Gamme de postes MiVoice 5000
Chiffrement des communications

10/2021

AMT/PTD/PBX/0103/5/7/FR

MANUEL DE MISE EN ŒUVRE

Avertissement

Bien que les informations contenues dans ce document soient considérées comme pertinentes, Mitel Networks Corporation (MITEL ®) ne peut en garantir l'exactitude.

Les informations sont susceptibles d'être modifiées sans préavis et ne doivent pas être interprétées de quelque façon que ce soit comme un engagement de Mitel, de ses entreprises affiliées ou de ses filiales.

Mitel, ses entreprises affiliées et ses filiales ne sauraient être tenues responsables des erreurs ou omissions que pourrait comporter ce document. Celui-ci peut être revu ou réédité à tout moment afin d'y apporter des modifications.

Aucune partie de ce document ne peut être reproduite ou transmise sous une forme quelconque ou par n'importe quel moyen - électronique ou mécanique – quel qu'en soit le but, sans l'accord écrit de Mitel Networks Corporation.

© Copyright 2021, Mitel Networks Corporation. Tous droits réservés.

Mitel ® est une marque déposée de Mitel Networks Corporation.

Toute référence à des marques tierces est fournie à titre indicatif et Mitel n'en garantit pas la propriété.

SOMMAIRE

1 A PROPOS DE CE DOCUMENT 4

1.1 OBJET DE CE DOCUMENT 4
1.2 AUDIENCE DE CE DOCUMENT 4
1.3 PORTEE DE CE DOCUMENT 4
1.4 TERMINOLOGIE 4
1.4.1 TERMES ET EXPRESSIONS 4
1.4.2 ABREVIATIONS 5
1.5 DOCUMENTS DE REFERENCE 5

2 CHIFFREMENT DES COMMUNICATIONS 6

2.1 INTRODUCTION 6
2.1.1 MODES ET PRINCIPES DE CHIFFREMENT 7
2.1.2 RAPPEL SUR LES CERTIFICATS 8
2.1.3 CONTENU DES CERTIFICATS 13
2.1.3.1 Règles 13
2.1.3.2 Champs à renseigner dans les certificats 13
2.1.4 CHIFFREMENT EN MODE BOTHWAY 15
2.1.5 DROIT ET LICENCE RELATIFS AU CHIFFREMENT 15
2.1.6 CHIFFREMENT CONFERENCE 16
2.1.7 RESTRICTIONS ET LIMITATIONS 16
2.2 CONFIGURATION DU CHIFFREMENT DES COMMUNICATIONS SUR UNE CONFIGURATION AVEC MIVOICE 5000 MANAGER 17
2.2.1 PRE-REQUIS 17
2.2.2 CONFIGURATION DU CHIFFREMENT DES COMMUNICATIONS SUR CHAQUE SYSTEME MITEL 5000 GATEWAYS OU MIVOICE 5000 SERVER 17
2.3 CONFIGURATION DU CHIFFREMENT DES COMMUNICATIONS SUR UNE CONFIGURATION SANS MIVOICE 5000 MANAGER 19
2.3.1 OPERATIONS PREALABLES 20
2.3.2 CONFIGURATION DU CHIFFREMENT DES COMMUNICATIONS SUR LE SYSTEME MITEL 5000 GATEWAYS OU MIVOICE 5000 SERVER 20
2.4 CONFIGURATION PAR TMA 21
2.4.1 COPIE DU CERTIFICAT AUTORITE DE CERTIFICATION UTILISE PAR LES TERMINAUX DANS LE SERVEUR DE TELECHARGEMENT 21
2.4.2 CONFIGURATION DES MITEL 6000 SIP PHONE 22
2.4.3 CONFIGURATION DES MIVOICE 5300 IP PHONE 26
2.5 VERIFICATIONS 28
2.5.1 CONFIGURATION DU CHIFFREMENT 28
2.5.2 FONCTIONNEMENT DU CHIFFREMENT DES COMMUNICATIONS SUR LES TERMINAUX 29
2.5.3 FONCTIONNEMENT DU CHIFFREMENT INTER-SITE 29
2.5.4 PRINCIPALES CAUSES D'ERREUR 29
2.6 CONFIGURATION DES TERMINAUX MITEL 6000 SIP PHONE EN MODE BOTHWAY 30
2.6.1 INTRODUCTION 30
2.6.2 CONFIGURATION DU CHIFFREMENT EN MODE BOTHWAY 31
2.6.2.1 Opérations préalables 31
2.6.2.2 Configuration du mode BOTHWAY 31
2.6.2.3 Méthode sur une maquette de préconfiguration 32
2.6.2.4 Configuration des terminaux Mitel 6000 SIP Phone par l'application TMA 32
2.6.2.5 Vérification du fonctionnement 32
2.7 ENVIRONNEMENT DECT 32
2.8 ARRET DU CHIFFREMENT DES COMMUNICATIONS 34
2.8.1 TOUT MODE 34
2.8.2 MODE BOTHWAY 35

1 A PROPOS DE CE DOCUMENT

1.1 OBJET DE CE DOCUMENT

Ce document décrit, pour la solution MiVoice 5000 (version ≥ R7.2), les mécanismes permettant de mettre en œuvre le chiffrement des communications sur les terminaux de la gamme MiVoice 5300 IP phone et Mitel 6000 SIP Phone.

Le chiffrement des communications concerne :

- Les flux voix
- Les flux de signalisation

1.2 AUDIENCE DE CE DOCUMENT

Ce document est destiné aux installateurs et leur fournit les informations suivantes :

- Principe de fonctionnement du chiffrement des communications dans différentes architectures réseaux
- Restrictions et limitations actuelles
- Configuration du chiffrement des communications sur les systèmes MiVoice 5000 Server et Mitel 5000 Gateways (y compris Mitel EX Controller Mitel GX Gateway)
- Configuration du chiffrement des communications sur les terminaux
- Désactivation du chiffrement des communications.

1.3 PORTEE DE CE DOCUMENT

Ce manuel s'applique aux postes propriétaires IP de la gamme MiVoice 5300 IP phone et aux postes SIP de la gamme Mitel 6700/6800/6900 SIP Phone dans le périmètre de la solution MiVoice 5000 (version ≥ R7.2).

1.4 TERMINOLOGIE

1.4.1 TERMES ET EXPRESSIONS

Mitel 5000 Gateways	Ce terme regroupe l'ensemble des systèmes, XS, XL et XD
MiVoice 5000 Server/EX Controller	Système de commutation téléphonique hébergé sur un PC Linux/CentOS
XS, XL, XD	Gateways physiques de la gamme MiVoice 5000.
LLDP	Le protocole LLDP (Link Layer Discovery Protocol, IEEE 802.1AB est un type de trame permettant à des équipements réseaux (station, switch, routeur, téléphone IP) de communiquer leur identité et leur fonction à leur environnement
Poste SIP	Poste IP utilisant le protocole SIP (Session Initiation Protocol).

1.4.2 ABREVIATIONS

CD-ROM: **C**ompact **D**isk-**R**ead **O**nly **M**emory

DHCP: **D**ynamic **H**ost **C**onnexion **P**rotocol

FTP: **F**ile **T**ransfert **P**rotocole

LAN: **L**ocal **A**rea **N**etwork

LLDP: **L**ink **L**ayer **D**iscovery **P**rotocol

NTP: **N**etwork **T**ime **P**rotocol

OS: **O**perating **S**ystem

PBX: **P**rivate **B**ranch e**X**change

PC: **P**ersonal **C**omputer

RAM: **R**andom **A**ccess **M**emory

RAZ: **R**emise **A** **Z**éro

RHM: **R**elation **H**omme **M**achine

SIP: **S**ession **I**nitiation **P**rotocol

TDW: **T**erminal **D**ownload **S**erver

TFTP: **T**rivial **F**ile **T**ransfert **P**rotocolr

TMA: **T**erminal **M**anagement **A**pplication

TMA-EP: **TMA E**xpert **P**rovisioning

VLAN: **V**irtual **L**ocal **A**rea **N**etwork

1.5 DOCUMENTS DE REFERENCE

Se référer à la documentation technique fournie sur le site Mitel.com.

2 CHIFFREMENT DES COMMUNICATIONS

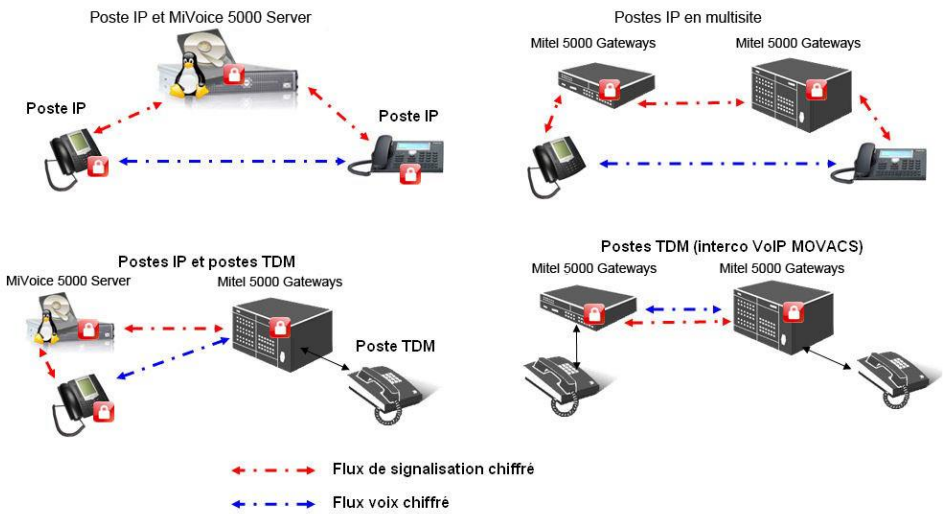
2.1 INTRODUCTION

La solution MiVoice 5000 offre le chiffrement complet des communications. Le chiffrement complet des communications concerne les flux voix et les flux de signalisation. Il est disponible sur les terminaux de la gamme MiVoice 5300 IP phone et Mitel 6000 SIP Phone.

La fonction chiffrement des communications permet de sécuriser dans une infrastructure réseau IP les flux de signalisation et de voix sur IP émis entre :

- Les terminaux MiVoice 5300 IP phone/Mitel 6000 SIP Phone, chiffrement de la voix (SRTP),
- Les terminaux MiVoice 5300 IP phone/Mitel 6000 SIP Phone et un système Mitel 5000 Gateways (carte EIP), chiffrement de la voix,
- Les terminaux MiVoice 5300 IP phone/Mitel 6000 SIP Phone et un système Mitel 5000 Gateways / MiVoice 5000 Server/EX Controller, chiffrement de la signalisation (TLS),
- Les systèmes Mitel 5000 Gateways/MiVoice 5000 Server/Cluster Server/EX Controller sur un lien inter-site (Multi-site IP), chiffrement de la signalisation (TLS),
- Les terminaux TDM (analogiques, numériques - MiVoice 5300 Digital phone, 675x Digital, DECT et S0), via des systèmes Mitel 5000 Gateways sur un lien inter-site ou inter-nœuds, chiffrement de la voix entre les deux cartes EIP (la communication entre la carte EIP et le poste TDM n'est pas chiffrée),
- Entre un terminal TDM (analogiques, numériques - MiVoice 5300 Digital phone, 675x Digital, DECT et S0) ou un trunk TDM et un terminal MiVoice 5300 IP phone/Mitel 6000 SIP Phone via des systèmes Mitel 5000 Gateways, chiffrement de la voix entre la carte EIP et le terminal MiVoice 5300 IP phone/Mitel 6000 SIP Phone,
- Et plus généralement entre deux terminaux ou applications supportant le chiffrement.

Chiffrement des communications : signalisation et voix



Le chiffrement est disponible sur :

- Terminaux MiVoice 5300 IP phone
- Terminaux Mitel 6700, 6800 et 6900 SIP Phone
- Terminaux TDM (analogiques, numériques - MiVoice 5300 Digital phone, 675x Digital, DECT et S0), via gateways X Series et avec cartes EIP
- Trunk TDM, via les Mitel Gateways X Series et avec carte EIP.
- Les terminaux DECT raccordés à une infrastructure Mitel SIP DECT Mitel
- Les terminaux analogiques et trunks analogiques ou T0/T2 raccordés sur Mitel EX Controller
- Les terminaux analogiques raccordés sur Mitel GX Gateways et Mitel TA 71xx.
- Et plus généralement, tous les terminaux SIP supportant le chiffrement.

2.1.1 MODES ET PRINCIPES DE CHIFFREMENT

Le chiffrement disponible dans la solution MiVoice 5000 repose sur les protocoles suivants :

- Chiffrement des flux voix par le protocole SRTP (Secured RTP) utilisant l'algorithme AES 128 Bits ou 256 (à partir de 7.2 et selon capacités des terminaux) avec l'algorithme HMAC pour l'authentification
- Chiffrement de la signalisation par le protocole TLS

Le chiffrement de la signalisation s'applique sur :

- Les liens inter-sites (notamment lien inter-site entre un Cluster Server et un site distant)
- Les liens entre le Cluster Server et les nœuds (liens intra-cluster)
- Le chiffrement de la signalisation des communications avec des terminaux MiVoice 5300 IP phone et Mitel 6000 SIP Phone.

Le protocole TLS est utilisé pour effectuer ce chiffrement.

Deux modes de chiffrement sont proposés par le MiVoice 5000 Manager :

- Chiffrement par certificat auto-signé
- Chiffrement par certificat externe.

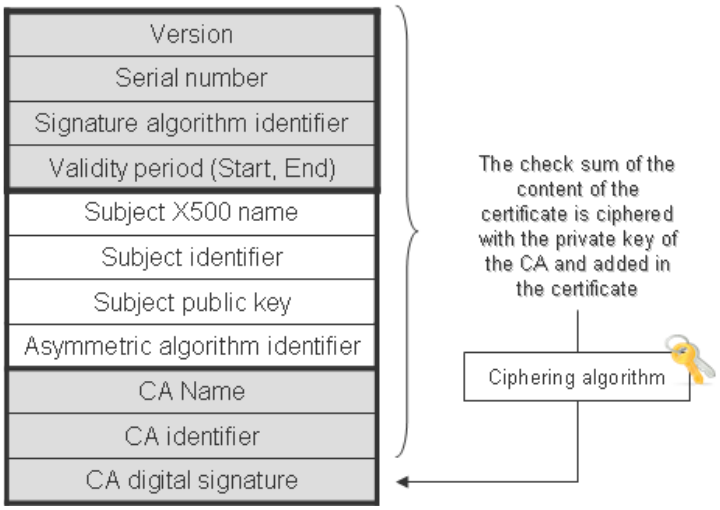
Dans le MiVoice 5000 Manager, le chiffrement est un paramètre de configuration à base Multisite mais l'administrateur peut autoriser ou non le chiffrement site par site.

ATTENTION : Dans le cas du chiffrement au sein du Cluster, les Nœuds héritent des propriétés du Cluster Server. Si le chiffrement est activé sur le Cluster Server depuis MiVoice 5000 Manager, il est alors implicitement activé sur les Nœuds Le chiffrement est opérationnel entre deux systèmes (Cluster Server et site distant) uniquement s'il est activé sur les deux systèmes concernés.

2.1.2 RAPPEL SUR LES CERTIFICATS

Quelques notions théoriques :

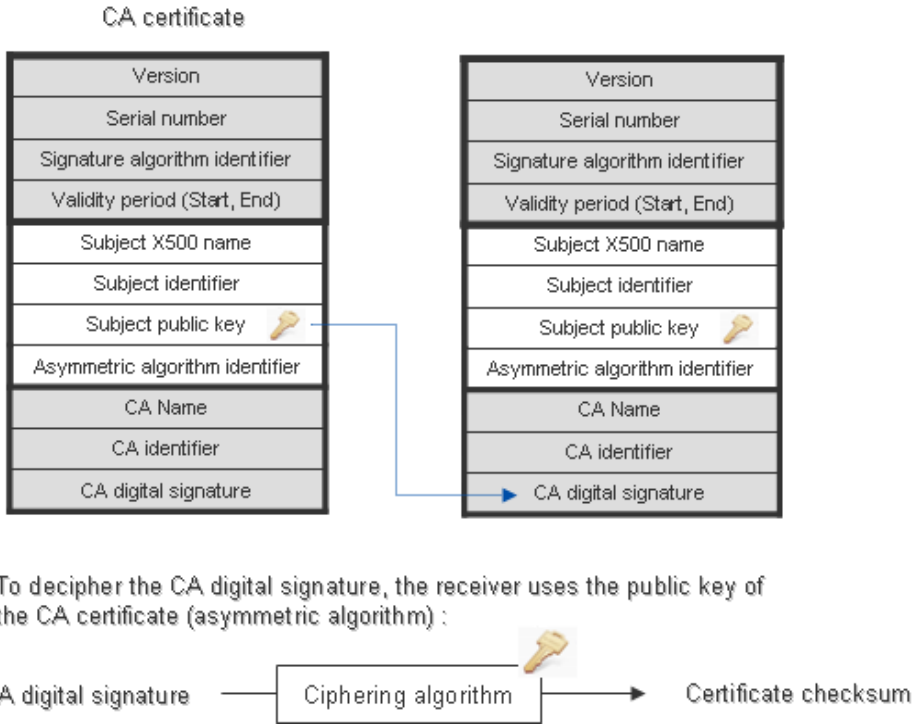
Le protocole TLS permet de sécuriser des échanges de données entre différentes parties. Il repose sur une infrastructure de clés publiques (ou PKI Public Key Infrastructure) mettant en œuvre un chiffrement asymétrique via l'utilisation de clés publiques et privées. Ces clés sont dérivées de certificats émis par une autorité de certification (CA Certification Authority).



Exemple de certificat

Le certificat contient 3 sections :

- La première section identifie le certificat
- La seconde section identifie l'entité qui envoie le certificat (i.e. le possesseur du certificat)
- La troisième section identifie l'autorité de certification (CA). Cette CA doit être connue (ou approuvée) du récepteur du certificat : la clé publique associée à la CA est utilisée par le récepteur pour déchiffrer la signature du possesseur du certificat



Pour valider un certificat reçu, les attributs suivants sont utilisés :

- *Validity period* : période de validité du certificat
- *Subject identifier* : pour identifier le possesseur du certificat (ex :@IP)
- *Subject Public Key* : clé public utilisée pour chiffrer la clé de session TLS
- *Algorithme utilisé pour chiffrer la signature* : ce même algorithme est utilisé pour déchiffrer la signature.

Le protocole TLS va donc permettre l'authentification des parties et le chiffrement des données en utilisant les certificats ; à l'initialisation de la session TLS, les certificats sont échangés pour authentifier les parties et négocier les protocoles de chiffrement à utiliser.

Rappels sur les protocoles utilisés dans les certificats :

- RSA est un algorithme de chiffrement utilisé en **cryptographie à clé publique. Il permet de générer un couple (clé privée, clé publique) qui est utilisé dans le dialogue d'établissement de la session TLS.**
- SHA est une fonction de hachage qui permet de faire une empreinte d'un certificat, appelée signature du certificat.

Il existe 2 types de certificats :

- Les certificats auto-signés (self-signed certificates) par l'iPbx/CS
- Les Certificats de confiance (trusted certificats) délivrés par une autorité de certification (CA) externe ou privée.

L'import d'un certificat trusted s'effectue à l'aide d'un fichier au format PKCS#12 qui est sécurisé par un mot de passe. Ce mot de passe devra également être saisi. Le fichier PKCS#12 doit contenir :

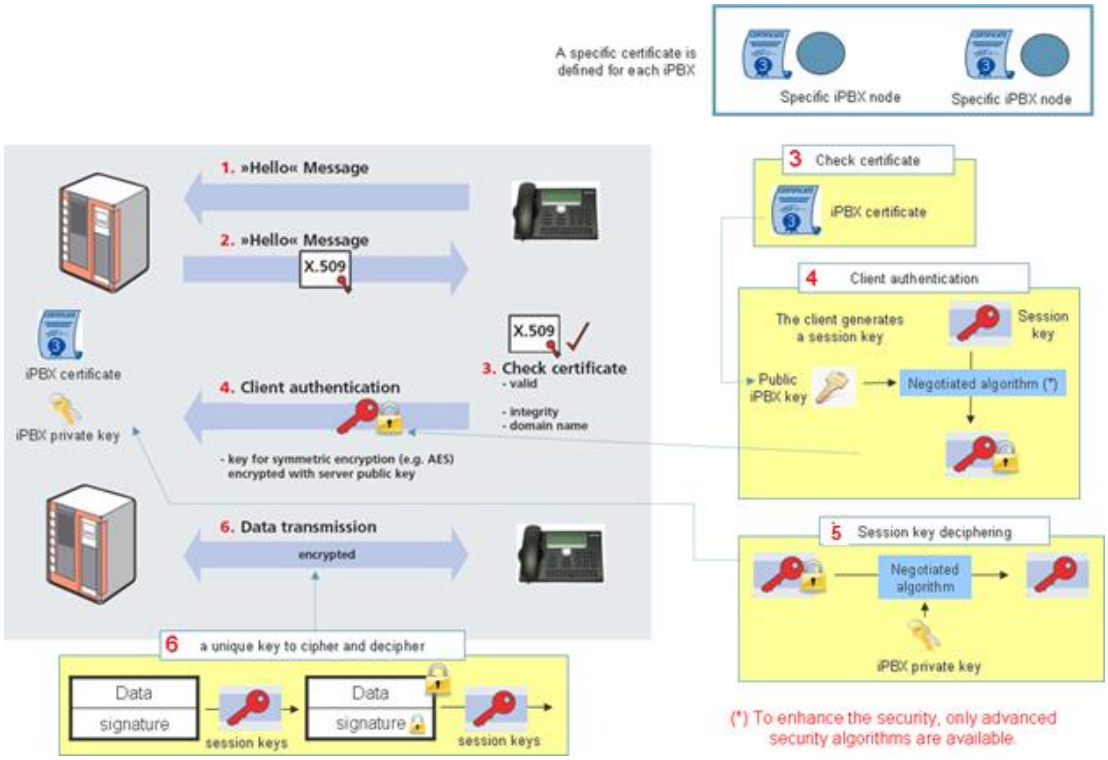
- La chaine de certification des autorités (CA),
- La clé privée et le certificat du serveur.

Note : Le chiffrement de la signalisation est obligatoire pour que le chiffrement de la voix soit effectif

L'activation de TLS sur les terminaux est réalisée par TMA.

Utilisation de certificats auto-signés (self-signed certificates)

Les différents échanges sont illustrés ci-dessous :



Chiffrement de la signalisation iPbx/Terminaux avec utilisation de certificats auto-signés

Les étapes sont les suivantes :

- Le terminal établit la session TLS et envoie un message TLS de type HELLO.
- L'iPbx/Call Server envoie en retour son certificat auto-signé au terminal
- Le terminal réalise un contrôle simple (intégrité, validité du certificat, nom de domaine)
- Les clés de session sont générées selon les algorithmes de chiffrement négociés entre l'iPbx et le terminal (pendant la session HELLO)

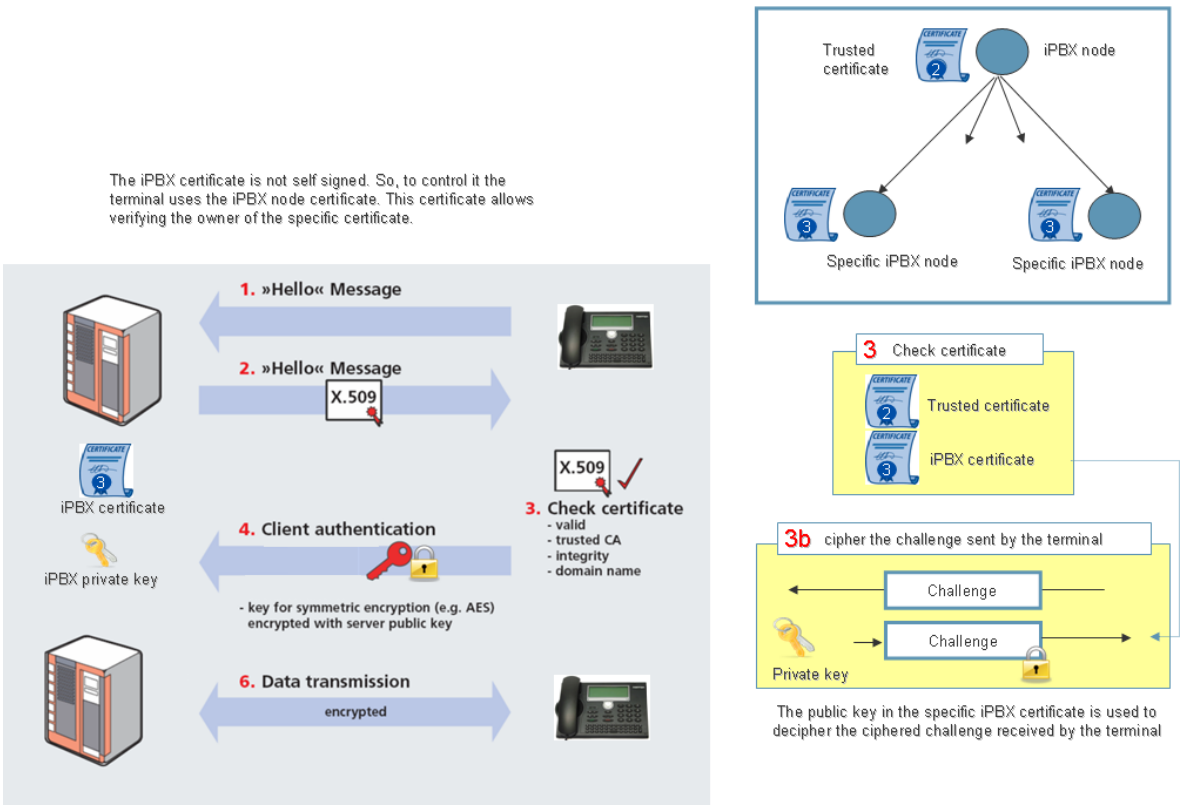
Cette solution permet de simplifier la gestion des certificats et d'ainsi simplifier le déploiement et le maintien en conditions opérationnelles de la solution. **Cependant elle ne permet pas d'authentifier l'entité qui envoie le certificat** (i.e. l'iPbx/CS) et ne peut empêcher sous certaines conditions des attaques de type *man-in-the-middle*.

Utilisation de certificats de confiance (trusted certificates)

Afin de pouvoir authentifier l'iPbx/Call Server et vérifier le certificat émis par celui-ci, le terminal peut utiliser un certificat de confiance.

Il lui est également possible d'envoyer un challenge à l'iPbx/CS pour vérifier que l'iPbx/CS possède bien la clé privée associée à ce certificat.

Cette méthode permet d'éviter les attaques de type man-in-the-middle. Elle requiert cependant un peu plus de moyens pour la mise en œuvre et le maintien en conditions opérationnelles. Le certificat émis par l'iPbx/CS étant lui-même construit et délivré par la CA externe.



Chiffrement de la signalisation iPbx/Terminaux avec utilisation de certificats de confiance

Mutual TLS (MTLS)

Le protocole Mutual TLS (MTLS) se réfère à deux parties s'authentifiant en même temps, étant un mode d'authentification par défaut dans certains protocoles (IKE, SSH) et facultatif dans d'autres (TLS).

Ce protocole assure une plus grande sécurité car il permet à chacune des deux extrémités de vérifier l'identité de l'autre.

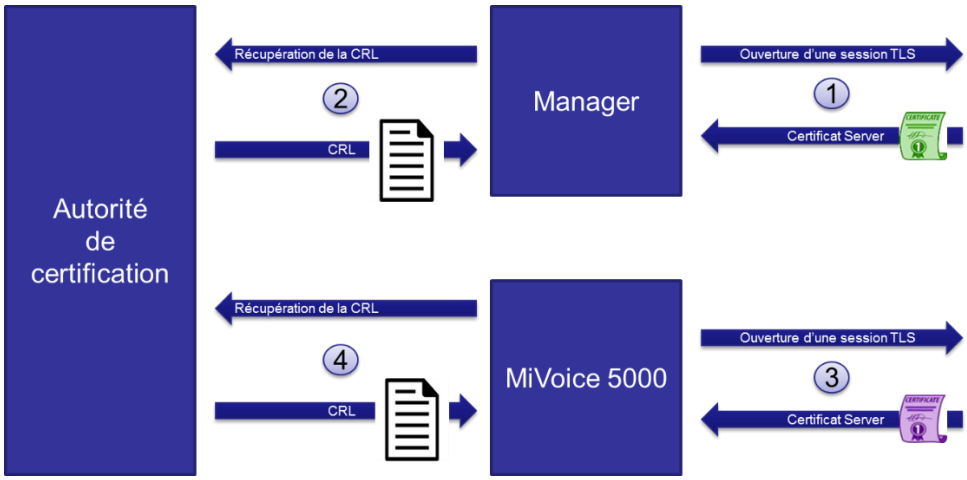
Par défaut, le protocole TLS ne prouve l'identité du serveur au client qu'à l'aide du certificat X.509 et l'authentification du client au serveur est laissée à la couche application. TLS propose également une authentification client-serveur à l'aide de l'authentification X.509 côté client.

L'authentification mutuelle TLS (MTLS) est beaucoup plus répandue dans les applications interentreprises (Business to Business), où un nombre limité de clients programmatiques et homogènes se connectent à des services Web spécifiques, la charge opérationnelle est limitée et les exigences de sécurité sont généralement beaucoup plus élevées par rapport aux environnements des utilisateurs.

Utilisation de certificats de confiance (trusted certificates) avec CRL

Avec la version R7.0, la solution MiVoice 5000 s'enrichit au niveau sécurité en permettant la mise en place de la vérification de validité des certificats « Trusted » grâce à la méthode des CRLs (Certificate Revocation List). Cette CRL contient une liste de certificats révoqué par l'autorité.

Lors d'une connexion cliente en mode TLS depuis le MiVoice 5000 ou un MiVoice 5000 Manager, une vérification de la validité du certificat est effectuée selon le principe suivant :



Si le certificat est présent dans la CRL, la confiance envers ce certificat X.509 est rompue et la connexion ne s'établie pas. Par ailleurs un audit périodique permet de rompre les connexions dont le certificat est révoqué.:.

Remarque : seul les certificats « trusted » peuvent être révoqués et permettent de vérifier l'authenticité du serveur/poste

2.1.3 CONTENU DES CERTIFICATS

2.1.3.1 Règles

Le contenu d'un certificat doit obligatoirement refléter et contenir les informations qu'utilisent tous les éléments de la configuration (clients, machines et terminaux).

Selon le type de connections au serveur, les informations suivantes sont impératives dans la constitution du certificat :

- Pour une connexion au serveur par l'adresse IP, le certificat doit contenir l'adresse IP,
- Pour une connexion au serveur par le FQDN, le certificat doit contenir le FQDN,
- Pour une connexion au serveur par l'un ou l'autre, le certificat doit contenir l'adresse IP et le FQDN.

Cas particulier du service SIP

L'adresse IP doit obligatoirement être indiquée dans le certificat,

Si les postes 53xxIP sont utilisés, l'adresse IP doit être dans le CN (Common Name).

Multisite

Pour un multisite, l'adresse IP peut être dans le CN ou les Alternatives names.

Pour une configuration en FQDN, l'adresse IP n'est pas nécessaire.

Si le champ **Extended Key Usage** est défini, il doit contenir **Client et Serveur** pour le multisite (double authentification).

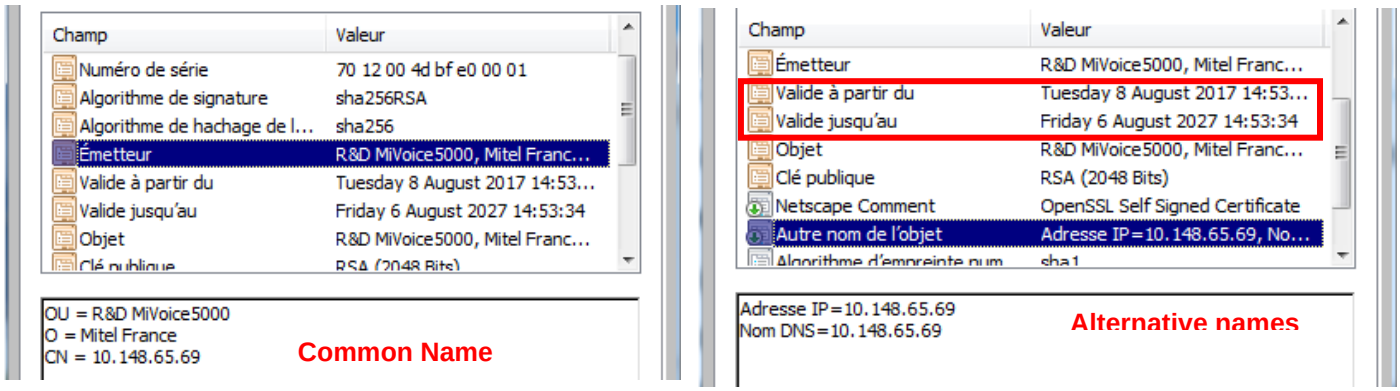
2.1.3.2 Champs à renseigner dans les certificats

Le certificat autosigné SHA2 ou SHA1 est généré par le PBX. Il n'est pas possible d'importer un certificat autosigné.

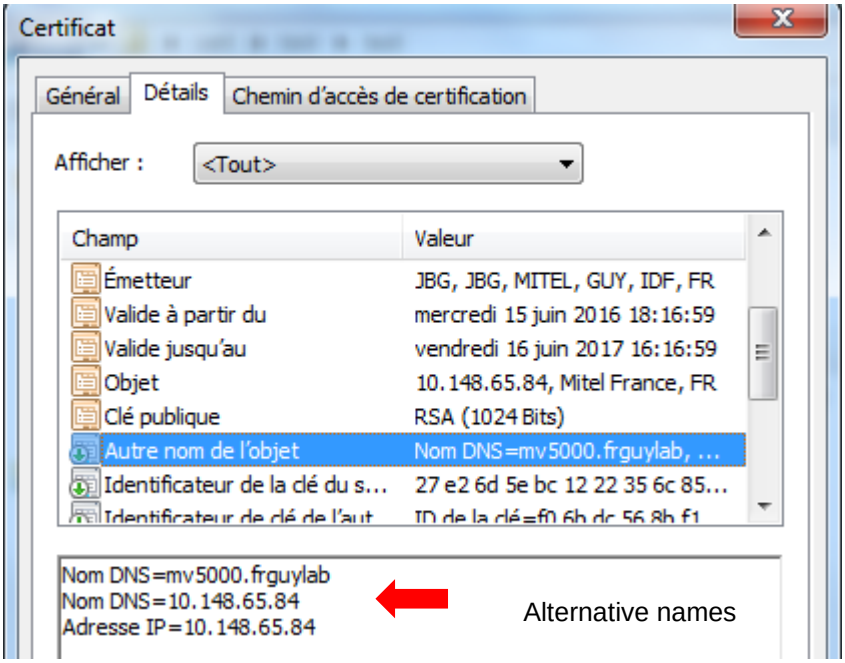
Principaux champs à renseigner :

- **Common name** : @IP (TEL si séparation de réseau) du PBX
- **Alternative names** : l'ensemble des @IP qui permettent d'accéder au PBX (ADMIN et TEL) et l'ensemble des FQDN qui sont associés aux interfaces TEL et ADMIN
- **Dates de validité**
- **X509v3 Extended Key Usage**: "TLS Web Server Authentication" et "TLS Web Client Authentication"

Exemple pour un iPBX accessible par l'adresse 10.148.65.69 (pas de FQDN) :



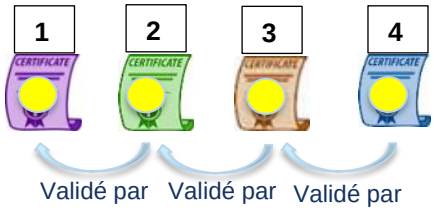
Exemple avec un FQDN pour les champs **alternative name**



Dans ce cas le champ **CN** est toujours configuré avec l'adresse IP TEL (ex: CN=10.148.65.84).

Dans le cas d'une chaine de certification, les certificats intermédiaires ne sont pas associés à un serveur particulier et ne sont donc pas associés à une adresse IP ou un FQDN.

C'est dans l'exemple suivant, le cas des certificats 1, 2 et 3 :



Ils doivent contenir l'attribut **X509v3 Basic Constraints** positionné à **CA:TRUE**. Cet attribut indique que le certificat est capable de signer un certificat.

Si l'attribut **X509v3 Key Usage** est défini, il doit également contenir l'autorisation de signer un certificat soit la valeur **Key Cert Sign**.

Les options **CA:TRUE** et **Key Cert Sign** ne sont pas positionnées dans le cas du certificat serveur (certificat 4 dans l'exemple) puisqu'il n'a pas cette capacité. Le certificat serveur est le dernier certificat de la branche des certificats.

Le format du certificat Serveur est similaire au certificat autosigné et donc contenir les champs suivants :

- **Common name** : @IP (TEL si séparation de réseau) du PBX
- **Alternative names** : l'ensemble des @IP qui permettent d'accéder au PBX (ADMIN et TEL) et l'ensemble des FQDN qui sont associés aux interfaces TEL et ADMIN
- **Dates de validité** (attention à ne pas installer un certificat qui n'est pas encore valide)
- **X509v3 Extended Key Usage**: "TLS Web Server Authentication" et "TLS Web Client Authentication".

2.1.4 CHIFFREMENT EN MODE BOTHWAY

Le chiffrement de la signalisation par le protocole TLS peut être configuré en mode BOTHWAY. Ce mode de fonctionnement doit être activé via le Web Admin à partir d'un paramètre spécifique (se référer au paragraphe considéré).

Note : Par défaut, le mode BOTHWAY est désactivé sur une nouvelle installation ou lors d'une mise à jour

Lorsque ce paramètre est activé, si un terminal SIP tente d'ouvrir une session TLS sur le port 5061, l'iPBX demande au terminal SIP de lui fournir un certificat. L'iPBX effectue alors une vérification de ce certificat :

- Le certificat doit être daté correctement (date de validité)
- Le certificat doit être correctement signé par l'un des certificats contenus dans le fichier d'autorité de certification téléchargé dans l'iPBX.

ATTENTION : Ce paramètre n'est pas géré par le MiVoice 5000 Manager. L'iPBX configuré en mode BOTHWAY n'accepte plus les terminaux se connectant en UDP ou TCP.

ATTENTION : Ce mode de fonctionnement n'est compatible qu'avec les postes IP pouvant contenir un certificat.

Le détail des procédures à suivre pour configurer le chiffrement des communications en mode BOTHWAY est précisé dans le chapitre considéré.

2.1.5 DROIT ET LICENCE RELATIFS AU CHIFFREMENT

Pour configurer le chiffrement des communications avec des terminaux, il est nécessaire de s'assurer que :

- Le système sur lequel le terminal est déclaré doit être déverrouillé au niveau du chiffrement. Une **licence** autorise le chiffrement.
- L'abonnement sur lequel le terminal est connecté possède le **droit au chiffrement**.
- Le système sur lequel le terminal est déclaré a le chiffrement de la voix activé (Paramètre **chiffrement voix**).
- Le chiffrement inter-site doit être activé sur le système où le poste est déclaré si le correspondant est sur un autre système ou si on est dans une architecture Cluster. Idem pour le distant (Paramètre **chiffrement inter-iPBX**).
- Le terminal IP doit avoir la capacité de faire du chiffrement de la voix. Cela nécessite une configuration du terminal.
- La signalisation entre le système et le terminal doit être chiffrante.
- Un certificat émanant d'un organisme de certification (certificat trusted) est installé sur chaque système Mitel 5000 Gateways ou MiVoice 5000 Server (chaque système possède son propre certificat et une Autorité de certification communs à tous les systèmes).
- Dans le cas de l'utilisation d'un certificat trusted sur les systèmes Mitel 5000 Gateways ou MiVoice 5000 Server, une autorité de certification du même organisme de certification est installé sur tous les terminaux (tous les terminaux utilisent la même Autorité de certification.

Pour les terminaux configurés en mode chiffrement, le flux de signalisation sera toujours crypté et le flux voix le sera en fonction de la configuration des paramètres du Web Admin (**chiffrement voix, chiffrement inter-sites, droit au chiffrement, licence**).

Un certificat a une durée limitée.

Un certificat auto-signé a une durée de vie de 1 an. Il sera renouvelé automatiquement.

Un certificat trusted a une durée de vie donné par l'organisme de certification, en général de plusieurs années. L'administrateur est averti de l'expiration du certificat 14 jours avant, puis tous les jours jusqu'à l'expiration effective. Lorsque le certificat a expiré, les communications sont toujours possibles mais la voix n'est plus chiffrée.

Note : Le certificat pour le système Mitel 5000 Gateways ou MiVoice 5000 Server est unique et généré par l'organisme de certification avec son adresse IP comme paramètre de commonName (Nom d'usage).

2.1.6 CHIFFREMENT CONFÉRENCE

La fonction conférence peut être chiffrée sur le MiVoice 5000 Server. Dans ce cas, l'ensemble des terminaux associés à un ou plusieurs ponts de conférence du MiVoice 5000 Server doivent obligatoirement être chiffrants eux-mêmes.

Le chiffrement d'une conférence sur le MiVoice 5000 Server concerne uniquement les terminaux maitres de conférence suivants enregistrés sur le MiVoice 5000 Server :

- MiVoice 5300 IP phone
- Virtual TDM (via EIP et lien multisite chiffrant)

Note : Les terminaux Mitel 6000 SIP Phone, maitres de conférence, gèrent par eux-mêmes la fonction conférence qu'elle soit chiffrée ou non (pas de ressources prises sur le MEDIA SERVER du MiVoice 5000 Server).

Les deux participants à la conférence chiffrée du MiVoice 5000 Server initiée par un terminal maitre de conférence MiVoice 5300 IP phone ou virtual TDM peuvent être :

- Des terminaux chiffrants enregistrés sur le MiVoice 5000 Server incluant Mitel EX Controller : MiVoice 5300 IP phone; Mitel 6000 SIP Phone, Virtual TDM
- Des terminaux enregistrés sur un système Mitel 5000 Gateways :
  - MiVoice 5300 IP phone et Mitel 6000 SIP Phone chiffrants
  - Postes TDM, postes analogiques, DECT TDM, accessibles via EIP et lien multisite chiffrant.
- Des terminaux distants accessibles via un accès RNIS ou LR analogique déclarés sur un système Mitel 5000 Gateways accessibles via EIP et lien multisite chiffrant.

ATTENTION : Si un participant non chiffrant est ajouté à un ou plusieurs ponts de conférence chiffrants déjà en communication, l'ensemble des participants des ponts de conférence se replient en mode non chiffrant.

ATTENTION : L'intrusion établit une conférence qui ne sera jamais chiffrée.

ATTENTION : En Ecoute/Intervention, il faut imposer la configuration de sorte que les 3 postes aient la même configuration (soit tous chiffrés, soit aucun.

2.1.7 RESTRICTIONS ET LIMITATIONS

Il n'est pas possible d'avoir une communication chiffrée entre un terminal MiVoice 5300 IP phone/Mitel 6000 SIP Phone et un terminal i7xx.

2.2 CONFIGURATION DU CHIFFREMENT DES COMMUNICATIONS SUR UNE CONFIGURATION AVEC MIVOICE 5000 MANAGER

En configuration multi-site avec certificat auto-signé :

Les terminaux chiffrants n'ont pas besoin de certificat car ils ne contrôlent pas sur quel système ils sont connectés.

Chaque système Mitel 5000 Gateways ou MiVoice 5000 Server possède son propre certificat basé sur son adresse IP.

En configuration multi-site avec certificat trusted :

Les terminaux MiVoice 5300 IP phone/Mitel 6000 SIP Phone chiffrants doivent disposer d'un certificat.

Chaque système Mitel 5000 Gateways ou MiVoice 5000 Server possède son propre certificat. Tous les certificats sont signés par la même autorité.

La procédure décrite dans ce chapitre s'appuie sur l'utilisation de l'application TMA du MiVoice 5000 Manager pour configurer les paramètres spécifiques des terminaux SIP nécessaires pour le chiffrement des communications.

ATTENTION : Les autres méthodes (Configuration manuelle du terminal par interface Web, par interface poste ou gestion manuelle des fichiers de configuration) sont fortement déconseillées.

2.2.1 PRE-REQUIS

- Multi-site configuré correctement et fonctionnel.
- Carte EIP présente et installé dans chacun des sites du multi-site (système Mitel 5000 Gateways)
- MiVoice 5000 Manager installé et configuré correctement pour gérer le multi-site
- Serveurs DHCP et FTP externes configurés correctement,
- Serveur NTP : Tous les sites doivent être configurés avec le même serveur NTP.
- Service postes non démarré sur chacun des sites

Note : Il est possible d'utiliser le serveur de téléchargement embarqué dans un système Mitel 5000 Gateways.

Dans le cas d'un **chiffrement à base Certificats Trusted** :

- Obtenir auprès de l'organisme compétent, les certificats considérés.

2.2.2 CONFIGURATION DU CHIFFREMENT DES COMMUNICATIONS SUR CHAQUE SYSTEME MITEL 5000 GATEWAYS OU MIVOICE 5000 SERVER

- Vérifier que la licence chiffrement est activée sur chacun des systèmes :
  - Se connecter à chacun des systèmes à partir de l'application MiVoice 5000 Manager (Menu **Actions immédiates>Configuration iPbx)** puis depuis le Web Admin parcourir les menus ci-dessous
  - Menu **Service téléphonie>Système>Info>Licences** (2.1.3)
  - La licence chiffrement doit être à l'état **Autorisé**
  - Dans le cas contraire saisir la nouvelle licence autorisant le chiffrement dans le champ **clé de déverrouillage**

- Vérifier que les classes de facilité utilisées par les abonnements téléphoniques sur lesquels sont enregistrés les terminaux ont droit à utiliser la fonction chiffrement :
  - A partir de l'application MiVoice 5000 Manager, aller dans le Menu **Caractéristiques techniques>Classes de facilités**
  - Vérifier pour chaque classe de facilité utilisée que le paramètre **Droit au chiffrement** est coché.

ATTENTION : Un terminal MiVoice 5300 IP phone/Mitel 6000 SIP Phone configuré chiffrant dont l'abonnement ne lui donne pas le Droit au chiffrement aura sa signalisation chiffrée et sa voix non chiffrée.

- Mettre en service la fonction Chiffrement voix :
  - Se connecter à chacun des systèmes à partir de l'application MiVoice 5000 Manager (Menu **Actions immédiates>Configuration iPbx)** puis depuis le Web Admin parcourir les menus ci-dessous
  - Menu **Service téléphonie>Réseau et liaisons>Qualité de service>Chiffrement et paramètres IP** (4.4.4)
  - Cocher la case **Chiffrement voix**
- Mettre en service la fonction Chiffrement de la signalisation et activer le certificat sur tous les systèmes du multi-site :
  - Sur le MiVoice 5000 Manager, menu **Administration**>**Topologie du réseau**
  - Sélectionner le **multisite** sur lequel le chiffrement par certificat doit être configuré puis cliquer sur le bouton **Configuration**,
  - Cocher **Chiffrement** pour autoriser le chiffrement sur le multisite,
  - Sélectionner **Type de chiffrement** :

Cas certificat autosigné

- Cliquer sur **Appliquer** puis sur **OK** : cela dégrise le bouton **Génération des certificats**,
  - Cliquer sur **Génération des certificats**,
  - A la question posée, **sélectionner Générer les certificats pour l'ensemble des sites du multisites** puis cliquer sur le bouton **Valider**
  - Dans le journal des opérations du MiVoice 5000 Manager, un message permet de vérifier le succès de l'opération de génération du certificat
  - Sélectionner le **multisite** sur lequel le chiffrement par certificat externe doit être configuré puis cliquer sur le bouton **Configuration**,
  - Cocher **chiffrement** pour autoriser le chiffrement sur le multisite,
  - Sélectionner Type de chiffrement à **Auto signé**,
- Cliquer sur **Appliquer** puis sur **OK** : cela dégrise le bouton **Génération des certificats**,
  - Cliquer sur **Génération des certificats**,
  - A la question posée, **sélectionner Générer les certificats pour l'ensemble des sites du multisites** puis cliquer sur le bouton **Valider**,
  - Dans le journal des opérations du MiVoice 5000 Manager, un message permet de vérifier le succès de l'opération de génération du certificat.

Note : Le MiVoice 5000 Manager envoie l'ordre de génération des certificats aux systèmes définis dans le multisite du MiVoice 5000 Manager (Cluster Server, Nœuds et sites distants) et le certificat est généré localement sur chaque système.

Note : Le chiffrement de la signalisation par certificat Auto-signé est alors opérationnel sur tous les systèmes du multisite.

Cas certificat Trusted

- Sélectionner Type de chiffrement à **Import**,
- Sélectionner le certificat externe à importer,
- Renseigner et confirmer le mot de passe associé au certificat,
- Cliquer sur **Importer** pour importer le certificat dans le MiVoice 5000 Manager,
- Cliquer sur **Appliquer** puis sur **OK** : cela dégrise le bouton **Génération des certificats**,
- Cliquer sur **Génération des certificats**,
- A la question posée, sélectionner **Générer les certificats pour l'ensemble des sites du multisites** puis cliquer sur le bouton **Valider**,
- Dans le journal des opérations du MiVoice 5000 Manager, un message permet de vérifier le succès de l'opération de génération du certificat.

Note : Le MiVoice 5000 Manager génère les certificats des systèmes (Cluster Server, Nœuds et sites distants) et les clés privées à partir des informations contenues dans le certificat externe et les diffuse vers chaque système.

Note : Le chiffrement par certificat externe est alors opérationnel sur tous les systèmes du multisite.

Lorsque le certificat est mis en service, la nouvelle date de début et de fin de validité du certificat actif est automatiquement mise à jour.

ATTENTION : Suite à l'installation du certificat, un redémarrage automatique du service SIP sera effectué.

2.3 CONFIGURATION DU CHIFFREMENT DES COMMUNICATIONS SUR UNE CONFIGURATION SANS MIVOICE 5000 MANAGER

En configuration avec certificat auto-signé :

En configuration monosite avec un certificat auto-signé, les terminaux MiVoice 5300 IP phone/Mitel 6000 SIP Phone "chiffrant" n'ont pas besoin de certificat car ils ne contrôlent pas sur quel système ils sont connectés.

Chaque système Mitel 5000 Gateways ou MiVoice 5000 Server possède son propre certificat basé sur son adresse IP.

En configuration avec certificat trusted :

En configuration monosite avec un certificat trusted, tous les terminaux MiVoice 5300 IP phone/Mitel 6000 SIP Phone "chiffrant" ont des certificats délivrés par la même autorité. Le système Mitel 5000 Gateways ou MiVoice 5000 Server possède son propre certificat. Tous les certificats sont signés par la même autorité.

La procédure décrite dans ce chapitre s'appuie sur l'utilisation de l'application TMA embarqué dans le Mitel 5000 Gateways pour configurer les paramètres spécifiques des terminaux MiVoice 5300 IP phone/Mitel 6000 SIP Phone nécessaires pour le chiffrement des communications.

ATTENTION : Les autres méthodes (Configuration manuelle du terminal par interface Web, par interface poste ou gestion manuelle des fichiers de configuration) sont fortement déconseillées.

2.3.1 OPERATIONS PREALABLES

- Vérifier que les services TMA et FTP (nécessaire pour les postes 53xxIP) sont démarrés.
  - Menu **Service téléphonie>Système>Configuration>Services** (2.3.1)
  - Service Postes : **DEMARRE**
- Configurer si nécessaire le service DHCP embarqué.

ATTENTION : Il ne faut pas configurer le paramètre SIP_PORT_PBX dans le serveur DHCP dans le cas du chiffrement des communications. Il doit être configuré dans le fichier de configuration global (cas de défense si le serveur de téléchargement n'est plus accessible et que le terminal MiVoice 5300 IP phone est chiffrant).

2.3.2 CONFIGURATION DU CHIFFREMENT DES COMMUNICATIONS SUR LE SYSTEME MITEL 5000 GATEWAYS OU MIVOICE 5000 SERVER

- Vérifier que la licence chiffrement est activée :
  - Menu **Service téléphonie>Système>Info>Licences** (2.1.3)
  - La licence chiffrement doit être à l'état **Autorisé**
  - Dans le cas contraire saisir la nouvelle licence autorisant le chiffrement dans le champ clé de déverrouillage
- Vérifier que les abonnements téléphoniques sur lesquels sont enregistrés les terminaux MiVoice 5300 IP phone/Mitel 6000 SIP Phone sont autorisés à utiliser la fonction chiffrement :
  - Menu **Service téléphonie>Abonnés>Abonnements>Caractéristiques** (1.2.3)
  - Vérifier pour chaque abonnement que le paramètre **Droit au chiffrement** est coché.

Note : Par défaut, tous les abonnements ont le Droit « Chiffrement autorisé ».

Note : Le droit au chiffrement peut également être associé à une classe de facilité via le menu Service téléphonie>Abonnés>Droits>Classes de facilités (1.4.3).

ATTENTION : Un terminal chiffrant dont l'abonnement ne lui donne pas le Droit au chiffrement aura sa signalisation chiffrée et sa voix non chiffrée.

- Activer le chiffrement voix et configurer le type à partir du menu **Service téléphonie>Réseau et liaisons>Qualité de service>Chiffrement et paramètres IP** (4.3.4).

Se référer au document MiVoice 5000 Server et Mitel Gateways - Manuel Exploitation aux paragraphes Chiffrement et paramètres IP et Sécurité (pour la gestion des certificats).

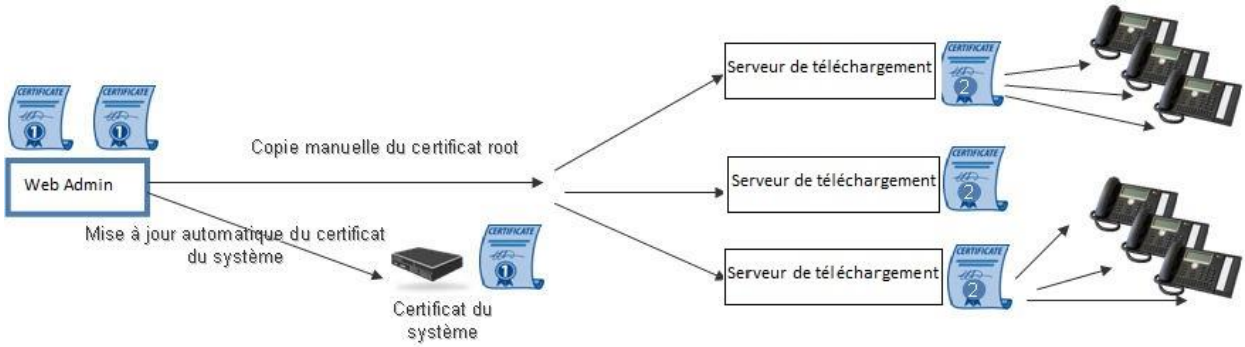
ATTENTION :

ATTENTION : Suite à l'installation du certificat, un redémarrage automatique du service SIP sera effectué.
Si le bouton Régénération du certificat est utilisé, un redémarrage automatique du service SIP sera effectué.

2.4 CONFIGURATION PAR TMA

2.4.1 COPIE DU CERTIFICAT AUTORITE DE CERTIFICATION UTILISE PAR LES TERMINAUX DANS LE SERVEUR DE TELECHARGEMENT

Dans le cas où on utilise un certificat émanant d'un organisme extérieur faisant autorité pour les terminaux, le certificat Autorité de certification doit être copié manuellement dans le serveur de téléchargement utilisé par les terminaux afin que ceux-ci le téléchargent.



Note : S'il n'y a pas de fichier d'autorité, le télécharger à partir du menu Service téléphonie>Système>Sécurité>Gestion des Certificats (2.4.1) (format pem).

Méthode Préconisée

A partir du MiVoice 5000 Manager, menu **Administration>Téléphonie>Gestion des terminaux**.

Note : Dans le cas d'une configuration avec plusieurs multisites, sélectionner la région, le multisite/site isolé puis cliquer sur le bouton Continuer.

- Saisir le login et le mot de passe attribués par l'administrateur
- La fenêtre d'accueil de l'application TMA s'ouvre :
  - Cliquer sur le menu **Déploiement**
  - Sélectionner la gamme **(**Mitel 6000 SIP Phone ou MiVoice 5300 IP phone)
  - Sélectionner dans la **Liste des serveurs**, le serveur de téléchargement vers lequel le certificat doit être téléchargé
  - Dans le champ **Autre fichier**, importer en cliquant sur **Parcourir**, le certificat ca.crt à télécharger
  - Cliquer sur le bouton **Valider**
  - Saisir le **Nom de l'action**
  - Indiquer **le type de Mise à jour** : immédiate ou différée
  - Cliquer sur le bouton **Valider**
  - Vérifier dans le **Suivi des actions** le bon déroulement du téléchargement unitaire du fichier vers le serveur de téléchargement.

ATTENTION : La sélection d'un serveur de téléchargement est obligatoire. Un seul fichier est autorisé par opération de provisioning Ce fichier n'est pas sauvegardé dans les répertoires de l'application TMA embarquée dans le MiVoice 5000 Manager.

ATTENTION : Des contrôles sur le nom du fichier sont réalisés :

- **Si le chiffrement des fichiers de configuration est activé, TMA interdit d'envoyer les fichiers *.cfg vers le serveur de téléchargement car ils ne seront pas pris en compte.**

2.4.2 CONFIGURATION DES MITEL 6000 SIP PHONE

Les paramètres à configurer sur les terminaux Mitel 6000 SIP Phone sont les suivants:

- **sip proxy port** => Spécifie le port utilisé par le Point d'accès SIP de l'iPBX. Ce port est obligatoirement égal à **5061** en mode TLS
- **sip registrar port** => Spécifie le port utilisé par le Point d'accès SIP de l'iPBX. Ce port est obligatoirement égal à **5061** en mode TLS
- **sip backup proxy port** => Spécifie le port utilisé par le Point d'accès SIP de l'iPBX de backup. Ce port est obligatoirement égal à **5061** en mode TLS
- **sip backup registrar port** => Spécifie le port utilisé par le Point d'accès SIP de l'iPBX de backup. Ce port est obligatoirement égal à **5061** en mode TLS
- **sip transport protocol** => Spécifie le protocole de transport utilisé par les terminaux Mitel 6700 SIP Phone. Ce paramètre a pour valeur soit **4** (protocole **TLS**), soit 1 (protocole UDP), soit 2 (protocole TCP). Ce paramètre doit avoir pour valeur **4**
- **sips persistent tls** => ce paramètre permet de valider (**1**) ou non (0) l'utilisation du mode TLS persistant. En mode TLS persistant, seul le fichier Trusted Certificate doit être défini. Ce paramètre doit avoir pour valeur **1**
- **sips persistent tls keep alive** => ce paramètre permet de définir la valeur du keepalive TLS (cela permet notamment au terminal de rétablir automatiquement sa session TLS persistante si celle-ci est déconnectée, de basculer si nécessaire vers le site de backup si la session TLS vers le site principal est déconnectée). Ce paramètre a pour valeur par défaut **30 secondes**
- **sips tls authentication** => Spécifie si on utilise un certificat auto signé par l'IPBX (**0**) ou un certificat émanant d'un organisme extérieur faisant autorité (**1**).
- **sips trusted certificates** => paramètre à configurer en mode auto signé, trusted ou BOTHWAY. Spécifie l'autorité de certification ayant signé le certificat des iPBX MiVoice 5000 (fichier avec extension .crt ou .pem). Dans le cas où on utilise un certificat auto signé par l'IPBX, ce champ doit être vide
- **sip srtp mode** => Spécifie si les appels SRTP sont interdits (0) , préférés (**1**) ou si seuls les appels SRTP sont acceptés/générés (2). Ce paramètre doit avoir pour valeur **1**
- **srtp aes256 key** => Activer ou non le SRTP AES 256. Valeur préconisée 1
- **time server1** => Spécifie l'adresse IP ou le nom d'hôte d'un serveur NTP. Le serveur NTP est obligatoire pour ouvrir une session **TLS**.
- **sips symmetric tls signaling** => ce paramètre permet de spécifier si on utilise systématiquement le port 5061 (**1**) ou si une valeur de port aléatoire est utilisé (0) (dans ce cas, à chaque redémarrage du terminal, un nouveau port est alloué). Valeur préconisée : **0**
- **sips root and intermediate certificates** => paramètre à configurer uniquement en mode BOTHWAY. Spécifie l'autorité de certification ayant signé le certificat des terminaux Mitel 6000 SIP Phone (fichier avec extension .crt ou .pem). En général, le contenu de ce paramètre est identique au paramètre **sips trusted certificates**
- **sips local certificate** => paramètre à configurer uniquement en mode BOTHWAY. Spécifie le certificat des terminaux Mitel 6000 SIP Phone (fichier avec extension .crt ou .pem)
- **sips private key** => paramètre à configurer uniquement en mode BOTHWAY. Clé privée associée au certificat des terminaux Mitel 6000 SIP Phone (fichier avec extension .crt ou .pem)

Note : Le paramètre sip local tls port spécifie le port utilisé par le poste Mitel 6700 SIP Phone pour émettre ses messages SIP en mode TLS. Ce port est obligatoirement égal à 5061 en mode TLS.Il est configuré par défaut à cette valeur dans le fichier de configuration global;

A partir du MiVoice 5000 Manager, menu **Administration>Téléphonie>Gestion des terminaux** :

Note : Dans le cas d'une configuration avec plusieurs multisites, une nouvelle fenêtre s'ouvre, sélectionner la région, le multisite/site isolé puis cliquer sur le bouton Continuer;

- Saisir le login et le mot de passe attribués par l'administrateur, la fenêtre d'accueil de l'application TMA s'ouvre.
- Effectuer la répartition des paramètres afin que les terminaux Mitel 6000 SIP Phone prennent en compte dans leur fichier spécifique les paramètres décrits ci-dessus pour le chiffrement des communications.
  - Menu Configuration des postes
  - Sélectionner la gamme Mitel 6000 SIP Phone
  - Sélectionner la version à configurer (paquet logiciel poste en production)

Une répartition des paramètres sous forme d'onglets est affichée uniquement pour la gamme Mitel 6000 SIP Phone :

- Encryption : paramètres de chiffrement des terminaux Mitel 6000 SIP Phone
- Config : paramètres de configuration usuels
- TimeZone : paramètres de configuration date et heure, serveur NTP, timezone
- Network : paramètres réseau (DHCP, VLAN, LLDP,..)
- RFC2833 : paramètres de configuration RFC2833 / SIP INFO
- 802.1X : paramètres de configuration 802.1X
- RTCP : paramètres de configuration RTCP
- Expert : tous les autres paramètres non présents dans les onglets précédents

Note : Afin de faciliter la mise en place de certaines fonctionnalités (chiffrement,..), des paramètres sont présentés deux fois dans l'onglet :

- **Dans la partie supérieure, les paramètres ont une portée et des valeurs figées**
- **Dans la partie inférieure, les mêmes paramètres ont une valeur par défaut pouvant être différente et une portée positionnée à ignorer.**

- Sélectionner l'onglet **Encryption** et positionner, pour les paramètres suivants présents dans cet onglet, leur portée à **Spécifique** :
  - sip proxy port
  - sip registrar port
  - sip backup proxy port
  - sip backup registrar port
  - sips symmetric tls signaling
  - sip transport protocol
  - sips persistent tls
  - sips trusted certificates
  - sips tls authentication
  - sip srtp mode
- Cliquer sur le bouton **Répartir** puis confirmer la répartition effectuée.

ATTENTION : Le paramètre time server1 se trouve dans l'onglet TimeZone avec une portée Globale par défaut. Lors du lancement d'une action manuelle de mise à jour des données globlales, ce paramètre devra être positionné avec l'adresse IP du système de référence.

- Définir et lancer une action de mise à jour des données spécifiques des terminaux Mitel 6000 SIP Phone. Cette action va permettre de configurer les terminaux Mitel 6000 SIP Phone pour le chiffrement des communications
- Cliquer sur le lien **Modifier les paramètres spécifiques.** Une nouvelle fenêtre s'ouvre:
- Celle-ci rappelle sur quels critères portent la mise à jour des données spécifiques:
- La **Région**, le **Multisite** et la **Gamme de poste** concerné: **Mitel 6000 SIP Phone**
- le **Modèle de poste** concerné: **tous les modèles**
- le **Logiciel** poste concerné
- Sélectionner la liste **All** (liste définie par défaut contenant tous les terminaux **Mitel 6000 SIP Phone** visibles dans l'inventaire)

Note : La liste "All" est définie par défaut et contient tous les postes connus de l'inventaire. A partir de R5.3, les postes logués et non logués sont visibles dans l'inventaire et sont gérés par l'application TMA embarqué dans le MiVoice 5000 Manager.

Note : Les valeurs grisées représentent les valeurs canoniques de chaque paramètre.

A partir de R6.1 SP1, une répartition des paramètres sous forme d'onglets est affichée uniquement pour la gamme Mitel 6000 SIP Phone:

- **Encryption** : paramètres de chiffrement des terminaux Mitel 6000 SIP Phone
- **Config** : paramètres de configuration usuels
- **TimeZone** : paramètres de configuration date et heure, serveur NTP, timezone
- **Network** : paramètres réseau (DHCP, VLAN, LLDP,..)
- **RFC2833** : paramètres de configuration RFC2833 / SIP INFO
- **802.1X** : paramètres de configuration 802.1X
- **RTCP** : paramètres de configuration RTCP
- **Expert** : tous les autres paramètres non présents dans les onglets précédents

Cette fenêtre présente également un tableau contenant trois colonnes :

- la colonne **C** permet, en la cochant, de sélectionner un paramètre spécifique pour lequel la nouvelle valeur saisie sera commune à l'ensemble des terminaux Mitel 6000 SIP Phone de la liste sélectionnée précédemment.
- la colonne **Paramètres** liste les paramètres contenus dans le fichier de configuration des données spécifiques présent dans l'application TMA. Cette liste est issue de la répartition réalisée précédemment.
- la colonne **Valeurs communes** permet de saisir la nouvelle valeur d'un paramètre spécifique sélectionnée via la colonne **C**.

Note : Des info-bulles permettent d'avoir une aide à la saisie sur la valeur de chacun des paramètres. Celles-ci apparaissent lorsque le curseur de la souris est positionné sur la valeur commune courante du paramètre.

- Vérifier les valeurs par défaut des paramètres

Note : Les valeurs par défaut des paramètres sont configurées de telle sorte que les terminaux Mitel 6000 SIP Phone sont chiffrants en mode auto signé.

- Cliquer sur le bouton **Enregistrer** puis sur le bouton **Valider**
- Saisir le **Nom de l'action**
- Sélectionner le **Type de mise à jour** :
  - o Immédiate
  - o Différée : préciser la date au format JJ/MM/AAAA et l'heure au format HHMM

Note :

En cliquant sur l'icône  **le calendrier s'ouvre et permet directement de sélectionner la date.**

- Cliquer sur le bouton **Valider** pour lancer l'action de mise à jour des données spécifiques communes aux terminaux Mitel 6000 SIP Phone.

ATTENTION : Une action lancée en mode différé permet de différer le transfert des données vers le serveur de téléchargement externe et l'ordre de mise à jour des données de l'iPBX.

Suite à l'exécution de l'action, lors de la réception du prochain REGISTER émis par un terminal Mitel 6000 SIP Phone, celui-ci redémarre automatiquement et ses paramètres sont mis à jour suite au téléchargement de son fichier spécifique : le terminal Mitel 6000 SIP Phone chiffre dès lors ses flux de voix et de signalisation.

2.4.3 CONFIGURATION DES MIVOICE 5300 IP PHONE

Les paramètres à configurer sur les terminaux MiVoice 5300 IP phone sont les suivants :

- **SIP_PORT_PBX** => Spécifie le port utilisé par l'iPBX en mode TLS. Ce port est obligatoirement égal à **5061** en mode TLS.

ATTENTION : Il ne faut pas configurer le paramètre SIP_PORT_PBX dans le serveur DHCP dans le cas du chiffrement des communications. Il doit être configuré dans le fichier de configuration global (cas de défense si le serveur de téléchargement n'est plus accessible et que le terminal MiVoice 5300 IP phone est chiffrant).

- **SIP_PORT_PBX_BACKUP** => Spécifie le port utilisé par l'iPBX de backup en mode TLS. Ce port est obligatoirement égal à **5061** en mode TLS
- **SIP_TRANS_PROTO** => Spécifie le protocole de transport utilisé par les terminaux MiVoice 5300 IP phone. Ce paramètre a pour valeur **TLS** (protocole **TLS**).
- **TRUSTED_CERTS** => Spécifie la liste des certificats importés ayant pour extension .pem ou .crt. Dans le cas où on utilise un certificat auto signé par l'IPBX, ce champ doit être vide.
- **TIME_SERVER** => Spécifie l'adresse IP du serveur NTP. Le serveur NTP est obligatoire pour ouvrir une session **TLS**. Le service NTP est relayé par le Mitel 5000 Gateways qui va se synchroniser sur un serveur NTP externe

A partir du MiVoice 5000 Manager, menu **Administration>Téléphonie>Gestion des terminaux**

Note : Dans le cas d'une configuration avec plusieurs multisites, sélectionner la région, le multisite/site isolé puis cliquer sur le bouton Continuer.

- Saisir le login et le mot de passe attribués par l'administrateur
- La fenêtre d'accueil de l'application TMA s'ouvre.
- Effectuer la répartition des paramètres afin que les terminaux MiVoice 5300 IP phone prennent en compte dans leur fichier spécifique les paramètres décrits ci-dessus pour le chiffrement des communications :
  - Menu **Configuration des postes**
  - Sélectionner la gamme de terminal
  - Sélectionner la version à configurer (paquet logiciel poste en production)
  - Modifier la portée et sélectionner les paramètres décrits ci-dessus dans la colonne spécifique
  - Cliquer sur le bouton **Répartir** puis confirmer la répartition effectuée.
- Définir et lancer une action de mise à jour des données spécifiques des terminaux.

Cette action va permettre de configurer les terminaux MiVoice 5300 IP phone pour le chiffrement des communications.

  - Cliquer sur le lien **Modifier les paramètres spécifiques.** Une nouvelle fenêtre s'ouvre
  - Sélectionner la liste **All** (liste définie par défaut contenant tous les terminaux MiVoice 5300 IP phone visibles dans l'inventaire)
  - Cette fenêtre présente également un tableau contenant trois colonnes :
  - La colonne **C** permet, en la cochant, de sélectionner un paramètre spécifique pour lequel la nouvelle valeur saisie sera commune à l'ensemble des terminaux MiVoice 5300 IP phone de la liste sélectionnée précédemment.
  - La colonne **Paramètres** liste les paramètres contenus dans le fichier de configuration des données spécifiques présent dans l'application TMA. Cette liste est issue de la répartition réalisée précédemment.
  - La colonne **Valeurs communes** permet de saisir la nouvelle valeur d'un paramètre spécifique sélectionnée via la colonne **C**.

Note : Des info-bulles permettent d'avoir une aide à la saisie sur la valeur de chacun des paramètres. Celles-ci apparaissent lorsque le curseur de la souris est positionné sur la valeur commune courante du paramètre.

- Dans la colonne **C**, cocher tous les paramètres décrits ci-dessus
- Dans la colonne **Valeurs communes,** saisir les valeurs suivantes à la place des valeurs par défaut :
  - 5061 (Paramètre SIP_PORT_PBX)
  - 5061 (Paramètre SIP_PORT_PBX_BACKUP)
  - TLS (Paramètre SIP_TRANS_PROTO)
  - Effacer la valeur par défaut ca.crt et laisser ce champ vide (Paramètre TRUSTED_CERTS)
  - Saisir l'adresse IP du système de référence (Paramètre TIME_SERVER)
- Cliquer sur le bouton **Enregistrer** puis sur le bouton **Valider**
- Saisir le **Nom de l'action**
- Sélectionner le **Type de mise à jour** :
  - Immédiate
  - Différée : préciser la date au format JJ/MM/AAAA et l'heure au format HHMM.

Note : En cliquant sur l'icône  le calendrier s'ouvre et permet directement de sélectionner la date

- Cliquer sur le bouton **Valider** pour lancer l'action de mise à jour des données spécifiques communes aux terminaux MiVoice 5300 IP phone.

ATTENTION : Une action lancée en mode différé permet de différer le transfert des données vers le serveur de téléchargement externe et l'ordre de mise à jour des données de l'iPBX

- Suite à l'exécution de l'action, lors de la réception du prochain REGISTER émis par un terminal MiVoice 5300 IP phone, celui-ci redémarre automatiquement et ses paramètres sont mis à jour suite au téléchargement de son fichier spécifique, le terminal MiVoice 5300 IP phone chiffre dès lors ses flux de voix et de signalisation

2.5 VERIFICATIONS

2.5.1 CONFIGURATION DU CHIFFREMENT

- Se connecter à chacun des systèmes à partir de l'application MiVoice 5000 Manager (Menu **Actions immédiates>Configuration iPbx)** puis depuis le Web Admin parcourir les menus ci-dessous
- Vérifier qu'il y a un certificat affecté au service SIP.

- Vérifier que la carte EIP présente sur chaque système est en service
  - Se connecter à chacun des systèmes à partir de l'application MiVoice 5000 Manager (Menu **Actions immédiates>Configuration iPbx)** puis depuis le Web Admin parcourir les menus ci-dessous
  - Menu **Service téléphonie>Système>Configuration>Cartes>Carte mère/migration** (2.3.4.2) : la carte EIP doit être à l'état en service

Note : La carte EIP est utilisée pour le chiffrement de la voix lors d'une communication entre un terminal TDM ou un trunk TDM et un terminal IP. La voix est chiffrée entre la carte EIP et le terminal IP.

Note : Par défaut la carte EIP a une adresse allouée automatiquement et sa mise en service est effectuée également automatiquement.

ATTENTION : Cette facilité peut entraîner des conflits d'adresse IP. Il est conseillé de vérifier que l'adresse IP de l'EIP est correcte pour votre plan d'adressage (Menu Service téléphonie>Système>Configuration>Cartes>paramètres des cartes ip).

- Tous les équipements chiffrants doivent raccordés sur un serveur NTP de référence
- Configurer les alarmes relatives à l'expiration éventuelle du certificat

Sur les systèmes sur lesquels le chiffrement a été configuré, les alarmes **AlmLocPers** et **EN ALARME** doivent être configurées pour générer des traps remontant au MiVoice 5000 Manager :

- Menu **Service téléphonie>Système>Configuration>Alarmes>Configuration** individualisée :
- Détection dans .....SITE LOCAL
- Par le groupe .....BLS EXPLOITATION
- "De l'alarme …….....
- Remontée vers .....TRAP SNMP
- Cliquer sur Sélectionner l'élément
- Vérifier que les alarmes AlmLocPers et EN ALARME sont bien transmises

ATTENTION : Un premier trap sera émis à l'expiration du certificat externe ou auto-signé et un deuxième trap sera émis quotidiennement 2 semaines avant l'expiration du certificat externe.

2.5.2 FONCTIONNEMENT DU CHIFFREMENT DES COMMUNICATIONS SUR LES TERMINAUX

- Etablir une communication entre deux terminaux enregistrés sur le même système ou sur deux systèmes distincts
- Vérifier sur la mire du terminal que le pictogramme chiffrement sous la forme d'un cadenas s'affiche correctement
  - o Pour les Mitel 6000 SIP Phone : 
  - o Pour les Mitel 5300 IP Phone : 

Note : Le pictogramme chiffrement affiché par le terminal ne concerne que le flux audio (SRTP) entre lui et son correspondant. Une conférence à trois semblera toujours chiffrée pour les deux correspondants internes alors que le correspond externe aura sa communication voix non chiffrée entre son terminal et la carte EIP du Mitel 5000 Gateways.

Dans le menu **Inventaire,** la colonne **Chiffrement** permet d'indiquer l'état du chiffrement des terminaux de la gamme considérée :

- Poste chiffré en SRTP (et TLS) : 
- Poste chiffré en TLS : 
- Poste non chiffré : Vide
- Information non disponible :  (fichier de configuration non présent ou paramètres de chiffrement non trouvés)

ATTENTION : Cet état est déduit de la lecture des fichiers de configuration présents dans l'application TMA embarquée dans le MiVoice 5000 Manager. Il peut se passer au maximum 1 heure avant que l'état fonctionnel du terminal corresponde à celui configuré dans les fichiers de configuration.

2.5.3 FONCTIONNEMENT DU CHIFFREMENT INTER-SITE

- Se connecter à chacun des systèmes à partir de l'application MiVoice 5000 Manager (Menu **Actions immediates>Configuration iPbx)** puis depuis le Web Admin parcourir les menus ci-dessous

Menu **Service téléphonie>Système>Supervision>Visu des états>Connexions tcp tunnel** : L'état des connexions tcp tunnel doit indiquer **connecté chiffré**.

ATTENTION : Dans le cas où l'état n'est pas correct, il faut s'assurer que tous les systèmes sont bien à la même date et heure.

2.5.4 PRINCIPALES CAUSES D'ERREUR

- CONTROLE ERRONE : Fichier PKCS12 introuvable.
- FONCTION INACTIVE : Fonction chiffrement non déverrouillée.
- ECHEC A LA GENERATION DU CERTIFICAT : Echec à la génération du certificat auto-signé.
- FIN DE VALIDITE DU CERTIFICAT : Certificat PBX périmé, fin de validité.
- FORMAT FICHIER INVALIDE : Certificat PBX inutilisable, adresse IP incorrecte.

2.6 CONFIGURATION DES TERMINAUX MITEL 6000 SIP PHONE EN MODE BOTHWAY

2.6.1 INTRODUCTION

ATTENTION : Les postes de la gamme MiVoice 5300 IP phone ne sont pas compatibles avec le mode Bothway. Ces terminaux ne seront pas fonctionnels dans un système dans lequel ce mode est activé.

Le chiffrement de la signalisation des terminaux Mitel 6000 SIP Phone par le protocole TLS peut être configuré en mode BOTHWAY. Ce mode de fonctionnement doit être activé via le Web Admin à partir d'un paramètre spécifique.

Note : Par défaut, le mode BOTHWAY est désactivé sur une nouvelle installation ou lors d'une mise à jour

ATTENTION : Ce mode de fonctionnement n'est pas compatible avec tous les terminaux SIP, car ceux-ci doivent pouvoir supporter un certificat local. Les terminaux compatibles sont :

- **Mitel 6739i phones,**
- **Mitel 6800 et 6900 SIP Phones.**

Le mode Bothway impose une double authentification pour établir la connexion TLS de la signalisation : Le terminal qui se connecte à l'iPBX authentifie celui-ci, et réciproquement l'iPBX authentifie le terminal.

Lorsque ce paramètre est activé, si un terminal SIP tente d'ouvrir une session TLS sur le port 5061, l'iPBX demande au terminal SIP de lui fournir un certificat. L'iPBX effectue alors une vérification de ce certificat :

- Le certificat doit être daté correctement (date de validité)
- Le certificat doit être correctement signé par l'un des certificats contenus dans le fichier d'autorité de certification téléchargé dans l'iPBX.

Si le terminal ne renvoie pas de certificat, l'ouverture de session TLS est refusée. Si le terminal renvoie un certificat qui n'est pas vérifié OK (par l'autorité de certification), la connexion est refusée. La configuration des certificats du terminal doit être cohérente avec celle de l'iPBX.

Lorsque ce paramètre est activé :

- Le port 5061 est ouvert
- Le port 5060 (UDP/TCP) reste ouvert pour le trunk. Aucun abonné UDP ou TCP ne pourra utiliser ce port

ATTENTION : Les messages arrivant sur le port 5060 vont être filtrés par l'iPBX : ils ne seront traités que s'ils correspondent à un trunk SIP déclaré.

Lorsque ce paramètre n'est pas activé, on conserve les 2 modes de fonctionnement actuels :

- Mode NO TLS : Les certificats sont absents de l'iPBX ; le TLS est désactivé et le port 5061 n'est pas ouvert : les terminaux ne peuvent se connecter à l'iPBX qu'en UDP ou TCP (port 5060 ouvert).
- Mode PBX CERT : Le TLS est activé sous réserve de la présence de certificats dans l'iPBX. Les ports 5060 et 5061 sont ouverts et les terminaux peuvent se connecter à l'iPBX en UDP, TCP ou en TLS trusted ou **auto-signé**.

ATTENTION : Dans le mode BOTHWAY, si les certificats ne sont pas présents dans l'iPBX (cas d'un Noeud non configuré correctement), aucune connexion ne peut se faire.

Après passage du mode PBX CERT au mode BOTHWAY, les éventuels terminaux configurés UDP ou TCP ne pourront plus :

- S'enregistrer
- Emettre un appel
- Recevoir un appel.

Les communications en cours sont conservées, mais la demande de libération de la communication, qu'elle soit initiée par le demandeur ou le demandé, ne sera pas répondue.

2.6.2 CONFIGURATION DU CHIFFREMENT EN MODE BOTHWAY

La procédure décrite dans ce chapitre s'appuie sur l'utilisation de l'application TMA pour configurer les paramètres spécifiques des terminaux Mitel 6000 SIP Phone nécessaires pour le chiffrement des communications en mode Bothway.

Dans ce mode de fonctionnement, les terminaux Mitel 6000 SIP Phone doivent être configurés avec des certificats locaux qui, pour des raisons de sécurité, seront mis en place par le client final.

2.6.2.1 Opérations préalables

- Obtenir auprès de l'organisme compétent les certificats nécessaires au chiffrement des communications en mode BOTHWAY :
  - Le certificat du terminal (fichier avec extension .crt ou .pem)
  - La clé privée associée au certificat du terminal (fichier avec extension .key)

Note : Le certificat et la clé privée peuvent être commun à tous les terminaux ou spécifiques à chaque terminal.

  - Le certificat de l'autorité de certification (racine ou intermédiaire) ayant signé le certificat des terminaux Mitel 6000 SIP Phone (fichier avec extension .crt ou .pem).
  - Le certificat de l'autorité de certification (racine ou intermédiaire) ayant signé le certificat des iPBX MiVoice 5000 (fichier avec extension .crt ou .pem).

Note : En général, ces deux derniers certificats sont identiques.

2.6.2.2 Configuration du mode BOTHWAY

Attendre que tous les terminaux Mitel 6000 SIP Phone soient chiffrants, puis à partir du Web Admin :

- Menu **Service téléphonie>Réseau et liaisons>Qualité de service>Chiffrement et paramètres** IP (4.4.4)
- Cocher la case vérification certificats postes SIP.

ATTENTION : Suite à l'activation du mode BOTHWAY, un redémarrage automatique du service SIP sera effectué.

Suite au redémarrage automatique du service SIP, l'ouverture d'une session TLS par les terminaux Mitel 6000 SIP Phone va s'effectuer en mode BOTHWAY :

Suite à l'échange Client/Serveur Hello, l'iPBX demande au terminal son certificat. Le terminal lui renvoie en même temps que sa clef secrète, son type de chiffrement et le handshake. Le certificat est vérifié par l'iPBX qui termine l'ouverture de session en émettant le type de chiffrement qui sera utilisé et le handshake : la session TLS est établie et le terminal envoie son REGISTER SIP.

Il y a double authentification :

- Le mode Trusted permet au poste d'authentifier le certificat que l'iPBX lui envoie.
- Le mode Bothway qui s'y superpose ajoute ce qui est écrit ici.

2.6.2.3 Méthode sur une maquette de préconfiguration

Il existe une seconde méthode d'installation pour configurer le mode Bothway :

1. Utiliser une maquette de préconfiguration dont le rôle est de charger les certificats sur les 6xxxi
2. Une fois configurés, les postes 6xxxi sont déplacés sur la maquette opérationnelle.

Sur la maquette de préconfiguration :

- L'iPBX de connexion a la même @IP que celle du iPBX de la maquette opérationnelle. Il a également la même PKI.
- Le DHCP doit préciser cette même adresse IP comme celle de l'iPBX de connexion des 6xxxi
- => Sur cette plate-forme de pré-configuration, suivre les étapes décrites dans ce doc, afin de charger les certificats sur les postes => les postes se connectent en banalisé sur le iPBX de connexion de cette plateforme (en utilisant les certificats téléchargés sur le serveur de téléchargement)

Sur la maquette opérationnelle :

- Les iPBX sont configurés en mode Bothway. La même PKI que celle de la plate-forme de pré-configuration est installée
- Les clés/certificats ne sont pas déposés sur le serveur de téléchargement
- Le serveur de téléchargement n'est pas activé (pour plus de sécurité)

=> Les terminaux 6xxxi utilisent leurs propres certificats, stockés en interne, pour se connecter en banalisé sur le iPBX de connexion => login manuel => optimisation de site de login (le tout en TLS Bothway).

2.6.2.4 Configuration des terminaux Mitel 6000 SIP Phone par l'application TMA

Procédure identique à celle décrite au paragraphe 2.4.1.

2.6.2.5 Vérification du fonctionnement

Procédure identique à celle décrite au paragraphe 2.5.2.

2.7 ENVIRONNEMENT DECT

Le chiffrement est disponible également pour les terminaux DECT raccordés à une infrastructure Mitel SIP DECT OMM utilisant les bornes Mitel RFP IP et WLAN (se référer au guide Produit).

Dans cet environnement, les fonctionnalités suivantes sont disponibles :

- Chiffrement de la signalisation entre le Mitel OMM et le MiVoice 5000 (TLS)
- Chiffrement des flux voix par le protocole SRTP (Secured RTP) utilisant l'algorithme AES 128 ou 256 bits avec l'algorithme HMAC pour l'authentification
- Amélioration de la sécurité DECT (implémentation de la technologie CAT-iq dans l'interface air entre les bornes Mitel RFP 35/36/37 IP et 43 WLAN et les terminaux 6x2d/650c):
  - Chiffrement de toutes les connexions (pas seulement la voix) comme les fonctions de consultation annuaire, de consultation du journal d'appels,…
  - Renégociation des clefs de chiffrement durant l'appel.
  - Sécurité accrue vis à vis de l'usager avec un affichage du niveau de sécurité

ATTENTION : Dans une installation mixte comportant des anciennes bornes DECT RFP 32/34 IP et 42 WLAN et des nouvelles bornes Mitel RFP 35/36/37 IP et 43 WLAN, le chiffrement des flux voix par le protocole SRTP ne doit pas être activé. Seules les nouvelles bornes Mitel RFP 35/36/37 IP et 43 WLAN supportent le chiffrement des flux voix par le protocole SRTP.

Note : Se référer au document considéré pour le détail de la configuration du chiffrement à effectuer coté Mitel OMM.

L'utilisation d'un certificat auto-signé ou émanant d'un organisme de certification (certificat trusted) est nécessaire pour établir une session TLS entre le MiVoice 5000 et le Mitel OMM.

ATTENTION : Le réalignement des paramètres systèmes du MiVoice 5000 vers le Mitel OMM n'écrase pas les valeurs des paramètres Proxy port et Registrar port si ceux ont comme valeur 5060 ou 5061. Si ces deux paramètres ont une valeur différente de 5060 ou 5061, alors le réalignement force ces deux paramètres à la valeur 5060.

2.8 ARRET DU CHIFFREMENT DES COMMUNICATIONS

2.8.1 TOUT MODE

La procédure à suivre si on ne souhaite plus chiffrer les communications est la suivante :

- Configurer les terminaux MiVoice 5300 IP phone en mode non chiffrant via l'application TMA embarquée dans le Web Admin ou le MiVoice 5000 Manager.
  - Définir et lancer une action de mise à jour des données spécifiques des terminaux MiVoice 5300 IP phone. Cette action va permettre de configurer les terminaux MiVoice 5300 IP phone en mode UDP

Se référer aux chapitres relatifs aux configurations monosite et multi-site

- Dans la colonne **Valeurs communes,** saisir les valeurs suivantes à la place des valeurs courantes :
  - 5060 (Paramètre SIP_PORT_PBX)
  - 5060 (Paramètre SIP_PORT_PBX_BACKUP)
  - UDP (Paramètre SIP_TRANS_PROTO)
  - Laisser la valeur courante. Ne pas cocher la colonne C. (Paramètre TRUSTED_CERTS)
  - Laisser la valeur courante. Ne pas cocher la colonne C. (Paramètre TIME_SERVER)

ATTENTION : Attendre la fin de la mise à jour de tous terminaux MiVoice 5300 IP phone avant de passer à l'étape suivante.

- Configurer les terminaux Mitel 6000 SIP Phone en mode non chiffrant via l'application TMA embarquée dans le Web Admin ou le MiVoice 5000 Manager.
  - Définir et lancer une action de mise à jour des données spécifiques des terminaux Mitel 6000 SIP Phone. Cette action va permettre de configurer les terminaux Mitel 6000 SIP Phone en mode UDP.

Se référer aux chapitres relatifs aux configurations monosite et multi-site

- Dans la colonne **Valeurs communes,** saisir les valeurs suivantes à la place des valeurs courantes :
  - 5060 (Paramètre sip proxy port)
  - 5060 (Paramètre sip registrar port)
  - 5060 (Paramètre sip backup proxy port)
  - 5060 (Paramètre sip backup registrar port)
  - Laisser la valeur courante. Ne pas cocher la colonne C.(Paramètre time server1)
  - 1 (Paramètre sip transport protocol : protocole UDP)
  - 0 (Paramètre sips persistent tls)
  - Laisser la valeur courante. Ne pas cocher la colonne C.(Paramètre sips tls authentication)
  - Laisser la valeur courante. Ne pas cocher la colonne C.(Paramètre sips trusted certificates)
  - 0 (Paramètre sip srtp mode
  - Laisser la valeur par défaut (champ vide) pour les paramètres sips root and intermediate certificates, sips local certificate et sips private key.

ATTENTION : Attendre la fin de la mise à jour de tous terminaux Mitel 6700 SIP Phone avant de passer à l'étape suivante

- Configurer le ou les systèmes en mode non chiffrant via le Web Admin ou le MiVoice 5000 Manager
  - Menu **Service téléphonie>Réseau et liaisons>Qualité de service>Chiffrement et paramètres IP** (4.4.4)
  - Décocher la case **chiffrement voix**.

2.8.2 MODE BOTHWAY

Pour sortir du chiffrement mode Bothway :

- Première étape = décocher le mode Bothway (la config passe alors en mode Trusted, les postes 6xxxi sont toujours fonctionnels, les certificats étant toujours utilisés en mode Trusted).
- Deuxième étape = réaliser les opérations qui sont décrites ci-dessus sur les 6xxxi (faire pointer les 6xxxi vers le 5060).

Mitel Powering connections | mitel.com

© Copyright 2015, Mitel Networks Corporation. All Rights Reserved. The Mitel word and logo are trademarks of Mitel Networks Corporation. Any reference to third party trademarks are for reference only and Mitel makes no representation of ownership of these marks.