thalescpl.com

THALES

SafeNet Data Protection On Demand Services

SafeNet Data Protection On Demand, powered by Gemalto, is a cloud-based platform that provides a wide range of Cloud HSM and key management services through a simple online marketplace. With SafeNet Data Protection On Demand, 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 an 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.

SafeNet Data Protection On Demand from Gemalto provides you with security you can trust: Secure Cloud Data

- Isolate keys and signing operations from certificate authorities, host platforms, and operating systems
- Automate otherwise manual key lifecycle control and processes
- Auto scale to unlimited number of services
- Proven reliability
- Set up a security service in under 5 minutes

HSM On Demand Services

HSM On Demand

Set up a certified key vault for applications or integration requirements using your own HSM on demand service

Key vaults are a secure and trusted mechanism used to protect cryptographic keys and secrets. You can use your Key Vault to generate and/or store cryptographic keys, establishing a common root of trust across all applications and services. You can also use your key vault to perform cryptographic operations such as encryption/decryption of Data Encryption keys, protection of secrets (passwords, SSH keys, etc.), and more.

HSM On Demand for CyberArk

CYBERARK

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

HSM on Demand for CyberArk provides a root of trust for the CyberArk Privileged Access Security Solution's top-level encryption key in an HSM. HSM On Demand 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.

HSM On Demand 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.

HSM On Demand for Hyperledger

Bring trust to blockchain transactions to perform the required crypto operations across distributed systems—protects cryptographic keys, the blockchain system and digital wallets.

HSM On Demand 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. HSM On Demand 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.

HSM On Demand for Digital Signing

Digitally sign the author of software and firmware packages or electronic documents in order 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 SafeNet Data Protection On Demand protect the private keys associated with signing applications in a HSM service and prevent compromise or theft private keys.

HSM On Demand for Oracle TDE

Ensure that Oracle TDE database data encryption keys are encrypted with a master key that resides within the HSM On Demand service for optimal performance and scalability

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 encrypt 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 HSM On Demand service key vault. This ensures that only authorized services are allowed to request the DEK to be decrypted.

HSM on Demand for Java Code Signer

Sign Java artifacts using an encryption key generated on an HSM

With HSM On Demand 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 HSM on Demand Service. In addition, this improves performance as cryptographic operations are off-loaded from the signing servers.

HSM on Demand for Microsoft Active Directory Certificate Services

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

HSM On Demand 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.

HSM on Demand for Microsoft Authenticode

Generate and secure your Microsoft Authenticode certificates on an HSM

HSM On Demand for Microsoft Authenticode provides hardened boundaries for Microsoft Authenticode digital certificates. HSMoD 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. HSM On Demand for Microsoft Authenticode ensures relevant Microsoft systems, software and hardware products meet approved standards, and prevent signing keys being accessed by unauthorized entities.

HSM on Demand for Microsoft SQL Server

Enable Microsoft SQL Server cryptographic operations on an HSM

The HSM On Demand 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 HSM on Demand service and cryptographic operations such as key creation, encryption, decryption, etc. can be offloaded to the HSM.

Key Management On Demand Services

Key Broker On Demand for Salesforce

Create key material (tenant secrets) for Salesforce and manage your keys and security policies in concert with Salesforce Shield across their lifecycle

Using the Key Broker On Demand, you can design and enforce policies, helping to ensure compliance. To further ensure the security and privacy of your data, you can Bring Your Own Key (BYOK) within the SafeNet Data Protection On Demand service in the cloud. Providing a service layer (GUI/API), Key Broker On Demand enables you to create key material (Salesforce tenant secret) for Salesforce and to manage your keys in concert with Salesforce Shield across their lifecycle.

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

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