thalescpl.com

THALES

SafeNet Network HSMs Provide High Assurance Key Security in Cloud Foundry

With the adoption of platform-as-a-service (PaaS) for the production of new cloud applications and services, businesses are bringing solutions to market faster, cheaper, and with lower risk than ever before. The Open Cloud Native Application Platform from Cloud Foundry gives companies the speed, simplicity, and control they need to maintain a competitive advantage in the market.

In the heightened legal and highly-regulated world in which we operate, there is an increasing need for high assurance security when developing on an open source PaaS environment, like Cloud Foundry. This is especially true when applications handle sensitive information or run in environments that are outside of the organizations direct control.

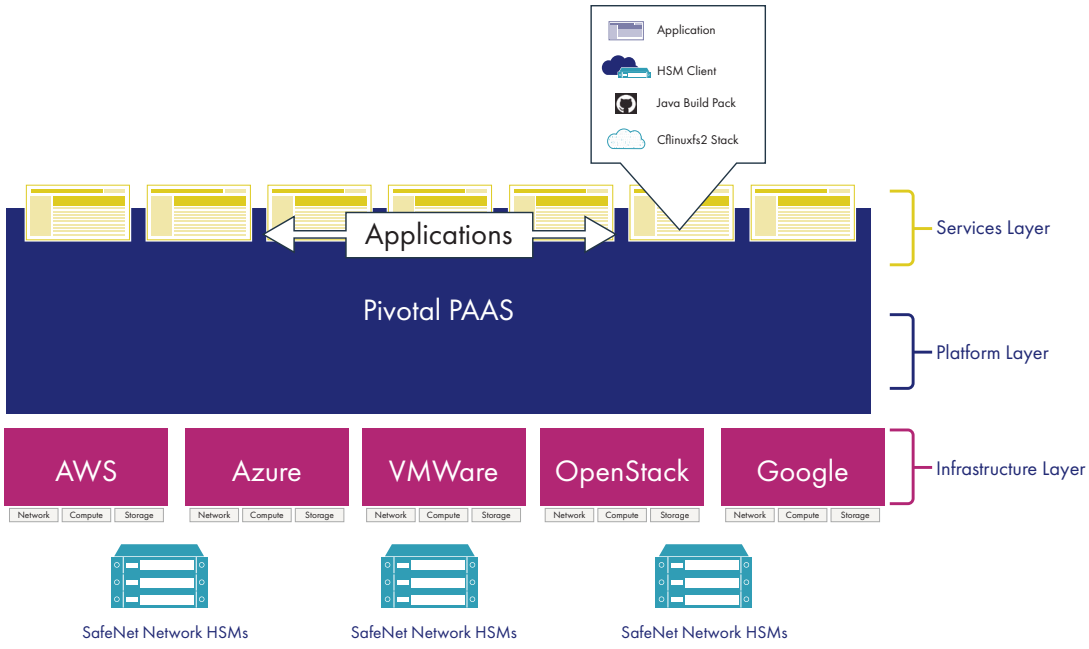
Cryptography provides a means for protecting and controlling data wherever it exists. However, when cryptography is used, the risk is transferred from the content of the data, to the cryptographic keys used to protect that data. For years organizations have turned to Hardware Security Modules (HSM) to isolate and secure their most sensitive cryptographic keys.

By leveraging Cloud Foundry Java Build pack, organizations can use SafeNet Network Hardware Security Modules (HSM) from Thales to attain the high assurance security needed to protect their cloud services and applications running on the Cloud Foundry Platform.

Approach to Security in Cloud Foundry: Making it Easy for Applications

SafeNet Network HSMs provide high assurance protection for cryptographic keys used by applications in on-premises, virtual, and cloud environments. With SafeNet Network HSMs, organizations can protect the entire key-lifecycle on a centralized platform, accelerate cryptographic operations, and leverage a single point of audit for cryptographic keys.

With the Cloud Foundry Java Build pack, organizations can seamlessly add SafeNet Network HSM as a service available to the application, much like how external databases can be added. By employing a keys-in-hardware approach, SafeNet Network HSMs protect cryptographic keys within the FIPS 140-2 validated confines of the hardware appliance. This method ensures that sensitive cryptographic keys always benefit from both physical and logical protections of the HSM appliance, no matter the environment and prevents unwanted access to the keys; even by third-party cloud infrastructure providers.



Using SafeNet Network HSM in Cloud Foundry to Provide High Assurance Key Security and Industry Compliance

Secure Application Portability

Cloud Foundry PaaS attracts deeply invested organizations to innovate and construct on the platform, by providing an application platform that can work across a variety of cloud infrastructures, making it easy for developers and organizations to optimize infrastructure without the need to customize their applications to support a multi-cloud deployment scenario. SafeNet Network HSMs work in the same fashion, supporting many deployment scenarios, from on-premises data centers to private, hybrid, public, and multi-cloud environments, providing a tremendous amount of flexibility as it enables customers to move keys in and out of cloud environments. With the open nature of Cloud Foundry applications, the SafeNet Network HSM service binding built into the Java Build pack can operate in a multi-cloud fashion on services such as Pivotal Cloud Foundry or IBM Bluemix, as well as in a private Cloud Foundry deployment.

Together, the deployment flexibility of Cloud Foundry PaaS and Thales SafeNet Network HSMs enable true application portability and multi-cloud use of high-assurance protection of cryptographic keys without the need for costly customization.

Compliance through Customer Control

SafeNet Network HSMs empowers organizations to demonstrate that only they can access the encryption keys that secure their data. This carries significant value when running Cloud Foundry in third party cloud Infrastructure environments that are outside of the organizations direct control. Being able to own and control your keys in any environment is essential for proving that you have complete control of all of your data for compliance purposes. Compliance can be facilitated by the SafeNet Network HSM service binding, which enables stateless Java applications to leverage the SafeNet Network HSM's security validations, such as FIPS 140-2, and Common Criteria. These validations are commonly referenced or required in industry compliance mandates, such as PCI DSS.

SafeNet Network HSM and Breadth of Integrations

SafeNet Network HSMs benefit from one of the broadest ecosystems available on the market and integrates with over 400 of the most commonly used enterprise applications for big data, code signing, TLS, web servers, application servers, databases, and many more.

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.

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com