cpl.thalesgroup.com

THALES

Cloud-basiertes HSM mit SafeNet Data Protection on Demand im Vergleich zu On-Prem HSM: Ein Vergleich der Gesamtbetriebskosten

Wählen Sie die kostengünstigste Lösung für Ihre Krypto-Sicherheit

White Paper

Inhalt

Cloud-basiertes HSM im Vergleich zu On-Prem HSM: Wie wählen Sie die richtige Lösung für die Krypto-Sicherheit Ihres Unternehmens aus? Und wie vergleichen Sie die Gesamtbetriebskosten (TCO) einer Vorabinvestition in ein vor Ort bereitgestelltes HSM mit umlagefinanzierten Cloud-basierten HSM-Diensten? In diesem Dokument beschäftigen wir uns mit einer Checkliste der Funktionen, die Sie bei der Wahl eines HSM berücksichtigen sollten. Anschließend werfen wir einen Blick auf den Primäraufwand, den Sie bei der Gegenüberstellung der Gesamtbetriebskosten einbeziehen sollten und stellen Ihnen abschließend ein Anwendungsbeispiel für eine mögliche Bewertung der Gesamtbetriebskosten vor.

Überblick

Unternehmen erhöhen ihre Cybersicherheit, um die zunehmende Zahl unterschiedlicher IT-Systeme zu schützen, Vertragspflichten zu erfüllen und neuen Datenschutzverordnungen zu entsprechen. Das hat dazu geführt, dass die Notwendigkeit, Daten mithilfe von Mechanismen wie Verschlüsselung sichern zu müssen, ein wichtiger Bestandteil unseres Alltags geworden ist. Für die meisten Unternehmen bedeutet dies, dass Hardware-Sicherheitsmodule (HSM) sich zunehmend durchsetzen und immer wichtiger für den Schutz sensiblen Schlüsselmaterials werden, das eingesetzt wird, um die Verschlüsselung wichtiger Daten sowie Managementanwendungen und Online-Transaktionen zu schützen.

Ein traditionelles, vor Ort bereitgestelltes HSM stellt jedoch hinsichtlich der benötigten finanziellen Mittel und Ressourcen eine bedeutende Investition dar. Daher wissen gebeutelte CIOs und IT-Leiter mit schmalen IT-Budgets und knappen Ressourcen häufig nicht, wie Sie diese Ausgaben rechtfertigen oder die entsprechende Sachkenntnis für den Aufbau und den Support der Infrastruktur finden können.

Gleichzeitig verändert sich die IT-Landschaft. Unternehmen migrieren ihre Anwendungen Schritt für Schritt von Rechenzentren vor Ort in die Cloud. Die renommierte Zeitschrift Forbes berichtet, dass 83 % des Arbeitsaufkommens von Unternehmen bis 2020 in die Cloud verlagert sein wird, und viele weitere Medienberichte sprechen davon, dass Unternehmen für den Wechsel in die Cloud eine „All-in"-Strategie verfolgen. Die Sicherheitsanforderungen eines Wechsels in die Cloud und die steigende Zahl an Datenschutzverletzungen (siehe: https://breachlevelindex.com) haben dazu geführt, dass die Sicherung von Verschlüsselungs- und Schlüsselverwaltungsrichtlinien immer wichtiger wird. Dieser Umstand hat eine neue HSM-Lösung hervorgebracht: HSM-as-a-Service oder Cloud-HSM, die auf dem On-Demand-Bereitstellungsmodell der Cloud basieren.

Thales hat mit SafeNet Data Protection On Demand (DPoD) eine einzigartige HSM-as-a-Service-Lösung entwickelt. Es handelt sich um eine Cloud-basierte Plattform, die eine Vielzahl an auf Abruf bereitgestellten HSM-Diensten sowie Schlüsselverwaltungs- und Verschlüsselungsdiensten über einen einfachen Online-Marktplatz anbietet. Dieser Dienst ergänzt die marktführenden, vor Ort bereitgestellten SafeNet Luna und Payment HSMs sowie das umfangreiche Portfolio an Datensicherheitslösungen von Thales.

Aber woher wissen Sie, welche Lösung die richtige für Ihr Unternehmen ist? Und wie vergleichen Sie die Gesamtbetriebskosten (TCO) einer Vorabinvestition in ein vor Ort bereitgestelltes HSM mit umlagefinanzierten Cloud-basierten HSM-Diensten?

In diesem Dokument beschäftigen wir uns mit einer Checkliste der Funktionen, die Sie bei der Wahl eines HSM berücksichtigen sollten. Anschließend werfen wir einen Blick auf den Primäraufwand, den Sie bei der Gegenüberstellung der Gesamtbetriebskosten einbeziehen sollten und stellen Ihnen abschließend ein Anwendungsbeispiel für eine mögliche Bewertung der Gesamtbetriebskosten vor.

Lassen Sie uns zunächst die Unterschiede zwischen den beiden HSM-Modellen betrachten.

On-Prem HSM und SafeNet Data Protection on Demand

Bei einem vor Ort bereitgestellten HSM und SafeNet Data Protection On Demand (in diesem Dokument als DPoD abgekürzt) handelt es sich um exakt die gleiche kryptographische Technologie, die aber auf unterschiedliche Weise bereitgestellt wird.

Vor Ort bereitgestellte HSMs sind aktuell das bekanntere Modell. Der Kunde kauft die Hardware vorab, installiert und konfiguriert sie vor Ort und ist während der gesamten Lebensdauer des Geräts bzw. der Geräte für deren Verwaltung verantwortlich.

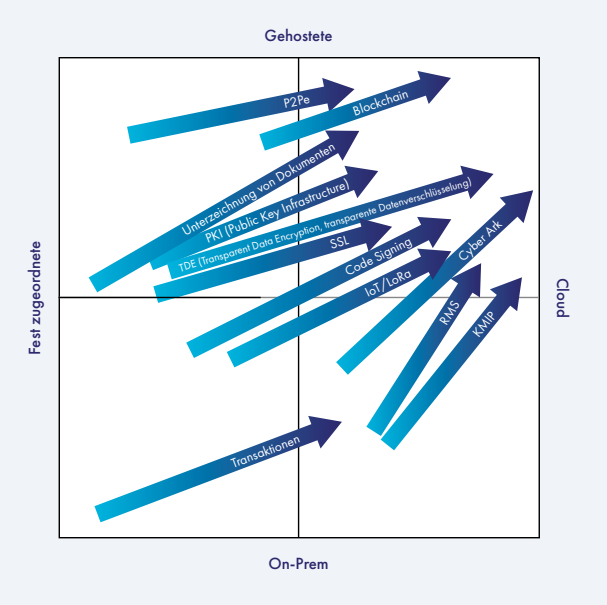
Bei DPoD handelt es sich hingegen um eine vollständig verwaltete Ressource. Thales hat in seinen eigenen Rechenzentren eine skalierbare Plattform aufgebaut, über die sie sichere Verschlüsselungsdienste als SaaS-Lösung bereitstellen. Der DPoD-Dienst ist vorkonfiguriert und bietet standardmäßig Redundanz, Widerstandsfähigkeit und hohe Verfügbarkeit.

Im Allgemeinen hängt die Entscheidung zwischen vor Ort bereitgestellten HSM und einer DPoD-Lösung im Großen und Ganzen von den allgemeinen langfristigen Gesamtbetriebskosten ab. Gleichzeitig eignet sich das einzelne Modell auch jeweils für andere, spezifische Anwendungsfälle und Kundenanforderungen.

On-Prem HSM

Vor Ort bereitgestellte HSMs sind auch weiterhin für Unternehmen von Bedeutung, die die alleinige Kontrolle über kryptographische Schlüssel und Richtlinien benötigen. Sie sind außerdem für die Sicherung von Anwendungen sinnvoll, die im gleichen Rechenzentrum vor Ort untergebracht sind. Dies führt zu geringerer Latenz, da die Hardwarekomponenten, die von einer Anwendung verwendet werden, näher beieinanderliegen – vorausgesetzt, sie befinden sich alle am selben Standort.

Darüber hinaus ziehen es einige Unternehmen vor, aufgrund von Architekturbeschränkungen bzw. hohen Sicherheits- und/oder Leistungsanforderungen speziell für Anwendungen mit intensiven kryptographischen Operationen ihre eigenen HSMs vor Ort bereitzustellen.



Die folgende Abbildung veranschaulicht, dass DPoD für immer mehr Anwendungen in Frage kommt, für die bislang HSMs verwendet werden. Der Pfeil zeigt die voraussichtliche Entwicklung in den nächsten zwei bis drei Jahren. Je näher der Pfeil der rechten oberen Ecke kommt und je dunkler er dargestellt ist, desto besser ist die Anwendung für einen Cloud-basierten HSM-Dienst geeignet. Diese Darstellung lässt darauf schließen, dass die Cloud für unterschiedliche Anwendungen oder Anwendungsfälle unmittelbar von Belang ist und dass in den kommenden zwei bis drei Jahren weitere Anwendungsfälle folgen werden, da Cloud-HSM-Dienste stetig an Bedeutung gewinnen. Bis zu diesem Punkt ist es daher wahrscheinlich, dass viele Unternehmen schließlich auf hybride Infrastrukturen setzen werden.

HSM-Anwendungen

Nutzung in den kommenden zwei bis drei Jahren

Data Protection On Demand

SafeNet Data Protection On Demand (DPoD) eignet sich wie auch andere Cloud-HSM-Dienste perfekt für eine Vielzahl von Anwendungen, DevOps, SecOps, abteilungsspezifische Anforderungen geringeren Ausmaßes, Start-ups sowie kleine und mittlere Unternehmen, die alle unter Umständen nicht über die Mittel oder die interne Expertise verfügen, um die komplexe Einrichtung und Wartung einer Bereitstellung vor Ort stemmen zu können. Darüber hinaus entscheiden sich viele größere Unternehmen dafür, die Vorteile eines Cloud-Dienstes zu nutzen, obwohl sie über die notwendigen internen Ressourcen verfügen, und ihr Angebot durch ein Cloud-HSM zu erweitern, unter anderem da es skalierbar ist und ausschließlich als Betriebsausgabe verbucht werden kann. DPoD eignet sich unabhängig von der Größe oder den verfügbaren Ressourcen im Prinzip für alle Unternehmen, die die Abrufbarkeit, Beweglichkeit und Elastizität der Cloud nutzen möchten.

Probieren Sie die Testversion eines Produkts aus, bevor Sie sich an einen bestimmten Anbieter binden. Sie können Pilotprojekte ohne große Vorabinvestitionen durchführen, Dienste innerhalb von Minuten anstatt Wochen bereitstellen, und ihre Ressourcen je nach Kapazitätsanforderungen herauf- oder herunterskalieren.

Bei Cloud-HSM-Diensten haben Sie die Wahl zwischen zwei Kategorien von Diensten:

Öffentliche Cloud-HSM-Dienste

Hierbei handelt es sich um die HSM-Lösungen der Anbieter öffentlicher Clouds. Während die führenden Anbieter von Cloud-Plattformen, Azure und AWS, sowohl Cloud-HSMs für einzelne Kunden (Single Tenant) als auch einen alternativen Schlüsselverwaltungsdienst (KMS) für mehrere Kunden (Multi-Tenant) anbieten, neigen andere dazu, ausschließlich auf Multi-Tenant-Lösungen zu setzen. Gängige Beispiele sind unter anderem Oracle Key Vault und Google Cloud KMS. In diesem Dokument befassen wir uns ausschließlich mit HSM-Technologie.

Öffentliche Cloud-HSM-Dienste setzen in der Regel auf Einfachheit. Dies geht häufig zu Lasten der Funktionalität. Darüber hinaus sind sie speziell auf einen Cloud-Anbieter zugeschnitten. Das heißt, sie eignen sich im Allgemeinen nur für Unternehmen, die an einen einzigen Cloud-Anbieter gebunden sind.

HSM-Dienste Dritter

HSM-Dienste Dritter wie z. B. DPoD, unterstützen mithilfe eines zentralen Verwaltungsportals eine Reihe unterschiedlicher Cloud-Plattformen. Daher eignen sie sich besser für Unternehmen mit Multi-Cloud-Strategien, die sie dabei unterstützen, die logistische Komplexität verschiedener Schlüsselverwaltungsmethoden unterschiedlicher Cloud-Umgebungen zu bewältigen.

Sie sind häufig ausgereifter als öffentliche Cloud-HSM-Dienste, die einen höheren Grad der Automatisierung für Aufgaben wie Online-Backups, Lastverteilung und Skalierung bieten.

Bestimmte Cloud-HSM-Dienste Dritter werden als „Click and Deploy"-Lösung in Form eines Online-Marktplatz für modulare Dienste angeboten. DPoD ist ein führendes Beispiel für diese Art von Diensten. Sie ermöglichen es Ihnen, nur die Lösungen zu kaufen, die Sie für bestimmte Anwendungsfälle benötigen. Dadurch reduzieren sie Ihre Kosten für die Datensicherheit. Die Dienste umfassen allgemeine Schlüsselverwaltung und Verschlüsselung für spezifischere Anwendungen wie Key Vault, digitale Unterschriften und Oracle TDE zur Speicherung von Schlüsselverschlüsselungsschlüsseln (Key Encryption Key, KEK).

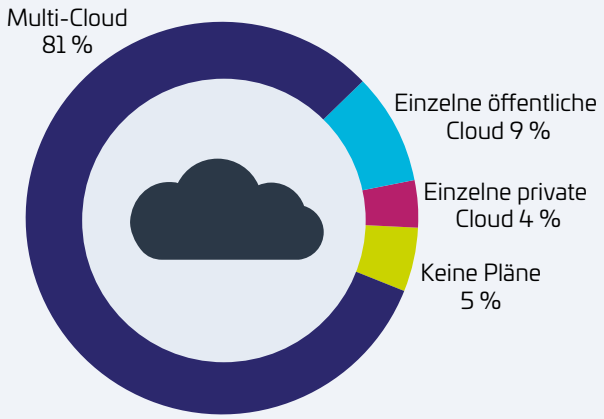
Die zentrale Rolle von HSM-Diensten Dritter

Laut dem RightScale's 2018 State of the Cloud Report, verfolgen **81 %** der Unternehmen heute eine Multi-Cloud-Strategie.

Dieser bestehende Trend hin zu Multi-Cloud-IT hebt die Wichtigkeit von DPoD-Lösungen hervor, die für eine Vielzahl von Cloud-Umgebungen einsetzbar sind.

Cloud-Strategie von Unternehmen

Mehr als 1.000 Mitarbeiter



Quelle: RightScale 2018 State of the Cloud Report

Checkliste Funktionen

Vor einem gegenüberstellenden Vergleich sollten Sie zunächst entscheiden, welche Funktionen Sie tatsächlich benötigen.

Alle HSMs, unabhängig davon, ob diese vor Ort bereitgestellt werden oder Cloud-basiert sind, sollten diese absoluten Mindestanforderungen erfüllen:

- Sichere Speicherung des kryptographischen Materials
- Sichere kryptographische Ausführungsumgebung (Schlüsselerstellung, Verwaltung, Funktionsausführung)
- Strikte Aufgabentrennung
- Strikte Trennung logischer Daten und Zugangsdaten (bei partitionierten bzw. Multi-Tenant-Lösungen)
- Zertifizierte physische und logische Sicherheitsmechanismen (Schutz gegen Manipulationen und Angriffe)
- Mechanismen für Ereignisprotokollierung und das Erstellen von Prüfberichten
- Sichere API für den Zugriff auf das HSM (PKCS#11, RESTful und andere)

Aber nicht alle HSM sind gleich angelegt. Sie zeichnen sich durch unterschiedliche Funktionsgrade, Sicherheitsniveaus, Benutzerfreundlichkeit usw. aus – all dies kann sich auf Ihre Gesamtbetriebskosten auswirken.

Im Folgenden finden Sie einige übliche Funktionen, die ganz oben auf Ihrer Prioritätenliste stehen sollten:

Sicherheit: FIPS und Common Criteria geben in Bezug auf Compliance-Anforderungen unterschiedliche Erfüllungsgrade vor. Daher ist die Zertifizierung der einfachste Weg, die Sicherheit eines Geräts stichprobenartig zu überprüfen. Dennoch sollten Sie stets beachten, dass die Zertifizierung sich auf die Hardware-spezifischen Kriterien bezieht und daher nicht notwendigerweise Sicherheit garantiert. Außerdem können Sie die Sicherheit eines Geräts beurteilen, indem Sie den Ruf des HSM-Anbieters prüfen und herausfinden, wozu andere Unternehmen dieses Produkt verwenden. Bei Cloud-Service-Anbietern ist es möglicherweise auch wichtig, darauf zu achten, inwieweit sie Wert auf physische und logische Sicherheit legen und nach ISO27001 und SOC2 zertifiziert sind.

Geografischer Standort: Gesetzliche Vorschriften geben unter Umständen vor, wo Daten gespeichert und wie diese Daten weitergegeben werden dürfen, selbst innerhalb des Unternehmens. Einige Unternehmen wählen bewusst Cloud-HSM-Dienste, die für eine bestimmte Region, z. B. Europa oder Nordamerika, angeboten werden.

Krypto-Agilität: Branchenübliche Algorithmen sind im Allgemeinen proprietären Algorithmen vorzuziehen. Manche Anwendungsfälle erfordern jedoch den Einsatz spezifischer Algorithmen oder Algorithmenfamilien. Damit gesetzliche Vorgaben eingehalten werden, können alte Algorithmen auf schwarzen Listen stehen oder abgelehnt werden. Ein HSM stellt eine Reihe von symmetrischen und asymmetrischen Krypto-Algorithmen bereit, die zur symmetrischen/asymmetrischen Verschlüsselung sowie für Unterschriften, Zeitstempel, Authentifizierung und sonstige Funktionen verwendet werden. Behörden und Organisationen wie das NIST oder ANSI, Branchengremien wie GSMA (für Machine-to-Machine, IoT) oder ETSI (Telekommunikationsnormen, Smartcards) und andere legen unter Umständen bestimmte Algorithmen/Schnittstellen für Anwendungen oder Branchen in ihrem Wirkungsbereich fest. Fragen Sie Ihren Anbieter, inwieweit dieser zukünftige Technologien wie Quantum unterstützt.

Random Number Generation (RNG): Die Verwendung zertifizierter Zufallsgeneratoren (Random Number Generators, RNG) kann ein Faktor bei der Einhaltung bestimmter Vorschriften oder Vorgaben sein. Prüfen Sie daher, ob der Anbieter ein zugelassenes bzw. zertifiziertes Verfahren anwendet.

Schlüsselsicherung: Die Sicherung von Schlüsselmaterial sollte nur in einer Umgebung erfolgen, die das gewünschte Sicherheitsniveau wie vom HSM bereitgestellt bietet. Ein weiterer wichtiger Faktor ist die Fähigkeit, Remote-Backups oder die Replikation kryptographischen Materials zu verwalten.

Benutzeroberfläche: HSMs werden größtenteils über eine Befehlszeile verwaltet. Dennoch werden häufig Benutzeroberflächen für „Krypto-Verwaltung" angeboten, um die HSM-Verwaltung, die Bereitstellung des HSM-Client und sonstige Lebenszyklusaktivitäten zu vereinfachen. Das erfordert spezifische Kenntnisse in Bezug auf HSMs, die die meisten Unternehmen nicht besitzen, bzw. den Erwerb des erforderlichen Fachwissens. Dies wiederum übersteigt möglicherweise die Kernkompetenzen vieler Unternehmen, vom Budget ganz zu schweigen. Darüber hinaus sind selbst große Unternehmen mit internen HSM-Teams, die die vorhandenen Geräte verwalten, nicht in der Lage, ihre Kapazitäten auszubauen, wenn sich ihre Anforderungen ändern.

Integration von Anwendungen: Eine große Auswahl an Integrationen wird immer wichtiger werden. Da Ihre IT-Vorgänge zunehmen und die gesetzlichen Vorgaben sich ändern, ist es wahrscheinlich, dass Sie mehr als die eigentliche Anwendung sichern müssen. Wählen Sie daher einen Anbieter mit mehreren bewährten Integrationen, mit denen Sie auch in Zukunft ausreichend versorgt sind.

Automatisierung: Zusätzlich zum Aufbau der HSM-Infrastruktur sind die Bereitstellung und fortlaufende Verwaltung der Lösung wichtige Faktoren. Um diese effektiv umzusetzen, empfehlen wir, einen Cloud-HSM-Dienst zu wählen, der die Automatisierung zumindest einiger Prozesse wie Bereitstellung und Integration der Clients sowie die Verwaltung laufender Aktualisierungen anbietet.

Schlüsselmigration: Die Fähigkeit, existierende Schlüssel in eine neue Umgebung zu übertragen, ist wichtig, um die Servicekontinuität Ihrer Anwendungen zu wahren. Einige HSMs bieten heute einfache Migrationsfunktionen.

Wichtige Kostenfaktoren

Nachdem Sie sich nun entschieden haben, welche HSM-Funktionen Sie für Ihre Anwendungen und Ihren Sicherheitsstatus benötigen, können Sie die Gesamtbetriebskosten einer vor Ort bereitgestellten Lösung mit denen von DPoD vergleichen. Dabei sollten Sie insbesondere die folgenden Kostenfaktoren berücksichtigen:

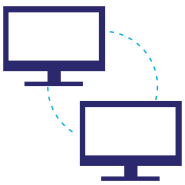
HSM Hardware

Eine Bereitstellung vor Ort eignet sich in der Regel für eine Reihe von unternehmenskritischen Anwendungen. Sie umfasst üblicherweise zwei HSMs und ein Backup-HSM an den einzelnen geografischen Standorten, damit Resilienz und hohe Verfügbarkeit garantiert sind.

All dies stellt eine bedeutende Investition in Infrastruktur und Konfiguration dar. Eine Cloud-basierte HSM-Lösung wie z. B. DPoD kann dagegen sofort eingesetzt werden und erfordert keine zusätzliche Hardware.

Tool für die Kryptoverwaltung

Ein Tool für die Kryptoverwaltung ist ein Hypervisor, der ein Netzwerk aus HSMs verwaltet. Es übernimmt die zentrale Verwaltung der HSM-Ressourcen wie Partitionierung, Fehlerbehebung, Überwachung und Alarmierung. Es ist zudem ein wichtiger Aspekt bei der Orchestrierung und Automatisierung der Bereitstellung der HSM-Clients in der Anwendungsumgebung. Viele dieser Art von Funktionen sind standardmäßig in DPoD enthalten.



Netzwerk und Infrastruktur

Dem Aufbau einer Infrastruktur zur Unterstützung eines widerstandsfähigen IT-Dienstes sollte beim Vergleich zwischen vor Ort bereitgestellten und cloudbasierten Diensten besondere Aufmerksamkeit gewidmet werden. Dies ist daher auch bei einem HSM-Ausbau von Belang – wenn Netzwerke, Router, Load Balancer, Server usw. erforderlich sind, um die Vorgaben eines Unternehmens an widerstandsfähige HSMs umzusetzen.

Viele Kunden nannten auch die Zeit, die Netzwerkteams benötigen, um die Infrastruktur für die Vor-Ort-Bereitstellung von HSMs vorzubereiten, als einen wichtigen Faktor in Ihren Überlegungen – der bei Cloud-basierten Diensten keine (oder nur eine geringe) Rolle spielt. Für einen Cloud-basierten Dienst wie DPoD benötigen Sie nichts weiter als Zugang zu den IP-Adressen und Ports.

Sicherheit

Der Aufbau einer sicheren Infrastruktur rund um Ihre HSMs ist ein wichtiger Faktor, um jegliches Risiko zu mindern. Daher stellt die strikte Überwachung von Firewalls, Anti-Virus-Software und sonstigen Aspekten, die dafür sorgen, dass diese Elemente stets mit den neusten Patches ausgerüstet und aktuell sind, einen bedeutenden Ressourcenaufwand und einen Risikofaktor dar. All diese Elemente sind in SafeNet Data Protection on Demand integriert.

Rechenzentrumsumgebung

Hinsichtlich der erforderlichen Stellfläche, des Strombedarfs sowie die Umweltaspekte und der für den Aufbau einer widerstandsfähigen HSM-Infrastruktur benötigten Ressourcen, sollten Sie überlegen, welche Standorte Sie für Ihre Rechenzentren wählen, wie diese Standorte miteinander vernetzt sind und welche Ressourcen Sie benötigen, um diese Umgebungen zu verwalten und zu überwachen.

Zahlungsmodell

Der Kauf eines vor Ort bereitgestellten HSMs kann sich basierend auf dem CAPEX-Modell auf wenige bis viele Tausend Dollar belaufen, je nachdem, welchen Funktionsumfang und welches Sicherheitsniveau Sie benötigen.

Dagegen stellt der OPEX-Ansatz eines Dienstes wie DPoD einen gangbareren Weg dar, um die Sicherheit von kryptographischen Schlüsseln zu finanzieren. Und nicht nur das – Sie bezahlen nur für die Kapazität und die Dienste, die Sie tatsächlich brauchen. Viele Kunden nutzen nur selten die gesamte Kapazität ihrer HSMs.

Diese unterschiedlichen Zahlungsmodelle erfordern auch verschiedene Ansätze bei der Berechnung der Gesamtbetriebskosten in Bezug auf Kapitalkosten usw.

Einrichtung

Die Einrichtung eines vor Ort bereitgestellten HSM stellt eine gewisse Herausforderung dar und erfordert erhebliche finanzielle Investitionen in Arbeitskräfte, die dieses beschaffen, konfigurieren und in einer Produktionsumgebung bereitstellen. Das kann Tage oder sogar Wochen dauern. Die Einrichtung von DPoD dauert meist nur wenige Minuten. Das reduziert nicht nur die Arbeitskosten drastisch, sondern steigert auch die Agilität Ihres Unternehmens und trägt dazu bei, das Ergebnis durch geringere Projektkosten und/oder kürzere Markteinführungszeiten zu verbessern.

Software

Zusätzlich zu Ihrem Tool für die Kryptoverwaltung benötigen Sie auch entsprechende Software, um auf die Funktionen Ihrer HSMs zuzugreifen. Hierfür sind möglicherweise für jede einzelne Partition bzw. jeden einzelnen HSM-Dienst sowie für jeden einzelnen Client separate Lizenzen erforderlich.

Schnell summieren sich die Lizenzkosten zu einer großen Unternehmenskonfiguration, da Sie separate HSM-Dienste logisch verschiedenen Anwendungen und Standorten zuweisen und Ihre Lizenzen entsprechend erweitern (und pflegen) müssen.

Mit DPoD ist es nicht erforderlich, dass Sie Ihre Softwarelizenzen separat berechnen, da alles im Preis enthalten ist.

Anwendungsintegration

Im Zug der Kalkulation Ihrer Gesamtbetriebskosten sollten Sie auch den Arbeitsaufwand für die Integration Ihrer Anwendungen schätzen. Die Integration jeglicher Art von HSMs in unternehmensinterne Systeme kann zeitaufwändig und kompliziert sein.

Ein guter HSM-Anbieter wird Ihnen eindeutige Anleitungen für die Integration seines Produkts in die üblichen Anwendungen zur Verfügung stellen. DPoD ist beispielsweise standardmäßig mit einer großen Auswahl von Diensten wie Datenbanken, Speicher- und Anwendungsentwicklungstools kompatibel.

Dennoch sollten Sie auch im Fall von DPoD bei der Kalkulation Ihrer Gesamtbetriebskosten die Integrations- und Migrationsaspekte Ihrer Umgebung betrachten.

Technisches Know-how und Schulung

Die Verwaltung einer HSM-Plattform erfordert ein hohes technisches Know-how. Daher sollten Sie auch die Kosten für die Schulung des Personals oder die Einstellung von entsprechend qualifizierten Mitarbeitern in die Beurteilung der Gesamtbetriebskosten einbeziehen. Dies gilt auch für die Bereitstellung Ihrer HSM-Infrastruktur.

Demgegenüber erfordert ein Cloud-basierter HSM weit weniger technisches Know-how. Bei SafeNet Data Protection on Demand wartet Thales die Hardware für Sie. Das macht DPoD insbesondere für Unternehmen, für die kryptographische Sicherheit relatives Neuland ist, zu einer kostengünstigen Option.

Einhaltung gesetzlicher Vorgaben

Die Einhaltung gesetzlicher Vorgaben ist nicht nur eine wesentliche Voraussetzung, sondern eröffnet weitere Geschäftsmöglichkeiten in stark regulierten Sektoren wie dem Gesundheits- und Finanzsektor sowie dem öffentlichen Sektor.

Die Einhaltung von Sicherheitsstandards wie DSGVO, FIPS, PCI-DSS usw. bei Bereitstellungen vor Ort kann ein komplexes Unterfangen sein, dass eine eingehende Kenntnis der Vorschriften und langwierige Verfahren erfordert. Ein Großteil dieses Aufwands ist durch die Verwendung eines anerkannten Cloud-basierten HSM-Dienstes wie SafeNet Data Protection on Demand automatisch abgedeckt. Das trägt dazu bei, die Gesamtbetriebskosten im Vergleich zur Bereitstellung vor Ort zu senken.

Dies trifft insbesondere zu, wenn Zertifizierungen gemäß den Normen SOC2 und ISO27001 wichtig für das Unternehmen, dessen Einhaltung von Branchenvorschriften sowie dessen Prozesse sind.

Operatives Management

Der Vergleich der Gesamtbetriebskosten sollte außerdem den Bereich abdecken, der in der Regel die größten Auswirkungen hat, d. h. die Kosten des operativen Managements. Daher sollten Ihre Zahlen für die Bereitstellung vor Ort den manuellen Arbeitsaufwand für Patches, Skalierung, Erweiterung, Überwachung, Sicherheitsprüfungen, Backup und allgemeines Housekeeping beinhalten.

Obwohl DPoD viele zeitaufwändige operative Aufgaben unnötig macht, müssen Sie dennoch die Lebenszyklusverwaltung, also z. B. die Verwaltung von Benutzerkonten und -berechtigungen, einberechnen. Wir haben diese an spätere Stelle in diesem Dokument in unsere Kalkulation der Gesamtbetriebskosten einbezogen und die Unterschiede zwischen einer Bereitstellung vor Ort und DPoD aufgezeigt.

Servicegrad

Welche Art von Dienstgütevereinbarung benötigen Sie? In Bezug auf ihre HSM-Architektur ist der Bedarf der meisten Unternehmen durch eine Dienstgütevereinbarung mit einer Verfügbarkeit von 99,95 % gedeckt. Zusätzlich zu den Hardwarekosten für den Aufbau einer widerstandsfähigen und hochverfügbaren HSM-Bereitstellung vor Ort, müssen Sie für eine solche Dienstgütevereinbarung auch in Personal und Tools investieren, um einen optimalen Servicegrad zu wahren. Daher sollte die Kalkulation Ihrer Gesamtbetriebskosten auch die Kosten für die Bereitstellung eines technischen Supports und das Beheben von Störungen, für Urlaubsvertretungen für Fachkräfte und laufende Wartungsverträge einbeziehen.

Im Fall von DPoD sind diese Leistungen zumeist Aufgabe von Thales und in Ihrem Vertrag, wie in der Dienstgütevereinbarung festgelegt, enthalten.

Vergleich auf einen Blick

	On-Prem HSM	DPoD-Dienst
Hardware	Erforderliche Hardware einschließlich zweier widerstandsfähiger HSMs plus einem Backup-HSM pro Standort, einer Kryptoverwaltungsplattform und der Netzwerkinfrastruktur.	Bereitgestellt über eine vollständig redundante Cloud-Architektur. Keine Hardware erforderlich
Zahlungsmodell	Hohe Anfangskosten (CAPEX).	Auf Nutzung basierende Abrechnung (OPEX) ohne Anfangskosten.
Einrichtung	Komplexe Einrichtung und Konfiguration	Bereitstellung nach wenigen Clicks („Click and Deploy").
Software	Für jede HSM-Partition und die Verwendung der HSM-Client-Software können Lizenzen erforderlich sein.	In den Kosten enthalten.
Client-Bereitstellung	Komplexe und zeitaufwändige Bereitstellung des Integrationsclient. Qualität der Produktunterlagen variiert je nach Hersteller.	Standardmäßige Bereitstellung einer großen Auswahl von Diensten wie Datenbanken, Speicher- und Anwendungsentwicklungstools.
Technisches Know-how und Schulung	Ein hohes Maß an interner Expertise erforderlich.	Vollständig von hochqualifizierten und erfahrenen Sicherheitsfachleuten verwaltet. Benutzerfreundliches Frontend-Interface. Minimale kryptographische Kenntnisse erforderlich.
Einhaltung gesetzlicher Vorgaben	Komplexe Unternehmungen erfordern eine eingehende Kenntnis geltender gesetzlicher Bestimmungen und Investitionen in zusätzliche Dienste wie z. B. Compliance-Beratung und Überwachungstools.	Verantwortlichkeit des DPoD-Anbieters
Operatives Management	Hoher manueller Arbeitsaufwand einschließlich regelmäßiger Fehlerbehebung, Skalierung, Erweiterung, Überwachung, Sicherheitsprüfung, Sicherung und allgemeiner Organisation.	Vollständig automatisierte, verwaltete Lösung mit geringem Betriebsaufwand.
Servicegrad	Investition in Mitarbeiter sowie Tools und Dienste von Dritten, um technischen Support und Urlaubsvertretungen bereitzustellen sowie Störungen zu beheben.	Dienstgütevereinbarungen für hohe Anforderungen mit Support rund um die Uhr.

Anschauliches Beispiel

Sobald Sie die wichtigsten Faktoren identifiziert haben, die Sie bei der Berechnung Ihrer Gesamtbetriebskosten berücksichtigen sollten, können Sie beginnen, die Zahlen Ihrer Kostenanalyse zu vergleichen.

Einmalige Kosten

Erstellen Sie zunächst eine Liste der einmaligen Kosten für jedes der beiden Bereitstellungsmodelle. Bei Ihrer Kalkulation für vor Ort bereitgestellte HSMs sollten Sie die Vorabkosten für Hardware (und alle fortlaufenden Softwarelizenzen) einbeziehen.

- Zwei widerstandsfähige HSMs
- Ein Backup-Gerät
- Ein Tool für die Kryptoverwaltung

Anschließend sollten Sie die Zeit und Kosten für die Einrichtung schätzen:

Entwurf und Planung der Installation, Konfiguration und Integration

- Prüfung und Übergabe
- Schulung der Mitarbeiter

Wir haben in diesem Dokument einige der Bereiche berücksichtigt, die Sie sich genau ansehen sollten. Die an späterer Stelle in diesem Dokument aufgeführten Berechnungen entsprechen realen Beispielen, die auf einigen typischen Projekten basieren, an denen wir beteiligt waren.

Als nächstes wollen wir die jährlichen Kosten betrachten.

Jährliche Kosten

Ihre Berechnung für die Bereitstellung von HSM vor Ort enthält Kosten für:

- Software-Lizenzen für Kryptoverwaltungsserver für die Bereitstellung einer einfachen GUI-basierten Verwaltungsplattform
- Kosten für die HSM-Partition, um mehrere Anwendungsfälle für die Nutzung Ihrer HSM-Plattform zu ermöglichen
- Lizenzen für HSM-Clients zur Integration in Ihre Anwendungen
- Laufende Support-Lizenzen

Darüber hinaus sollten Sie die laufenden Kosten für Systeme und Infrastrukturverwaltung schätzen. Diese Berechnung erfolgt spezifisch für Ihr Unternehmen. Dennoch stellt das folgende Beispiel, das an unsere interne Kostenanalyse angelehnt ist, die wichtigsten Kosten heraus, die Sie berücksichtigen sollten.

Kostenbereich	Beschreibung der Überlegungen
Beheben von Störungen	Fehler innerhalb der Infrastruktur beheben – entweder vom Servicedesk aus oder mithilfe automatisierter Tools (z. B. Leistung, Speicherplatz, Benutzersupport)
Änderungen der Installation	Umsetzung von Änderungen innerhalb der Infrastruktur, z. B. zusätzlicher Speicherplatz, Arbeitsspeicher, weitere Service Packs usw.
Systemdokumentation	Dokumentation der Infrastruktur, Pflege der Dokumentation und der Konfiguration.
Anti-Virus/ Sicherheitsverwaltung	Garantieren, dass Lösungen und Updates bereitgestellt werden, um den Server und die Infrastruktur zu schützen.
Berichterstattung	Überwachung der Leistung und der Verfügbarkeit des Servers und der Infrastruktur usw.
Housekeeping	Löschen/Archivieren von Protokolldateien, allgemeines Dateimanagement, Speicherplatz freimachen usw.
Verwaltung der Leistungsfähigkeit	Sicherstellung laufender Serververfügbarkeit und -kapazität.

Erweiterungen der Systemsoftware	Sicherstellen, dass die neuesten Patches installiert sind, präventive Analyse und Ausführung.
Sicherheitsprüfung	Überprüfung der Sicherheitsprotokolle, Wahrung der Integrität des Dienstes, Umsetzung und Pflege einer Sicherheitsrichtlinie.
Druckverwaltung	Verwaltung des Datei- und Druckservers
Benutzerverwaltung	Verwaltung von Benutzerkonten, Zugriffssteuerung (Media Access Control, MAC), Berechtigungen
Speicherverwaltung	Konnektivität, Belastbarkeit, Failover usw. der Speicher
Tokenverwaltung	Verwaltung der Bereitstellung, Sperrung und sonstiger Lebenszyklusereignisse.
Systemüberwachung	Fortlaufende Überwachung mithilfe von Systemtools und -berichten, Korrelation und Überprüfung
Backup-Vorgänge	Backup und Speicherung der Anwendung sowie der Benutzerdaten Einschließlich: Überwachung der Sicherungskopien; Speicherung; Vorgänge außerhalb des Standorts
Teamleitung	Leitung des Teams, das Server, Anwendung, Infrastruktur, Helpdesk, Eskalationsverfahren usw. betreut.

Zusätzlich zu diesen Ressourcen werden Sie wahrscheinlich ein Krypto-Team benötigen, das sich mit den laufenden operativen Aspekten Ihrer HSM-Infrastruktur befasst. Die folgenden Bereiche betreffen in der Regel den Großteil unserer Kundenbasis:

HSM-Client-Verwaltung	Steuerung der Beschaffung, der Bereitstellung von Updates usw.
HSM-Verwaltung	Steuerung der Beschaffung, der Bereitstellung von Updates usw.
Teamleitung	Leitung des Teams, das Server, Anwendung, Infrastruktur, Helpdesk, Eskalationsverfahren, Key Ceremony usw. betreut.

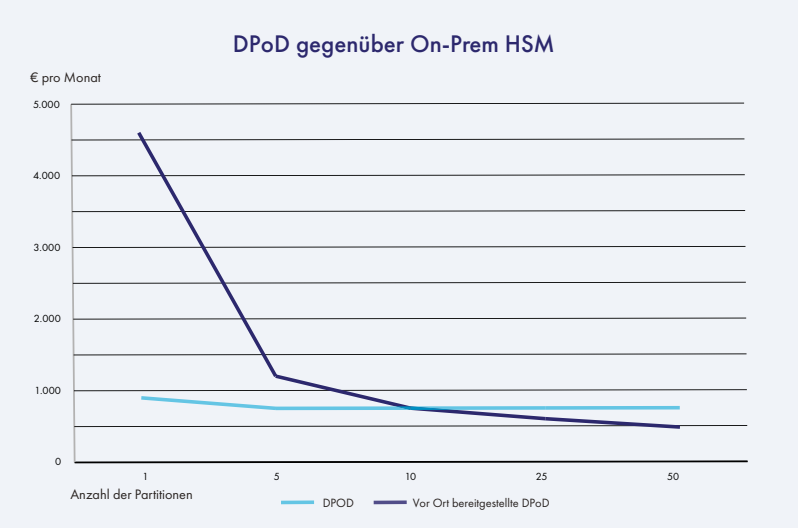
Kalkulation der Gesamtbetriebskosten

Um Ihre Kalkulation abzuschließen, kombinieren Sie diese einmaligen und jährlichen Kosten sowie die Verwaltungs-/Leitungskosten und erhalten so für beide Bereitstellungsmodelle jeweils die Gesamtbetriebskosten.

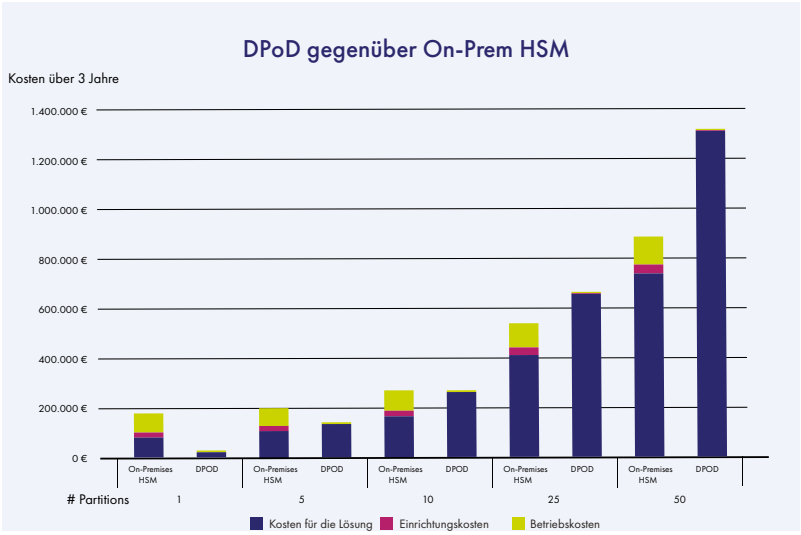
Das folgende Beispiel basiert auf unserer internen Kostenanalyse. Die oben genannten Kosten werden über einen dreijährigen Zeitraum verteilt und in jährliche Zahlen umgerechnet.

Einige Unternehmen haben nur einen geringen HSM-Bedarf, während andere HSMs intensiv nutzen. Daher enthält unser folgendes erstes Beispiel Berechnungen für unterschiedlichen HSM-Bedarf – von 5 bis zu 50 Anwendungsfällen – und führt die monatlichen Kosten auf, die wahrscheinlich entstehen würden. Kurz gesagt: Für Unternehmen, die planen, kleine oder mittelgroße DevOps-Projekte umzusetzen oder Shared-Service-Umgebungen einzurichten, sowie für kleine und mittlere Unternehmen ist ein auf DPoD basierender Service eine attraktive Option für bis zu 12 bis 15 einzelne Anwendungsfälle.

Das folgende alternative Beispiel verfolgt einen etwas anderen Ansatz und zeigt die Unterschiede zwischen vor Ort bereitgestellten HSMs und einer auf DPoD basierenden Bereitstellung, allerdings bezogen auf die Kosten. So können sie eine erste Bewertung der Unterschiede hinsichtlich des Investitionsbedarfs der Lösung und der zusätzlichen Ressourcen durchführen, die entscheidend für die Frage ist, wie viele qualifizierte Mitarbeiter Ihr Unternehmen benötigt:



Die Ergebnisse unseres einfachen Vergleichs der Gesamtbetriebskosten beruhen auf Annahmen hinsichtlich der typischen Kosten für die Umsetzung der einzelnen HSM-Lösungen über einen Zeitraum von drei Jahren. Auch wenn deutlich wird, dass DPoD für kleine und mittlere Unternehmen wesentlich kostengünstiger als vor Ort bereitgestellte HSMs ist, variieren die Kosten jedoch von Unternehmen zu Unternehmen. Daher ist es unerlässlich, dass Sie Ihre eigene Kostenanalyse durchführen, bevor Sie eine Kaufentscheidung treffen.



Dennoch zeigen die Ergebnisse deutlich, dass DPoD bei bestimmten Arten der Bereitstellung, wenn sie möglicherweise nur für eine begrenzte Zahl von Anwendungen kryptographische Dienste sichern müssen, besonders kostengünstig ist. Das leuchtet ein, wenn man sich vor Augen führt, dass eine vor Ort bereitgestellte Lösung jeglicher Größe erhebliche Investitionen in Hardware und Einrichtung erfordert.

Schlussfolgerungen

Cloud-basierte HSMs wie DPoD sind dann die richtige Lösung, wenn die Vorabinvestitionen oder die Fachkenntnisse, die für die Bereitstellung eines Geräts erforderlich sind, weit über die Investition in ein HSM oder ein zusätzliches HSM (wenn Sie überlegen, Ihre bestehende HSM-Infrastruktur zu erweitern) hinausgehen – oder die Möglichkeiten von beispielsweise kleinen oder mittleren Unternehmen übersteigen.

Zu den wichtigsten Entscheidungskriterien gehören die Verfügbarkeit und/oder die Kosten einer Finanzierung der Investition in eine vor Ort bereitgestellte Lösung. Die Analyse macht deutlich, dass es wichtig ist, sich die langfristigen Gesamtbetriebskosten anzusehen und diese mit den vorab erforderlichen Investitionen abzuwägen. Für kleine und mittlere Unternehmen oder auch abteilungs- bzw. projektorientierten Bedarf können die zur Verfügung stehenden Mittel ein wichtiger Entscheidungsfaktor bei der Wahl der richtigen Lösung sein. Dies kann auch auf große Unternehmen wie z. B. Tier-1-Banken zutreffen, die, obwohl sie über die nötige Expertise für die Verwaltung ihrer bestehenden HSMs verfügen, in Betracht ziehen können, ihre vorhandene Lösung durch Cloud-basierte HSM-Dienste zu erweitern, um alle Vorteile eines Cloud-Dienstes zu nutzen.

Auch die Überlegung, inwieweit die erforderlicher Qualifikationen vorhanden sind, kann sich auf die Entscheidung von Kunden auswirken. Die Verfügbarkeit von und die laufenden Kosten für die Einstellung von Mitarbeitern mit kryptographischer Fachkenntnis sind wichtige Überlegungen für viele Unternehmen, die vor der Entscheidung zwischen einer vor Ort bereitgestellten oder einer ausgelagerten Option stehen. Die Analyse zeigt, dass für die Einrichtung und Wartung einer vor Ort bereitgestellten Lösung ein erheblicher Bedarf an entsprechend qualifizierten Mitarbeitern besteht – ein Sachverhalt, den viele Unternehmen erkennen und der ein wichtiger Beweggrund für einen Wechsel in die Cloud ist.

Die vorstehenden Grafiken zeigen, dass sich eine vor Ort bereitgestellte Lösung bei mehr als 15 bis 20 Partitionen oder einzelnen Anwendungsfällen für Sie als vorteilhaft erweist. Daher ist eine Lösung wie DPoD für die Mehrzahl der Unternehmen, die HSM nur für eine begrenzte Anzahl von Anwendungen verwenden, sehr kostengünstig.

Sie sollten unbedingt berücksichtigen, für welche Anwendung oder für welchen Anwendungsfall Sie das HSM einsetzen möchten. Vor Ort bereitgestellte HSMs eignen sich eher für die Anforderungen großvolumiger Transaktionen, bei denen die Latenz der Cloud die Leistung und die Reaktionszeiten beeinträchtigen könnte. Dennoch sollten die meisten Unternehmen für einen Großteil der Anwendungsfälle von der Nutzung von Cloud-basierten HSM-Diensten wie DPoD profitieren.

Echten Nutzen ziehen Sie aus einer umfassenden Datenschutzlösung wie DPoD, wenn Sie andere Sicherheits- und Datenschutzanwendungen wie die Steuerung und den Besitz von Schlüsseln, Schlüsselverwaltung oder Verschlüsselung von Data-at-Rest (z. B. in virtuellen Maschinen oder Ordner bzw. Dateien gespeicherte Daten) in Betracht ziehen. Für die Verwaltung von so unterschiedlichen Datenschutz-Assets bietet sich eine Cloud-basierte Plattform an, die eine zentrale und einheitliche Verwaltung, Orchestrierung und Bereitstellung ermöglicht. Die Kosten für die Bereitstellung von Vor-Ort-Lösungen für so unterschiedliche Umgebungen kann die Kosten eines Cloud-basierten Dienstes potenziell um ein Vielfaches übersteigen.

Viele Kunden sehen den Nutzen eines Cloud-basierten Dienstes vor allem in der einfachen und schnellen Einrichtung und Verwaltung von Projekten oder Sandbox-Umgebungen. Vor Ort bereitgestellt Lösungen erfordern in diesen Fällen viele Änderungen wie z. B. Netzwerkänderungen, Infrastrukturanpassungen, Ressourcenplanung und vieles mehr.

Kurz gesagt: Zusätzlich zu einigen überzeugenden Vorteilen bei den Gesamtbetriebskosten, die in den vorstehenden Grafiken dargestellt sind, bietet eine Cloud-basierte Lösung wie SafeNet Data Protection on Demand erhebliche Vorteile für kleinere Unternehmen oder Projekte sowie einfach zu erzielenden Nutzen für Unternehmen jeglicher Größe, die auf der Suche nach einem Cloud-basierten HSM-Dienst sind, der einfach bereitzustellen und zu verwalten ist.

Über Thales

Die Menschen, denen Sie den Schutz Ihrer Daten anvertrauen, vertrauen beim Datenschutz auf Thales. Beim Thema Datensicherheit stehen Unternehmen immer häufiger vor entscheidenden Momenten. Egal, ob es darum geht, eine Verschlüsselungsstrategie zu entwickeln, Ihre Daten auf die Cloud zu übertragen oder Compliance-Anforderungen zu erfüllen – Sie können sich bei der Sicherung Ihrer digitalen Transformation auf Thales verlassen. Entscheidende Technologie für entscheidende Momente

Americas – Thales eSecurity Inc.
2860 Junction Avenue, 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) Ltd
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

> cpl.thalesgroup.com <