

# Modules de sécurité Alcatel-Lucent

## Server Security Module (SSM), Media Security Module (MSM)



Les modules de sécurité Alcatel-Lucent sécurisent les communications professionnelles sur le réseau d'entreprise. Les communications sont chiffrées et l'intégrité des logiciels et des protocoles utilisés sont contrôlés. Les modules utilisent

une technologie conçue par Thales®, acteur majeur du marché de la sécurité. Sécuriser les communications d'entreprise favorise la continuité d'activité.

Les modules de sécurité sont des serveurs montés sur châssis. Ils protègent les communications professionnelles contre les attaques de déni, de service et de vol d'information. Le Server Security Module (SSM) protège le serveur de communication, les téléphones IP, les Media Gateways et les faisceaux SIP. Le Media Security Module (MSM) protège les serveurs d'application offrant enregistrement des communications, messagerie et conférences.

Fonctions clés	Avantages
Les téléphones IP et les Media Gateways téléchargent des binaires et des fichiers de configuration sécurisés. Chiffrement de la signalisation d'appel et du flux média	Protection des données : prévention contre les attaques d'usurpation de téléphones IP et les écoutes clandestines de communications Conformité aux politiques d'entreprises et aux réglementations concernant la confidentialité
Authentification mutuelle de l'intégralité des équipements et de la signalisation d'appel ( pas de modification des messages)	Continuité d'activité : protège les communications professionnelles contre les attaques par déni de service
Intégration directe avec le serveur de communication OmniPCX Enterprise	Rentabilité : mise en place de processus de sécurité de haute qualité sans aucun impact sur la gestion du système téléphonique.
Aucun impact sur les paramètres de qualité de service (QoS) et la configuration du réseau	Simplicité : pas d'impact sur l'infrastructure réseau
Redondance géographique	Continuité d'activité : fournit une protection des communications professionnelles en cas de défaillance du réseau, du serveur ou du centre de données

Thales est l'un des leaders européens de la sécurité et se positionne comme intégrateur de systèmes à forte valeur ajoutée, équipementier et fournisseur de services. Les solutions de Thales sécurisent les 4 espaces identifiés comme vitaux dans notre société moderne : l'État ou un ensemble d'États, la ville, les infrastructures critiques et le cyberspace.

**THALES**

S'appuyant notamment sur ses compétences fortes en cryptographie, Thales est l'un des leaders mondiaux des produits et solutions de cybersécurité pour les infrastructures critiques gouvernementales et militaires, les réseaux de satellites, les entreprises industrielles et financières. Présent sur l'ensemble de la chaîne de la sécurité, Thales propose une gamme complète de solutions et de services depuis le conseil en sécurité, les tests d'intrusion et le design des architectures, jusqu'à l'homologation de système, le développement de produits et services ainsi que leur gestion tout au long de leur durée de vie, et la supervision de la sécurité (Security Operation Centers en France et au Royaume-Uni).

## Spécifications techniques

### Spécifications physiques

#### Dimensions

- Appareils 1U montés sur châssis de 482 mm (19")
  - Largeur : 371 mm (14,6")
  - Profondeur : 215 mm (8,5")
  - Hauteur : 43,6 mm (1,7")
- Poids : 2,5 kg (5,5 lb) (accessoires inclus)

#### Alimentation

- Tension en entrée 110/220 V AC
  - 50/60 Hz
  - 40 W

#### Environnement d'exploitation

- 5°C à 45°C
- Hygrométrie : 5 % à 95 %

#### Environnement de stockage

- 25°C à 55°C
- Hygrométrie : 5 % à 95 %

#### MTBF

- À terre, installation fixe, 25 °C : 88 000 heures

#### Interfaces réseau

- Console : port 1 RJ-45 (RS232C)
- Ports réseau :
  - Côté clair : 4 ports commutés Gigabit Ethernet RJ-45
  - Côté crypté : 1 port Gigabit Ethernet RJ-45

## Sécurité

### Chiffrement

- AES-CBC 128 bits, AES-CM 128 bits
- Signalisation :
  - Téléphones IP, Media Gateways et serveur de communication passif (PCS), serveurs d'application : IPSEC transport mode
  - Faisceaux SIP publics : TLS

- Voix : SRTP

- IPV4 et IPV6

### Authentification mutuelle et contrôle d'intégrité

- AES-XCBC (128 bits), HMAC-SHA1 (160 bits)
- Certificats X.509 (RSA 2048 bits)

### Gestion

- Mise à jour centralisée et sécurisée des logiciels :
  - SSM
  - MSM
  - Téléphones IP
  - Media Gateways
- Centre de personnalisation de clés

### Qualité de service

- Préserve le marquage 802.1p/q
- Gère le marquage de qualité de service niveau 3

### Protection par SSM

- Serveurs de communication (CS) :
  - OmniPCX Enterprise CS version 11.1 ou ultérieure
  - Redondance du serveur OmniPCX Enterprise CS
  - Réseaux ABC entre OmniPCX Enterprise CS
  - Alcatel-Lucent OpenTouch® Business Edition version 2.1 ou ultérieure
- Media Gateways :
  - Sécurité intégrée
  - Cartes GD3, GA3, INTIP3
- Téléphones IP :
  - Sécurité intégrée
  - Alcatel-Lucent Premium DeskPhones 8018, 8028, 8038, 8068, 8028S, 8058S, 8068S, 8078S
  - Téléphones Alcatel-Lucent IP Touch® 4028, 4038, 4068

### Protection par MSM

- OmniPCX Enterprise PCS
- Media Gateways : cartes migrées sans sécurité intégrée
- Serveurs d'application :
  - OpenTouch Multimedia Services
  - OpenTouch Message Center
  - 4645 Voice Messaging Services
  - OmniPCX RECORD Suite
  - Enregistreurs externes utilisant le protocole IP DR-Link

### Réglementations

- CE mark
- ETL mark
- FCC part 15 B
- ICES 003
- ROHS

## Fonctions de la plateforme

	SSM	MSM
Téléphones IP par SSM (max)	15 000	-
Media Gateways par SSM (max)	240	-
Communications chiffrées simultanées par MSM pour la protection de PCS ou de serveurs d'application (max)	-	400
Flux d'enregistrements chiffrés simultanés par MSM pour la protection d'enregistreurs IP DR-Link (max)	-	800