

Case Study

Thales Luna HSMs and DigiCert Secure Next Generation 911 Phone Services

For Canadian
Telecommunications
Company

cpl.thalesgroup.com

THALES
Building a future we can all trust

A Canadian Telecommunications Company was mandated to build a secure Next Generation 9-1-1 (NG9-1-1) phone system.

This phone system was developed to modernize emergency services operations to support all types of media (voice, text, and data) as well as location handling. It includes a new public safety answering point (PSAP) system that uses IP-based technology to deliver emergency services. These improvements enable responders to locate and respond to incidents with more efficiency and speed.

With the introduction of this new technology, the security and reliability of the system is of utmost importance. For this reason, the solution requires a robust and secure PKI infrastructure to support the secure exchange of information between PSAPs and other public safety agencies.

The challenges

The Canadian Telecommunications Company needed to deliver a secure and interoperable NG9-1-1 service to fulfill the mandate requirements.

The solution

Thales and DigiCert partnered together to deliver a certificate authority (CA) based on PKI technology to PSAP customers to meet the strict security and interoperability requirements of NG9-1-1. DigiCert provided the root and intermediate certificates and Thales provided the Luna hardware security modules (HSMs) to protect the keys used for code signing each of the certificates.

This joint Public Key Infrastructure (PKI) solution was developed for establishing unique identifiers for emergency workers and their devices. The technology enables secure communication between all parties in the ecosystem, and the collaboration between Thales and DigiCert will secure the NG9-1-1 service offering through the operation of a root of trust, a mechanism that securely encrypts communications using digital certificates and the associated private keys used for signing operations. The PKI ensures that only authorized parties can access the NG9-1-1 system to ensure the integrity of operations.

The results

The partnership between Thales and DigiCert has delivered a number of benefits for the Canadian Telecommunications Company, including:

Increased security: Thales Luna HSMs securely generate, store, and manage the keys used in code signing the digital certificates within the secure confines of the HSM. Keys and signing material never leave the intrusion-resistant, tamper-evident FIPS 140-2 Level 3 and

Common Criteria EAL 4+ certified hardware device. Luna HSMs also provide strict access control to the use of code signing keys (which must be kept inside the HSM to perform the code signature), as well as generate a secure audit log.

Improved interoperability: The use of a common PKI standard ensures that PSAPs and their key ecosystem partners can interoperate with each other securely and with other public safety agencies.

Reduced costs: The use of a robust, secure, cloud-based PKI solution reduces the cost of ownership for PSAPs.

Conclusion

The partnership between Thales and DigiCert has delivered a secure and interoperable NG9-1-1 CA PKI service for the Canadian Telecommunications Company. This service will help to ensure that PSAPs are able to provide the highest level of service to the public in the event of an emergency.

In the long term, the NG9-1-1 compliant solution will also position it to have the capability to accommodate a trust relationship with other jurisdictions. Further, the PKI solution supports standard security certificates assigned to Canadian 911 call centers.



DigiCert

DigiCert, Inc. is the world's leading provider of digital trust, enabling individuals and businesses to engage online with the confidence that their footprint in the digital world is secure. DigiCert ONE, the platform for digital trust, provides organizations with centralized visibility and control over a broad range of public and private trust needs, securing websites, enterprise access and communication, software, identity, content and devices. DigiCert pairs its award-winning software with its industry leadership in standards, support and operations, and is the digital trust provider of choice for leading companies around the world. For more information, visit www.digicert.com or follow @digicert.

Thales Luna HSM

Luna HSMs provide high-assurance protection for cryptographic keys used by applications in on-premises, cloud and across hybrid environments to protect the cryptographic infrastructure by securely managing, processing, and storing cryptographic keys inside a hardened, FIPS 140-2 Level 3 tamper-resistant device.

Communication providers around the globe rely on Luna HSMs as their foundation of trust when preparing for Next Generation solutions, including securing PKI infrastructure, and other use cases where confidentiality, integrity, and availability are paramount.