Alcatel-Lucent Security Modules

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

The Alcatel-Lucent Security Modules provide business continuity and information protection for Voice over IP business communications by offering software and protocol integrity protection as well as encrypted communications. The security architecture is based on technology from Thales® – a leading player in the security market.

The Security Modules are rack-mounted appliances that protect IP-based business communications against denial of service and information theft attacks. A Server Security Module (SSM) protects business communications between Alcatel-Lucent Communication Servers and IP phones, IP media gateways and SIP trunks. Media Security Modules (MSM) protect communications with application servers that handle IP media flows such as recording, messaging or conferencing servers.

Features	Benefits
Secure downloading of binary and configuration files in IP Phones and IP Media Gateways. Call control signaling and media encryption	Data protection: Prevent malicious attacks, IP phone spoofing and communications eavesdropping Compliance: Ensure enterprise complies with internal and external governance and privacy regulations
Mutual authentication of all equipment and integrity of call control signaling (ensuring that messages have not been modified)	Business continuity: Protect business communications from denial of service attacks
Seamless integration with the OmniPCX® Enterprise Communication Server	Cost-effective operations: Implement high-grade security processes without impacting the manageability of the phone system
Zero impact on Quality of Service (QoS) settings and network configuration	Simplicity: Does no impact the network infrastructure
Geographic redundancy support	Business continuity: Provide secure business communications in case of network, server or datacenter failures

THALES

As a value-added systems integrator, equipment supplier and service provider, Thales is one of Europe's leading players in the security market. The Thales security teams work with government agencies, local authorities and enterprise customers to develop and deploy integrated, resilient solutions to protect citizens, sensitive data and critical infrastructure.

Drawing on its strong cryptographic capabilities, Thales is one of the world leaders in cyber security products and solutions for critical state and military infrastructures, and satellite networks, as well as industrial and financial companies. With a presence throughout the entire security chain, Thales offers a comprehensive range of services and solutions from security consulting, intrusion detection and architecture design to system certification, development and through-life management of products and services, and security supervision with Security Operation Centers in France and the United Kingdom.

Alcatel·Lucent Enterprise

Technical specifications

Physical specifications

Dimensions

- Rack-mounted 482 mm (19 in), 1U appliances
  - ¬ Width: 371 mm (14.6 in)
  - ¬ Depth: 215 mm (8.5 in)
  - ¬ Height: 43.6 mm (1.7 in)
- Weight: 2.5 kg (5.5 lb) (including accessories)

Power supply

- 110/220 V AC input voltage
  - ¬ 50/60 Hz
  - ¬ 40 W

Operating environment

- -5°C to +45°C
- 5% to 95% relative humidity

Storage environment

- -25°C to +55°C
- 5% to 95% relative humidity

MTBF

- Ground fixed 25°C : 88,000 hours

Network interfaces

- Console: 1 RJ-45 (RS232C) port
- Network ports:
  - ¬ Clear side: 4 RJ-45 Gigabit Ethernet switched ports
  - ¬ Encrypted side: 1 RJ-45 Gigabit Ethernet port

Security

Encryption

- AES-CBC 128 bits, AES-CM 128 bits
- Signaling:
  - ¬ IP Phones, Alcatel-Lucent OmniPCX Enterprise media gateways and Passive Communication Server (PCS), application servers: IPSEC transport mode
  - ¬ Public SIP trunks: TLS
- Voice: SRTP
- IPV4 and IPV6

Mutual authentication and integrity control

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

Management

- Centralized secured software update:
  - ¬ SSM
  - ¬ MSM
  - ¬ IP Phones
  - ¬ Media gateways
- Key customization center

QoS

- Preserves 802.1p/q tags
- Manages QoS Layer 3 tags

Protection by SSM

- Communication Servers (CS):
  - ¬ OmniPCX Enterprise CS release 11.1 and above
  - ¬ OmniPCX Enterprise CS server redundancy
  - ¬ OmniPCX Enterprise CS ABC networks
  - ¬ Alcatel-Lucent OpenTouch® Business Edition 2.1 and above
- Media Gateways:
  - ¬ Built-in security
  - ¬ GD3, GA3, INTIP3 boards
- IP phones:
  - ¬ Built-in security
  - ¬ Alcatel-Lucent 8018, 8028, 8038, 8068, 8028S, 8058S, 8068S, 8078S Premium DeskPhones
  - ¬ Alcatel-Lucent 4028, 4038, 4068 IP Touch® phones

Protection by MSM

- OmniPCX Enterprise PCS
- Media gateways: legacy boards without built-in security
- Application servers:
  - ¬ OpenTouch Multimedia Services
  - ¬ OpenTouch Message Center
  - ¬ Alcatel-Lucent 4645 Voice Messaging Services
  - ¬ OmniPCX RECORD Suite
  - ¬ External recorders using IP DR-Link Protocol

Regulatory

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

Platform capabilities

	SSM	MSM
IP Phones per SSM (max)	15 000	-
Media gateways per SSM (max)	240	-
Simultaneous encrypted communications per MSM when protecting PCS or application servers (max)	-	400
Simultaneous encrypted recording legs per MSM when protecting IP DR-Link recorders (max)	-	800

Alcatel·Lucent Enterprise