

ZAPYTANIE O INFORMACJĘ DLA USŁUGI CLOUD KEY MANAGEMENT SERVICE (CLOUD KMS)



Bank Polski

PKO Bank Polski SA poszukuje informacji na temat usług Cloud Key Management Service (Cloud KMS) w celu zabezpieczenia danych i zarządzania kluczami kryptograficznymi w środowisku chmurowym. Niniejsze zapytanie ma na celu uzyskanie szczegółowych informacji na temat dostępnych rozwiązań, ich funkcjonalności, bezpieczeństwa, kosztów oraz zgodności z regulacjami (np. KNF Rekomendacja D/DORA/etc).

1. Celem niniejszego RFI jest:

- a) Ocena dostępnych usług Cloud KMS od różnych dostawców.
- b) Porównanie funkcjonalności i bezpieczeństwa rozwiązań.
- c) Zrozumienie kosztów wdrożenia i utrzymania.
- d) Identyfikacja możliwości integracji Cloud KMS z naszymi systemami IT.

2. Zakres informacji do dostarczenia:

- a) Ogólny opis usługi m.in.:
 - a. Nazwa usługi i dostawcy.
 - b. Opis działania Cloud KMS.
 - c. Model wdrożenia: public cloud, private cloud, hybrid cloud, on-premises.
 - d. Modelowa architektura rozwiązania
 - e. Lista dostępnych regionów geograficznych, w których usługa jest oferowana, w szczególności w ramach EOG
- b) Typy i mechanizmy zarządzania kluczami:
 - a. Obsługiwane typy kluczy kryptograficznych
 - b. Obsługa zarówno kluczy symetrycznych, jak i asymetrycznych.
 - c. Obsługa kluczy typu PGP/GPG
 - d. Mechanizmy generowania, rotacji i przechowywania kluczy.
 - e. Obsługa kluczy przynoszonych przez klienta (Bring Your Own Key – BYOK).
 - f. Obsługa zarządzania kluczami w sprzętowych modułach bezpieczeństwa (HSM-backed keys)
 - g. Mechanizm backupu materiału kryptograficznego poza system Cloud KMS
 - h. Mechanizm synchronizacji materiału kryptograficznego z zewnętrznymi systemami KMS (Azure Key Vault, Google Cloud KMS)
- c) Bezpieczeństwo i compliance:
 - a. Mechanizmy ochrony kluczy (np. FIPS 140-2, HSM).
 - b. Szyfrowanie danych at-rest, in-transit oraz in-use.
 - c. Mechanizmy audytu i logowania operacji na kluczach.
 - d. Zgodność z regulacjami (np. GDPR, HIPAA, PCI DSS, ISO 27001).
 - e. Mechanizmy Disaster Recovery i dostępność usługi (SLA).
 - f. Mechanizmy

3. Zarządzanie dostępem (IAM) i kontrola użytkowników:

- a. Integracja z systemami IAM dostawcy chmurowego (Google IAM, AWS IAM, Azure AD).
- b. Możliwość przypisywania uprawnień do kluczy na poziomie użytkownika, grupy lub aplikacji.
- c. Możliwość delegacji zarządzania kluczami na różnych poziomach organizacyjnych.
- d. Integracja z systemami powiadamiania o dezaktualizacji kluczy kryptograficznych

4. Integracja z innymi systemami

- a. Obsługa API do integracji z aplikacjami i systemami firmowymi.
- b. Integracja z usługami chmurowymi (np. Google Cloud Storage, AWS S3, Azure Blob Storage).

- c. Obsługa szyfrowania baz danych (np. Google Cloud SQL, AWS RDS, Azure SQL).
- d. Obsługa integracji z mechanizmami szyfrowania maszyn wirtualnych w chmurach (Google Compute Engine, Azure VM)
- e. Obsługa protokołu KMIP i integracji z mechanizmami szyfrowania macierzy dyskowych
- f. Możliwość użycia Cloud KMS w scenariuszach DevOps (np. Terraform, Kubernetes).
- g. Dostępność bibliotek programistycznych dla popularnych języków programowania
- h. Informacje dot. wydajności rozwiązania, np. maksymalnej ilości zapytań o klucz na sekundę

5. Model licencyjny i utrzymaniowy w podziale:

- a. Struktura kosztów
- b. Możliwości optymalizacji
- c. Wycena przykładowego scenariusza użycia

6. Sposób składania informacji oraz pytania

Na ewentualne pytania czekamy do dnia 24.04.2025 r.

Pytania do RFI można przesłać w jednym pliku zbiorczym korzystając ze wzoru, który określa „Załącznik nr 1 „Formularz pytań i odpowiedzi”. Pytania prosimy kierować na adres mailowy kupca prowadzącego RFI: jakub.chwedoruk@pkobp.pl. Bank rezerwuje prawo do odmowy udzielenia odpowiedzi na pytania, które zostały przesłane po upływie wyżej wskazanego terminu. terminie nie będą rozpatrywane.

Potencjalni Oferenci zainteresowani udziałem w RFI proszeni są o przesłanie informacji wiadomością elektronicznie na adres e-mail: jakub.chwedoruk@pkobp.pl, w terminie do dnia 29.04.2025 r. do godz. 13:00.

Informujemy, że z uwagi na ograniczenia w zakresie pojemności korespondencji przesyłanej mailem niezbędnym jest jej skompensowanie do wielkości 20 MB lub jej podzielenie na kilka części z dokładnym opisem w tytule, której części korespondencja dotyczy.

Załączniki:

Załącznik nr 1 – Formularz pytań i odpowiedzi

Załącznik nr 2 – Formularz informacji