cpl.thalesgroup.com

THALES
Building a future we can all trust

Fortune 500 biotech firm uses Thales and Keyfactor to protect life-sustaining IoMT devices

A well-known Fortune 500 biotech company was developing next-generation Internet of Medical Things (IoMT) devices. Among the innovations was a line of Bluetooth-connected pacemakers that could be implanted in patients and updated and monitored remotely. This allows for firmware updates, remote diagnostics, and ultimately better patient outcomes.

The Challenge

From the start the organization recognized the need for continuous security for pacemakers installed at a global scale. The organization needed high assurance that data transferred between patients and back-end networks was consistently secure and would remain authentic throughout all communication channels. This secure connection needed to be accessible under every circumstance – wherever the patient would be, anywhere in the world.

Requirements also included that the firmware be securely signed by the manufacturer and verified by the pacemaker. In healthcare, protecting the firmware signing keys can literally be a matter of life and death.

The Solution

Thales and Keyfactor have partnered to enable digital transformation and secure cloud migration for enterprises with an end-to-end IoT identity platform purpose-built for manufacturers to build, deliver, and maintain the most trusted connected devices on the market.

The combination of Thales' Luna Hardware Security Modules (HSM) and Keyfactor's PKI solutions allows enterprises and creators of IoT-enabled products to secure the entire public key infrastructure (PKI) hierarchy whether in the cloud or in client-hosted environments.

For this biotech company, the implementation of Thales Luna HSMs and Keyfactor Control includes:

- Issuing secure device credentials
- Firmware code signing and verification
- Code signing private keys protected by Keyfactor
- Thales's tight, auditable private key controls and private key secured in Luna HSMs at all times

Luna HSMs are the foundation of digital security for traditional and emerging technologies. They afford the institution the flexibility to meet its business and compliance needs securely and efficiently with a high assurance, FIPS certified root of trust.

The solution allowed the customer to create an innovative process that maintains data safety throughout every communication. The data encryption public key and root of trust are installed in the pacemakers, and the pacemakers then verify signed firmware against root of trust. The pacemakers encrypt patient data with the public key and then that encrypted data flows through Windows Azure, enabling global data access reach. All the data remains encrypted and can only be decrypted inside the manufacturer's data center using the data encryption private key and Luna HSMs.

The Results

By combining the features from two proven platforms, the biotech company found the perfect balance between agility, resilience, and security. The Thales and Keyfactor solution allows the customer to create an innovative product that maintains medical data safety ensuring data is encrypted at rest or in motion. It secures communications enabling constant device updates, increasing device effectiveness and life-span, and enhancing patient prospects.

The solution also enables flexibility during device manufacturing and operational cost savings by consolidating HSMs and the support of global deployments, wherever bluetooth-connected pacemakers are being used by patients.

The Future

Thales Luna HSMs can be deployed either in the cloud, as-a-service, on-premises, or across hybrid environments. For this particular use case, the biotech company elected to use Luna HSMs on-premises, but the enterprise is planning to expand into Luna Cloud HSMs. Thales Luna Cloud HSM is a cloud based HSM service available on Thales Data Protection on Demand (DPoD), Thales' own security services marketplace. With a comprehensive SLA, and the flexibility to enable seamless integration with the on-premises HSMs, Luna Cloud HSM securely stores and manages customer cryptographic keys, establishing a secure foundation of trust across all applications and services.

The organization has valued Keyfactor's strong expertise and overall responsiveness to answer questions and put in place the right processes to establish a robust PKI program for their IoT devices. Going forward, they plan to expand their use of Keyfactor as the organization prioritizes DevOps and cloud and data localization.

About Keyfactor

Keyfactor is the machine and IoT identity platform for modern enterprises. The company helps security teams manage cryptography as critical infrastructure by simplifying PKI, automating certificate lifecycle management, and enabling crypto-agility at scale. Companies trust Keyfactor to secure every digital key and certificate for multi-cloud enterprises, DevOps, and embedded IoT security.

KEYFACTOR

Highlights

- **The Thales and Keyfactor solution allows the customer to deploy a line of Bluetooth-connected pacemakers that maintain medical data safety ensuring data is encrypted at rest or in motion.**

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.