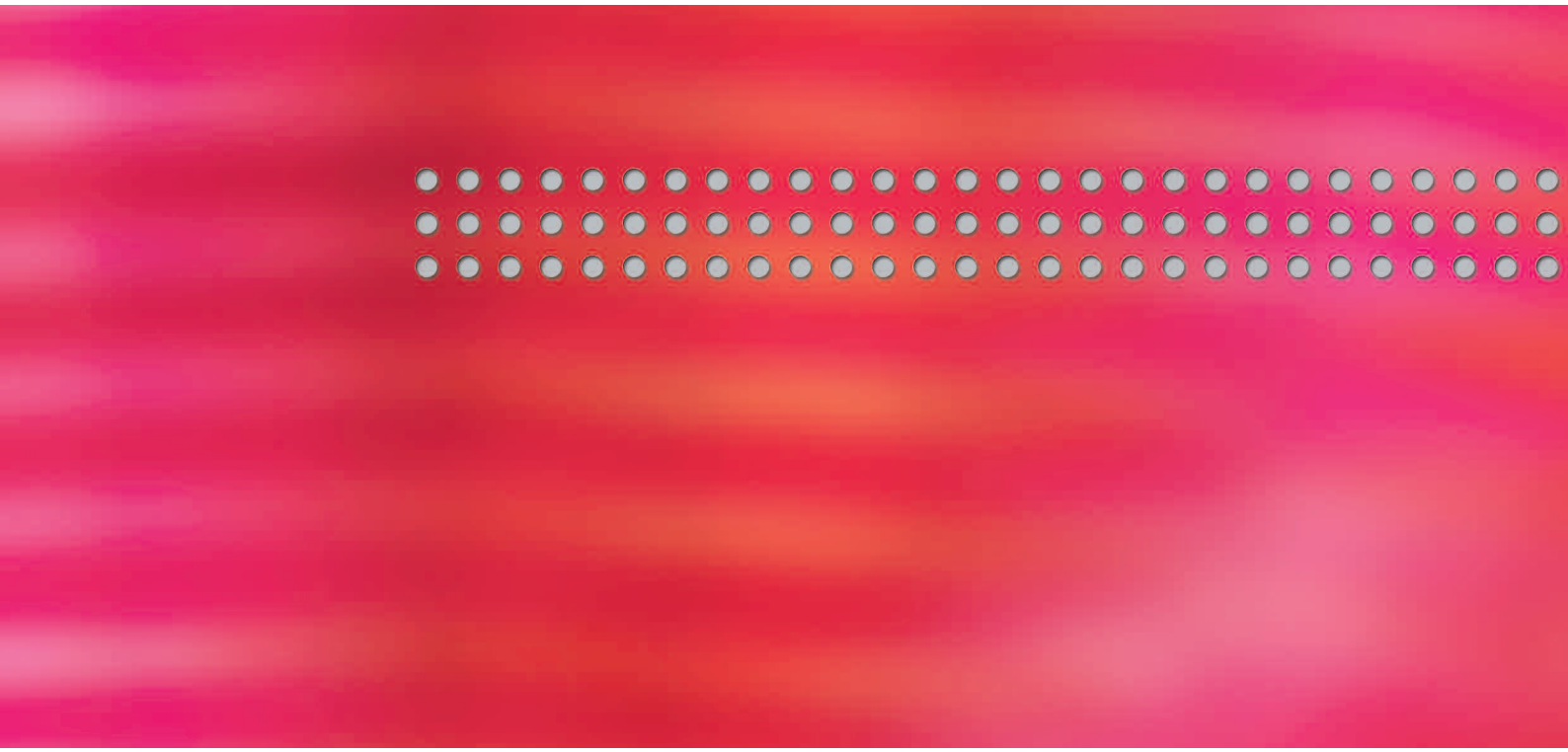
THALES

Alcatel·Lucent

APPLICATION NOTE

IP Touch Security Solution

Performance assessments



Abstract

The Alcatel-Lucent IP Touch Security Solution is a partnership between Thales and Alcatel-Lucent for securing IP communications on the Alcatel-Lucent OmniPCX™ Enterprise Communication Server solution.

Security is provided through:

- Mutual authentication of all equipment
- Encryption of telephony over IP (ToIP) flows (signaling and voice)
- Integrity of call control signaling (ensuring that messages have not been modified)
- Secure downloading of binaries and configuration files in IP phones and IP media gateways

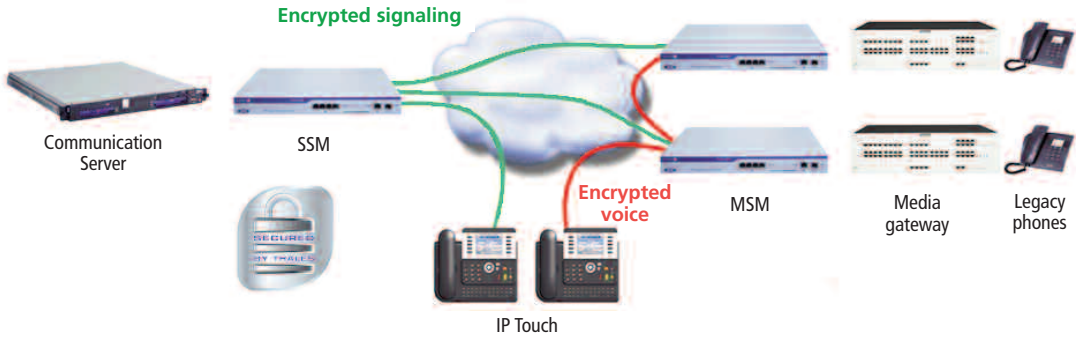
Table of Contents

IP Touch Security Solution

The IP Touch Security Solution is based on IPSec transport mode for signaling using Internet Key Exchange (IKE) protocol and standard Secure Real-time Transport Protocol (SRTP) for voice communications:

- Server Security Module (SSM) secures the communication server and is mainly dedicated to signaling encryption
- Media Security Module (MSM) secures other IP server components (such as media gateways, media servers, voicemail, etc.) and is mainly dedicated to voice encryption

Figure 1. Security Solution



Due to the SSM position, IKE negotiations are sent together to the SSM at start-up. The SSM has to provide high performance in order to give an operational status to the system in the shortest time.

That's why SSM software (since version 2.0.02) introduced the following enhancements:

- Start-up duration
- Server infrastructure priority (CS redundancy, MG, applications)

This paper provides lab results of each model's performances using a complete start-up simulation. Voice communications are also simulated in order to evaluate audio quality in case of high MSM usage.

Complete start-up performance

SSM secures the communication server and is primarily dedicated to signaling encryption. At start-up, traffic keys must be negotiated using IKE.

To measure start-up duration, the SSM is first disconnected from the network and rebooted. At this step, the SSM only knows the server infrastructure but can't yet establish secure channels to it.

While simulated IP Touch phones are trying to connect to the SSM and remote server infrastructure is waiting, SSM is re-connected to start the key negotiations. Only signaling is simulated; other data streams are specific to each deployment and are not taken in account here.

Figure 2 shows the results of complete start-up duration for a system equipped with the max number of IP Touch phones and the max number of MSM:

Figure 2. SSM-BOX vs. SSM-RM

	SSM-BOX	SSM-RM
Timescale for secured IP Touch start-up	< **30 min** (3,000 secured IP Touch)	< **30 min** (15,000 secured IP Touch)
Timescale for managed MSM start-up	**2 min** (30 managed MSM)	**10 min** (300 managed MSM)

Note: A complete start-up is exceptional and will only appear if there is a complete network or power blackout. For the case where only IP phones, not the SSM, are restarted the start-up time is the same as for a non-encrypted system.

The following paragraphs provide more detail showing the progression of a complete system start-up:

- Figure 3 represents measurements for the complete infrastructure
- Figure 4 focuses on the server infrastructure start-up

Figure 3. SSM-BOX – Measurement for the complete infrastructure

Test Configuration	
SSM model	
SSM binary version	2.0.06
Secured IP Touch	3,000
Managed MSM	30

Each managed MSM protects one IP address connected on its clear port (IPMG GD or application). Consequently, it generates three secured channels for server infrastructure use on SSM equipment (3 x 30 MSM = 90 secured channels).

Figure 4. Timescale since complete startup – IP Touch

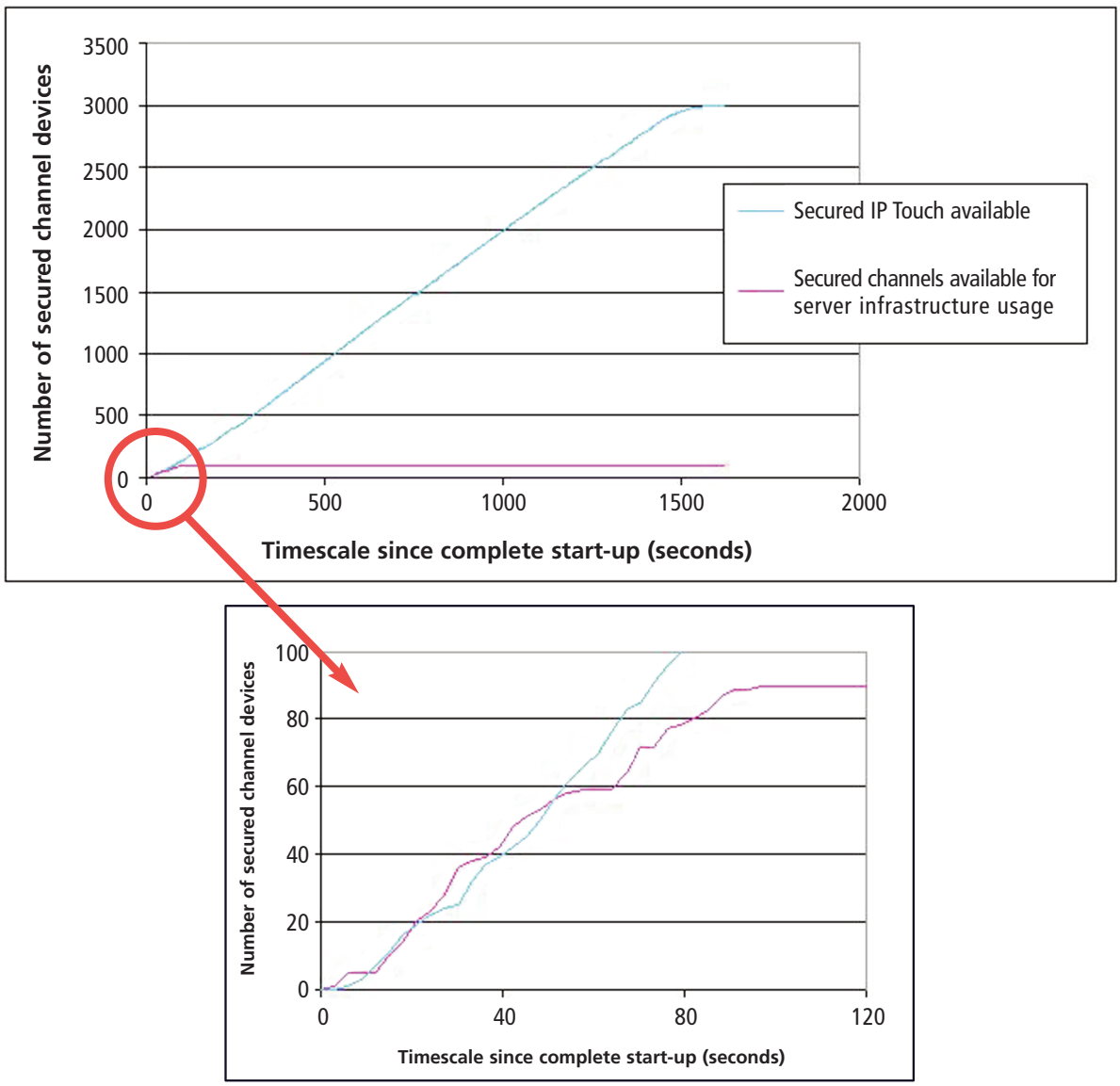
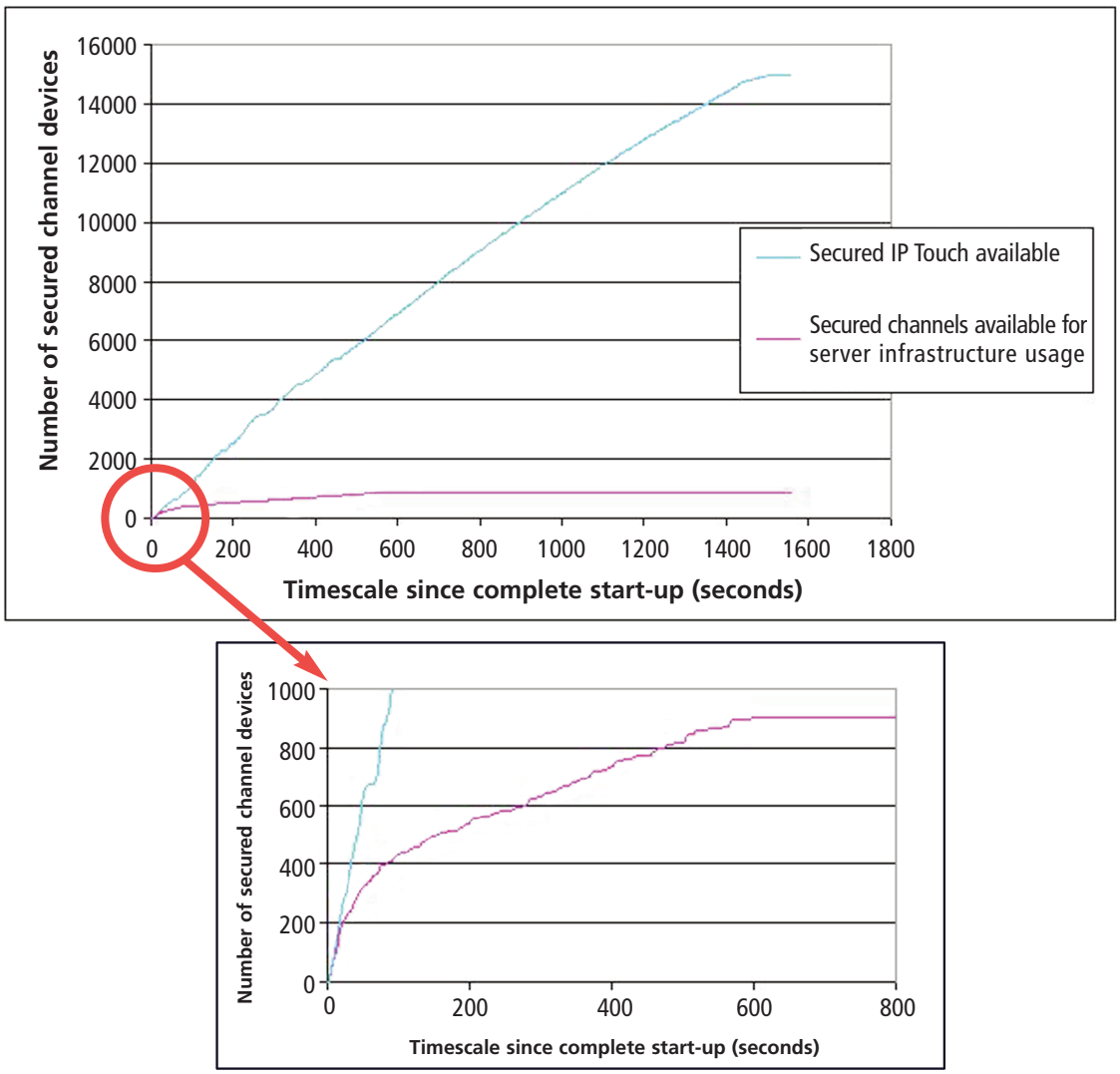


Figure 5. SSM-RM (rack mounted)

Test Configuration	
SSM model	
SSM binary version	**2.0.06**
Secured IP Touch	**15,000**
Managed MSM	**300**

Each managed MSM protects one IP address connected on its clear port (IPMG GD or application). Consequently, it generates three secured channels for server infrastructure use on SSM equipment (3 x 300 MSM = 900 secured channels).

Figure 6. Timescale since complete start up - IP Touch



Audio quality

MSM secures IP server components other than the communication server (such as media gateways, media servers, voicemail, etc.), and is mainly dedicated to voice encryption.

A simulation of the maximum number of secured voice communications is made through the MSM. Audio quality is evaluated by the audibility of an additional communication by human ear.

Figure 7. MSM-BOX

Test Configuration	
MSM model	
MSM binary version	2.0.06

Figure 8. Measurements for different codecs

Codec	G729		G723.1	G711	
Secured voice communications	120		120	120	
Framing (ms)	20	30	30	20	30
Ethernet frame size (byte)	78	88	82	218	298
Bidirectional frames rate (frames per second)	6,000	4,000	4,000	6,000	4,000
Audio quality	☺	☺	☺	☺	☺

Figure 9. MSM-RM (rack mounted)

Test Configuration	
MSM model	
MSM binary version	2.0.06

Figure 10. Measurements for different codecs

Codec	G729			G723.1	G711	
Secured voice communications	250			250	250	
Framing (ms)	10	20	30	30	20	30
Ethernet frame size (byte)	68	78	88	82	218	298
Bidirectional frames rate (frames per second)	25,000	12,500	8,333	8,333	12,500	8,333
Audio quality	☺	☺	☺	☺	☺	☺

032125 Rev. F 1/09

Alcatel·Lucent