THALES E-SECURITY PROVIDES A ROOT OF TRUST FOR POLYCOM PHONES

EXECUTIVE SUMMARY

The name "Polycom" has long been synonymous with telecommunications and Voice over Internet Protocol (VoIP) equipment from the desktop to the conference room. The ability to distribute these connected devices across geographies offers valuable functionality but also exposes organizations to new security vulnerabilities introduced by rapidly expanding network connections. In order to enhance its VoIP security, Polycom turned to Thales nShield hardware security modules (HSMs) to provide PKI-based IoT device security functionality -- giving their phones a unique identity, making it easier to identify them on customer and service providers' networks while thwarting would-be counterfeiters and fraudsters.

THE CHALLENGE

While the advances in Voice over Internet Protocol (VoIP) have had many positive impacts and offer many options in terms of communications for far flung business operations, the threats posed to those who utilize these services have grown more sophisticated as well. Like today's device-level threats in the IoT, those threats start with the phones themselves, where without adequate protection, phones can be counterfeited or spoofed. Traditional means of VoIP identification/authentication like passwords clearly lack adequate strength, and add to setup time for end users and service providers as well. The challenge is to embed something in the device at the time of manufacture that provides the device producer with the right level of security and process control, and provides the eventual end user a trustworthy means by which the device can be verified as authentic prior to use. And, as many IoT device manufacturers must face as the industry grows, scalability to large numbers of devices is a critical consideration. In order to build a secure and scalable system, it was determined that outside help would be required.

THE SOLUTION

Polycom explored several options to improve the security of its VoIP devices, soliciting advice from a number of companies with expertise in the field. Their goal was to find security technology that was already proven to be effective, rather than developing an entirely new system. It was also desired that the company providing the new security system have knowledge about the secure generation of cryptographic keys and creation of a supporting public key infrastructure (PKI) to create and distribute digital certificates as part of the device manufacturing process as a whole.

Polycom eventually decided that they would employ Thales e-Security due to their previous experience with design and implementation of digital certificate systems. As a result, the newly manufactured VoIP devices have distinct advantages over their predecessors. The unique key and associated digital certificate for each device is created within the certified secure confines of a Thales hardware security module (HSM), and protected with encryption until they are placed into the new device. An authorized number of keys and certificates are created in an encrypted "package" at the Polycom North America data center, and transmitted overseas to one of Polycom's manufacturing facilities. This embedded root of trust provides a customer who eventually purchases the devices with assurance that they are authentic when they bring the device online, thereafter providing secure VoIP services. This type of protection against counterfeiting is a critical security service as new types of devices proliferate in the IoT.

RESULTS

Polycom and its customers benefit from the integration of unique digital identities into its new VoIP devices, protected by the use of HSMs during the creation and signing of the unique digital identity. Customers are assured that that their devices are highly secure and can be connected with greatly reduced risk of fraud or counterfeit. Polycom has a secured manufacturing process which has scaled across multiple manufacturing facilities, and helps them drive sales of devices to security-conscious customers.

About Thales e-Security

Thales e-Security is the leader in advanced data security solutions and services that deliver trust wherever information is created, shared or stored. Thales ensures that the data belonging to companies and government entities is both secure and trusted in any environment – on-premise, in the cloud, in data centers or big data environments – without sacrificing business agility. Thales e-Security is part of Thales Group.

About Thales Group

Thales is a global technology leader for the Aerospace, Transport, Defence and Security markets. With 64,000 employees in 56 countries, Thales reported sales of €14.9 billion in 2016. With over 25,000 engineers and researchers, Thales has a unique capability to design and deploy equipment, systems and services to meet the most complex security requirements. Its exceptional international footprint allows it to work closely with its customer all over the world.

About the Industrial Internet Consortium

Thales has been a member of the Industrial Internet Consortium since May, 2017. The Industrial Internet Consortium is a global, member supported organization of over 250 members that promotes the accelerated growth of the Industrial Internet of Things by coordinating ecosystem initiatives to securely connect, control and integrate assets and systems of assets with people, processes and data using common architectures, interoperability and open standards to deliver transformational business and societal outcomes across industries and public infrastructure. Founded by AT&T, Cisco, General Electric, IBM and Intel in March 2014, the Industrial Internet Consortium catalyzes and coordinates the priorities and enabling technologies of the Industrial Internet. Visit www.iiconsortium.org.