DECT™ Security

EPOS | SENNHEISER

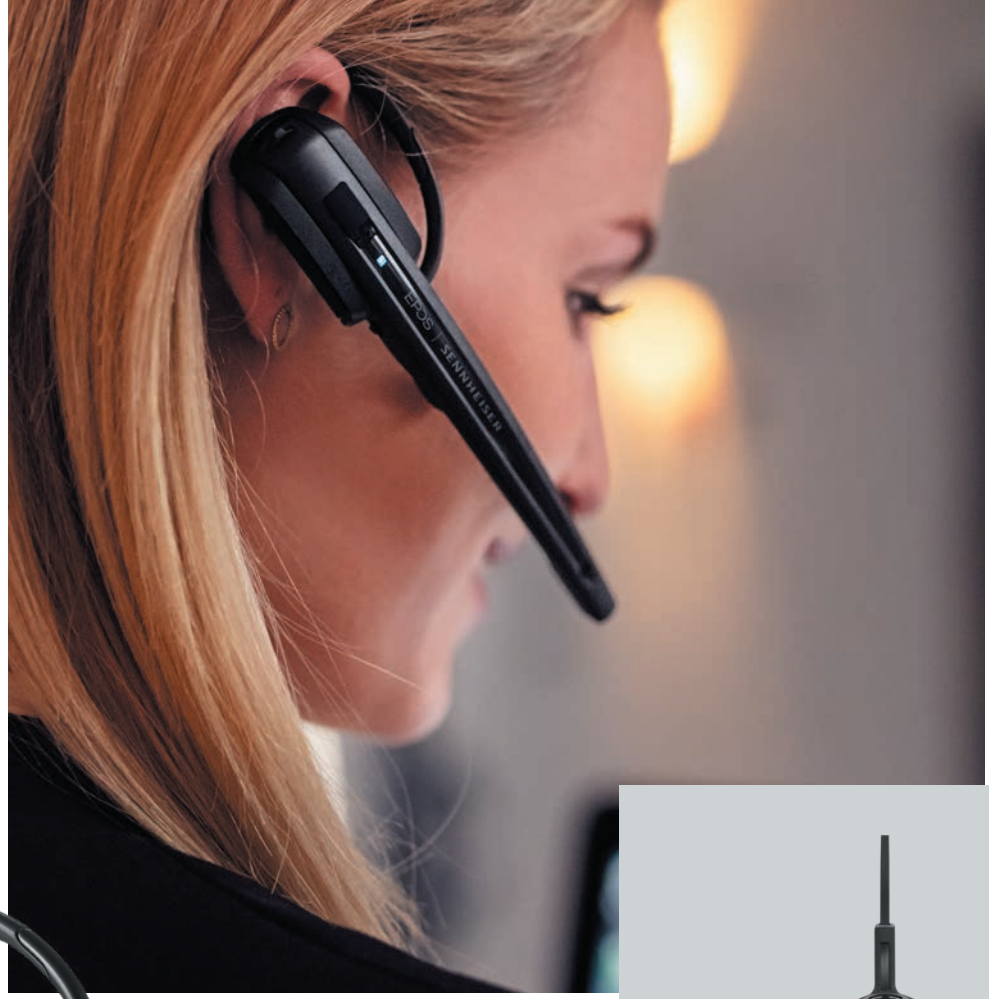
Executive Summary

This paper addresses the security of EPOS DECT Contact Center and Office (CC&O) headsets. It describes the DECT security chain comprised of “Pairing”, “Per Call Authentication” and “Encryption”, which are all part of the standard DECT protocol.

Furthermore, it explains that an intruder can only compromise the security of a DECT system by gaining access to the data exchanged between the headset and base station during initial pairing. Therefore, protecting the pairing process from unauthorized access is at the heart of a secure wireless communication system.

In EPOS devices, pairing is only possible when the headset is physically docked in the base station. A potential intruder therefore has no way of calculating or intercepting the pairing data wirelessly.

This, together with the added security layers provided by the standard DECT protocol, makes the overall security of EPOS DECT products very high. As a result, they are virtually immune to the commonly perceived threats to a wireless system, namely – passive eavesdropping, base station impersonation and fraud.



About DECT Technology[1]

Digital Enhanced Cordless Telecommunications (DECT™) is the European Telecommunications Standards Institute's (ESTI) 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.

1. Please refer to www.etsi.org and www.dect.org for more information.

The DECT Security Chain

The DECT security chain is made up of the three main processes:

Most DECT enabled devices follow these processes. The DECT standard however, does not define exactly how pairing data should be exchanged. The sections below detail the generic DECT processes, as well as the two common pairing methods used by headset manufacturers.

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

The Pairing Process – The Backbone of a Wireless Communication System's Security

An overview of Validation and Pairing
In order for a DECT headset and base station to pair, they first need to validate each other with a matching 4-digit PIN code. An automatic process known as 'easy pairing' is used in most DECT headsets, enabling pairing to start without the user having to manually enter a PIN code.

When validation is complete, pairing can initiate. This process is driven by an algorithm only available to DECT manufacturers, called the DECT Standard Authentication Algorithm (DSAA). The algorithm is executed simultaneously in the headset and base using the 4-digit PIN code and a random number stream. The results of the algorithm are exchanged and must match for successful pairing.

The Master Security Key – the key to keeping out DECT intruders
Another output of the DSAA algorithm is the Master Security Key (also known as the 128-bit UAK). The Master Security Key is used in all subsequent DECT security procedures. Since it could be used to compromise the security of a DECT communication system, it is critical to keep the Master Security Key protected from potential intruders.

Wireless pairing – a vulnerable area in the DECT security chain – in some DECT devices
It is a DECT requirement that the PIN code and Master Security Key are never exchanged 'over the air'. However, some DECT devices transfer the data used to calculate the Master Security Key wirelessly. This opens up the possibility of an attacker 'sniffing' the pairing data, using highly sophisticated equipment. With very deep and specialized knowledge about DECT encryption, the intruder could, in theory, calculate the Master Security Key and thereby compromise the security of the system.

Protected pairing – the key to security in EPOS DECT devices
EPOS DECT devices have a very high security level, due to the process required to pair a EPOS headset and base station.

Rather than transferring pairing data 'over the air', the charging terminals are used for data communication. This means that a EPOS headset needs to be physically docked in a EPOS base, in order for the registration and security bindings to be established. This makes it virtually impossible for a third party to 'sniff' or intercept the pairing data from a remote location.
Since the Master Security Key is stored on the devices and never transmitted over the air, this feature provides best in class security against any kind of unauthorized access.

Conference pairing – a unique Master Security Key in each headset ensures no misuse
In EPOS headsets, it is possible to establish a DECT conference with up to four headsets connected to one base. In this scenario, each headset will get its own unique Master Security Key. This ensures that the Master Security Key stored in a guest headset cannot be misused later on the conference base station.

Protecting Pairing (EPOS)

Data exchanged over the charging interface

Wireless Pairing (Alternative)

Data exchanged 'over the air'

Other Security Measures in DECT Devices

Per Call Authentication
Every time a call is made, the base needs to ensure that the connected headset has been paired – and is therefore safe to communicate with. The base does this by sending a random number stream – also known as a 'challenge' – to the headset. The headset and base station then simultaneously run an authentication algorithm, using the random numbers and Master Security Key as input. The headset sends its 'response' back to the base station 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 Session Encryption Key, which is further described in the "Encryption" section below.

The Per call authentication process flow:

BASE STATION	AIR	HEADSET
1 Generate **Random number stream**	2 **Send** 'Challenge' →	3 **Calculate** response
5 **Calculate** response	4 **Send** response ←	
6 **Check** if Base station and headset responses match		
7a Match: **Continue call** 'Session Key' generated		
7b No match: **Call rejected**		

About DECT Technology[1]

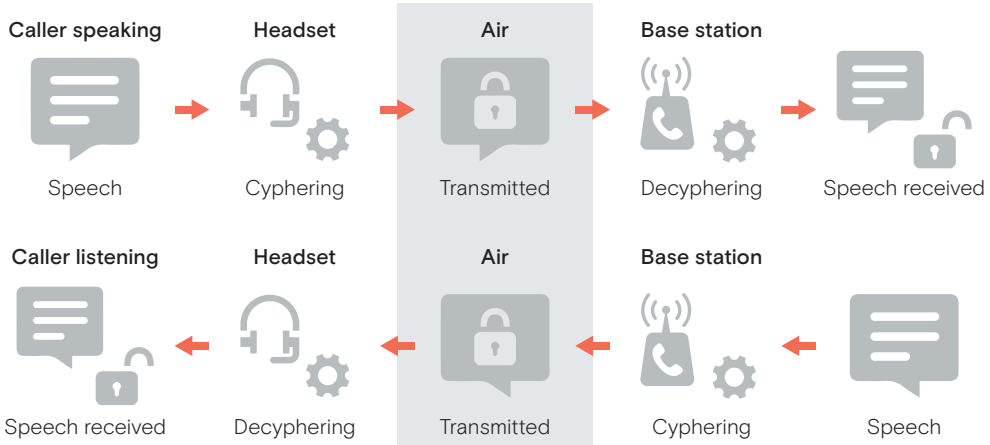
It is the industry standard to authenticate headsets 'over the air' prior to each call. While this data can be 'sniffed' by an intruder, it is of little value without knowing the Master Security Key. In the case of EPOS devices, it would only be possible to retrieve the data used to calculate the Master Security Key with physical access, making it even more difficult, and virtually impossible, for intruders to attack.

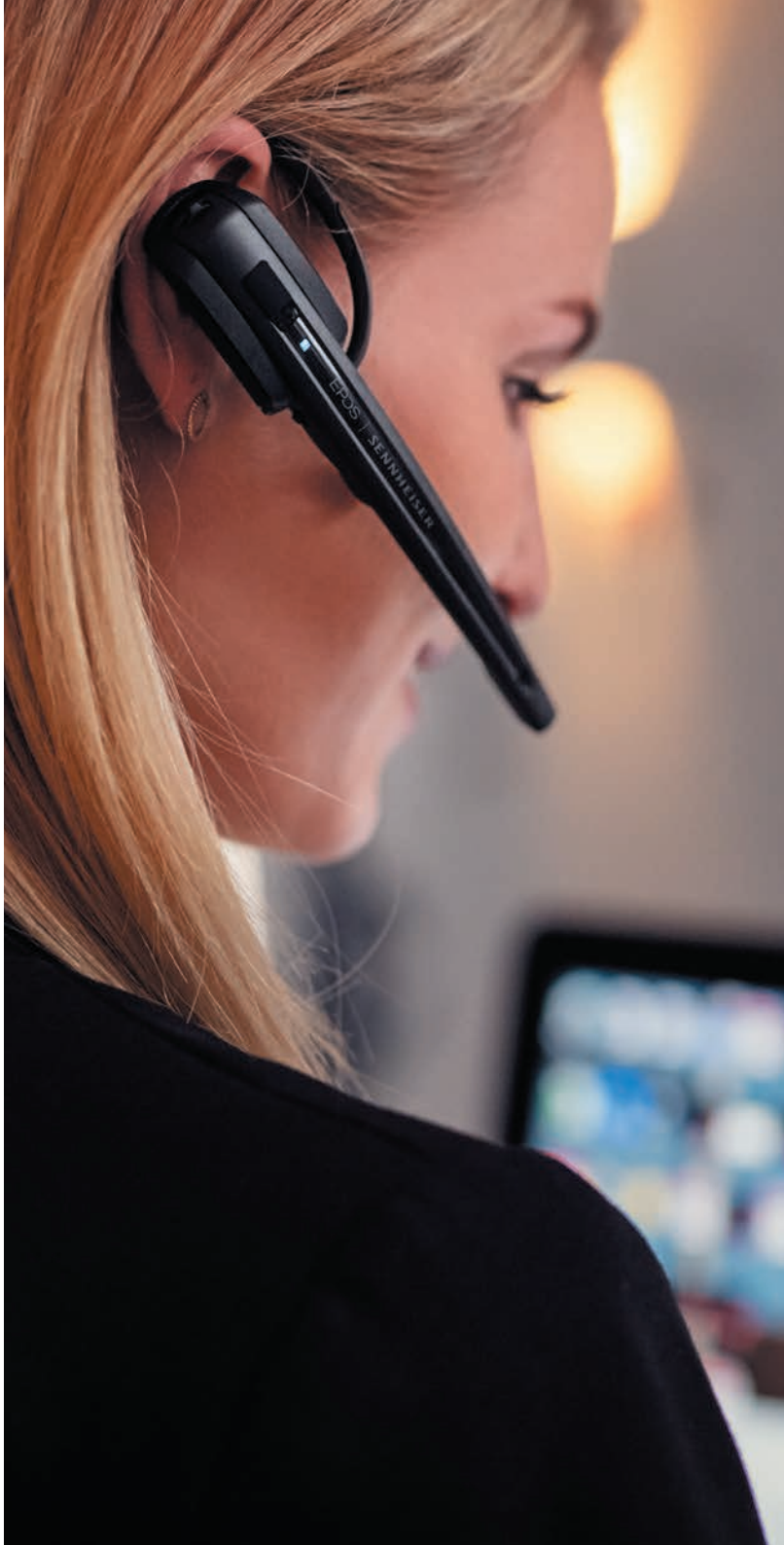
Encryption

Once a secure link is established between the headset and base, the units can communicate. To protect against passive eavesdropping, voice data is encrypted in both directions. A DECT standard encryption algorithm called DSC (with 64-bit encryption key) is used to encrypt voice data and call-related digital signaling. For an unauthorized user, the encrypted data would look like a meaningless stream of digital data.

A new Session Encryption Key is produced for each call during the Per Call Authentication process (as described previously). As a result, an intruder cannot gain access to the Session Encryption Key without hacking into the pairing process. In the case of EPOS devices, this can only be done through a physical connection between headset and base, making the exchange of voice data extremely secure.

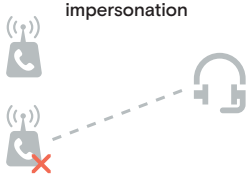
The encryption process flow:





Security Concerns and Countermeasures

The security features described provide a very high security level against unauthorized access. The table below summarizes the main perceived threats and countermeasures.

Security breach	Description of threat	Security level: Standard DECT devices*	Security level: EPOS DECT devices
Eavesdropping 	A third-party gains access to a call and listens in.	**High** The standard built-in DECT protocol provides a high level of security. However, the system is exposed during the pairing process if data is transferred wirelessly. The security level is further weakened if 'easy pairing' is enabled; Specialized skills and equipment would be required.	**Very high** An intruder would require access to the Master Security Key, which is never exchanged 'over the air'. The standard built-in DECT protocol provides additional security.
Base station impersonation 	A third-party uses an unauthorized base station to gain access to an authorized headset. The unauthorized base can then be used to listen to or redirect calls.	**High** There are practical barriers to this type of intrusion and even more specialized knowledge and equipment are required. If access is gained, the chances of deciphering anything meaningful from the data are slim.	**Very high** Due to the Protected Pairing process, physical access to the devices would be required to try to impersonate the base station.
Fraud 	A third-party uses an unauthorized headset to connect to an authorized base. The unauthorized headset is then used to place unauthorized calls.	**High** This is unlikely, since a user would need to gain access to a headset and know how to re-program the identities. It also requires a 'sniffing tool' and to physically be in the DECT range to capture the identities.	**Very high** A 'sniffing tool' would be of no use since pairing data is transferred over the charging terminals. Physical access to the headset would be required, which makes this kind of intrusion extremely challenging to execute in practice.

Intruders' focus point

* Standard DECT devices defined as those using 'over the air' pairing procedures

406883196

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