http://www.aerohive.com

AEROHIVE NETWORKS

PRIVATE PRESHARED KEY

Le meilleur compromis entre sécurité et souplesse d'utilisation pour l'accès aux réseaux Wi-Fi

OCTOBRE 2009

(ES) Equipements Scientifiques SA - Département Réseaux sans fil - 127 rue de Buzenval BP 26 - 92380 Garches
Tél. 01 47 95 99 50 - Fax. 01 47 01 16 22 - e-mail: reseaux@es-france.com - Site Web: www.es-france.com

SOMMAIRE

INTRODUCTION

Les réseaux sans-fil ont connu de nombreuses évolutions afin d'atteindre – voire dépasser dans certains cas – le niveau de sécurité des réseaux filaires.

Le paradigme des clés partagées (PSK)

La première étape fut le développement des clés partagées, ou *PreShared Key* (PSK). Chaque équipement d'un réseau sans-fil utilise une clé PSK afin de chiffrer le trafic, combattant ainsi toute tentative d'écoute du média radio. Le problème majeur dans l'utilisation de clés PSK est l'impossibilité de révoquer une clé lorsque, par exemple, un employé quitte l'entreprise. Or tous les employés utilisent la même clé PSK. En outre, l'usage d'une clé identique à longue durée de vie fournit le temps nécessaire à une personne malveillante pour tenter de casser la clé cryptographique – ce qui est maintenant particulièrement simple dans le cas de clés WEP et beaucoup plus laborieux, mais néanmoins possible, pour WPA.

Le standard 802.1X

Pour y remédier, le standard 802.1X a été défini afin de permettre aux entreprises d'élever le niveau de sécurité de leurs réseaux sans-fil. C'est la deuxième étape. Cependant, la migration d'un réseau utilisant une clé PSK vers la norme 802.1X ne se fait pas sans douleur. En effet, il n'est pas rare de voir des clients Wi-Fi anciens ne supportant pas ou n'étant pas compatibles avec ce standard ; et pour la plupart des autres clients Wi-Fi, en particulier lorsqu'il s'agit de systèmes d'exploitation Microsoft, leur configuration en mode 802.1X est loin d'être triviale. En outre, 802.1X pose un véritable problème lorsqu'il s'agit d'autoriser l'accès au réseau à des personnes externes à l'entreprise et utilisant des clients Wi-Fi non maîtrisés, par exemple des invités, des étudiants, des consultants,… Puisque 802.1X nécessite une configuration particulière, voire même l'installation d'un client logiciel spécifique (*supplicant*), il est parfois impossible de le déployer sur un réseau auquel se connectent des équipements non-gérés.

La solution *Private PSK* d'Aerohive

La solution brevetée *Private PSK* d'Aerohive combine la simplicité et la souplesse d'utilisation d'une clé PSK avec les avantages et le niveau de sécurité associés à la technologie 802.1X.

Un administrateur réseau, tout comme une hôtesse d'accueil, peuvent ainsi créer et attribuer à chaque utilisateur du réseau sans-fil une clé PSK unique, non connue des autres utilisateurs, rompant ainsi avec le paradigme du partage de clé PSK dans les réseaux classiques, et permettant alors d'identifier chaque utilisateur individuellement et d'en contrôler l'accès au réseau. On retrouve ici les caractéristiques, en termes de niveau de sécurité, du standard 802.1X, tout en s'affranchissant des contraintes de configuration et de déploiement sur le poste client puisqu'il s'agit d'une simple clé PSK.

Alors que l'usage d'une clé PSK classique ne permet pas la révocation d'un des utilisateurs puisque tous partagent la même clé, la technologie *Private PSK* d'Aerohive lie chaque client à une clé unique, qui peut donc être facilement révoquée sans impacter les autres utilisateurs du réseau sans-fil.

En outre, puisqu'une clé *Private PSK* est propre à chaque utilisateur et permet, tout comme dans le standard 802.1X, d'identifier celui-ci lorsqu'il se connecte à un SSID, il devient alors possible d'associer à l'utilisateur un profil réseau contenant des paramètres personnalisés – par exemple le numéro de VLAN, les règles de *firewall*, la politique de qualité de service, … Différents utilisateurs peuvent ainsi se connecter au même réseau sans-fil, mais disposer de niveaux de services distincts, par exemple en fonction de leur rôle au sein de l'entreprise.

Simplicité, souplesse, sécurité et réduction des coûts

Les bénéfices de la solution *Private PSK* d'Aerohive sont nombreux :

- La facilité de création des clés PSK, de leur distribution et de leur révocation réduit considérablement la complexité et les coûts liés à l'usage d'une clé unique PSK ou d'une technologie complexe telle que 802.1X.

- Les utilisateurs invités peuvent se voir attribuer des clés uniques par une hôtesse d'accueil, simple d'utilisation sur tout type de clients Wi-Fi. Par exemple, la solution *Private PSK* d'Aerohive permet de s'affranchir de l'usage d'un portail Web captif et donc de la contrainte de devoir ouvrir un navigateur pour accéder aux pages Web demandant l'authentification par nom d'utilisateur / mot de passe. On supprime ainsi des problématiques liées à la nature ou la configuration du poste de l'invité :
    - De plus en plus d'invités veulent connecter leurs téléphones multifonctions au réseau sans-fil. Or il est peut aisé d'accéder à un portail captif au travers d'un navigateur sur un téléphone mobile ou sur un assistant électronique personnel.
    - Les navigateurs des invités sont souvent configurés avec des paramètres de leur entreprise – par exemple un proxy – qui rendent ardus l'accès au portail captif et nécessitent une assistance technique.

- Si un employé vient à quitter l'entreprise, la clé partagée PSK traditionnelle impose un changement sur l'ensemble des postes de l'entreprise et des points d'accès Wi-Fi, ce qui peut devenir rapidement fastidieux. Avec la solution *Private PSK*, il suffit de révoquer la clé personnelle dudit employé, sans aucune action nécessaire sur les autres postes de travail.

- De nombreux clients ne supportent toujours pas 802.1X, le standard WPA2 et les options avancées – notamment pour l'itinérance (*roaming*) entre points d'accès Wi-Fi. Grâce à la solution *Prive PSK*, et puisqu'il s'agit in-fine d'une clé PSK standard mais propre à chaque utilisateur, les fonctions classiquement disponibles sur les clients Wi-Fi, même les moins récents, restent opérationnelles. C'est le cas en particulier pour l'itinérance transparente au sein de l'infrastructure Wi-Fi.

- Globalement, tous les clients supportant WPA-PSK peuvent bénéficier, avec la solution *Private PSK*, du niveau de sécurité de 802.1X sans ajouter de logiciel ou mettre à jour le poste de travail et sans avoir à implémenter une configuration complexe.

LES METHODES TRADITIONNELLES D'ACCES AU RESEAU WI-FI

Lorsqu'elles déploient un réseau Wi-Fi, les entreprises disposent de diverses options de sécurité afin de contrôler l'accès au réseau en fonction de l'identité de l'utilisateur. Le choix entre ces différentes options résulte souvent d'un compromis entre sécurité et complexité. Les trois méthodes classiques sont :

- Réseau ouvert – Pas de sécurité.
  - Tout le trafic est émis en clair, non chiffré, sur le média radio.
  - Un portail Web captif est habituellement utilisé pour l'auto-enregistrement ou l'authentification des utilisateurs.
  - Le trafic est parfois segmenté sur des VLANs distincts sur le réseau Ethernet.

- Clé partagée (PSK) – Standard IEEE 802.11i WPA ou WPA2 Personnel.
  - Utilisation d'un secret unique partagé entre tous les clients d'un même SSID.
  - Le secret – ou clé partagée (PSK) – est utilisé pour chiffrer le trafic véhiculé par la radio entre les clients et les points d'accès Wi-Fi à l'aide des algorithmes TKIP ou AES-CCMP.

- IEEE 802.1X (EAPOL) – Standard 802.11i WPA ou WPA2 Entreprise.
  - Les utilisateurs sont authentifiés à l'aide d'un couple nom d'utilisateur / mot de passe.
  - Optionnellement, l'équipement de l'utilisateur peut être authentifié à l'aide d'un certificat machine,
  - Les clés cryptographiques utilisées par le client et le point d'accès Wi-Fi sont négociées de manière dynamique et sécurisée avec le serveur RADIUS à l'aide du protocole 802.1X (EAPOL).
  - Le client et le point d'accès utilisent les clés pour générer d'autres clés temporaires pour chaque session RADIUS.
  - Le trafic est chiffré à l'aide des algorithmes TKIP ou CCMP-AES.

Réseau ouvert

Les SSID à réseau ouvert sont les plus simples à configurer, à déployer et à utiliser. C'est pourquoi la grande majorité des réseaux invités utilisent cette méthode. Cependant, de nombreux problèmes interviennent, notamment en termes de sécurité.

L'intégralité du trafic échangé entre un client et un point d'accès Wi-Fi au travers d'un réseau ouvert circule en clair et est donc écoutable sur la radio. En outre, il n'y a aucune authentification ni aucun contrôle possible du client, de sorte que n'importe qui peut s'associer au SSID. D'ailleurs, il n'est pas rare de voir des cartes Wi-Fi se connecter automatiquement à de tels SSID ouverts, sans même en avertir l'utilisateur.

Le réseau ouvert est donc particulièrement vulnérable aux attaques, et nécessite la mise en œuvre de moyens de sécurité additionnels sur l'infrastructure réseau.

Clé partagée (PSK)

Par rapport aux réseaux ouverts, les réseaux implémentant une clé partagée – ou *PreShared Key (PSK)* – apportent un niveau substantiel de sécurité.

En plus d'être plus sûre, la technologie PSK est supportée par la quasi-totalité des clients Wi-Fi actuellement déployés, et est particulièrement simple à mettre en œuvre puisqu'elle ne nécessite pas d'authentification serveur, de certificat ou de configuration particulière sur le poste client (mis à part le renseignement de la clé).

Cependant, il existe plusieurs problèmes inhérents au fait d'utiliser une clé identique pour tous les utilisateurs :

- Si un utilisateur quitte l'entreprise ou se fait dérober son ordinateur portable, il est nécessaire de modifier la clé partagée par tous les utilisateurs sur l'ensemble des postes clients et des points d'accès Wi-Fi.

- Les utilisateurs disposant de la même clé partagée, il est impossible de les différencier. De sorte que tous disposent alors du même profil réseau : même numéro de VLAN, même règles de *firewall* et de qualité de service,… Il est donc impossible d'appliquer des politiques discrètes de sécurité ou de priorisation de trafic, de limitation de bande passante,…

- Dans le cas des accès invités, il est nécessaire de communiquer, au préalable, la clé partagée aux utilisateurs. Elle peut alors facilement être dévoilée.

Authentification 802.1X

Les réseaux Wi-Fi utilisant l'authentification 802.1X résolvent la plupart des problèmes liés à l'usage d'une clé partagée commune en assignant une clé individuelle à chaque utilisateur.

Une fois l'utilisateur authentifié par un serveur RADIUS, le serveur renvoi au client et au point d'accès Wi-Fi une clé PMK (*pairwise master key*) qu'ils utilisent pour dériver une clé temporaire PTK (*pairwise temporary keys*) servant à chiffrer le trafic de la session courante.

Le serveur RADIUS peut également renvoyer des attributs spécifiques afin de définir différents profils d'utilisateurs. Grâce à cette technique, la norme 802.1X permet de mettre en œuvre, sur un même SSID, des profils d'accès au réseau et de qualité de service propres à chaque utilisateur, en fonction de leur identité ou de leur appartenance à un groupe fonctionnel.

Ceci fournit également la capacité de bloquer l'accès au réseau à un utilisateur ou à une machine si, par exemple, un employé vient à quitter l'entreprise ou un ordinateur portable est dérobé ou compromis.

Cependant, pour fournir ces services avancés, le standard 802.1X requière une configuration particulière des clients Wi-Fi et nécessite, au niveau de l'infrastructure, un serveur RADIUS, des certificats serveurs, une base de données pour les utilisateurs – qui peut être locale au serveur RADIUS ou externe sur un annuaire Active Directory ou LDAP. Enfin les clients Wi-Fi 802.1X, également dénommés *supplicants* RADIUS, doivent être préconfigurés.

L'ACCES AU RESEAU WI-FI AVEC LA TECHNOLOGIE *PRIVATE PSK* D'AEROHIVE

Bien que le standard 802.1X constitue en soi l'approche la plus sécurisée pour l'authentification Wi-Fi, cette méthode, de par sa complexité d'implémentation, n'est quasiment déployée que sur les postes administrés par les équipes informatiques de l'entreprise qui disposent du contrôle sur l'infrastructure réseau, les comptes utilisateurs et les clients sans-fil utilisés.

Pour les utilisateurs occasionnels, tels que les consultants, les stagiaires ou les invités, les équipes informatiques ne disposent alors pas nécessairement de l'accès au poste client, des connaissances pour configurer le logiciel 802.1X (*supplicant*) et la myriade de cartes Wi-Fi potentielles, voire même du temps et des ressources nécessaires pour effectuer de telles tâches, et en assurer le support.

Cela devient carrément impossible lorsque les clients Wi-Fi, et il en existe toujours une quantité non négligeable, ne supportent pas 802.1X ou le dernier standard WPA2 et ses options associées. D'ailleurs, dans ce cas, la seule solution consiste à recourir à une clé partagée PSK, mais on perd alors tous les avantages du 802.1X.

Afin de tirer partie des bénéfices de chacune des deux solutions et sans en hériter les contraintes, Aerohive a développé une nouvelle approche pour l'authentification sur les réseaux sans-fil WLAN : la technologie *Private PSK*.

Les clés privées *Private PSK* sont des clés PSK uniques et individuelles, permettant l'accès à un même SSID par différents utilisateurs auxquels les clés ont été attribuées au préalable. *Private PSK* offre l'unicité des clés et la flexibilité du contrôle d'accès du standard 802.1X tout en conservant la simplicité de configuration des clés partagées PSK.

Le diagramme ci-après est une illustration comparative d'un réseau WLAN traditionnel à clés partagées PSK et de l'équivalent utilisant la technologie Aerohive *Private PSK*.

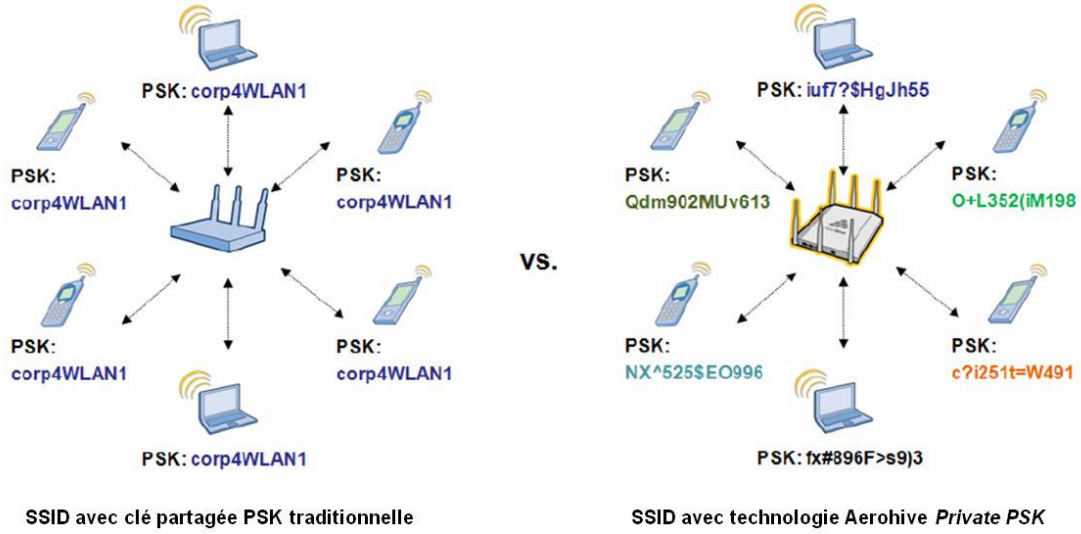

Figure 1 : SSID avec clé partagée PSK traditionnelle versus SSID avec technologie Aerohive Private PSK

Dans le premier cas, tous les utilisateurs, quelque soit leur client Wi-Fi ou leur rôle dans l'entreprise, partagent la même clé et le même profil d'utilisation du réseau puisqu'ils ne sont pas différentiables.

Dans le cas de la solution Aerohive, avec la technologie *Private PSK*, chaque utilisateur se voit assigner une clé partagée PSK unique et individuelle, d'où la notion de clé partagée privée. Cette clé peut être générée manuellement ou automatiquement par l'outil d'administration centralisée HiveManager d'Aerohive puis ensuite communiquée à l'utilisateur correspondant par e-mail, badge imprimé, ou même message SMS. Chaque clé *Private PSK* étant attribuée à un unique utilisateur, un profil d'utilisation et d'accès au réseau particulier peut être mis en œuvre : durée de validité de la clé, horaires de connexion autorisés, numéro de VLAN, règles de *firewall* et de qualité de service, …

Puisque les clés *Private PSK* sont uniques, il est impossible de déduire ou dériver la clé d'un utilisateur depuis celle d'un autre utilisateur. En outre, une clé *Private PSK* peut être révoquée à tout instant empêchant immédiatement l'accès de l'utilisateur au réseau Wi-Fi.

Enfin, vis-à-vis du client, la configuration pour l'accès au réseau Wi-Fi est strictement la même que dans le cas d'une clé partagée. C'est donc particulièrement simple.

Besoins et fonctionnalités d'un réseau sans-fil WLAN	**Clé partagée PSK WPA/WPA2 Personnel**	**Aerohive *Private PSK* WPA/WPA2 Personnel**	**IEEE 802.1X WPA/WPA2 Entreprise**
Pas de configuration complexe sur les postes clients	✓	✓	✗
Clé unique par utilisateur pour un SSID	✗	✓	✓
Possibilité de révoquer individuellement un utilisateur	✗	✓	✓
Profils d'utilisation différenciée (VLAN, Firewall, QoS, horaires de connexion,…)	✗	✓	✓
Compatibilité avec les clients ne supportant pas les fonctions avancées d'itinérance (*roaming*)	✓	✓	✗
Pas de certificat à installer sur les postes clients	✓	✓	*Dépend du client*
Utilisation des mécanismes standards 802.11i pour la sécurisation du SSID	✓	✓	✓
Création dynamique et rotation des clés de chiffrement	✗	✗	✓
Support de l'authentification machine	✗	✗	✓
Si un utilisateur est compromis, les autres utilisateurs ne sont pas atteints	✗	✓	✓

Tableau 1 : Comparaison des différentes solutions d'authentification

DEPLOIEMENT DE CLES *PRIVATE PSK* AVEC L'OUTIL AEROHIVE HIVEMANAGER

L'administration centralisée des points d'accès HiveAP d'Aerohive s'effectue au travers de l'outil HiveManager. C'est également cet outil qui permet de créer, distribuer et administrer les clés *Private PSK*.

Le HiveManager est utilisé pour configurer la politique globale WLAN qui sera déployée sur chacun des points d'accès HiveAP. Cette politique contient notamment les différents SSID diffusés sur les points d'accès Wi-Fi.

La figure ci-dessous présente une politique WLAN dans laquelle un SSID utilisant des clés *Private PSK* est configuré sur les différents points d'accès HiveAP. Dans ce scénario, le HiveManager est utilisé pour générer automatiquement des clés privées partagées PSK qui seront ensuite assignées à des clients Wi-Fi non gérés par l'entreprise tels que des téléphones portables multifonctions, et des utilisateurs invités. Chaque utilisateur dispose alors de sa propre clé PSK et est associé un groupe auquel correspond une politique de contrôle d'accès et de qualité de service.

La 1ère étape consiste, pour l'administrateur, à configurer le SSID utilisant des clés *Private PSK* et à créer la base des utilisateurs correspondant qui sera ensuite téléchargée sur les points d'accès HiveAP. Ces utilisateurs peuvent être configurés manuellement, générés automatiquement ou bien chargé dans le HiveManager depuis un fichier .csv, par exemple depuis un export de l'annuaire Active Directory ou LDAP de l'entreprise.

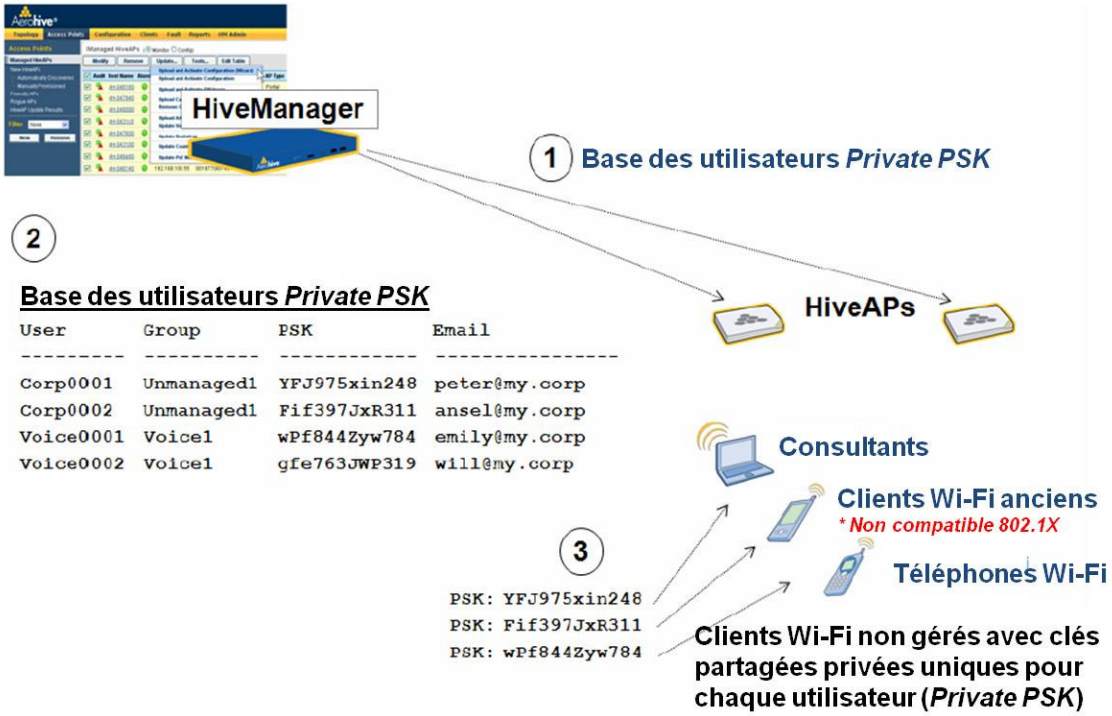

Figure 2 : Génération et distribution des clés Private PSK par le HiveManager

Dans un deuxième temps, l'administrateur peut, au travers du HiveManager, sélectionner les utilisateurs et leur envoyer leur clé privée *Private PSK* par e-mail. La figure ci-après montre comment simplement l'administrateur choisit les utilisateurs concernés et clique sur le bouton d'envoi de courrier électronique (« *Email PSK* »).

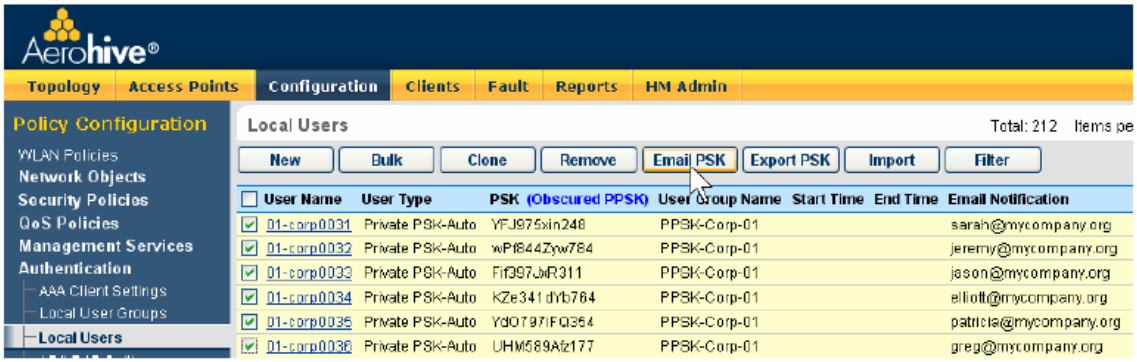

Figure 3 : Envoi des clés privées Private PSK aux utilisateurs par courrier électronique

Une fois la clé communiquée à chacun des utilisateurs, ceux-ci peuvent, dans un troisième temps, se connecter au réseau et se voir assigner les droits adéquats en fonction de leur profil.

Enfin, dans une quatrième étape, si un utilisateur vient à quitter l'entreprise ou se voir interdire l'accès au réseau Wi-Fi, l'administrateur le révoque simplement de la liste. La figure ci-dessous montre comment en sélectionnant les utilisateurs à révoquer et en les supprimant de la liste (« *Remove* ») puis en mettant à jour les points d'accès HiveAP, il devient alors impossible auxdits utilisateurs de se connecter à nouveau.

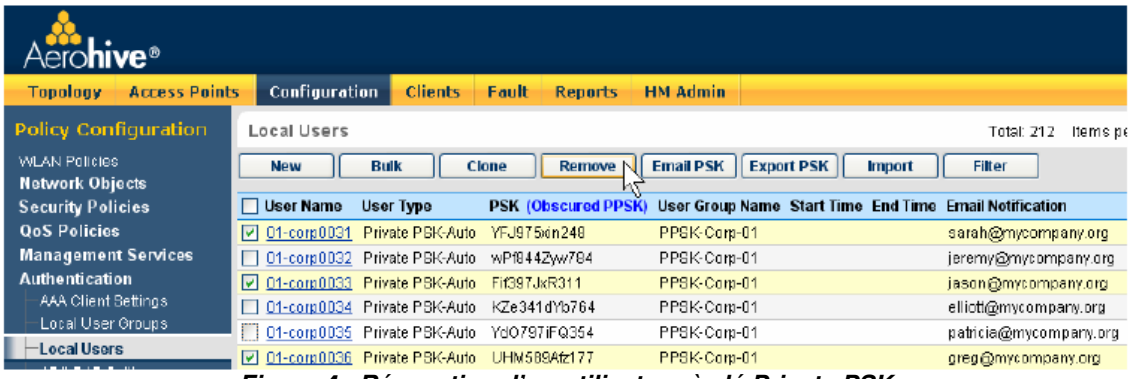

Figure 4 : Révocation d'un utilisateur à clé Private PSK

SECURISER ET SIMPLIFIER L'ACCES DES INVITES A L'AIDE DU GUESTMANAGER ET DE CLES *PRIVATE PSK*

Grâce à la simplicité de son interface, le GuestManager permet à une hôtesse d'accueil de créer et gérer facilement des comptes invités utilisant une clé *Private PSK* au travers d'une interface Web conviviale.

Grâce à l'intégration entre l'outil GuestManager et la fonction de *Private PSK*, il est possible de bénéficier des avantages suivants :

- Interface web légère et simple d'utilisation, avec délégation granulaire de l'administration.
- Création et association de clés *Private PSK* à des utilisateurs.
- Définition des droits associés aux utilisateurs (durée et horaires de connexion, profils associés,…)
- Possibilité d'imprimer un badge avec le rappel de l'ensemble des éléments nécessaires à la connexion de l'utilisateur (instructions de connexion, clé *Private PSK*, contact support, …).
- Des modèles de badges sont disponibles de base et il est possible de créer ses propres badges personnalisés (logos, couleurs, contenus,…).
- Révocation des utilisateurs à l'aide de messages RADIUS Changement dynamique d'authentification (RFC 3576) ne nécessitant pas la mise à jour de la base des utilisateurs sur les points d'accès HiveAP.
- Comptabilité RADIUS pour le traçage.

La figure ci-après illustre le mode de fonctionnement du GuestManager et des points d'accès HiveAP dans le cas de l'utilisation de clés *Private PSK*.

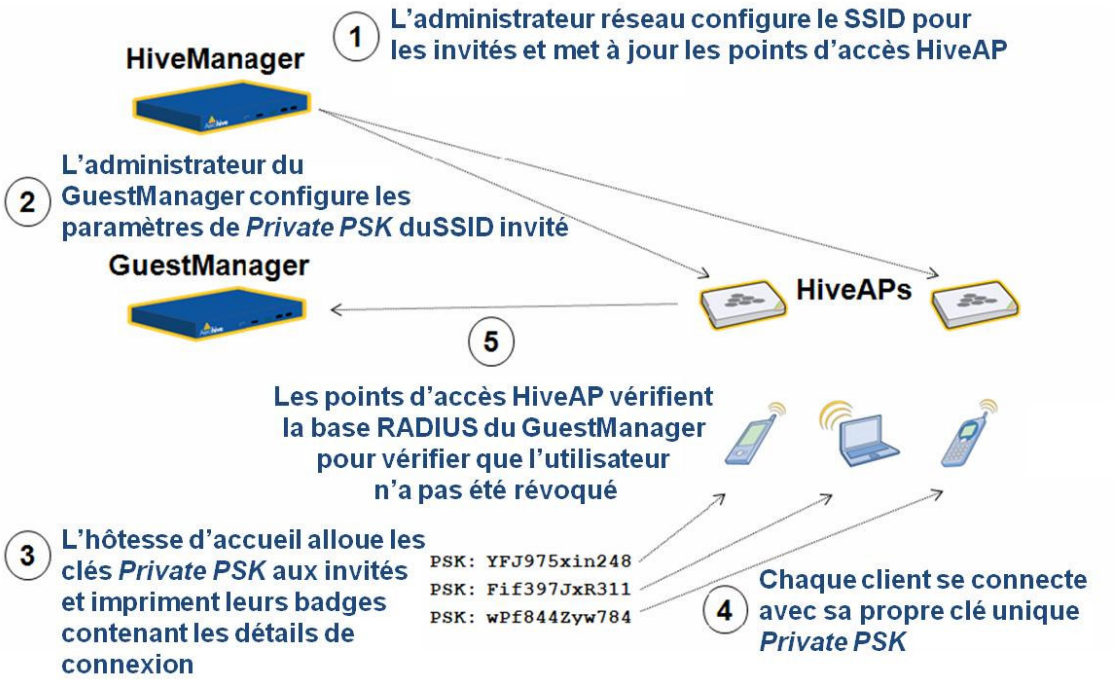

Figure 5 : Gestion des clés Private PSK par le GuestManager

Les 5 étapes du processus sont :

1. L'administrateur du HiveManager crée la politique WLAN globale incluant notamment les paramètres propres aux accès invités (SSID, profils d'utilisation, configuration *Private PSK*,…). Les paramètres de configuration des clés *Privae PSK* incluent notamment : le délai de renouvellement de la clé, la clé privée et l'option de validation des clés par le GuestManager. L'administrateur peut créer jusqu'à 1000 clés *Private PSK*. Lorsque les points d'accès HiveAP sont mis à jour, ils génèrent les clés *Private PSK* en fonction des paramètres configurés.

2. Pour permettre la délégation du contrôle et de la distribution des clés *Private PSK*, l'administrateur doit ensuite configurer les mêmes paramètres dans le GuestManager. Ceci permet au GuestManager de générer exactement les mêmes clés que celles présentes sur les points d'accès HiveAP. Dès lors, le contrôle de l'affectation des clés aux utilisateurs et de leur activation peut être délégué à un autre administrateur ou à une hôtesse d'accueil, sans que ceux-ci n'aient besoin de comprendre ou modifier la configuration.

3. Lorsqu'un invité se présente à l'accueil, l'hôtesse se connecte sur l'interface web du GuestManager. Son profil d'hôtesse lui restreint l'accès à la page de création d'un compte invité. Elle renseigne alors les éléments nécessaires puis génère le compte utilisateur et imprime le badge correspondant. Badge qu'elle délivre ensuite à l'invité.

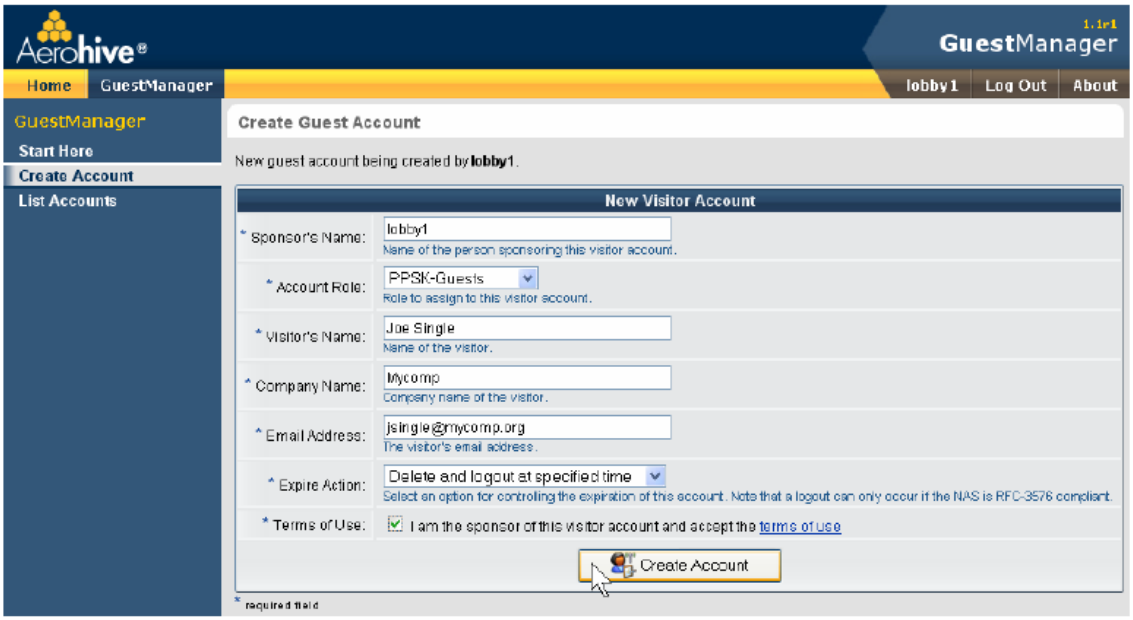

Figure 6 : Interface de création d'un compte invité par un hôtesse d'accueil

4. L'invité peut alors connecter son terminal Wi-Fi à l'aide des paramètres inscrits sur son badge (nom du SSID, clé PSK individuelle, …).

5. Le point d'accès HiveAP valide alors la clé *Private PSK* de l'utilisateur avec le GuestManager en utilisant la clé comme nom de compte utilisateur et ce afin de vérifier que le compte est toujours valide/autorisé et n'a pas été révoqué. Si tel est le cas, le GuestManager renvoi un message d'autorisation d'accès au HiveAP pour permettre à l'utilisateur de s'associer au SSID et d'accéder au réseau sans-fil WLAN.
   Le GuestManager peut également être configuré pour renvoyer des attributs supplémentaires permettant d'assigner un profil d'utilisation particulier à l'invité.

6. Si l'hôtesse d'accueil ou un administrateur réseau révoque le compte de l'invité dans le GuestManager, alors celui-ci va émettre un message RADIUS de changement d'autorisation au point d'accès HiveAP. Ceci va entrainer la suppression du cache d'authentification de l'utilisateur dans le point d'accès et ainsi forcer l'invité à se ré-authentifier. Or, la clé privée PSK ayant été révoquée, l'authentification RADIUS échouera et l'utilisateur ne pourra plus se connecter au réseau sans-fil.

En combinant ainsi l'utilisation de clés PSK individuelles pour le chiffrement et la validation de l'utilisation par le serveur GuestManager, on obtient une solution de gestion des invités particulièrement sécurisée et simple d'utilisation, quelque soit le type de client ou de terminal Wi-Fi.

CONCLUSION

A l'heure actuelle, 802.1X est considéré par les analystes, les administrateurs réseau et les constructeurs et éditeurs de logiciels comme le standard de-facto pour la sécurité et l'authentification sur un réseau Wi-Fi d'entreprise. Malheureusement, le processus de migration vers la norme 802.1X est considérablement ralentit par la complexité de configuration et de déploiement, le coût de mise à jour du parc existant et l'inadaptation aux besoins des accès invités.

La solution Aerohive *Private PSK* permet de résoudre ces problèmes en supportant l'ensemble du parc de clients Wi-Fi existant et déjà déployé, en permettant l'accès au réseau sans-fil à de nouveaux types de clients – notamment les téléphones Wi-Fi – et aux utilisateurs invités avec un niveau de simplicité équivalent à une clé partagée PSK traditionnelle.

L'intégration au HiveManager et au GuestManager simplifie drastiquement la gestion des utilisateurs et en diminue le coût opérationnel,

Cette solution est un complément parfait au standard 802.1X : elle permet aux administrateurs réseaux d'utiliser 802.1X sur leurs équipements maîtrisés et pour leurs employés, tout en offrant une alternative de même niveau de sécurité pour les autres utilisateurs.