



KIRK Release Note
KWS300

Firmware Version PCS05B_
Q2/2010

Table of Contents

1. GENERAL	1
1.1 IMPORTANT NOTES	1
1.2 FEATURE LICENSE AND PLATFORM LIMITATIONS	1
1.3 SYSTEM REQUIREMENTS.....	1
2. DISTRIBUTION FILES	1
3. CHANGES	1
3.1 VERSION PCS05B_ Q2-2010.....	1
3.1.1 <i>Added or Changed Features</i>	1
3.1.2 <i>Removed Features</i>	2
3.1.3 <i>Corrections</i>	2
3.1.4 <i>Configuration File Parameter Changes</i>	2
3.2 VERSION PCS05_ Q1 - 2010.....	3
3.2.1 <i>Added or Changed Features</i>	3
3.2.2 <i>Removed Features</i>	4
3.2.3 <i>Corrections</i>	4
3.2.4 <i>Configuration File Parameter Changes</i>	5
3.3 VERSION PCS04B_ - OCTOBER 20, 2009.....	7
3.3.1 <i>Added or Changed Features</i>	7
3.3.2 <i>Removed Features</i>	7
3.3.3 <i>Corrections</i>	7
3.3.4 <i>Configuration File Parameter Changes</i>	7
3.4 VERSION PCS04A_ - OCTOBER 12, 2009.....	7
3.4.1 <i>Added or Changed Features</i>	7
3.4.2 <i>Removed Features</i>	7
3.4.3 <i>Corrections</i>	7
3.4.4 <i>Configuration File Parameter Changes</i>	8
3.5 VERSION PCS04_ Q4-2009	8
3.5.1 <i>Added or Changed Features</i>	8
3.5.2 <i>Removed Features</i>	9
3.5.3 <i>Corrections</i>	9
3.5.4 <i>Configuration File Parameter Changes</i>	9
3.6 VERSION PCS03B_ Q3-2009.....	11
3.6.1 <i>Added or Changed Features</i>	11
3.6.2 <i>Removed Features</i>	11
3.6.3 <i>Corrections</i>	11
3.6.4 <i>Configuration File Parameter Changes</i>	13
3.7 VERSION PCS03A_ Q2-2009	13
3.7.1 <i>Added or Changed Features</i>	13
3.7.2 <i>Removed Features</i>	13
3.7.3 <i>Corrections</i>	13
3.7.4 <i>Configuration File Parameter Changes</i>	14
3.8 VERSION PCS03_ Q1-2009	14
3.8.1 <i>Added or Changed Features</i>	14

3.8.2	<i>Removed Features</i>	15
3.8.3	<i>Corrections</i>	15
3.8.4	<i>Configuration File Parameter Changes</i>	15
3.9	VERSION PCS02_ Q4-2008	17
3.9.1	<i>Added or Changed Features</i>	17
3.9.2	<i>Removed Features</i>	18
3.9.3	<i>Corrections</i>	18
3.10	VERSION PCS01B_.....	18
4.	OUTSTANDING ISSUES	18

1. General

These release notes apply to released versions of the KWS300 Firmware. This version specifically applies to version PCS05B_ of the firmware. This release replaces the PCS05__ release as the latest generally available (GA) release.

1.1 Important Notes

- Starting from PCS05B_ the KWS300 is produced with DHCP enabled per default. Previously the default setting was a static IP address. This only affects new devices and not devices that are upgraded. The change is performed in response to customer demands.
- If downgrading from PCS04A_ or newer to PCS04__ or older the firmware needs to be loaded and rebooted twice to work correctly.
- If upgrading from PCS01B__ to a newer version and subsequently downgrading from the newer version back to PCS01B__ the user database will be lost. It will however be possible to restore a backup made while running PCS01B__.

1.2 Feature License and Platform Limitations

None.

1.3 System Requirements

Hardware Platform:	Description
KWS300 HW PCS 10 or newer	KWS300 Server

2. Distribution Files

Click [here >>](#) to find the firmware image of the KWS300.

3. Changes

3.1 Version PCS05B_ Q2-2010

3.1.1 Added or Changed Features

- Default DHCP: Starting from this release the KWS300 is produced with DHCP enabled instead of a static IP address. This only affects new devices and not devices that are upgraded.
If the KWS300 fails to retrieve IP configuration via DHCP it will fall back to the static IP address 192.168.0.1.
The IP address of the device can easily be discovered using UPnP.
- Support handling of pauses in phone numbers: This makes it possible to include pauses in dialed phone numbers. If pauses are added in a phone number the part before the first pause is sent in an INVITE and the KWS will wait for a 200 OK before sending the pauses and the rest of the number via DTMF. Typical applications for this feature are nurse call system integration or voicemail applications. As an example it is now possible to store the following number in the

phonebook/speed dial.

“5555pp8888#” where

- 5555 could be the number to the voice mail application.
- pp would indicate two pauses (this would give the voicemail application time to send out a new dial tone and be ready to receive an access code.
- 8888# would be the access code.

Phone numbers including pauses can be entered on the handset or received as call back numbers via the XML-RPC application interface or MSF application interface (a comma “,” or a p “p” can be used to denote a pause in a call-back number).

- Added syslog facility configuration: This makes it possible to configure the source facility used for syslog messages. The default is local0. For further details on remote syslog facilities refer to RFC5424.
- The internal messaging feature added in firmware PCS05__ has been improved: Previously, internal messages were echoed on the XML-RPC application interface, this is removed.
- Reduced production time: Due to increasing demand and increasing amount of delivered devices the initial creation of an empty file system has been optimized. This only impacts the production process and has no impact on devices in the field.

3.1.2 Removed Features

None

3.1.3 Corrections

- Fixed problem with local call forward in a setup with local call forward enabled and call waiting disabled.
In this setup if a user is in an active call, and a second call is received the system previously would send busy to the second caller. This is now corrected so a second caller will be forwarded.
- Mask DECT high priority bit to remove problem with subscribing some Bosch handsets.
- Eliminated potential memory leak when failing to decode SIP replaces header.

3.1.4 Configuration File Parameter Changes

config.xml	Added	config.log.syslog.facility	Used to specify the remote syslog facility used for log messages. Refer to RFC5424 for details. Values: The facility number to be used for the device. An integer between 0 and 23. Default: 16 (“local 0”)
------------	-------	----------------------------	---

3.2 Version PCS05__ Q1 - 2010

3.2.1 Added or Changed Features

- Call waiting is now supported. It must be enabled to be active (default off). Call waiting is supported on the whole range of Polycom DECT Handsets. However, due to differences in keyboard layout, audio processing capabilities and display types, the appearance (audio as well as visual) differs between the different handsets. The solution implemented is a trade-off between back-ward compatibility and appearance. Note: The 5020 and 5040 handsets require firmware PCS_08Ca or newer.

Accepting a new call: If call waiting is enabled a second call can be accepted by pressing “R”, in which case the other end will be set on hold and a connection will be established to the new/call waiting caller.

Rejecting a new call: Pressing left arrow/ok button will reject the call waiting call.

Ending the old call and taking the new call: Pressing on-hook while the second call (the call waiting call) is alerting, will terminate the old call and the handset will start/continue ringing. It is now possible to answer the new call.

Ending an established call (if two calls are active):

- If two calls are established due to call transfer pressing on-hook will complete a call transfer.

- If two calls are established due to an incoming Call Waiting which is accepted, pressing on-hook will terminate both calls.

Toggle between two active calls: Pressing “R” will toggle between two active calls.

Ending the active call if two calls are present: Pressing left arrow/ok button will terminate the current call (but not the second call).

- Add Message Waiting Indication (MWI) for the 2010 handset. With this addition Message Waiting Indication is supported on the complete range of Polycom DECT handsets.
- Local call forward (unconditional) is now supported. The number to forward to is configurable from the web-GUI as well as directly from the handset. Using the web-gui the Local Call Forward number can be viewed/edited directly from the user entry of the user in question. The feature code for enabling/disabling local call forward from the handset can be configured from the “Configuration|Wireless Server” menu. The default code is “*21*\$#” where “\$” denotes the number to forward to. If a handset has call forward enabled the standby text will be pre-pended with (CFU) to give the user an indication that the handset is forwarded.
- It is now possible to disconnect the active call if two calls are active (either due to an attended call transfer, or due to an accepted call waiting call). If two calls are active pressing left-arrow will disconnect the active call (without disconnecting the in-active call).
- Increased string lengths for SIP parameters.
 - Default domain 32 -> 256.
 - User name 32 -> 64.
 - User domain 32 -> 64.
 - User authentication 32 -> 64.

- Introduced remote syslog (RFC5424) via UDP. The remote syslog allows for using a PC to receive messages/logging from a KWS.
- Added internal messaging for sending text messages between handsets without requiring an external application.
The feature is enabled per default but can be disabled if it interferes with an external application.
- Failure to read ARI is now logged as EMERGENCY (was KSF_CRITICAL).
- MSF/XML-RPC: Release DECT connection immediately when a PP_STATUS_ind initiated by the handset is received.
- Support for advanced messaging features introduced. This includes MSF_SMS_SETUP_req (MSF format 3) and support for MSF_SMS_RESPONSE_ind & ExtenHwReq/Cfm. These features will become available with the release of the upcoming next-generation handset series (the 60xx and 70xx series). The advanced features include alarm buttons, tear-off cord, multicolour LED controllable from an application and motion sensor etc.
- Do not send XML-RPC/MSF messages to a handset while messages are queued for the handset.
- Added XML-RPC endpoint_release event.
- Provisioning improved detection of firmware version inconsistency to avoid problems if firmware is updated manually.
- Provisioning is made more verbose. Download of users, firmware and configuration from a provisioning server is now logged to the message log.
- Also log line number when failing to parse users.xml.
- Do not stop user import if displayname or standby text is invalid or too long - just skip or truncate and log a message.
- Do not abort provisioning process when one of the steps fails.
- When exporting logs, the message log is stored in clear text. The message log can now be read with standard software.
- Improved logging of SIP failures.
- Improve log export speed.
- Attended transfer: Send the REFER to inactive dialog instead of active. This is required by Siemens HiPath and Toshiba.
- Create a KSF log on RFP crash.

3.2.2 Removed Features

- None

3.2.3 Corrections

- Add double-quotes to SIP display names to allow special characters and international letters. This is required by the RFC and e.g. Cisco Call Manager.
- Fixed problem with provisioning polling interval. This could result in the fact that the device stopped polling for updates.
- Increase SIP dialog local cseq when a request is re-send. This solves a problem with mid-dialog authentication of requests. The problem was originally seen with a Nortel IPBX (DECT-142).
- Do not require that a SIP dialog is established when 180 Ringing is received. Fixes problem with missing dialog parameters for Aastra and Splice.com.

- Fixed resolver CNAME problem. DNS CNAME records now supported.
- Handle a comma(,) in the username part of the URI in a Refer-To header (DECTESC-167).
- Removed a lot of unnecessary writes to the flash. These induced unnecessary tear on the flash, especially during boot.
- Changing sip.media.symmetric setting would issue an error in the message log: “Unknown SIP configuration key: sip.media.symmetric”, this is fixed.
- XML-RPC: Fixed problem with zero length data in PP_STATUS_ind.
- Removed a few large buffers from the stack. These may have caused sporadic failures.
- Minor NTP client improvement which reduces the amount of “NTP failed” errors in the log.
- XML-RPC/MSF: Handle PP_STATUS_req/ind in more states.
- Report SIP transaction failed if decoding the unauthorized header fails.
- Re-classified some log messages.
- Removed memory leak when receiving a SIP MESSAGE.
- Validate configuration keys when setting them. This avoids malforming the config.xml.
- Improved logging of failures in connection with the DNS resolver.
- MSF: Handle XML escaped characters correctly for incoming messages.
- XML-RPC/MSF: Clean up release reasons to comply with the documentation. Normal release reasons (0x00) are unchanged but the values of other release reasons have changed. For XML-RPC refer to the XML-RPC SDK version 1.1 or later for details.
- Fixed problem with UPnP UUID not being unique. If more devices on the network have the same UUID only one of them will be shown when UPnP devices are listed.
- Fixed problem with device not falling back to static IP address when DHCP fails.

3.2.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	config.log.syslog.host	Specifies the remote syslog server host address. Default: Empty
config.xml	Added	config.log.syslog.port	Used to specify the remote port of the syslog server. Values: The port number on a remote syslog server. Default: Empty which

			defaults to 514
config.xml	Added	config.feature_codes.enable	Used to enable/disable local handling of feature codes. Values: true/false Default: false
config.xml	Added	config.feature_codes.call_forward.unconditional.enable	Used to specify the feature code used for enabling unconditional call forward (CFU). Values: The feature code users must dial to enable unconditional call forward. Default: *21*\$.
config.xml	Added	config.feature_codes.call_forward.unconditional.disable	Used to specify the feature code used for disabling unconditional call forward (CFU). Values: The feature code users must dial to disable unconditional call forward. Default: #21#.
config.xml	Added	config.application.internal_messaging	Used to control if messaging between handsets is handled internally or

			by an external application. If enabled messages will be handled internally. Values: true/false Default: true
--	--	--	---

3.3 Version PCS04B_ - October 20, 2009

3.3.1 Added or Changed Features

- None

3.3.2 Removed Features

- None

3.3.3 Corrections

- Removed potential RFP problem present in firmware PCS04__ and PCS04A_. This problem would result in the loss of all active calls on the KWS and a subsequent restart of the RFP process.
- Corrected handling of re-configuration of media with re-INVITE. For example, placing a call on and off hold could cause voice problems in other calls on the same KWS.

3.3.4 Configuration File Parameter Changes

- None

3.4 Version PCS04A_ - October 12, 2009

3.4.1 Added or Changed Features

- None

3.4.2 Removed Features

- None

3.4.3 Corrections

- Corrected missing radio firmware update when using provisioning. In previous versions of the firmware the device will continue to use an old radio firmware if the firmware is updated using automatic provisioning. If using provisioning for upgrading firmware and then enabling encryption, this would cause problems.
- Corrected provisioning check at specific time.

If the device was configured to check for updates at a specific time each day the device would only check for updates twice.

- XML-RPC application interface: The method `end_call_display()` ignored the `setupspec1` parameter.
- Corrected the user-agent name for the HTTP provisioning client. The previous firmware presented the KWS300 as a KWS6000.
- Removed memory leak related to DECT encryption. After handling 100,000 calls with DECT encryption the device will run out of memory.

3.4.4 Configuration File Parameter Changes

- None

3.5 Version PCS04__ Q4-2009

3.5.1 Added or Changed Features

- Added support for entering more SIP proxies for failover and load balancing. This feature is relevant in a setup with more than one SIP proxy. In this case, it is now possible to manually enter the SIP URI of the proxies, in earlier releases this could only be done with DNS-SRV.
- Added UPnP for discovery of devices. UPnP is an acronym for Universal Plug and Play. If for some reason the IP-address of the device is unknown (e.g. forgotten or DHCP-assigned), UPnP can be utilized to easily identify the IP-address of the device. If “My Network Places” in Windows is setup to show icons for networked UPnP devices, every KWS300/6000, Media-resource and Base station will be present in “My Network Places”.
- Added method for manipulating settings by requesting an URL.
 - `http[s]://<host>/config/get?<key>` –
`http://192.168.0.1/config/get?sip.proxy.domain`
 - `http[s]://<host>/config/set?<key>=<value>` –
`http://192.168.0.1/config/set?sip.proxy.domain=example.com`
- Improved jitter buffer. The sound quality on IP-connections experiencing jitter issues is improved considerably.
- Improved the user interface for managing users. Several improvements are made based upon customer feedback. Previously when e.g. manually editing or adding e.g. users, after pressing "Save" the GUI would present a new screen acknowledging that the user was edited/added ok. On this screen the user had to press "OK". This is now changed so that after pressing save the user is returned to the list. A dialog screen is only presented to the user if something goes wrong. As a result, the number of mouse-clicks required to do repetitive tasks with regard to editing/creating items in a list is reduced.
- Added XML-RPC application interface. The new XML-RPC based application interface uses open standards and is easy to use. This interface gives access to the same functionality as the existing MSF interface but is not based on a Microsoft Windows API. The existing MSF interface will not be affected.

- Added HTTP/1.1 persistent connections support to the built-in HTTP server. This is mainly done to increase performance on the XML-RPC interface when using HTTPS.
- Improved security measures. Formerly every time a dect device would enter the range of the system (making a location registration) the device was authenticated. Starting with this release additional authentication is performed every time a call is established. Furthermore it is now possible to enable dect encryption of voice sent over the air. In previous firmware revisions all dect communication in the air is scrambled, enabling encryption will additionally encrypt voice with an encryption key. A new key will be calculated for each new call.
IMPORTANT NOTICE!! If dect encryption is enabled it is NOT possible to use repeaters on the system.
- Removed unnecessary warning: HL_ME_RESOURCE_ALLOCATE_req resource already allocated.
- Changed the User-Agent name for the provisioning HTTP client.

3.5.2 Removed Features

- Removed notice “Base Station disturbed xx times by foreign DECT system” from the log.

3.5.3 Corrections

- Dialog event package – notify dialog terminated when a call is rejected.
- Drop RTP packages with unexpected payload without trying to play them.
- Do not crash with high load of MSF and message waiting indication (MWI) traffic.
- Fixed problem where the maximum CLMS broadcast data length was reduced with one byte.
- Do not show 0kB captured when less than 1kB is captured by the packet capture function.
- Fixed a bug not allowing the user to enter POSIX time zones via the GUI.
- Do not crash when using DNS SRV and deleting a user.
- When users are controlled via provisioning – do not indicate users as changed when the handset has reported a firmware version. This caused the system to report the user data as changed when auto provisioning users even with no changes.
- Removed crash when attempting to change the standby text for non-KIRK handset.

3.5.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	application.enable_rpc	Specifies if the XML-RPC application interface is enabled. true – The XML-RPC interface is enabled and applications can connect. false – The XML-RPC interface is disabled. Default: false
config.xml	Added	dect.auth_call	Specifies if DECT authentication should

			<p>be used when establishing calls.</p> <p>true – DECT authentication is required when establishing calls. false – DECT authentication of calls is disabled.</p> <p>Default: true</p>
config.xml	Added	dect.encrypt_voice_data	<p>Specifies if DECT encryption should be used for voice calls.</p> <p>Disabled – DECT encryption is disabled. Enabled – DECT encryption is enabled. Enforced – DECT encryption is enforced and calls are terminated if the handset do not support encryption.</p>
config.xml	Added	sip.proxy.domain[2-4]	<p>Specifies domain/host name for additional SIP proxies.</p> <p>Default: Empty</p>
config.xml	Added	sip.proxy.port[2-4]	<p>Specifies port for additional SIP proxies.</p> <p>Default: Empty</p>
config.xml	Added	sip.proxy.priority sip.proxy.priority[2-4]	<p>Specifies the priority for using a SIP proxy. Proxies with lowest priority will be preferred and higher priorities will be used for failover.</p> <p>Values: 1-4</p> <p>Default: 1, 2, 3, 4</p>
config.xml	Added	sip.proxy.weight sip.proxy.weight[2-4]	<p>Specifies the weight for using a proxy. If more proxies have the same priority the KWS will do load balancing using the weight to determine how much each proxy will be loaded.</p> <p>Values: 0-100</p> <p>Default: 100</p>
config.xml	Added	upnp.enable	<p>Specifies if UPnP support is enabled. If enabled the device will respond to UPnP broadcasts.</p> <p>Values: true/false</p> <p>Default: true</p>
config.xml	Added	upnp.broadcast	<p>Specifies if UPnP announcements are broadcasted. If enabled the device will</p>

			periodically broadcast announcements. Values: true/false Default: false
--	--	--	---

3.6 Version PCS03B_ Q3-2009

3.6.1 Added or Changed Features

- DECT-97: Add service codes to read system information via handset. Initiated by typing codes and then pressing off hook from the handset. This information can be read from the system.
 - IP address: ***999*00
 - MAC address: ***999*01
 - Server Firmware: ***999*02
- Allow custom posix timezone specification strings.
 - It is now possible to configure the system to show “½-hour timezones”, by entering a posix string
- Add revision to User Agent string.
 - Firmware version can be obtained from traces, inspecting the User Agent field
- Include DNS traffic when capturing SIP.
- Allow custom capture filters.
 - Customize the captured data to a trace by entering a filter in pcap format.
- DECT-63: New and improved NTP client.
 - Improved error recovery.
 - Information for the NTP client included in the log file
- Add user/password and enable/disable options to MSF.
 - Possible to change login username and password for MSF applications (text messaging interface)
 - MSF functionality can be enabled/disabled
- Send unregister and unsubscribe when deleting an endpoint.
 - Inform the PBX when a DECT handset is deleted
- Clean out parameters in usernames received from some PBX'es.
- Handle "302 Multiple Choices" - for now just pick the first choice.
- Handle SDP in multipart body.
- Added timestamp and synchronization statistics duration to rfps.xml.
- If SIP registration fails, re-register within a short time and then wait.

3.6.2 Removed Features

- None

3.6.3 Corrections

- Fixed problem with authentication on some PBX'es.

- Fixed problem with wrong answer to SDP update offers.
- Fixed timer problem that might break provisioning.
- MSF callback number length increased.
- Check for required SIP headers before creating a dialog.
- Handle timeout for SUBSCRIBE requests.
 - Retry if SIP subscription fails
- Remove Require 100rel header from PRACK as this is wrong according to RFC3262.
- DECT-111: Handle MSF timestamps.
- Does not crash in some rare call transfer scenarios.

3.6.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	application.enable_msf	Specifies if the MSF application interface is enabled. true – The MSF interface is enabled and applications can connect. false – The MSF interface is disabled. Default: true
config.xml	Added	application.username	Specifies the username required for applications to log in. Default: "GW-DECT/admin"
config.xml	Added	application.password	Specifies the encrypted password required for applications to log in. Default: "f621c2268a8df24955ef4052bfbb80cf" (password "ip6000" encrypted)

3.7 Version PCS03A_ Q2-2009

3.7.1 Added or Changed Features

- Retrieving a big file from the internal web server no longer blocks the server.
- Retain any existing other call when a REFER triggered INVITE fails, otherwise release the handset.
- Do not require username in URI in REFER.
- Handle "423 Interval to brief" REGISTER response.
- Default log level in the GUI increased from INFO to NOTICE.
- Add support for international letters using UTF-8.
- DECT-83: If no protocol is specified in the provisioning URL then default to TFTP.
- DECT-81: Do not repeatedly program flash if version and binary firmware files are inconsistent.
- Log an error if configuration XML contains invalid XML.
- Add support for keep-alive used by version 18 or later of MSF.DLL.
- Send "unknown op" error when an unknown operation is requested via MSF.

3.7.2 Removed Features

- None

3.7.3 Corrections

- Fixed bug in Refer-To handling.
- Fixed bug in Record-Route handling.
- Fixed problem with time drift making NTP stop correcting the time.

- Allow changing remote RTP address during a call.
- Fixed handling of too long dialed numbers.
- DECTESC-75: Fixed bug making it impossible to save Wireless Server Configuration.
- Disable unsupported media lines correctly.
- Parse remote SDP ptime attribute correctly.
- Do not send SDP with new version if remote SDP version has not changed.
- Only check for remote SDP version changes if remote SDP was received earlier.
- Fix bug not allowing MSF multi-byte status requests – required for RTLS.
- Handle MSF call release without call record correctly.

3.7.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Changed	provisioning.server.url	<p>Specifies the static boot server URL from where the KWS will retrieve configuration information. The format is [<code><protocol>://[<user>:<password>@]<host>[/<path>]</code>]. Protocol can be either tftp, ftp or http.</p> <p>It is optional to specify a protocol. If the protocol is not specified the KWS will default to tftp.</p> <p>Example: ftp://kws:ip6000@boot.example.com/phones or 192.168.0.1</p> <p>Default: Empty</p>

3.8 Version PCS03_ Q1-2009

3.8.1 Added or Changed Features

- Optional individual ports per handsets for SIP signaling. Extend support to SIP PBXs using per port registration.
- Cisco Unified Call Manager 6.1 support.
- Auto provisioning: Possible to centralize configuration and maintenance.
- Users export to XML and CSV format: Decrease installation and maintenance cost.
- Allow adding users with unspecified IPEI: Option of adding handsets without knowing the IPEI of the handset. Decrease installation and maintenance cost by allowing field subscription of handset(s) and possibility for remote configuration.
- Added system wide DECT access code: Possible to create a default DECT access code for all users – instead of per user (access code in user will overrule the system default value)
- Added automatic standby text update. When the standby text is updated (either through the GUI or through auto-provisioning) the change appears instantly on the handset (no power-cycle of the handset is needed).

- In overlap dialing send digits when # is pressed (optional). Optional: Default is disabled.
- When a user is deleted, unsubscribe the handset. When the user is deleted the handset is signaled to remove the subscription to the system.
- Added RFC3896 Referred-By handling.
- BMC Allow dummy bearer on neighbor slot.
- BMC Do not scan RSSI - only move dummy bearer based on timer.
- BMC Do not ask RFP IP process for dummy bearer.
- BMC Added BMC/radio configuration.

3.8.2 Removed Features

- No longer use local number – the SIP user name is now used for MSF.

3.8.3 Corrections

- Fix RTP handling when call is on hold.
- Fix DTMF payload type.
- Fix order in route sets for SIP dialogs.
- Fix statistics for failed MSF calls.
- Fix handling of escaped SIP URI parameters.
- Pass all parameters and headers from REFER to the sent INVITE.
- BMC EEPROM read bug fixed.
- BMC Remove bug stopping dummy bearer.
- BMC Do not print from interrupt.

3.8.4 Configuration File Parameter Changes

File	Action	Parameter	Description
config.xml	Added	provisioning.server.method	Specifies how the KWS300 will obtain the boot server address. dhcp – obtain from DHCP option 66. static – use static configured. disabled – do not check for updates. Default: dhcp
config.xml	Added	provisioning.server.url	Specifies the static boot server URL from where the KWS will retrieve configuration information. The format is <protocol>://[<user>:<password>@]<host>/<path>. Protocol can be either tftp, ftp or http. Example: ftp://kws:ip6000@boot.example.com/phones

File	Action	Parameter	Description
			Default: Empty
config.xml	Added	provisioning.check.interval	Specifies an interval for checking for updates. 0 – do not check for updates periodically. >1 – interval in minutes. Default: 0
config.xml	Added	provisioning.check.time	Specifies a specific time for checking each day. The format is HH:MM. 00:00 – 23:59 Default: Empty
config.xml	Added	provisioning.check.check_sync	Specifies how the KWS300 will react to SIP NOTIFY check-sync events. disabled – do nothing if a check-sync event is received.. reboot – reboot and check for updates. update – check for updates and reboot if necessary. Default: disabled
config.xml	Added	provisioning.users.check	Specifies if the KWS300 will try to download and import users from the provisioning server. false – do not check for users. true – check for users. Default: false
config.xml	Added	provisioning.firmware.kws	Specifies the name of the firmware image to use for the KWS300. The KWS300 will check for a version file and a binary file. They must be located as <URL>/<firmware>.ver and <URL>/<firmware> Example: kws300-flash.bin Default: Empty
config.xml	Added	sip.send_to_current_registrar	Specifies how requests outside a dialog are sent if a list of SIP servers is received via DNS SRV. false – perform a DNS SRV lookup for each request and determine the destination from

File	Action	Parameter	Description
			<p>this. true – send each request to the server currently holding the registration.</p> <p>Default: false</p>
config.xml	Added	sip.separate_endpoint_ports	<p>Specifies if each user should use an individual UDP for its signalling or all users should use the local port defined in the SIP configuration.</p> <p>false – use one UDP port for all users. true – use individual UDP ports for each user.</p> <p>Default: false</p>
config.xml	Added	sip.pound_dials_overlap	<p>Specifies if pressing # while off hook dialling will dial the entered extension.</p> <p>false – do not dial when # is pressed. true – dial when # is pressed.</p> <p>Default: false</p>
config.xml	Added	dect.accesscode	<p>Specifies a system wide DECT access code required for subscribing handsets. The access code is from 0 to 8 decimal digits. Access codes assigned for specific users will override this setting.</p> <p>Example: 1234</p> <p>Default: Empty</p>

3.9 Version PCS02_ Q4-2008

3.9.1 Added or Changed Features

- Added auto creation of users on subscription attempt.
- Allow insecure HTTP traffic to be redirected to HTTPS.
- Improved GUI, new icons for better user experience. Improved WCAG compliance. Status icons on WEB-gui now distinguishable even for the colour blind.
- NTP server is now obtained via DHCP if provided. Multiple DNS servers are now also supported.
- Encrypt Admin GUI password.
- Log when an unknown IPEI tries to subscribe.

- DTMF sending improved. When DTMF tones are overlapping, terminate tones correctly.
- Added enable/disable send date and time to handsets.
- Add distinctive alerting by interpreting the Alert-Info SIP header. Use external ring tone as default.
- Update MWI when a handset subscribes or makes a location registration.
- Always respond with 200 OK when a MWI NOTIFY is received. This is done to avoid terminating an existing subscription.
- Added MWI retransmission.
- Allow for special characters like &_ in authentication user/password.
- Allow alphanumeric SIP username.
- Implement RFC4235 Dialog state event package. Used for e.g. call pickup support.
- Allow for receiving asymmetric RTP (option). This is required to operate with e.g. a Mitel NuPoint voice mail server.
- Detect merged invites after a fork and respond with “482 Loop Detected”.
- Added full system backup facility. Instead of separate backups of configuration, users etc. everything is now in one backup and it is optional how much is restored.
- Standby text length increased from 16 to 24 characters.
- Implemented Type-of-Service/DiffServ. Replaced old Quality-of Service approach with new Type-of-Service approach.

3.9.2 Removed Features

None

3.9.3 Corrections

- Corrected error in subscription statistics (subscriptions which failed due to e.g. wrong or missing DECT access code was logged as a success).
- Release MSF-call correctly when no CR is assigned.
- Fixed problems with ntp and the clock which could cause the clock to drift.
- Send opaque param in authorization reply.
- Fix reversed time zones. GMT time zones were reversed – GMT+2 meant GMT-2. This has now been fixed.

3.10 Version PCS01B_

Initial KWS300 version.

4. Outstanding Issues

The following issues will be fixed in a subsequent release

- None identified.