cpl.thalesgroup.com

THALES
Building a future we can all trust

Scalable Application Delivery with Trusted Key and Data Protection

F5 and Thales Team-Up to Secure and Scale Digital Transformation and High-Performance Web Applications

Securing High-Performance Web Applications

The global digital transformation market is expected to grow from USD 469.8 billion in 2020 to USD 1009.8 billion by 2025[1], driven by the rapid adoption of mobile, web and IoT applications. According to recent report[2], 80% of primary applications sit across multiple public and private clouds, increasing the cost, complexity and risks of managing application delivery. SSL/TLS, is a standard for establishing an encrypted link between a server and a client to protect Internet-based communications.

SSL/TLS makes websites more secure; however, SSL/TLS systems are vulnerable to a variety of attacks that are the result of stolen keys and digital certificates. Creating self-signed digital certificates by using software-based public-private key pairs makes it easy for attackers to compromise credentials and attack SSL/TLS systems with:

- Advanced persistent malware
- SSL stripping attacks
- Man-in-the-middle (MITM) attacks.

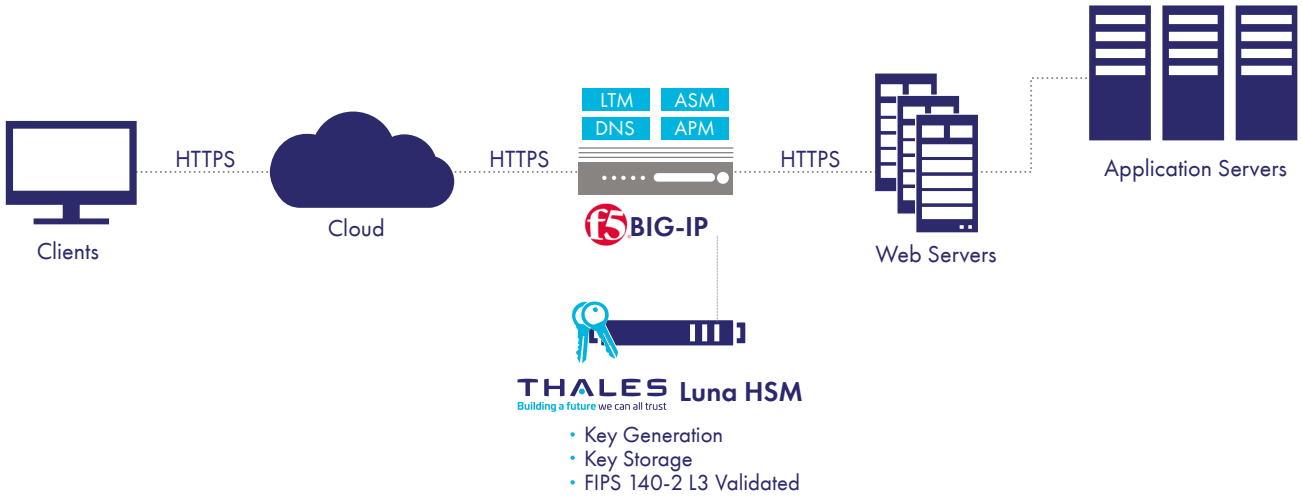
F5 and Thales have teamed-up to provide a secure and scalable web application delivery solution for data center and cloud environments by integrating the industry leading F5 BIG-IP application delivery controller (ADC) and the Thales Luna hardware security module (HSM). The joint solution provides application delivery performance, security, flexibility, and compliance at scale while encrypting communications and securing digital credentials. The joint solution includes:

- FIPS 140-2 level 3-validated key generation and storage for SSL/TLS digital certificates
- HTTPS-encrypted data optimized for application delivery
- Consistent key management across the hybrid multi-cloud.
- Network-connected HSM to service multiple ADC devices

1 "Digital Transformation Market by Technology – Global Forecast to 2025." Markets and Markets. July 2020. https://www.marketsandmarkets.com/Market-Reports/digital-transformation-market-43010479.html

2 "Accelerate: State of DevOps 2019." Google. 2019. https://services.google.com/fh/files/misc/state-of-devops-2019.pdf

Secure Application Delivery with F5 and Thales



The F5 BIG-IP ADC provides traffic management and application security, including SSL offload, to reduce the CPU load on web servers. By using the FIPS 140-2 Level 3-validated Thales Luna HSM for key generation and key storage, the F5 BIG-IP can generate encryption keys and TLS certificates using keys generated in hardware that meet the required authentication assurance levels for digital security.

F5 BIG-IP Application Delivery Controller

F5 BIG-IP ADC is a best-in-market SSL offload platform with unique core technology to provide scalability and performance.

F5 BIG-IP is available in multiple form factors to support data center and cloud deployments:

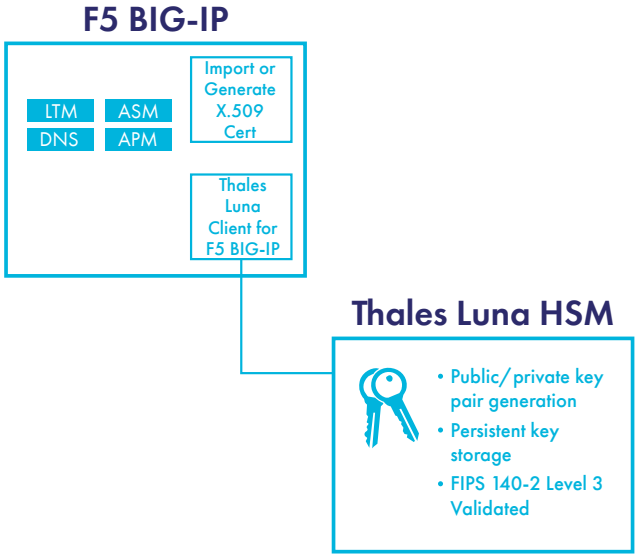
- BIG-IP iSeries appliance
- BIG-IP VIPRION chassis/blades
- BIG-IP virtual edition (VE).

Thales Luna Hardware Security Module (HSM)

Thales Luna Network HSMs and Luna Cloud HSMs are the industry's leading HSMs across both on premise and cloud environments. The FIPS 140-2 level 3-validated, tamper-resistant systems provide a root of trust, secure key generation, and key storage for improving the trustworthiness of SSL encryption, KMIP, authentication, certificate management, device integrity, application security, and DevOps.

Advantages of FIPS 140-2 Level 3-Validated Key Generation and Storage for SSL/TLS

- Thales Luna HSM Client for F5 BIG-IP simplifies integration across both on premise and Cloud HSMs
- Enables the ADC to generate self-signed TLS certificates using Luna HSM-generated key pairs
- Private keys are stored safely within the HSM, enabling the BIG-IP to use public and local keys for secure crypto operations
- The flexible solution can be implemented with an on-premise certificate authority (CA), third-party root CA, and third-party public CA.
- Security can be managed seamlessly with the F5 Application Policy Manager and Application Security Manager



Benefits of the F5 BIG-IP and Thales HSM Integrated Solution

Secure Data-in-Motion Optimized for Application Delivery

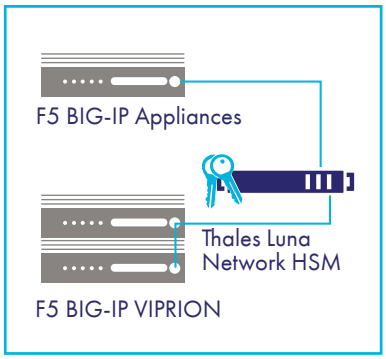
- F5 BIG-IP enables HTTPS between the client and the BIG-IP as well as the BIG-IP and the web servers, protecting the confidentiality of data-in-motion while providing the application layer protocol and persistent cookie visibility the ADC needs to accelerate application services
- Thales Luna HSM provides Trusted hardware-based key generation and storage for SSL/TLS and application security

Consistent Key Management Across the Hybrid Multi-Cloud

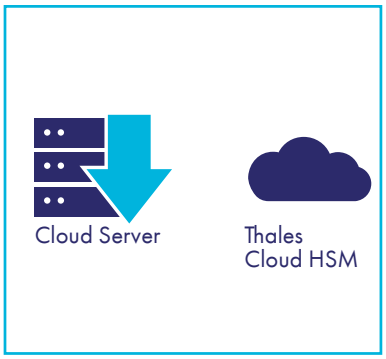
The Thales HSMs are available as an on-prem appliance or as cloud-based service that integrates with cloud IaaS and F5 BIG-IP Virtual Editions. Luna Cloud customers are able to manage keys and certificates consistently across private, public and hybrid multi-clouds. This ensures that your TLS keys are always protected and regardless of the location and deployment model of your web services infrastructure.

F5 & Thales Solution Benefits

- √ Scalable and fast performance
- √ Hardware-based key generation and storage for SSL/TLS encryption
- √ Digital certificate generation using HSM-generated keys
- √ Flexibility to support on-prem and third-party certificate authorities
- √ Simple integration
- √ Seamless key management via F5 console
- √ Compliance with the highest level of US NIST authentication assurance (AAL-3)



Private Cloud



Public Cloud

Multi-Cloud

Learn More About F5 and Thales

For more information how to implement secure, scalable and high-performance web:

- Thales Luna Network Hardware Security Module (HSM)
- Thales Luna Cloud HSM
- Thales CipherTrust Data Security Protection (CDSP)
- F5 BIG-IP Application Services
- F5 BIG-IP and Thales Luna HSM Installation Guide
- Implementing the Thales Luna with BIG-IP System

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us