White Paper

Security Features in the SDW 5000 Headset Series

SENNHEISER

Executive Summary

This white paper addresses the security level of Sennheiser's triple connectivity DECT headset system, the SDW 5000 Series.

First, it describes DECT technology and the DECT Security certification program. Second, it outlines the DECT security chain comprised of "Pairing", "Per Call Authentication" and "Encryption", while highlighting the benefits of the DECT Security Certification.

Sennheiser has a Protected Pairing process which transfers sensitive pairing data via the charging terminal of the SDW 5000 base station instead of 'over the air'. The security of the pairing process is further enhanced by the authentication algorithm (DSAA2), which uses AES-128-bit keys. By having implemented this enhanced algorithm, the SDW 5000 Series has reached step B in the DECT security level. Step B makes the SDW 5000 Series even more secure than DECT products that have only implemented the DECT security step A. Per call authentication ensures that the headset and base station authenticate each other prior to every call. The encryption of voice data is strengthened by early encryption and re-keying, two features mandatory for the DECT Security Certification which are explained further in the white paper.

Additional security is added by not supporting the GAP mode on the base station. Sennheiser is the first and only manufacturer certified within the DECT Security Certification program, who is not supporting the GAP mode.

Finally, this white paper presents more security measures controllable via the software application HeadSetup™ Pro Manager. The IT administrator can disable conference mode, call merging or the USB port of the base station. Consequently, intruders are not able to listen in on calls and Bluetooth® restricted environments are safeguarded against any attempts to misuse the USB port on the base station.

Overview of Security Benefits

Features in the SDW 5000 Series

DECT Security certified ☑

Sennheiser Protected Pairing ☑

GAP mode not supported on base station ☑

Features in Sennheiser HeadSetup™ Pro Manager

Disable conference mode ☑

Disable call merging ☑

Disable USB port ☑

Figure 1 Overview of Security Benefits

About DECT Technology & Security

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.

DECT Security Certification

To meet the increased demand for secure communications, the DECT Forum, which is the international association of the wireless home and enterprise communication industry, 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. The SDW 5000 Series has successfully been assessed by the qualification body and as a result, obtained the DECT Security Certificate of Conformity.

The DECT Security Chain

The DECT security chain consists of the three main processes "Pairing", "Per Call Authentication" and "Encryption".

DECT enabled devices usually follow these processes. However, the SDW 5000 Series adds security on top of the standard pairing and encryption processes:

1. Pairing: The SDW 5000 Series has a Protected Pairing process for the initial pairing which happens via the charging terminal of the base station (provisional patent pending). During the pairing process, it uses AES-128-bit keys which correspond to step B of the DECT security level. This is twice as much as standard DECT products using only 64-bit keys (step A of the DECT security level).

3. Encryption: The SDW 5000 Series changes the Derived Cipher Key (DCK) at short intervals used for encryption during an ongoing call.

In the following chapters, the three processes will be described in detail.

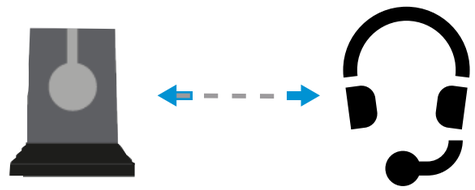
Order	Process	Description	Main purpose	Frequency
1	Pairing	Registration of security bindings between headset & base station	Ensure connection established between authorized devices	Once, during set-up
2	Per Call Authentication	Verification of security bindings between registered headset & base	Verify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

Figure 2 The DECT Security Chain

Protected Pairing (Sennheiser)

Data exchanged over the charging interface

Wireless pairing (Alternative)



Data exchanged ‘over the air’

Figure 3 Protected Pairing vs Wireless Pairing

1

Protected Pairing

Sennheiser’s SDW 5000 Series has a Protected Pairing process (provisional patent pending) ensuring a very high degree of security.

Rather than transferring pairing data (or Master Security Key) ‘over the air’, the charging terminals are used for data communication. This means that a Sennheiser headset needs to be physically docked into a Sennheiser base station, so that the registration and security bindings can 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.

When the SDW headset is paired to the base station, the Master Security Key is randomly generated. The improved authentication algorithm (DSAA2) uses AES-128-bit-keys to verify that the Master Security Key in the headset and base station is identical.

One Master Security Key is generated per headset per pairing and is never shared between headsets. For any new headset that registers on the base station, a new Master Security Key will be generated and the previous one will be forgotten. When a DECT conference is established on the base station, a unique Master Security Key will be generated for each individual DECT connection in the conference.

2

Per Call Authentication

Every time a call is made, the base station needs to ensure that the connected headset has been paired – and is therefore safe to communicate with. The base station 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 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 little value without knowing the Master Security Key. In the case of Sennheiser devices, it would only be possible to retrieve the data used to generate the Master Security Key with physical access, making it even more difficult, and virtually impossible, for intruders to attack.

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**		

Figure 4 The Per Call Authentication Process Flow

3

Encryption

The overall purpose of encryption is to protect the confidentiality of digital data transmitted between parties and thereby preventing unauthorized third parties from accessing the data. For a business headset system the data transmitted ‘over the air’ partly consist of digitized voice and partly 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, it is a process which cannot be by-passed. Early encryption is a process required by the DECT Security certification, 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 from the very beginning until the first Derived Cipher Key has been calculated.

The encryption protocol is designed to detect if the peer (headset) behaves slightly differently than expected. If this happens, the system will assume that it is an attempt to breach security and the link will be released. This feature is required in order to comply with the DECT Security certification, and will not risk the termination of legitimate calls.

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

Consequently, an intruder cannot gain access to the Derived Cipher Key without hacking into the pairing process. In the case of Sennheiser devices, this can only be done through a physical connection between headset and base, making the exchange of voice data extremely secure.

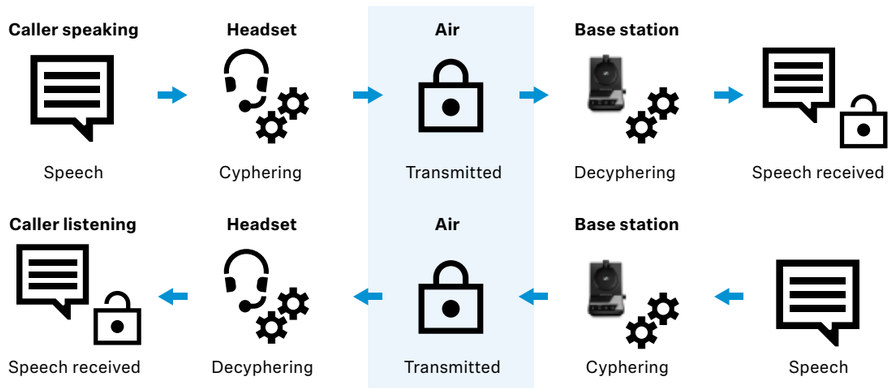


Figure 5 The Encryption Process Flow

Re-keying

SDW 5000 has 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 base station 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 hack 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 a wrong authentication result, the base will immediately drop the call. Trying to decode the data stream using the wrong Derived Cipher Key will create a monotonous tone.

GAP mode not supported in the base station

The purpose of the Generic Access Profile (GAP) is to ensure interoperability ‘over the air’ between equipment from difference manufactures. The SDW base station does not allow pairing with any other headset than Sennheiser’s SDW headset. This is an added security benefit as it prevents passive listening-in via a remote GAP headset.

Sennheiser is the first and only manufacturer certified within the DECT Security Certification program, who does not support the GAP mode on the base station. All other manufactures have, until now, been required to support it.

Security controls in HeadSetup™ Pro Manager

The SDW 5000 Series offers more security measures controllable via the software application HeadSetup™ Pro Manager. The IT administrator can lock settings such as disabling the conference mode, call merging or the USB port of the base station.

Disable conference mode

If the IT administrator wants to ensure that no third party can secretly join any call in the company, the conference mode can be disabled via HeadSetup™ Pro Manager. This measure secures that any given base station can only connect with one headset at a time and no additional headset can be paired with the base station.

When the conference mode is enabled, the Master headset user has full control over all DECT conference participants. Once a participant wants to join the conference, the Master headset user will be notified and needs to accept the participant in the call by pressing the headset's hook button. The conference can be terminated by the Master headset user when docking the headset in the base station.

Disable call merging

With HeadSetup™ Pro Manager is it also possible to disable the "call merging" feature to ensure that no external party can accidently be merged into a confidential call by the user of the SDW 5000 Series. When call merging is disabled, the user can only toggle between two calls, but not merge them together into one call.

Disable USB port

The USB port can be disabled via HeadSetup™ Pro Manager which means that all power running through the USB port is cut. Consequently, neither the BTD 800 USB dongle nor any other headsets or devices can be powered through the USB port.

Even though the USB port can be disabled, it should be noted that when the USB port is enabled, the functionality is intentionally restricted. Besides supplying charging current for a mobile device, it can only convey audio data, USB HID for call control and firmware update. The latter three functionality areas are restricted to Sennheiser audio devices only. Since only audio is supported on the USB port, it cannot be misused for purposes of accessing data or other kinds of information.

In high security environments where Bluetooth® is not allowed, the IT administrator can disable the USB port to prevent users from using a Bluetooth® connection via the BTD 800 USB dongle. Bluetooth® is considered by some to be somewhat less secure than DECT, since the devices must be set into pairing mode and become "discoverable" for a short while. Even though the security threat in that moment is hypothetical, Sennheiser has addressed the issue through the intelligent use of innovative solutions.

When the Bluetooth® devices have discovered each other, they exchange a 128-bit security key for authentication. After exchanging the security key, the devices are successfully paired. The secret key is the "bridge" between the devices that is formed after the initial pairing. After pairing is complete, the devices can continue to use this key, which eliminates the need for repeating the pairing process each time the devices are used.

It is extremely difficult to eavesdrop or to interfere with Bluetooth® communication for many reasons, including the short range and the authentication that must take place to use the devices.

www.sennheiser.com

SENNHEISER

1152 5-2018 GLOBAL