poly

WHITE PAPER

SAVI 7300 OFFICE SERIES DECT™ SECURITY

WIRELESS HEADSETS PROVIDE HANDSFREE FREEDOM

As employees spend more time collaborating on voice and video calls the productivity and wellbeing benefits of a wireless headset becomes greater. In certain industries the perceived concerns around the security of wireless headsets meant they were often rejected as an option. The Poly Savi 7300 Office Series has been designed to go beyond the highest security level from the DECT™ forum by including military level encryption, now all organisations can benefit from the use of wireless headsets.

CYBERSECURITY A TOP 5 GLOBAL THREAT

Cybersecurity threats represent one of the five top key risks facing the world as identified by the **World Economic Forum (WEF) 2019 Global Risk Report**[1]. The survey represents results from decision-makers across public sector, private sector, academia and civil society.

For businesses that fall victim to a cyber-attack, the financial costs can be enormous with ransomware damage costs expected to reach $20 trillion by 2021 according to **Cybersecurity Ventures**[2].

To address the growing Cybersecurity threats, end-user spending for the information and security risk management market is estimated to grow at a compound annual growth rate of 8.3 percent from 2019 through 2024 to reach $211.4 billion in constant currency according to Gartner[3].

ACHIEVING ULTRA-SECURE COMMUNICATIONS WITH THE LATEST GENERATION OF POLY DECT™ HEADSETS

Digitally Enhanced Cordless Telecommunication (DECT) is an established 1.9 gigahertz* technology that utilises a dedicated part of the wireless spectrum to provide high levels of security and audio quality in enterprise office and home environments with up to 180m line of sight range. DECT™ technology is often referred to as being “interference-free” since it does not share spectrum with other technologies such as wi-fi networks.

Security is one of the many strong points of DECT™ technology, that has evolved over time to keep up with increased threats. A DECT™ headset system consists of a headset and a base that uses Time Division Multiple Access (TDMA) digital radio and dynamic channel selection over 10 carrier frequencies for European DECT™ implementation and 5 carrier frequencies for US DECT™ implementation and 24 time slots, together with a multi-layer security system. This layered system, which includes subscription, encryption and authentication, ensures a very high level of protection against eavesdropping. Certain industries, such as healthcare and finance, require DECT™-based wireless communications to help ensure maximum security and confidentiality.

3 STEPS IN THE DECT™ SECURITY CHAIN

The DECT™ security chain is made up of three steps as shown below:

PAIRING

The first and important step in the process is to bind the headset with the base. This can be done either over the air or for greater security by physical docking the headset into the base. This ensures that the secret key shared during this process is exchanged via the charging contacts and not over the air.

AUTHENTICATION

For each call the secret key shared during the pairing process is used to establish authentication between the subscribed headset and the base. A non-paired headset will not work with the base.

ENCRYPTION

For each call the audio between the headset and the base is encrypted so that it cannot be read by intruders – the encryption keys are regenerated every 60 seconds.

DECT™ SECURITY EVOLUTION

Protecting the confidentiality of wireless conversations has always been paramount. As the need for enhancements to the DECT™ standard became apparent in 2009 when a group of white-hat hackers known as the DeDECTed Group published a paper outlining the security weaknesses of basic DECT™ products. In part, the hacker group exposed the threat of breach when DECT™ products did not use the standard authentication and encryption as outlined in the ETSI standards. Poly DECT™ headset products have always incorporated authentication and encryption.

The DECT™ Forum, of which Poly (Plantronics) is a member, reviewed the DeDECTed Group's findings and released a DECT™ security roadmap. The first stage was known as Step A and added 4 enhanced DECT™ security features which reduces the risk of eavesdropping and keeps conversation secure (see table below).

STEP A

ENHANCED DECT™ SECURITY FEATURES

#1
NEW RANDOM NUMBER GENERATOR

Virtually impossible that the random number can be guessed with successive attempts and then used to create keys

#2
EVALUATION OF PEER SIDE BEHAVIOR

Any hacking attempt would have to be flawless in all aspects every time as any headset to base communication outside of the expected pattern will cause the connection to be discontinued

#3
EARLY ENCRYPTION

Guarantees encryption activation immediately after connection establishment, before any useful information is exchanged

#4
PROCEDURE FOR RE-KEYING

With a new derived cipher key during a call – The cipher key used by the encryption engine is updated at least once per 60 seconds, to foil any attempt to crack the ciphering by brute-force techniques, like supercomputing

An official DECT™ Security Certification Programme was launched in 2013 in which products are independently tested and verified at an approved laboratory.

Poly was the first provider in the wireless product industry to fully meet the security standards outline by the DECT™ forum with the Poly (Plantronics) CS500 Series shipping with the enhanced security features in October 2013, other products in the Poly range followed soon after.

Further stages were also defined known as Step B and Step C each adding increased security over the previous steps.

STEP B

Defines improvements to the authentication algorithm based on AES 128-bit encryption called DECT™ Standard Authentication Algorithm 2 (DSAA2) and was published during 2012

STEP C

Defines improvements to encryption algorithm based on AES 128-bit keys called DECT™ Standard Cypher 2 (DSC2) and includes True random number generator to further enhance security. ETSI has completed and published this standard.

POLY SAVI 7300 OFFICE SERIES DESIGNED FOR DECT™ SECURITY STEP C AND BEYOND

Poly with the Savi 7300 Office Series has been designed to meet the requirements of DECT™ Security Step C and in fact goes beyond this requirement with the use of AES 256-bit encryption in place of the Step C defined AES 128-bit. The use of AES 256-bit encryption is one of the approved security functions listed in FIPS140-2 which is mandated by the US government and used worldwide including by banking and finance companies.

The Savi 7300 Office Series has also been designed without a Bluetooth® radio and hence will not connect to mobile phones, making it ideal for use in areas where Bluetooth is banded or where all calls must be routed via the company's telecommunication network for recording and compliance purposes.

POLY REMOTE DEVICE MANAGEMENT

The Savi 7300 Office Series are supported by Poly remote device management solutions ensuring that these devices can be kept up to date with the latest firmware fixes and patches. Device settings can also be remotely configured such as disabling the ability to subscribe a headset over the air for even greater security.

POLY DECT™ HEADSET SECURITY COMPARISON

	 **POLY SAVI 7300 OFFICE SERIES**	 **POLY SAVI 7200**	 **POLY CS540**	 **POLY SAVI 8200 OFFICE AND UC SERIES**
SUBSCRIPTION METHOD	Configurable for either physical or over the air	Physical and over the air	Physical and over the air	Configurable for either physical or over the air (not Savi 8200 UC series)
DECT™ SECURITY LEVEL	Beyond Step C	Step A – DECT™ Certified	Step A – DECT™ Certified	Step A – DECT™ Certified
AUTHENTICATION	128 Bit DSAA2 (AES)	64 Bit DSAA	64 Bit DSAA	64 Bit DSAA
ENCRYPTION	256 Bit AES beyond Step C	64 Bit DSC	64 Bit DSC	64 Bit DSC
INCLUDES BLUETOOTH RADIO	–	–	–	• (not Savi 8200 UC Series)
INCLUDES FIPS 140-2 LISTED FUNCTION	• (256-Bit AES)	–	–	–

GLOSSARY

AES
Advanced Encryption Standard adopted by the US government as well as being used worldwide to encrypt data

AUTHENTICATION
The act of the headset and the base asserting their identity to each other. For Security Step B this is defined in an improved algorithm called DECT™ Standard Authentication Algorithm 2 (DSAA2) that is an update to DSAA defined in DECT™ security standard ETSI EN 300 175-7

DECT™ FORUM
Supports a collaborative environment of the DECT™ industry and drive programs to develop and improve DECT™ wireless technology. Poly (Plantronics) is a full member of the DECT™ forum

DSAA
DECT™ Standard Authentication Algorithm defined in DECT™ security standard ETSI EN 300 175-7 and is used by the base and the headset the result of which must match for a successful paring to take place.

DSAA2
DECT™ Standard Authentication Algorithm 2 improved algorithm for DECT™ security Step B

DSC
DECT™ Standard Cypher defined in DECT™ security standard ETSI EN 300 175-7

DSC2
DECT™ Standard Cypher 2 improved algorithm for DECT™ security step C

ENCRYPTION
The process of information being converted into a secret code hiding its true meaning. For Security Step C this is defined in an improved encryption algorithm called DECT™ Standard Cypher 2 (DSC2) that is an update to DSC defined in DECT™ security standard ETSI EN 300 175-7

FIPS140-2
Security requirements for cryptographic modules written by the US NIST (National Institute of Standards and Technology) includes a list of approved security functions - AES is one of those approved functions. Required by US government agencies.

STEP B
Defines improvements to the authentication algorithm based on AES 128-bit encryption called DECT™ Standard Authentication Algorithm 2 (DSAA2) and was published during 2012

STEP C
Defines improvements to encryption algorithm based on AES 128-bit keys called DECT™ Standard Cypher 2 (DSC2) ETSI has completed and published this standard.

SUBSCRIPTION
The process by which the headset and base are paired together and in which they exchange a unique authorisation and encryption code. The headset and base are already paired together at the factory.

*Note different DECT™ frequencies are used around the world and hence Poly offers different skus for different markets.

[1]The Global Risks Report 2019 14th Edition, Wold Economic Forum http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

[2]Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) by 2021, Cyber Security Ventures

[3]Gartner, Forecast: Information Security and Risk Management Worldwide, 2018-2024, 3Q20 Update – Published 5 October 2020