On-Demand Key Management and Encryption in the Cloud

Dr. Götz Güttich

With SafeNet Data Protection on Demand, Gemalto offers a cloud-based platform that encompasses a large number of on-demand code signing, key management and encryption services which are usable via an online marketplace. Gemalto’s platform is intended to make security management simpler and less costly for its clients because no hardware needs to be purchased and operated. Gemalto claims that the platform’s central management tool can accomplish all work steps via point and click. We tested the product to find out if this really works.

SafeNet Data Protection on Demand encompasses a whole series of services offered according to a pay-as-you-grow principle. This assures flexible usage for the client and guarantees that he must pay only for the features he actually uses. In this way, the service seamlessly adapts to suit the requirements of each individual company.

The platform, which builds upon Gemalto’s SafeNet Identity and Data Protection solutions, enables its users to secure critical data in every environment, i.e. also in the cloud, on the premises or in virtual installations. Moreover, it helps its users to implement security policies and to comply with compliance regulations. Furthermore, it enables IT managers to administrate their encryption keys from a central location across all cloud services. APIs also help administrators to integrate on-demand services for encryption, key management and HSM (Hardware Security Module) in their surroundings, thus securing their applications and data. If necessary, an availability of 99.95% can be guaranteed by a service level agreement. An automatic failover function and key backups are delivered along with the platform. Comprehensive reporting functions complete the scope of the service offer.

**The Existing Security Services**

Let’s take a quick look at the scope of services that are included in SafeNet Data Protection on Demand. According to its manufacturer, the offer undergoes continual expansion. It currently encompasses six services. First, there’s the “Key Vault,” which IT managers can use as their own HSM on-demand service for their applications. By contrast, “PKI Private Key Protection” protects private keys which belong to certificate authorities (CAs). “Digital Signing” enables IT staff to digitally sign software packages, firmware packages and electronic documents, thus guaranteeing the server’s integrity. The “Oracle TDE Database Key Vault,” on the other hand, assures the encryption of the
Oracle TDE data-encryption keys with a master key depos-ited within the HSM on-de-mand service. With the aid of the “Hyperledger,” responsible staff members secure block-chain artifacts via keys, which likewise land in the HSM on-demand service.

The last service is the “Salesforce Key Broker on De-

mand.” It generates tenant se-crets for Salesforce and facili-
tates the administration of keys and security policies in collaboration with Salesforce Shield.

The Test
For our test, Gemalto made available to us a test account which we could use to scruti-
nize the functionality of the solu-
tion. We created several test users on this account and activated various services to secure our test data, e.g. the

key of a certificate authority. We especially concentrated on the management of the so-

lution and the work in ongoing operation.

The First Work Steps
After the first login at the abo-
vementioned test account, the solution began by requiring us to change the password that we had previously received

and the administrators in the system. In the next step, we accordingly set up an applica-
tion owner account. To ac-

complish this, the solution re-

quired a so-called “subscriber group.” The system imme-

diately generated this group du-

ring the configuration of the account and afterwards added it to the user account. The ac-

counts were defined by an email address and a pass-

word. The users of these new accounts were likewise re-

quired to change their passwords immediately after their first lo-

gin.

The First Service
After a user logs in as “appli-
cation owner,” he or she is shown an overview of the available services, i.e. “Digital Signing,” “Hyperledger,” “Key Vault,” “Oracle TDE Databa-

se,” “Salesforce Key Broker” and “PKI Private Key Protecti-
on.” In the first step, we want-
ted to generate a key vault. Adding the services to our own account always occurs according to the same princi-

ple. An employee first clicks on the entry of the desired service. Afterwards, the sys-
tem show him or her the terms of service, which the employ-
ee is required to accept. Next, the solution asks for a name for the service and, in the ca-

se of the key vault, the solu-

tion also wanted to know whe-

ther to allow or deny algo-

rithms that are not in confor-
mity with FIPS. After the rele-

vant details had been provi-
ded, the system showed an overview of the steps that needed to be performed and afterwards configured the ser-

vice: this task took only a few
seconds. Next, the solution also offered to immediately set up the client service, which is implemented on the target system in the enterprise. As soon as this task is complete, the responsible employees are able to download the client and install the client onto whichever computer they intend for this purpose.

### The Configuration of the Key Vault

After the download, we first unpacked the zip package with the client software onto our test computer, which ran under Windows Server 2012 R2. As software, we had imported onto this system only the current updates from Microsoft. Gemalto's documentation specified that the Microsoft Visual C++ 2015 Redistributable Update 3 package is indispensable for operating the client, so we installed that update too. In the next step, we had to unpack the contents of the “cvclientmin.zip” zip file (which was located in the original client zip package) into the same folder as the original installation package. Finally, it was also necessary to run the “setenv.cmd” file as administrator in order to set the environmental variable. Afterwards, we could start the service by calling up the “lunacm” file.

### The Configuration of the Service

A few configuration steps were now necessary in order to be able to work with the service. To provide an HSP application partition to store cryptographic objects for the utilized applications, we needed to initialize the roles for the Security Officer (SO), the Crypto Officer (CO) and the Crypto User (CU). All steps necessary for this are described in the documentation, so there’s no need to go into greater detail about them here. Suffice it to say that setting up the service took less than five minutes in our test and that the key vault was available for us to use afterwards.

Once we had put the service into operation, we used the “ckdemo” test program (which is included in the client’s scope of delivery) to generate keys, retrieve session data, etcetera, thus assuring that everything functioned as intended. There were no unwelcome surprises.

### The Work with the Private Key Protection

In the next phase of our test, we turned our attention to the “Private Key Protection” service. Here, we wanted to secure a CA key in order to take a closer look at the work with SafeNet Data Protection on Demand in praxis. For this purpose, we again logged onto our test account as application owner and used the “Add New Service” command to create a PKI Private Key Protection service.

Here too we were first required to accept the terms of service. Afterwards, we could give a name to the service and specify whether we wanted it to permit or deny algorithms that are not in conformity with FIPS. After the service was created, we again generated the service client and downloaded the client onto our test system. The installation of the service runs exactly the same way here as it does with the
key vault service. Incidentally: in operation, the client software sets up only one configuration through which the system can access the service and therefore does not always need to be active in ongoing operation. The appearance of the utilized configuration depends on the implemented application and is precisely described for the relevant applications in the documentation on the website of the Data Protection on Demand service.

We relied here on the “Microsoft Active Directory Certificate Services Integration Guide” and set up our CA so that its key would be secured by the service. To accomplish this, we first had to switch into the “KSP” subfolder of the client installation and register there our security library (a DLL that likewise belongs to the scope of delivery of the client) with the aid of the “KspConfig.exe” tool and the existing HSM slot (for the HSM on demand solution offered via the service). The slot must be registered twice to operate the solution: once for the administrator of the current domains and once again for the system account of the “NT Authority” domain.

As a slot password for the registration, we used the password of the previously created Crypto Officer because this officer has the right to write in the service partition. As soon as this task was accomplished, we began installing the active directory certification services on the server that we had set up as domain controller. To do this, we performed a standard installation of a certificate authority with the server manager.

Configuration of the Certificate Authority

After completing the setup, we configured the certificate authority with the aid of the intended wizard. In this context, we set up the system as an enterprise certification site and as “Root CA.” Afterwards, we attempted to create a new private key for the CA. Gemalto’s documentation states that for this purpose, one should select a Cryptographic Service Provider (CSP) from SafeNet from the corresponding dropdown menu. Unfortunately, no such provider appeared among the configuration choices shown to us, which were limited to providers from Microsoft.

We accordingly contacted the manufacturer’s support, who told us that it is not only possible to use the KSpConfig tool to register the utilized slot with one’s name (as we had done), but that it was also possible with one’s slot ID. The support person said that to solve the problem described here, it can sometimes help to perform the registration via the slot ID.

We then erased the existing registrations and performed them again with the aid of the slot ID. This unfortunately did not improve the situation, even after we had restarted the computer. The manufacturer’s support recommended that we check to see if the “SafeNetKsP.dll” file (which likewise belongs to the scope of delivery of the client) was listed in the “C:\Windows\System32” directory. This file was not listed in our test installation, so we copied the file into the aforementioned directory. Afterwards, we were indeed able to access the SafeNet CSPs. We then began finalizing the configuration. First, we needed to use the “sc query cert svc” command to check whether the CA service was active and to verify the CA key via “certutil -verify keys”. In this context, we noticed that the CA service on our system always stopped a few seconds after it started. Here again we needed to contact the manufacturer’s support, who told us that this was due to our German Windows Ser-
ver 2012 R2. We had, however, previously registered our HSM slot for the administrator-
dings. Gemalto responded to our suggestion after the test. The manufacturer told us that

cryption and key management available to companies for which the necessary efforts and the associated costs had previously been too much. Users of this service do not need to purchase and admin-
istrate any special hardware, and all clients pay only for the services they actually use. SafeNet Data Protection on Demand can also be a big help toward achieving GDPR conformity (in the context of the “right to be forgotten”) because stored data and keys can simply be erased whenever desired.

The solution was convincing in our test because it was comparatively quick to set up and relatively simple to use. The documentation is comprehensive and the manufacturer’s support was convincingly

and system account with the aid of the KspConfig.exe tool. The corresponding domain in the system account is named “NT Authority” and the tool didn’t offer us any other name for this domain. But on one of the German servers, the correct name is “NTAutorität”. We solved the problem by register-
ing the slot anew via the “ksp-
cmd.exe password /s {partition name} /u SYSTEM /d NTAU-
TORITÄT” command-line command. Afterwards, the integration of the active directory certificate service in the HSM on demand service was complete and we could use the system to archive keys, re-
create keys and perform similar tasks. The configuration basically proceeds quickly and it doesn’t confront the admin-
istrator with any insur-
mountable challenges. However, we suggested one modification to avoid potential misunder-

The user template after installation.

Summary
With SafeNet Data Protection on Demand, Gemalto offers an exceedingly interesting ser-
vice which has the potential to also make code signing, en-
good. If the abovementioned issues with the configuration tools and the localization have not already been rectified, they will most probably be sol-
ved in the very near future.

Sysbus