Sécurité Bluetooth®

Introduction Sécurité Bluetooth®

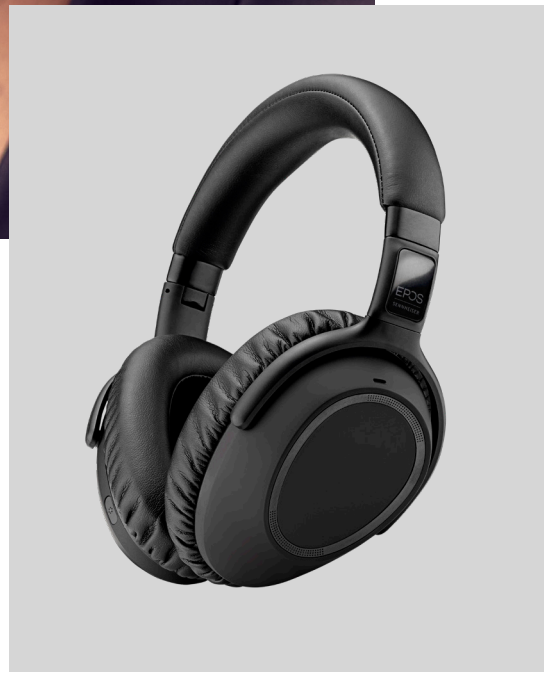
Pour EPOS, le confort, la qualité et la sécurité sont des domaines prioritaires. Ce document aborde la sécurité de la technologie Bluetooth® et la sécurité supplémentaire que le Centre d'appel de EPOS et les micro-casques de bureau (CC&O) fournissent.

Introduction

Bluetooth® est une norme de technologie sans fil pour l'échange de voix et de données sur de courtes distances entre des appareil Bluetooth®. Ericsson a introduit le Bluetooth® sur le marché en 1994 pour surmonter les défis de la connexion des appareils avec différents types de technologie et protocoles de sécurité.

Depuis son introduction, le Bluetooth® Special Interest Group regroupe plus de 20 000 entreprises partenaires et la norme Bluetooth® est devenue une méthode répandue et populaire pour connecter des appareils. Plus de 2 milliards d'unités peuvent utiliser la technologie Bluetooth®, ce qui a soulevé des inquiétudes concernant les problèmes de sécurité.

Avant d'entrer dans les détails sur la sécurité Bluetooth®, on doit préciser que globalement, le risque d'un accès non autorisé à la communication via Bluetooth® est limité. En général, le Bluetooth® offre un très haut niveau de sécurité, que EPOS a choisi d'améliorer à travers l'utilisation intelligente de solutions innovantes.



Comment le Bluetooth® fonctionne

La norme Bluetooth offre une connexion sans fil entre les appareils à proximité les uns des autres. Pour ce faire, les deux appareils doivent être appairés. L'appairage est comme une « poignée de main technologique » qui présente les deux appareils l'un à l'autre et leur permet de communiquer.

L'appairage nécessite que les deux appareils puissent se trouver – ils doivent être rendus « découvrables ». Pour la plupart des appareils Bluetooth, cela nécessite un processus actif de placement des appareils en mode d'appairage. Dans cette configuration, les appareils deviennent découvrables pendant une brève période et peuvent commencer à échanger une clé de sécurité pour l'authentification.

Une fois cette clé de sécurité échangée, qui n'est pas transmise sur le réseau et ne peut pas être volée, les appareils sont appairés avec succès. La clé secrète sert de « passerelle » entre les appareils et est générée après l'appairage initial. À l'avenir, ces appareils peuvent continuer à utiliser cette clé. De cette manière, il n'est pas nécessaire de répéter l'appairage à chaque fois que les appareils sont utilisés.

Cryptage pendant l'utilisation

Une fois les clés secrètes échangées, les deux appareils Bluetooth® peuvent communiquer. Tous les produits EPOS profitent du meilleur niveau de cryptage en utilisant une clé 128 bits créée par le processus d'appairage. Grâce à ce cryptage, les données envoyées entre les appareils peuvent uniquement être lues par le destinataire prévu. L'unité de réception décrypte les données à leur format d'origine selon le même algorithme.

Haut niveau de sécurité

Comme précédemment mentionné, la technologie Bluetooth® offre un haut niveau de sécurité à l'utilisateur. Il est extrêmement difficile d'écouter ou d'interférer avec la communication Bluetooth® pour de nombreuses raisons, y compris la courte portée et le processus d'authentification requis pour utiliser les appareils.

En théorie, le point le plus vulnérable pour les appareils Bluetooth® est lorsqu'ils sont en cours d'appairage car ils doivent être visibles/découvrables pour ce faire. Même si la menace de sécurité est hautement hypothétique, EPOS a résolu le problème avec plusieurs mesures intelligentes.

Différents types de menaces

Pour expliquer les avantages des micro-casques sécurisés de EPOS il est utile de lister les différents types de menaces dont nous parlons.

Attaque Man in the middle – Un pirate essaie d'intercepter des informations sur son appareil sans connaître l'attaqué. Il est très difficile de faire cela dans la vie réelle, car le pirate devrait être très proche des appareils.

Virus – Transmission sans fil d'un virus dangereux. Le micro-casque Bluetooth® EPOS et le dongle Bluetooth® ne transmettent que la parole, et non pas les données comme d'autres appareils Bluetooth®. Par conséquent, il n'y a aucun environnement permettant à un virus de s'exécuter.

Eavesdropping – Un pirate écoute une conversation. Le pirate doit être présent lors de l'appairage et avoir un équipement extrêmement avancé. Les voix sont cryptées et converties en flux numérique.

Les appareils modernes utilisent la norme Bluetooth® 4.0 et supérieure, en particulier pour l'utilisation de la transmission vocale, qui fournit un haut niveau de protection.

Sécurité supplémentaire de EPOS

Pour EPOS, la sécurité de l'utilisateur joue un rôle important dans le développement de produits. Nous avons pris des mesures supplémentaires pour renforcer le haut niveau de sécurité que la technologie Bluetooth® offre. Voici des exemples :

Gestion de puissance intelligente – Pendant l'appairage, la puissance de transmission des appareils Bluetooth® EPOS est réduite. Ce donne une portée bien plus courte lors de l'exécution du processus d'appairage. Les attaques « Man in the Middle » deviennent extrêmement difficiles à mener car l'appareil attaquant devrait être très proche des appareils s'appairant.

Sécurité d'accès à l'appareil hôte – Les micro-casques EPOS et les dongles USB correspondants ne prennent en charge que les profils Bluetooth® audio. Le contenu de données stocké sur l'appareil hôte ne peut jamais être transmis dans le micro-casque ou d'autres appareils. Cela signifie que les virus ne peuvent pas être transférés non plus.

Fenêtre d'appairage court – Les micro-casques EPOS ne peuvent être découverts que pendant de très courtes durées pendant l'appairage. Après cette courte durée, ils désactivent automatiquement l'accès Bluetooth® jusqu'à ce que l'accès soit réactivé par l'utilisateur autorisé.

Avis de non-responsabilité de EPOS

Chez EPOS, nous mettons tout en œuvre pour garantir les plus mesures de sécurité les plus élevées dans nos produits Bluetooth®. Toutefois, nous ne pouvons pas être tenus pour responsables quant à tout remboursement pour des dommages ou dépenses causées par des failles de la sécurité du côté du client en utilisant nos produits Bluetooth®.

Bien que EPOS ait mis en place des mesures de précaution pour garantir un haut niveau de sécurité, il est de la responsabilité du client de contrôler et configurer les paramètres appropriés de cet appareil Bluetooth® pour assurer la sécurité. Les mesures de sécurité mis en place dans l'appareil EPOS peuvent ne pas être prises en charge par l'appareil du client ce qui peut réduire le niveau de sécurité d'une connexion Bluetooth®.

Le client reconnaît que le cryptage de la connexion Bluetooth® ne s'applique qu'à la connexion sans fil entre les appareils appairés. Les liaisons et le contenu des communications transférés par une connexion Bluetooth® cryptée (ex. Appels téléphoniques) ne sont cryptés que par l'appareil Bluetooth® EPOS. Le client reconnaît également qu'aucune technologie ne fournit une sécurité complète. Pour des exigences de sécurité plus élevées que ce qui est offert par la norme Bluetooth®, d'autres mesures doivent être mises en œuvre par le client.

Néanmoins, EPOS sera responsable des dommages allant des blessures mortelles, corporelles ou de santé causées par une négligence ou un non-respect d'une obligation par EPOS ou de dommages découlant d'une violation causée par une négligence grossière ou d'une intention volontaire de EPOS.

EPOS est également responsable du non-respect de ses obligations contractuelles essentielles. Obligations contractuelles essentielles signifie obligations dont le respect est une condition préalable à la bonne exécution du contrat et sur laquelle partie contractante peut se reposer. Dans ce cas, le remboursement se limite aux dommages prévisibles et typiques.

Les provisions ci-dessus s'appliquent également aux dommages causés par un représentant légal ou une personne utilisée pour exécuter une obligation de EPOS.

La responsabilité de EPOS selon la Loi danoise/européenne sur la responsabilité du produit non affectée.

406839258

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