

Charte MIP-WIFI

1-Objectifs du projet

Le projet MIP-WIFI (Midi-Pyrénées - WIFI) a pour but la mise en place d'une infrastructure d'authentification répartie pour les établissements membres du projet désirant faciliter la mobilité de leurs étudiants et de leurs personnels sur les sites des autres membres en Midi Pyrénées. Cette mobilité concerne essentiellement la connexion aux réseaux sans fil des établissements. Les accès utilisateurs habituels sont de type portail captif ou 802.1x. Cette mobilité est d'échelle régionale et est indépendante du projet ARREDU/EDUROAM.

Sont concernés : tous les établissements d'enseignement supérieur et recherche en Midi Pyrénées et tout organisme public accueillant des usagers d'établissement d'enseignement supérieur et recherche en Midi-Pyrénées.

Tout établissement membre du projet MIP-WIFI s'engage auprès du CICT au respect des principes ci-dessous :

- Offrir à ses utilisateurs la possibilité d'utiliser, lors de leurs déplacements, les infrastructures réseau des autres établissements membres en utilisant leurs identifiant et mot de passe habituels ;
- Réciproquement, offrir l'accès à l'Internet, via son infrastructure réseau, aux utilisateurs des autres établissements membres;
- Mettre en oeuvre les moyens nécessaires pour protéger les données d'authentification, le trafic des utilisateurs et la traçabilité des sessions.

2-Engagements

Les choix techniques correspondants sont décrits dans les spécifications techniques (cf ci-dessous).

On définit :

- **Etablissement de rattachement** : l'établissement administratif de rattachement de l'utilisateur du service MIP-WIFI et qui gère l'authentification de celui-ci.
- **Etablissement visité** : tout établissement, autre que l'établissement de rattachement, où se trouve l'utilisateur du service MIP-WIFI .

2.1-Engagements en tant qu'établissement de rattachement

- Mettre en oeuvre un service d'authentification RADIUS;
- Mettre en service une méthode d'authentification de type portail captif et si le site le souhaite 802.1X ;
- Informer ses utilisateurs sur l'existence du service et la manière d'y accéder;
- Offrir un service d'assistance à ses utilisateurs.

2.2-Engagements en tant qu'établissement visité

- Offrir le service à travers des points d'accès sans fil et une infrastructure d'authentification RADIUS conformément aux spécifications techniques.
- Mettre de l'information sur le service et les conditions d'utilisation à disposition des visiteurs .

2.3-Engagements communs sur la sécurisation du service

Protection des données d'authentification des utilisateurs

Les deux méthodes d'authentification Portail captif et 802.1X peuvent être utilisées sur MIP-WIFI.

Pour la connexion de type portail captif une authentification HTTPS sur le portail captif doit obligatoirement être mise en place.

Les serveurs Radius de la chaîne de communication ne doivent pas faire apparaître les mots de passe des utilisateurs dans leurs journaux système (pas de fonctionnement opérationnel en mode debug).

En 802.1X, les identifiants et mots de passe des utilisateurs, transitant via l'infrastructure MIP-WIFI , doivent être chiffrés de bout en bout, c'est à dire entre leur poste de travail et le serveur d'authentification de leur établissement de rattachement.

Protection du trafic des utilisateurs

Pour le portail captif, la limitation, hors smtp et http, aux seuls protocoles sécurisés ssh, pops, sftp... est fortement conseillée. Une information des

utilisateurs sur le fait que le réseau sans fil n'est pas sécurisé est obligatoire. Dans le contexte 802.1X, les établissements doivent mettre en oeuvre des méthodes de chiffrement efficaces sur les points d'accès sans fil donnant accès au service MIP-WIFI.

Serveurs RADIUS

Ils doivent être installés et gérés suivant les règles de bonnes pratiques en matière d'installation, de configuration, d'administration et de sécurité afin d'offrir le niveau de sécurité et de confiance nécessaire à l'infrastructure.

Il est souhaitable d'avoir une infrastructure protégée par des pare-feu ou routeurs filtrants.

Traçabilité

Les mesures appropriées doivent être mises en oeuvre pour identifier l'utilisateur d'une adresse IP à un moment donné. Une collaboration est alors nécessaire entre les administrateurs du service de l'établissement visité et de celui de rattachement.

3-Spécifications techniques de mise en oeuvre :

Ce chapitre décrit les modalités de mise en oeuvre du service de mobilité MIP-WIFI

3.1 Architecture

Chaque établissement raccorde son ou ses serveurs RADIUS au serveur proxy de MIP-WIFI à qui il délègue toute demande d'authentification pour les établissements partenaires du projet et uniquement pour ces établissements. Le serveur proxy de MIP-Wifi ne gère pas la mobilité des authentifications au niveau national (ARREDU) ou international (EDUROAM), ceci reste du ressort des serveurs proxies radius des établissements.

3.2 Infrastructure sans fil, recommandations

- type : 802.11g de préférence, sinon 802.11b
- SSID : Il n'est pas prévu de ssid spécifique pour l'utilisation de la mobilité mip-wifi. Chaque établissement est maître en la matière. Il serait plus simple que tous les établissements adhérents donnent accès à la mobilité MIP-Wifi à partir de l'ensemble des SSID qu'ils utilisent (portail captif, 802.1x). Si, pour des raisons internes, l'accès à la mobilité MIP-Wifi devait être restreint à quelques ssid, il serait préférable que, parmi ceux-ci, il y ait un accès simple type portail captif et un accès sécurisé par cryptage radio. Dans ce dernier cas, le(les) nom(s) des ssid éligibles à la mobilité MIP-Wifi doivent être diffusés dans les pages d'information du service et indiqué lors de l'inscription au service MIP-Wifi.
- chiffrement : pour l'utilisation de 802.1X, le trafic doit être chiffré à l'aide de WPA2, WPA ou, à défaut, WEP 128 initié par le serveur d'authentification avec rotation fréquente de clé pour déjouer les crackeurs de WEP (5mn). Le(s) type(s) de chiffrement utilisé devra être indiqué sur les pages d'informations.
- portail captif : Dans tous les cas l'accès par portail captif devra être activé sur le site adhérent au projet MIP-WIFI
- support de 802.1X : les points d'accès au service MIP-WIFI peuvent s'ils le souhaitent mettre en oeuvre le protocole d'accès 802.1X
- DHCP : un service DHCP doit communiquer les informations réseau de base aux clients
- services réseau accessibles : au moins les services suivants doivent être accessibles depuis le réseau sans fil:

HTTP, HTTPS,

ICMP (echo/reply),

IPSec (ESP, AH, IKE),

SSH,

POPS,

IMAPS,
SMTPS.

- protection vis à vis de l'extérieur : le réseau d'accueil des utilisateurs du service MIP-WIFI doit être protégé des accès venant de l'extérieur, tout accès doit être authentifié. Un visiteur ne devra pas pouvoir se connecter via un accès n'offrant pas les garanties demandées dans la charte.

3.3 Méthodes d'authentification

Les deux méthodes d'authentification 802.1X et Portail captif peuvent être utilisées sur MIP-WIFI.

Pour la connexion de type portail captif une authentification HTTPS sur le portail captif et la limitation, hors http et éventuellement smtp, aux seuls protocoles sécurisés ssh, pops, sftp... doivent obligatoirement être mises en place.

En 802.1X, les identifiants et mots de passe des utilisateurs, transitant via l'infrastructure MIP-WIFI, doivent être chiffrés de bout en bout, c'est à dire entre leur poste de travail et le serveur d'authentification de leur établissement de rattachement.

Le cadre du projet concerne un petit nombre d'entités entre lesquelles une relation de confiance peut être facilement établie entre administrateurs du service. Cette relation de confiance associée à une sécurisation obligatoire des serveurs radius et au fonctionnement des réseaux REMIP 2000 et ASTER peut garantir une certaine confidentialité des données d'authentification même dans une connexion de type portail captif.

3. Traçabilité

L'établissement doit garder les traces nécessaires à l'identification d'un usager à partir de l'adresse IP utilisée en cas d'abus constaté. Ces traces doivent comporter un horodatage fiable.

3.5 Formation/information

Chaque établissement doit mettre en ligne une rubrique web publique décrivant le service MIP-WIFI (ssids utilisés, chiffrement supporté, zones couvertes,...). L'url de la page "portail" sera communiquée dans les informations du compte MIP-WIFI et sera publiée sur le site du CICT dans la rubrique mip-wifi.

L'établissement doit informer ses utilisateurs :

- sur l'accès portail captif (SSID avec ses restrictions d'utilisation...) et s'il offre une connexion de type 802.1X dans le contexte de mobilité, dans ce dernier cas il doit aussi préciser s'il fournit des clients et /ou offre un support technique individualisé aux usagers.

- de l'existence et de l'intérêt de l'infrastructure MIP-WIFI et de la façon de l'utiliser.
- que les chartes MIP-WIFI et RENATER s'appliquent également sur les autres sites partenaires.
- qu'ils se doivent de respecter les règles d'utilisation du réseau d'accueil.
- que le service d'assistance réseau (de l'établissement de rattachement, cf ci-dessous) doit être contacté en cas de problème de connexion sur un autre site et leur en communiquer les coordonnées.

L'établissement doit informer les visiteurs :

- de la manière d'accéder au service (par l'intermédiaire d'une page de portail web "captif" par exemple)
- des éventuelles conditions d'utilisation des ressources mises à leur disposition

3.6 Support

Dans le contexte de l'utilisation du portail captif, chaque établissement doit offrir un service d'assistance à ses utilisateurs pour les aider notamment en cas de problème lors de leurs déplacements sur un autre site MIP-WIFI, ce service n'a pas à être sollicité par les visiteurs. Ceux-ci doivent s'adresser à leur propre support en cas de problème.

Si un site souhaite proposer un moyen d'accès 802.1X dans le contexte de la mobilité MIP-WIFI, il doit offrir une assistance aussi bien aux visiteurs qu'à ses propres utilisateurs lors de l'utilisation de ce service, ou bien informer les visiteurs qu'en cas de problème en 802.1X ils n'auront pas de support et devront utiliser le portail captif.

3.7 Le "compte" MIP-WIFI

Ce compte, géré par les exploitants du service, est associé à l'établissement partenaire ayant souscrit au service mobilité. Il permet de gérer les informations nécessaires au fonctionnement du service au niveau MIP-WIFI. Il est créé lors de l'adhésion au service MIP-WIFI et permettra de gérer les informations relatives à l'entité ayant adhéré au service.

Principales informations gérées :

- noms de domaines (realms Radius) : tout utilisateur de la communauté **MIP-Wifi** a un identifiant de la forme <user>@<domaine>. La partie <domaine> est, à priori, un domaine DNS de l'établissement et doit se terminer par ".fr" (exemple : "cict.fr"). C'est logiquement la partie domaine (ou une sous-partie) de l'identifiant institutionnel stocké dans l'attribut eduPersonPrincipalName des entrées de personnes dans l'annuaire SupAnn de l'établissement. Il peut en être déclaré plusieurs. Seuls ceux des communautés susceptibles d'utiliser le service MIP-WIFI doivent être déclarés.
- serveur Radius principal : adresse ou nom du serveur principal.

- serveur(s) Radius de secours : (facultatif) adresse(s) ou nom(s) du ou des serveurs de secours éventuels.
- ports : ports utilisés pour l'authentification et l'accounting Radius.
- type d'authentification : la ou les méthodes d'authentification utilisées.
- secret partagé : le secret partagé entre le serveur Radius régional Mip-wifi et le ou les serveurs de l'établissement. Un secret initial est proposé, il peut être modifié.
- compte de test : **afin d'effectuer des tests et de surveiller la disponibilité du service, un compte de test spécifique (même nom, même mot de passe) à chaque realm (établissement) déclaré sera créé. Le nom par défaut pourra être de la forme “mp-<identifiantEtablissement>”** et un mot de passe est proposé automatiquement à la création du compte. Il est conseillé de le changer de temps en temps. **Ce compte ne sera connu que du CICT et de l'administrateur du site concerné.**
- SSIDs : Il n'est pas prévu de ssid spécifique pour l'utilisation de la mobilité mip-wifi. Chaque établissement est maître en la matière. Il serait plus simple que tous les établissements adhérents donnent accès à la mobilité MIP-Wifi à partir de l'ensemble des SSID qu'ils utilisent (portail captif, 802.1x). Si, pour des raisons internes, l'accès à la mobilité MIP-Wifi devait être restreint à quelques ssid, il serait préférable que, parmi ceux-ci, il y ait un accès simple type portail captif et un accès sécurisé par cryptage radio. Dans ce dernier cas, le(les) nom(s) des ssid éligibles à la mobilité MIP-Wifi doivent être diffusés dans les pages d'information du service et indiqué lors de l'inscription au service MIP-Wifi.
- type de serveur : logiciel ou appliance utilisé.
- pages d'information : url des pages publiques décrivant le service MIP-WIFI mis en place.
- coordonnées du service d'assistance : email et téléphone du service d'assistance. Ces informations ne seront pas diffusées mais seront utiles pour les administrateurs du réseau wifi du site visité.
- coordonnées du correspondant MIP-WIFI

3.8 Infrastructure RADIUS, configuration

- noms de domaines (realms) : configurer les domaines choisis (dans le fichier *proxy.conf* dans le cas de FreeRadius)
- méthodes d'authentification : configurer la ou les méthodes d'authentification choisies (dans les fichiers *radius.conf*, *eap.conf* dans le cas de FreeRadius)
- compte de test : configurer pour chaque domaine le compte de test enregistré dans le compte MIP-WIFI (fichier *users* dans le cas de FreeRadius)
- sécurisation : les clients (points d'accès) et serveurs Radius doivent être configurés et administrés dans les règles de l'art (patchs de sécurité par exemple) et situés sur des réseaux/vlans dédiés. Le trafic Radius ne doit pouvoir être intercepté en aucun point de

la chaîne.

- proxy MIP-WIFI de rattachement : configurer le proxy MIP-WIFI (nom ou adr IP, ports, secret partagé associé) (fichiers *clients.conf* et *proxy.conf* dans le cas de FreeRadius)

Exemple pour proxy.conf :

```
# le proxy MIP-WIFI ne doit pas être déclaré dead si un 1 de
ses clients ne répond pas :
    dead_time = 0

realm ups-tlse.fr{
    type          = radius
    authhost      = rad1.cict.fr:1812
    accthost      = rad1.cict.fr:1813
    secret        = <secret partagé>
    nostrip
}

realm realm2-mipwifi {
    type          = radius
    authhost      = rad1.cict.fr:1812
    accthost      = rad1.cict.fr:1813
    secret        = <secret partagé>
    nostrip
}
```

Exemple pour clients.conf :

```
# le proxy MIP-WIFI rad1.cict.fr :
client 195.220.59.2{
    secret        = <secret partagé>
    shortname     = rad1.cict.fr
}
```