DECT™ Security

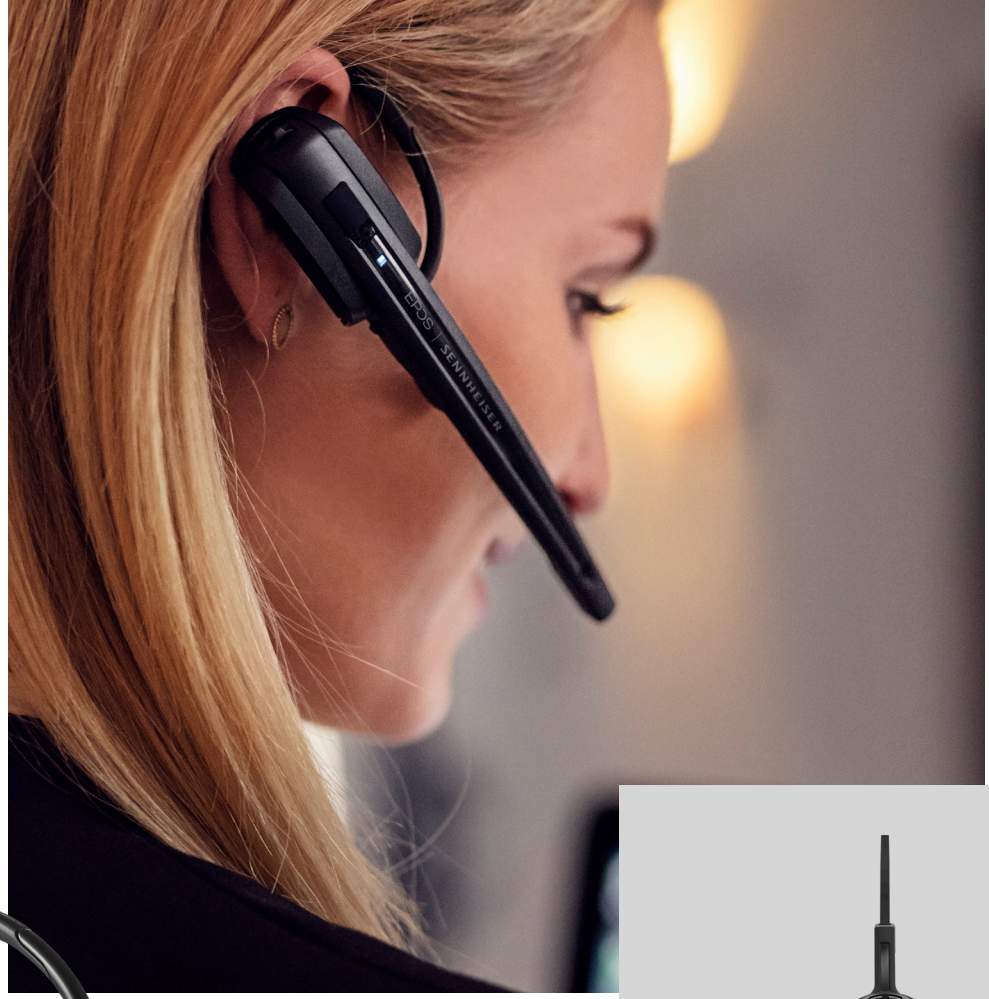
Kurzfassung

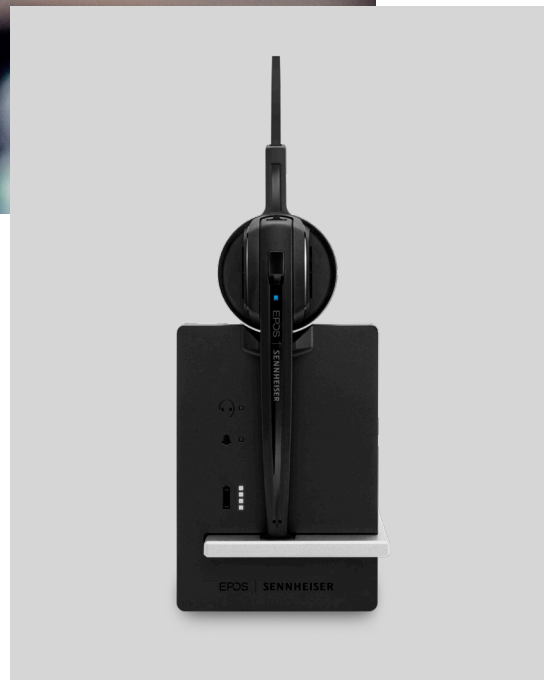
In diesem Whitepaper geht es um die Sicherheit von EPOS DECT-Headsets für Contact Center und Büros. Es beschreibt die DECT-Sicherheitskette, die sich aus den Schritten „Pairing“, „Authentifizierung pro Anruf“ und „Verschlüsselung“ zusammensetzt, die alle Bestandteil des DECT-Standardprotokolls sind.

Darüber hinaus wird erläutert, dass ein Eindringling die Sicherheit eines DECT-Systems nur dadurch beeinträchtigen kann, dass er Zugriff auf die Daten erhält, die bei der ersten Pairing von Headset und Basisstation ausgetauscht werden. Daher ist der Schutz des Pairingvorgangs vor nicht autorisierten Zugriffen entscheidend für die Sicherheit eines kabellosen Kommunikationssystems.

Bei Geräten von EPOS ist ein Pairing nur dann möglich, wenn das Headset tatsächlich an der Basisstation angedockt ist. Dadurch hat ein potenzieller Eindringling keine Möglichkeit, die Informationen kabellos zu berechnen oder abzufangen.

Durch diese Sicherheitsvorkehrung in Kombination mit den zusätzlichen Sicherheitsebenen des DECT-Standardprotokolls ist die Sicherheit bei DECT-Produkten von EPOS insgesamt sehr hoch. Sie sind praktisch immun gegen die gemeinhin wahrgenommenen Bedrohungen für kabellose Systeme: passives Mithören, Imitation der Basisstation und Betrug.





Über die DECT-Technologie[1]

DECT™ steht für „Digital Enhanced Cordless Telecommunications“, einen Standard der Europäischen Normenorganisation ETSI (European Telecommunications Standards Institute) für kabellose Kommunikation über kurze Strecken, der für viele Anwendungen im Bereich Sprach-, Daten- und Netzwerktechnik verwendet werden kann.

Die DECT-Technologie hat sich zum weltweiten Standard für die sichere Kommunikation mit Schnurlostelefonen im Privat- und Geschäftsbereich entwickelt. Über 110 Länder haben das DECT-System übernommen und jährlich werden über 100 Millionen Neugeräte verkauft.

1. Weitere Informationen finden Sie unter www.etsi.org und www.dect.org

Die DECT-Sicherheitskette

Die DECT-Sicherheitskette umfasst die drei Hauptprozesse:

Diese Prozesse werden von den meisten DECT-Geräten befolgt. Der DECT-Standard legt jedoch nicht exakt fest, wie der Austausch von Pairingdaten erfolgen soll. In den folgenden Abschnitten werden sowohl die generischen DECT-Prozesse als auch die zwei üblichen Pairingmethoden, die von Headset-Herstellern verwendet werden, detailliert behandelt.

Folge	Ablauf	Beschreibung	Zweck	Frequenz
1	Pairing	Registrierung der Sicherheitsanbindung zwischen Headset und Basisstation	Überprüfung der Verbindung zwischen autorisierten Geräten	Einmal, bei Einrichtung
2	Pro Anruf Authentifizierung	Verifizierung der Sicherheitsanbindungen zwischen registriertem Headset und Basisstation	Verfizierung, dass der Anruf zwischen autorisierten Geräten erfolgt	Jeder Anruf
3	Verschlüsselung	Verschlüsselung von Sprachdaten bei Anrufen	Unbrauchbarmachung der Anrufdaten für Eindringlinge	Jeder Anruf

Das Pairing – das Rückgrat der Sicherheit eines kabellosen Kommunikationssystems

Eine Übersicht über Validierung und Pairing
Damit zwischen einem DECT-Headset und einer Basisstation ein Pairing erfolgen kann, müssen sie sich zuerst über einen übereinstimmenden 4-stelligen PIN-Code validieren. In den meisten DECT-Headsets kommt ein automatischer Vorgang, das sogenannte „Easy Pairing", zum Einsatz. Er ermöglicht die Initiierung des Pairings, ohne dass der Benutzer manuell einen PIN-Code eingeben muss.

Sobald die Validierung abgeschlossen ist, kann das Pairing initiiert werden. Dieser Vorgang wird von einem Algorithmus gesteuert, der nur für DECT-Hersteller verfügbar ist, dem sogenannten DECT Standard Authentication Algorithm (DSAA). Der Algorithmus wird gleichzeitig im Headset und in der Basisstation ausgeführt, wobei der 4-stellige PIN-Code und eine Reihe von Zufallszahlen verwendet werden. Die Ergebnisse des Algorithmus werden ausgetauscht und müssen für eine erfolgreiche Kopplung übereinstimmen.

Der Master Security Key – so sperren Sie DECT-Eindringlinge aus
Eine weitere Ausgabe des DSAA-Algorithmus ist der Master Security Key (auch bekannt als 128-Bit UAK). Dieser Master Security Key wird auch von allen folgenden DECT-Sicherheitsverfahren verwendet. Da er verwendet werden könnte, um die Sicherheit eines DECT-Kommunikationssystems zu beeinträchtigen, sollte der Master Security Key unbedingt vor potenziellen Eindringlingen geschützt werden.

Kabellose Kopplung – ein verwundbarer Bereich in der DECT-Sicherheitskette – bei manchen DECT-Geräten
Eine Voraussetzung für DECT besagt, dass PIN-Code und Master Security Key niemals „over the air" ausgetauscht werden dürfen. Von manchen DECT-Geräten werden die zur Berechnung des Master Security Key verwendeten Daten jedoch kabellos übertragen. Dies bietet Angreifern die Möglichkeit, die Pairingdaten mit hoch entwickelten Geräten durch „Sniffing" abzufangen. Wenn der Eindringling über umfassendes Spezialwissen zur DECT-Verschlüsselung verfügt, dann könnte er theoretisch den Master Security Key berechnen und dadurch die Sicherheit des Systems beeinträchtigen.

Geschützte Kopplung – der Schlüssel zur Sicherheit der DECT-Geräte von EPOS
Die DECT-Geräte von EPOS haben aufgrund des zum Pairing eines Headsets mit der Basistation erforderlichen Vorgangs ein sehr hohes Sicherheitsniveau.

Statt die Pairingdaten „over the air" zu übertragen, werden die Ladestationen für die Datenkommunikation verwendet. Das bedeutet, dass ein Headset von EPOS tatsächlich an einer Basisstation von EPOS angedockt sein muss, damit die Registrierung und die Sicherheitsanbindung durchgeführt werden können. So ist es für Dritte praktisch unmöglich, die Pairingdaten von einem Remote-Standort aus per „Sniffing" abzufangen.

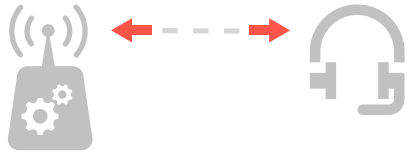
Da der Master Security Key auf den Geräten gespeichert und niemals kabellos übertragen wird, bietet diese Funktion den bestmöglichen Schutz gegen jegliche Art von nicht autorisiertem Zugriff.

Telefonkonferenzen durchführen – ein eindeutiger Master Security Key für jedes Headset verhindert Missbrauch
Die Headsets von EPOS ermöglichen die Durchführung einer DECT-Konferenz mit bis zu vier Headsets über eine Basisstation. In diesem Szenario erhält jedes Headset einen eigenen eindeutigen Master Security Key. Dadurch ist sichergestellt, dass der in einem Gast-Headset gespeicherte Master Security Key später nicht auf der für die Konferenz verwendeten Basisstation missbraucht werden kann.

Protecting Pairing (EPOS)

Datenaustausch über die Lade schnittstelle

Wireless Pairing (Alternative)



Datenaustausch „over the air"

Weitere Sicherheitsmaßnahmen in DECT-Geräten

Authentifizierung pro Anruf
Bei jedem Anruf muss die Basisstation sicherstellen, dass das angeschlossene Headset gekoppelt wurde und somit eine sichere Kommunikation möglich ist. Diese Überprüfung wird durchgeführt, indem die Basisstation eine Reihe von Zufallszahlen an das Headset sendet. Headset und Basisstation führen dann gleichzeitig einen Authentifizierungsalgorithmus aus, für den sie die Zufallszahlen und den Master Security Key als Eingabe verwenden. Das Headset sendet dann seine Antwort an die Basisstation und falls die Ergebnisse der Berechnungen übereinstimmen, kann der Anruf getätigt werden. Falls nicht, wird der Anruf abgelehnt. Ein weiteres Ergebnis der „Authentifizierung pro Anruf“ ist das Generieren eines Session Encryption Key, der weiter unten im Abschnitt „Verschlüsselung“ genauer beschrieben wird.

Der Prozessablauf bei der Authentifizierung pro Anruf:

BASISSTATION	AIR	HEADSET
1 Reihe von **Zufallszahlen erzeugen**	2 **Senden** von Zufallszahlen →	3 **Berechnung** der Antwort
5 **Berechnung** der Antwort	4 **Senden** der Antwort ←	
6 **Überprüfung** der Übereinstimmung der Antworten von Basisstation und Headset		
7a Übereinstimmung: **Anruf fortsetzen** Generieren des „Sitzungsschlüssels“		
7b Keine Übereinstimmung: **Anruf ablehnen**		

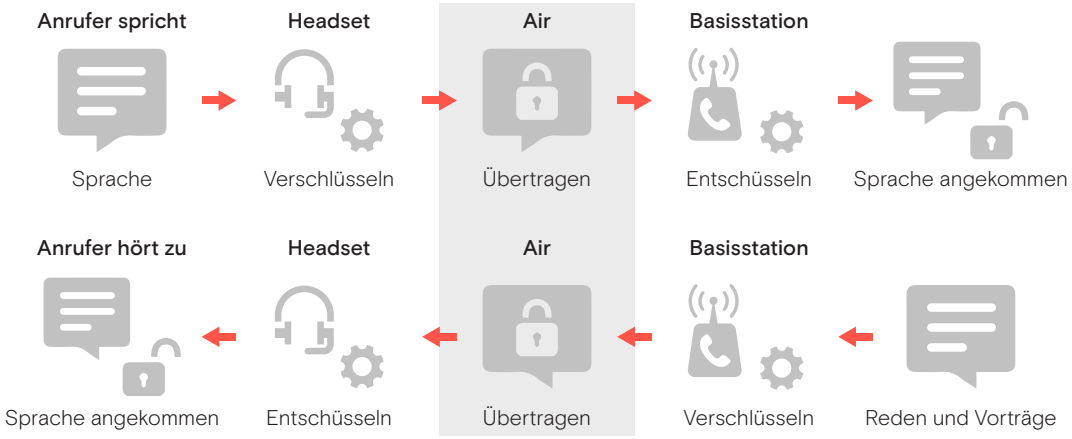
Über die DECT-Technologie

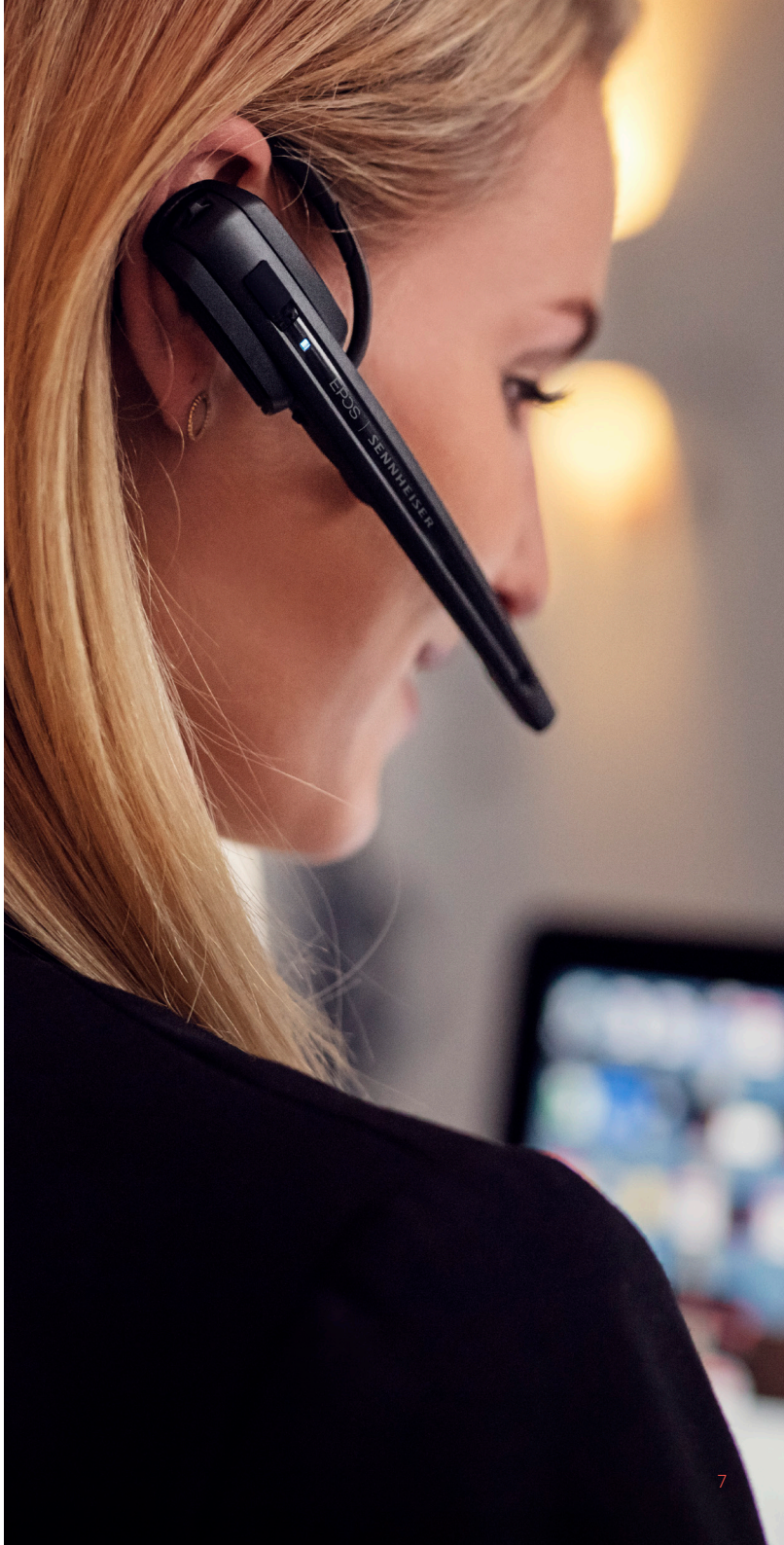
In der Branche ist es üblich, bei Headsets vor jedem Anruf eine Over-the-Air-Authentifizierung durchzuführen. Obwohl diese Daten von einem Eindringling per „Sniffing“ abgefangen werden können, sind sie ohne den Master Security Key absolut wertlos. Bei Geräten von EPOS könnten die zur Berechnung des Master Security Key verwendeten Daten nur dann abgerufen werden, wenn physisch auf das Gerät zugegriffen werden kann. Auf diese Weise ist ein Angriff für Eindringlinge sogar noch schwieriger und praktisch unmöglich.

Verschlüsselung
Sobald eine sichere Verbindung zwischen Headset und Basisstation besteht, können die Einheiten miteinander kommunizieren. Als Schutz vor passivem Mithören werden die Sprachdaten in beide Richtungen verschlüsselt. Für die Verschlüsselung dieser Sprachdaten sowie der anrufbezogenen digitalen Signale wird ein DECT-Verschlüsselungsalgorithmus mit der Bezeichnung DSC verwendet. Dieser Algorithmus arbeitet mit einer Schlüssellänge von 64 Bit. Für einen nicht autorisierten Benutzer wären die verschlüsselten Daten nichts weiter als ein bedeutungsloser digitaler Datenstrom.

Für jeden Anruf wird während der Authentifizierung pro Anruf ein neuer sitzungsspezifischer Verschlüsselungsschlüssel generiert (wie bereits beschrieben). Dadurch kann kein Eindringling auf den sitzungsspezifischen Verschlüsselungsschlüssel zugreifen, ohne sich in den Kopplungsvorgang zu hacken. Bei Geräten von EPOS ist dies nur über eine physische Verbindung zwischen Headset und Basisstation möglich, was den Austausch von Sprachdaten extrem sicher macht.

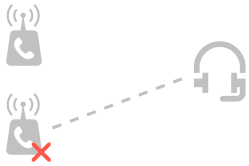
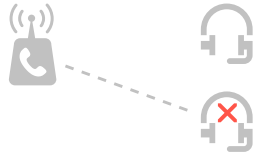
Der Prozessablauf der Verschlüsselung:





Sicherheitsbedenken und Gegenmaßnahmen

Die beschriebenen Sicherheitsfunktionen sorgen für einen sehr starken Schutz vor nicht autorisierten Zugriffen. Die nachstehende Tabelle fasst die wichtigsten Bedrohungen und entsprechende Gegenmaßnahmen zusammen.

Sicherheitsverstoß	Beschreibung der Bedrohung	Sicherheitsniveau: Standardmäßiges DECT-Gerät*	Sicherheitsniveau: DECT-Gerät von EPOS
Mithören 	Ein Dritter verschafft sich Zugriff auf einen Anruf und hört mit.	**Hoch** Das integrierte DECT-Standard-protokoll bietet einen sehr hohen Schutz. Falls die Daten jedoch kabellos übertragen werden, ist das System während des Kopplungsvorgangs gefährdet. Bei Aktivierung von „Easy Pairing“ ist die Sicherheit noch stärker beeinträchtigt. Spezielle Fähigkeiten und Ausrüstung wären erforderlich.	**Sehr hoch** Ein Eindringling würde Zugriff auf den Master Security Key benötigen, der niemals „over the air“ ausgetauscht wird. Das integrierte DECT-Standardprotokoll bietet zusätzlichen Schutz.
Imitation der Basisstation 	Ein Dritter verwendet eine nicht autorisierte Basisstation, um sich Zugriff auf ein autorisiertes Headset zu verschaffen. Diese nicht autorisierte Basisstation kann dann verwendet werden, um Anrufe mitzuhören oder umzuleiten.	**Hoch** Gegen diese Art der Bedrohung gibt es praktische Vorkehrun-gen und man benötigt noch größeres Fachwissen und noch ausgefeiltere Ausrüstung. Falls sich ein Eindringling auf diese Weise Zugriff verschaffen sollte, dann wäre die Wahrscheinlich-keit, dass er etwas Sinnvolles aus den Daten herauslesen könnte, überaus gering.	**Sehr hoch** Durch das geschützte Pairing wäre der physische Zugriff auf das Gerät nötig, um zu versuchen, die Basisstation zu imitieren.
Betrug 	Ein Dritter verwendet ein nicht autorisiertes Headset, um sich Zugriff auf eine autorisierte Basisstation zu verschaffen. Anschließend wird das nicht autorisierte Headset verwendet, um nicht autorisierte Anrufe zu tätigen.	**Hoch** Dieses Szenario ist unwahr-scheinlich, da ein Benutzer hierfür an ein Headset gelangen und dazu in der Lage sein müsste, die Identitäten neu zu programmieren. Des Weiteren wäre ein „Sniffing-Tool“ nötig und man müsste sich physisch innerhalb der DECT-Reichweite befinden, um an die Identitäten gelangen zu können.	**Sehr hoch** Ein „Sniffing-Tool“ wäre nutzlos, da die Pairingdaten über die Ladestationen übertragen werden. Man müsste physisch auf das Headset zugreifen können, wodurch diese Art des Eindringens in der Praxis äußerst schwer zu realisieren wäre.

✕ Hauptziel der Eindringlinge

* Standardmäßige DECT-Geräte sind in diesem Fall solche, bei denen das Pairing „over the air“ erfolgt.

406883196

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