Technical Bulletin CS-18-08

Q3-2018 DECT Release: Delivering enhanced OTA Security, deployment automation and much more…

This technical bulletin reviews the new DECT Q3 2018 Software Release including key enhancements such as; early encryption and regular cipher key exchanges for added voice and data protection over radio links, support for redirection service to achieve near zero-touch-provisioning and increased support for operation behind NATs and Firewalls, plus all the general service updates. Full Technical Release Notes are available when you download the Software.

System Affected

All DECT servers, IP-DECT servers and handsets.

Key IP-DECT Server & Handset Security Enhancements

DECT OTA Security (Step A)

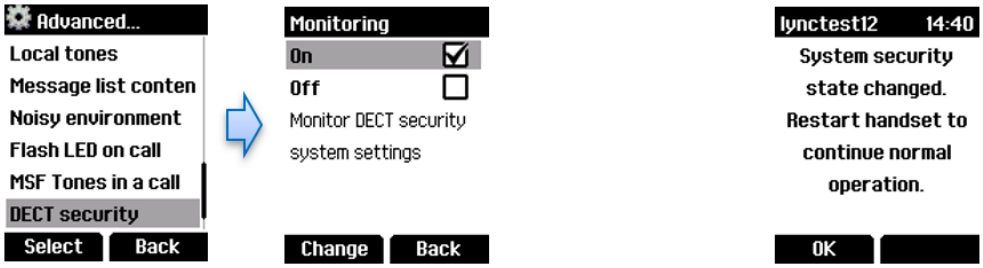
7000 Series Handsets

Available on handsets including 7502 entry level handset, 75-Series, 76-Series and 77-Series handsets, Step-A, the new DECT Security Standards, provides enhanced level of OTA encryption including early encryption during call setup and cipher key exchanges at short regular intervals during calls, providing one of the highest levels of DECT security and delivering greater security between DECT base stations and the mentioned DECT handsets.

In addition, with the implementation of this DECT Security Standards, there is now a monitoring function, enabling the monitoring of the DECT server security from the handset. This function notifies users via their handsets if there is a change in the security state of the system during normal operation. With the feature enabled, when security state of the server changes - the handset will automatically inform the users that the system security has changed state, and that

the user needs to restart the handsets to continue normal operation. Any calls made from this point onwards will be disconnected after 15 seconds, until the handset is restarted.

Note: The new DECT security implementation is only available on our feature handsets 75x2, 76x2 and 77x2, but NOT on the base level 72x2 series.



IP-DECT Servers

For the IP-DECT server portfolio, including the 200, 400 and 6500 servers extensive work has been completed for this software release to introduce DECT Security (Step A) Standards, where the encryption is enhanced and improved ways of exchanging cipher keys for encryption has been introduced.

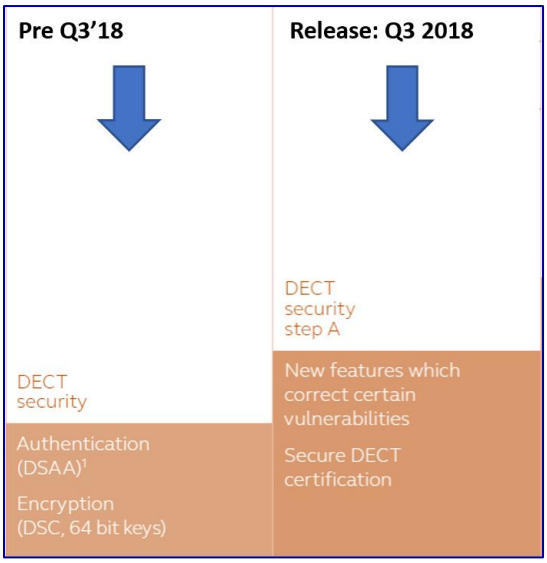


Figure 1 - DSAA and DSC are the authentication and encryption algorithms defined in the DECT security standard ETSI EN 300 175-7 applicable for DECT security and DECT security step A. Step-A has been introduced by the DECT standards body to correct certain known vulnerabilities in the standard to ensure enhanced security.

In addition to early encryption, authentication of handsets, and a whole host of security features have been introduced, including the cipher keys renewal every 60 seconds throughout a call, – enhancing the DECT encryption between the IP-DECT base stations and DECT handsets over AIR. For details see table below.

Feature	DECT GAP	DECT Security
Registration procedure and time limits for setting of a44 bit	O	M
"Encryption activation FT initiated" (Base & Handset) Note : all voice calls encrypted	O	M
On air key allocation (Base & Handset)	O	M
Authentication of PP (Base & Handset)	O	M
Evaluation of peer sides behavior regarding encryption including timeout values for triggering of call release	O	M
Early encryption	O	M
Procedure for re-keying with a new derived cipher key during a	O	M

Table 1 – Security features – DECT Step-A | O means Optional and M means Mandatory

It should be noted that any DECT subscription on the IP-DECT server is, by default, only allowed to be "open" for up to 120 seconds or until a handset is subscribed. However, this setting can be disabled in the IP-DECT servers via the web GUI to speed up and enable DECT subscriptions.

Note:

- *Due to the way the DECT Security (Step-A) standard is defined and described, any system that has this feature enabled becomes more "sensitive" to signal noise – meaning the need to have a much better coverage becomes more important. Hence, customers who wants to use DECT security (Step-A) MUST ensure to have Site-Survey for radio coverage done professionally with DECT security (Step-A) set to ON prior to the actual Base Station deployments. Please reach out to Spectralink support, or contact our professional services to arrange for Site-survey.*

For further information regarding DECT Security (Step A) Standards please click here: **DECT Security Certification**

NAT Keepalive to support ITSP/UCaaS providers

New Features for both DECT and IP-DECT Servers

Due to a significant growth in cloud based UC/UCaaS offerings from ITSPs and all leading telephony solution providers – it has been identified that there are often issues with CPE kits being deployed behind firewalls/NATs and NAT traversal is required for all operations.

In order to proactively address this issue - Spectralink has introduced support for using SIP OPTIONS in addition to CRLF techniques for achieving NAT traversals as a new NAT keepalive option for both DECT and IP-DECT servers to help DECT systems stay connected to cloud based UC/UCaaS platforms even when behind standard enterprise routers/firewalls.

By selecting the NAT keepalive interval, small packets are sent at regular selectable intervals, between 10 and 30 seconds, to keep the NAT from closing the port and changing the internal port mapping ensuring smooth operation of incoming/outgoing calls.

ICE Enhancement – Supporting Polycom Call Hold or Transfers

Enhancement to Interactive Connectivity Establishment (ICE) protocol for NAT traversal has also been implemented where ICE candidates are no longer treated as unique. This also helps to ensure that during all conversations between Polycom VVX phones and Spectralink servers/handsets – the Polycom phones correctly display the call hold/transfer mid-call operation softkeys.

MAC address based authentication for UCaaS poviders

All DECT servers and IP-DECT servers now also have the ability to optionally add the systems' MAC Address to ALL SIP Message headers.

UC/UCaaS and Service Providers that want to protect their platforms from possible DoS attacks can now, as part of admission control, use the MAC address to further authenticate that the SIP messages are arriving from their legitimate users (customers) and allow the SIP messages through using MAC address as a security token.

New DECT Handsets Functionality

Missed Call Notification

Any missed calls, including a second call arriving while a user is busy on another call, is now displayed on the handset LCD screen when the current user finishes the call. This is to ensure that the user is aware of the missed call and can respond accordingly.

Redirection Service for Zero-Touch Provisioning

In order to simplify and support near zero-touch-provisioning of IP-DECT servers – Spectralink has launched a cloud based redirection service that can be used by Spectralink channel partners, ITSP & traditional communication service providers looking to automate deployment of thousands of IP-DECT servers, and finally large end-customers looking to deploy hundreds of sites. The process simply requires that each IP-DECT server is registered with the Redirection Service online together with a target Provisioning server where the relevant IP-DECT server can find all its configuration settings as well as any firmware that needs to be rolled out for the particular site deployment.

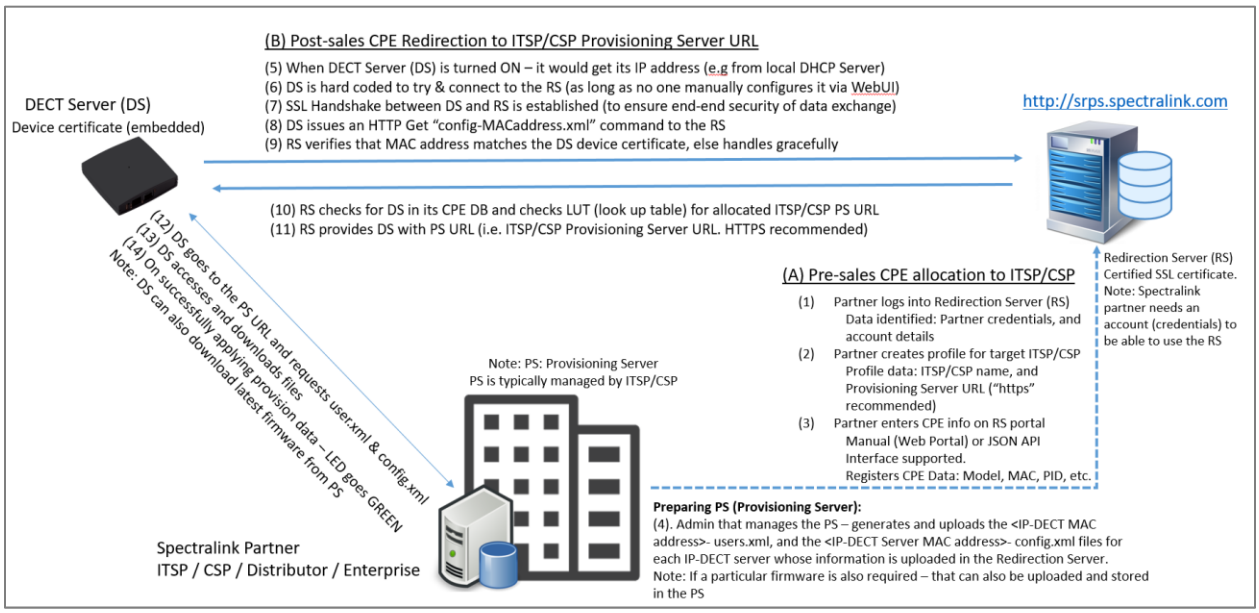


Figure 2 - Automating deployment using Redirection services

When the DECT server starts – if it doesn't receive or find the local provisioning server url either via DHCP option 66, or via manual web GUI entry to the DECT server - it searches for and connects to the global Spectralink Redirection & Provisioning server services (SRPS) portal. The SRPS receives unique identity information from each DECT server (typically MAC address, & P-ID) and based on a database lookup based on these specific fields of data – previously entered into the SRPS database – the SRPS provides back to the DECT server a url that points the DECT server to the correct & relevant Provisioning server deployed by Spectralink or a specific partner or customer. The DECT server then reaches out and connects securely to the specified url and downloads all relevant firmware, configuration and user settings as part of configuration and provisioning update. The partner provisioning server can also provide approved DECT server firmware, base station firmware, media resource firmware, and DECT handset firmware for easy firmware release management & roll-out.

Using Spectralink SRPS Redirection services platform together with partner Provisioning servers - it should no longer be necessary for channel partners to unpack, configure and then repack a DECT server before shipping to the end-customer. This greatly simplifies mass deployment by automatic configuration, and saves a lot of time and resources for Spectralink partners – achieving what is termed as near "Zero-Touch" provisioning.

If you would like to use the redirection service – please reach out to the support team to get credentials so that you can log into the system and start saving time and automating your DECT server deployments.

New DECT Server Functionality

Lone-Worker Test Automation via XML-RPC API

New implementations into the XML-RPC interface to the DECT servers have been added – to support "self-testing" in the handset, allowing users to test different sensors, buttons and functionality. The handset can be told to initiate the testing and the conclusion of the testing – the handset can display the results – which can be collected by AIMS partner solutions offering lone-worker support to show successful completion of testing prior to lone-worker functionality use.

New IP-DECT Server Functionality

Software Assurance License

Starting with Q3 2018 IP-DECT Server Software Release – all IP-DECT servers can now track a Software Assurance license key to ensure that all IP-DECT servers are registered and customers have the ability to continue to receive future software releases and service updates in order to ensure that the platform continues to run using the latest firmware releases, runs with the latest technology mobility solutions, and has the latest software security enhancements. Further information regarding Software Assurance will be communicated by Spectralink shortly.

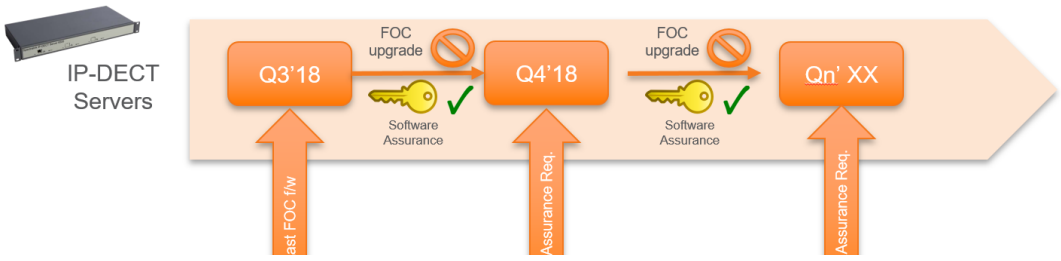


Figure 3 - IP-DECT Servers with software assurance

New Files in Exported Logs

With the Q3 2018 DECT Software Release, new files can be found in the exported log, including; a HTML Page with Licensing information, a screenshot of the WEB GUI licence page, with full names of the licenses and the license codes.

General DECT Handset Solution Enhancements

Site Survey and Free Channels

With the Q3 2018 DECT Software Release it is now possible to see all channels and timeslots, including the dummy bearer channel and the two side channels – which previously were not visible from the handsets. This is to ensure improved site troubleshooting for onsite technical staff.

Bluetooth Headset and Answer Button Updates

To overcome issues with some Bluetooth headsets, Spectralink has introduced new protocol within the DECT handsets, to recognise the Bluetooth headset when it connects to ensure audio is immediately played through the headset when answer button is selected. Note that Bluetooth option is available in only selected model handsets.

Local Language Contact Sorting in Phonebook.

With the Q3 2018 DECT Software Release the Phonebook can now be used to correctly sort contacts in non-english language as well – improving the ability for non-english speakers to sort phonebook using the language of their choice.

General IP-DECT Server Solution Enhancements

GAP Handsets

Improved support for dial and ringback tones on some GAP handsets has been added along with reject reason information, if a call fails during authentication.

For details on these and ALL other enhancements and corrections – please ensure that you also read and review the relevant product release notes available via **Spectralink's support site**.

Document Status Sheet

Document Control Number: CS-18-08

Document Title: Q3 2018 DECT Release – delivering key OTA Security Standard ehancements and much much more…

Revision History: I01 – Released 10, 16, 2018

Date: *10-16-2018*

Status: ☐Draft ☒Issued ☐Closed

Distribution Status: ☐Author Only ☐Internal ☐Partner ☒Public

Copyright Notice

Notice

Warranty

The *Product Warranty and Software License and Warranty* and other support documents are available at http://support.spectralink.com.

Contact Information

US Location
+1 800-775-5330

Spectralink Corporation
2560 55th Street
Boulder, CO 80301
USA

info@spectralink.com

Denmark Location
+45 7560 2850

Spectralink Europe ApS
Bygholm Soepark 21 E Stuen
8700 Horsens
Denmark

infoemea@spectralink.com

UK Location
+44 (0) 20 3284 1536

Spectralink Europe UK
329 Bracknell, Doncastle Road
Bracknell, Berkshire, RG12 8PE
United Kingdom

infoemea@spectralink.com