Solution Brief

Thales Data Protection on Demand Services

cpl.thalesgroup.com

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Thales Data Protection on Demand (DPoD) is a cloud-based platform that provides a wide range of Cloud HSM and key management services through a simple online marketplace. With DPoD's extensive platform of Luna Cloud HSM, CipherTrust Key Management, payment, and partner-led services, security is made simpler, more cost effective and easier to manage because there is no hardware to buy, deploy and maintain. Just click and deploy the protection you need, provision services, add security policies and get usage reporting in minutes.

With a growing menu of cloud based security applications at your fingertips, including hundreds that work with the industry standard PKCS11 interface, select the security service you require from an expanding range of options and integrations.

Data Protection on Demand provides you with security you can trust:

- Secure cloud data
- Isolate keys and signing operations from certificate authorities, host platforms, and operating systems
- Automate key lifecycle control and processes
- Auto scale services at the click of a button
- Proven reliability with 99.95% SLA
- Set up a security service in under 5 minutes

Luna Cloud HSM Services

Luna Cloud HSM

Set up and access a Cloud HSM service for your organization's cryptographic operations

HSMs are a secure and trusted mechanism used to protect cryptographic keys and secrets. You can use your Luna Cloud HSM to generate and/or store cryptographic keys, establishing a common root of trust across all applications and services. You can also use your HSM to perform cryptographic operations such as encryption/decryption of data encryption keys, protection of secrets (passwords, SSH keys, etc.), and more. Thales Luna HSMs can be deployed in the cloud, as a service, on-premises, and across multiple environments to create a purpose-built hybrid HSM solution. Thales Luna HSMs have led the market for more than 25 years, and are the foundation of digital trust for traditional and emerging technologies across all environments.

Luna Cloud HSM for CyberArk

Secure CyberArk Privileged Access Security Solution's top-level encryption key within an HSM

Luna Cloud HSM for CyberArk provides a root of trust for the CyberArk Privileged Access Security Solution's top-level encryption key in an HSM. Luna Cloud HSM for CyberArk generates and stores the server keys, providing private key protection and strong entropy for key generation for CyberArk Privileged Access Security Solution system keys.

Luna Cloud HSM for Digital Signing

Digitally sign the author of software and firmware packages or electronic documents to ensure the integrity of the sender

Digital Signatures are used to establish the identity of the publisher of documents, software and firmware packages, and to prove the integrity of the signed data. Compromise of digital signature keys allow attackers to impersonate the original author and create their own malicious updates (malware). Digital Signing services within Data Protection on Demand protect the private keys associated with signing applications in a HSM service and prevent compromise or theft of private keys.

Luna Cloud HSM for Hyperledger

Bring trust to blockchain transactions to perform the required cryptographic operations across distributed systems

Luna Cloud HSM for Hyperledger stores the private keys used by blockchain Hyperledger members to sign all transactions, and ensures cryptographic keys cannot be used by unauthorized devices or people for a range of blockchain Hyperledger applications. Luna Cloud HSM for Hyperledger provides high assurance security in data centers and the cloud, enabling multi-tenancy of blockchain identities per partition as proof of transaction and for auditing requirements.

Luna Cloud HSM for Java Code Signer

Generate and protect the private keys associated with your Java Code Signer application in an HSM

With Luna Cloud HSM for Java Code Signer you can prevent private keys from being stolen or compromised by off-loading Java application server cryptographic operations to an HSM. Security is significantly enhanced by generating signing keys and certificates using HSM entropy and Java code signing crypto operations are performed inside the Luna Cloud HSM Service. In addition, this improves performance as cryptographic operations are off-loaded from the signing servers.

Luna Cloud HSM for Microsoft Active Directory Certificate Services

Secure the keys of your Microsoft Root Certificate Authority (CA) in an HSM

Luna Cloud HSM for Microsoft ADCS (Active Directory Certificate Services) provides a root of trust for Microsoft Root Certificate Authority (CA) signing key in an HSM. This enforces hardened boundaries for the CA's root cryptographic signing key, which is used to sign the public keys of certificate holders. By providing the root of trust for the CA's public key Microsoft's security is bolstered for example when configuring applications servers hosting Microsoft ADCS in dispersed data centers.

Luna Cloud HSM for Microsoft Authenticode

Generate and secure your Microsoft Authenticode certificates on an HSM

Luna Cloud HSM for Microsoft Authenticode provides hardened boundaries for Microsoft Authenticode digital certificates. The Luna Cloud HSM service integrates with Microsoft Authenticode to provide a trusted system for protecting the organizational credentials of the software publisher, and secures the keys used by the code signing application within the HSM service. Luna Cloud HSM for Microsoft Authenticode ensures relevant Microsoft systems, software and hardware products meet approved standards, and prevent signing keys being accessed by unauthorized entities.

Luna Cloud HSM for Microsoft SQL Server

Off-load Microsoft SQL Server cryptographic operations to an HSM

The Luna Cloud HSM service provides root of trust for storage of keys used in Microsoft SQL so that encryption keys do not reside with encryption data. Data can be encrypted by using encryption keys that only the database user has access to on in the Luna Cloud HSM service and cryptographic operations such as key creation, encryption, decryption, etc. can be offloaded to the HSM.

Luna Cloud HSM for Oracle TDE

Ensure that Oracle TDE encryption keys are protected by a master key that resides within the HSM

Encryption keys are generally stored locally with the database for performance and scalability reasons but this introduces the challenge of how to protect the encryption keys that were used to encrypt the data. The solution is to protect the local encryption keys, commonly referred to as Data Encryption Keys (DEK) with a Key Encryption Key (KEK) or master key that resides in the Luna Cloud HSM service key vault. This ensures that only authorized services are allowed to request the DEK to be decrypted.

Luna Cloud HSM for PKI Private Key Protection

Secure private keys belonging to Certificate Authorities responsible for establishing PKI trust hierarchy.

PKI root keys are the private keys belonging to the Certificate Authority (CA) responsible for establishing the PKI trust hierarchy. Root Certificate Authorities are the anchor of trust in PKI deployments and compromise of the CA keys would compromise the entire PKI trust hierarchy, leaving your data at risk. PKI Private Key Protection establishes trust by protecting your private keys.

Luna HSM Backup

Backup and restore for your organization's on-premises Luna HSMs

Luna HSM Backup is a Luna Cloud HSM service offering that provides a dedicated backup and restore location for your organization's on-premises Luna HSMs. With Luna HSMs, you can securely backup and restore HSM key material. The keys are directly cloned and can flow from on-premises to cloud and cloud to on-premises. Automatic key replication is enabled for backup to Luna Cloud HSM, Luna HSMs on-premises (including Luna Backup HSM) and also for Azure, IBM and AWS dedicated Luna HSMs, and between PED-authenticated Luna HSM partitions and Luna Cloud HSMs. When backing up to Luna Cloud HSM Services, you can be assured that the backup is to a resilient Luna Cloud HSM service (99.95% SLA), and your keys are securely stored in NIST FIPS 140-2 Level 3 certified hardware.

Luna Cloud HSM with Key Export

Export high quality private asymmetric keys from the HSM for use on other devices.

This mode is designed for generating key pairs for identity issuance, where transient key-pairs are generated, wrapped off, and embedded on a device. They are not used on the HSM, but generated and issued securely, and then deleted from the HSM.

The Luna Cloud HSM key export facility provides a simple cloud based key export that is fast to deploy and easy to export. Unlike traditional software-based solutions that have limited security and auditability, Luna Cloud HSM services ensure a FIPS certified key generation solution.

CipherTrust Key Management and Encryption Services

CipherTrust Data Security Platform as a Service (CDSPaaS)

CDSPaaS is a cloud-based SaaS deployment model that enables you to deploy key management and data protection services quickly—making security simpler, more cost effective, and easier to manage. CDSPaaS uses the same underlying security technology as the CDSP product portfolio—enabling a broad range of use cases, starting with CipherTrust Cloud Key Management (CCKM).

Services available on CDSPaaS on DPoD include:

- **CipherTrust Cloud Key Management as a Service (CCKM)** —Control and manage your multi cloud encryption keys in minutes.
- **CipherTrust Transparent Encryption (CTE)** enables you to meet compliance and best practice requirements for protecting data, wherever it resides—across multiple clouds, on-premises, and within container environments.
- **Live Data Transformation (LDT)** enables non-disruptive initial encryption and simplified, more-compliant encryption key rotations. Users continue to work as usual while encryption is in process.
- **Ransomware Protection (RWP)** (currently for Windows Server environments only) continuously monitors processes for abnormal I/O activity and alerts or blocks malicious activity before ransomware can take complete hold of your endpoints and servers.

Partner Services

Ascertia

Ascertia ADSS PKI and Signing Server Secure and scalable solution for digital signing and PKI management.

Encryption Consulting CertSecure Manager

CertSecure Manager helps you automate and seamlessly manage all certificates across different cloud environments and Kubernetes Clusters.

Encryption Consulting CodeSign Secure

CodeSign Secure is a secure and flexible solution to your code-signing needs for all operating systems including Windows, Linux, Macintosh, Docker and Android/iOS apps.

GaraSign

Securely manage keys, certificates, users, and permissions for all your DPoD-protected keys. Private keys stay in the HSM at all times, while cryptographic operations remain simple, fast, and secure.

Keyfactor Command

Keyfactor Command is the world's most complete and scalable cloud-based certificate management platform, providing the freedom to secure every identity across the enterprise. Get all the benefits of owning PKI without the risks. Absolutely, positively need to run it yourself? Keyfactor Command is also available for client-hosted environments.

KeyTalk PKI Management

KeyTalk's Certificate Key Management System (CKMS) automates the management, distribution and installation of certificates (PKI) from multiple public and internal CA's to any endpoint device running on any OS.

KeyTalk Secure E-mail Service

The Key Talk Secure E-mail service is based on the fully automated enrolment, installation and configuration of S/MIME certificates.

KeyTalk Secure Email is a unique, patented solution that not only creates the certificates, but also manages the keys.

PrimeKey EJBCS Software

EJBCS Software is a powerful and flexible Certificate Authority and a complete PKI (Public Key Infrastructure) Management System.

PrimeKey SignServer Software

Server-side digital signatures give maximum control and security, allowing your staff and applications to conveniently sign code and documents.

SignPath

Code and Macro Signing: Policy-driven automation for your processes and tools.

SureDrop

File-sharing and collaboration solution providing end-to-end encryption security and control over data sovereignty.

Venafi Platform

Venafi orchestrates connections to machines needing certificates, while protecting cryptographic keys with Thales Luna HSMs. This solution delivers full visibility, centralized control and full automation over HTTPS web application keys and certificates. All keys are generated, stored, and used for within the safe confines of Luna HSMs to reduce the risk of unauthorized data access and loss.

Don't see what you are looking for here, contact us to find out what services are coming next: dpondemand@thalesgroup.com

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.

Scan to sign up for a DPoD free trial

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