Des communications vraiment sécurisées grâce à des solutions conformes à la norme DECT.

Plantronics offre les seuls micro-casques certifiés DECT du marché et une gestion centralisée simplifiée.

La norme DECT (Digitally Enhanced Cordless Telecommunication/télécommunication sans fil numérique amélioré) est une technologie de 1,9 gigahertz qui utilise une partie dédiée du spectre sans fil pour offrir un niveau élevé de sécurité et de qualité audio aux entreprises et aux particuliers. On dit souvent que la technologie DECT est « sans interférence » puisqu'elle ne partage pas de spectre avec d'autres technologies telles que les réseaux Wi-Fi.

La sécurité est l'un des nombreux points forts de la technologie DECT. Elle utilise la radio numérique TDMA (Time Division Multiple Access) et la sélection dynamique des canaux sur plus de 10 fréquences opérateurs et 24 intervalles de temps, avec un système de sécurité multicouches. Ce système à plusieurs niveaux (connexion, cryptage, authentification, etc.) assure un degré élevé de protection contre les écoutes indiscrètes. Certains secteurs, comme les soins de santé et la finance, exigent des communications sans fil basées sur la norme DECT afin de garantir une sécurité et une confidentialité maximales.

REPONDRE AU BESOIN D'UNE SECURITE DECT AMELIOREE

Les solutions sans fil DECT de Plantronics sont les seuls appareils du marché à répondre aux exigences de sécurité de base et améliorée de la norme DECT, telles qu'elles sont stipulées par l'Institut européen des normes de télécommunications (ETSI).

La nécessité de renforcer la norme DECT est apparue en 2009, lorsqu'un groupe de white hats (hackers bien intentionnés) connu sous le nom du DeDECTed Group a publié un document mettant en avant les faiblesses des produits DECT de base au niveau de la sécurité. Le groupe de hackers a notamment exposé la menace de brèche des produits DECT qui n'utilisaient pas l'authentification et le cryptage tels que décrits dans les normes de l'ETSI. Les produits DECT de Plantronics ont toujours intégré l'authentification et le cryptage.

Le DECT Forum, dont Plantronics est membre, a examiné les conclusions du DeDECTed Group et a répondu en lançant le programme officiel de certification de sécurité DECT en 2013. Ce programme garantit que les produits sont testés et vérifiés de façon indépendante par un laboratoire certifié.

PLANTRONICS EST LA SEULE ENTREPRISE A OFFRIR UNE SECURITE DECT AVANCEE

Les nouvelles normes DECT présentent des lignes directrices pour l'amélioration de quatre nouveaux domaines (voir ci-dessous), ce qui porte le nombre total de catégories de sécurité à huit. Plantronics fut en fait le premier fournisseur dans le secteur des produits sans fil à répondre entièrement aux normes de sécurité indiquées par le DECT Forum. La série CS500 de Plantronics a commencé à être livrée avec les fonctions améliorées de sécurité en octobre 2013.

Depuis janvier 2016, les séries Savi 400 et Savi 700 de Plantronics ont été dotées de fonctions de sécurité DECT améliorées, afin de compléter la gamme de produits DECT de Plantronics. Plantronics restant le seul fournisseur de solutions sans fil entièrement conformes à la norme DECT, tous ses produits DECT respectent les huit fonctionnalités de sécurité du DECT Forum :

FONCTIONNALITES DE SECURITE DECT STANDARD

1. Procédure d'enregistrement et limites de temps pour la mise en place d'une clé d'authentification de 64 bits : la base ne restera pas « ouverte à l'enregistrement » pendant plus de 120 secondes. Ceci permet de s'assurer que toute tentative d'enregistrement d'un micro-casque avec la base peut uniquement avoir lieu lorsque l'utilisateur a lancé l'enregistrement et doit s'effectuer dans un délai de 120 secondes.
2. Activation du cryptage démarrée (base et micro-casque/oreillette) : la station de base et le micro-casque prendront en charge l'activation du cryptage et la base l'activera pour tous les appels. Certains appareils DECT ne démarraient auparavant pas le cryptage pour tous les appels.
3. Attribution sans fil d'une clé : la station de base créera et attribuera une clé d'authentification de l'utilisateur de 64 bits (UAK) lors de l'enregistrement du micro-casque. Ceci permet de garantir que la base et les micro-casques ne sont pas susceptibles de subir une attaque « de l'homme du milieu ». La base et le micro-casque utilisent la clé d'authentification dans leur communication.
4. Authentification du micro-casque : la base peut authentifier le micro-casque pour s'assurer qu'il s'agit de l'appareil authentique et non pas d'un intrus ou d'une tentative d'imitation de l'appareil authentique. Cette fonction garantit qu'aucune communication ne peut avoir lieu entre le micro-casque et la base s'ils ne peuvent pas s'authentifier mutuellement.

FONCTIONNALITES DE SECURITE DECT AMELIOREES

5. Générateur de nombre aléatoire amélioré : algorithme plus solide pour éviter tout doublon dans les nombres de démarrage utilisés pour la génération de clés de cryptage. Grâce à cette amélioration, il est impossible de deviner par des tentatives successives le nombre aléatoire qui serait ensuite utilisé pour créer des clés.
6. Evaluation du comportement des pairs concernant les valeurs d'expiration du cryptage pour le déclenchement de la coupure de l'appel : si le pair ne se comporte pas comme prévu, c'est-à-dire s'il ne démarre pas le cryptage en temps opportun, alors l'appareil assumera qu'il s'agit d'une tentative de violation de la sécurité et l'appel sera interrompu.

   Toute tentative de piratage devra être parfaite dans tous les aspects, à chaque fois, étant donné que toute communication appareil-base qui sort du schéma attendu entraînera l'interruption de la connexion.
7. Cryptage anticipé : garantit l'activation du cryptage immédiatement après l'établissement de la connexion, avant tout échange de messages de protocole supérieur, notamment l'identité de l'appelant, la composition des numéros, etc. Aucune information n'est échangée sans être cryptée.
8. Procédure pour activer une nouvelle clé de chiffrement dérivée pendant un appel : la clé de chiffrement utilisée par le moteur de cryptage est mise à jour au moins une fois toutes les 60 secondes, afin de déjouer toute tentative de déchiffrement par la force, par exemple avec des superordinateurs.

DECT 101 : l'avantage DECT de Plantronics

VERIFICATION DE CONNEXION
La base et les appareils distants sont couplés entre eux de façon à identifier facilement leur base ou leur appareil correspondant. Une clé secrète d'authentification est calculée à l'aide de l'algorithme d'authentification DSAA (DECT Standard Authentication Algorithm). Seuls les fabricants de ce type d'équipements ont accès à la définition de cet algorithme dans son intégralité. La durée de connexion des appareils est limitée pour plus de sécurité.

AUTHENTIFICATION
Les deux appareils vérifient que la clé d'authentification adéquate est utilisée et calculent des cryptogrammes (utilisés pour crypter les données envoyées par ondes radio) à l'aide du protocole DECT Standard Cipher (DSC). Seuls les fabricants de ce type d'équipements ont accès à la définition de cet algorithme.

CRYPTAGE
Une clé de chiffrement de 64 bits est utilisée pour crypter numériquement les données vocales transmises par communication radio. Au point de réception, la clé calculée dans l'étape d'authentification est utilisée pour décrypter les données.

DEPLACEMENT DYNAMIQUE DU CANAL
Dans le cadre du protocole DECT, les périphériques se déplaceront dynamiquement vers de nouveaux canaux pour répondre aux interférences. Le moment et la destination de ce saut étant imprévisibles, la sécurité de la transmission est renforcée.

CONTROLE DYNAMIQUE DE LA PUISSANCE
La gamme Savi® de Plantronics et la série CS500 de produits DECT utilisent le contrôle adaptatif de la puissance. Ils baissent les niveaux de puissance des fréquences radio nécessaires à communiquer lorsque l'utilisateur se trouve à proximité de la base, comme c'est souvent le cas. Les cyber-attaquants potentiels devraient se trouver dans cette portée ou utiliser des antennes directionnelles à gain élevé pour tenter d'écouter. Cela limite donc le risque.

CONFORMITE SARBANES-OXLEY
Les appareils DECT de Plantronics respectent la loi Sarbanes-Oxley (2002) art. 404. Cette déclaration se base sur le respect des mesures de cryptage intégrées au produit conformément aux exigences de la loi américaine 45 CFR 164.312(a)(2)(iv).

FACILITE DE DEPLOIEMENT ET DE GESTION EN ENTREPRISE

En plus des séries Savi 400 et Savi 700 qui sont dotées des dernières fonctionnalités DECT, les fonctionnalités DECT des appareils Plantronics actuels peuvent être mises à niveau grâce à une mise à jour firmware. Les départements informatiques des entreprises peuvent facilement procéder à cette mise à niveau avec Plantronics Manager Pro, une application logicielle basée sur le Cloud qui offre une gestion et un suivi des périphériques audio inégalés, une application des politiques et une assistance aux utilisateurs.

Dans le cadre de l'offre des logiciels Plantronics Spokes, Plantronics Manager Pro met à disposition des responsables informatiques des outils simples pour configurer les paramètres et mettre à jour les logiciels et firmwares des périphériques audio des utilisateurs finaux dans leur entreprise. Plantronics Manager Pro propose des outils de rapport qui permettent aux responsables informatiques de mieux comprendre leur environnement DECT afin de garantir la conformité des micro-casques/oreillettes de tous les utilisateurs.

Principales caractéristiques :

- Permet de paramétrer les périphériques selon la politique de l'entreprise ou la réglementation en vigueur
- Permet aux différents utilisateurs de mettre à niveau les paramètres DECT quand ils le souhaitent, tout en renforçant leur responsabilisation
- Surveillez le paramétrage et l'utilisation des périphériques audio quasiment en temps réel
- Permet de générer des inventaires et des rapports d'utilisation pour la gestion des ressources
- Permet d'afficher l'inventaire de tous les périphériques, y compris les périphériques non Plantronics

Plantronics est le seul fournisseur à proposer des logiciels de gestion permettant de répondre au déploiement de la technologie DECT, tout en maintenant la productivité des utilisateurs et en conservant une configuration conforme des appareils. Ces capacités, alliées aux seules véritables fonctionnalités DECT améliorées du secteur, font de Plantronics le leader des communications sans fil sécurisées.

[1] Il est possible de mettre à niveau les précédents modèles Savi 400 et Savi 700 avec les dernières fonctionnalités de sécurité DECT grâce à une mise à jour firmware.

Ne s'applique pas à la série CS500.