DECT Security & Remote work

EPOS

Executive Summary

DECT security is vital for the modern workforce

DECT technology offers the modern workforce many advantages, especially when it comes to the security of the communication and data of businesses. In light of the recent shift to the remote workplace, security is one of the biggest issues for businesses globally. How can we ensure that those working from home, remotely or indeed while away travelling can still rely on the security of their audio solutions? Ensuring peace-of-mind that no-one is listening in on your business calls is a vital consideration for every serious professional.

Get to know DECT security

To address this issue and describe the latest advances in the EPOS DECT offering, this white paper first describes DECT technology and the DECT Security Certification Program. Secondly, it outlines the DECT security chain comprised of “Pairing”, “Per Call Authentication” and “Encryption”, while highlighting the benefits of DECT Security Certification.

Mobile solutions and the DECT security chain

The white paper goes on to describe the advances in DECT security built into our mobile DECT solution – the SDW D1 USB dongle. The security of the pairing process between headset and dongle has been enhanced by the authentication algorithm (DSAA2). This algorithm, means both headset and dongle have already reached the necessary criteria as if they had been certified for step B of the DECT Security Certification. This process provides an added layer of security in addition to the standard step A.

The future of secure, mobile DECT solutions

By focusing on pioneering audio technology and refining its DECT audio solutions, EPOS has been able to provide a new level of DECT security with its IMPACT 5000 Series premium wireless DECT headsets and a flexible, dynamic DECT dongle – the SDW D1 USB. Over the course of this white paper you will see how this new secure solution enables peace of mind for our users through advances in DECT security, a keen understanding of mobile working practices and a response to the needs of the modern workforce.

Introducing DECT Technology & Security

DECT security

Digital Enhanced Cordless Telecommunications (DECT™) is the European Telecommunications Standards Institute's (ETSI) standard for short-range, cordless communications, which can be adapted for voice, data and networking applications*.

DECT technology has become the global standard for secure residential and business cordless phone communications. More than 110 countries have adopted the DECT system with more than 100 million new devices sold annually.

IMPACT 5000 Series headsets & the SDW D1 USB dongle are DECT security certified
To meet the increased demand for secure communications, the DECT Forum has established the DECT Security Certification Program. The certification program consists of a set of requirements and security features, which when implemented in a product are validated by an accredited and independent test laboratory to show compliance. IMPACT 5000 Series headsets and the SDW D1 USB dongle have successfully been assessed by the qualification body and as a result, obtained the DECT Security Certificate of Conformity.

* Find more information at: www.dect.org

The DECT Security Chain

The DECT security chain consists of the three main processes “Pairing”, “Per Call Authentication” and “Encryption”. Later in the white paper these three processes will be described in detail.

DECT enabled devices usually follow these processes. However, with the SDW D1 USB dongle, a further layer of security is added on top of the standard pairing process:

The SDW D1 USB dongle uses AES-128-bit keys which corresponds to step B of the DECT security standard. Products that achieve step A of the DECT security standard only use 64-bit keys. For every extra “bit” the number of key combinations doubles. I.e. 65-bit enables double the number of key combinations that 64-bit can, and 66-bit doubles that number again. The number of combinations increases exponentially with every bit added up to 128-bit keys (step B of the DECT security standard), therefore increasing security correspondingly.

Order	Process	Description	Main purpose	Frequency
1	Pairing	Registration of security bindings between headset & base station	Ensure connection established between authorized devices	Once, during set-up
2	Per Call Authentification	Verification of security bindings between registered headset & base	Verify that call is made between authorized devices	Every call
3	Encryption	Encoding of voice data during calls	Make call data unusable to intruders	Every call

1. Pairing

Pairing is a mutual process between the headset and dongle when both devices are in range and signal to each other that they are ready to establish a secure binding. This pairing then establishes a secure connection between both dongle and headset to enable secure communication. The DECT Security Certification has certain standard requirements (step A) which have been satisfied and exceeded by the IMPACT 5000 Series headset and the SDW D1 USB dongle. In order to reach a higher level of security EPOS has added the following improvements:

DECT Security Certification step B – even more secure pairing

The enhanced authentication algorithm (DSAA2) uses AES-128-bit keys to establish and ensure that the Master Security Key in the headset and dongle is identical. One Master Security Key is generated per headset per pairing and is never shared between headsets. For any new headset that registers with the dongle a new Master Security Key will be generated and the previous one will be forgotten. The improved DSAA2 algorithm is an ETSI standard planned for step B within DECT Security Certification, meaning that EPOS is reaching beyond the norm to achieve an enhanced level of security for your business.

Reduced pairing range:

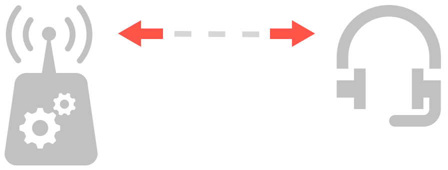
When initiating pairing, the distance between the headset and the dongle varies and is dependent on the density of the DECT environment, i.e. the number of DECT systems present in the office and the signal they are emitting. The experienced pairing distance depends on the actual radio environment where the pairing is performed. The higher the density of the DECT environment, the shorter the distance between the dongle and headset must be in order to pair. This is a security measure so that only headsets in close proximity of the dongle will be able to pair. As the DECT environment in every office is unique we could never put exact figures on the pairing distance, but the following gives some indication of the pairing distance when it comes to pairing range in environments of varying DECT density:

In a high-density environment, the pairing distance is approximately 5-10 cm, whereas in a low density it's in the range of 0,5-1 m. In the situation where there are no other DECT systems in the DECT radio spectrum, the pairing distance is up to 3-4 m.

Pairing with IMPACT 5000 Series headsets only

All other DECT devices are rejected by the SDW D1 USB dongle during the pairing process and only IMPACT 5000 Series headsets can connect.

Wireless Pairing



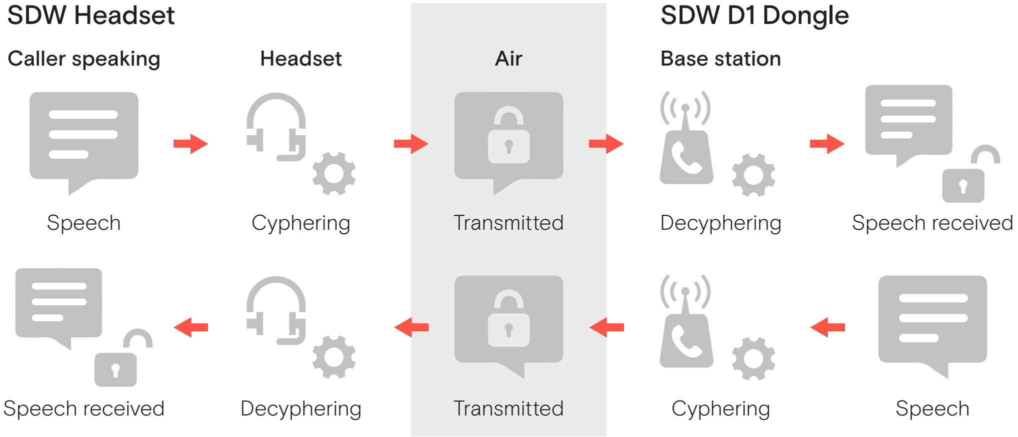
Data exchanged 'over the air'

2. Per Call Authentication

Every time a call is made, the SDW D1 USB dongle needs to ensure that the connected headset has been paired – and is therefore safe to communicate with. The dongle does this by sending a random number stream – also known as a 'challenge' – to the headset. The headset and dongle then simultaneously run an authentication algorithm, using the random numbers and Master Security Key as input. The headset sends its 'response' back to the dongle and if the calculation outputs match, the call can be placed. If not, the call is rejected. Another output of the Per Call Authentication process is the generation of a Derived Cipher Key, which is further described in the Encryption section.

It is the industry standard to authenticate headsets 'over the air' at the beginning of each call. While this data can be 'sniffed' by an intruder, it is of no value without knowing the Master Security Key.

3. Encryption



The overall purpose of encryption is to protect the confidentiality of digital data transmitted between parties, thereby preventing unauthorized third parties from accessing the data. For a business headset system, the data transmitted 'over the air' consist of a combination of digitized voices and of link control information. An encryption system consists of an algorithm which does the encryption and an input key to the algorithm.

A DECT standard encryption algorithm called DSC (with 64-bit keys) is used to encrypt voice data (in both directions) and call-related digital signaling. To protect against passive eavesdropping by an unauthorized user, the encrypted data would look like a meaningless stream of digital data.

Initiation of encryption
All calls are encrypted, a process which cannot be bypassed. Early encryption is a process required by the DECT Security Certification program, which guarantees that no voice or call data can be exchanged before the encryption has been activated. With early encryption, a Default Cipher Key is generated during pairing which is then used for encryption. This will be used until the first Derived Cipher Key has been calculated. The encryption protocol is designed to detect if the peer (headset) behaves in an unexpected manner. In this event the system will assume it is an attempt to breach security and the link will be terminated. This feature is required in order to comply with DECT Security Certification.

A new Derived Cipher Key is produced for each call during the Per Call Authentication process (as previously described). As a result, any previous encrypted information becomes invalid for the establishment of a new call.

Re-keying
IMPACT 5000 Series headsets have a re-keying procedure, which is another feature certified by the DECT Security Certification Program. It consists of modifying the Derived Cipher Key approximately every minute during a call. This means that when the SDW D1 USB dongle and headset have established a call, the 64-bit keys are renewed continuously throughout the call.

In the very unlikely case that a threat actor manages to determine the Derived Cipher Key, it will become invalid within max. 60 seconds. This is a safeguard against any brute-force attempts to crack the ciphering.

If the headset rejects the authentication or answers with an incorrect authentication result, the dongle will immediately drop the call. Trying to decode the data stream using the wrong Derived Cipher Key will generate noise.

IMPACT 5000 Series Headsets & SDW D1 USB Enabling DECT in and Out of the Office

The migration to the remote workplace has been underway for years and its many advantages are well documented. Indeed, due to the flexibility of working wherever, whenever, employee productivity is often seen to increase. Today working from home is a new reality for the vast majority of modern professionals, which demands maintaining professionalism in the home office and other remote locations. The right audio tools are key to achieving a professional, seamless communication experience. Wireless DECT headsets like those from the IMPACT 5000 Series and the innovative SDW D1 USB dongle are able to offer users mobility, comfort, excellent communication and user density – as well as an added layer of advanced security that exceeds the industry standard.

Stay mobile with a secure DECT dongle
For those that work in open offices and need to stay mobile and those that work remotely and still require the advantages of DECT devices, the SDW D1 USB is a plug-and-play dongle that connects your PC to your IMPACT 5000 Series headset – providing freedom to move while you work. It means you get a neat, portable solution that complements today's clean office aesthetic and keeps you mobile in high-density DECT environments. Furthermore, you can switch working stations very easily and maintain call quality with a simple gadget that keeps your laptop and headset seamlessly connected.

Maintain security wherever you work
The IMPACT 5000 Series headset & the SDW D1 USB dongle makes your DECT solution extremely portable, meaning you can take the same headset home with you to maintain call quality form your home office and get peace of mind that your headset/ dongle solution complies with the DECT Security Certification program.

Meeting the needs of the mobile workforce
Through tailoring DECT security to a flexible, mobile audio solution, EPOS has managed to bring all the advantages of DECT to the modern, mobile workforce. Now that the mobility of professional audio solutions has transitioned from "nice to have" to "need to have", EPOS is ensuring that the advantages of DECT are made available to those for whom remote working is a daily reality.

IMPACT SDW D1 USB
IMPACT SDW 5011/5031/5061
Get organized. Get mobile

Choose between three headset/dongle variants with different wearing styles to suit your working preference – 3-in-1 wearing style, single-sided or double-sided headsets. Each with its own SDW D1 USB dongle. All variants come with a charging cable and soft carry pouch to optimize the portability of your IMPACT 5000 headset, designed for audio excellence, security, mobility and productivity whether in the office or the remote workplace. The dongle is also compatible with existing IMPACT 5000 Series headsets if the user wants to take the headset into the remote workplace away from its base station.

560352772

EPOS Group A/S
Industriparken 27
2750 Ballerup, Denmark
eposaudio.com