Sicherheits-funktionen der Headset-Serie SDW 5000

Zusammen-fassung

Dieses White Paper befasst sich mit dem Sicherheitskonzept der IMPACT SDW 5000-Serie, des DECT-Headset-Systems mit dreifacher Konnektivität von EPOS.

Zunächst werden die DECT-Technologie und das DECT-Sicherheitszertifizierungsprogramm beschrieben. Danach wird die DECT-Sicherheitskette erläutert, die aus „Pairing“, der „Authentifizierung pro Anruf“ und der „Verschlüsselung“ besteht. Dabei werden die Vorteile der DECT-Sicherheitszertifizierung hervorgehoben.

EPOS verfügt über einen Protected Pairing-Prozess, der sensible Pairing-Daten anstatt over-the-air über die Ladekontakte der IMPACT SDW 5000-Basisstation überträgt. Die Sicherheit des Pairing-Prozesses wird durch den Authentifizierungsalgorithmus (DSAA2) weiter verbessert, der AES-128-Bit-Keys verwendet. Durch die Implementierung dieses verbesserten Algorithmus konnte die IMPACT SDW 5000-Serie DECT-Sicherheitsstufe B erreichen. Stufe B macht die IMPACT SDW 5000-Serie noch sicherer als DECT-Produkte, die nur über DECT-Sicherheitsstufe A verfügen. Die Authentifizierung pro Anruf stellt sicher, dass sich das Headset und die Basisstation vor jedem Anruf gegenseitig authentifizieren. Die Verschlüsselung der Sprachdaten wird durch die frühzeitige Verschlüsselung und die erneute Eingabe verstärkt – zwei für die DECT-Sicherheitszertifizierung obligatorische Funktionen, die im White Paper näher erläutert werden.

Zusätzliche Sicherheit wird gewährleistet, indem der GAP-Modus an der Basisstation nicht unterstützt wird. EPOS ist der erste und einzige Hersteller, der im Rahmen des DECT-Sicherheitszertifizierungsprogramms zertifiziert wurde und den GAP-Modus nicht unterstützt.

Und schließlich werden in diesem White Paper weitere Sicherheitsmaßnahmen vorgestellt, die über die Software-Anwendung EPOS Manager gesteuert werden können. Der IT-Administrator kann den Konferenzmodus, das Zusammenführen von Anrufen oder den USB-Anschluss der Basisstation deaktivieren. Folglich können Anrufe nicht abgehört werden und Umgebungen, in denen Bluetooth® gesperrt ist, sind gegen jeglichen Versuch geschützt, den USB-Anschluss an der Basisstation zu missbrauchen.

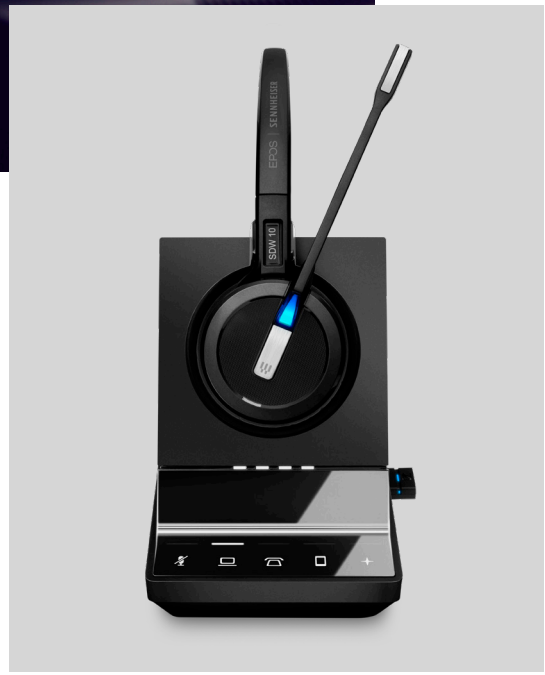
Über DECT-Technologie und Sicherheit

Digital Enhanced Cordless Telecommunications (DECT™) ist der Standard des Europäischen Instituts für Telekommunikationsnormen (ESTI) für die kabellose Kommunikation über kurze Strecken und kann für Sprach-, Daten- und Netzwerkanwendungen angepasst werden.

Die DECT-Technologie ist zum weltweiten Standard für die sichere private und geschäftliche kabellose Telefonkommunikation geworden. Über 110 Länder haben das DECT-System eingeführt, mit dem über 100 Millionen neue Geräte pro Jahr verkauft werden.

DECT-Sicherheitszertifizierung

Um der gestiegenen Nachfrage nach sicherer Kommunikation gerecht zu werden, hat das DECT-Forum, die internationale Vereinigung der drahtlosen Heim- und Unternehmenskommunikationsindustrie, das DECT-Sicherheitszertifizierungsprogramm eingeführt. Das Zertifizierungsprogramm besteht aus einer Reihe von Anforderungen und Sicherheitsfunktionen, die bei ihrer Implementierung in einem Produkt durch ein akkreditiertes und unabhängiges Testlabor validiert werden, um deren Einhaltung zu gewährleisten. Die IMPACT SDW 5000-Serie wurde erfolgreich von der Prüfstelle für Qualifikationen bewertet und erhielt folglich die DECT-Sicherheitskonformitätsbescheinigung.



Sicherheitsvorteile auf einen Blick

Funktionen der SDW 5000-Serie

- DECT-Sicherheitszertifiziert ☑
- EPOS Protected Pairing ☑
- GAP-Modus nicht unterstützt an der Basisstation ☑

Funktionen im EPOS Manager

- Deaktivierung des Konferenz-Modus ☑
- Deaktivierung der Zusammenführung von Anrufen ☑
- Deaktivierung des USB-Anschlusses ☑

Die DECT-Sicherheitskette

Die DECT-Sicherheitskette besteht aus drei Hauptprozessen: „Pairing“, „Authentifizierung pro Anruf“ und „Verschlüsselung“.

DECT-fähige Geräte folgen normalerweise diesen Prozessen. Die IMPACT SDW 5000-Serie verfügt jedoch neben den standardmäßigen Pairing- und Verschlüsselungsprozessen über zusätzliche Sicherheitsfunktionen:

1. Pairing: Die IMPACT SDW 5000-Serie verfügt über einen Protected Pairing-Prozess für das erstmalige Pairing, das über den Ladekontakt der Basisstation erfolgt (vorläufig angemeldetes Patent). Während des Pairing-Prozesses werden AES-128-Bit-Keys verwendet, die der DECT-Sicherheitsstufe B entsprechen. Das sind doppelt so viele Bit-Keys wie die 64-Bit-Keys, die von Standard-DECT-Produkten verwendet werden (DECT-Sicherheitsstufe A).

3. Verschlüsselung: Die IMPACT SDW 5000-Serie ändert den abgeleiteten Chiffrierschlüssel (DCK) in kurzen Intervallen, die der Verschlüsselung während eines aktiven Anrufs dienen.

In den folgenden Kapiteln werden die drei Prozesse detailliert beschrieben.

Folge	Prozess	Beschreibung	Hauptzweck	Häufigkeit
1	Pairing	Registrierung von Sicherheitsbindungen zwischen Headset und Basisstation	Sicherstellen, dass die Verbindung zwischen autorisierten Geräten hergestellt wurde	Einmal, während der Einrichtung
2	Authentifizierung pro Anruf	Überprüfung der Sicherheitsbindungen zwischen dem registrierten Headset und der Basisstation	Sicherstellen, dass die Verbindung zwischen autorisierten Geräten hergestellt wurde	Jeder Anruf
3	Verschlüsselung	Verschlüsselung von Sprachdaten während eines Anrufs	Gesprächsdaten für Eindringlinge unbrauchbar machen	Kurze Intervalle während eines Anrufs

1.
Protected Pairing

Die IMPACT SDW 5000-Serie von EPOS verfügt über einen Protected Pairing-Prozess (vorläufig angemeldetes Patent), der ein sehr hohes Maß an Sicherheit gewährleistet.

Anstatt Pairing-Daten (bzw. den Master Security Key) over-the-air zu übertragen, werden die Ladekontakte für die Datenkommunikation verwendet. Dies bedeutet, dass ein Headset von EPOS an eine Basisstation von EPOS angedockt werden muss, um die Registrierung und die Sicherheitsbindungen einzurichten. Dadurch ist es praktisch unmöglich für Dritte, die Pairing-Daten von einem entfernten Standort aus „aufzuspüren“ oder abzufangen.

Da der Master Security Key auf den Geräten gespeichert ist und niemals over-the-air übertragen wird, bietet diese Funktion bestmöglichen Schutz vor unbefugten Zugriffen jeglicher Art.

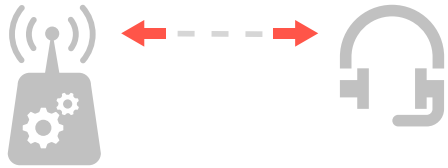
Wenn das SDW-Headset mit der Basisstation verbunden ist, wird der zentrale Sicherheitsschlüssel zufällig generiert. Der verbesserte Authentifizierungsalgorithmus (DSAA2) verwendet AES-128-Bit-Keys, um sicherzustellen, dass die Master Security Key des Headsets und der Basisstation identisch sind.

Pro Headset und pro Pairing wird ein Master Security Key generiert, der nie zwischen Headsets geteilt wird. Für jedes neue Headset, das an der Basisstation registriert wird, wird ein neuer Master Security Key generiert und der vorherige wird vergessen. Wenn eine DECT-Konferenz an der Basisstation eingerichtet wird, wird für jede einzelne DECT-Verbindung der Konferenz ein eindeutiger Master Security Key generiert.

Protected Pairing (EPOS)

Datenaustausch über die Ladekontakte

Kabelloses Pairing (Alternative)



Datenaustausch over-the-air

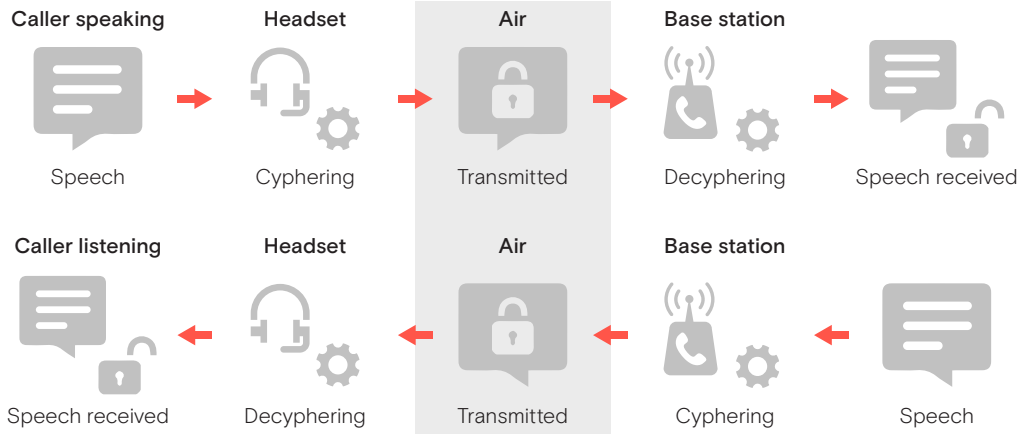
2. Authentifizierung pro Anruf

Bei jedem Anruf muss durch die Basisstation sichergestellt werden, dass das verwendete Headset verbunden wurde und die Kommunikation damit sicher ist. Dies wird von der Basisstation überprüft, indem sie eine zufällige Zahlenabfolge – was auch als Herausforderung bekannt ist – an das Headset sendet. Das Headset und die Basisstation führen dann gleichzeitig einen Authentifizierungsalgorithmus aus, für den die Zufallszahlen und der Master Security Key als Eingabe verwendet werden. Das Headset sendet seine „Antwort" zurück an die Basisstation und wenn die Berechnungsausgaben übereinstimmen, kann der Anruf getätigt werden. Wenn dies nicht der Fall ist, wird der Anruf abgewiesen. Eine weitere Ausgabe des Prozesses „Authentifizierung pro Anruf" ist die Generierung eines abgeleiteten Chiffrierschlüssels. Dies wird im Abschnitt zur Verschlüsselung näher erläutert.

Headsets zu Beginn jedes Anrufs over-the-air zu authentifizieren ist Industriestandard. Obwohl diese Daten von Unbefugten „aufgespürt" werden können, sind sie ohne den Master Security Key von geringem Wert. Bei Geräten von EPOS wäre es nur möglich, die für die Generierung des Master Security Key verwendeten Daten durch physischen Zugriff zu erlangen. Dies macht es unbefugten Zugriffen noch schwerer und ein Angriff ist praktisch unmöglich.

BASISSTATION	AIR	HEADSET
1 Generierung einer zufälligen Zahlenabfolge	2 „Herausforderung" **senden** →	3 Antwort **berechnen**
5 Antwort **berechnen**	4 Antwort **senden** ←	
6 Überprüfen, ob die Antworten der Basisstation und des Headsets übereinstimmen		
7a Übereinstimmung: **Anruf fortsetzen** „Session Key" wurde generiert		
7b Keine Übereinstimmung: **Anruf abgewiesen**		

3. Verschlüsselung



Der allgemeine Zweck der Verschlüsselung besteht darin, die Vertraulichkeit digitaler Daten zu schützen, die zwischen Parteien übertragen werden, und dadurch unbefugte Dritte daran zu hindern, auf diese Daten zuzugreifen. Bei einem professionellen Headset-System bestehen die over-the-air übertragenen Daten zum Teil aus digitalisierter Sprache und zum Teil aus Informationen zur Verbindungssteuerung. Ein verschlüsseltes System besteht aus einem Algorithmus, der die Verschlüsselung durchführt, und einem Eingabeschlüssel für den Algorithmus.

Ein standardmäßiger DECT-Verschlüsselungsalgorithmus namens DSC (mit 64-Bit-Keys) wird für die Verschlüsselung von Sprachdaten (in beide Richtungen) und anrufbezogenen digitalen Signalisierungen verwendet. Um sich vor passivem Abhören durch einen unbefugten Dritten zu schützen, erscheinen die verschlüsselten Daten als eine bedeutungslose Reihe von digitalen Daten.

Initiation der Verschlüsselung

Alle Anrufe werden verschlüsselt. Dieser Prozess kann nicht umgangen werden. Die frühzeitige Verschlüsselung ist ein Prozess, der für die DECT-Sicherheitszertifizierung erforderlich ist und sicherstellt, dass keine Sprach- oder Gesprächsdaten vor der Aktivierung der Verschlüsselung ausgetauscht werden können. Bei der frühzeitigen Verschlüsselung wird beim Pairing ein standardmäßiger Chiffrierschlüssel generiert, der von Anfang an für die Verschlüsselung verwendet wird, bis der erste abgeleitete Chiffrierschlüssel berechnet wurde.

Das Verschlüsselungsprotokoll ist so ausgerichtet, dass es erkennt, ob sich der Peer (Headset) etwas anders verhält als erwartet. Wenn dieser Fall eintritt, wird dies vom System als Sicherheitsverstoß angesehen und die Verbindung wird gelöst. Diese Funktion ist erforderlich, um der DECT-Sicherheitszertifizierung zu entsprechen und es besteht dadurch kein Risiko, dass legitime Anrufe beendet werden.

Für jeden Anruf wird während des Prozesses „Authentifizierung pro Anruf“ ein neuer abgeleiteter Chiffrierschlüssel erzeugt (wie zuvor beschrieben). Dadurch werden alle vorherigen Verschlüsselungsinformationen für den neuen Verbindungsaufbau ungültig.

Folglich haben unbefugte Dritte keinen Zugriff auf den abgeleiteten Chiffrierschlüssel, ohne sich in den Pairing-Prozess einzuhacken. Bei Geräten von EPOS ist dies nur durch die physische Verbindung zwischen dem Headset und der Basisstation möglich, was den Austausch von Sprachdaten äußerst sicher macht.

Erneute Eingabe

Das IMPACT SDW 5000 verfügt über einen Re-Keying-Prozess. Dabei handelt es sich um eine weitere Funktion, die durch das DECT-Sicherheitszertifizierungsprogramm zertifiziert wurde. Dafür wird der abgeleitete Chiffrierschlüssel ungefähr alle 60 Sekunden während eines Anrufs geändert. Dies bedeutet, dass die 64-Bit-Keys während eines Anrufs kontinuierlich erneuert werden, wenn die Basisstation und das Headset die Verbindung für den Anruf hergestellt haben. Im sehr unwahrscheinlichen Fall, dass es ein Threat Actor schafft, den abgeleiteten Chiffrierschlüssel zu hacken, wird dieser innerhalb von max. 60 Sekunden ungültig. Dies dient als Schutz gegen Brute-Force-Angriffe zum Knacken der Verschlüsselung.

Wenn das Headset die Authentifizierung ablehnt oder mit einem falschen Authentifizierungsergebnis antwortet, beendet die Basisstation den Anruf unverzüglich. Der Versuch, den Datenstrom mit dem falschen abgeleiteten Chiffrierschlüssel zu dekodieren, führt zur Erzeugung eines monotonen Tones.

GAP-Modus wird an der Basisstation nicht unterstützt

Der Zweck des Generic Access Profile (GAP) besteht darin, die Interoperabilität zwischen Geräten verschiedener Hersteller over-the-air zu gewährleisten. Die SDW-Basisstation kann mit keinem anderen Headset als dem SDW-Headset von EPOS verbunden werden. Dies ist ein zusätzlicher Sicherheitsvorteil, da dadurch das passive Abhören mit Hilfe eines dezentralen GAP-Headsets verhindert wird.

EPOS ist der erste und einzige Hersteller, der im Rahmen des DECT-Sicherheitszertifizierungsprogramms zertifiziert wurde und den GAP-Modus an der Basisstation nicht unterstützt. Für alle anderen Hersteller war es bisher erforderlich, diesen zu unterstützen.

Sicherheits-kontrollen des EPOS Manager

Die SDW 5000-Serie bietet mehr Sicherheitsmaßnahmen, die über die Software-Anwendung EPOS Manager gesteuert werden können. Der IT-Administrator kann Einstellungen sperren und beispielsweise den Konferenzmodus, das Zusammenführen von Anrufen oder den USB-Anschluss der Basisstation deaktivieren.

Konferenzmodus deaktivieren
Wenn der IT-Administrator sicherstellen möchte, dass keine unberechtigten Dritten an Anrufen im Unternehmen teilnehmen können, kann der Konferenzmodus über den EPOS Manager deaktiviert werden. Durch diese Maßnahme wird sichergestellt, dass jede Basisstation nur mit jeweils einem Headset verbunden werden kann und keine Verbindung zwischen einem weiteren Headset und der Basisstation hergestellt werden kann.

Wenn der Konferenzmodus aktiviert ist, hat der Nutzer des Master-Headsets die volle Kontrolle über alle Teilnehmer der DECT-Konferenz. Wenn ein Teilnehmer an der Konferenz teilnehmen möchte, wird der Nutzer des Master-Headsets darüber benachrichtigt und muss den Teilnehmer in der Leitung durch Drücken der Verbindungstaste des Headsets annehmen. Die Konferenz kann durch den Nutzer des Master-Headsets beendet werden, indem das Headset an die Basisstation angedockt wird.

Zusammenführen von Anrufen deaktivieren
Mit dem EPOS Manager ist es auch möglich, die Funktion „Anrufzusammenführung“ zu deaktivieren, um sicherzustellen, dass Dritte nicht versehentlich vom Nutzer der IMPACT SDW 5000-Serie in einen vertraulichen Anruf eingebunden werden können. Wenn die Anrufzusammenführung deaktiviert ist, kann der Benutzer nur zwischen zwei Anrufen hin- und herwechseln, diese aber nicht zu einem Anruf zusammenführen.

USB-Anschluss deaktivieren
Der USB-Anschluss kann durch den EPOS Manager deaktiviert werden, was zur Unterbrechung der Stromversorgung des USB-Anschlusses führt. Folglich können weder der BTD 800 USB-Dongle noch jegliche andere Headsets oder Geräte über den USB-Anschluss mit Strom versorgt werden.

Obwohl der USB-Anschluss deaktiviert werden kann, sollte beachtet werden, dass die Funktionalität des USB-Anschlusses bei der Aktivierung absichtlich eingeschränkt ist. Neben der Bereitstellung des Ladestroms für ein mobiles Gerät können damit nur Audiodaten, USB-HID zur Call Control und Firmware-Updates übertragen werden. Die letzten drei Funktionsbereiche sind ausschließlich auf Audiogeräte von Sennheiser beschränkt. Da der USB-Anschluss nur Audio unterstützt, kann er nicht für den Zugriff auf Daten oder andere Arten von Informationen missbraucht werden.

In Umgebungen mit erhöhtem Sicherheitsbedarf, in denen Bluetooth® nicht zulässig ist, kann der IT-Administrator den USB-Anschluss deaktivieren, um zu verhindern, dass Benutzer eine Bluetooth®-Verbindung über den BTD 800 USB-Dongle herstellen. Bluetooth® wird manchmal als weniger sicher als DECT angesehen, da die Geräte in den Pairing-Modus versetzt werden müssen und für eine kurze Zeit „sichtbar“ werden. Obwohl die Sicherheitsbedrohung in diesem Moment hypothetisch ist, hat sich EPOS mit dem Problem durch die intelligente Verwendung von innovativen Lösungen befasst.

Wenn Bluetooth®-Geräte einander erkannt haben, tauschen sie einen 128-Bit-Key zur Authentifizierung aus. Nach dem Austausch des Sicherheitsschlüssels sind die Geräte erfolgreich miteinander verbunden. Der geheime Schlüssel bildet die „Brücke“ zwischen den Geräten, die nach dem erstmaligen Pairing gebildet wird. Wenn das Pairing abgeschlossen ist, können die Geräte diesen Schlüssel weiterhin verwenden. Dadurch muss der Pairing-Prozess nicht bei jeder Nutzung der Geräte wiederholt werden.

Es ist aus vielen Gründen sehr schwierig, die Bluetooth®-Kommunikation abzuhören oder zu stören. Zu diesen gehören die kurze Reichweite und die Authentifizierung, die für die Verwendung der Geräte durchgeführt werden muss.

1068407745

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