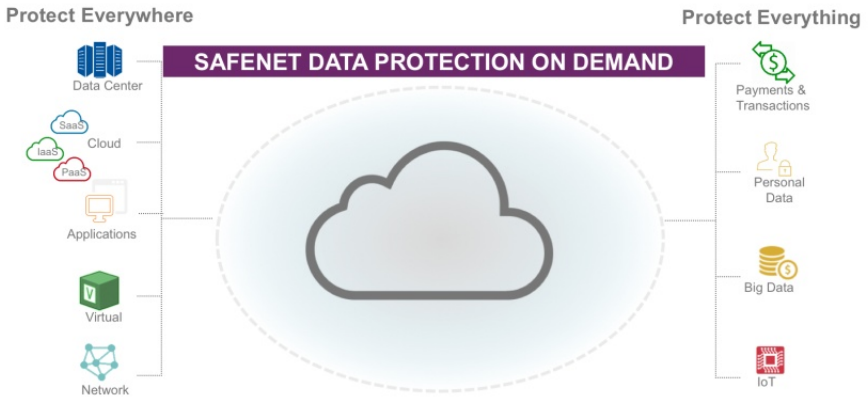
On Demand Key Management und Verschlüsselung in der Cloud

Dr. Götz Güttich

Mit SafeNet Data Protection on Demand bietet Gemalto eine Plattform auf Cloud-basis, die etliche On Demand-Code Signing-, Key Management- und Verschlüsselungs-Dienste umfasst, die über einen Online-Marktplatz nutzbar sind. Damit möchte das Unternehmen das Security-Management für seine Kunden einfacher und kostengünstiger machen, da keine Hardware angeschafft und betrieben werden muss. Sämtliche Arbeitsschritte sollen sich über das zentrale Management-Werkzeug der Plattform einfach über Point-and-Klick realisieren lassen. Wir haben uns im Test angesehen, ob das wirklich funktioniert.

SafeNet Data Protection on Demand umfasst eine ganze Reihe von Diensten, die nach dem Pay as you grow-Prinzip angeboten werden. Dies erlaubt den Kunden eine flexible Nutzung und garantiert ihnen, dass nur wirklich verwendete Features bezahlt werden müssen. Auf diese Weise passt sich der Dienst nahtlos an die Anforderungen des jeweiligen Unternehmens an.



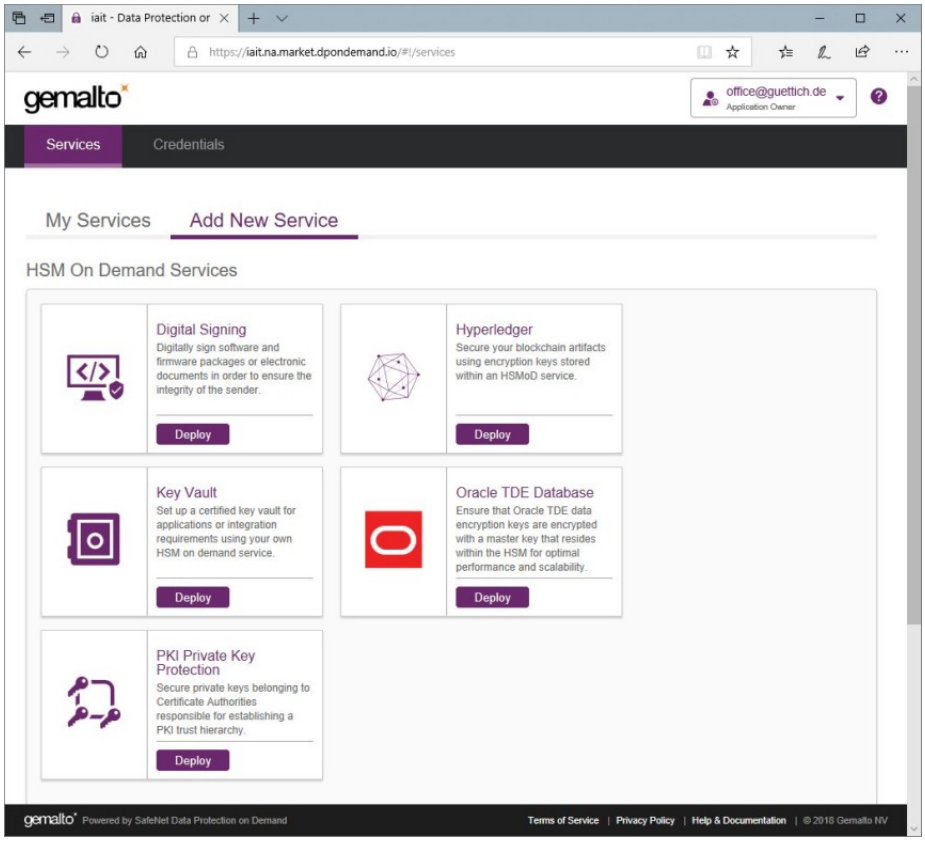
Über die Plattform, die auf die SafeNet Identity and Data Protection-Lösungen von Gemalto aufbaut, lassen sich kritische Daten in jeder Umgebung absichern, also in der Cloud, on-premise oder auch in virtuellen Installationen. Außerdem hilft sie beim Durchsetzen der Security Policies und beim Einhalten von Compliance-Vorschriften. Darüber hinaus versetzt sie die IT-Verantwortlichen in die Lage, ihre Verschlüsselungs-Keys über alle Cloud-Dienste hinweg an einer zentralen Stelle zu verwalten. APIs helfen den Administratoren zudem, die On Demand-Dienste für Verschlüsselung, Key-Management und HSM (Hardware Security Module) in ihre Umgebungen zu integrieren und so ihre Anwendungen und Daten abzusichern. Bei Bedarf lässt sich über ein Service Level Agreement eine Verfügbarkeit von 99,95 Prozent sicherstellen. Eine automatische Failover-Funktion gehört mit zum Lieferumfang, genau wie Schlüssel-Backups. Umfassende Reporting-Funktionen schließen den Leistungsumfang des Service-Angebots ab.

Die vorhandenen Sicherheitsdienste

Gehen wir nun kurz auf den Leistungsumfang der Dienste ein, die in SafeNet Data Protection on Demand enthalten sind. Das Angebot wird nach Angaben des Herstellers laufend erweitert. Zur Zeit umfasst es sechs Services. Zunächst einmal den „Key Vault“, den IT-Verantwortliche als eigenen HSM On Demand-Dienst für ihre Anwendungen nutzen können. Die „PKI Private Key Protection“ kommt im Gegensatz dazu zum Einsatz, um Private Keys zu schützen, die zu Certificate

Authorities (CAs) gehören. Über das „Digital Signing“ werden IT-Mitarbeiter in die Lage versetzt, Software- und Firmware-Pakete sowie elektronische Dokumente digital zu signieren, um so die Integrität des Senders zu garantieren. Der „Oracle TDE Database Key Vault“ sorgt wiederum für die Verschlüsselung des Oracle TDE Datenverschlüsselungs-Keys mit einem Master Key, der seinerseits innerhalb des HSM On Demand-Dienstes abgelegt wird. Mit Hilfe des "Hyperledgers" sichern die zuständigen Mitarbeiter Blockchain-Artifakte über Schlüssel ab, die dann ebenfalls im HSM On Demand-Service landen.

Der letzte Service ist der „Salesforce Key Broker on Demand“. Dieser erzeugt Tenant Secrets für Salesforce und ermöglicht das Verwalten der Schlüssel und Sicherheits-Policies in Zusammenarbeit mit Salesforce Shield.



Das Web-Interface der Lösung mit den vorhandenen Diensten

Der Test

Für unseren Test stellte uns Gemalto einen Test-Account zur Verfügung, über den wir die Funktionalität der Lösung unter die Lupe nehmen konnten. Wir legten unter diesem Account diverse Test-Benutzer an und aktivierten diverse Dienste, um unsere Testdaten – wie zum Beispiel den Key einer Zertifizierungsstelle – abzusichern. Dabei konzentrierten wir uns besonders auf das Management der Lösung und die Arbeit im laufenden Betrieb.

Die ersten Arbeitsschritte

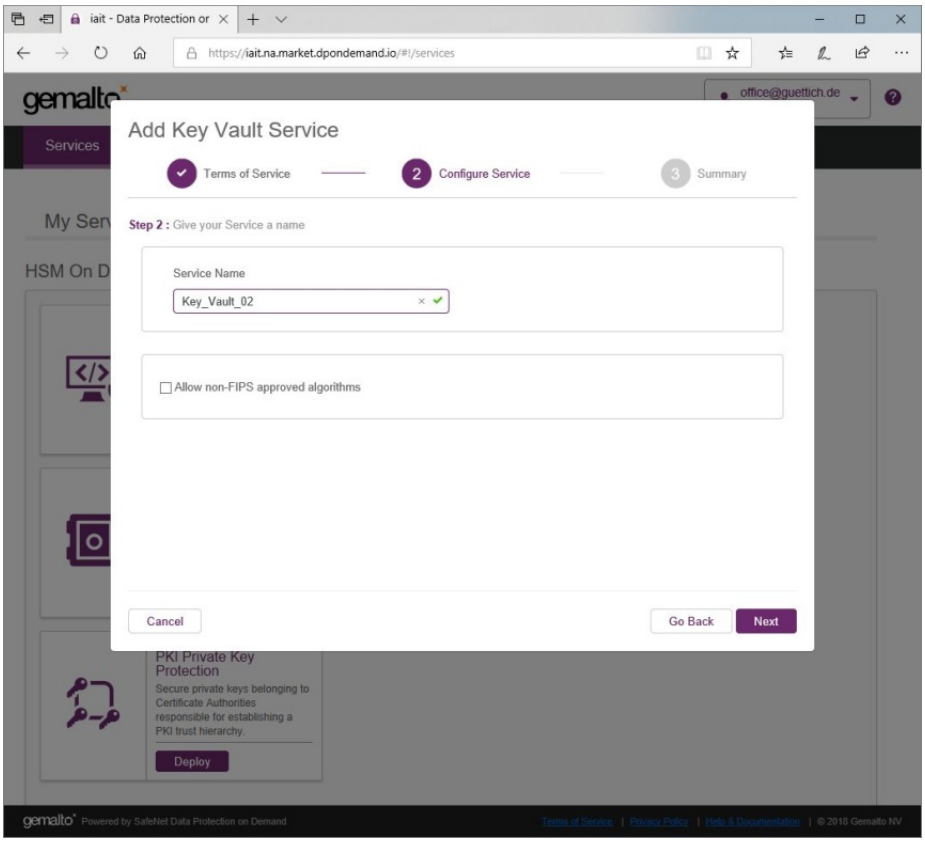
Nach dem ersten Login bei dem genannten Test-Account, forderte uns die Lösung zunächst einmal dazu auf, unser Passwort, das wir zuvor per Mail erhalten hatten, zu ändern. Das ist gut, weil das System so dafür sorgt, dass keiner mit potentiell unsicheren Passwörtern auf die Dienste zugreift.

Sobald wir unser Passwort modifiziert hatten, machte uns das Management-Tool darauf aufmerksam, dass keine „Application Owners“ im System vorhanden waren. Unser eigener Test-Account arbeitete als „Tenant Administrator“ und war folglich dazu gedacht, die Benutzer und Administratoren im System zu verwalten. Im nächsten Schritt legten wir folgerichtig ein Applikationsbesitzerkonto an. Dazu benötigt die Lösung eine so genannte Subscriber Group. Diese generierte sie im Test gleich während der Konfiguration des Kontos und fügte ihr in der Folgezeit den Besitzer-Account hinzu. Die Definition der Konten erfolgt mit einer E-Mail-Adresse und einem Passwort. Auch die Nutzer der neuen Accounts müssen nach der ersten Anmeldung sofort ihre Passwörter ändern.

Der erste Dienst

Nach dem Login als „Application Owner“ sieht man eine Übersicht der vorhandenen Dienste, also „Digital Signing“, „Hyperledger“, „Key Vault“, „Oracle TDE Database“, "Salesforce Key Broker" und „PKI Private Key Protection“. Im ersten Schritt wollten wir einen Key Vault erzeugen. Das Hinzufügen der Dienste zum eigenen Account läuft immer nach dem gleichen Schema ab: Zunächst klickt der Mitarbeiter auf den Eintrag des entsprechenden Dienstes.

Daraufhin zeigt das System ihm die Terms of Service an, die er annehmen muss. Danach fragt die Lösung nach einem Namen für den Dienst und wollte im Fall des Key Vaults auch noch wissen, ob Algorithmen, die nicht FIPS-konform sind, zugelassen werden sollten. Nachdem die entsprechenden Angaben gemacht wurden, zeigt das System einen Überblick über die durchzuführenden Schritte an und konfiguriert anschließend den Dienst, was ein paar Sekunden in Anspruch nimmt. Danach bietet die Lösung an, auch gleich den Client Service zu erstellen, der auf dem Zielsystem im Unternehmen zum Einsatz kommt. Sobald das erledigt ist, sind die zuständigen Mitarbeiter dazu in der Lage, diesen Client herunterzuladen und auf dem von ihnen dafür vorgesehenen Rechner einzuspielen.



Das Anlegen eines Dienstes läuft über einen einfachen Wizard ab

Die Konfiguration des Key Vaults

Nach dem Herunterladen entpackten wir zunächst einmal das Zip-Paket mit der Client-Software auf unserem Testrechner, der unter Windows Server 2012 R2 lief. Als Software hatten wir auf diesem System nur die aktuellen Updates von Microsoft eingespielt. Da in der Dokumentation von Gemalto angegeben war, dass zum Betrieb des Clients zwingend das Microsoft Visual C++ 2015 Redistributable Update 3-Paket erforderlich war, installierten wir dieses ebenfalls.

Im nächsten Schritt mussten wir den Inhalt des Zip-Files "cvclient-min.zip", das sich innerhalb des ursprünglichen Client Zip-Pakets befand, in den gleichen Ordner entpacken, wie das originale Installation Package. Zum Schluss war es noch erforderlich, die Datei "setenv.cmd" als Administrator auszuführen, um die Umgebungsvariable zu setzen. Danach konnten wir den Dienst durch den Aufruf der Datei "lunacm" starten.

Die Konfiguration des Dienstes

Um mit dem Dienst arbeiten zu können, waren jetzt ein paar Konfigurationsschritte erforderlich. Um eine HSM Applikationspartition zum Speichern kryptografischer Objekte für die genutzten Anwendungen bereit zu stellen, mussten wir die Rollen für den Security Officer (SO), den Crypto Officer (CO) und den Crypto User (CU) initialisieren. Die dazu benötigten Schritte finden sich alle in der Dokumentation, so dass wir an dieser Stelle nicht weiter darauf eingehen müssen. Es genügt zu sagen, dass das Einrichten des Dienstes im Test keine fünf Minuten in Anspruch nahm und dass der Key Vault anschließend zur Verfügung stand.

Nachdem wir den Dienst in Betrieb genommen hatten, verwendeten wir das zum Lieferumfang des Clients gehörende Testprogramm "ckdemo", um Schlüssel zu erstellen, Session Informationen abzufragen und so weiter, um so sicherzustellen, dass alles so funktionierte, wie vorgesehen. Dabei kam es zu keinen Überraschungen.

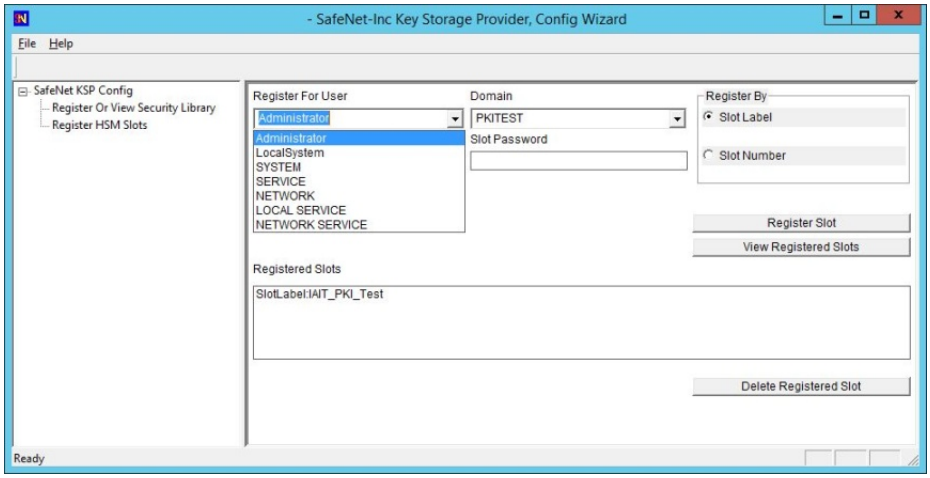
Die Arbeit mit der Private Key Protection

Im nächsten Testschritt nahmen wir uns den Dienst „Private Key Protection“ vor. Mit

diesem wollten wir einen CA-Key absichern, um die Arbeit mit SafeNet Data Protection on Demand in der Praxis unter die Lupe zu nehmen. Dazu loggten wir uns wieder als Application Owner bei unserem Testkonto ein und erstellten über den Befehl "Add New Service" einen PKI Private Key Protection-Dienst. Auch hier mussten wir zunächst die Terms of Service akzeptieren und konnten dann dem Dienst einen Namen geben und festlegen, ob nicht FIPS-konforme Algorithmen zugelassen sein sollten.

Nachdem der Dienst erstellt war, erzeugten wir wieder den Dienst-Client und luden ihn auf unser Testsystem herunter. Die Installation des Service läuft genau so ab, wie bei dem Key Vault Dienst. Die Client-Software legt im Betrieb übrigens nur eine Konfiguration an, über die das System auf den Service zugreifen kann und muss deswegen im laufenden Betrieb nicht immer aktiv sein. Das Aussehen der verwendeten Konfiguration hängt von der zum Einsatz kommenden Applikation ab und wird in der Dokumentation auf der Webseite des Data Protection on Demand-Dienstes für die relevanten Anwendungen genau beschrieben. Wir nahmen uns an dieser Stelle den "Microsoft Active Directory Certificate Services Integration Guide" vor, und setzten unsere CA so auf, dass ihr Key über den Dienst abgesichert wurde.

Dazu mussten wir zunächst einmal in den Unterordner "KSP" der Client-Installation wechseln und dort mit Hilfe des Tools "KspConfig.exe" unsere Security-Library (eine DLL, die ebenfalls zum Lieferumfang des Clients gehört) sowie den vorhandenen HSM-Slot (für die über den Service angebotene HSM on Demand-Lösung) registrieren. Der Slot muss für den Betrieb der Lösung zweimal registriert werden, einmal für den Administrator der aktuellen Domäne und einmal für das Systemkonto der Domäne "NT Authority". Als Slot-Passwort verwendeten wir bei der Registrierung das Passwort des zuvor angelegten Crypto Officers, da dieser auch das Recht hat, in der Dienstpartition zu schreiben. Sobald das erledigt war, machten wir uns daran, auf dem Server, den wir als Domänencontroller eingerichtet hatten, die Active Directory Zertifizierungsdienste einzuspielen. Dazu führten wir mit dem Server Manager eine Standardinstallation einer Zertifizierungsstelle durch.



Das Tool „KspConfig“ bei der Registrierung des Slots

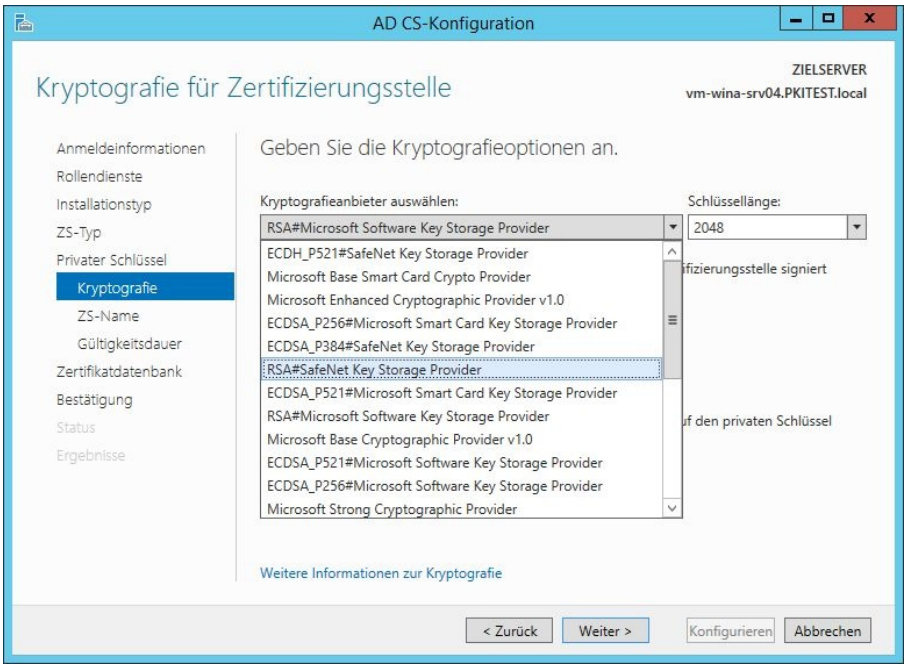
Konfiguration der Zertifizierungsstelle

Nach dem Abschluss des Setups konfigurierten wir die Zertifizierungsstelle mit Hilfe des dafür vorgesehenen Wizards. Dabei richteten wir das System als Unternehmenszertifizierungsstelle und als "Root CA" ein. Anschließend versuchten wir, einen neuen Private Key für die CA zu erzeugen. In der Dokumentation von Gemalto steht, dass man dazu einen Cryptographic Service Provider (CSP) von SafeNet aus dem dazugehörigen Drop-Down-Menü auswählen solle. Leider erschien bei uns kein solcher Provider in der Konfigurationsauswahl, er waren lediglich Provider von Microsoft vorhanden.

Deswegen kontaktierten wir an dieser Stelle den Support des Herstellers, der uns sagte, dass es mit dem Tool KspConfig nicht nur möglich sei, den zu verwendenden Slot mit seinem Namen zu registrieren, wie wir es getan hatten, sondern auch mit seiner Slot ID. Manchmal solle es helfen, die Registrierung über die Slot ID durchzuführen um unser genanntes Problem zu beseitigen. Wir löschten daraufhin die vorhandenen Registrierungen und führten sie erneut mit Hilfe der Slot ID durch. Leider brachte das keine Bes-

serung, auch nicht nach einem Neustart des Rechners. Daraufhin wies uns der Support an, zu überprüfen, ob sich die Datei "SafeNetKsP.dll", die ebenfalls zum Lieferumfang des Clients gehörte, im Verzeichnis "C:\Windows\System32" befand. Das war bei unserer Testinstallation nicht der Fall, wir kopierten die Datei folglich in das genannte Verzeichnis und konnten anschließend tatsächlich auf die SafeNet-CSPs zugreifen. Danach machten wir uns daran, die Konfiguration abzuschließen. Dazu mussten wir zunächst mit dem Befehl "sc query certsvc" prüfen, ob der CA-Dienst aktiv war und über "certutil -verifykeys" den CA-Key verifizieren.

Bei dieser Gelegenheit stellten wir fest, dass der CA-Dienst auf unserem System stets wenige Sekunden nach seinem Start wieder anhielt. Auch hier mussten wir wieder den Support kontaktieren, der uns darauf hinwies, dass dies an unserem deutschen Windows Server 2012 R2 liege. Wir hatten ja zuvor mit Hilfe des Tools KspConfig.exe unseren HSM-Slot für das Administrator- und das Systemkonto registriert. Bei dem Systemkonto lautete die dazugehörige Domäne „NT Authority“. Eine andere Bezeichnung für diese Domäne bot uns das Tool auch nicht an. Auf einem deutschen Server heißt die korrekte Bezeichnung aber „NT-Autorität“. Das Problem ließ sich durch eine Neuregistrierung des Slots über den Kommandozeilenbefehl „kspcmd.exe password /s {Partitionsname} /u SYSTEM /d NT-AUTORITÄT“ lösen. Danach war die Integration des Active Directory Zertifikatdienstes in den HSM on Demand-Service komplett und wir konnten das System nutzen, um Keys zu archivieren, wiederherzustellen und ähnliches. Die Konfiguration geht im Prinzip schnell von der Hand und wird keinen Administratoren vor unüberwindbare Herausforderungen stellen, allerdings wurde von unserer Seite eine Anpassung angeregt, um jegliche Missverständnisse auszuschließen. Im Zuge des Tests hat Gemalto reagiert. Der Hersteller gibt an, dass mittlerweile die Konfigurationswerkzeuge überarbeitet wurden.



Nach einigem Hin und Her erschien auch SafeNet als Kryptografieanbieter in der Zertifikatsdienstekonfiguration

Fazit

Mit SafeNet Data Protection on Demand bietet Gemalto einen äußerst interessanten Dienst an, der das Potential hat, Code Signing, Verschlüsselung und Key Management auch solchen Unternehmen zugänglich zu machen, denen der dafür erforderliche Aufwand und die damit verbundenen Kosten bislang zu viel waren. Nutzer dieses Services müssen keine spezielle Hardware anschaffen und verwalten und alle Kunden zahlen nur für die Dienste, die sie auch tatsächlich nutzen.

SafeNet Data Protection on Demand kann auch beim Erreichen von DSGVO-Konformität (in Zusammenhang mit dem „Recht auf Vergessen“) von großer Hilfe sein, da sich die gespeicherten Daten und Schlüssel jederzeit einfach löschen lassen. Bei uns im Test konnte die Lösung überzeugen, da sie sich verhältnismäßig schnell einrichten und auch relativ einfach nutzen ließ. Die Dokumentation ist ausführlich und der Support überzeugte. Die oben genannten Probleme mit den Konfigurations-Tools und der Lokalisierung dürften in kürzester Zeit beseitigt sein, falls das nicht bereits geschah.