

> Thales accelerates Polycom's integration of digital certificates into phones



Polycom turns to Thales Professional Services and Thales HSMs to enhance VoIP Security.

Best known for its iconic triangular-shaped conference phones, Polycom transformed business communication in the early 1990s, making it easier, more efficient, and more pleasant to collaborate with colleagues and partners around the globe. The company's brand continues to be synonymous with quality, clarity, and convenience among IT buyers. With the market for Voice over Internet Protocol (VoIP) devices growing and a portfolio of VoIP phones spanning from the desktop to the conference room, Polycom decided to enhance its phones by giving them a unique identity, making it easier to identify them on customer and service providers' networks while thwarting would-be counterfeiters and fraudsters. How? With digital certificates and encryption keys generated and secured by Thales hardware security modules (HSMs) from the nCipher product line.

"Our VoIP devices can authenticate themselves on a network using digital certificates," says Marek Dutkiewicz, director of product management for Polycom. "Because the certificates are issued as part of the manufacturing process, it's easy for our customers and partners to authenticate themselves while also stopping potential counterfeiters or 'spoofers.' Our success is built on Thales HSMs deployed by Thales Professional Services."

“Thales provided the expertise needed to design and implement a tailored, secure VoIP solution.”

Marek Dutkiewicz, Polycom

Securing VoIP

VoIP has two key advantages over traditional telecommunications technology: lower costs and the potential for integration with other IP applications. However, as with other forms of Internet-based communication, there are security concerns, such as the uncertain identity of devices and persons on the network. Traditionally, VoIP phones used passwords for identification purposes, making definite identity verification difficult and adding to setup time for end users or service providers. Moreover, this password-based process did not protect phone manufacturers from counterfeit devices.

Digital certificates overcome some of the challenges of password-based security. Unlike passwords, digital certificates are unique identifiers that allow devices to authenticate themselves and the networks they join. For example, a device with a valid certificate can verify that it is connected to an authorized server and the authorized server can check the authenticity of the device. If digital certificates are generated and distributed securely, they cannot be forged, making spoofed or counterfeit devices easy to identify.

"If phones can be 'spoofed,' you run the risk of fraudulently placed and inaccurately billed calls," explains Dutkiewicz. "Polycom is committed to delivering solutions that meet the needs of our customer and partners, and security is no exception. Using digital certificates to identify phones, we can significantly reduce security risks. We realized we needed a solution that would allow us to generate certificates and a corresponding private key, place them in the phones, and maintain the system across our manufacturing process."

BENEFITS WITH THALES PROFESSIONAL SERVICES:

- > Accelerated project completion
- > Secured process to prevent spoofing and counterfeiting
- > Tailored solution to fit manufacturing process
- > Delivered unmatched expertise for high tech manufacturing

Turning to the experts

After deciding on its approach, Polycom began looking for the right solution and implementation partner. The company discussed its options with several technology vendors and solution developers, but—with one exception—none offered everything Polycom was looking for: proven technology, experience with encryption key generation and digital certificate issuance in manufacturing, and the ability to develop a secure end-to-end process. Thales Professional Services was the exception. Its team explained how Thales HSMs secure the digital certificate issuance and key generation processes. Most importantly, the team also understood how to engineer and execute upon a solution that integrated with Polycom's manufacturing process.

"We decided to use Thales HSMs, and to implement our solution with help from Thales Professional Services," says Dutkiewicz. "Thales provided the expertise needed to design and implement a tailored, secure VoIP solution."

Developing an effective process

To design a process that fully met Polycom's needs, Thales Professional Services worked closely with Polycom's staff. Polycom explained how it wanted certificates to work within its manufacturing process, and Thales detailed a system that could deliver the capabilities Polycom wanted.

Thales consultants developed a solution that generates keys and uses a Microsoft certificate authority (CA) to sign digital certificates at Polycom's data center in North America. All key generation and certificate signing takes place within the HSM environment. Then the keys and certificates are transferred to the Thales HSM in Polycom's manufacturing facility in Thailand. There the keys and certificates are stored encrypted until they are placed into a newly manufactured VoIP phone.

"We wanted to generate keys and certificates at our data center and transfer them to the manufacturing facility and into new devices securely," says Dutkiewicz. "Thales Professional Services delivered what we asked for and needed. The Thales team helped us to develop and implement a process that protects our customers' calls and our company from counterfeiting."

Secure execution

Thales used the Secure Execution Environment (SEE) within Thales HSMs to enable end-to-end protection of the certificate and key generation, transmission, and device insertion process. The Thales SEE allows Thales HSMs to execute a variety of processes within a secured environment. To take advantage of it, the Thales Professional Services team wrote code that generates phone key pairs, requests certificate signing, and transmits the encrypted package to Polycom's

Organization Profile

Polycom, Inc. is the global leader in telepresence, video, and voice solutions and a visionary in unified communications (UC) solutions that empower people to connect and collaborate everywhere. In today's economy, Polycom solutions offer a rapid ROI and help customers reduce costs, increase productivity and lower their carbon footprint.

To learn more about Polycom UC solutions, visit <http://www.polycom.com>.

For more information about Thales, visit <http://www.thales-esecurity.com>.

manufacturing facility. The team also engineered a process that initiates an encrypted secure socket layer (SSL) connection within the HSM at the manufacturing facility and that terminates in the newly manufactured phone. This connection enables the secure delivery of keys and certificates into the phones.

"Our Thales HSMs keep the certificates and private keys that identify phones secure, and the Thales SEE protects the issuing process half way around the world," explains Dutkiewicz. "We have found the process to be a very effective and secure way to include digital certificate issuance in our manufacturing process."

"The Thales team helped us to develop and implement a process that protects our customers' calls and our company from counterfeiting."

Marek Dutkiewicz, Polycom

A foundation for continued success

Polycom sees its Thales HSM-powered device authentication process as delivering two key bottom-line benefits to the company: reduced risk of counterfeits and increased sales opportunities. "No matter how authentic a counterfeit device might seem, it shouldn't be able to fool an authorized VoIP network without a valid certificate," observes Dutkiewicz. "Thales HSMs are the foundation to the entire process—from manufacturing to everyday use. I think of them as a bank vault, but really they are more secure than that. Most importantly, of course, they benefit our customers. Customers definitely want security without hassle in their VoIP devices. We see digital certificates helping us to drive sales and increase our market share."



Thales Information Technology Security