MiVoice 5000 Phones
Call encryption

11/2021

AMT/PTD/PBX/0103/5/7/EN

OPERATING MANUAL

Mitel®

Warning

Although the information contained in this document is considered as pertinent, Mitel Networks Corporation (MITEL ®) cannot guarantee the accuracy thereof.

The information may be changed without notice and should never be interpreted as a commitment on the part of Mitel, its affiliates or subsidiaries.

Mitel, its affiliates and subsidiaries shall not be held liable for any errors or omissions made in this document. This document may be reviewed or re-edited at any time in order to add new information. -

No part of this document may be reproduced or transmitted in any form whatsoever or by any means - electronic or mechanical - regardless of the objective, without the written consent of Mitel Networks Corporation.

Any reference to third-party trademarks is made for information purposes only, and Mitel does not guarantee its ownership.

CONTENTS

1 ABOUT THIS DOCUMENT

1.1 PURPOSE OF THIS DOCUMENT

This document describes, for MiVoice 5000 (release ≥ R7.2), the systems used to implement call encryption on MiVoice 5300 IP Phones and Mitel 6000 SIP Phones.

Call encryption concerns:

- Voice flows
- Signal flows.

1.2 DOCUMENT AUDIENCE

This document is meant for installers and provides them with the following information:

- Principle of call encryption in different network architectures
- Current restrictions and limitations
- Configuring call encryption on MiVoice 5000 Server and Mitel 5000 Gateways (including Mitel EX Controller Mitel GX Gateway)
- Configuring call encryption on terminals
- Deactivating call encryption.

1.3 SCOPE OF THIS DOCUMENT

This manual applies to proprietary MiVoice 5300 IP phones and Mitel 6700/6800/6900 SIP Phones within the scope of the MiVoice 5000 solution (release ≥ R7.2).

1.4 TERMINOLOGY

1.4.1 TERMS AND EXPRESSIONS

Mitel 5000 Gateways	This term refers to all XS, XL and XD systems.
MiVoice 5000 Server/EX Controller	Telephone switching system hosted by a PC running with Linux/CentOS
XS, XL, XD	MiVoice 5000 physical gateways.
LLDP	Link Layer Discovery Protocol (IEEE 802.1AB) is a type of frame that allows network devices (station, switch, router, IP phone) to communicate their identity and function to their environment.
SIP phone	IP phone using SIP (Session Initiation Protocol).

1.4.2 ABBREVIATIONS

CD-ROM:	**C**ompact **D**isk-**R**ead **O**nly **M**emory
DHCP:	**D**ynamic **H**ost **C**onnection **P**rotocol
FTP:	**F**ile **T**ransfert **P**rotocol
LAN:	**L**ocal **A**rea **N**etwork
LLDP:	**L**ink **L**ayer **D**iscovery **P**rotocol
NTP:	**N**etwork **T**ime **P**rotocol
Operating system:	**O**perating **S**ystem
PBX:	**P**rivate **B**ranch e**X**change
PC:	**P**ersonal **C**omputer
RAM:	**R**andom **A**ccess **M**emory
RST:	**R**eset
MMC:	**M**an **M**achine **C**ommand
SIP:	**S**ession **I**nitiation **P**rotocol
TDW:	**T**erminal **D**ownload **S**erver
TFTP:	**T**rivial **F**ile **T**ransfer **P**rotocol
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 REFERENCE DOCUMENTS

See the technical documentation provided on Mitel.com.

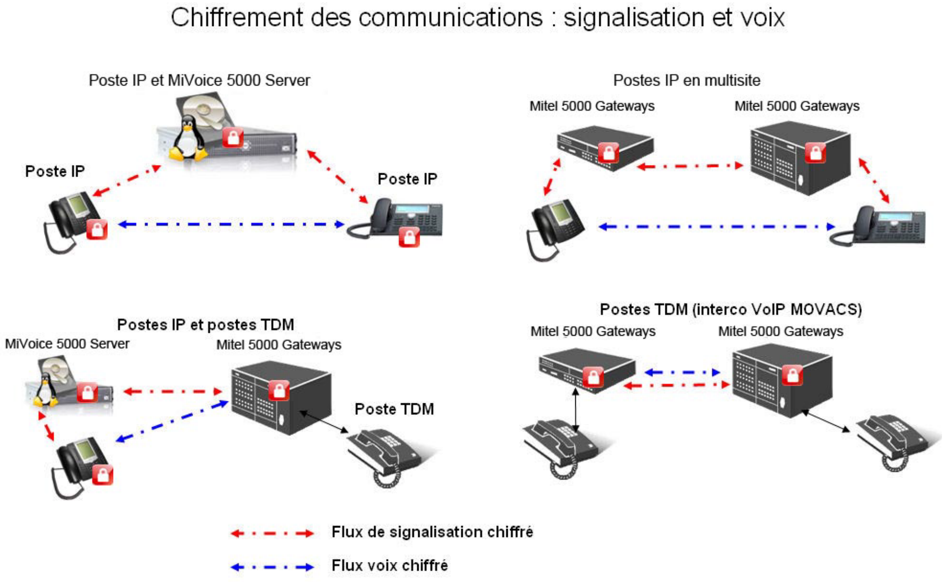
2 CALL ENCRYPTION

2.1 INTRODUCTION

MiVoice 5000 offers full call encryption. Full call encryption concerns voice and signal flows. It is available on MiVoice 5300 IP phones and Mitel 6000 SIP phones.

The call encryption function is used to secure, in an IP network infrastructure, signal and voice over IP flows transmitted between:

- MiVoice 5300 IP phones/Mitel 6000 SIP Phones, voice encryption (SRTP),
- MiVoice 5300 IP phones/Mitel 6000 SIP Phones and a Mitel 5000 Gateways system (EIP card), voice encryption,
- MiVoice 5300 IP phones/Mitel 6000 SIP Phones and a Mitel 5000 Gateways / MiVoice 5000 Server/EX Controller system, signal encryption (TLS),
- Mitel 5000 Gateways/MiVoice 5000 Server/Cluster Server/EX Controller systems on an inter-site link (IP multi-site), encrypted signalling (TLS),
- TDM terminals (analogue, digital - MiVoice 5300 Digital phone, 675x Digital, DECT and S0), via Mitel 5000 Gateways systems on an inter-site or inter-node link, voice encryption between the two EIP cards (communication between the EIP card and the TDM station is not encrypted),
- A TDM terminal (analogue, digital terminals - MiVoice 5300 Digital phone, 675x Digital, DECT and S0) or a TDM trunk and a MiVoice 5300 IP phone/Mitel 6000 SIP Phone via Mitel 5000 Gateways systems, voice encryption between the EIP card and MiVoice 5300 IP phone/Mitel 6000 SIP Phone.
- And more generally between two terminals or applications supporting encryption.



Encryption is available on:

- MiVoice 5300 IP phones
- Mitel 6700, 6800 and 6900 SIP phones
- TDM terminals (analogue, digital - MiVoice 5300 Digital phone, 675x Digital, DECT and S0), via X Series gateways and with EIP cards
- TDM trunk, via X Series Mitel Gateways and with EIP card
- DECT terminals connected to a Mitel SIP DECT infrastructure
- Analogue terminals and analogue or T0/T2 trunks connected to Mitel EX Controller
- Analogue terminals connected to Mitel GX Gateways and Mitel TA 71xx
- And more generally, all SIP phones compatible with encryption.

2.1.1 ENCRYPTION METHODS AND PRINCIPLES

The encryption available in MiVoice 5000 is based on the following protocols:

- Voice encryption via SRTP (Secured RTP) using the 128-bit AES algorithm or 256-bit AES algorithm (as of 7.2 and depending on terminal capacity), with the HMAC for authentication
- Signal encryption through TLS protocol

Signal encryption is based on:

- Inter-site links (especially between a cluster server and a remote site)
- Links between the cluster server and nodes (intra-cluster links)
- Signal encryption for communications with MiVoice 5300 IP phone and Mitel 6000 SIP Phone.

The TLS protocol is used carry out this encryption.

Two encryption modes are proposed by MiVoice 5000 Manager:

- Encryption through a self-signed certificate
- Encryption through an external certificate

In MiVoice 5000 Manager, encryption is a multi-site-based configuration parameter, but the administrator may or may not allow site-by-site encryption.

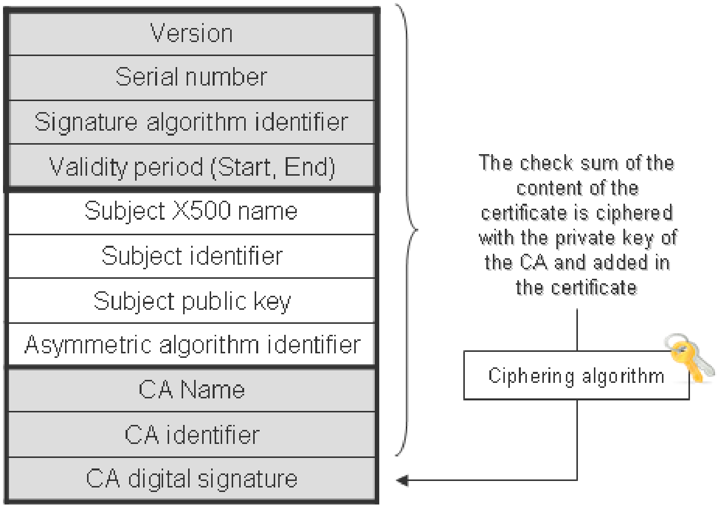
ATTENTION : In case of encryption inside the cluster, the nodes adopt the properties of the cluster server. If encryption is activated on the cluster server from MiVoice 5000 Manager, it is then implicitly activated on the nodes.

ATTENTION : Encryption works between two systems (cluster server and remote site) only if it is activated on the systems concerned.

2.1.2 REMINDER CONCERNING CERTIFICATES

Some theories:

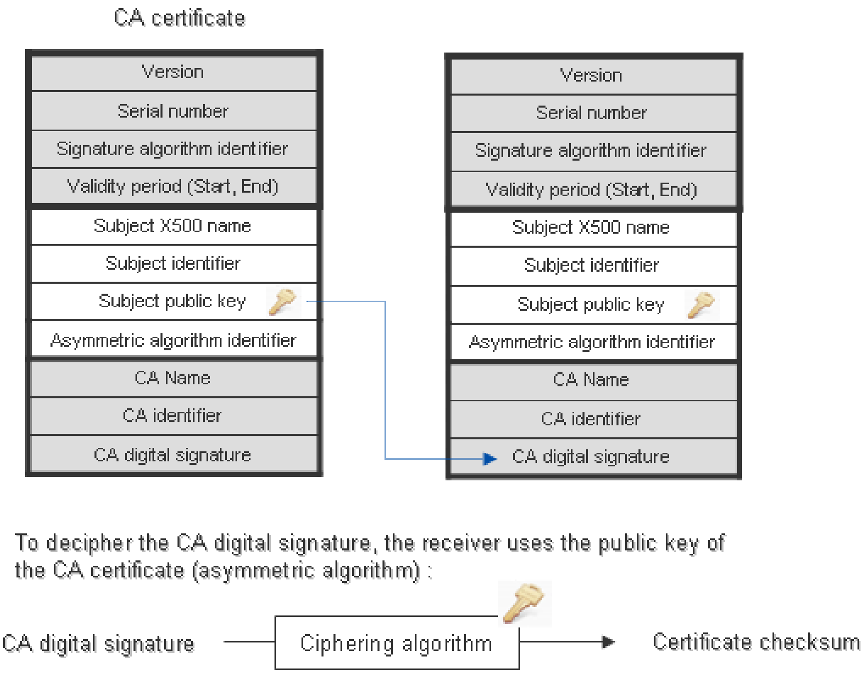
The TLS protocol secures data exchanges between different parties. It is based on a public key infrastructure (PKI) which implements an asymmetric encryption through the use of public and private keys. These keys are derived from certificates issued by a CA (Certification Authority).


Version
Serial number
Signature algorithm identifier
Validity period (Start, End)
Subject X500 name
Subject identifier
Subject public key
Asymmetric algorithm identifier
CA Name
CA identifier
CA digital signature
The check sum of the content of the certificate is ciphered with the private key of the CA and added in the certificate
Ciphering algorithm

Example of certificate

The certificate contains three sections:

- The first section identifies the certificate.
- The second section identifies the entity sending the certificate (that is the certificate processor).
- The third section identifies the certification authority (CA). This CA must be known (or approved) by the certificate recipient: the public key associated with the CA is used by the recipient to decipher the signature of the certificate owner.



To decipher the CA digital signature, the receiver uses the public key of the CA certificate (asymmetric algorithm) :

The following attributes are used to validate a certificate received:

- *Validity period*: period during which the certificate can be used
- *Subject identifier*: for identifying the certificate owner (example: IP address)
- *Subject Public Key*: public key used to encrypt the TLS session key
- *Algorithm used to encrypt the signature*: the same algorithm is used to decrypt the signature.

The TLS protocol will, therefore, allow the parties to be authenticated, and the data encrypted using the certificates; when the TLS session is initialised, the certificates are exchanged in order to authenticate the parties and negotiate the encryption protocols to use.

Reminders on the protocols used in the certificates:

- RSA is an encryption algorithm used in **public key cryptography. It is used to generate a private key and public key which are in turn used in TLS session set-up dialogue.**
- SHA is a hashing function which allows the creation of a certificate fingerprint called certificate signature.

There are 2 types of certificates:

- Self-signed certificates used by the iPbx/CS
- Trusted certificates issued by an external or private certification authority (CA).

A trusted certificate is imported with the help of a file in PKCS#12 format, which is password-protected. This password must also be entered. The file PKCS#12 must contain:

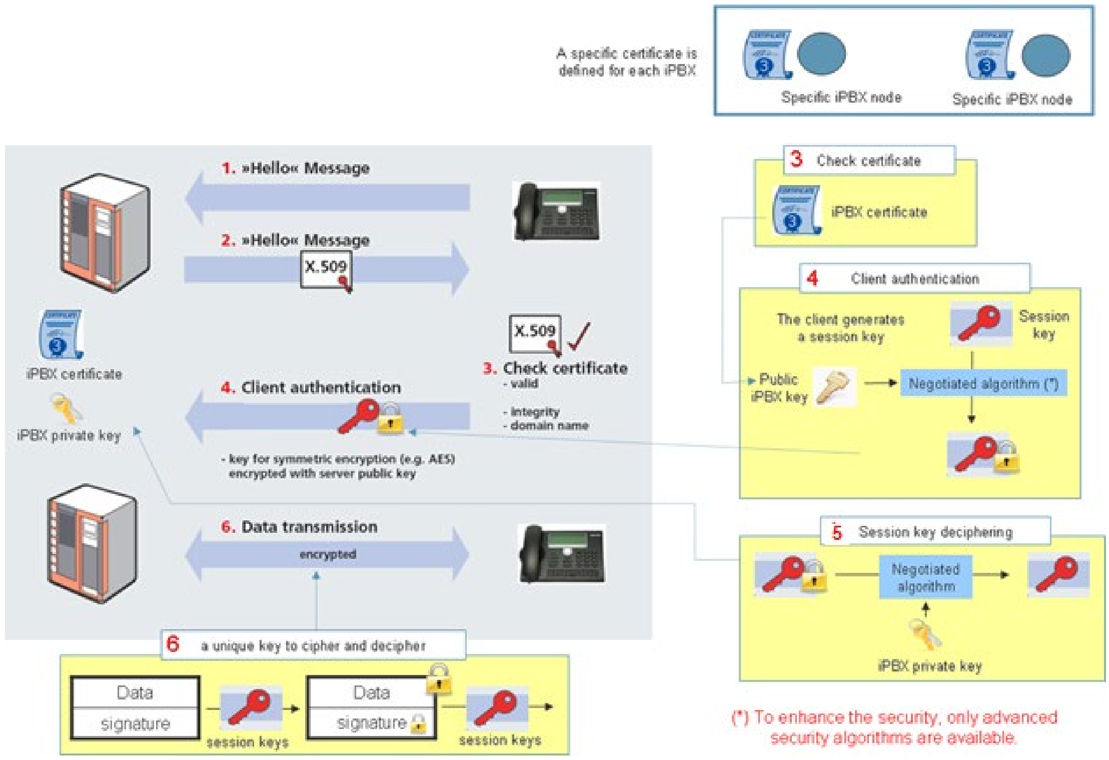
- The different certificates from the certification authority (CA)
- The private key of this certificate.

Note: Signal encryption is required for voice encryption to be effective.

TLS is activated on terminals by TMA (Terminal Management Application – see the section on. § deployment).

Use of self-signed certificates

The various exchanges are illustrated below:



iPBX / terminal signal encryption, with the use of self-signed certificates

The procedures are as follows:

- The terminal opens the TLS session and sends a TLS message, such as HELLO.
- The iPBX/Call Server in return sends its self-signed certificate to the terminal.
- The terminal makes a simple check (integrity, validity of the certificate, domain name).
- The session keys are generated according to the encryption algorithms negotiated between the iPBX and the terminal (during the HELLO session).

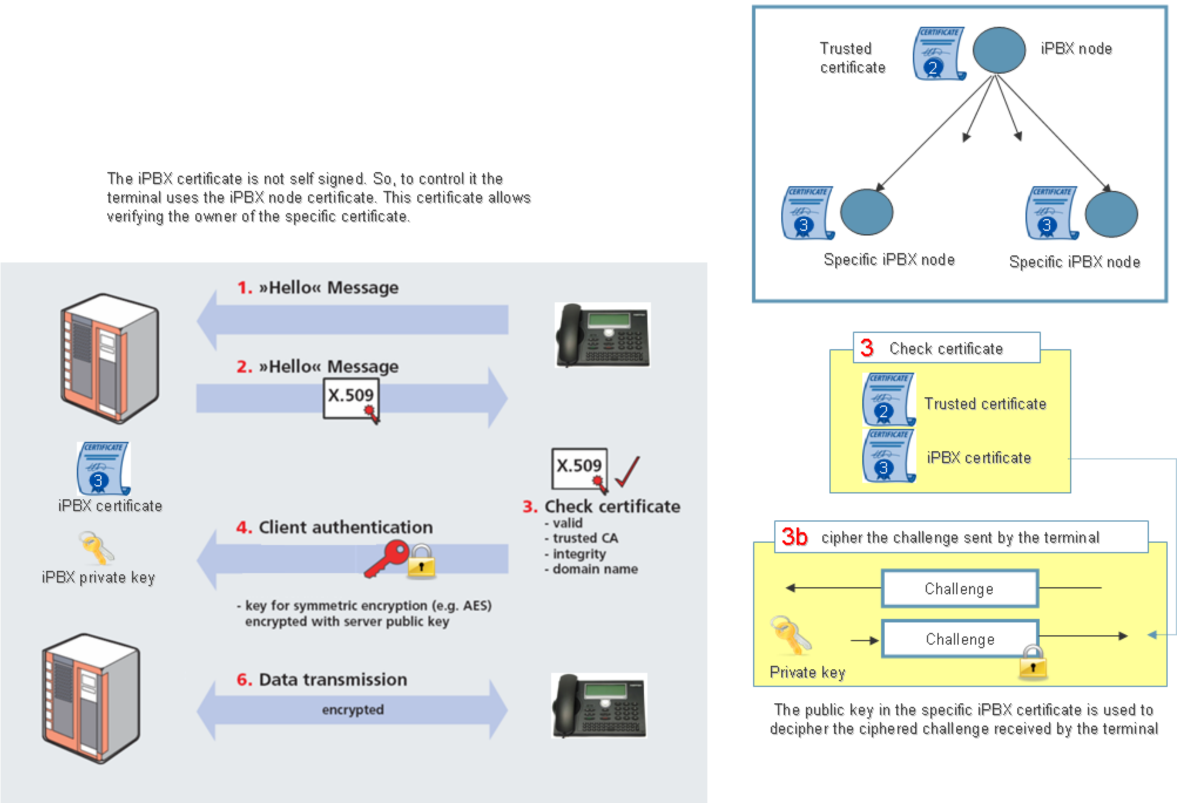
This solution simplifies the management of certificates as well as the deployment and maintenance of the solution. **However, it does not allow the authentication of the entity sending the certificate** (the iPBX/CS) and under certain circumstances cannot prevent *man-in-the-middle* attacks.

Use of trusted certificates

The terminal may use a trusted certificate to authenticate the iPBX/Call Server and check the certificate issued by this latter.

It can also send a challenge to the iPBX/CS, to check that the iPBX/CS actually has the private key associated with this certificate.

This method is used to avoid man-in-the-middle attacks. However, it requires a bit more resources to implement and maintain it. The certificate issued by the iPBX/CS is itself designed and issued by the external CA.



The iPBX certificate is not self signed. So, to control it the terminal uses the iPBX node certificate. This certificate allows verifying the owner of the specific certificate.

The public key in the specific iPBX certificate is used to decipher the ciphered challenge received by the terminal

iPBX / terminal signal encryption, with the use of trusted certificates

Mutual TLS (MTLS)

The Mutual TLS (MTLS) protocol refers to two parties authenticating at the same time: a default authentication mode in some protocols (IKE, SSH) and optional in others (TLS).

This protocol offers greater security because it allows both terminals to check each other’s identity.

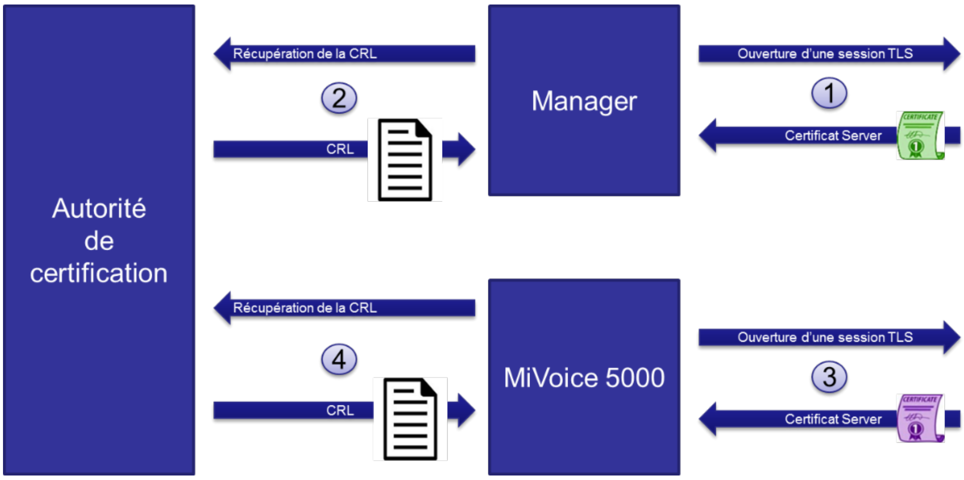
By default, the TLS protocol only proves the identity of the server to the client using the X.509 certificate, while client authentication to the server is left to the application layer. TLS also offers client-server authentication using X.509 authentication on the client’s side.

Mutual TLS authentication (MTLS) is much more common in business-to-business applications, where a limited number of programmatic and homogeneous clients connect to specific web services, the operational load is limited, and the security requirements are generally much higher than in user environments.

Using trusted certificates with CRL

With R7.0, MiVoice 5000 security has been reinforced by allowing the implementation of Trusted certificate validity check using the CRL (Certificate Revocation List) method. This CRL contains a list of certificates revoked by the authority.

When a client connects in TLS mode from MiVoice 5000 or from MiVoice 5000 Manager, the validity of the certificate is checked according to the following principle:



If the certificate is present in the CRL, trust in this X.509 certificate is broken and connection is not set up. Moreover, periodic audits allow connections whose certificate is revoked to be cut.

Note: Only "trusted" certificates can be revoked and allow the authenticity of the server/terminal to be checked.

2.1.3 CONTENT OF THE CERTIFICATES

2.1.3.1 Rules

The content of a certificate must reflect and contain the information used by all the configuration items (clients, machines and terminals).

Depending on the type of connection to the server, the following information is required in the constitution of the certificate:

- For a connection to the server by IP address, the certificate must contain the IP address,
- For a connection to the server via the FQDN, the certificate must contain the FQDN,
- For a connection to the server by either of them, the certificate must contain the IP address and the FQDN.

Special case of SIP service

The IP address must be indicated in the certificate.

If 53xxIP phones are used, the IP address must be in the CN (Common Name).

Multi-site configuration

For a multi-site configuration, the IP address can be in the CN or alternate names.

The IP address is not necessary for an FQDN configuration.

If the Extended Key Usage field is set, it must contain Client and Server for multi-site (two-factor authentication).

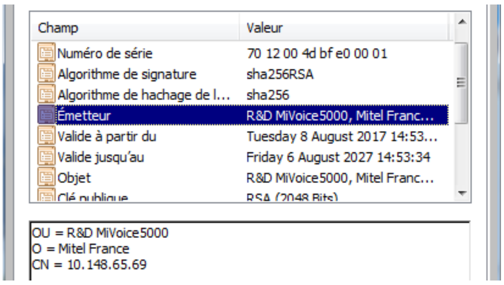
2.1.3.2 Fields to be completed in the certificates

The self-signed SHA2 or SHA1 certificate is generated by the PBX. It is not possible to import a self-signed certificate.

Main fields to be filled in:

- **Common name**: PBX IP address (TEL in case of network separation)
- **Alternative names**: all the IP addresses that give access to the PBX (ADMIN and TEL) and all the FQDNs associated with the TEL and ADMIN interfaces
- **Validity dates**
- **X509v3 Extended Key Usage**: TLS Web Server Authentication and TLS Web Client Authentication

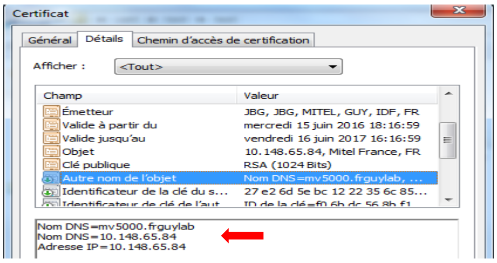
Example for an iPBX accessible via the address 10.148.65.69 (no FQDN):



Champ	Valeur
Numéro de série	70 12 00 4d bf e0 00 01
Algorithme de signature	sha256RSA
Algorithme de hachage de l...	sha256
Émetteur	R&D MiVoice5000, Mitel Franc...
Valide à partir du	Tuesday 8 August 2017 14:53...
Valide jusqu'au	Friday 6 August 2027 14:53:34
Objet	R&D MiVoice5000, Mitel Franc...
Clé publique	RSA (2048 Bits)

OU = R&D MiVoice5000
O = Mitel France
CN = 10.148.65.69

Example with FQDN for **alternative name** fields



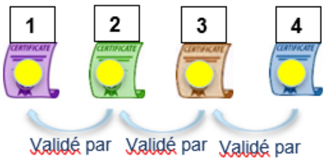
Champ	Valeur
Émetteur	JBG, JBG, MITEL, GUY, IDF, FR
Valide à partir du	mercredi 15 juin 2016 18:16:59
Valide jusqu'au	vendredi 16 juin 2017 16:16:59
Objet	10.148.65.84, Mitel France, FR
Clé publique	RSA (1024 Bits)
Autre nom de l'objet	Nom DNS=mv5000.frguylab, ...
Identificateur de la clé du s...	27 e2 6d 5e bc 12 22 35 6c 85...
Identificateur de clé de l'aut	ID de la clé=f0 6b dc 56 8b f1

```
Nom DNS=mv5000.frguylab
Nom DNS=10.148.65.84
Adresse IP=10.148.65.84
```

In this case the **CN** field is always configured with the TEL IP address (e.g.: CN=10.148.65.84).

For a certification chain, intermediate certificates are not associated with a particular server and are therefore not associated with an IP address or FQDN.

In the example below, this is the case for Certificates 1, 2 and 3:



They must contain the attribute **X509v3 Basic Constraints**, set to **CA:TRUE**. This attribute indicates that the certificate is capable of signing a certificate.

If the attribute **X509v3 Key Usage** is set, it must also contain the permission to sign a certificate, i.e. the value **Key Cert Sign**.

The **CA:TRUE** and **Key Cert Sign** options are not set for the server certificate (Certificate 4 in the example) as it does not have this capability. The server certificate is the last certificate in the certificate branch.

The server certificate format is similar to the self-signed certificate and therefore contains the following fields:

- **Common name**: PBX IP address (TEL in case of network separation)
- **Alternative names**: all the IP addresses that give access to the PBX (ADMIN and TEL) and all the FQDNs associated with the TEL and ADMIN interfaces
- **Validity dates** (be careful not to install a certificate that is not yet valid)
- **X509v3 Extended Key Usage**: "TLS Web Server Authentication" and "TLS Web Client Authentication".

2.1.4 TWO WAY ENCRYPTION

Signal encryption through TLS protocol may be set to BOTHWAY mode. This new operating mode must be activated via Web Admin from a new parameter (see the section concerned).

Note : By default, BOTHWAY mode is disabled on a new installation or during an update.

When this new parameter is enabled, if an SIP terminal tries to open a TLS session on Port 5061, the iPBX prompts the SIP terminal to provide a certificate. The iPBX then checks this certificate:

- The date of the certificate must be correct (validity date).
- The certificate must be correctly signed by any of the certificates contained in the certification authority file downloaded into the iPBX.

ATTENTION : This parameter is not managed by MiVoice 5000 Manager. The iPBX set to BOTHWAY mode no longer accepts terminals logging on in UDP or TCP mode.

ATTENTION : This mode of operation is only compatible with IP phones that can contain a certificate.

The procedures for configuring call encryption in BOTHWAY mode are described in detail in the relevant chapter.

2.1.5 ENCRYPTION RIGHT AND LICENCE

To configure call encryption with terminals, it is necessary to ensure that:

- The system on which the terminal is declared is locked for encryption. A **licence** authorises the encryption.
- The subscription to which the terminal is connected has **an encryption right**.
- Voice encryption is enabled on the system on which terminal is declared (**voice encryption** parameter).
- Inter-site encryption must be enabled on the system on which the terminal is declared if the correspondent is on another system or if a Cluster architecture is used. The same thing obtains for the remote device (**inter-iPBX encryption** parameter).
- The IP terminal must have voice-encryption capacity. This requires configuring the terminal.
- Signalling between the system and the terminal must be encrypting.
- A certificate from a certification authority (trusted certificate) is installed on each Mitel 5000 Gateways or MiVoice 5000 Server system (each system has its own certificate and a common certification authority for all the systems).
- If a trusted certificate is used on the Mitel 5000 Gateways or MiVoice 5000 Server systems, a certificate from the same certification authority is installed on all the terminals (all the terminals use the same certification authority).

For terminals set to encryption mode, signals will always be encrypted while voice will be encrypted according to Web Admin settings (**voice encryption, inter-site encryption, encryption right, licence)**.

A certificate has a limited validity period.

A self-signed certificate is valid for 1 year. It is renewed automatically.

A trusted certificate has a validity period indicated by the certification authority, in general several years. The administrator is notified about the expiration of the certificate 14 days prior to the end of validity, then every day until the actual expiration date. When the certificate expires, calls are still possible but voice is no longer encrypted.

Note : The certificate for the Mitel 5000 Gateways or MiVoice 5000 Server system is unique and generated by the certification authority, with its IP address as commonName parameter.

2.1.6 CONFERENCE ENCRYPTION

The conference function can be encrypted on MiVoice 5000 Server. In this case, all the terminals associated with one or more MiVoice 5000 Server conference bridges must themselves be encrypting.

Conference encryption on MiVoice 5000 Server only concerns the following conference master terminals registered on MiVoice 5000 Server:

- MiVoice 5300 IP phone
- Virtual TDM (via EIP and encrypting multi-site link)

Note : Conference master Mitel 6000 SIP Phones manage the conference function themselves, regardless of whether or not they are encrypted (no resources taken on the MEDIA SERVER of MiVoice 5000 Server).

The two participants in the encrypted MiVoice 5000 Server conference initiated by a conference master MiVoice 5300 IP phone or virtual TDM may be:

- Some encrypting terminals registered on MiVoice 5000 Server, including Mitel EX Controller: MiVoice 5300 IP phone; Mitel 6000 SIP Phone, Virtual TDM
- Some terminals registered on a Mitel 5000 Gateways system:
  - Encrypting MiVoice 5300 IP phone and Mitel 6000 SIP Phone.
  - TDM terminals, analogue terminals, TDM DECT, accessible via EIP and encrypting multi-site link
- Remote terminals, accessible via an ISDN or analogue LR access declared on a Mitel 5000 Gateways system accessible via EIP and the encrypting multi-site link.

ATTENTION : If a non-encrypting participant is added to one or more encrypting conference bridges already in communication, all the conference bridge participants return to non-encrypting mode.

ATTENTION : The intrusion sets up a conference which will never be encrypted.

ATTENTION : In listening/intervention mode, the configuration must be imposed in such a way that the three terminals have the same configuration (either they are all encrypted or unencrypted).

2.1.7 RESTRICTIONS AND LIMITATIONS

It is not possible to have an encrypted call between a MiVoice 5300 IP phone/Mitel 6000 SIP Phone and a terminal i7xx.

2.2 CONFIGURING CALL ENCRYPTION ON A CONFIGURATION WITH MIVOICE 5000 MANAGER

In a multi-site configuration with a self-signed certificate:

Encrypting terminals do not need any certificate because they do not check the system to which they are connected.

Each Mitel 5000 Gateway or MiVoice 5000 Server has its own certificate based on its IP address.

In a multi-site configuration with a trusted certificate:

Encrypting MiVoice 5300 IP phones/Mitel 6000 SIP Phones must have a certificate.

Each Mitel 5000 Gateway or MiVoice 5000 Server has its own certificate. All the certificates are signed by the same authority.

The procedure described in this chapter is based on the use of the MiVoice 5000 Manager's TMA application to define the specific parameters of the SIP terminals needed for call encryption.

ATTENTION : Other methods (manual terminal configuration through web interface, terminal interface or manual configuration file management) are not recommended.

2.2.1 PREREQUISITES

- The multi-site network must be correctly configured and working.
- The EIP card must be available and installed on each site of the multi-site network (Mitel 5000 Gateways).
- MiVoice 5000 Manager must be installed and correctly configured to manage the multi-site network.
- External DHCP and FTP servers must be configured correctly.
- NTP server: All the sites must be configured on the same NTP server.
- The terminal service is not started on each site.

Note : It is possible to use the integrated download server in a Mitel 5000 Gateways system.

For **trusted-certificates-based** encryption:

- Obtain the relevant certificates from the competent authority.

2.2.2 CONFIGURING CALL ENCRYPTION ON EACH MITEL 5000 GATEWAY OR MIVOICE 5000 SERVER

- Check that the encryption licence is activated on each system:
  - Connect to each system from the MiVoice 5000 Manager application (Menu **Immediate actions>iPBX configuration)** then from Web Admin browse through the menus below
  - Menu **Telephony service>System>Info>Licences** (2.1.3).
  - The status of the encryption licence must be **Authorised**.
  - If not, enter the new licence authorising encryption in the **Keycode** field.
- Check that the feature classes used by the telephone subscriptions on which terminals are registered have the right to use the encryption function:
  - From the MiVoice 5000 Manager application, go to Menu **Technical characteristics>Feature classes**.

- For each feature class used, check that the parameter **Right to encryption** is ticked.

ATTENTION : A MiVoice 5300 IP phone/Mitel 6000 SIP Phone set as encrypting but whose subscription does not give an encryption right will have its signals encrypted but not its voice.

- Implementing the voice encryption function:
  - Connect to each system from the MiVoice 5000 Manager application (Menu **Immediate actions>iPBX configuration)** then from Web Admin browse through the menus below
  - Menu **Telephony service>Network and links>Quality of service>Encryption and IP parameters** (4.4.4).
  - Tick the **Voice encryption** checkbox.
- Implement the signal encryption function and activate the self-signed certificate on all the multi-site systems:
  - On MiVoice 5000 Manager, Menu **Administration**>**Network topology**
  - Select the **multi-site** network on which certificate-based encryption must be configured then click **Configuration**.
  - Tick **Encryption** to authorise encryption on the multi-site network.
  - Select **Encryption type**:

Self-signed certificates

- Click **Apply** and then **OK**: this enables the **Generate Certificates** button.
  - Click **Generate certificates**.
  - To the question asked, select **Generate certificates for all the sites on the multi-sites** then click **Confirm**.
  - In the MiVoice 5000 Manager operations log, a message is used to check the success of the certificate generation operation.
  - Select the **multi-site** on which encryption through external certificate must be configured then click **Configuration**.
  - Tick **encryption** to authorise encryption on the multi-site network.
  - Set Encryption type to **Self-signed**.
- Click **Apply** and then **OK**: this enables the **Generate Certificates** button.
  - Click **Certificate generation**.
  - To the question asked, select **Generate certificates for all the sites on the multi-sites** then click **Confirm**.
  - In the MiVoice 5000 Manager operations log, a message is used to check the success of the certificate generation operation.

Note : MiVoice 5000 Manager sends the certificate generation command to the systems defined in MiVoice 5000 Manager (Cluster Server, nodes and remote sites), and the certificate is generated locally on each system.

Note : Signal encryption through self-signed certificate is then operational on all the multi-site systems.

Trusted certificate

- Set Encryption type to **Import**.
- Select the external certificate to be imported.
- Enter and confirm the password associated with the certificate.

- Click **Import** to import the certificate into MiVoice 5000 Manager.
- Click **Apply** and then **OK**: this enables the **Generate Certificates** button.
- Click **Generate certificates**.
- To the question asked, select **Generate certificates for all the sites on the multi-sites** then click **Confirm**.
- In the MiVoice 5000 Manager operations log, a message is used to check the success of the certificate generation operation.

Note : MiVoice 5000 Manager generates system certificates (cluster server, nodes and remote sites) and private keys from the information contained in the external certificate and sends them to each system.

Note : Encryption through external certificate is then operational on all the multi-site systems.

When the certificate is activated, the certificate's new validity start and end date is automatically updated.

ATTENTION : The SIP service restarts automatically after the certificate is installed.

2.3 CONFIGURING CALL ENCRYPTION ON A CONFIGURATION WITHOUT MIVOICE 5000 MANAGER

In a configuration with a self-signed certificate:

In a single-site configuration with a self-signed certificate, "encrypting" MiVoice 5300 IP phones/Mitel 6000 SIP Phones do not need any certificate because they do not check the system to which they are connected.

Each Mitel 5000 Gateway or MiVoice 5000 Server has its own certificate based on its IP address.

In a configuration with a trusted certificate:

In a single-site configuration with a trusted certificate, all "encrypting" MiVoice 5300 IP phones/Mitel 6000 SIP Phones have certificates issued by the same authority. Mitel 5000 Gateways or MiVoice 5000 Server have their own certificate. All the certificates are signed by the same authority.

The procedure described in this chapter is based on the use of the TMA integrated into Mitel 5000 Gateways to define the specific parameters of MiVoice 5300 IP phones/Mitel 6000 SIP Phones required for call encryption.

ATTENTION : Other methods (manual terminal configuration through web interface, terminal interface or manual configuration file management) are not recommended.

2.3.1 PRELIMINARY OPERATIONS

- Check that the TMA and FTP services (required for 53xxIP terminals) are started.
  - Menu **Telephony service>System>Configuration>Services (2.3.1)**
  - Terminal service: **START**
- If necessary, configure the integrated DHCP service.

ATTENTION : Do not configure the SIP_PORT_PBX parameter in the DHCP server in case of call encryption. It must be configured in the global configuration file (case of defence if the downloading server is no longer accessible and MiVoice 5300 IP phone is encrypting).

2.3.2 CONFIGURING CALL ENCRYPTION ON MITEL 5000 GATEWAY OR MIVOICE 5000 SERVER

- Check that the encryption licence is activated:
  - Menu **Telephony service>System>Info>Licences** (2.1.3).
  - The status of the encryption licence must be **Authorised**.
  - If not, enter the new licence authorising encryption in the Keycode field.
- Check that the telephone subscriptions on which MiVoice 5300 IP phones/Mitel 6000 SIP Phones are registered are allowed to use the encryption function:
  - **Menu Telephony service >Subscribers>Subscriptions>Characteristics** (1.2.3)
  - For each subscription, check that the parameter **Right to encryption** is ticked.

Note : By default, all the subscriptions have the "Right to encryption".

Note : The encryption right may equally be associated with a feature class via Menu Telephony service>Subscribers>Rights>Feature classes (1.4.3).

ATTENTION : An encrypting terminal whose subscription does not give it the right to encryption will have encrypted signals but unencrypted voice.

- Enable voice encryption and configure the type from Menu **Telephony service>Network and links>Quality of service>IP encryption and parameters** (4.3.4).

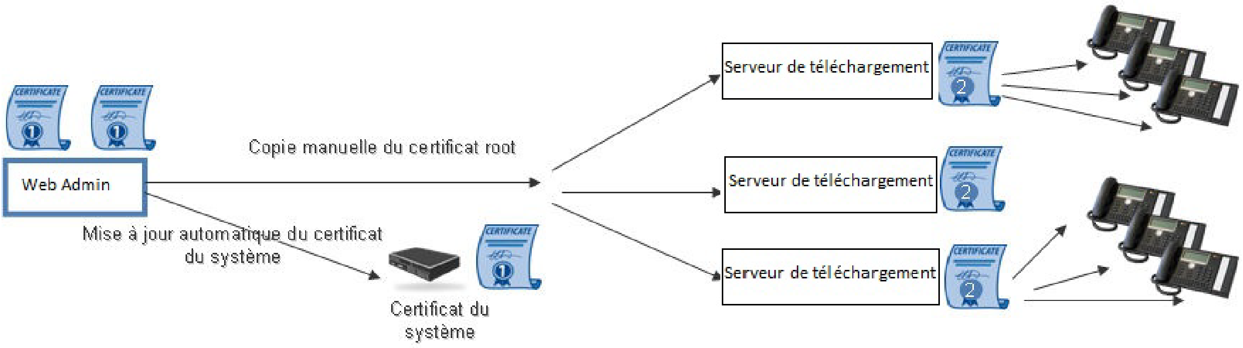
Refer to the MiVoice 5000 Server and Mitel Gateways User manual, section IP encryption and parameters.

ATTENTION : The SIP service will restart automatically if the certificate regeneration button is used.

2.4 CONFIGURATION BY TMA

2.4.1 COPY OF THE CA CERTIFICATE USED BY THE TERMINALS IN THE DOWNLOAD SERVER

If a certificate from an external certification authority is used for terminals, the CA certificate must be copied manually to the download server used by the terminals so it can be downloaded by these latter.


Web Admin
Copie manuelle du certificat root
Mise à jour automatique du certificat du système
Certificat du système
Serveur de téléchargement
Serveur de téléchargement
Serveur de téléchargement
CERTIFICATE
1
2

Note : If there is no authority file, download it from Menu Telephony Service>System>Security>Certificate management (2.4.1) (pem format).

Recommended method

From MiVoice 5000 Manager, Menu **Administration>Telephony>Terminal management**.

Note : For a configuration with several multi-site architectures select the region, multi-site/standalone site then click Continue.

- Enter the login and password assigned by the administrator.
- The TMA welcome window opens:
  - Click Menu **Deployment**.
  - Select the range **(**Mitel 6000 SIP Phone or MiVoice 5300 IP phone).
  - From the **List of servers**, select the download server to which the certificate must be downloaded.
  - In the **Other file** field, click **Browse** to import the ca.crt certificate to be downloaded.
  - Click **Validate**.
  - Enter the **Action name**.
  - Select **the type of update**: immediate or deferred.
  - Click **Validate**.
  - In **Action monitoring** check that the file is correctly downloaded individually to the download server.

ATTENTION : A download server must be selected. Only one file is authorised per provisioning operation. This file is not backed up in the directories of the TMA application integrated into MiVoice 5000 Manager.

ATTENTION : Some file name checks are made:

- **If configuration file encryption is activated, TMA does not allow *.cfg files to be sent to the download server as they will not be taken into account.**

2.4.2 CONFIGURING MITEL 6000 SIP PHONES

The parameters to define on MiVoice 6000 SIP phones are:

- **sip proxy port** => Specifies the port used by the iPBX's SIP access point. This port must be equal to **5061** in TLS mode.
- **sip registrar port** => Specifies the port used by the iPBX's SIP access point. This port must be equal to **5061** in TLS mode.
- **sip backup proxy port** => Specifies the port used by the backup iPBX's SIP access point. This port must be equal to **5061** in TLS mode.
- **sip backup registrar port** => Specifies the port used by the backup iPBX's SIP access point. This port must be equal to **5061** in TLS mode.
- **sip transport protocol** => Specifies the transport protocol used by Mitel 6700 SIP Phones. The value for this parameter is either **4** (TLS **protocol**), or 1 (UDP protocol), or 2 (TCP protocol). The value for this parameter must be **4.**
- **sips persistent tls** => Value used to validate (**1**) or not (0) the use of persistent TLS mode. In persistent TLS mode, only the Trusted Certificate file must be defined. The value for this parameter must be **1.**
- **sips persist tls keep alive** => This parameter is used to define the value of TLS keep alive (this allows the terminal, in particular, to automatically restore its persistent TLS session if it is disconnected, and to switch over, if necessary, to the backup site if the TLS session to the main site is disconnected). The default value of this parameter is **30 seconds**.
- **sips tls authentication** => Indicates whether to use a self-signed certificate from the iPBX (**0**) or a certificate from an external certification authority (**1**).
- **sips trusted certificates** => Parameter to be set to self-signed, trusted or BOTHWAY. Specifies the certification authority that signed the MiVoice 5000 iPBX certificate (file with the extension .crt or .pem). If a self-signed certificate from the iPBX is used, this field must be left empty.
- **sip srtp mode** => Indicates whether SRTP calls are forbidden (0) , preferred (**1**) or whether the SRTP calls alone are accepted/generated (2). The value for this parameter must be **1**.
- **srtp aes256 key** => Enable or disable SRTP AES 256. Recommended value 1
- **time server1** => Specifies the IP address or hostname of an NTP server. The NTP server is required to open a **TLS** session.
- **sips symmetric tls signalling** => This parameter is used to specify whether Port 5061 is used systematically (**1**) or whether a random port value is used (0) (in this case, a new port is assigned each time the terminal restarts). Recommended value: **0**
- **sips root and intermediate certificates** => Parameter to be defined in BOTHWAY mode only. Specifies the certification authority that signed the Mitel 6000 SIP Phone terminal certificate (file with the extension .crt or .pem). Generally, the content of this parameter is the same as the parameter **sips trusted certificates**.
- **sips local certificate** = Parameter to be defined in BOTHWAY mode only. Specifies the Mitel 6000 SIP Phone certificate (file with extension .crt or .pem).
- **sips private key** => Parameter to be defined in BOTHWAY mode only. Key associated with the Mitel 6000 SIP Phone certificate (file with extension .crt or .pem).

Note : The sip local tls port parameter specifies the port used by the Mitel 6700 SIP Phone to send its SIP messages in TLS mode. This port must be 5061 in TLS mode and is set to this value by default in the global configuration file;

From MiVoice 5000 Manager, Menu **Administration>Telephony>Terminal management**:

Note : For a configuration with several multi-site architectures, a new window opens, select the region, multi-site/isolated site then click Continue;

- Enter the login and password assigned by the administrator, the TMA welcome window opens.
- Assign the parameters so Mitel 6000 SIP Phones take into account in their specific file the parameters described above for call encryption.
  - Menu Terminal configuration
  - Select Mitel 6000 SIP Phones.
  - Select the release to configure (production terminal software package).

A distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones:

- Encryption: encryption parameters for Mitel 6000 SIP Phones
- Config: the usual configuration parameters
- TimeZone: date and time, NTP server, time zone configuration parameters
- Network: network parameters (DHCP, VLAN, LLDP,etc.)
- RFC2833: RFC2833 / SIP INFO configuration parameters
- 802.1X: 802.1X configuration parameters
- RTCP: RTCP configuration parameters
- Expert: all the other parameters not available in the previous tabs

Note : To facilitate the introduction of certain features (encryption, etc.), some parameters are available twice in the tab:

- **in the upper part, the parameters have a range and some fixed values.**
- **In the lower part, the same parameters have a default value which may differ and a range set to ignored.**

- Select the **Encryption** tab then set, for the following parameters available in this tab, their range to **Specifc**:
  - sip proxy port
  - sip registrar port
  - sip backup proxy port
  - sip backup registrar port
  - sips symmetric tls signalling
  - sip transport protocol
  - sips persistent tls
  - sips trusted certificates
  - sips tls authentication
  - sip srtp mode
- Click the **Distribute** button then confirm the distribution made.

ATTENTION : The parameter time server1 is located in the TimeZone tab with a default global range. When manual global data update is started, this parameter must be set with the IP address of the reference system.

- Define and start an update operation for the specific data of Mitel 6000 SIP Phones. This action configures Mitel 6000 SIP Phones for call encryption.
- Click the link **Modify specific parameters**. A new window opens:

- This indicates the criteria concerned by specific data update:
- The **Region**, **Multi-site** and **Terminal range** concerned: **Mitel 6000 SIP Phone**
- The **terminal model** concerned: **all models**.
- The terminal **software** concerned
- Select the **All** list (list defined by default, containing all the **Mitel 6000 SIP Phones** visible in the inventory).

Note : The "All" list is defined by default and contains all the terminals known in the inventory. In R5.3 and later, logged and unlogged terminals are visible in the inventory and are managed by the TMA integrated into MiVoice 5000 Manager.

Note : The greyed out values represent the canonical values of each parameter.

As of R6.1 SP1, a distribution of the parameters in form of tabs is only displayed for Mitel 6000 SIP Phones:

- **Encryption**: encryption parameters for Mitel 6000 SIP Phones
- **Config**: the usual configuration parameters
- **TimeZone**: date and time, NTP server, time zone configuration parameters
- **Network**: network parameters (DHCP, VLAN, LLDP,...)
- **RFC2833**: RFC2833 / SIP INFO configuration parameters
- **802.1X**: 802.1X configuration parameters
- **RTCP**: RTCP configuration parameters
- **Expert**: all the other parameters not available in the previous tabs

This window also presents a table containing three columns:

- When ticked, the **C** column is used to select a specific parameter for which the new value entered will be the same for all Mitel 6000 SIP Phones on the previously selected list.
- The **Parameters** column lists the parameters contained in the specific data configuration file available in TMA. This list is from the distribution made previously.
- The **Common values** column is used to enter the new value of a specific parameter selected via the **C** column.

Note : Pop-ups give information on how to enter the value of each of the parameters. These latter appear when the cursor is placed over the current common value of the parameter.

- Check the default values of the parameters.

Note : The default values of the parameters are defined in such a way that Mitel 6000 SIP Phones are encrypted in self-signed mode.

- Click **Save** then **Confirm**.
- Enter the **Action name**.
- Select the **Type of update**:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

Note :

Clicking the 📅 icon opens the calendar so the date can be selected directly.

- Click **Confirm** to start updating the common specific data of all Mitel 6000 SIP Phones.

ATTENTION : Any action started in deferred mode defers the transfer of data to the external download server and the iPBX data update order.

After the action is executed, when the next REGISTER issued by a Mitel 6000 SIP Phone is received, this latter restarts automatically and its parameters are updated after its specific file is downloaded: the Mitel 6000 SIP Phone then encrypts its voice and signal flows.

2.4.3 CONFIGURING MIVOICE 5300 IP PHONES

The parameters to be define on MiVoice 5300 IP phones are:

- **SIP_PORT_PBX** => Specifies the port used by the iPBX in TLS mode. This port must be equal to **5061** in TLS mode.

ATTENTION : Do not configure the SIP_PORT_PBX parameter in the DHCP server in case of call encryption. It must be configured in the global configuration file (case of defence if the downloading server is no longer accessible and MiVoice 5300 IP phone is encrypting).

- **SIP_PORT_PBX_BACKUP** => Specifies the port used by the backup iPBX in TLS mode. This port must be equal to **5061** in TLS mode.
- **SIP_TRANS_PROTO**=> Specifies the transport protocol used by MiVoice 5300 IP phones. The value for this parameter is **TLS** (**TLS** protocol).
- **TRUSTED_CERTS** => Gives the list of imported certificates with the extension .pem or .crt. If a certificate self-signed by the iPBX is used, this field must be blank.
- **TIME_SERVER** => Specifies the NTP server IP address. The NTP server is required to open a **TLS** session. The NTP service is relayed by Mitel 5000 Gateways which synchronises on an external NTP server.

From MiVoice 5000 Manager, Menu **Administration>Telephony>Terminal management**:

Note : For a configuration with several multi-site architectures select the region, multi-site/standalone site then click Continue.

- Enter the login and password assigned by the administrator.
- The TMA welcome window opens.
- Assign the parameters so MiVoice 5300 IP phones take into account in their specific file the parameters described above for call encryption:
  - Menu **Terminal configuration**
  - Select terminal range.
  - Select the release to configure (production terminal software package).
  - Modify the range and select the parameters described above in the specific column.
  - Click the **Distribute** button then confirm the distribution made.
- Define and start updating the specific data of the terminals.

This action configures MiVoice 5300 IP phones for call encryption:

- Click the link **Modify specific parameters**. A new window opens.
- Select the **All** list (list defined by default, containing all the MiVoice 5300 IP phones visible in the inventory).
- This window also displays a table containing three columns:
- When ticked, the **C** column is used to select a specific parameter for which the new value entered will be the same for all MiVoice 5300 IP phones on the previously selected list.

  - The **Parameters** column lists the parameters contained in the specific data configuration file available in TMA. This list is from the distribution made previously.
  - The **Common values** column is used to enter the new value of a specific parameter selected via the **C** column.

Note : Pop-ups give information on how to enter the value of each of the parameters. These latter appear when the cursor is placed over the current common value of the parameter.

- In the **C** column, tick all the parameters described above.
- In the **Common values** column, enter the following values instead of the default values:
  - 5061 (Parameter SIP_PORT_PBX)
  - 5061 (Parameter SIP_PORT_PBX_BACKUP)
  - TLS (parameter SIP_TRANS_PROTO)
  - Delete the default value ca.crt and leave this field empty (Parameter TRUSTED_CERTS).
  - Enter the reference system IP address (Parameter TIME_SERVER).
- Click **Save** then **Confirm**.
- Enter the **Action name**.
- Select the **Type of update**:
  - Immediate
  - Deferred: specify the date in DD/MM/YYYY format and time in HHMM format.

Note :

Clicking the 📅 icon opens the calendar so the date can be selected directly.

- Click **Confirm** to start updating the common specific data of all MiVoice 5300 IP phones.

ATTENTION : Any action started in deferred mode defers the transfer of data to the external download server and the iPBX data update order.

- After the action is taken, when the next REGISTER issued by a Mitel 5300 SIP Phone is received, this latter restarts automatically and its parameters are updated after its specific file is downloaded: the MiVoice 5300 IP phone then encrypts its voice and signal flows.

2.5 CHECKING THE WORKING OF CALL ENCRYPTION ON THE TERMINALS

- Set up a call between two terminals registered on the same system or on two distinct systems.
- Check on the terminal screen that the encryption pictogram in form of a lock is correctly displayed.
  - For Mitel 6000 SIP phones: 🔒
  - For Mitel 5300 SIP phones: 🔑

Note : The encryption icon displayed by the terminal only concerns the audio flow (SRTP) between it and its correspondent. A three-way conference will always seem to be encrypted for the two internal correspondents while the external correspondent's voice communication will not be encrypted between his terminal and the EIP card of Mitel 5000 Gateways.

In the **Inventory** menu, the **Encryption** column indicates the encryption status of the terminals range concerned:

- Encrypted terminal in SRTP (and TLS): 🔒SRTP
- Encrypted terminal in TLS: 🔒
- Terminal not encrypted: Empty
- Information not available: ? (configuration file not present or encryption parameters not found)

ATTENTION : This status is deduced from the reading of the configuration files available in the TMA application integrated into MiVoice 5000 Manager. It may take maximum one hour for the functional status of the terminal to correspond to the one defined in the configuration files.

2.5.1 CHECKING INTER-SITE ENCRYPTION

- Connect to each system from the MiVoice 5000 Manager application (Menu **Immediate actions>iPBX configuration)** then from Web Admin browse through the menus below

Menu **Telephony service>System >Supervision>Status display>Connections of tcp tunnel**: the tcp tunnel connection status must show **"connected encrypted"**.

ATTENTION : If the status is not correct, check that all the systems actually have the same date and time.

2.6 SETTING MITEL 6000 SIP PHONES TO BOTHWAY MODE

2.6.1 INTRODUCTION

ATTENTION : MiVoice 5300 IP phones are not compatible with Bothway mode. These terminals will not work in a system in which this mode is activated.

Signal encryption for Mitel 6000 SIP Phones through the TLS protocol may be set to BOTHWAY mode. This new operating mode must be activated via Web Admin from a specific parameter.

Note : By default, BOTHWAY mode is disabled on a new installation or during an update.

ATTENTION : This operating mode is not compatible with all the SIP terminals as they must support a local certificate. Compatible terminals are:

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

Bothway mode imposes double authentication to set up signalling TLS connection: the terminal logging on to the iPBX authenticates this latter, and the iPBX authenticates the terminal.

When this new parameter is enabled, if an SIP terminal tries to open a TLS session on Port 5061, the iPBX prompts the SIP terminal to provide a certificate. The iPBX then checks this certificate:

- The date of the certificate must be correct (validity date).
- The certificate must be correctly signed by any of the certificates contained in the certification authority file downloaded into the iPBX.

If the terminal does not send any certificate, a TLS session cannot be opened. If the terminal sends a certificate which has not been certified as OK (by the certification authority) the connection is rejected. The terminal certificate configuration must be consistent with that of the iPBX.

When this parameter is enabled:

- Port 5061 is opened.
- Port 5060 (UDP/TCP) remains open for the trunk. No UDP or TCP trunk can use this port.

ATTENTION : Messages arriving on Port 5060 will be filtered by the iPBX: they will only be processed if they correspond to a declared SIP trunk.

When this parameter is not activated, the current two operating modes are retained:

- NO TLS mode: Certificates are not available in the iPBX; TLS is disabled and Port 5061 is not open: terminals can only connect to the iPBX via UDP or TCP (Port 5060 open).
- PBX CERT mode: TLS is activated if certificates are available in the iPBX. Ports 5060 and 5061 are open, and the terminals can log on to the iPBX in UDP, TCP, trusted TLS or **self-signed** mode.

ATTENTION : In BOTHWAY mode, if the certificates are not available in the iPBX (case of a wrongly configured node), no connection can be set up.

After changing from PBX CERT mode to BOTHWAY mode, any terminal set to UDP or TCP will no longer be able to:

- register
- make a call

- receive a call.

Ongoing calls are kept, but call release requests, no matter the origin (caller or called party), shall not be responded to.

2.6.2 CONFIGURING BOTHWAY ENCRYPTION

The procedure described in this chapter is based on the use of the TMA integrated into Mitel 5000 Gateways to define the specific parameters of Mitel 6000 SIP Phone required for call encryption in Bothway mode.

In this operating mode, Mitel 6000 SIP Phones must be configured with some local certificates which, for security reasons, will be put in place by the end-customer.

2.6.2.1 Preliminary operations

- Obtain from the relevant authority the certificates needed for call encryption in BOTHWAY mode:
  - o the terminal certificate (file with extension .crt or .pem),
  - o the private key associated with the terminal certificate (file with .key extension).

Note : The certificate and private key may be the same for all the terminals or specific to each terminal.

- o The certificate from the (root or intermediary) certification authority that signed the Mitel 6000 SIP Phone terminal certificate (file with the extension .crt or .pem)
- o The certificate from the (root or intermediary) certification authority that signed the MiVoice 5000 iPBX certificate (file with the extension .crt or .pem).

Note : In general, these last two certificates are identical.

2.6.2.2 Configuring BOTHWAY mode

Wait for all Mitel 6000 SIP Phones to be encrypting, then from Web Admin:

- Menu **Telephony service>Network and links>Quality of service>Encryption and IP parameters** (4.4.4).
- Tick the SIP terminal certificate verification box.

ATTENTION : The SIP service restarts automatically after BOTHWAY mode is activated.

After the SIP service has restarted automatically, a TLS session is opened by Mitel 6000 SIP Phones in BOTHWAY mode:

The iPBX prompts the terminal for its certificate after the client/server have exchanged Hello. The terminal sends its secret key, encryption type and handshake at the same time. The certificate is checked by the iPBX which completes the session opening operation by issuing the type of encryption which will be used and the handshake: the TLS session is set up and the terminal sends its REGISTER SIP.

There is double authentication:

- Trusted mode allows the terminal to authenticate the certificate sent to it by the iPBX.
- Bothway mode, which superimposes itself on it, is written here.

2.6.2.3 Method on a pre-configuration mock-up

There is a second installation method for configuring Bothway mode:

1. Use a preconfiguration mock-up the role of which is to load the certificates on 6xxxi.
2. Once configured, the terminals 6xxxi are moved to the working mock-up.

On the pre-configuration mock-up:

- the login iPBX has the same IP address as the iPBX of the working mock-up. It also has the same PKI.
- The DHCP must specify this same IP address as that of the 6xxxi login iPBX.
- => On this pre-configuration platform, follow the procedures described in this document in order to load the certificates on the terminals.
  => The terminals log on in general-purpose mode to the login iPBX of this platform (using the certificates downloaded on the download server).

On the working mock-up:

- The iPBXs are configured in Bothway mode. The same PKI as the one on the pre-configuration platform is installed.
- The keys/certificates are not stored on the download server.
- The download server is not activated (for more security).

=> Terminals 6xxxi use their own certificates, stored internally, to log on in general-purpose mode to the login iPBX => manual login => login site optimisation (all in Bothway TLS).

2.6.2.4 *Configuring Mitel 6000 SIP Phones via TMA*

The procedure is the same as the one described in Section 2.4.1.

2.6.2.5 *Checking the operating principle*

The procedure is the same as the one described in Section 2.5.

2.7 DECT ENVIRONMENT

Encryption is also available for DECT terminals connected to a Mitel SIP DECT OMM infrastructure using Mitel RFP IP and WLAN base stations (refer to the Product Guide).

In this environment, the following features are available:

- Signal encryption between Mitel OMM and MiVoice 5000 (TLS)
- Voice encryption via SRTP (Secured RTP) using the 128 or 256 bits AES algorithm, with the HMAC algorithm for authentication.
- Better DECT security (implementation of the CAT-iq technology in the air interface between Mitel RFPs 35/36/37 IP, 43 WLAN and terminals 6x2d/650c):
  - o Encryption of all connections (not only voice) such as the directory and call log consultation functions, etc.
  - o Renegotiation of encryption keys during a call.
  - o Reinforced user security with a display of security level

ATTENTION : In a mixed installation containing old DECT RFPs 32/34 IP and 42 WLAN as well as new Mitel RFPs 35/36/37 IP and 43 WLAN, voice encryption through SRTP should not be activated. Only Mitel RFPs 35/36/37 IP and 43 WLAN support voice encryption through SRTP.

Note : See the document in question for more information on how to configure encryption on the Mitel OMM side.

The use of a self-signed certificate or a certificate from a certification authority (trusted certificate) is necessary to set up a TLS session between MiVoice 5000 and Mitel OMM.

ATTENTION : Realigning the MiVoice 5000 system settings to the Mitel OMM does not overwrite the values of the Proxy port and Registrar port settings if they are set to 5060 or 5061. If these two parameters have a value other than 5060 or 5061, then the realignment forces these two parameters to the value 5060.

2.8 STOPPING CALL ENCRYPTION

2.8.1 ANY MODE

If you no longer wish to encrypt your calls, proceed as follows:

- Configure MiVoice 5300 IP phones in non-encrypting mode via the TMA integrated into Web Admin or MiVoice 5000 Manager.
  - Define and start an update operation for the specific data of MiVoice 5300 IP phone. This action allows you to set MiVoice 5300 IP phones to UDP mode.

See the chapters on single-site and multi-site configurations.

- In the **Common values** column, enter the following values instead of the current values:
  - 5060 (Parameter SIP_PORT_PBX)
  - 5060 (Parameter SIP_PORT_PBX_BACKUP)
  - UDP (parameter SIP_TRANS_PROTO)
  - Leave the current value. Do not tick column C (Parameter TRUSTED_CERTS).
  - Leave the current value. Do not tick column C (Parameter TIME_SERVER).

ATTENTION : Wait for all the MiVoice 5300 IP phone to be updated before taking the next step.

- Configure Mitel 6000 SIP Phones in non-encrypting mode via the TMA integrated into Web Admin or MiVoice 5000 Manager.
  - Define and start an update operation for the specific data of Mitel 6000 SIP Phones. This action allows you to set Mitel 6000 SIP Phones to UDP mode.

See the chapters on single-site and multi-site configurations.

- In the **Common values** column, enter the following values instead of the current values:
  - 5060 (Parameter sip proxy port)
  - 5060 (Parameter sip registrar port)
  - 5060 (Parameter sip backup proxy port)
  - 5060 (Parameter sip backup registrar port)
  - Leave the current value. Do not tick column C (Parameter time server1).
  - 1 (Parameter sip transport protocol: UDP protocol).
  - 0 (Parameter sips persistent tls)
  - Leave the current value. Do not tick column C (Parameter sips tls authentication).
  - Leave the current value. Do not tick column C (Parameter sips trusted certificates).
  - 0 (Parameter sip srtp mode).
  - Leave the default value (empty field) for the parameters sips root and intermediate certificates, sips local certificate and sips private key.

ATTENTION : Wait for all the Mitel 6700 SIP Phones to be updated before taking the next step.

- Configure the system(s) in non-encrypting mode via Web Admin or MiVoice 5000 Manager

- Menu **Telephony service>Network and links>Quality of service>Encryption and IP parameters** (4.4.4).
- Untick the **Voice+ encryption** checkbox.

2.8.2 BOTHWAY MODE

To leave Bothway mode encryption:

- Step 1 = untick Bothway mode (the configuration then changes to Trusted mode, terminals 6xxxi are still working; the certificates are still used in Trusted mode).
- Step 2 = perform the operations described above on terminals 6xxxi (point the terminals 6xxxi to 5060).