP 35/55G.

The syntax for each Item is `<Item name="ItemName">Value</Item>`.

Example: `<Item name="e164">49897223290</Item>`

4.1 Applications

> Applications are available for OpenStage 60/80 and OpenScape Desk Phone IP 55G only.

4.1.1 XML applications

The XML interface enables running server-based applications on the phone with a set of GUI elements. The technologies commonly used in web applications can be used. For more information, please refer to the following documentation:

- Administration Manual OpenStage Asterisk, available under
  http://wiki.unify.com/index.php/OpenStage_and_Asterisk

- Developer's Guide XML Applications, available under
  http://wiki.unify.com/index.php/OpenStage_XML_Applications

By means of the `index` attribute, more than one application can be configured at once. The count starts with `1`.

To determine what to do with an application, that is, create, modify, or delete it, the `XML-app-action` item is used. For each indexed application, an individual action can be defined. As the creation of an application is treated as a modification/update, two values are possible, `delete` and `update`. In the following snippet, the application with the index number 1 is modified, or created:

```
<Item name="XML-app-action" index="1">update</Item>
```

In order to assign the appropriate privileges, the phone must be informed whether the application is an Xpressions or XMLPhonebook application or a regular XML application. Xpressions is a special Unified Communications application which uses the same XML interface as regular XML applications. XMLPhonebook is a preconfigured phonebook application. The information about the type of application is provided in the `XML-app-special-instance` item. In the following snippet, the application with the index number 1 is defined as a normal application, which is the default value:

```
<Item name="XML-app-special-instance" index="1">0</Item>
```

4.1.1.1   Add application

For regular (not Xpressions, not XMLPhonebook) applications, the
`XML-app-special-instance` item must be set to 0 (see Section 4.1.1, "XML applications").
The `XML-app-control-key` is mandatory when using the WPI.

WBM Name	Item name	Type	Values	Description
Display name	`XML-app-display-name <index>`	Text. Max. 20 characters.	Default: NULL	Displayed in the applications tab once the application is configured.
Application name	`XML-app-name <index>`	Text. Max. 20 characters.	Cannot be empty. Cannot contain ^ character. Must be different to the Display Name assigned to other applications. Default: NULL	Used by the phone software to identify the XML application running on the phone.
HTTP Server address	`XML-app-server-addr <index>`	IP address or hostname. Max. 64 characters.	Cannot be empty. Default: NULL	IP address or domain name of the server which hosts the remote program.
HTTP Server port	`XML-app-server-port <index>`	Integer	Port number. Cannot be empty. Default: NULL	Number of the port used by the server to provide the XML application.
Protocol	`XML-app-transport <index>`	Enumeration	`0`=HTTP; `1`=HTTPS; Default: `0`	Communication protocol for data exchange with the server.
Program name on server	`XML-app-program-name <index>`	Text. Max. 100 characters	Cannot be empty. Default: NULL	Relative path to the servlet or to the first XML page of the application on the server.

WBM Name	Item name	Type	Values	Description
Auto start	`XML-app-auto-start<index>`	Boolean	`true`/`false` Default: `false`	Determines whether the application is automatically started in the background or only when first selected. Available with firmware version V2.
Use proxy	`XML-app-proxy-enabled<index>`	Boolean	`true`/`false` Default: `false`	Enables or disables the use of a proxy for communication with the server hosting the application.
XML Trace enabled	`XML-app-remote-debug<index>`	Boolean	`true`/`false` Default: `true`	Enables or Disables the debugging function. If disabled, the phone will send specific debug information to a specified server.
Debug program on server	`XML-app-debug-prog-name<index>`	Text. Max. 100 characters.	Default: NULL	The relative path to a special service, or program, that receives the debug information created by the phone.
Number of tabs	`XML-app-num-tabs<index>`	Integer	`0` to `3` Default: `0`	Number of internal tabs for an XML application. To make an application with internal tabs work, one of the application names (Tab 1...3 Application Name) must be the same as the overall application name.
All tabs Start	`XML-app-all-tabs-start<index>`	Boolean	`true`/`false` Default: `false`	Determines whether all tabs of the application or only the first tab is started on application startup. Only meaningful for application with 2 or 3 tabs. Available with firmware version V2.

WBM Name	Item name	Type	Values	Description
Tab 1 Display Name	`XML-app-tab1-display-name<index>`	Text. Max. 20 characters.	Default: NULL	Name to be displayed on the first internal tab.
Tab 1 Application Name	`XML-app-tab1-name<index>`	Text. Max. 20 characters.	Default: NULL	Internal application name for the first tab, used by the phone software.
Tab 2 Display Name	`XML-app-tab2-display-name<index>`	Text. Max. 20 characters.	Default: NULL	Name to be displayed on the second internal tab.
Tab 2 Application Name	`XML-app-tab2-name<index>`	Text. Max. 20 characters.	Default: NULL	Internal application name for the second tab, used by the phone software.
Tab 3 Display Name	`XML-app-tab3-display-name<index>`	Text. Max. 20 characters.	Default: NULL	Name to be displayed on the third internal tab.
Tab 3 Application Name	`XML-app-tab3-name<index>`	Text. Max. 20 characters.	Default: NULL	Internal application name for the third tab, used by the phone software.
Restart after change	`XML-app-restart<index>`	Boolean	`true`/`false` Default: `false`	Indicates whether the application is to be automatically stopped and restarted in case another application by the same name is already running.

WBM Name	Item name	Type	Values	Description
	`XML-app-control-key <index>`	Enumeration	0=no mode key; 1=CallView mode key (not support with OS60/80 V3R1); 2=Phonebook mode key, as used with preconfigured special applications; 3=CallLog mode key; 4=Messages mode key, as used with preconfigured special applications; 5= Settings mode key (not support with OS60/80 V3R1); 6=Help mode key, like the application type "help application" Default: 0	Specifies which mode key starts the application. The following mode keys can be used to start an XML application: ⊕ phonebook/directory key ✉ messages key ⊙ call log key (available with OS60/80 version V2) ⓘ help key (OS60/80 only, available with version V2R1) If set to "0" the application is controlled via the applications menu rather than a dedicated key.
	`XML-app-special-instance <index>`	Enumeration	0=Normal; 1="Xpressions"; 2="XMLPhonebook";	DLS use only. Else, set automatic depending on use of "Add application", "Add Xpressions", or "Add XMLPhonebook"

4.1.1.2 Modify Application

Regarding the provisioning interface, the modification of an application is the same procedure as the creation. The `XML-app-action` item must be set to `update`, as in the following snippet:

```
<Item name="XML-app-action" index="1">update</Item>
```

4.1.1.3 Xpressions

For Xpressions applications, the `XML-app-special-instance` item must be set to 1 (see Section 4.1.1, "XML applications").

4.1.1.4 Messages Application

This is intended for a regular XML application with voicemail/mailbox functionality. When configured on the phone, a press on ⌂ or Messages will invoke this application. For messages applications, the `XML-app-control-key` item must be set to 4 and `XML-app-special-instance` to 0 (see Section 4.1.1, "XML applications").

4.1.1.5 XMLPhonebook/Directory Application

This is a preconfiguration intended for a regular XML application with phonebook/directory functionality. When configured on the phone, a press on ⌂ or Directory will invoke this application, in place of the personal (local) or corporate (LDAP) phonebook. For XML phonebook/directory applications, the `XML-app-special-instance` item must be set to 2 (see Section 4.1.1, "XML applications").

4.1.1.6 Phonebook/Directory Application

This is intended for a regular XML application with phonebook/directory functionality. When configured on the phone, a press on ⌂ or Directory will invoke this application, in place of the personal (local) or corporate (LDAP) phonebook. For phonebook/directory applications, the `XML-app-control-key` item must be set to 2 and `XML-app-special-instance` to 0 (see Section 4.1.1, "XML applications").

4.1.1.7 Call Log Application

This is intended for a regular XML application with call log functionality. When configured on the phone, a press on ⌂ or Call Log will invoke this application. For Call Log applications, the `XML-app-control-key` item must be set to 3 and `XML-app-special-instance` to 0 (see Section 4.1.1, "XML applications").

4.1.1.8   Help Application (V2R1)

This is intended for a regular XML application with help functionality (OS60/80 only). When configured on the phone, a press on ⑦ will invoke this application. For messages applications, the `XML-app-control-key` item must be set to 6 and `XML-app-special-instance` to 0 (see Section 4.1.1, "XML applications").

4.2   Bluetooth

WBM Name	Item name	Type	Values	Description
Enable Bluetooth interface	`enable-bluetooth-interface`	Boolean	`true`/`false` Default: `true`	Enables or disables the Bluetooth interface. Read only if locked by provisioning service. Available for OpenStage 60/80.

4.3   Network

4.3.1   General IP configuration

WBM Name	Item name	Type	Values	Description
Protocol Mode	`ip-protocol-mode`	Enumeration	`0`=IPv4; `1`=IPv6; `2`=IPv4_IPv6 (dual stack)	IP version to be used by the phone.
LLDP-MED Enabled	`lldp-enabled`	Boolean	`true`/`false` Default: `false`	If enabled, a VLAN ID and Quality of Service parameters can be provided via LLDP-MED.
DHCP Enabled	`dhcp-enabled`	Boolean	`true`/`false` Default: `true`	Enable or disable DHCP discovery.
DHCPv6 Enabled	`ipv6-dhcp-enabled`	Boolean	`true`/`false` Default: `true`	Enable or disable DHCPv6 discovery.
VLAN discovery	`vlan-method`	Enumeration	`0`=Manual; `1`=DCHP; `2`=LLDP; Default: `1`	VLAN discovery method.

WBM Name	Item name	Type	Values	Description
VLAN ID	`vlan-id`	Integer	`0` to `4095` Default: NULL	VLAN ID for the phone. Only writable when not already defined by DHCP.
DNS domain	`dns-domain-name`	Text	Text Default: NULL	DNS domain wherein the phone is residing. Only writable when not already defined by DHCP.
Primary DNS	`dns-server-addr`	IP address	IP address Default: NULL	Primary DNS server address. Only writable when not already defined by DHCP.
Secondary DNS	`dns-server-addr2`	IP address	IP address Default: NULL	Secondary DNS server address. Only writable when not already defined by DHCP.
HTTP proxy	`http-proxy-addr`	IP address or hostname. Max. 64 characters.	IP address or hostname. Default: NULL	HTTP proxy to be used for XML applications.

4.3.2 IPv4 Configuration

WBM Name	Item name	Type	Values	Description
LLDP-MED En-abled	`lldp-enabled`	Boolean	`true/false` Default: `false`	If enabled, a VLAN ID and Quality of Service parameters can be provided via LLDP-MED.
DHCP Enabled	`dhcp-enabled`	Boolean	`true/false` Default: `true`	Enable or disable DHCP discovery.
DHCP lease reuse	`dhcp-reuse`	Boolean	`true/false` Default: `false`	If enabled, the phone will keep its DHCP-based IP address even if the lease expires. To prevent address conflicts, the phone will send ARP requests in 5 second intervals. Additionally, it will send discovery messages periodically to obtain a new DHCP lease. Available with OpenStage V2R1.
IP address	`ipaddress`	IP address	IP address Default: NULL	IP address for the phone. Only writable when not already defined by DHCP.
Subnet mask	`mask`	Subnet mask	Subnet mask Default: NULL	Network mask for the phone. Only writable when not already defined by DHCP.
Default route	`route`	IP address	IP address Default: NULL	Default network route for the phone. Only writable when not already defined by DHCP.
Route 1 IP ad-dress	`route1`	IP address	IP address Default: NULL	Specific route 1.
Route 1 gateway	`gw1`	IP address	IP address Default: NULL	Gateway for specific route 1.

WBM Name	Item name	Type	Values	Description
Route 1 mask	`mask1`	Subnet mask	Subnet mask Default: NULL	Subnet mask for specific route 1.
Route 2 IP address	`route2`	IP address	IP address Default: NULL	Specific route 2.
Route 2 gateway	`gw2`	IP address	IP address Default: NULL	Gateway for specific route 2.
Route 2 mask	`mask2`	Subnet mask	Subnet mask Default: NULL	Subnet mask for specific route 2.

4.3.3 IPv6 Configuration (V3)

WBM Name	Item name	Type	Values	Description
LLDP-MED Enabled	`lldp-enabled`	Boolean	`true/false` Default: `false`	If enabled, a VLAN ID and Quality of Service parameters can be provided via LLDP-MED.
DHCPv6 Enabled	`ipv6-dhcp-enabled`	Boolean	`true/false` Default: false	Enable or disable DHCPv6 support.
DHCPv6 lease reuse	`ipv6-dhcp-addr-reuse`	Boolean	`true/false` Default: `false`	If enabled, the phone will keep its DHCP-based IP address even if the lease expires.
Global Address	`ipv6-ipaddress-global`	IP address	IP address Default: NULL	Global IPv6 address
Global Address Prefix Len	`ipv6-ipaddress-global-prefix-length`	Integer	0 to128	Prefix length for the global IPv6 address.
Global Gateway	`ipv6-ipaddress-global-gw`	IP address	IP address Default: NULL	Global Gateway IPv6 address
Link Local Address	`ipv6-ipaddress-link-local`	IP address	IP address Default: NULL	Link-local IPv6 address.

WBM Name	Item name	Type	Values	Description
Route 1 Dest.	`ipv6-route1-destination`	IP address	IP address Default: NULL	Destination IPv6 address for the first static route.
Route 1 Prefix Len	`ipv6-route1-prefix-length`	Integer	0 to 128	Prefix length for the first static route.
Route 1 Gateway	`ipv6-route1-gw`	IP address	IP address Default: NULL	IPv6 address of the router/gateway for the first static route.
Route 2 Dest.	`ipv6-route2-destination`	IP address	IP address Default: NULL	Destination IPv6 address for the second static route.
Route 2 Prefix Len	`ipv6-route2-prefix-length`	Integer	0 to 128	Prefix length for the second static route
Route 2 Gateway	`ipv6-route2-gw`	IP address	IP address Default: NULL	IPv6 address of the router/gateway for the second static route.

4.3.4 Update Service

WBM Name	Item name	Type	Values	Description
DLS address	`dls-addr`	IP address or hostname. Max. 64 characters.	IP address or hostname. Default: NULL	IP address of the provisioning server. Only writable when not already defined by DHCP.
DLS port	`dls-port`	Integer	Default: `18443`	Port the provisioning service is listening at. Only writable when not already defined by DHCP.

WBM Name	Item name	Type	Values	Description
Contact gap	`dls-contact-interval`	Integer	Default: `300`	Minimum time interval in seconds that must elapse between responses to contact-me requests. Not supported on OpenStage phones.
Revert to default security	`goto-default-mode`	Boolean	`true/false` Default: false	Enable or disable default security.
Mode	`dls-mode-secure`	Enumer-ation	0="Default" 1="Secure no PIN" 2="Secure PIN" 3="Awaiting PIN" 4="Processing PIN" 5="Re-enter PIN" 6="Secure PIN failed" 7="Restart boot-strap" Default: `0`	For detailed description of security status see Section 4.3.4, "Security Status".
Security PIN	`pin-password`	Pass-word	8 to 32 charac-ters Default: NULL	A string containing <pass-word><tan> where <password> is used to decrypt data sent during bootstrapping and <tan> is the last 3 characters in the PIN and is used to confirm the mode back to the provisioning service. The password is not persisted over restart.

Detailed Description of Mode

Value	Description
0 = Default	The phone uses HTTPS with a built-in default certificate for connections to the provisioning service
1 = Secure no PIN	Phone uses HTTPS with a non-PIN protected certificate downloaded during bootstrap for connections to provisioning service but a PIN was not required for bootstrap and thus the TAN is null
2 = Secure PIN	Phone uses HTTPS with a PIN protected certificate downloaded during bootstrap for connections to provisioning service and since a PIN was required for bootstrap the TAN is not null
3 = Awaiting PIN	Phone has been bootstrapped into Secure Mode but requires a PIN to be entered to decrypt the bootstrap data.
4 = Processing PIN	Phone has been bootstrapped into Secure Mode and is using the PIN entered to decrypt the bootstrap data.
5 = Re-enter PIN	Phone has been bootstrapped into Secure Mode but the PIN was determined to be invalid (i.e. either unable to decrypt the bootstrap data, or the bootstrap data was decrypted OK but the provisioning service rejected the TAN), hence the correct PIN must be re-entered.
6 = Secure PIN failed	The PIN was entered more times than has been allowed by the provisioning service. And now no further PIN entry attempts are permitted until the DLS restarts the bootstrap process.
7 = Restart bootstrapp	The bootstrap data is no longer available for decrypting and the DLS must restart the bootstrap process to provide new data and a PIN (if appropriate).

Table 4-1   Security Status

Parameters Only Accessible Via Provisioning Service

Item name	Type	Values	Description

`contact-me-uri`	URI	Example:
		`http://`
		`137.223.231.`
		`41:8085/`
		`contact_dls.`
		`html/`
		`ContactDLS`
			URI to which the provisioning server must send its contact-me messages.
			Read-only.

Item name	Type	Values	Description
`configuration-changed-flag`	Boolean	`true/false`	Set to `true` when the configuration has been changed, either via local menu, or web interface, or phone manager.
`configuration-attached-flag`	Boolean	`true/false`	Used in messages from the phone which inform the provisioning service about local configuration changes. By setting this parameter to true, the phone indicates that the current item list contains the changed configuration parameters. Supported with OpenStage V2R2.
`configuration-changed-number`	Integer		Sequential number which is increased with every startup message or configuration change message from the phone. This enables the provisioning service to keep track of sequential changes on the phone side. Supported with OpenStage V2R2.
`goto-secure-mode`	Enumeration	0="nopin" 1="pin" Default: `0`	Sensitive data for Secure Mode are transferred unencrypted (= 0) or protected by a password (= 1)
`goto-default-mode`	Boolean	`true/false`	Disable Secure Mode and go back to Default Mode
`max-pin-retries`	Integer	`1` to `10` Default: `NULL`	Maximum number of PIN entries allowed by provisioning service. If exceeded the phone does not attempt to contact the provisioning service in Secure Mode until provisioning service restarts the bootstrap procedure.
`bootstrapping-tan`	Password	3 characters Default: `NULL`	TAN part of the PIN, i.e. last 3 characters of PIN entered by user. Read by provisioning service to confirm correct PIN entry. Only applicable if "goto-secure-mode" is set to "pin".

Item name	Type	Values	Description
`secure-mode-data`	String		Provisioning service provides phones with encrypted data required for Secure Mode (bootstrapping = PIN).
`dls-secure-port`	Integer	Portnumber Default: `18444`	Portnumber to reach provisioning service in Secure Mode (bootstrapping = no PIN)
`dls-client-certificate`	PEM file (single certificate)	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Provisioning service provides phones with client certificate (bootstrapping = no PIN)
`dls-server-ca <index=0>`	PEM file (single certificate)	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Provisioning service provides phones with server CA (bootstrapping = no PIN)
`dls-server-ca <index=1>`	PEM file (single certificate)	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Provisioning service provides phones with server CA (bootstrapping = no PIN)
`local-control-feature-availability`	Boolean	`true/false` Default: `true`	Enable or disable local control of features.

4.3.5 QoS

> With firmware version V3, MLPP capabilities has been added; however, the associated parameters are not relevant for this document.

WBM Name	Item name	Type	Values	Description
Layer 2	`qos-layer2`	Boolean	`true/false` Default: `true`	Enable or disable QoS layer 2.
Layer 2 voice	`l2qos-voice`	Integer	`0` to `7` Default: `5`	Sets the layer 2 CoS (Class of Service) value for voice data (RTP streams).
Layer 2 signalling	`l2qos-signalling`	Integer	`0` to `7` Default: `5`	Sets the CoS (Class of Service) value for signaling.
Layer 2 default	`l2qos-default`	Integer	`0` to `7` Default: `0`	Sets the default CoS (Class of Service) value.
Layer 3	`qos-layer3`	Boolean	`true/false` Default: `true`	Activates or deactivates QoS on layer 3.
Layer 3 voice	`l3qos-voice`	Enumeration	`0`=BE; `10`=AF11; `12`=AF12; `14`=AF13; `18`=AF21; `20`=AF22; `22`=AF23; `26`=AF31; `28`=AF32; `30`=AF33; `34`=AF41; `36`=AF42; `38`=AF43; `46`=EF; `56`=CS7; Default: `46`	Sets the layer 3 CoS (Class of Service) value for voice data (RTP streams).

WBM Name	Item name	Type	Values	Description
Layer 3 signalling	`l3qos-signalling`	Enumeration	0=BE; 10=AF11; 12=AF12; 14=AF13; 18=AF21; 20=AF22; 22=AF23; 24=CS3; 26=AF31; 28=AF32; 30=AF33; 32=CS4; 34=AF41; 36=AF42; 38=AF43; 40=CS5; 46=EF; 56=CS7; Default: 26	Sets the layer 3 CoS (Class of Service) value for signaling.
Priority				Not applicable.
Immediate				Not applicable.
Flash				Not applicable.
Flash override				Not applicable.

4.3.6 Port configuration

WBM Name	Item name	Type	Values	Description
SIP server	`reg-port`	Integer	Port number Default: 5060	Port of the SIP proxy server.
SIP registrar	`registrar-port`	Integer	Port number Default: 5060	Port of the server at which the phone registers.
SIP gateway	`sgnl-gateway-port-user`	Integer	Port number Default: 5060	Port of the SIP gateway.
SIP local	`phone-port`	Integer	Port number Default: 5060	Port used by the phone for sending and receiving SIP messages.

WBM Name	Item name	Type	Values	Description
Backup proxy	`backup-port`	Integer	Port number Default: `5060`	Port of the backup proxy server.
RTP base	`rtp-base-port`	Integer	Port number Default: `5010`	Base port number used for negotiating the RTP port.
Download server (default)				Not available in the provisioning interface.
LDAP server	`ldap-server-port`	Integer	Port number Default: `389`	Port on which the LDAP server is listening for requests. If ldap-transport type is TLS then use the secure LDAP port (ldap-encrypted-port), otherwise use LDAP Server Port (ldap-server-port), see Section 6.12, "LDAP", on page 6-249.
LDAP encrypted port	`ldap-encrypted-port`	Integer	Port number Default: `636`	Secure LDAP Port - Specifies the TLS port on the LDAP server to be used for an LDAPS. If ldap-transport type is TLS then use the secure LDAP port (ldap-encrypted-port), otherwise use LDAP Server Port (ldap-server-port), see Section 6.12, "LDAP", on page 6-249.
HTTP proxy	`http-proxy-port`	Integer	Port number Default: NULL	Port of the proxy used for XML applications.

WBM Name	Item name	Type	Values	Description
LAN port speed	`port1`	Enumeration	0=Automatic; 1=10 Mbit/s Half Duplex; 2=10Mbit/s Full Duplex; 3=100 Mbit/s Half Duplex; 4=100 Mbit/s Full Duplex; 5=Gigabit/s Half Duplex; 6=Gigabit/s Full Duplex; Default: 0	Speed of the ethernet port connected to the LAN switch.
PC port speed	`port2`	Enumeration	0=Automatic; 1=10 Mbit/s Half Duplex: 2=10Mbit/s Full Duplex; 3=100 Mbit/s Half Duplex; 4=100 Mbit/s Full Duplex; 5=Gigabit/s Half Duplex; 6=Gigabit/s Full Duplex; Default: 0	Speed of the ethernet port connected to the PC.
PC port mode	`port2-mode`	Enumeration	0=Disabled; 1=Enabled; 2=Mirror; Default: 0	Controls the PC port.
PC port autoMDIX	`port2-auto-mdix-enabled`	Boolean	`true`/`false` Default: `false`	If enabled, the LAN port connected to the PC switches automatically between MDI and MDI-X.

4.3.7 LLDP-MED Operation

WBM Name	Item name	Type	Values	Description
Time to live (seconds)	`lldp-timetolive`	Enumeration	`40` / `60` / `80` / `100` / `110` / `120` / `140` / `180` / `240` / `320` / `400`	In order to keep the stored LLDP information up-to-date, a specific TTL (Time To Live) is specified. This value tells a device how long the received information is valid.

4.4　　　System

4.4.1　　　System Identity

WBM Name	Item name	Type	Values	Description
Terminal number	`e164`	Text	Default: `NULL`	Number to be registered at the SIP registrar.
Terminal name	`sip-name`	Text	Default: `NULL`	Used as a display name in a SIP message.
Display identity	`display-id-unicode`	Unicode text. Max. 24 characters.	Default: `NULL`	When Enable ID is enabled, this value is displayed in the phone's status bar instead of the Terminal number or Terminal name.
Enable ID	`use-display-id`	Boolean	`true` / `false` Default: `false`	Enables the display of the Display identity.
Web name	`hostname`	Text	Default: Based on phone type and MAC address	Default DNS hostname for the phone. Available with OpenStage V2.
DNS name construction	`automatic-hostname-type`	Enumeration	`0`=no DDNS hostname; `1`=only hostname; `2`=only number; `3`=prefix number; `4`=MAC based Default: `2`	Determines how the DNS host name for the phone is constructed. Available with OpenStage V2.

Table 4-2

4.4.2 SIP interface

WBM Name	Item name	Type	Values	Description
Outbound proxy	`outbound-proxy-user`	Boolean	`true` / `false` Default: `false`	If true, the SIP server will resolve the domain in the SIP request. Otherwise, the phone will perform this task.
Default OBP domain	`default-domain`	DNS name	DNS name Default: Null	If the number or name dialed by the user does not provide a domain, this value will be appended to the name or number. Otherwise, the domain of the Outbound proxy will be appended.
SIP transport	`sip-transport-user`	Enumeration	0=UDP; 1=TCP; 2=TLS; Default: `0`	Transport protocol to be used for SIP messages.
Call transaction response timer (ms)	`transaction-timer`	Integer	`3700` to `32000` (milliseconds) Default: `32000`	A SIP response to an INVITE message must arrive within a timespan not greater than this value. It is also used as wait timer for retransmissions of non-INVITE requests.
NonCall transaction response timer(ms)	`transaction-timer-f`	Integer	`3700` to `32000` (milliseconds) Default: `32000`	A SIP response to a non-INVITE message must arrive within a timespan not greater than this value. On expiry, the phone attempts to contact the backup server, if configured. It is also used for TCP connect timeout.
Reg. backoff (seconds)	`registration-backoff-timer`	Integer	`60` to `600` (seconds) Default: `60`	Maximum waiting time before sending another REGISTER message in case the first attempt has failed.

WBM Name	Item name	Type	Values	Description
Connectivity check timer (seconds)	`voip-connectivity-check-interval`	Integer	`10` to `3600` (seconds) `0` disables the check. Default: 120	When set to a non-zero value, test messages will be sent at the defined interval to check the TLS connection. Relates to sending of keep-alive message. For keyset working, applies to all lines.
Keep alive format	`sip-keepalive-method`	Enumeration	0="Sequence"; 1="CRLF" Default: 0	Selects the keep-alive method to be used between Comms and the switch. Ignored for a TCP keep alive.
Media Negotiation	`media-negotiation-mode`		0="Single IP"; 1="ANAT"	When Media negotiation is set to "ANAT", ANAT is supported; the phone will re-register with the SIP server and advertise ANAT support in the SIP header. When set to "Single IP", ANAT support is disabled. Available with OpenStage V3.
Media IP Mode	`sip-media-IP-mode`		0="IPv4"; 1="IPv6"; 2="IPv4_IPv6"; 3="IPv6_IPv4"	Defines which IP version is to be used for voice transmission. With "IPv4", only IPv4 is used; with "IPv6", only IPv6 is used; with "IPv4_IPv6", both IPv4 and IPv6 can be used, but IPv4 is preferred; with "IPv6_IPv4", both IPv6 and IPv4 can be used, but IPv6 is preferred. Available with OpenStage V3.

4.4.3 Registration

WBM Name	Item name	Type	Values	Description
SIP server address	`reg-addr`	IP address or hostname. Max. 64 characters.	IP address or hostname. Default: NULL	IP address or host name of the SIP proxy server.
SIP registrar address	`registrar-addr`	IP address or hostname. Max.64 characters.	IP address or hostname. Default: NULL	IP address or host name of the registration server.
SIP gateway address	`sgnl-gateway-addr-user`	IP address or hostname. Max. 64 characters.	IP address or hostname. Default: NULL	IP address or host name of the SIP gateway. To clear the SIP Gateway address it must be set to 0.0.0.0
Session timer enabled	`session-timer`	Boolean	`true`/`false` Default: `false`	Basic keep-alive mechanism between 2 user agents or phones. If enabled, the phone sends periodic re-INVITEs to keep the session alive. If no re-INVITE is received before the interval passes, the session is considered terminated.
Session duration (seconds)	`session-duration`	Integer	Number of seconds. Default: `3600`	Expiration time for a SIP session timer.
Registration timer (seconds)	`reg-ttl`	Integer	Number of seconds. Default: `3600`	Expiry time of a registration.

WBM Name	Item name	Type	Values	Description
Server type	`server-type`	Enumer-ation	`0`=Other; `1`=OpenScape Voice; Default: `0`	Type of server the phone will register to, or is regis-tered at.
Realm	`realm`		Default: NULL	Protection domain for au-thentication at the SIP server.
User ID	`sip-user-id`		Default: NULL	Username required for an authenticated registra-tion.
Password	`sip-pwd`	Pass-word	Default: NULL	Password required for an authenticated registra-tion.
MLPP base				Not applicable
MLPP Domain				Not applicable
Other Domain				Not applicable
Backup registra-tion allowed	`backup-registration`	Boolean	`true`/`false` Default: `true`	Determines whether or not the backup proxy is used as a SIP registrar.
Backup proxy ad-dress	`backup-addr`	IP ad-dress or host-name. Max. 64 charac-ters.	IP address or hostname. Default: NULL	IP address or hostname of the backup proxy server.
Backup registra-tion timer (sec-onds)	`backup-reg-timer`	Integer	Number of seconds. `0` or `11` to `4320`.	Expiry time of the regis-tration with the backup server in seconds.
Backup transport	`backup-transport`	Enumer-ation	`0`=UDP; `1`=TCP; Default: `0`	Transport protocol to be used for messages to the backup proxy.
Backup OBP flag	`backup-outbound-proxy`	Boolean	`true`/`false` Default: `false`	Determines whether or not the backup proxy is used as an outbound proxy.

4.4.4   SNMP

WBM Name	Item name	Type	Values	Description
Trap sending enabled	`snmp-traps-active`	Boolean	`true`/`false` Default: `false`	Enables or disables the sending of a TRAP message to the SNMP manager.
Trap destination	`snmp-trap-addr`	IP address or hostname. Max.64 characters.	IP address or hostname. Default: NULL	IP address or hostname of the SNMP manager that receives traps.
Trap destination port	`snmp-trap-port`	Integer	Port number Default: `162`	Port on which the SNMP manager is receiving TRAP messages.
Trap community	`snmp-trap-pwd`	Text	Default: `snmp`	SNMP community string for the SNMP manager receiving TRAP messages.
Queries allowed	`snmp-queries-allowed`	Boolean	`true`/`false` Default: `false`	Enables or disables queries from the SNMP manager.
Query password	`snmp-pw`	Text	Any string except "public", "private", "PUBLIC", "Public", "puBlic" and other case related variants.	Password for the execution of a query by the SNMP manager.
Diagnostic sending enabled	`diagnostic-traps-active`	Boolean	`true`/`false` Default: `false`	Enables or disables the sending of diagnostic data to the SNMP manager.

WBM Name	Item name	Type	Values	Description
Diagnostic destination	`diagnostic-trap-addr`	IP address or hostname. Max. 64 characters.	IP address or hostname. Default: NULL	IP address or hostname of the SNMP manager receiving diagnostic data.
Diagnostic destination port	`diagnostic-trap-port`	Integer	Port number. Default: `162`	Port on which the SNMP manager is receiving diagnostic data.
Diagnostic community	`diagnostic-trap-pwd`	Text	Default: `snmp`	SNMP community string for the SNMP manager receiving diagnostic data.
Diagnostic to generic destination	`diagnostic-snmp-active`	Boolean	`true`/`false` Default: `false`	Enables or disables the sending of QoS traps to a generic destination.
QoS traps to QCU	`qdc-qcu-active`	Boolean	`true`/`false` Default: `false`	Enables or disables the sending of TRAP messages to the QCU server.
QCU address	`qdc-collection-unit-addr`	IP address or hostname. Max. 64 characters	IP address or hostname. Default: NULL	IP address or hostname of the QCU server.
QCU port	`qdc-collection-unit-port`	Integer	Port number. Default: `12010`	Port on which the QCU server is listening for messages.
QCU community	`qdc-trap-pwd`	Text	Default: `QOSDC`	QCU community string.
QoS to generic destination	`qdc-snmp-active`	Boolean	`true`/`false` Default: `false`	Enables or disables the sending of QoS traps to a generic destination.

4.4.5　Features

4.4.5.1　Configuration

WBM Name	Item name	Type	Values	Description
Emergency number	`emergency-e164`	Text	Default: `NULL`	If the phone is locked, a clickable area for making an emergency call is created.
Voice mail number	`voice-mail-e164`	Text	Default: `NULL`	Call number of the voice mail box.
MWI LED	`mwi-led-setting`	Enumeration	`0`=Key only `1`=Key & Alert-Bar `2`=AlertBar only Default: `1`, for OS40 US / DPIP35 / DPIP55: `2`	Defines how a new Voice-Mail is indicated.
Missed call LED	`missed-call-led`	Enumeration	`0`=Key only `1`=Key & Alert-Bar `2`=AlertBar only `3`=no LED OS 20 only: `0`=Key Only `3`=no LED Defaults: OS20/15/40/60/80 : `0` OS40 US / DPIP35: `3`	Defines how a new Missed Call is indicated.

WBM Name	Item name	Type	Values	Description
Allow refuse	`refuse-call`	Boolean	`true`/`false` Default: `true`, OS40 US/ DPIP35 / DPIP55: `false`	Defines whether the Refuse call feature is available on the phone.
Hot/warm phone	`hot-line-warm-line`	Enumer-ation	1=No action; 2=Hot phone; 3=Warm phone	The number specified in Hot/warm destination is dialed immediately (hot phone) or after a configurable delay (warm phone) when the user goes off-hook. Available with OpenStage V2.
Hot/warm desti-nation	`hot-line-warm-line-digits`	Text	Call number.	Number to be dialed when Hot phone or Warm phone is enabled. Available with OpenStage V2.
Initial digit timer (seconds)	`initial-digit-timer`	Integer	1 to 120 (seconds) Default: 30	Timeout for entering the first digit after going off-hook. On expiry, the phone will change to idle mode. Available with OpenStage V2.
Allow uaCSTA	`uaCSTA-enabled`	Boolean	`true`/`false` Default: `true`	If set to true, applications which support the uaCSTA standard will have access to the phone.

WBM Name	Item name	Type	Values	Description
Server features	`server-based-features`	Boolean	`true`/`false` Default: `false`	Must be set to true for using server based Call Forwarding. When phone based DND and phone based call forwarding are to be used, it must be set to false. Before changing the value, please ensure that both Call Forwarding and DND are not activated. Otherwise, the user will not be able to control the feature any more. It is recommended to set this parameter when setting up the phone, and avoid further changes, as possible.
Not used timeout (minutes)	`not-used-timeout`	Integer	`1` to `5` (minutes) Default: `2`	Timeout for the local user and admin menu. When the time interval is over, the menu is closed and the administrator/user is logged out.
Transfer on hangup	`unconditional-transfer`	Boolean	`true`/`false` Default: `false`	This feature applies to the following scenario: While A is talking to B, C calls A. A accepts the call, so B is on hold and the call between A and C is active. If Transfer on hangup is enabled, and A goes on-hook, B gets connected to C. If disabled, C will be released when A hangs up, and A has the possibility to reconnect to B. By default, the feature is disabled.

WBM Name	Item name	Type	Values	Description
Bridging enabled	`bridging-enabled`	Boolean	`true`/`false` Default: `false`	Determines whether bridging is enabled
Dial plan enabled	`dial-plan-enabled`	Boolean	`true`/`false` Default: `false`	If active, dialplan is enabled.
FPK program timer	`fpk-long-press-timer`	Enumeration	`0` to `5` Default: `2`, DPIP35: `0`	0 (=OFF) means no long-press timer is active. If set to 2 (=ON) and an FPK is pressed for 2 seconds, it enters programming mode. Other values are not active and reserved for future use. Relevant for OpenStage 15/40/60/80. Available with OpenStage V2R2.
Group pickup tone allowed	`group-pickup-tone-allowed`	Boolean	`true`/`false` Default: `true`	If enabled, an acoustic signal is created for incoming pickup group calls.
Group pickup as ringer	`group-pickup-as-ringer`	Boolean	`true`/`false` Default: `true`	Determines whether the current ringtone or an alert beep is used.
Group pickup visual alert	`group-pickup-alert-type`	Enumeration	`0`=Prompt; `1`=Notify; Default: `0`	Defines the user action required to accept a pickup call.
BLF alerting	`blf-tone-type`	Enumeration	`0`=beep; `1`=ring tone Default: `0`	Selects the sound for indicating an incoming call for the monitored extension. Available with OpenStage V2R1.
MLPP ringer				Not relevant.

WBM Name	Item name	Type	Values	Description
Callback ringer	`ccss-ringer`	Enumeration	0=alert-internal 1=alert-external Default: 0	Specifies a distinctive ringer to be be used with the Call back prompt to announce the availability of a call back call to a target
Impact ringer level	`IL-lower-ringer`	Enumeration	0=alert-internal 1=alert-external 2=Impact-level Default: empty	Select ringer to be played to alert the user to a new incoming call from a Lower IL
Recorder Address	`call-record-phone-number`	Call number		SIP DN / call number of the voice recorder.
Recording mode="Disabled"	`call-record-auto-start`	Boolean	`false`	No call will be recorded, and the corresponding FPK function (Section 4.4.5.3, "Call recording") is disabled. Available with OpenStage V2R2.
	`call-record-all-calls`	Boolean	`false`	
	`feature-availability index="24"`	Boolean	`false`	
Recording mode="Manual"	`call-record-auto-start`	Boolean	`false`	Call recording can be started and stopped with the FPK function. Available with OpenStage V2R2.
	`call-record-all-calls`	Boolean	`false`	
	`feature-availability index="24"`	Boolean	`true`	
Recording mode= "Auto-start"	`call-record-auto-start`	Boolean	`true`	Call recording is started when a call is established, and can be stopped with the FPK function. Available with OpenStage V2R2.
	`call-record-all-calls`	Boolean	`false`	
	`feature-availability index="24"`	Boolean	`true`	

WBM Name	Item name	Type	Values	Description
Recording mode= "All calls"	`call-record-auto-start`	Boolean	`true`	Call recording is started when a call is established, and can not be stopped with the FPK function. Available with OpenStage V2R2.
	`call-record-all-calls`	Boolean	`true`	
	`feature-availability index="24"`	Boolean	`true`	
Audible Notification="Off"	`call-record-audible-indication`	Boolean	`false`	The user will not notice that a call is being recorded. Available with OpenStage V2R2.
	`call-record-audible-indication-continuous`	Boolean	`false`	
Audible Notification="Single-shot"	`call-record-audible-indication`	Boolean	`true`	A single short beep tone is played through the handset, headset or loudspeaker when call recording starts, i.e. when the connection to the voice recorder has been established. Available with OpenStage V2R2.
	`call-record-audible-indication-continuous`	Boolean	`false`	
Audible Notification="Repeated"	`call-record-audible-indication`	Boolean	`true`	A short beep tone is played repeatedly through the handset, headset or loudspeaker when call recording starts, i.e. when the connection to the voice recorder has been established. Available with OpenStage V2R2.
	`call-record-audible-indication-continuous`	Boolean	`true`	

4.4.5.2 DSS Settings

> This function is not available with WPI.

4.4.5.3 Free Programmable Keys (FPK)

The function associated with a programmable feature key is represented by a feature id number. In the provisioning interface, this number is stored as content of the `function-key-def` element. The key number is stored in the `index` attribute, starting from 1 for the first key.

The possible key numbers depend on the OpenStage model:

- OpenStage 15: 1 to 8
- OpenStage 40: 1 to 6
- OpenStage 60: 1 to 8
- OpenStage 80: 1 to 9
- OpenScape Desk Phone IP 35: 1 to 3
- OpenScape Desk Phone IP 55G: 1 to 8

The shifted keys are indexed as follows:

- OpenStage 15: 1001 to 1008
- OpenStage 40: 1001 to 1006
- OpenStage 60: 1001 to 1008
- OpenStage 80: 1001 to 1009
- OpenScape Desk Phone IP 35: 1001 to 1003
- OpenScape Desk Phone IP 55G: 1001 to 1008

In the following example, the repeat dialling function is assigned to the first key:

```
<Item name="function-key-def" index="1">3</Item>
<Item name="key-label-unicode" index="1">Repeat Dialling</Item>
```

Selected dialing

A predefined call number is dialed on key press.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 12 characters.	Unicode text Default: `Call` `...`	Label for the key.
	`function-key-def <index>`	Integer	`1`	Feature ID which defines the function.
Dial number	`select-dial <index>`	Text	Default: NULL	Number to be dialed when pressing the key.

Repeat dialing

On key press, the call number that has been dialed lastly is dialed again.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text.	Maximum of 12 characters. Default: `Repeat dial`	Label for the key.
	`function-key-def <index>`	Integer	`3`	Feature ID which defines the function.

Forwarding

This is the phone's built-in forwarding function. An incoming call is forwarded to the predefined call number, depending on the forwarding type, that is, the current conditions at the phone.

> With firmware version V2, server-side forwarding can be assigned to the phone's fixed forwarding key; please refer to Section 4.4.5.4, "Fixed Keys".

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 24 characters.	`Forwarding`	Label for the key.
	`function-key-def <index>`	Integer	6	Feature ID which defines the function.
Forwarding type	`forwarding-type <index>`	Enumeration	0=Unconditional; 1=No reply; 2=Busy; 3=Immediate-External; 4=Immediate-Internal; 5=No reply-External; 6=No reply-Internal; 7=Busy-External; 8=Busy-Internal; Default: 0	Call forwarding type.
Destination	`forwarding-dest <index>`	Text	Default: NULL	Destination for call forwarding.

Mute (OpenStage 15 only)

On pressing this key, the microphone is turned off. This programmable key function is available only for OpenStage 15 phones, which have no fixed mute key.

WBM Name	Item name	Type	Values	Description
Key label <n>	key-label-unicode <index>	Unicode text. Max. 12 characters.	Default: `Mute`	Label for the key.
	function-key-def <index>	Integer	8	Feature ID which defines the function.

Release (OpenStage 15 only)

On pressing this key, the current call is disconnected. This programmable key function is available only for OpenStage 15 phones, which have no fixed release key.

WBM Name	Item name	Type	Values	Description
Key label <n>	key-label-unicode <index>	Unicode text. Max. 12 characters.	Default: `Cancel/ Release`	Label for the key.
	function-key-def <index>	Integer	8	Feature ID which defines the function.

Ringer off

Turns off the ringtone. Incoming calls are indicated via LEDs and display only.

WBM Name	Item name	Type	Values	Description
Key label <n>	key-label-unicode <index>	Unicode text. Max. 12 characters.	Default: `Ringer off`	Label for the key.
	function-key-def <index>	Integer	9	Feature ID which defines the function.

Hold

The call currently active is put on hold.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 12 charac- ters.	Default: `Hold`	Label for the key.
	`function-key-def <index>`	Integer	`10`	Feature ID which defines the function.

Alternate

Toggles between two calls; the previously active call is put on hold.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 12 charac- ters.	Default: `Alternate`	Label for the key.
	`function-key-def <index>`	Integer	`11`	Feature ID which defines the function.

Move blind / Blind transfer

A call is transferred without consultation, as soon as the phone goes on-hook or the target phone goes off-hook.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 12 characters.	Default: `Move blind`	Label for the key.
	`function-key-def <index>`	Integer	`12`	Feature ID which defines the function.

Transfer Call

Call transfer, applicable when there is one active call and one call on hold. The active call and the held call are connected to each other, while the phone that has initiated the transfer is disconnected.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Move Call`	Label for the key.
	`function-key-def <index>`	Integer	`13`	Feature ID which defines the function.

Deflect

On key press, an incoming call is deflected to the specified destination.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Deflect`	Label for the key.
	`function-key-def <index>`	Integer	14	Feature ID which defines the function.
Destination	`key-deflect-destination <index>`	Text	Default: NULL	Destination for call deflection.

Shift

Shift the level for the program keys. When activated, the functions assigned to the shift level are available on the program keys.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Shift`	Label for the key.
	`function-key-def <index>`	Integer	18	Feature ID which defines the function.

Conference

Establish a phone-based three-party conference from an active call; the behaviour is similar to the "Consult" key function. Available with firmware version V2R2.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 charac- ters.	Default: `Conference`	Label for the key.
	`function-key-def <index>`	Integer	`22`	Feature ID which defines the function.

Headset (OpenStage 40/60/80)

Accept an incoming call via headset.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 charac- ters.	Default: `Headset`	Label for the key.
	`function-key-def <index>`	Integer	`24`	Feature ID which defines the function.

Do Not Disturb

If this feature is activated, incoming calls will not be indicated to the user.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `DND`	Label for the key.
	`function-key-def <index>`	Integer	`25`	Feature ID which defines the function.

Callback

When the remote phone called is busy does not reply, the user can send a callback request to the server by pressing this key.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Callback`	Label for the key.
	`function-key-def <index>`	Integer	`48`	Feature ID which defines the function.

Cancel callbacks

With this this function, the user can cancel all callback requests on the server..

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 charac- ters.	Default: `Cancel cbks`	Label for the key.
	`function-key-def <index>`	Integer	`49`	Feature ID which defines the function.

Repertory dial

This feature is similar to the selected dialing function, but additionally, special calling functions are possible. The desired number and/or function is selected via the **Dial string** parameter. The following call functions are available:

- `$Q` Disconnect a call.
- `~` Start a consultation call. Example: `~3333$S`
- `$S` Start a call. Example: `3333$S`
- `–` Enter a pause, e. g. for exit code or international dialing. Example: `0-011511234567$S`

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 charac- ters.	Default: `Dial ...`	Label for the key.
	`function-key-def <index>`	Integer	`30`	Feature ID which defines the function.
Dial string	`repertory-dial <index>`	Unicode text	Maximum of 60 characters.	Call number and/or special strings for call control.

Line

When this function is assigned to a key, the phone will automatically activate the MAA (Multiple Address Appearance) feature. This feature, also commonly known as "Multiple Line Appearance", provides the user with multiple addresses, resp. lines, appearing on a single telephone. The user has the ability to originate, receive and otherwise control calls on each of these address appearances. The individual address appearances behave independently of each other.

A phone operating in MAA mode is also referred to as keyset. A keyset has one primary line and, typically, one or more secondary lines.

Unless the phones are connected to a specific PBX with appropriate protocol extensions, only private lines are possible. That is, a line can be registered and handled only by one single phone at a given time.

For further information, please refer to
http://wiki.unify.com/images/a/a3/White_Paper_MAA.pdf

The following parameters can be configured individually for each line handled by the phone

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: Line	Label for the line key.
	`function-key-def <index>`	Integer	`31`	Feature ID which defines the function.
Primary line	`line-primary <index>`	Boolean	`true`/`false` Default when this is the first line key that is configured: `true` Default when this is not the first line key that is configured: `false`	Determines whether this line is the primary line.

WBM Name	Item name	Type	Values	Description
Ring on/off	`line-ring` `<index>`	Boolean	`true`/`false` Default: `true`	When set to `true`, the line will ring on an incoming call, and a popup will appear on the display. When set to `false`, the incoming call will be indicated only by the key's LED. Also configurable by the user.
Ring delay (seconds)	`line-ring-delay` `<index>`	Integer	`0` to `65 535` (seconds) Default: `0`	Delay before the ring tone will start on an incoming call.
Selection order	`line-hunt-sequence` `<index>`	Integer	`1` to maximum number of lines for this phone.	When the user lifts the handset in order to initiate a call, the line to be used is determined by this value. If more than one lines have the same rank, the selection is made according to the key number.
Address	`line-sip-uri` `<index>`	Text	Default: NULL	Call number resp. SIP name corresponding to the entry in the SIP registrar (AoR) at which the line is to be registered.
Realm	`line-sip-realm` `<index>`	Text	Default: NULL	Used for authenticated access to the SIP server. Any combination of user id and password is meaningful only within the realm it is assigned to.

WBM Name	Item name	Type	Values	Description
User Identifier	`line-sip-user-id`	Text	Default: NULL	User id for authenticated access to the SIP server.
Password	`line-sip-pwd`	Text	Default: NULL	Password for authenticated access to the SIP server.
Shared type	`line-shared-type`	Enumeration	`0`=shared `1`=private	Determines whether the line is a shared line, i. e. shared with other phones, or a private line, i .e. available exclusively for this phone.
Hot warm action	`line-hot-line-warm-line`	Enumeration	`1`=No action ; `2`=hot line; `3`=warm line Default: `1`	As the hotline/warmline function is used in special scenarios only, it is generally recommended not to use this option in MAA environments.
Hot warm line dial string	`line-hld`	Text		As the hotline/warmline function is used in special scenarios only, it is generally recommended not to use this option in MAA environments.
Allow in overview	`line-hidden`	Boolean	`true`/`false` Default: `true`	Determines whether this line will be visible in line overview. When the value is `true`, the line will be visible in line overview; when it is `false`, it will not be visible. Also configurable by the user.

WBM Name	Item name	Type	Values	Description
Line overview position	`line-mlo-pos`	Text		
Inter-line notification allowed	`line-int-allow`	Boolean	`true`/`false` Default:	

Show phone screen (OpenStage 15 and OpenStage 40 only)

Switches back to call view.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Show Phone`	Label for the key.
	`function-key-def <index>`	Integer	`33`	Feature ID which defines the function.

Consultation

When the phone is an active call, this function opens a dialing menu to make a consultation call.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Consultation`	Label for the key.
	`function-key-def <index>`	Integer	`50`	Feature ID which defines the function.

Call waiting toggle

Enables or disables the Call waiting feature. If enabled, calls from a third party are allowed during an active call.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Call waiting`	Label for the key.
	`function-key-def <index>`	Integer	`53`	Feature ID which defines the function.

Immediate ring

Enables or disables the preset delay for all line keys. This feature only applies to keyset lines.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Show ringing`	Label for the key.
	`function-key-def <index>`	Integer	`54`	Feature ID which defines the function.

Line preview

Enables the preview mode, which allows the user to preview a line before using it. Relevant for OpenScape Voice only.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Temp.preview`	Label for the key.
	`function-key-def <index>`	Integer	`55`	Feature ID which defines the function.

Call recording

Enables or disables the preset delay for all line keys. This feature only applies to keyset lines.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Recording`	Label for the key.
	`function-key-def <index>`	Integer	`56`	Feature ID which defines the function.

AICS Zip tone

If activated, and a headset is plugged in, the phone will automatically accept incoming calls without ringing and without the necessity to press a key. Moreover, additional signalling information from OpenScape Voice is not required.

To indicate a new call to the user, a zip tone is played through the headset when the call is accepted.

Available for OpenStage 40/60/80.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `AICS`	Label for the key.
	`function-key-def <index>`	Integer	`57`	Feature ID which defines the function.

Server feature

Invokes a feature on the SIP server. The status of the feature can be monitored via the LED associated to the key.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Server feature`	Label for the key.
	`function-key-def <index>`	Integer	`54`	Feature ID which defines the function.
Feature code	`stimulus-feature-code<index>`	String	Default: NULL	This code will be sent in a SIP INVITE to the SIP server when the key is pressed. When a call is active during keypress, it is put on hold.

WBM Name	Item name	Type	Values	Description
DTMF digits	`stimulus-DTMF-sequence <index>`	String	Default: NULL	This code will be sent to the SIP server as a DTMF signal. As a precondition, an audio path which is routed via the SIP server must exist.
LED control	`stimulus-led-control-uri<index>`	String	Default: NULL	This SIP URI will receive the status notifications (SIP NOTIFY) from the SIP server. The LED is switched on or off accordingly.

BLF

Offers the possibility to monitor another phone, and to pick up calls for the monitored phone.

For the pickup function (OpenStage V2R1 onwards), the appropriate code must be provided (see `blf-code` in Section 4.4.5.8, "Addressing (V3) / Services (up to V2R2)").

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `BLF`	Label for the key.
	`function-key-def <index>`	Integer	`59`	Feature ID which defines the function.
Monitored phone	`stimulus-led-control-uri<index>`	Text	Default: NULL	Call number (SIP URI) of the monitored phone.
Audible alert	`blf-audible <index>`	Boolean	`true`/`false` Default: `false`	If enabled, an alert beep or ring tone will indicate an incoming call for the monitored phone. For determining whether a beep or the ring tone is used, `blf-tone-type` is used (see Section 4.4.5.1, "Configuration").
Popup on alert	`blf-popup <index>`	Boolean	`true`/`false` Default: `false`	If enabled, a popup window will indicate an incoming call for the monitored phone.

Start application

Starts an XML application.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max.12 characters.	Default: `Start application`	Label for the key.
	`function-key-def <index>`	Integer	`60`	Feature ID which defines the function.
Application name	`FPK-app-name <index>`	Text	Default: NULL	Name of the application to be started.

Send URL

With this function, the phone can send a specific HTTP or HTTPS request to a server. The function is available at any time, irrespective of registration and call state. Possible uses are HTTP-controlled features on the SIP server, e. g. hunt group login/logout, or functions on a web server that can only be triggered by HTTP/HTTPS request, e. g. login/logout for flexible working hours.

To define this function for a key, `function-key-def` must be set to `63`.

This function is available with firmware version V2.

With OpenStage V2R2, push support is available. If activated, the LED is controllable by a combination of an HTTP push request and an XML document. For further information, see the XML Applications Developer's Guide.

If you want to use the HTTP push solution, please ensure that no `stimulus-led-control-uri` item is sent. Otherwise, the phone will only use the SIP mechanism for LED control, and ignore the push request.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Text	Default: `Local application`	Label for the key.
	`function-key-def <index>`	Integer	`63`	Feature ID which defines the function.
Protocol	`send-url-protocol <index>`	Enumer-ation	`0`=TLSv1 (HTTPS); `3`=TCP (HTTP); Default: `3`	Defines whether HTTP or HTTPS is to be used for sending the URL to the server. For HTTPS, a certificate especially for the send URL function can be provided by the provisioning service; please refer to Section 6.13, "Certificates".
Web server address	`send-url-address <index>`	String	Default: NULL	IP address or DNS name of the remote server to which the URL is to be sent.
Port	`send-url-port <index>`	String	Default: NULL	Target port at the server to which the URL is to be sent.
Path	`send-url-path <index>`	String	Default: NULL	Server-side path to the desired function, i. e. the part of the URL that follows the IP address or DNS name.

WBM Name	Item name	Type	Values	Description
Parameters	`send-url-query <index>`	String	Default: NULL	One or more key/value pairs in the format `<key>=<value>` to be added to the request. If there are more than one parameters, they are separated by an ampersand (`&`). Please note that, for the WPI, the ampersand must be represented by `&`.
Method	`send-url-method <index>`	Enumeration	0=get; 1=post Default: `0`	HTTP method to be used. If GET is selected, the additional parameters and the user id/password are part of the URL. If POST is selected, these data form the body of the message.
Web server user ID	`send-url-user-id<index>`	String	Default: NULL	User ID to be sent to the web server, in case authentication is required.
Web server password	`send-url-passwd <index>`	String	Default: NULL	Password to be sent to the web server, in case authentication is required.
LED controller URI	`stimulus-led-control-uri <index>`	String	Default: NULL	This SIP URI will receive status notifications (SIP NOTIFY) from a SIP server. The LED is switched on or off accordingly.
Push support	`send-url-push-support <index>`	Boolean	`true`/`false` Default: `false`	If set to `true`, the LED is controllable by a combination of an HTTP push request and an XML document. For further information, see the XML Applications Developer's Guide. Available with OpenStage V2R2.

WBM Name	Item name	Type	Values	Description
Symbolic name	`send-url-symbolic-name <index>`	Text	Default: NULL	Used to assign a push request from the application server to the appropriate key. This value must be unique for all keys involved. Available with OpenStage V2R2.

Built-in forwarding

Toggles phone-based call forwarding.

> To enable phone-based call forwarding, the server-based-features item must be set to false; for further information, please see the parameter description in Section 4.4.5.1, "Configuration".

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 12 characters.	Default: `Call forward`	Label for the key.
	`function-key-def <index>`	Integer	`64`	Feature ID which defines the function. Available on all unshifted FPKs and the Fixed Forwarding Key. No parameters associated. This is the default function for the Fixed Forwarding Key, and when set on an FPK, allows it to act in the same way as the default Fixed Forwarding Key.

2nd alert (V3)

This function allows monitoring and accepting a second incoming call. When a call is ringing while the user is dialing, the LED will light up. As soon as the user presses the key, information about the incoming call is presented, and the user can accept the call. If a call is ringing, and another call starts ringing shortly after, the LED will light up, and the user has the possibility to toggle between these calls via key press.

WBM Name	Item name	Type	Values	Description
Key label \<n\>	`key-label-unicode <index>`	Unicode text. Max. 12 characters.	Default: `2nd alert`	Label for the key.
	`function-key-def <index>`	Integer	`69`	Feature ID which defines the function.

Personal Directory

This key function opens a menu which enables the user to start the local phonebook. (Prior Start Phonebook OpenStage 40 only)

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 12 characters.	Default: `Personal`	Label for the key.
	`function-key-def <index>`	Integer	`68`	Feature ID which defines the function.

Pause callbacks (V3)

This key function allows postponing all callbacks. To reactivte the callback key function 'Resume callbacks' is used, see Section 4.4.5.3, "Resume callbacks (V3)".

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 12 characters.	Default: `Pause cbks`	Label for the key.
	`function-key-def <index>`	Integer	`70`	Feature ID which defines the function.

Resume callbacks (V3)

This key function allows reactivating all callbacks. To postpone callbacks key function 'Pause callbacks' is used, see Section 4.4.5.3, "Pause callbacks (V3)".

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 12 characters.	Default: `Resume cbks`	Label for the key.
	`function-key-def <index>`	Integer	`71`	Feature ID which defines the function.

Video call (V3R3)

This key function allows activating video calls. Available only on OpenStage 60/80 and OpenScape DP IP 55G.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 12 characters.	Default: `Enable video`	Label for the key.
	`function-key-def <index>`	Integer	`72`	Feature ID which defines the function.

Corporate Directory (V3R3)

This key function allows activating corporate directory.

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 12 characters.	Default: `Corpo-rate`	Label for the key.
	`function-key-def <index>`	Integer	`72`	Feature ID which defines the function.

Unallocated (no feature assigned)

No function is associated with this key. (Prior named Clear)

WBM Name	Item name	Type	Values	Description
Key label <n>	`key-label-unicode <index>`	Unicode text. Max. 12 characters.	Default: NULL	Label for the key.
	`function-key-def <index>`	Integer	`0`	Feature ID which defines the function.

4.4.5.4 Fixed Keys

With software versionOpenStage V2, the fixed function keys (release, forwarding ⊡, voice dial , repeat dial) can be modified. The underlying functionality and parameters are the same as those used in the server feature function for the program keys (see Section 4.4.5.3, "Server feature").

Forwarding Key

Depending on the firmware version installed on the phone, various functions can be assigned to the fixed forwarding key.

The server feature function can be assigned to the forwarding key ⊡; for the function specific parameters, please see Section 4.4.5.3, "Server feature". If the server feature function is assigned to the key, `key-functionality` determines the key's behaviour. Unless this parameter is set to "unspecified", built-in forwarding will be disabled.

• Built-in forwarding

WBM Name	Item name	Type	Value	Description
Built-in forwarding	`function-key-def index="4002"`	Integer	`64`	Feature ID which defines the function. Available with OpenStage V2R0 onwards.

- Key functionality

WBM Name	Item name	Type	Values	Description
Key functionality	`key-functionality index="4002"`	Enumeration	0="Toggle Call Forwarding"; 1="Unspecified Call Forwarding"; 2="Unspecified" Default: 0	Valid if the server feature or send URL function is assigned to the key. Controls the behaviour of the forwarding key. "Toggle call forwarding": On pressing the key, the user will be presented with a prompt. When accepted, the configured feature code or DTMF sequence will be sent to the external server. The forwarding icon in the call view screen and the LED will be controlled by the SIP server. "Unspecified call forwarding": No prompt will be presented to the user. The configured feature code or DTMF sequence will be sent to the external server immediately. "Unspecified": No prompt will be presented to the user. The configured feature code or DTMF sequence will be sent to the external server immediately. The phone's built-in forwarding is not disabled. Available with OpenStage V2R0 onwards.

For the function specific parameters, please refer to Section 4.4.5.3, "Server feature".

- Server feature

WBM Name	Item name	Type	Values	Description
Server feature	`function-key-def index="4002"`	Integer	`58`	Feature ID which defines the function. Available with OpenStage V2R0 onwards.

If this function is assigned to the key, `key-functionality` determines the key's behaviour; please refer to Section 4.4.5.4, "Key functionality". For the function specific parameters, please refer to Section 4.4.5.3, "Server feature".

- Send URL

WBM Name	Item name	Type	Values	Description
Send URL	`function-key-def index="4002"`	Integer	`63`	Feature ID which defines the function. Available with OpenStage V2R1 onwards.

If this function is assigned to the key, `key-functionality` determines the key's behaviour; please refer to Section 4.4.5.4, "Key functionality". For the function specific parameters, please refer to Section 4.4.5.3, "Send URL".

- Start XML application

WBM Name	Item name	Type	Values	Description
Start XML application / Start app	`function-key-def index="4002"`	Integer	`60`	Feature ID which defines the function. Available with OpenStage V2R1 onwards.

For the function specific parameters, please refer to Section 4.4.5.3, "Start application".

- Show phone screen

WBM Name	Item name	Type	Values	Description
Show phone screen	`function-key-def index="4002"`	Integer	`33`	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Show phone screen (OpenStage 15 and OpenStage 40 only)".

- Hold

WBM Name	Item name	Type	Values	Description
Hold	`function-key-def index="4002"`	Integer	`10`	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Hold".

- Consultation

WBM Name	Item name	Type	Values	Description
Consultation	`function-key-def index="4002"`	Integer	`50`	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Consultation".

- Conference

WBM Name	Item name	Type	Values	Description
Conference	`function-key-def index="4002"`	Integer	`22`	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For the function specific parameters, please refer to Section 4.4.5.3, "Conference".

- Repertory dial

WBM Name	Item name	Type	Values	Description
Repertory dial	`function-key-def index="4002"`	Integer	`30`	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Repertory dial".

Release Key

- Built-in release

WBM Name	Item name	Type	Values	Description
Built-in release	`function-key-def index="4001"`	Integer	`65`	Feature ID which defines the function. Available with OpenStage V2R0 onwards.

- Server feature

WBM Name	Item name	Type	Values	Description
Server feature	`function-key-def index="4001"`	Integer	`58`	Feature ID which defines the function. Available with OpenStage V2R0 onwards.

- Send URL

WBM Name	Item name	Type	Values	Description
Send URL	`function-key-def index="4001"`	Integer	`63`	Feature ID which defines the function. Available with OpenStage V2R1 onwards.

For the function specific parameters, please refer to Section 4.4.5.3, "Send URL".

- Start XML application

WBM Name	Item name	Type	Values	Description
Start XML application / Start app	`function-key-def index="4001"`	Integer	`60`	Feature ID which defines the function. Available with OpenStage V2R1 onwards.

For the function specific parameters, please refer to Section 4.4.5.3, "Start application".

- **Show phone screen**

WBM Name	Item name	Type	Values	Description
Show phone screen	`function-key-def index="4001"`	Integer	33	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Show phone screen (OpenStage 15 and OpenStage 40 only)".

- **Consultation**

WBM Name	Item name	Type	Values	Description
Consultation	`function-key-def index="4001"`	Integer	50	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Consultation".

- **Conference**

WBM Name	Item name	Type	Values	Description
Conference	`function-key-def index="4001"`	Integer	22	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For the function specific parameters, please refer to Section 4.4.5.3, "Conference".

- **Repertory dial**

WBM Name	Item name	Type	Values	Description
Repertory dial	`function-key-def index="4001"`	Integer	30	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Repertory dial".

Voice Dial / Voice Recognition Key (OpenStage 60/80)

- Server feature

WBM Name	Item name	Type	Values	Description
Server feature	`function-key-def index="4003"`	Integer	`58`	Feature ID which defines the function. Available with OpenStage V2R0 onwards.

- Send URL

WBM Name	Item name	Type	Values	Description
Send URL	`function-key-def index="4003"`	Integer	`63`	Feature ID which defines the function. Available with OpenStage V2R1 onwards.

For the function specific parameters, please refer to Section 4.4.5.3, "Send URL".

- Start XML application

WBM Name	Item name	Type	Values	Description
Start XML application / Start app	`function-key-def index="4003"`	Integer	`60`	Feature ID which defines the function. Available with OpenStage V2R1 onwards.

For the function specific parameters, please refer to Section 4.4.5.3, "Start application".

- Hold

WBM Name	Item name	Type	Values	Description
Hold	`function-key-def index="4003"`	Integer	`10`	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Hold".

- Consultation

WBM Name	Item name	Type	Values	Description
Consultation	`function-key-def index="4003"`	Integer	50	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Consultation".

- Conference

WBM Name	Item name	Type	Values	Description
Conference	`function-key-def index="4003"`	Integer	22	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For the function specific parameters, please refer to Section 4.4.5.3, "Conference".

- Repertory dial

WBM Name	Item name	Type	Values	Description
Repertory dial	`function-key-def index="4003"`	Integer	30	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Repertory dial".

Redial Key (OpenStage 20/40)

- Built-in redial

WBM Name	Item name	Type	Values	Description
Built-in redial	`function-key-def index="4009"`	Integer	`67`	Feature ID which defines the function. Available with OpenStage V2R0 onwards.

- Server feature

WBM Name	Item name	Type	Values	Description
Server feature	`function-key-def index="4009"`	Integer	`58`	Feature ID which defines the function. Available with OpenStage V2R0 onwards.

- Send URL

WBM Name	Item name	Type	Values	Description
Send URL	`function-key-def index="4009"`	Integer	`63`	Feature ID which defines the function. Available with OpenStage V2R1 onwards.

For the function specific parameters, please refer to Section 4.4.5.3, "Send URL".

- Show phone screen

WBM Name	Item name	Type	Values	Description
Show phone screen	`function-key-def index="4009"`	Integer	`33`	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Show phone screen (OpenStage 15 and OpenStage 40 only)".

- Consult and transfer

WBM Name	Item name	Type	Values	Description
Consult and transfer	`function-key-def index="4009"`	Integer	50	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Consultation".

- Conference

WBM Name	Item name	Type	Values	Description
Conference	`function-key-def index="4009"`	Integer	22	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For the function specific parameters, please refer to Section 4.4.5.3, "Conference".

- Repertory dial

WBM Name	Item name	Type	Values	Description
Repertory dial	`function-key-def index="4009"`	Integer	30	Feature ID which defines the function. Available with OpenStage V2R2 onwards.

For a description, please refer to Section 4.4.5.3, "Repertory dial".

Forwarding Key (OpenScape Desk Phone IP 55G)

• Forwarding

WBM Name	Item name	Type	Values	Description
Forwarding	`function-key-def index="4010"`	Integer	`10`	Feature ID which defines the function.

4.4.5.5 Key Module 1

The settings are the same as those for programmable keys on the phone (see Section 4.4.5.3, "Free Programmable Keys (FPK)").

4.4.5.6 Key Module 2

The settings are the same as those for programmable keys on the phone (see Section 4.4.5.3, "Free Programmable Keys (FPK)").

4.4.5.7 Keyset operation

WBM Name	Item name	Type	Values	Description
Rollover ring	`line-rollover-type`	Enumer-ation	`0`=no ring; `1`=alert ring; `2`=standard ring; `3`=alert beep Default: `3`	Determines how an incoming call on a different line is indicated during an active call. When "no ring" is selected, the incoming call will not ring; "alert ring" selects a 3 seconds burst of the configured ring tone; "alert beep" selects a beep instead of a ring tone; "Standard ring tone" selects the default ringer.
LED on registration	`line-registration-leds`	Boolean	`true`/`false` Default: `true`	Determines whether the line LEDs will be lit for a few seconds if they have been registered successfully with the SIP server on phone startup.
Originating line preference	`originating-line-preference`	Enumer-ation	`0`=idle line; `1`=primary; `2`=last `3`=none Default: `0`	Determines which line will be used when the user goes off-hook or starts on-hook dialing. When "idle" is selected, the line selection is based on the rank specified for each line; with "primary", the primary line is selected; with "last", the line that has been used last is selected, and with "none", the user must select a line manually.

WBM Name	Item name	Type	Values	Description
Terminating line preference	`terminating-line-preference`	Enumeration	0="ringing line" 1="ringing PLP" 2="incoming" 3="incoming PLP" 4="none" Default: 0	Decides which terminating line, i. e. line with an incoming call, is selected when the user goes off-hook. When "ringing line" is selected, the line in ringing state is automatically selected when the user goes off-hook. If multiple lines are ringing, the line that has been alerting the longest is selected. With "ringing PLP", the line in ringing state is automatically selected when the user goes off-hook. If the prime line is alerting, it is given priority. With "incoming", the earliest line to start ringing is selected, or else the earliest alerting line is selected. With "incoming PLP", the earliest line to start ringing is selected, or else the earliest alerting line is selected. However, if the prime line is alerting, it is given priority. With "none", the user manually selects a line by pressing its line key before going off-hook to answer a call.

WBM Name	Item name	Type	Values	Description
Line action mode	`line-key-operating-mode`	Enumeration	0="hold" 1="release" Default: 0	Determines the consequence for an established connection when the line key is pressed. If "hold" is selected, the call currently active is set to hold as soon as the line key is activated. If "release" is selected, the previously established call is ended.
Show focus	`keyset-use-focus`	Boolean	`true`/`false` Default: `true`	If `true`, the LED of a line key flutters when the line is in use. If `false`, the line key is lit steady when it is in use.
Reservation timer (seconds)	`keyset-reservation-timer`	Integer	Default: `60`	Sets the period after which the reservation of a line is canceled. A line is automatically reserved for the keyset whenever the user has selected a line for an outgoing call and hears a dial tone. If set to `0`, the reservation timer is deactivated.
Forwarding indicated	`keyset-remote-forward-ind`	Boolean	`true`/`false` Default: `false`	Only relevant when the phone is connected to a specific PBX.

WBM Name	Item name	Type	Values	Description
Preselect mode	`line-button-mode`	Enumeration	0=single button 1=preselection Default: 0	Determines the phone's behaviour when a call is active, and another call is ringing. If set to "single button", the user can accept the call a single press on the line key. If set to "preselection", the user must first press the line key to select it and then press it a second time to accept the call.
Preselect timer	`line-preselection-timer`	Integer	`0 to 60`	Relevant if `line-button-mode` is set to `1`. The parameter sets the timeout in seconds for the second key press that is required to accept the call. After the timeout has expired, the call is no longer available.
Preview mode	`preview-mode-locked`	Boolean	`true/false`	Relevant for OpenScape Voice only. When set to false, preview mode will end when the user uses the previewed line, or a new call is started in any other way, or if the focus is changed away from call view. When set to true, preview mode remains active until the user cancels it by pressing the key again.

WBM Name	Item name	Type	Values	Description
Preview timer	`preview-timer`	Integer	2/ 3/ 4/ 6/ 8/ 10/ 15/ 20/ 30/ 40/ 50/ 60 Default: 8	Relevant for OpenScape Voice only. Determines the timespan in seconds during which the line preview will remain on the screen.
Bridging priority	`bridging-over-rides-preview`	Enumeration	0=Preview overrides bridging 1=Bridging overrides preview Default: 0	The Bridging priority parameter affects the behavior of the line key, when Bridging is enabled

4.4.5.8 Addressing (V3) / Services (up to V2R2)

WBM Name	Item name	Type	Values	Description
MW server URI	`mwi-e164`	IP address, hostname or NULL.	Max. 24 characters. IP address, hostname or NULL. Non-NULL=explicit subscription to service; NULL = implicit subscription. Default: NULL	Address or host name of the server that sends message waiting notifications to the phone.
Conference	`conference-factory-uri`	Text	Default: NULL	Call number/URI used for system based conference.
Group pickup URI	`pickup-group-uri`	Text	Default: NULL	URI of the Call Pickup group service provided by the server.To be a member of a Call Pickup group, the phone must be configured with the corresponding URI.

WBM Name	Item name	Type	Values	Description
Callback: FAC (V3) / Code for callback busy (up to V2R2)	`callback-busy-code`	Text	Default: NULL	Access code that is sent to the server if the line is busy.
Callback cancel all (V3) / Code for callback cancel all	`callback-cancel-code`	Text	Default: NULL	Access code for cancel-ing all callback requests on the server.
BLF pickup code	`blf-code`	Text	Default: NULL	Code sent to the SIP server for BLF call pickup. Available with OpenStage V2R1 onwards.

4.4.5.9 Call completion (V3)

WBM Name	Item name	Type	Values	Description
Functional CCSS	`ccss-enabled`	Boolean	`true/false` Default: `false`	When activated, the func-tional callback mecha-nism will be used instead of FAC (Feature Access Code).
Callback ringer	`ccss-ringer`	Text	0=alert-internal 1=alert-external Default: 0	Selects a distinctive ringer (see Section 4.11, "Ringer Setting") to be used with the callback prompt to announce the availability of a call back call to a target.

WBM Name	Item name	Type	Values	Description
Allow after call (seconds)	`ccss-retain-time`	Enumer- ation	0=1; 1=2; 2=3; 3=4; 4=5; 5=10; 6=15; 7=20; 8=30; 9=40; 10=50; 11=60; 12=90; 13=120; 14=Unlimited Default: `8`	Specifies how long (in seconds) to retain server provided information required to request a call back after the call has disconnected.
Max. callbacks	`ccss-max`	Enumer- ation	0=1; 1=2; 2=3; 3=4; 4=5; 5=6; 6=7; 7=8; 8=9; 9=10 Default: `4`	Specifies how many callback requests are allowed to be pending at the same time.

4.4.5.10   Feature access (V3 and onwards)

WBM Name	Item name	Type	Values	Description
Blind transfer	`feature-availability <index=27>`	Boolean	`true/false` Default: `true`	Enables or disables blind transfer / transfer on ring.
3rd call leg	`feature-availability <index=34>`	Boolean	`true/false` Default: `true`	Enables or disables the possibility to handle a third call.

WBM Name	Item name	Type	Values	Description
Callback	`callback-busy-allow`	Boolean	`true/false` Default: `true`	Enables or disables the possibility to request a callback.
Call pickup	`feature-availability <index=23>`	Boolean	`true/false` Default: `true`	Enables or disables the possibility to pick up a call.
Group pickup	`feature-availability <index=35>`	Boolean	`true/false` Default: `true`	Enables or disables the possibility to pick up a group call.
Call deflection	`feature-availability <index=1>`	Boolean	`true/false` Default: `true`	Enables or disables the possibility to deflect a call.
Call forwarding	`feature-availability <index=2>`	Boolean	`true/false` Default: `true`	Enables or disables the possibility to control call forwarding.
Do not disturb	`feature-availability <index=11>`	Boolean	`true/false` Default: `true`	Enables or disables the possibilty to control the "do not disturb" feature.
Refuse call	`refuse-call`	Boolean	`true/false` Default: `true`	Enables or disables the possibilty to refuse a call.
Repertory dial key	`feature-availability <index=28>`	Boolean	`true/false` Default: `true`	Enables or disables the possibilty to program a repertory dial key.
Ext/Int forwarding	`cf-int-ext-ui-allowed`	Boolean	`true/false` Default: `true`	Enables or disables the possibilty to use call forwarding by call type.
Phone book lookups	`pb-lookups-allowed`	Boolean	`true/false` Default: `true`	Enables or disables the possibilty to look up numbers in the phonebook.
DSS feature	`feature-availability <index=30>`	Boolean	`true/false` Default: `true`	Enables or disables the possibilty to program a DSS key.
BLF feature	`feature-availability <index=29>`	Boolean	`true/false` Default: `true`	Enables or disables the possibilty to program a BLF key.
Line overview	`feature-availability <index=33>`	Boolean	`true/false` Default: `true`	Enables or disables the possibilty to use the line overview.

WBM Name	Item name	Type	Values	Description

Video calls	`video-allowed`	Boolean	`true/false`
			Default:
			`false`
				When set to `true`, video call is allowed.Available with V3R3 onwards.

CTI control	`feature-availability <index=32>`	Boolean	`true/false` Default: `true`	Enables or disables CTI (Computer Telephony Interface).
Bluetooth	`enable-bluetooth-interface`	Boolean	`true/false` Default: `true`	Enables or disables Bluetooth. Available for OpenStage 60/80.
Web based mang.	`enable-WBM`	Boolean	`true/false` Default: `true`	Enables or disables the WBM (Web Based Management).
USB device access	`usb-access-enabled`	Boolean	`true/false` Default: `true`	Enables or disables the possibility to connect to a USB device. Available for OpenStage 60/80.
Backup to USB	`usb-backup-enabled`	Boolean	`true/false` Default: `true`	Enables or disables the possibility to backup phone data via USB storage device. Available for OpenStage 60/80.
Feature toggle	`feature-availability <index=31>`	Boolean	`true/false` Default: `true`	Enables or disables the possibility to use the "feature toggle" function, that is, signal Busy status in a hunt group.
Phone lock	`feature-availability <index=36>`	Boolean	`true/false` Default: `true`	Enables or disables the possibility to lock the phone.

4.4.6 Security

	With firmware version V3, the parameters listed underneath have been moved to sub-menus.

4.4.6.1 System (V2)

WBM Name	Item name	Type	Values	Description
SIP server certificate validation	`voip-server-validation`	Boolean	`true`/`false` Default: `false`	If enabled, the phone will validate the server certificate sent by the SIP server in order to establish a TLS connection.
Backup SIP server certificate validation	`voip-backup-server-validation`	Boolean	`true`/`false` Default: `false`	If enabled, the phone will validate the backup server certificate sent by the SIP server in order to establish a TLS connection.
Use secure calls	`voip-payload-security-allowed`	Boolean	`true`/`false` Default: `false`	If activated, the encryption of outgoing calls is enabled, and the phone is capable of receiving encrypted calls.

With software version OpenStage V2R2 onwards, the authentication policy for file transfer (see Section 4.5, "File Transfer") via HTTPS and for the "Send URL" function (see Section 4.4.5.3, "Send URL") can be configured. When "None" is selected, no certificate check is performed. With "Trusted", the certificate is only checked against the signature credentials provided by the remote server, and the expiry date is checked. When "Full" is selected, the certificate is fully checked against the credentials provided by the remote server for signature, the fields must match the requested subject/usage, and the expiry date is checked.

Apart from the provisioning service, this can only be done via the local phone menu: Admin > Security & policies > Certificates > Authentication policy.

Local menu name	Item name	Type	Values	Description
Secure file transfer	`https-ftp-authentication-policy`	Enumeration	0=None; 1=Trusted; 2=Full	Sets the authentication level for the HTTPS server to be used for file transfer. Available with OpenStage V2R2.
Secure send URL	`send-url-authentication-policy`	Enumeration	0=None; 1=Trusted; 2=Full	Sets the authentication level for the HTTPS server to be used for the "Send URL" function.

4.4.6.2 System (V3)

WBM Name	Item name	Type	Values	Description
SIP server certificate validation	See Section 4.4.6, "Security".			
Use secure calls	See Section 4.4.6, "Security"			
SRTP type	`srtp-key-negotiation-method`	Enumeration	0=MIKEY; 1=SDES	Sets the key exchange method for SRTP.
Use SRTCP	`srtcp-encryption-enabled`	Boolean	`true`/`false`	When activated (together with `voip-payload-security-allowed`), the phone will use SRTCP (Secure RTCP) to transmit and receive RTP control packets.

4.4.6.3 SDES Config (V3)

> ⓘ Some configurations described in the following table require specific combinations of configuration items, indices, and values. In cases where one configuration can easily be derived from a similar configuration, like "SHA1-32 disabled, SHA1-80 enabled" vs. "SHA1-80 disabled, SHA1-32 enabled", only one possible configuration is described.

WBM Name	Item name	Type	Values	Description
SDES status	`srtp-key-negotiation-method`	Enumeration	`0`=Disabled; `1`=Enabled	Described in Section 4.4.6.2, "System (V3)".
SDP negotiation	`secure-call-payload-options`	Enumeration	`0`="SRTP + RTP"; `1`="SRTP only"; `2`="RTP + SRTP" Default: `0`	Specifies whether the use of SRTP will be forced by the phone. When "RTP + SRTP" is selected, both secure and non-secure media connections are offered. With "SRTP only", only a secure media connection is allowed; if the remote party should not support SRTP, no connection will be established. With "SRTP + RTP", the phone will try to establish a SRTP connection, but fall back to RTP if this should fail.

WBM Name	Item name	Type	Values	Description
SHA1-80 ranking = disabled; SHA1-32 ranking = enabled	`srtp-encryption-allowed <index=1>`	Boolean	`true`	SHA1-32 is enabled for SRTP encryption.
	`srtp-encryption-allowed <index=2>`	Boolean	`false`	SHA1-80 is disabled for SRTP encryption.
	`srtp-encryption-method <index=1>`	Enumer-ation	`0`	The value `0` denotes SHA1-32. This effects that the `srtp-encryption-allowed` item with `index=1` refers to SHA1-32.
	`srtp-encryption-method <index=2>`	Enumer-ation	`1`	The value `1` denotes SHA1-80. This effects that the `srtp-encryption-allowed` item with `index=2` refers to SHA1-80.
SHA1-80 ranking = 1; SHA1-32 ranking = 2;	`srtp-encryption-rank <index=1>`	Enumer-ation	`2`	SHA1-32 ranking is set to 2.
	`srtp-encryption-rank <index=2>`	Enumer-ation	`1`	SHA1-80 ranking is set to 2.
	`srtp-encryption-method <index=1>`	Enumer-ation	`0`	The value `0` denotes SHA1-32. This effects that the `srtp-encryption-allowed` item with `index=1` refers to SHA1-32.
	`srtp-encryption-method <index=2>`	Enumer-ation	`1`	The value `1` denotes SHA1-80. This effects that the `srtp-encryption-allowed` item with `index=2` refers to SHA1-80.

4.4.6.4   Access Control (V3)

WBM Name	Item name	Type	Values	Description
CCE access	`cce-enabled`	Enumeration	`0`=Disable; `3`=Enable;	Controls TCP and UDP access for the CCE (CommsChannel Extender). This affects the operation of the OpenStage Manager, local CTI access, and HPT access. When "Disable all" is selected, both TCP and UDP are disabled. With "Enable all", there are no restrictions.
Factory reset claw	`factory-reset-hooded-claw-enabled`	Boolean	`true`/`false`	Enables or disables the 'hooded claw' keypad mechanism to initiate a factory reset without requiring an authenticated access.
Allow user access to diagnostic data	`allow-user-access-to-diagnostic-data`	Boolean	`true`/`false` Default:`true`	Enables or disables the user access to diagnostic data

WBM Name	Item name	Type	Values	Description
Serial port	`serial-port-mode`	Enumer-ation	`0`=Password re-quired; `1`=No Password; `2`=Unavailable Default: 1	When "Passwd required" (=interactive_login) is se-lected, the serial port re-quires a password for ac-cess (root user is not available).When set to "No password" (=interactive_no_login), a terminal connected to the serial port can interact with the phone's operat-ing system without re-strictions. When "Unavail-able" (=non_interactive) is chosen, the serial port is not accessible."Config-ures the access available via the serial port.

4.4.6.5 Logging (V3)

WBM Name	Item name	Type	Values	Description
Max. lines	`slog-max-lines`	Numeric	`100` to `1000` Default: `500`	Defines the maximum number of entry lines that can be kept in the security log before old entries are overwritten.
Archive to DLS	`slog-archive-to-DLS`	Boolean	`true`/`false`	When set to `true`, the DLS is used to automati-cally archive the security log so that no log entries will be lost.

WBM Name	Item name	Type	Values	Description
Archive when at	`slog-archive-on-percentage`	Enumeration	0=send immediate 1=10%; 2=20%; 3=30%; 4=35%; 5=40%; 6=45%; 7=50%; 8=55%; 9=60%; 10=65%; 11=70%; 12=80%; 13=90% Default: 7	Automatic archiving of new security log entries will occur when the percentage of unarchived entries in the log is as specified or more. When set to 0%, every new entry will trigger a save.
Last archived	`slog-date-last-archived`	Alphanumeric	Date	Date when the security log was last archived to the DLS.

4.4.6.6   Faults (V3)

> (i)   This function is not available with WPI.

4.5 File Transfer

Due to the organization of the file transfer parameters in the provisioning interface, the presentation will differ from the other sections. However, the WBM names which correspond to the parameters will be retained in order to make them more findable.

For in-deep information, see Section 3.6.7, "File Provisioning". Note that multiple file deployment is possible using the index attribute (see Section 3.6.7.3, "XML Data Exchange For Multiple File Deployment").

4.5.1 FTP/HTTPS Access Data

WBM Name	Item name	Type	Values	Description
Download method	Not applicable			The method is determined by the presence or absence of `file-server` and `file-https-base-url`.
FTP Server address	`file-server <index>`	IP address or hostname	IP address or hostname Default: NULL	IP address or hostname of the FTP/HTTPS server to be used.
FTP Server port	`file-port <index>`	Integer	Port number Default: `21`	Port number of the server to be used.
FTP account	`file-account <index>`	Text	Max. 92 characters. Default: NULL	Account at the server to be used (if applicable).
FTP username	`file-username <index>`	Text	Max. 93 characters. Default: NULL	User name for accessing the server.
FTP password	`file-pwd <index>`	Text.	Max. 24 characters. Default: NULL	Password corresponding to the user name.
FTP path	`file-path <index>`	Text	Default: NULL	Path of the directory containing the files.
HTTPS base URL	`file-https-base-url <index>`	Text	Max. 255 characters. Default: NULL	IP address or hostname of the HTTPS server in use.

WBM Name	Item name	Type	Values	Description
Filename	`file-name`	Text	Default: NULL	Name of the file to be deployed.

4.5.2 File Provisioning Data

Item name	Type	Values	Description
`file-type` `<index>`	Text	See Section 4.5.3, "Specifications For Media Files and LDAP Templates".	Type of file to be downloaded by the phone.
`file-action` `<index>`	Text	`deploy`/`delete` Default: NULL	If set to `deploy`, the phone will download the file. If set to delete, the specified file will be `deleted`. Used for multiple file deployment.
`file-priority`	Text	`normal`/ `immediate` Default: `immediate`	Priority for the software (phone firmware) deployment. When set to `immediate`, the current status will be disregarded, and the software will be deployed unconditionally. When set to `normal`, software deployment will only be executed when the phone is in idle state.

4.5.3 Specifications For Media Files and LDAP Templates

For non-software files, the file types are specified as content of the `file-type` tag.

Example: `<Item name="file-type">LOGO</Item>`

The file types are listed here:

WBM Name	`file-type`	Type/Extension	Description
Hold music	MOH	WAV/.wav MIDI/.mid MP3/.mp3 (OpenStage 60/80 only)	This sound file is played when a call is put on hold. Recommended WAV specifications: PCM; bit rate: 16 kB/sec; sampling rate: 8 kHz; quantization: 16 bit. Recommended MP3 bit rate: 48 kbit/sec.
Picture Clip	PIC	JPEG/.jpg PNG/.png	Small images used for displaying a picture of a person that is calling on a line. The file size is limited to 300 kB. OpenStage 60/80 only.
LDAP	LDAP	TXT/.txt	Allocation list to assign directory server attributes to input and output fields on an LDAP client.
Logo	LOGO	JPEG/.jpg (OpenStage 60/80) PNG/.png (OpenStage 60/80) BMP/.bmp (black/white, for OpenStage 40)	Custom background image for the telephony interface. Ideal size for OpenStage 40: width: 144px; height: 32 px. Ideal size for OpenStage 60: width: 240 px; height: 70 px. Ideal size for OpenStage 80: width: 480 px; height: 148 px. OpenStage 40/60/80 only.

WBM Name	`file-type`	Type/Extension	Description
Screensaver	`SCREENSAVER`	JPEG/.jpg PNG/.png	Images for a slideshow which is displayed when the phone is in idle mode. Ideal resolution for Open-Stage 60: 320x640 Ideal resolution for Open-Stage 80: 640x480 OpenStage 60/80 only.
Ringer file	`RINGTONE`	WAV/.wav MIDI/.mid MP3/.mp3 (OpenStage 60/80/DPIP55G only)	Custom Ringtones. The file size for a ringer file is limited to 1 MB. Recommended WAV specifications: PCM; bit rate: 16kB/sec; sampling rate: 8 kHz; quantization: 16 bit. Recommended MP3 bit specifications: bit rate: 48 to 112 kbit/sec; length: up to 1 min; mono.
Dongle key	`HPT DONGLE FILE`		The HPT dongle key is a special file that contains a secret hash number which is required to connect the HPT tool to the phone. This testing tool is used exclusively by the service staff.

4.6   Local functions

4.6.1   Directory settings

	These settings are relevant for OpenStage 15/20/40/60/80 and OpenScape Desk Phone IP 35/55G.

WBM Name	Item name	Type	Values	Description
LDAP Server address	`ldap-server-address`	IP address or hostname. Max. 64 characters.	Default: NULL	IP address or hostname of the LDAP server.
LDAP Server port	`ldap-server-port`	Integer	Port number. Default: `389`	Port on which the LDAP server is listening for requests. If ldap-transport-type is TLS than use the secure LDAP port (ldap-encrypted-port), otherwise use LDAP Server Port (ldap-server-port).
LDAP encrypted port	`ldap-encrypted-port`	Integer	Port number. Default: `636`	Port on which the LDAP server is listening for requests. If ldap-transport-type is TLS than use the secure LDAP port (ldap-encrypted-port), otherwise use LDAP Server Port (ldap-server-port).
Authentication	`ldap-authentication`	Enumeration	`0`=Anonymous; `1`=Simple; Default: `0`	Authentication method used for connecting to the LDAP server.

WBM Name	Item name	Type	Values	Description
User name	`ldap-user`	Text	Default: NULL	User name for authentication with the LDAP server in the LDAP bind request.
Password	`ldap-pwd`	Text	Default: NULL	Password used for authentication with the LDAP server.
Search trigger timeout	`ldap-search-trigger-timeout`	Enumeration	1/2/3/4/5/6/7/8/9/10/60 (seconds)	The search string is submitted to the LDAP server as soon as the OK key is pressed, or when the Search trigger timeout expires. Available with firmware version V2.

4.6.2   Messages settings

The indication of old and new messages on the display can be configured. There are 4 categories of voicemail messages: new, new urgent, old, and old urgent. For each category, the message count can be shown or hidden, and a label for the category can be defined.

If a label item is empty, the phone will show the default label.

> These settings are available with firmware version V2.

WBM Name	Item name	Type	Values	Description
New items				Not applicable
Alternative label	`MWI-new-label`	Text Max.17 characters	Default: NULL	Label for new items.
New urgent items	`MWI-new-urgent-show`	Boolean	`true`/`false` Default: `true`	Determines whether new urgent items are indicated.

WBM Name	Item name	Type	Values	Description
Alternative label	`MWI-new-urgent-label`	Text Max. 17 characters	Default: NULL	Label for new urgent items.
Old items	`MWI-old-show`	Boolean	`true`/`false` Default: `true`	Determines whether old items are indicated.
Alternative label	`MWI-old-label`	Text Max.17 characters	Default: NULL	Label for old items.
Old urgent items	`MWI-old-urgent-show`	Boolean	`true`/`false` Default: `true`	Determines whether old urgent items are indicated.
Alternative label	`MWI-old-urgent-label`	Text Max. 17 characters	Default: NULLs	Label for old urgent items.

4.6.3 Locality

4.6.3.1 Canonical dial settings

WBM Name	Item name	Type	Values	Description
Local country code	`Canonical-dialing-local-country-code`	Text	Default: NULL	E.164 Country code, e.g. "49" for Germany, "44" for United Kingdom.
National prefix digit	`Canonical-dialing-national-prefix`	Text	Default: NULL	Prefix for national connections, e.g. "0" in Germany and United Kingdom.
Local national code	`Canonical-dialing-local-area-code`	Text	Default: NULL	Local area code or city code, e.g. "89" for Munich, "20" for London

WBM Name	Item name	Type	Values	Description
Minimum local number length	`Canonical-dialing-min-local-number-length`	Text	Default: NULL	Minimum number of digits in a local PSTN number.
Local enterprise node	`Canonical-dialing-local-node`	Text	Default: NULL	Number of the company/ PBX wherein the phone is residing.
PSTN access code	`Canonical-dialing-external-access`	Text; comma separated if multiple values. Max. 50 characters	Default: NULL	Access code used for dialing out from a PBX to a PSTN.
International access code	`Canonical-dialing-international-prefix`	Text; comma separated if multiple values. Max. 50 characters	Default: NULL	International prefix used to dial to another country, e.g. "00" in Germany and United Kingdom.
Operator codes	`Canonical-dialing-operator-code`	Text; comma separated if multiple values. Max. 50 characters	Default: NULL	List of extension numbers for a connection to the operator.
Emergency numbers	`Canonical-dialing-emergency-number`	Text; comma separated if multiple values. Max. 50 characters	Default: NULL	List of emergency numbers to be used for the phone.

WBM Name	Item name	Type	Values	Description
Initial extension digits	`Canonical-dialing-extension-initial-digits`	Text; comma separated if multiple values. Max. 50 characters	Default: NULL	List of initial digits of all possible extensions in the local enterprise network.

4.6.3.2 Canonical dial lookup

WBM Name	Item name	Type	Values	Description
Local code <n>	`Canonical-lookup-local-code<index>`	Text. Max. 10 characters.	Default: NULL	Local enterprise code for the node/PBX the phone is connected to. <n> can be a number from 1 to 5, which enables up to 5 entries, and is represented in the `index`.
International code <n>	`Canonical-lookup-international-code<index>`	Text. Max. 30 characters.	Default: NULL	Full canonical format for the enterprise node. <n> can be a number from 1 to 5, which enables up to 5 entries, and is represented in the `index`.

4.6.3.3 Canonical dial

WBM Name	Item name	Type	Values	Description
Internal numbers	`Canonical-dialing-dial-internal-form`	Enumeration	`0`=Local enterprise form; `1`=Always add node; `2`=Use external numbers; Default: `0`	Defines how dial strings for internal numbers are generated.

WBM Name	Item name	Type	Values	Description
External numbers	`Canonical-dialing-dial-external-form`	Enumeration	0=Local public form; 1=National public form; 2=International form; Default: 0	Defines how dial strings for external numbers are generated.
External access code	`Canonical-dialing-dial-needs-access-code`	Enumeration	0=Not required; 1=For external numbers; Default: 1	Defines in which cases the external access code is added.
International gateway code	`Canonical-dialing-dial-needs-intGWcode`	Enumeration	0=Use national code; 1=Leave as +; Default: 0	Defines whether the international gateway code is added.

4.6.3.4 Phone location

WBM Name	Item name	Type	Values	Description
NG911 Location	`ng911-location-signalling`	Enumeration	0= Include location information in appropriate SIP messages 1= Do not include location information in any SIP messages but allow such information to be configured Default: 0	Defines whether location information are included in SIP messages. See also Section 6.16, "Phone Location". Available V3R3 and upwards.

4.6.4 Energy Saving

WBM Name	Item name	Type	Values	Description
Backlight timeout (hours)	`pixelsaver-timeout`	Enumer-ation	`2`=2; `3`=3; `4`=4; `5`=5; `6`=6; `7`=7; `8`=8; Default: `3`	After the phone has been inactive within the timespan specified in hours, the display back-light is switched off. Only used for OpenStage V2R1 and lower.
Backlight time	`pixelsaver-timeout-xt`	Enumer-ation	`1`=5s (not used); `2`=30s (not used); `3`=1min (LED); `4`=90s (not used); `5`=5min (LED); `6`=30min (LED); `7`=60min (LED); `8`=2h (CCFL/LED); `9`=3h (CCFL); `10`=4h (CCFL/LED); `11`=5h (CCFL); `12`=6h (CCFL); `13`=7h (CCFL); `14`=8h (CCFL/LED); `15`=45min (not used); Default LED: `3` (1min) Default CCFL: `8` (2h)	After the phone has been inactive within the timespan, the display backlight is switched off. The allowed value set de-pends on the backlight-type, see Section 4.9, "General information" s=seconds, min=minutes, h=hours.

4.6.5 Call logging

This function is not available with WPI.

4.6.6　　Video call

<table>
<tr><td>ⓘ</td><td>This function is available with firmware version V3.1.</td></tr>
</table>

WBM Name	Item name	Type	Values	Description
Video on	`video-on`	Boolean	`true`/`false` Default: `false`	When set to true, video call is on. Available with V3R3 onwards.

4.7 Date and time

WBM Name	Item name	Type	Values	Description
SNTP IP address	`sntp-addr`	IP address or hostname. Max. 64 characters.	Default: NULL	IP address or hostname of the SNTP server.
Timezone offset (hours)	`sntp-tz-offset`	Integer	Default: `0`	Shift in minutes in relation to UTC. For HFA only relevant if time source is SNTP.
Daylight saving	`daylight-save`	Boolean	`true`/`false` Default: `false`, OS40 US / DPIP35 / DPIP55: `true`	This item indicates whether daylight saving is required on the phone.This is effectively the master switch for the feature, if it is set to false then all daylight saving Operation (auto or manual) is disabled. For HFA only relevant if time source is SNTP.
Difference (minutes)	`daylight-save-minutes`	Integer	`60`	Time difference in relation to regular time when daylight saving time is in effect. For HFA only relevant if time source is SNTP.
Auto time change	`auto-daylight-save`	Boolean	`true`/`false` Default: `false`, OS40 US / DPIP35 / DPIP55: `true`	Enables or disables automatic control of daylight saving time according to the DST (Daylight Saving Time) zone selected. For HFA only relevant if time source is SNTP.

WBM Name	Item name	Type	Values	Description
DST zone	`daylight-save-zone-id`	Enumeration	0=Not set; 1=Australia 2007 (ACT, South Australia, Tasmania, Victoria); 2=Australia 2007 (New South Wales); 3=Australia (Western Australia); 4=Australia 2008+ (ACT, New South Wales, South Australia, Tasmania, Victoria); 5=Brazil; 6=Canada; 7=Canada (Newfoundland); 8=Europe (PT, UK); 9=Europe (AT, BE, HR, DK, FR, DE, HU, IT, LU, NL, NO, PL, SK, ES, SE, CH); 10=Europe (FI); 11=Mexico; 12=United States; 13=New Zealand; 14=New Zealand (Chatham); Default: 0	Specifies the zone for determining the date to automatically apply/remove daylight saving. "Not set" means no automatic changes. For the DLS and WEBM, the Daylight Saving Zone identities are currently defined by this fixed enumeration. Locally in the phone, this value correlates with the "daylight-save-zone-index" OCMS id. For HFA only relevant if time source is SNTP.

4.8   Speech

4.8.1   Codec preferences

The settings for each codec are specified by assigning a corresponding index to a generic parameter. The following XML snippet allows the use of the G.729 codec, and assigns a 10ms packet size as well as a selection rank of 2 to this codec.

> The same packet size must be used for all codecs.

The index number 3 is assigned to the G.729 codec, which is identified internally by the code number 2:

```
<Item name="codec-type" index="3">2</Item>
```
G.729 is allowed:
```
<Item name="codec-allowed" index="3">true</Item>
```
The packet size for G.729 is set to 10ms:
```
<Item name="codec-packet-size" index="3">0</Item>
```
G.729 has selection rank 2, that is, it will be second choice when the codec is negotiated:
```
<Item name="codec-rank" index="3">2</Item>
```

WBM Name	Item name	Type	Values	Description
Silence suppression	`audio-silence-suppression`	Boolean	`true`/`false` Default: `false`	Suppression of data transmission on no conversation.
Allow "HD" icon	`allow-hd-icon-display`	Boolean	`true`/`false` Default: `true`	Switches the "HD" icon displayed if and when the OpenStage is connected using a high quality (G.722 or better) codec.
Packet size	`codec-packet-size<index>`	Enumeration	`0`=10 ms; `1`=20 ms; `2`=Automatic; `3`=30ms; Default: `2`	Size of RTP packets in milliseconds.
	`codec-type`	Enumeration	`0`=G.711; `1`=G.722; `2`=G.729	Binds a codec type to a set of items using the `index`.

WBM Name	Item name	Type	Values	Description
G.711 ranking G.729 ranking G.722 ranking	`codec-rank` `<index>`	Integer	`1` to number of codec types. Default: `1` for G.722; `2` for G.711; `3` for G.729	Ranking for each codec.

G.711 allowed
G.729 allowed
G.722 allowed
	`codec-`
	`allowed`
	`<index>`
		Boolean	`true`/`false`
			Default:
			`false` for G.722;
			`true` for G.711;
			`true` for G.729
				Allows or disallows a co-dec.

4.8.2 Audio settings

The usage of microphone and speaker for speakerphone mode can be controlled by the provisioning interface. Both microphone and loudspeaker can be switched on or off separately. By default, both microphone and loudspeaker are switched on.

> The microphone control is not valid for OpenStage 20E, as this model has no builtin microphone.

WBM Name	Item name	Type	Values	Description
Mute Settings > Microphone ON - Loudspeaker ON	`loudspeech-enabled`	Boolean	`true`	Both microphone and loudspeaker are switched on.
	`disable-microphone`	Boolean	`false`	
Mute Settings > Microphone OFF - Loudspeaker ON	`loudspeech-enabled`	Boolean	`true`	The microphone is switched off, but the loudspeaker is switched on.
	`disable-microphone`	Boolean	`true`	
Mute Settings > Microphone OFF - Loudspeaker OFF	`loudspeech-enabled`	Boolean	`false`	Both microphone and loudspeaker are switched off.
	`disable-microphone`	Boolean	`true`	
DTMF playback	`play-dtmf`	Boolean	`true`/`false` Default: false	The DTMF playback feature aims at the capability to play DTMF digits received using RFC2833 coding (i.e. Rtp events) in the current active audio device (headset / loudspeaker /handset).

4.9 General information

> These parameters are read only.

WBM Name	Item name	Type	Values	Description
MAC address	`mac-addr`	Text. 17 charac-ters		Shows the phone's MAC address.
Software version	`software-version`	Text. Max. 20 charac-ters		Displays the version of the phone's firmware.
Related Soft-ware version	`related-software-version`	Text. Max. 20 charac-ters		Displays the version of the phone's firmware.
Last restart	Not applicable.			Shows date and time of the last reboot.
Backlight type	`backlight-type`	Enumer-ation	`0`=none `1`=CCFL `2`=LED	Indicates whether the phone has a backlight, and, if applicable, the type of backlight. Available with OpenStage V2R2.

4.10   Security and Policies

> The menu structure has changed with firmware version V3. The corresponding section in the V2 menu is called "Authentication".

4.10.1   Password

4.10.1.1   Generic Policy (V3)

WBM Name	Item name	Type	Values	Description
Expires after (days)	`passw-expiry-days`	Number	`0` to `255`; `0`= passwords do not expire.	Maximum validity period of a password.
Warn before (days)	`passw-warn-days`	Number	`0` to `255`	Specifies when the user/admin is notified that his password will expire.
Force changed	`force-update`	Boolean	`true`/`false` Default: `false`	When set to `true`, the user/admin will be forced to change the password at next login.
Tries allowed	`pwd-retries`	Integer	`0;2;3;4;5`	Specifies the maximum number of password entry trials before the password is suspended.
No change for (hours)	`pwd-min-reset-period`	Integer	`0` to `24`	Specifies a period before a password is allowed to be changed again.
Suspended for (mins)	`pwd-suspended-duration`	Integer	`0` to `99`	Defines how long a password will be suspended after the number of failed retries has exceeded

WBM Name	Item name	Type	Values	Description
History valid for (days)	`pwd-history-days`	Integer	Default: `180`	Defines a period in days during which the history is valid. Passwords no longer used are kept in history lists for the user and admin passwords to prevent reuse of past passwords. This list is organised as FIFO (First In, First Out) so that it always contains the latest passwords.

4.10.1.2   Admin Policy (V3)

WBM Name	Item name	Type	Values	Description
Expiry date	`admin-pwd-expiry`	Date/ Time	Display only	Shows the date and time when the admin password will expire.
Minimum length	`min-admin-passw-length`	Integer	`6` to `24` Default: `6`	Defines the minimum number of characters for the admin password.
Password history	`admin-pwd-history`	Integer	`0` to `6` Default: `0`	Specifies the number of entries to be kept in the admin password history. New passwords must not match any password in the history.

WBM Name	Item name	Type	Values	Description
Current status	`admin-pwd-status`	Enumer-ation	0="active"; 1="suspended"; 2="disabled"	When set to "active", the admin password is avail-able for use. With "sus-pended", the admin pass-word is not available for a period or until reset. When set to "disabled", all access via the admin password is disabled. The status of the admin password can only be set via WPI. It is changed in-ternally to "suspended" when the password has been entered incorrectly more times than allowed.

4.10.1.3 User Policy (V3)

WBM Name	Item name	Type	Values	Description
Expiry date	`user-pwd-expiry`	Date/Time	Display only	Shows the date and time when the user password will expire.
Minimum length	`min-user-passw-length`	Integer	6 to 24 Default: 6	Defines the minimum number of characters for the user password.
Password history	`user-pwd-history`	Integer	0 to 6 Default: 0	Specifies the number of entries to be kept in the user password history. New passwords must not match any password in the history.

WBM Name	Item name	Type	Values	Description
Current status	`user-pwd-status`	Enumer-ation	0="active"; 1="suspended"; 2="disabled" Default: 0	When set to "active", the user password is avail-able for use. With "sus-pended", the user pass-word is not available for a period or until reset. When set to "disabled", all access via the user password is disabled.

4.10.1.4 Character Set (V3)

WBM Name	Item name	Type	Values	Description
Ucase chars reqd.	`pwd-upper`	Integer	0 to 24 Default: 0	Defines the minimum number of uppercase characters.
Lcase chars reqd.	`pwd-lower`	Integer	0 to 24 Default: 0	Defines the minimum number of lowercase characters.
Digits required	`pwd-digit`	Integer	0 to 24 Default: 0	Defines the minimum number of digits.
Special chars reqd	`pwd-punct`	Integer	0 to 24 Default: 0	Defines the minimum number of special charac-ters. The set of possible characters is ` `` - = [ ] ; ' # \ , . / ¬ ! " £ $ % ^ & * ( ) _ + { } : @ ~ | < > ? `
Bar repeat length	`pwd-sequence-length`	Integer	0 to 24, but not 1 (with 1 set as val-ue, no password would be valid, because it would be forbidden to use any charac-ter once) Default: 0	Specifies the maximum number of consecutive uses of a character.

WBM Name	Item name	Type	Values	Description
Min char difference	`pwd-min-no-differences`	Integer	`0` to `24` Default: `0`	Specifies the minimum number of characters by which a new password must differ from the previous password.

4.10.1.5   Change Admin password

The Admin password is a write only item, and therefore cannot be read by the provisioning server.

WBM Name	Item name	Type	Values	Description
Current / New / Confirm password	`admin-pwd`	String. Min. 6 characters; max. 24 characters.	Default: `123456`	Password for the admin section in the local menu and web interface.

4.10.1.6   Change User password

WBM Name	Item name	Type	Values	Description
Current/ New / Confirm password	`user-pwd`	String. Min. 6 characters; max. 24 characters.	Default: NULL	Password for the user section in the local menu and web interface.

4.10.2 Certificates (V3)

4.10.2.1 Generic

WBM Name	Item name	Type	Values	Description
OCSP check	`ocsp-check-allowed`	Boolean	`true`/`false` Default: `false`	When set to `true`, the configured OCSR is requested to check if the certificate has been revoked.
OCSR 1 address	`ocsr1-addr`	IP address or FQDN	Default: `NULL`	Specifies the IP address (or FQDN) of a primary OCSP responder.
OCSR 2 address	`ocsr2-addr`	IP address or FQDN		Specifies the IP address (or FQDN) of a secondary OCSP responder.

4.10.2.2 Authentication Policy

WBM Name	Item name	Type	Values	Description
Secure file transfer	See Section 4.4.6, "Security".			
Secure send URL				
Secure SIP server	`sip-tls-authentication-policy`	Enumeration	0=None; 1=Trusted; 2=Full Default: 0	Sets the authentication level for the SIP server connected to the phone.
Secure 802.1x server	`dot1x-authentication-policy`	Enumeration	0=None; 1=Trusted; 2=Full Default: 1	Sets the authenticating level for the Radius server. Currently no distinction between "Full" & "Trusted". Supersedes radius-server-validation but the old item is retained and synchronised to the policy.

WBM Name	Item name	Type	Values	Description
XML applications	`xml-app-authentication-policy`	Enumeration	`0`=None; `1`=Trusted; `2`=Full Default: 0	Sets the authentication level for the XML applications server.

4.11 Ringer Setting

4.11.1 Distinctive

> This function is available with firmware version V3R3.

The SIP server may provide information which indicates a specific type of call within an incoming call. The relevant information is carried as a string in the SIP Alert-Info header. When this string matches a specific string stored on the phone (the "Name" parameter), the corresponding ringer is triggered. In the Asterisk dial plan (`extensions.conf`), this is done by the `SIPAddHeader()` function. The following example line from an extensions.conf, which precedes the line containing the `Dial()` function, adds the specific string `alert-internal` to the SIP header for a specific number pattern:

```
exten => _3XXX,1,SIPAddHeader("Alert-Info:alert-internal")
```

Thus, in this example, the value for the "Name" parameter would be "alert-internal".

The parameters for distinctive ringing are encoded as a single string within one `alert` item, with ^ as separation markers. In the following example, the SIP Alert-Info header string `alert-internal` selects pattern melody `7`, with pattern sequence `2`, a duration of `60` seconds, and the sound file `Ringer2.mp3`:

```
<Item name="alert" index="1">alert-internal^7^2^60^Ringer2.mp3</Item>
```

Distinctive Ringers per Keyset Lines

For implicit mapping of line ringer names on Keyset Lines following format is to be used: "Line-<DN of line>-Reserved". Thus for a line with Destination Number (DN)=1234 the mapped distinctive ringer name is "Line-1234-Reserved". The name is case-sensitive, mind the uppercase L and R in name. The name needs to be manually constructed and configured by Admin as a new ringer name and each such name should be manually checked as being unique in the table. When using 'Distinctive Ringers per Keyset Lines', it is not allowed to define 'bellcore_dr1', 'bellcore_dr2', and 'bellcore_dr3' in the same distinctive ringer table. Otherwise these settings will be used because of higher priority in SIP-INVITE header. MLPP and Lowel Impact Level calls are also with higher priority.

The "User>Configuration>Keyset>Lines" form has the 'Destination Number' of the line being configured and this can be used to map directly to distinctive ringer names in the "Admin>Ringer setting" form. If a distinctive ringer with a matching name has not been configured into the table then the Ringer related items Ringer, Ringer tone melody, and Ringer sequence in the "User>Configuration>Keyset>Lines" form will be absent. If a matching distinctive ringer name is found then the "Ringer" items are editable with the initially shown value being the same as

the value in the "Admin>Ringer setting" form. Changes made to the "Ringer" values by the User will also change the matching distinctive ringer values in "Admin>Ringer setting". Distinctive Ringers are not applicable for DSS Keys.

WBM Name	Item name	Type	Values	Description
Name	`alert <index>` (1st value)	Text Max. 50 charac- ters	Default: NULL	String to be matched for selecting a particular ring- tone. For Ringers per Keyset Line see above Section 4.11.1, "Distinc- tive Ringers per Keyset Lines"
Ringer sound	`alert <index>` (5th value)	Text	File name Default: NULL	Name of a file containing the ringer sound in "/data/ ringtones" (or "/data/vis- tor/ringtones") or NULL (no file assigned, in this case "ringer-melody[in- dex]" and "ringer-tone[in- dex]" are applicable). All OpenStage/OpenScape Desk phones support WAV and MIDI files; OpenStage 60/80/OSD- PIP55G also support MP3 files.
Pattern melody / Audible	`alert <index>` (2nd value)	Integer	`0`=silence; `1` to `8` Default: `0`	Selects a ringer melody from a variety of 8 melo- dies. If the value is zero, the internal tag alert-type- [index] is set to silence(1) and ringer-melody-[index] is not changed as it has no significance. If value is non-zero, the internal tag alert-type-[in- dex] is set to ring(0) and ringer-melody-[index] is set to the melody 1-8.

WBM Name	Item name	Type	Values	Description
Pattern sequence	`alert <index>` (3rd value)	Enumeration	`1`=1 sec ON, 4 sec OFF; `2`=1 sec ON, 2 sec OFF; `3`=0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3 sec OFF; `4`=2 sec ON, 4 sec OFF; (SIP only) `5`=1.64 sec ON, 0.36 sec OFF; (SIP only) Default: `2`	Selects a ringer sequence consisting of melody patterns and silent periods.
Duration (seconds)	`alert <index>` (4th value)	Integer	`0` (continuous ring); `1` to `300` Default: `60`	Determines how many seconds the phone will ring.

4.11.2   Map To Specials

WBM Name	Item name	Type	Values	Description
Internal	`map-special-ringer-0`	Text Max. 50 characters	Default: Bellcore-dr1	SIP Alert-info ringer names like: Bellcore-dr1, alert-emergency indicating ringing call type. The string ringer name must match an existing alert-identifier entry in the alert-identifier indexed list. The same ringer name should not be configured for a different map entry.
External	`map-special-ringer-1`	Text	Default: Bellcore-dr2	see Internal
Recall	`map-special-ringer-2`	Text	Default: Bellcore-dr3	see Internal

WBM Name	Item name	Type	Values	Description
Emergency	`map-special-ringer-3`	Text	Default: alert-emergency	see Internal
Special1	`map-special-ringer-4`	Text	Default: NULL	see Internal
Special2	`map-special-ringer-5`	Text	Default: NULL	see Internal
Special3	`map-special-ringer-6`	Text	Default: NULL	see Internal

4.12 Mobility

> This function is not available with WPI.

4.13   Diagnostics

4.13.1   Diagnostic information

4.13.1.1   View

> This function is not available with WPI.

4.13.1.2   User access

WBM Name	Item name	Type	Values	Description
User access	`allow-user-access-to-diagnostic-data`	`Boolean`	`true/false` Default: `true`	Enables user access to diagnostic data.

4.13.2   LLDP-MED TLVs

> This function is not available with WPI.

4.13.3   Fault trace configuration

Error tracing and logging can be configured separately for all services and applications running on the OpenStage phone. The resulting files can be viewed in the WBM web pages over the Download links.

WBM Name	Item name	Type	Values	Description
File size (bytes)	`trace-file-size`	Enumeration	1048576 to 6291456 (i.e. 64KB to 6MB) Default: `1048576`	Maximum size of the trace file.

WBM Name	Item name	Type	Values	Description
Trace timeout (minutes)	`trace-timeout`	Integer	`0` to `999` Default: `60`	Determines when to stop writing to the trace file. When the value is 0, the timeout is disabled.
Automatic clear before start	`trace-autoclear`	Boolean	`true`/`false` Default: `false`	If set to `true`, the existing trace file will be deleted on pressing the Submit button, and a new, empty trace file will be generated. After deletion of trace file the phone will reset the value to "false".
Administration	`trace-level index="0"`	Enumeration	0=NONE; 1=FATAL; 2=ERROR; 3=WARNING; 4=LOG; 5=TRACE; 6=DEBUG; Default: `0`	Deals with the changing and setting of parameters within the phone database, from both the user and admin menus.
AGP Phonelet (V3)	`trace-level index="37"`	Enumeration	As with "Administration"	Any Java applications running on the phone will be run in the Java sandbox controlled by the Java service. Available for OS60/80, DPIP55 phones.
Application framework	`trace-level index="35"`	Enumeration	As with "Administration"	All applications within the phone, e.g. Call view, Call log or Phonebook, are run within the application framework. It is responsible for the switching between different applications and bringing them into and out of focus as appropriate.

WBM Name	Item name	Type	Values	Description
Application menu	`trace-level index"=5"`	Enumer-ation	As with "Adminis-tration"	This is where applications to be run on the phone can be started and stopped. Available for OpenStage 60/80, DPIP55 phones.
Bluetooth service	`trace-level index="40"`	Enumer-ation	As with "Adminis-tration"	Handles the Bluetooth interactions between external Bluetooth devices and the phone. Bluetooth is available only on OpenStage 60/80 phones.
Call Log	`trace-level index="1"`	Enumer-ation	As with "Adminis-tration"	The Call log application displays the call history of the phone.
Call View	`trace-level index="2"`	Enumer-ation	As with "Adminis-tration"	Handles the representation of telephony calls on the phone screen.
Certificate management	`trace-level index="6"`	Enumer-ation	As with "Adminis-tration"	Handles the verification and exchange of certificates for security and verification purposes.
Clock Service	`trace-level index="50"`	Enumer-ation	As with "Adminis-tration"	Handles the phone's time and date, including daylight saving and NTP functionality.
Communications	`trace-level index="7"`	Enumer-ation	As with "Adminis-tration"	Involved in the passing of call related information and signaling to and from the CSTA service.
Component registrar	`trace-level index="8"`	Enumer-ation	As with "Adminis-tration"	Handles data relating to the type of phone, e.g. OpenStage 20/40 HFA/SIP, OpenStage 60/80 HFA/SIP.

WBM Name	Item name	Type	Values	Description
CSTA service	`trace-level index="9"`	Enumeration	As with "Administration" Default: 6	Any CSTA messages are handled by this service. CSTA messages are used within the phone by all services as a common call progression and control protocol.
Data Access service	`trace-level index="10"`	Enumeration	As with "Administration"	Allows other services to access the data held within the phone database.
Desktop	`trace-level index="36"`	Enumeration	As with "Administration"	Responsible for the shared parts of the phone display. Primarily these are the status bar at the top of the screen and the FPK labels.
Digit analysis service	`trace-level index="11"`	Enumeration	As with "Administration"	Analyses and modifies digit streams which are sent to and received by the phone, e. g. canonical conversion.
Directory service	`trace-level index="13"`	Enumeration	As with "Administration"	Performs a look up for data in the phonebook, trying to match incoming and outgoing numbers with entries in the phonebook.
DLS client management	`trace-level index="14"`	Enumeration	As with "Administration"	Handles interactions with the provisioning service.
Health service	`trace-level index="15"`	Enumeration	As with "Administration"	Monitors other components of the phone for diagnostic purposes and provides a logging interface for the services in the phone.
Help	`trace-level index="4"`	Enumeration	As with "Administration"	Handles the help function.
HTTP Service				Not applicable.

WBM Name	Item name	Type	Values	Description
Instrumentation service	`trace-level index="16"`	Enumer-ation	As with "Adminis-tration"	Used by the HPT (Husim Phone Tester) to ex-change data with the phone for remote control, testing, and monitoring purposes.
Journal service	`trace-level index="17"`	Enumer-ation	As with "Adminis-tration"	Responsible for saving and retrieving call history information, which is used by the Call log applica-tion.
Media control service	`trace-level index="18"`	Enumer-ation	As with "Adminis-tration"	Provides the control of media streams (voice, tones, ringing etc.) within the phone.
Media processing service	`trace-level index="19"`	Enumer-ation	As with "Adminis-tration"	This is a layer of software between the media con-trol service, the tone generation, and voice en-gine services. It is also in-volved in the switching of audio devices such as the handset and loudspeaker.
Media recording service	`trace-level index="53"`	Enumer-ation	As with "Adminis-tration"	Handles call recording.
Mobility service	`trace-level index="20"`	Enumer-ation	As with "Adminis-tration"	Not relevant.
OBEX service	`trace-level index="21"`	Enumer-ation	As with "Adminis-tration"	Involved with Bluetooth accesses to the phone. Bluetooth is available only on OpenStage 60/80 phones.
OpenStage client management	`trace-level index="22"`	Enumer-ation	As with "Adminis-tration"	Provides a means by which other services with-in the phone can interact with the database.
Password management service	`trace-level index="24"`	Enumer-ation	As with "Adminis-tration"	Verifies passwords used in the phone.

WBM Name	Item name	Type	Values	Description
Phonebook	`trace-level index="3"`	Enumer-ation	As with "Adminis-tration"	Responsible for the phonebook application. Available for OpenStage 60/80, DPIP55 phones.
Performance Marks	`trace-level <index=23>`	Enumer-ation	As with "Adminis-tration"	Aid for measuring the per-formance of the phone. For events triggered by the user, a performance mark is written to the trace file, together with a timestamp in the format hh:mm:ss:yyyy.millisec-onds, and information about the event. The timespan between two performance marks is an indicator for the perfor-mance of the phone. The trace level must be set to "TRACE" or "DEBUG".
Physical interface service	`trace-level index="25"`	Enumer-ation	As with "Adminis-tration"	Handles any interactions with the phone via the keypad, mode keys, fixed feature buttons, click-wheel and slider.
Security Log Service	`trace-level index="52"`	Enumer-ation	As with "Adminis-tration"	Handles the Security Logs
Service frame-work	`trace-level index="38"`	Enumer-ation	As with "Adminis-tration"	This is the environment within which other phone services operate. It is in-volved in the starting and stopping of services.
Service registry	`trace-level index="39"`	Enumer-ation	As with "Adminis-tration"	Keeps a record of all ser-vices currently running in-side the phone.
Sidecar service	`trace-level index="26"`	Enumer-ation	As with "Adminis-tration"	Handles interactions between the phone and any attached sidecars.

WBM Name	Item name	Type	Values	Description
SIP call control	`trace-level index="33"`	Enumer-ation	As with "Adminis-tration" Default: `6`	Contains the call model for the phone and is asso-ciated with telephony and call handling.
SIP messages	`trace-level index="34"`	Enumer-ation	As with "Adminis-tration" Default: `6`	Traces the SIP messages exchanged by the phone.
SIP signalling	`trace-level index="32"`	Enumer-ation	As with "Adminis-tration" Default: `6`	Involved in the creation and parsing of SIP mes-sages. This service com-municates directly with the SIP stack.
Team service	`trace-level index="27"`	Enumer-ation	As with "Adminis-tration"	Primarily concerned with keyset operation.
Tone generation service	`trace-level index="28"`	Enumer-ation	As with "Adminis-tration"	Handles the generation of the tones and ringers on the phone.
Transport service	`trace-level index="29"`	Enumer-ation	As with "Adminis-tration"	Provides the IP (LAN) in-terface between the phone and the outside world.
USB backup service	`trace-level index="44"`	Enumer-ation	As with "Adminis-tration"	Used to make backup/re-store to/from USB stick by using password. This item is available in the phone GUI. Available for OpenStage 60/80, DPIP55 phones.
vCard parser ser-vice	`trace-level index="42"`	Enumer-ation	As with "Adminis-tration"	Handles parsing and identification of VCard in-formation while sending or getting VCards via Bluetooth.
Video service en-gine	`trace-level index="55"`	Enumer-ation	As with "Adminis-tration"	Handles the video func-tionality.

WBM Name	Item name	Type	Values	Description
Voice engine service	`trace-level index="30"`	Enumeration	As with "Administration"	Provides a switching mechanism for voice streams within the phone. This component is also involved in QDC, Music on hold and voice instrumentation.
Voice mail	`trace-level index="43"`	Enumeration	As with "Administration"	Handles the voice mail functionality.
Voice recognition	`trace-level index="46"`	Enumeration	As with "Administration"	Used by the voice dial facility for recognizing spoken dialing commands.
Web server service	`trace-level index="31"`	Enumeration	As with "Administration"	Provides access to the phone via web browser.
802.1x service	`trace-level index="45"`	Enumeration	As with "Administration"	Provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. The service is used for certain closed wireless access points.

4.13.4   EasyTrace Profiles

ℹ️ This function is not available with WPI.

4.13.5   Bluetooth Advanced Traces

ℹ️ This function is not available for OpenStage Desk Phone IP.

WBM Name	Item name	Type	Values	Description
Automatic clear before start	`bt-hci-del-before-start`	`Boolean`	`true/false` Default: `true`	Flag, if dumpfile should be deleted before starting new trace
File size (Max. 6290000 bytes)	`bt-hci-dump-file-size`	`Enumer-ation`	1 to 6300000 Default: `256000`	Maximum size of the trace file.
Extended dump	`bt-hci-extended-dump`	`Boolean`	`true/false` Default: `true`	Changes command line parameter for call of Dump tool
Verbose decod-ing	`bt-hci-ver-bose`	`Boolean`	`true/false` Default: `true`	
Tracing is stopped				Not applicable

4.13.6 QoS Reports

4.13.6.1 Generation

The generation of QoS (Quality of Service) reports which are sent to a QCU server (see Section is configured here.

WBM Name	Item name	Type	Values	Description
Report mode	`qdc-report-mode`	Enumer-ation	`0`=OFF; `1`=EOS Threshold ex-ceeded; `2`=EOR Threshold ex-ceeded; `3`=EOS (End of Session); `4`=EOR (End of Report Interval); Default: `0`	Sets the conditions for generating a QoS report.

WBM Name	Item name	Type	Values	Description
Report interval (seconds)	`qdc-report-int`	Integer	`10` to `3600`. Value must be an integer multiple of the "Observation interval" value, that is, a multiple of 10. Default: `60`	Time interval between the periodical observations.
Observation interval (seconds)	`qdc-obs-int`	Integer	`10` (only)	During this time interval, the traffic is observed.
Minimum session length (100 milli-second units)	`qdc-session`	Integer	`0` to `255` Default: `20`	Depending on the report mode, a report can be created only if the duration of the conversation exceeds this value.
Maximum jitter (milliseconds)	`qdc-jitter-buffer-threshold`	Integer	`0` to `255` Default: `20`	When the jitter exceeds this value, a report is generated.
Average round trip delay (milliseconds)	`qdc-delay-thresh`	Integer	`0` to `5000` Default: `100`	When the average round trip time exceeds this value, a report is generated.
Non-compressing codec threshold values - Lost packets (per 1000 packets)	`qdc-ncc-packet-loss-threshold`	Integer	`0` to `255` Default: `10`	When the number of lost packets exceeds this maximum value during the observation interval, a report is created.
Non-compressing codec threshold values - Consecutive lost packets	`qdc-ncc-consecutive-packet-loss`	Integer	`0` to `255` Default: `2`	When the number of lost packets following one another exceeds this maximum value during the observation interval, a report is created.
Non-compressing codec threshold values - Consecutive good packets	`qdc-ncc-consecutive-good-packets`	Integer	`0` to `255` Default: `8`	When the number of good packets following one another falls below this minimum value, a report is created.

WBM Name	Item name	Type	Values	Description
Compressing codec threshold values - Lost packets (per 1000 packets)	`qdc-cc-packet-loss-threshold`	Integer	0 to 255 Default: 10	When the number of lost packets exceeds this maximum value during the observation interval, a report is created.
Compressing codec threshold values - Consecutive lost packets	`qdc-cc-consecutive-packet-loss`	Integer	0 to 255 Default: 2	When the number of lost packets following one another exceeds this maximum value during the observation interval, a report is created.
Compressing codec threshold values - Consecutive good packets	`qdc-cc-consecutive-good-packets`	Integer	0 to 255 Default: 8	When the number of good packets following one another falls below this minimum value, a report is created.
Compressing codec threshold values - Resend last report	`action-submit-resend-last-qdc-reports`	Integer	`true`/`false` Default: `false`	Set to `true` to invoke the action and set back to `false` on completion of the action.

4.13.6.2 View Session Data

QoS reports can be viewed using the phone's web interface. The WBM path is Diagnostics > QoS reports > View Session Data.

4.13.7 Miscellaneous

4.13.7.1 IP tests

This area is applicable only when using the web interface.

4.13.7.2 Memory information

This area is applicable only when using the web interface.

4.13.7.3   Core Dump

WBM Name	Item name	Type	Values	Description
Enable core dump	`core-dump-enabled`	Boolean	`true`/`false` Default: `true`	If enabled, a core dump will be initiated in case of a severe error. Phone re-start required to bring changes to this item into effect.
Delete core dump		Boolean	`true`/`false` Default: `false`	Not applicable.

4.14 Maintenance

4.14.1 Remote trace

This area is applicable only when using the web interface.

WBM Name	Item name	Type	Values	Description
Remote Trace Status	`remote-trace-enable`	Bool	`true`/`false` Default: `false`	If enabled, syslog server will be used for remote trace.
User Notification	`remote-trace-user-notify`	Bool	`true`/`false` Default: `false`	If enabled, the user gets a notification
Remote Server IP	`remote-trace-ip`	IP Number	Default: Null	Defines IP address of Remote Server
Remote Server Port	`remote-trace-port`	Port Number	Default: 514	Defines port number of Remote Server

4.14.2 Restart Phone

The regular phone restart, which retains the phone's settings, is triggered by a special `Action`, whose content is `Restart`. For further information, see Section 3.6.5, "Restart Phone".

4.14.3 Factory reset

This procedure resets all parameters to factory settings and reboots the phone. To start a factory reset, the `Action` has to be set to `Restart`, as with the regular phone restart. Additionally, the special, fixed password must be provided in the `restart-password` item, and the `restart-type` item must be set to `FactoryReset`. See the following snippet:

```
<Item name="restart-password">124816</Item>
<Item name="restart-type">FactoryReset</Item>
```

4.14.4 HPT interface

WBM Name	Item name	Type	Values	Description
Disable HPT	`enable-test-interface`	Bool	`true`/`false` Default: `true`	Used to disable test interface.

4.14.5 Secure Shell

> ℹ This function is available with firmware OpenStage V2.

The phone's operating system can be accessed via SSH for special troubleshooting tasks. Hereby, the administrator, or service technician, is enabled to use the phone's built-in Linux commands. As soon as SSH access has been enabled using the web interface, the system can be accessed by the user "admin" for a specified timespan.

The provisioning service can define whether it shall be possible to enable SSH access. If disabled, the Secure Shell input mask will not appear on the web interface.

WBM Name	Item name	Type	Values	Description
Enable access	`ssh-enable-allowed`	Boolean	`true`/`false` Default: `true`	Determines whether SSH access can be enabled.
Session password	`ssh-password`	Text	Charcters min. length 6, max. length 24.	Defines Password for secure shell. Available only if Enable access = true.
Access minutes	`ssh-timer-connect`	Enumeration	1=1; ...10=10; Default: `3`	The session is disabled if not used within this timeout in minutes.
Session minutes	`ssh-timer-session`	Enumeration	5=5; 10=10; 20=20; 30=30; 60=60; Default: `10`	The session is disabled after use for this time in minutes.

4.14.6 Diagnostic Call

> ℹ This function is available with firmware version V3.1.

This feature provides the possibility to place a diagnostic call, which starts call related tracing on the phone and on involved OS Voice and collect these traces at OpenStage Voice Trace Manager (OSVTM). With all these traces available, a call can be followed throughout the voice

system and a possible problem can be detected faster. As all traces from all involved components are available at the first level support, the analysis of a possible problem can be started immediately. Admin is not able to change trace settings or can not clear the existing phone traces during an active diagnostic tracing. If admin tries this, admin will get an error message.

WBM Name	Item name	Type	Values	Description
Prefix Code	`diagnostic-call-prefix`	Text	Digits, max. length 5 including starting "*" and ending "#"	Prefix code guishes normal calls from diagnostic calls. It MUST start with "*" character and MUST end with "#" character.

5 Phone Parameters - User

This section provides a comprehensive survey of the configuration and control parameters in the user area. The structure and order in which the data are presented corresponds to the web interface of the OpenStage phones and OpenScape Desk Phone IP. For example, Section 5.3.1, "Outgoing calls" is located under Section 5.3, "Configuration", which represents the navigation path "**Configuration** > **Outgoing calls**" in the web interface. However, deviations are possible due to changes between firmware versions.

If not otherwise stated, the Items are available on all phone variants, that is, OpenStage 15/20/40/60/80 and OpenScape Desk Phone IP 35/55G.

The syntax for each Item is `<Item name="ItemName">Value</Item>`.

Example: `<Item name="e164">49897223290</Item>`

5.1 Date and Time

WBM Name	Item name	Type	Values	Description
Local time / Local date (day, month, year)	`time`	Numeric	Unix time stamp	Sets time and date, if not provided by SNTP. The Unix Time Stamp is the number of seconds elapsed since January 1st. In messages from the phone, `000` is appended to the Unix Time Stamp as the milliseconds part; this part can be ignored.
Use daylight saving	`daylight-save`	Boolean	`true`/`false` Default: `false`, OS40 US/ DPIP35 / DPIP55: true	Enables or disables daylight saving time in conjunction with Auto time change. For HFA, only relevant if time source is SNTP.
Difference (minutes)	`sntp-tz-off-set`	Enumeration	0 ...60	Defines how many minutes the clock is put forward for daylight saving time. For HFA, only relevant if time source is SNTP.

WBM Name	Item name	Type	Values	Description
Auto time change	`auto-daylight-save`	Boolean	`true`/`false` Default: `false`, OS40 US/ DPIP35 / DPIP55: true	Enables or disables automatic control of daylight saving time according to the Time zone. For HFA, only relevant if time source is SNTP.

5.2 Audio

5.2.1 Standard Ringer

WBM Name	Item name	Type	Values	Description
Ringer melody	`ringer-melody`	Enumeration	`1` to `8` Default: 2	Selects a melody for the ringer.
Ringer tone sequence	`ringer-tone-sequence`	Enumeration	`1`=1.0 sec ON, 4.0 sec OFF; `2`=1.0 sec ON, 2.0 sec OFF; `3`=0.7 sec ON, 0.7 sec OFF, 0.7 sec ON, 3.0 sec OFF; `4`=2.0 sec ON, 4.0 sec OFF; `5`=1.64 sec ON, 0.36 sec OFF; Default: `2`	Defines the lengths of singular rings and the length of pauses in between .
Ringer	`ringer-audio-file`	Text	Default: `NULL`	Name of the ringtone file to be used (WAV or, on OpenStage 60/80, OpenScape DPIP 55G, MP3).
Room Character				Not applicable.
Open listening	`loudspeaker-function-mode`	Enumeration	`0`=Standard mode; `1`=US mode; Default: `0`, OS40 US / DPIP35 / DPIP55/ country= USA: `1`	Country-specific setting for speakerphone mode.
Headset socket	`socketed-headset-mode`	Enumeration	0=Wired headset; 1=Cordless headset; 2=Conference unit Default: `0`	Type of headset resp. conference unit connected to the phone. Relevant for OpenStage 40/60/80/ DPIP35/55.

5.2.2　Special ringers

Defines the ringer played for a limited range of special incoming calls where the type of call is signalled to the phone.

WBM Name	Item name	Type	Values	Description
Internal	`map-special-ringer-0`	Text	SIP Alert-info ringer names. Default: Bellcore-dr1	The string ringer name must match an existing alert-identifier entry in the alert-identifier indexed list. The same ringer name should not be configured for a different map entry.
External	`map-special-ringer-1`	Text	see Internal Default: Bellcore-dr2	see above Internal
Recall	`map-special-ringer-2`	Text	see Internal Default: Bellcore-dr3	see above Internal
Emergency	`map-special-ringer-3`	Text	see Internal Default: alert-emergency	see above Internal
Special 1	`map-special-ringer-4`	Text	see Internal Default: NULL	see above Internal
Special 2	`map-special-ringer-5`	Text	see Internal Default: NULL	see above Internal
Special 3	`map-special-ringer-6`	Text	see Internal Default: NULL	see above Internal

5.3 Configuration

5.3.1 Outgoing calls

WBM Name	Item name	Type	Values	Description
Autodial delay (seconds)	`autodialtimer`	Integer	1 to 9 Default: `6`	After this delay, which follows the last digit entered, a number is dialed.
Allow callback: busy	`callback-busy-enabled`	Boolean	`true`/`false` Default: `true`	Permits sending a callback request to the server when the remote party is busy.
Allow callback: no reply	`callback-ring-enabled`	Boolean	`true`/`false` Default: `true`	Permits sending a callback request to the server when the remote party does not answer the call.
Allow busy when dialing	`busy-when-dialling-enabled`	Boolean	`true`/`false` Default: `false`	If enabled, the phone switches to busy state when the user starts dialing.
Allow transfer on ring	`allow-transfer-on-ring-enabled`	Boolean	`true`/`false` Default: `true`	If enabled, it is possible to transfer a call to another party without any previous consultation with this party.
Allow immediate dialing	`hot-keypad-dialing`	Boolean	`true`/`false` Default: `false`	If enabled, immediate dialing is executed as soon as the entered string matches a dial plan entry.

5.3.2 Incoming calls

5.3.2.1 Deflecting

WBM Name	Item name	Type	Values	Description
Allow deflection	`call-deflection-enabled`	Boolean	`true`/`false` Default: `true`	If enabled, the user can deflect an incoming call.
Default deflect destination	`deflect-destination`	Text	Default: `NULL`	Target for deflected calls.
Deflect to DSS	`dss-sip-deflect`	Boolean	`true`/`false` Default: `false`	If enabled, a call can be deflected to a DSS number using the DSS key.

5.3.2.2 Forwarding

WBM Name	Item name	Type	Values	Description
Forwarding Favourites - Destination 1	`default-forwarding-1`	Text	Default: NULL	First forwarding destination.
Forwarding Favourites - Destination 2	`default-forwarding-2`	Text	Default: NULL	Second forwarding destination.
Forwarding Favourites - Destination 3	`default-forwarding-3`	Text	Default: NULL	Third forwarding destination.
Forwarding Favourites - Destination 4	`default-forwarding-4`	Text	Default: NULL	Fourth forwarding destination.
Forwarding Favourites - Destination 5	`default-forwarding-5`	Text	Default: NULL	Fifth forwarding destination.
Forward all calls allowed	`cfu-activated`	Boolean	`true`/`false` Default: `false`	Allows unconditional forwarding.
to	`cfu-address`	Text	Default: NULL	Forward destination if Forward all calls is active.

WBM Name	Item name	Type	Values	Description
Forward on busy allowed	`cfb-activated`	Boolean	`true`/`false` Default: `false`	Allows forwarding in case the user is engaged in another call.
to	`cfb-address`	Text	Default: NULL	Forward destination if Forward on busy is active.
Forward on no reply allowed	`cfnr-activated`	Boolean	`true`/`false` Default: `false`	Allows forwarding in case the user does not reply.
to	`cfnr-address`	Text	Default: NULL	Forward destination if Forward on nor reply is active.
No reply delay (seconds)	`cfnr-delay`	Integer	1 to `60` Default: `16`	After this delay, the call will be forwarded, if the user does not reply.
Visual alerts	`forwarding-notification-visual`	Boolean	`true`/`false` Default: `true`	If `true`, prompts and popups will provide full information about parties involved during the forwarding. If `false`, only information about ringing and connected parties is shown.
Audible alerts	`forwarding-notification-audible`	Boolean	`true`/`false` Default: `true`	Enable or disable audible alerts for call forwarding.
Forwarding party	`forwarding-party-display`	Enumeration	`0` = Display first; `1` = Display last Default: `1`	For incoming calls that have been forwarded by two or more parties, this parameter determines whether the first or the last forwarding party is indicated. Available with firmware version V2.

5.3.2.3   Forwarding by Call Type

This feature enhances the Call Forwarding (Standard) operation (Section 5.3.2.2, "Forwarding") by adding support for additional Call Forwarding settings explicitly for External and Internal calls, as well as the existing capability to forward any call, using functional menus that

extend the existing Call Forwarding UI. This is a serverbased feature provided by SIP Server with CSTA Phase III / ECMA-269. To use extended call forwarding, Server features and Allow uaCSTA must be switched on (See Section 4.4.5.1, "Configuration"). This feature can be enabled or disabled under System > Features > Feature access > Ext/int forwarding (See Section 4.4.5.10, "Feature access (V3 and onwards)". The label displayed to the left of the key is defined in Key label <key number>. It is possible to have an extra key defined for each Call Forwarding Call Type.

The provisioning service may read/write the new data items even if 'Forwarding on Call Type' is not in operation. The settings are used when 'Forwarding on Call Type' is active. However the provisioning service should read the changeable status of each setting and only attempt to write settings that are changeable. Attempts to write an unchangeable setting will be rejected by the phone as per other pre-existing read-only provisioning service items.

The provisioning service may set an FPK to one of the new functions. This will be accepted by the phone even if 'Forwarding on Call Type' is not in operation or the use is not allowed on the phone. However the provisioning service should avoid setting an FPK to such a function when it is not possible for it to be used.

The provisioning service will be able to configure the phone to use or not use the settings, even if the SIP server does currently support them.

WBM Name	Item name	Type	Values	Description
Forwarding unconditional external is active	`cfu-ext-activated`	Boolean	`true`/`false` Default: `false`	Allows unconditional forwarding for external calls.
Forwarding unconditional external destination URI	`cfu-ext-address`	Text	Default: NULL	Forwarding destination.
Forwarding unconditional internal is active	`cfu-int-activated`	Boolean	`true`/`false` Default: `false`	Allows unconditional forwarding for internal call.
Forwarding unconditional internal destination URI	`cfu-int-address`	Text	Default: NULL	Forwarding destination.
Forwarding on busy external is active	`cfb-ext-activated`	Boolean	`true`/`false` Default: `false`	Allows forwarding when busy for external calls.

WBM Name	Item name	Type	Values	Description
Forwarding on busy external destination URI	`cfb-ext-address`	Text	Default: NULL	Forwarding destination.
Forwarding on busy internal is active	`cfb-int-activated`	Boolean	`true`/`false` Default: `false`	Allows forwarding when busy for internal calls.
Forwarding on busy internal destination URI	`cfb-int-address`	Text	Default: NULL	Forwarding destination.
Forwarding on no reply external is active	`cfnr-ext-activated`	Boolean	`true`/`false` Default: `false`	Allows forwarding on no reply for external calls.
Forwarding on no reply external destination URI	`cfnr-ext-address`	Text	Default: NULL	Forwarding destination.
Forwarding on no reply internal is active	`cfnr-int-activated`	Boolean	`true`/`false` Default: `false`	Allows forwarding on no reply for internal calls.
Forwarding on no reply internal destination URI	`cfnr-int-address`	Text	Default: NULL	Forwarding destination.
Forwarding unconditional settings is unchangeable	`cfu-unchangeable`	Boolean	`true`/`false` Default: `false`	The SIP server can restrict individual settings and indicates to the phone that they are unchangeable. The SIP server will still provide the current values for an unchangeable setting but the phone/provisioning service must treat them as read only. When a setting has been indicated as unchangeable its activated status and destination address become read only.

WBM Name	Item name	Type	Values	Description
Forwarding un-conditional exter-nal settings is un-changeable	`cfu-ext-unchangeable`	Boolean	`true`/`false` Default: `false`	See above "Forwarding unconditional settings is unchangeable"
Forwarding un-conditional inter-nal settings is un-changeable	`cfu-int-unchangeable`	Boolean	`true`/`false` Default: `false`	See above "Forwarding unconditional settings is unchangeable"
Forwarding on busy settings is unchangeable	`cfb-unchangeable`	Boolean	`true`/`false` Default: `false`	See above "Forwarding unconditional settings is unchangeable"
Forwarding on busy external set-tings is un-changeable	`cfb-ext-unchangeable`	Boolean	`true`/`false` Default: `false`	See above "Forwarding unconditional settings is unchangeable"
Forwarding on busy internal set-tings is un-changeable	`cfb-int-unchangeable`	Boolean	`true`/`false` Default: `false`	See above "Forwarding unconditional settings is unchangeable"
Forwarding on no reply settings is unchangeable	`cfnr-unchangeable`	Boolean	`true`/`false` Default: `false`	See above "Forwarding unconditional settings is unchangeable"
Forwarding on no reply external settings is un-changeable	`cfnr-ext-unchangeable`	Boolean	`true`/`false` Default: `false`	See above "Forwarding unconditional settings is unchangeable"
Forwarding on no reply internal set-tings is un-changeable	`cfnr-int-unchangeable`	Boolean	`true`/`false` Default: `false`	See above "Forwarding unconditional settings is unchangeable"

5.3.2.4 Handling

WBM Name	Item name	Type	Values	Description
Allow call waiting	`call-waiting-enabled`	Boolean	`true`/`false` Default: `true`	If set to `true`, the user can accept a second incoming call in the course of an ongoing call.
Allow DND	`call-dnd-enabled`	Boolean	`true`/`false` Default: `true`	If set to `true`, the phone will not ring, and the caller hears the busy signal.
Allow busy when dialling	`busy-when-dialling-enabled`	Boolean	`true`/`false` Default: `false`	If set to `true`, an incoming call received while the user is dialing is rejected.

5.3.2.5 CTI calls

WBM Name	Item name	Type	Values	Description
Allow auto-answer	`auto-answer`	Boolean	`true`/`false` Default: `false`	If set to `true`, calls are accepted and set up automatically.
Allow beep on auto-answer	`beep-on-auto-answer`	Boolean	`true`/`false` Default: `false`	If set to `true`, an alert beep sounds when a call is automatically accepted.
	`auto-reconnect`	Boolean	`true`/`false` Default: `false`	If set to `true`, the user can resume a held call with either the CTI application or phone.
Allow beep on auto-reconnect	`beep-on-auto-reconnect`	Boolean	`true`/`false` Default: `false`	If set to `true`, a beep sounds when the user toggles between an active call and a held call.

5.3.3 Connected calls

WBM Name	Item name	Type	Values	Description
Allow call transfer	`call-transfer-enabled`	Boolean	`true`/`false` Default: `true`	If set to `true`, call transfer is enabled.
Allow call joining	`call-join-enabled`	Boolean	`true`/`false` Default: `true`	If set to `true`, the user can join the first party with the consulted party.
Allow exit conference	`join-allowed-in-conference`	Boolean	`true`/`false` Default: `false`	Determines whether or not the user's call partners are allowed to join calls after the user has exited the conference call.
Allow hold reminder	`call-hold-ringback-enabled`	Boolean	`true`/`false` Default: `true` OS40 US: `false`	If set to `true`, the user will be reminded that there is a call on hold after a specified timespan.
Hold reminder delay (minutes)	`holdringback-timer`	Integer	3 to 15 Default: 3	Timespan, after which the user will be reminded that there is a call on hold.
Hold and hang-up	`hold-and-hang-up`	Boolean	`true`/`false` Default: `no` OS40 US: `true`	When set to `true`, the held call is signalled after the time set with "Hold reminder delay". When set to `false`, it will be signalled immediately.
Allow music on hold	`moh-enabled`	Boolean	`true`/`false` Default: `true`	Music is played back to the user when the user is placed on hold by another party.
Allow conferences	`user-conference-enabled`	Boolean	`true`/`false` Default: `true`	Enables or disables local conferences.
Allow secure call alert	`secure-call-alert`	Boolean	`true`/`false` Default: `false`	If set to `true`, an alert tone will sound when the voice connection changes from secure to insecure.

WBM Name	Item name	Type	Values	Description
Toggle associate	`implicit-call-association`	Boolean	`true`/`false` Default: `false`	When set to `true`, the following procedure will ensue: The user has accepted a second call, whereby the first call is put to hold. As soon as the user has alternated back to the first call, and then again to the second call, he/she can connect both calling parties by going on-hook. Available with firmware version V2.
Lower IL alert	`IL-alert-notification-enabled`	Boolean	`true`/`false` Default: `true`	When set to `true`, notification popup is displayed when level changes during call (connected or alerting) or when connects without ringing

5.3.4 Context menu

> This function is available on OpenStage phones.

WBM Name	Item name	Type	Values	Description
Auto show menu	`context-menu-auto-show`	Boolean	`true`/`false` Default: `true`	When set to `true`, the context menu for call handling will open automatically as soon as a call is established. Relevant for OpenStage 40/60/80 and OpenScape DPIP 55G. Available with firmware version V2R1.

WBM Name	Item name	Type	Values	Description
Auto hide time (sec.)	`context-menu-auto-hide-time`	Enumer-ation	5=**5**; 10=**10**; 20=**20**; 30=**30**; 60=**60**; 120=**120**; `No auto hide=0` (context menu will stay open) Default: `20`, OS40 US: `0`	Timeout in seconds after which the automatically opened context menu will disappear. Relevant for OpenStage 40/60/80/41 and Open-Scape DPIP 55G. Available with firmware version V2R1.

5.3.5   Keyset

5.3.5.1   Lines

The following parameters can be configured individually for each line handled by the phone. As they are already described in the administrator chapter, only cross-references to the corre-sponding section are given here.

WBM Name	See
Ring delay (seconds)	Section 4.4.5.3, "Line"
Allow in overview	Section 4.4.5.3, "Line"
Address	Section 4.4.5.3, "Line"
Primary line (read only)	Section 4.4.5.3, "Line"
Ring on/off (read only)	Section 4.4.5.3, "Line"
Ringer file	Section 4.11.1, "Distinctive Ringers per Keyset Lines"
Ringer/Pattern melody	Section 4.11.1, "Distinctive Ringers per Keyset Lines"
Ringer/Pattern sequence	Section 4.11.1, "Distinctive Ringers per Keyset Lines"
Selection order	Section 4.4.5.3, "Line"
Hot/warm line	Section 4.4.5.3, "Line" (Hot warm action)
Hot/warm destination	As the hotline/warmline function is used in special scenarios only, it is generally recommended not to use this option in MAA environ-ments.

5.3.5.2 Overview

WBM Name	Item name	Type	Values	Description
<Key label> (for the relevant line)	`line-mlo-pos <index>`	Integer	`1` to number of lines	Determines the position of this line in the line overview. In the WBM, the value is incremented or decremented by arrow buttons.

5.3.6   BLF

As the BLF parameters are already described in the administrator chapter, only cross-references to the corresponding section are given here.

WBM Name	See
Monitored phone (read only)	Section 4.4.5.3, "BLF"
Audible alert	Section 4.4.5.3, "BLF"
Popup on alert	Section 4.4.5.3, "BLF"

5.3.7   Bluetooth

> This function is available on OpenStage phones.

WBM Name	Item name	Type	Values	Description
Bluetooth device address	`bt-local-bda`	Text. Char(17).	Same format as MAC address	Bluetooth address of the phone. This value is read only. OpenStage 60/80 only.
Phone name	Not applicable			
Status	Not applicable			
Active	Not applicable			
Discoverable	Not applicable			
Pairing mode	Not applicable			
PIN for pairing	Not applicable			
Last connected device - Device address	Not applicable			
Last connected device - Device name	Not applicable			

WBM Name	Item name	Type	Values	Description
Last connected device - Device class	Not applicable			

5.3.8 Call logging

WBM Name	Item name	Type	Values	Description
Enable call log	`call-log-enabled`	Boolean	`true`/`false` Default: `true`	Enables or disables the call log.
Missed call logging	`missed-logging`	Enumaration	0=Include; 1=Exclude; Default: `0`	This item is required to allow logging or not logging calls that are completed elsewhere. 0=Include (Calls completed elsewhere will be logged as missed calls and in call log they will be seen with a special indication) 1=Exclude (Calls completed elsewhere will not be visible on phone; they will not be logged at all.)
Delete entry when called	`delete-missed-when-called`	Enumaration	0=manually 1=when called Default: `0`	Defines call logging of all calls or only those, which are not answered remotely.

5.3.9 Video Call

WBM Name	Item name	Type	Values	Description
Video on	`video-on`	Boolean	`true`/`false` Default: `false`	Enables/Disables making and accepting video calls. NOTE: This item is user configurable only if "video-allowed" is "true". It is hidden from user if "video-allowed" is "false".

5.4 Phone

5.4.1 Display

WBM Name	Item name	Type	Values	Description
Display brightness	`display-brightness`	Enumeration	`0`=-3; `1`=-2; `2`=-1; `3`=Default; `4`=+1; `5`=+2; `6`=+3	Adjusts the brightness for the phone display. Only available for phones with a LED display (see the `backlight-type` item in Section 4.9, "General information") and software version V2R2 onwards.
Slider brightness	Not applicable			
Sidecar contrast	Not applicable			
Touchguide	Not applicable			
Skin	`display-skin`	Enumeration	`0`=Silver Blue; `1`=Anthracite Orange; Default: `0`	Select the style for the graphical display. Open-Stage 60/80/ DPIP55 only.

5.4.2 Screensaver

WBM Name	Item name	Type	Values	Description
Screensaver enabled	`screensaver-enabled`	Boolean	`true`/`false` Default: `false`	Enables or disables the screensaver. OpenStage 60/80 / DPIP55 only.
Start (minutes)	`inactivity-timeout`	Enumeration	`0`=0 (no timeout); `5`=5; `10`=10; `20`=20; `30`=30; `60`=60; Default: `5`	When there has been no activity on the phone for this timespan, the screensaver will start. OpenStage 60/80 / DPIP55 only.
Picture time (secs)	`screensaver-image-timeout`	Enumeration	`5`=5; `10`=10; `20`=20; `30`=30; `60`=60; Default: `10`	Sets the intervals in seconds at which the screensaver images change. OpenStage 60/80 / DPIP55 only.

5.4.3 Program Keys

See Section 4.4.5.3, "Free Programmable Keys (FPK)".

5.4.4 Key Module 1

The settings for the first key module are the same as those for programmable keys on the phone (see Section 4.4.5.3, "Free Programmable Keys (FPK)").

For the first key module, the key numbers represented by the `index` attribute are 301 to 312 for the first level, and 1301 to 1312 for the shift level.

5.4.5 Key Module 2

The settings for the second key module are the same as those for programmable keys on the phone (see Section 4.4.5.3, "Free Programmable Keys (FPK)").

For the second key module, the key numbers represented by the `index` attribute are 401 to 412 for the first level, and 1401 to 1412 for the shift level.

5.4.6   OpenStage 15 Key Module

The settings for the key module 15 are the same as those for programmable keys on the phone (see Section 4.4.5.3, "Free Programmable Keys (FPK)").

For this key module, the key numbers represented by the `index` attribute are 501 to 518 for the first level, and 1501 to 1518 for the shift level.

5.4.7   Key click

If this function is activated, a beep tone will sound on every key press.

WBM Name	Item name	Type	Values	Description
Volume	`key-click-volume`	Enumer-ation	0=Off 1=Low 2=Medium 3=High Default: 0 , OS40 US / DPIP35 / DPIP55: 2	Sets the volume of the beep tone. Available with firmware version V2R2.
Keys	`click-keys`	Enumer-ation	0=Keypad only 1=All keys Default: 0	Determines for which keys the beep tone is cre-ated. Available with firmware version V2R2.

5.5   Locality

WBM Name	Item name	Type	Values	Description
Country	`country-iso`	2 character string	See Section 7.2, "Country codes" Default: `GB`, OS40 US / DPIP35 / DPIP55: `US`	Country wherein the phone resides.
Language	`language-iso`	2 character string	See Section 7.3, "Language Codes" Default: `en`, OS40 US / DPIP35 / DPIP55: `en_US`	Language for the user interface.
Date format	`date-format`	Enumeration	`0`=DD.MM.YY `1`=YY-MM-DD `2`=MM/DD/YY Default: `0`, OS40 US / DPIP35 / DPIP55: `2`	Display format for the current date.
Time format	`time-format`	Enumeration	`0`=24 hour; `1`=12 hour (i.e. with AM/PM or language variants); Default: `0 (but depends on country,` OS40 US / DPIP35 / DPIP55: `1`	Display format for the current time.

5.6   Security

See Section 4.10.1.6, "Change User password".

5.7 Diagnostic information

> ℹ️ This function is not available with WPI.

6 Phone Parameters - Provisioning

In this section, those parameters are listed which are neither configurable via local/web interface nor associated with parameters configurable via local/web interface.

6.1 Provisioning Service Related

Item name	Type	Values	Description
`dcmp-enable`	Boolean	`true`/`false` Default: `false`	Determines whether the phone shall wait for contact-me messages from the provisioning service, or poll the provisioning service resp. a special proxy for new configuration data. For further information, please refer to Section 1.3.2, "Firewall and NAT".
`dcmp-url`	Text (URL)	Complete URL, port included Default: NULL	Relevant if `dcmp-enable` is set to `true`. The phone will poll this URL for new configuration data.
`dcmp-interval`	Integer	`1` to `1440` (minutes)	Relevant if `dcmp-enable` is set to `true`. The phone will poll the provisioning service resp. the proxy periodically using this time interval.

6.2 Phone Specific, Hardware Related

Item name	Type	Values	Description

`related-device-type`	Text.
	Max. 50 characters
		`OpenStage 15;`
		`OpenStage 20E;`
		`OpenStage 20;`
		`OpenStage 40;`
		`OpenStage 60;`
		`OpenStage 80`
			Sent to the provisioning service to identify the phone variant. Value is read only. The value is built up during phone start up, querying the hardware variant.
			OpenScape DPIP35 = OpenStage 20, OpenScape DPIP55 G = OpenStage 60

Item name	Type	Values	Description
`device-type`	Text. Max. 50 characters	`OpenStage 15;` `OpenStage 20E;` `OpenStage 20;` `OpenStage 40;` `OpenStage 60;` `OpenStage 80`	Sent to the provisioning service to identify phone variant. Value is read only. Displayed in the web page banner. The value is built up during phone start up, querying hardware variant. OpenScape DPIP35 = OpenStage 20, OpenScape DPIP55 G = OpenStage 60
`gigabit-ethernet-enabled`	Boolean	`true`/`false`	Relevant for OpenStage 20/40/60/80 G / DPIP55G only. Indicates whether the phone's network interface is switched to 1Gb/s speed. Value is read only.
`related-software-type`	Text. Max. 30 characters	`Siemens SIP` [SIP]	Sent to the priovisioning service to identify phone software type. Value is read only.
`software-type`	Text. Max. 30 characters	`Siemens SIP` [SIP]; `Siemens HFA` [HFA]	Sent to the priovisioning service to identify phone software type. Value is read only.
`part-number`	Text. Max. 25 characters		Sent to the priovisioning service to communicate the phone's part number. Value is read only.
`slk-modules`	Integer	For OpenStage 20E and OpenStage 20, the value is always `0`. For OpenStage 15, the value may be 0 or 1. For OpenStage 40 to 80, the value may be `0`, `1` or `2`.	Number of OpenStage Key Modules. Sent to the provisioning service in "ReadAllItems" message response. Value is read only.
`blf-modules`	Integer	For OpenStage SIP phones, the value is always `0`.	Number of BLF Modules. Sent to the provisioning service in "ReadAllItems" message response. Value is read only.

Item name	Type	Values	Description
`km15-modules`	Integer	For OpenStage 10/20/60/80, the value is always 0. For OpenStage 15/40, the value may be `0` or `1`.	Number of OpenStage Key Modules 15. Sent to the provisioning service in "ReadAllItems" message response. Value is read only. Available with firmware version V2.
`slk-module-1-hardware` or `slk-module-2-hardware`	Text	Default: NULL	Sent to the provisioning service in the "ReadAllItems" message response for each SLK key unit connected to phone. Not applicable for a BLF key module unit. Value is read only.
`slk-module-1-version` or `slk-module-2-version`	Text. Max. 7 characters	Default: NULL	Software version of the SLK module. Sent to the provisioning service in "ReadAllItems" message response for each SLK key unit connected to phone. Not applicable for a BLF key module unit. Value is read only.

6.3 Files Stored on the Phone

After a file transfer initiated by the provisioning service is completed, the phone gives feedback to indicate if the transfer has been successful.

Additionally, when the provisioning service sends a "ReadAllItems" request (see Section 3.4.2, "Action Type"), the phone informs about all files that have been deployed.

For each file, the following data are given.

Item name	Type	Values	Description
`file-deployment-status <index>`	Text	`ok`/`failed` Default: NULL	Indicates whether the file transfer has succeeded or failed.
`file-deployment-date <index>`	Text	Default: NULL	Date at which the file has been stored on the phone.
`file-deployment-time <index>`	Text	Default: NULL	Time at which the file has been stored on the phone.
`file-deployment-name <index>`	Text	Default: NULL	Name of the file that has been stored on the phone.
`file-deployment-type <index>`	Text	`MOH` / `PIC` / `LDAP` / `LOGO` / `SCREENSAVER` / `RINGTONE`	Type of the file that has been stored on the phone. For further information, see Section 4.5.3, "Specifications For Media Files and LDAP Templates".

6.4 Network/DNS

Item name	Type	Values	Description
`e164-hostname`	Boolean	`true`/`false` Default: `true`	If activated, the E.164 number is used as the DNS host name for the phone.

6.5 802.1x Security

Item name	Type	Values	Description
`802.1x-authentication`	Enumeration	`001`= EAP-TLS; `002`= PEAP; `099`= None; `255` = respond to all types of challenge where related credentials have been installed; Default: `255`	Type of 802.1x authentication.
`radius-server-validation`	Boolean	`true`/`false` Default: `true`	If `true`, the certificate sent by the RADIUS Server during the EAP-TLS handshake is validated against the CA certificates installed on the phone. If `false`, this check is omitted.
`mschap-identity`	Text	Default: NULL	(For future) Device name for MSCHAP-V2 when using 802.1x authentication methods PEAP or EAP-TTLS.
`mschap-pw`	Text	Default: NULL	(For future) Device password for MSCHAP-V2 when using 802.1x authentication methods PEAP or EAP-TTLS. Requires encrypted storage.
`eap-ttls-digest`	Text	Default: NULL	(For future) Digest for MD5 challenge when using 802.1x authentication method EAP-TTLS.

Item name	Type	Values	Description
`eap-ttls-otp`	Text	Default: NULL	(For future) One time password when using 802.1x authentication method EAPTTLS.
`eap-fast-secret`	Text	Default: NULL	(For future) Shared secret when using 802.1x authentication method EAP-FAST.

6.6　　　　USB

Item name	Type	Values	Description
`usb-access-enabled`	Boolean	`true`/`false` Default: `true`	Allows USB access (for all purposes) to be enabled or disabled from a security perspective.
`usb-backup-enabled`	Boolean	`true`/`false` Default: `true`	Allows user data backup to a USB device and allows such backup data to be restored.

6.7　　　　SIP/System

Item name	Type	Values	Description
`sgnl-route`	Enumeration	`0`=Server; `1`=Gateway (not supported currently); `2`=Direct (not supported currently), Default: `0`	SIP routing method.

6.8　　　　Audio

Item name	Type	Values	Description
`line-rollover-volume`	Integer	`1` to `8` Default: `2`	Volume of the line rollover tone. Can be adjusted by the user via the local menu.

6.9 Feature Keys

Item name	Type	Values	Description
`locked-function-key <index>`	Boolean	`true`/`false` Default: `false`	If `true`, the provisioning service has locked down the key specified by the index. The assigned function and any associated parameters cannot be modified, neither by the user nor Administrator, nor can the key be moved.
`locked-config-menus-<n>`	Boolean	`true`/`false` Default: `false`	If `true`, the function resp. menus specified by <n> is locked for user configuration. For details, please refer to Section 7.4, "Locked Configuration Menus".

6.10 Passwords

Item name	Type	Values	Description
`min-admin-passw-length`	Integer	6 to `24`	Minimum length of the administrator password.
`min-user-passw-length`	Integer	6 to `24`	Minimum length of the user password.

6.11 Provisioning Service Communication

Item name	Type	Values	Description
`dls-chunk-size`	Integer	Default: `5492`	Chunk size for transferring profile data to/from the provisioning service. When the XML message exceeds this size, the message is split into fragments.

6.12 LDAP

Item name	Type	Values	Description
ldap-transport	Enumeration	0=TCP; 1=TLS; Default: 0	Transport Type allows the LDAP interface to be encrypted using TLS (via LDAPS) or unencrypted using TCP LDAP transport

6.13 Certificates

> If a certificate item is empty, then this implies the certificate at that index is to be deleted.

Item name	Type	Values	Description
application-server-ca <index=0>	PEM file (single certificate or certificate chain)	Note: If the XML item received from the provisioning service is empty, the corresponding certificate at the phone will be deleted.	For HTTPS access to one or more application servers (XML applications). This certificate enables the phone to verify the authenticity of an application server. Certificates in the item replace existing certificates.
application-server-ca <index=1>	PEM file (single certificate or certificate chain)	Note: If the XML item received from the provisioning service is empty, the corresponding certificate at the phone will be deleted.	To support transition in case the certificate on the application server should change to a certificate signed by a new CA.
wbm-server-certificate	Passphrase protected PKCS#12 file (single certificate + private key + optional certificate of signing CA	Note: If the XML item received from the provisioning service is empty, the corresponding certificate at the phone will be deleted.	For secure communication with phone's web server. The optional certificate is available for the Web Browser to import. Also used for the HTTPS connection with the provisioning service when listening for contact-me requests.

Item name	Type	Values	Description
`wbm-server-certificate-info`	PEM file (single certificate)	Note: If the XML item received from the provisioning service is empty, the corresponding certificate at the phone will be deleted.	Created from `wbm-server-certificate` (removing private key and optional CA certificate).
`voip-server-ca <index=0>`	PEM file (single certificate or certificate chain)	Note: If the XML item received from the provisioning service is empty, the corresponding certificate at the phone will be deleted.	SIP server CA certificate, used to secure TLS interface with SIP server.
`voip-server-ca <index=1>`	PEM file (single certificate or certificate chain)	Note: If the XML item received from the provisioning service is empty, the corresponding certificate at the phone will be deleted.	Next server CA certificate, to support transition in case the certificate on the SIP server should change to a certificate signed by a new CA.
`802.1x-certificate`	Passphrase protected PKCS#12 file (single certificate + private key)	Note: If the XML item received from the provisioning service is empty, the corresponding certificate at the phone will be deleted.	RADIUS supplicant credentials, for 802.1x network access (using EAP-TLS). Used to authenticate the phone to RADIUS server. The certificate subject has to match the account for the phone in the authentication server with which the RADIUS server interacts.
`802.1x-certificate-info`	PEM file (single certificate)	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	RADIUS supplicant certificate. Created from 802.1x-certificate (removing private key).

Item name	Type	Values	Description
`radius-server-ca1`	PEM file (single certificate or certificate chain)	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Current RADIUS server CA certificate. For 802.1x network access (using EAP-TLS, PEAP or EAP-TTLS). To allow phone to verify certificate received from RADIUS server. Stored as encrypted within DAS only. Certificate Management knows the decryption key.
`radius-server-ca2`	PEM file (single certificate or certificate chain)	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Next RADIUS server CA certificate, to support transition in case the certificate on the RADIUS server should change to a certificate signed by a new CA.
`send-url-server-ca <index=0>`	PEM file (single certificate or certificate chain)	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	First certificate to enable a secure connection with the web server specified for the "send URL" function (see Section 4.4.5.3, "Send URL"). Available with firmware version V2.
`send-url-server-ca <index=1>`	PEM file (single certificate or certificate chain)	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Second certificate to enable a secure connection with the web server specified for the "send URL" function (see Section 4.4.5.3, "Send URL"). Available with firmware version V2.
`send-url-server-ca <index=2>`	PEM file (single certificate or certificate chain)	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Third certificate to enable a secure connection with the web server specified for the "send URL" function (see Section 4.4.5.3, "Send URL"). Available with firmware version V2.

Item name	Type	Values	Description
`dls-client-certificate`	PEM file (single certificate)	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Provisioning service provides phones with client certificate for phone Secure Mode
`dls-server-ca<index=0>`	PEM file (single certificate or certificate chain	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Provisioning service provides phones with server CA for phone Secure Mode
`dls-server-ca<index=1>`	PEM file (single certificate or certificate chain	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Provisioning service provides phones with server CA for phone Secure Mode
`https-server-ca<index=0>`	PEM file (single certificate or certificate chain	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Provisioning service or Secure Configuration Download only. Write and read. (Config. Server does not read back).
`https-server-ca<index=1>`	PEM file (single certificate or certificate chain	Note: If the XML item received from the provisioning service is empty, this means delete the corresponding certificate at the phone.	Provisioning service or Secure Configuration Download only. Write and read. (Config. Server does not read back).

6.14   Call Log

Item name	Type	Values	Description
`clear-calllog`	Boolean	`true`/`false` Default: `false`	When the phone receives this parameter with the value set to `true`, the call log will be deleted. In case the value should be set to `false`, the phone will ignore the parameter. On a read request from the provisioning server, the phone will always return `false`. Please note that all redial numbers will be deleted when the call log is cleared. Available with firmware version V2R1.

6.15   Diagnostics

Item name	Type	Values	Description
`allow-user-access-to-diagnostic-data`	Boolean	`true`/`false` Default: `true`	If set to true, extended phone data is displayed to the user. To view the data, the user must click on the "Diagnostic information" link in the user menu.

6.16 Phone Location

Item name	Type	Values	Description
ng911-location-ca	String	Civic Address element in a CSV format	CSV element format according to LLDP-MED Standard ANSI/TIA-1057/ANNEX B: <CAtype>=<location string>, Note: CAtype 0 represents the country in this data item rather than the language as specified for LLDP-MED Standard. Example: ng911-location-ca = "0=DE,3=Munich,19=51,34=Hofmannstraße, 22=Room 100,27=1". See also Section 4.6.3.4, "Phone location"
ng911-location-source	Enumeration	0=unknown/not set; 1=LLDP-MED; 2=DLS; Default: 0	Sets the source of phone location information

7 Appendix

7.1 XML Schemas

This sections provides the XML schemas to be associated with the message structures described in Section 3, "Basic Communication Procedures".

7.1.1 Common Message Elements

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:dls="http://www.siemens.com/DLS"
   targetNamespace="http://www.siemens.com/DLS"
   elementFormDefault="qualified">
   <xsd:annotation>
      <xsd:documentation xml:lang="en">
         Common types
      </xsd:documentation>
   </xsd:annotation>
   <xsd:simpleType name="ActionType">
      <xsd:restriction base="xsd:string">
         <xsd:enumeration value="ReadAllItems"/>
         <xsd:enumeration value="ReadItems"/>
         <xsd:enumeration value="WriteItems"/>
         <xsd:enumeration value="Restart"/>
         <xsd:enumeration value="FileDeployment"/>
         <xsd:enumeration value="SoftwareDeployment"/>
         <xsd:enumeration value="CleanUp"/>
         <xsd:enumeration value="GetNextFragment"/>
      </xsd:restriction>
   </xsd:simpleType>
   <xsd:simpleType name="FragmentType">
      <xsd:restriction base="xsd:string">
         <xsd:enumeration value="next"/>
         <xsd:enumeration value="final"/>
      </xsd:restriction>
   </xsd:simpleType>
   <xsd:complexType name="ItemListType">
      <xsd:sequence>
         <xsd:element name="Item" type="dls:ItemType" nillable="true"
         minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
   </xsd:complexType>
```

```
<xsd:complexType name="ItemType">
   <xsd:simpleContent>
      <xsd:extension base="xsd:string">
         <xsd:attribute name="name" type="xsd:string"/>
         <xsd:attribute name="index" type="xsd:string"
         use="optional"/>
         <xsd:attribute name="type" type="xsd:string"
         use="optional"/>
         <xsd:attribute name="status" type="xsd:string"
         use="optional"/>
      </xsd:extension>
   </xsd:simpleContent>
</xsd:complexType>
</xsd:schema>
```

7.1.2   Phone Message

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:dls="http://www.siemens.com/DLS"
   targetNamespace="http://www.siemens.com/DLS"
   elementFormDefault="qualified">
   <xsd:annotation>
      <xsd:documentation xml:lang="en">
         DLS upstream schema
      </xsd:documentation>
   </xsd:annotation>
   <xsd:include schemaLocation="common.xsd"/>
   <xsd:element name="WorkpointMessage"
   type="dls:WorkpointMessageType" />
   <xsd:complexType name="WorkpointMessageType">
      <xsd:sequence>
         <xsd:element name="Message" type="dls:WPMessageType"/>
      </xsd:sequence>
   </xsd:complexType>
   <xsd:complexType name="WPMessageType">
      <xsd:sequence>
         <xsd:element name="ReasonForContact"
         type="dls:ReasonForContactType"/>
         <xsd:element name="ItemList" type="dls:ItemListType"
         minOccurs="0" maxOccurs="1"/>
      </xsd:sequence>
      <xsd:attribute name="nonce" type="xsd:hexBinary"/>
      <xsd:attribute name="maxItems" type="xsd:int" use="optional"/>
      <xsd:attribute name="fragment" type="dls:FragmentType"
      use="optional"/>
   </xsd:complexType>
   <xsd:complexType name="ReasonForContactType">
      <xsd:simpleContent>
         <xsd:extension base="dls:ReasonType">
            <xsd:attribute name="action" type="dls:ActionType"
            use="optional"/>
            <xsd:attribute name="status" type="dls:StatusType"
            use="optional"/>
         </xsd:extension>
      </xsd:simpleContent>
   </xsd:complexType>
   <xsd:simpleType name="ReasonType">
      <xsd:restriction base="xsd:string">
```

```
            <xsd:enumeration value="start-up"/>
            <xsd:enumeration value="local-changes"/>
            <xsd:enumeration value="inventory-changes"/>
            <xsd:enumeration value="status"/>
            <xsd:enumeration value="solicited"/>
            <xsd:enumeration value="reply-to"/>
            <xsd:enumeration value="clean-up"/>
            <xsd:enumeration value="get-next-fragment"/>
        </xsd:restriction>
    </xsd:simpleType>
    <xsd:simpleType name="StatusType">
        <xsd:restriction base="xsd:string">
            <xsd:enumeration value="accepted"/>
            <xsd:enumeration value="failed"/>
            <xsd:enumeration value="busy"/>
        </xsd:restriction>
    </xsd:simpleType>
</xsd:schema>
```

7.1.3   Provisioning Service Message

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:dls="http://www.siemens.com/DLS"
   targetNamespace="http://www.siemens.com/DLS"
   elementFormDefault="qualified">
   <xsd:annotation>
      <xsd:documentation xml:lang="en">
         DLS downstream schema
      </xsd:documentation>
   </xsd:annotation>
   <xsd:include schemaLocation="common.xsd"/>
   <xsd:element name="DLSMessage" type="dls:DLSMessageType"/>
   <xsd:complexType name="DLSMessageType">
      <xsd:sequence>
         <xsd:element name="Message" type="dls:MessageType"/>
      </xsd:sequence>
   </xsd:complexType>
   <xsd:complexType name="MessageType">
      <xsd:sequence>
         <xsd:element name="Action" type="dls:ActionClass"/>
         <xsd:element name="ItemList" type="dls:ItemListType"
         minOccurs="0" maxOccurs="1"/>
      </xsd:sequence>
      <xsd:attribute name="nonce" type="xsd:hexBinary"/>
      <xsd:attribute name="fragment" type="dls:FragmentType"
      use="optional"/>
   </xsd:complexType>
   <xsd:complexType name="ActionClass">
      <xsd:simpleContent>
         <xsd:extension base="dls:ActionType">
            <xsd:attribute name="status"
            type="dls:ActionStatusType" use="optional"/>
         </xsd:extension>
      </xsd:simpleContent>
   </xsd:complexType>
   <xsd:simpleType name="ActionStatusType">
      <xsd:restriction base="xsd:string">
         <xsd:enumeration value="ambiguous-phone-number"/>
         <xsd:enumeration value="reg-addr-undefined"/>
      </xsd:restriction>
   </xsd:simpleType>
</xsd:schema>
```

7.2 Country codes

- Argentina - `AR`

- Australia - `AU`

- Austria - `AT`

- Belgium - `BE`

- Brazil - `BR`

- Canada - `CA`

- Chile - `CL`

- China - `CN`

- Croatia - `HR`

- Czech Republic - `CZ`

- Denmark - `DK`

- Finland - `FI`

- France - `FR`

- Georgia - `GE`

- Germany - `DE`

- Hungary - `HU`

- India - `IN`

- Ireland - `IE`

- Italy - `IT`

- Japan - `JP`

- Luxembourg - `LU`

- Mexico - `MX`

- Netherlands - `NL`

- New Zealand - `NZ`

- Norway - `NO`

- Poland - `PL`

- Portugal - `PT`

- Republic of Korea - `KR`

- Russian Federation - `RU`

- Singapore - `SG`

- Slovakia - `SK`

- South Africa - `ZA`

- South Korea - `KR`

- Spain - `ES`

- Sweden - `SE`

- Switzerland - `CH`

- Thailand - `TH`

- Turkey - `TR`

- United Kingdom - `GB`

- United States - `US`

7.3 Language Codes

- Brazilian (= Portuguese) - `pt_Br`

- Bulgarian - `bg`

- Catalan - `ca`

- Chinese - `zh`

- Croatian - `hr`

- Czech - `cs`

- Danish - `da`

- Dutch - `nl`

- English (GB) - `en`

- English (US) - `en_US`

- Estonian - `et`

- Finnish - `fi`

- French - `fr`

- German - `de`

- Greek - `el`

- Hungarian - `hu`

- Indonesian - `id`

- Italian - `it`

- Japanese - `ja`

- Korean - ko

- Latvian - `lv`

- Lithuanian - `lt`

- Macedonian - `mk`

- Malayan - `ms`

- Norwegian - `no`

- Polish - `pl`

- Portuguese - `pt`

- Romanian - `ro`

- Russian (Cyrillic characters) - `ru`

- Serbian (Cyrillic characters) - `sr_Cyrl`

- Serbian (Latin characters) - `sr_Latn`

- Slovak - `sk`

- Slovenian - `sl`

- Spanish - `es`

- Swedish - `sv`

- Turkish - `tr`

- Welsh - `cy`

7.4 Locked Configuration Menus

The following functions resp. menus can be locked, so that the user can not modify the settings.

7.4.1 Local

Feature/Menu	Item name	Description
Country options	`locked-config-menus-01`	Select a country from a list to adapt the phone to country specific conditions.
Language	`locked-config-menus-02`	Set the language for the user menu.

7.4.2 Display Settings

Feature/Menu	Item name	Description
Display Skin	`locked-config-menus-65`	Choose the display theme.
Screen Saver	`locked-config-menus-66`	Activate and configure the phones's screensaver.
Call context menu	`locked-config-menus-67`	Control the behaviour of the call context menu.

7.4.3 Clock Settings

Feature/Menu	Item name	Description
Date display format	`locked-config-menus-03`	Select date and time format.
Daylight saving	`locked-config-menus-14`	Enable and configure daylight saving.

7.4.4   Telephony Features

Feature/Menu	Item name	Description
Auto answer	`locked-config-menus-32`	Enable auto answer.
Auto answer beep	`locked-config-menus-33`	Enable beep on auto answer.
Auto reconnect	`locked-config-menus-34`	Enable auto reconnect.
Auto reconnect beep	`locked-config-menus-35`	Enable beep on auto reconnect.
Idle display static	`locked-config-menus-36`	Enables and configures indication of system messages in idle state on display
Inactivity timeout	`locked-config-menus-38`	Enables and configures timespan for return to idle state after last entry
APM/DSM Call view	`locked-config-menus-39`	Enables call view on application module (optiPoint only)
USB keyboard type	`locked-config-menus-40`	Enables modification of USB keyboard (optiPoint only)
Transfer on hangup	`locked-config-menus-57`	Enable transfer on hangup.
Join in conference	`locked-config-menus-63`	Allow joining in a conference.
Immediate dialling (hot keypad dialling)	`locked-config-menus-48`	Allow immediate dialling.
Call Deflection	`locked-config-menus-04`	Allow call deflection.
Call Waiting	`locked-config-menus-08`	Allow call waiting.
Call Transfer	`locked-config-menus-09`	Allow call transfer.
Transfer on ring	`locked-config-menus-53`	Enable transfer on ring.
Mobility LED flash	`locked-config-menus-54`	Allows LED flashing during mobility logon /logoff
Call Join	`locked-config-menus-10`	Enable call joining.

Feature/Menu	Item name	Description
Do Not Disturb	`locked-config-menus-19`	Enable Do Not Disturb (DND).
Message waiting	`locked-config-menus-20`	Enables LED indication of new messages in mailbox
Hold Ringback	`locked-config-menus-21`	Enable ringback for calls on hold.
Conference	`locked-config-menus-22`	Enables system based conferences (optiPoint only)
Busy when dialling	`locked-config-menus-52`	When enabled, the phone will send a busy signal to any calling party when the user is dialling.
Call back busy	`locked-config-menus-49`	Enable a callback request when the called is busy.
Call back on ring/no reply	`locked-config-menus-50`	Enable a callback request when the called does not reply.
Idle missed calls	`locked-config-menus-51`	Allows notification of missed calls on display
User conferencing enabled	`locked-config-menus-23`	Enable local conferences.
Autodial timer	`locked-config-menus-15`	Configure the auto dial timer.
Call Forwarding on No Reply delay	`locked-config-menus-16`	Set the delay for call forwarding on no reply.
Hold Ringback timer (minutes)	`locked-config-menus-17`	Set the time interval after which the user will be reminded of a held call.
Open Listening audio mode	`locked-config-menus-61`	Enable loudspeaker for open listening.
Deflect default destination URI	`locked-config-menus-43`	Set the default address for call deflection.
Line Settings	`locked-config-menus-44`	Enables modification of line keys
Call view icons	`locked-config-menus-45`	Determines the indication of calls (optiPoint only)
Call park	`locked-config-menus-46`	Allow call parking
Call pickup	`locked-config-menus-47`	Allow call pickup

Feature/Menu	Item name	Description
Indication of for-warded calls	`locked-config-menus-62`	Enable a visual and acoustic alert when a call is being forwarded.
Secure call alert en-abled	`locked-config-menus-56`	Enable an alert on insecure calls.
Call Forwarding	`locked-config-menus-05`	Control and configure call fowarding.
Log forwarded calls	`locked-config-menus-06`	Logs the fowarded calls.
Call Duration	`locked-config-menus-07`	Enables the indication of call duration on display.
Contrast	`locked-config-menus-11`	Enables the contrast setting on display.
Dialing Mode	`locked-config-menus-12`	Enables to determine whether dialing by number or by name (optiPoint only).
Call Display	`locked-config-menus-13`	Controls which information about the caller of an incoming call are to be displayed
Toggle associate	`locked-config-menus-69`	Enables toggle on held calls and connection after hook-on
Forwarding party display	`locked-config-menus-70`	Determines for multiple forwarding which party will be displayed
Headset	`locked-config-menus-71`	Enables and configures type of headset (Open-Stage 40/60/80 only)
Key klick	`locked-config-menus-72`	Enables and configures mode of key klick (Open-Stage 40/60/80 only)
Call Log Enabled	`locked-config-menus-73`	Enables Call Log
Hold and Hangup	`locked-config-menus-74`	Enables the 'Hold and Hangup' notification (Non-Keyset OpenStage only)
Lower IL alert notifi-cation	`locked-config-menus-75`	Enables the 'Lower Impact Level' notification
Video on	`locked-config-menus-76`	Enables the video functionality
Missed Logging	`locked-config-menus-77`	Enables the missed logging functionality
Display Brightness	`locked-config-menus-78`	Controls the display brightness

Feature/Menu	Item name	Description
Backlight Timeout Energy Saving Display	`locked-config-menus-79`	Controls the screensaver timeout
Special ringer-Internal	`locked-config-menus-80`	Controls the ringer played for a limited range of special incoming calls where the type of call is signalled to the phone.
Special ringer-External	`locked-config-menus-81`	See above Special ringer-Internal
Special ringer-Recall	`locked-config-menus-82`	See above Special ringer-Internal
Special ringer-Emergency	`locked-config-menus-83`	See above Special ringer-Internal
Special ringer-Special 1	`locked-config-menus-84`	See above Special ringer-Internal
Special ringer-Special 2	`locked-config-menus-85`	See above Special ringer-Internal
Special ringer-Special 3	`locked-config-menus-86`	See above Special ringer-Internal

7.4.5 Audio Settings

Feature/Menu	Item name	Description
Ringer	`locked-config-menus-60`	Set melody, tone sequence, and audio file for the ringer.
Music on Hold (MoH)	`locked-config-menus-18`	Enable music on hold.

7.4.6 Busy Lamp Fields (BLF)

Feature/Menu	Item name	Description
BLF alert	`locked-config-menus-68`	Enable an audible and visible alert on an incoming call for the call number supervised by the BLF key.

7.4.7 Passwords

Feature/Menu	Item name	Description
Set user password	`locked-local-function-menus-02`	Set/modify the user password.

7.4.8 Phone Lock

Feature/Menu	Item name	Description
Phone lock	`locked-local-function-menus-03`	Lock the phone.

7.4.9 Bluetooth Settings

Feature/Menu	Item name	Description
Bluetooth	`locked-config-menus-64`	Control and configure Bluetooth.

7.4.10 Call Recording Settings

Feature/Menu	Item name	Description
Call recording	`locked-config-menus-55`	Control and configure call recording.

7.5 Glossary

Term/Abbreviation	Definition/Description
Bootstrapping	Process that raises the interface security between devices and provisioning service from Default Mode to Secure Mode.
HTTP	**H**yper**T**ext **T**ransport **P**rotocol. Used for contact-me messages issued by the provisioning service.
HTTPS	**H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. Used for XML data exchange between provisioning service and OpenStage phones.
MAA	**M**ultiple **L**ine **A**ppearance. When operating in MAA mode, a single phone can handle multiple lines.
PIN	**P**ersonal **I**dendification **N**umber. Concatenation of password and TAN. Generated by provisioning service to be used in Secure Mode. The password is used to protect the sensitive data during bootstrapping.
SIP	**S**ession **I**nitiation **P**rotocol. Used for call signaling by OpenStage phones.
TAN	**T**arget's **A**uthentication **N**umber. Last 3 characters of PIN to be used by provisioning service to authenticate the target device in Secure Mode.
TCP	**T**ransport **C**ommunication **P**rotocol. Underlying protocol for HTTP.
TLS	**T**ransport **L**ayer **S**ecurity. Used as a security layer between TCP and HTTP to form HTTPS.
URI	**U**niversal **R**esource **I**ndicator.
URL	**U**niversal **R**esource **L**ocator.
VoIP	**V**oice **o**ver **IP**. Implementation of telephony using IP networks instead of traditional technologies applied in the PSTN.
WBM	**W**eb **B**ased **M**anagement. Web interface for configuring the phone. It is used via a standard web browser.
XML	E**X**tensible **M**arkup **L**anguage.