gemalto
security to be free

SOLUTION BRIEF

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 on demand key management and encryption 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 ever-expanding menu of data protection on demand applications at your fingertips, choose the security service you require from a range of options, and integrations.

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 PKI Private Key Protection

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

In a public key infrastructure (PKI), 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 (i.e. Root CA signs the Sub-CA certificates which are used in turn to sign user and device certificates), leaving your data at risk and vulnerable to un-authorized access. Using PKI Private Key Protection establishes trust by protecting your private keys, which are generated, stored and used within the confines of your dedicated HSM service for the highest security.

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 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 that 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. With HSM On Demand for Hyperledger, you can secure keys for every role in your Hyperledger framework and blockchain Hyperledger artifacts include admin CA secure within the SafeNet Data Protection On Demand's HSM On Demand service.

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 also used to prove the integrity of the signed data. Digital signing enables the recipient of the package to trust the Digital Signature that was applied to the update. If an attacker was able to compromise the digital signature keys, they would have the ability to impersonate the original author/publisher and create their own malicious updates (malware) that would be inherently trusted by the recipient since they trust the Digital Signature associated with the author/publisher. This could affect software security patches or hardware appliances such as routers for example. Using your own Digital Signing service within SafeNet Data Protection On Demand, you can protecting the private keys associated with your signing application in a HSM service to avoid the private keys from being stolen or compromised.

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. If an attacker steals the database, the content of the database is encrypted and inaccessible as the attacker does not have access to the Oracle TDE Database Key Vault where the KEK is kept.

Encryption on Demand

VM Encryption on Demand

Single pane of glass encryption across cloud, hybrid, and on-premises environments

Full disk encryption of bare metal servers, virtual machines and cloud instances so you can securely run even your most sensitive workloads or any highly regulated data in the cloud.

Whether using Microsoft Azure, Microsoft Hyper-V, Amazon Web Services (AWS), AWS GovCloud, Fujitsu Cloud Service K5 (based on OpenStack), IBM Bluemix (formerly SoftLayer), or VMware vSphere, VM Encryption powered by SafeNet Data Protection On Demand provides on demand cloud-enabled security as a service across multiple cloud/hybrid environments.

Key Management On Demand Services

Salesforce Key Broker On Demand

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

A key broker enables you to retain control of your keys and align your key management policies across environments. A key broker serves as a custodian of keys, providing a consolidated key management directory to manage, search and audit all keys. 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. Now you can use and manage your keys across Salesforce and supported applications, providing much needed security policy enforcement, essential audit capability and reducing administration overhead while naturally ensuring your data is always protected.

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

Contact Us: For all office locations and contact information, please visit safenet.gemalto.com/contact-us

Follow Us: blog.gemalto.com/security

GEMALTO.COM

gemalto
security to be free