AWS Panduan Keputusan

# Memilih layanan AWS kriptografi

# Memilih layanan AWS kriptografi: AWS Panduan Keputusan

# Table of Contents

# Memilih layanan AWS kriptografi

Mengambil langkah pertama

| | |
|---|---|
| Tujuan | Bantu menentukan layanan AWS kriptografi mana yang paling cocok untuk organisasi Anda. |
| Terakhir diperbarui | Januari 31, 2025 |
| Layanan yang tercakup | • AWS Certificate Manager<br>• AWS CloudHSM<br>• AWS SDK Enkripsi Basis Data<br>• AWS Encryption SDK<br>• AWS KMS<br>• AWS Private CA<br>• AWS Secrets Manager |
| Panduan terkait | Memilih AWS layanan keamanan, identitas, dan tata kelola |

## Pengantar

Kriptografi adalah landasan keamanan dalam komputasi awan, membantu memastikan kerahasiaan, integritas, dan keaslian data. Dalam lingkungan cloud, data sensitif dapat melintasi jaringan publik dan berada di infrastruktur bersama, membuat langkah-langkah kriptografi yang kuat penting untuk melindungi terhadap akses atau gangguan yang tidak sah.

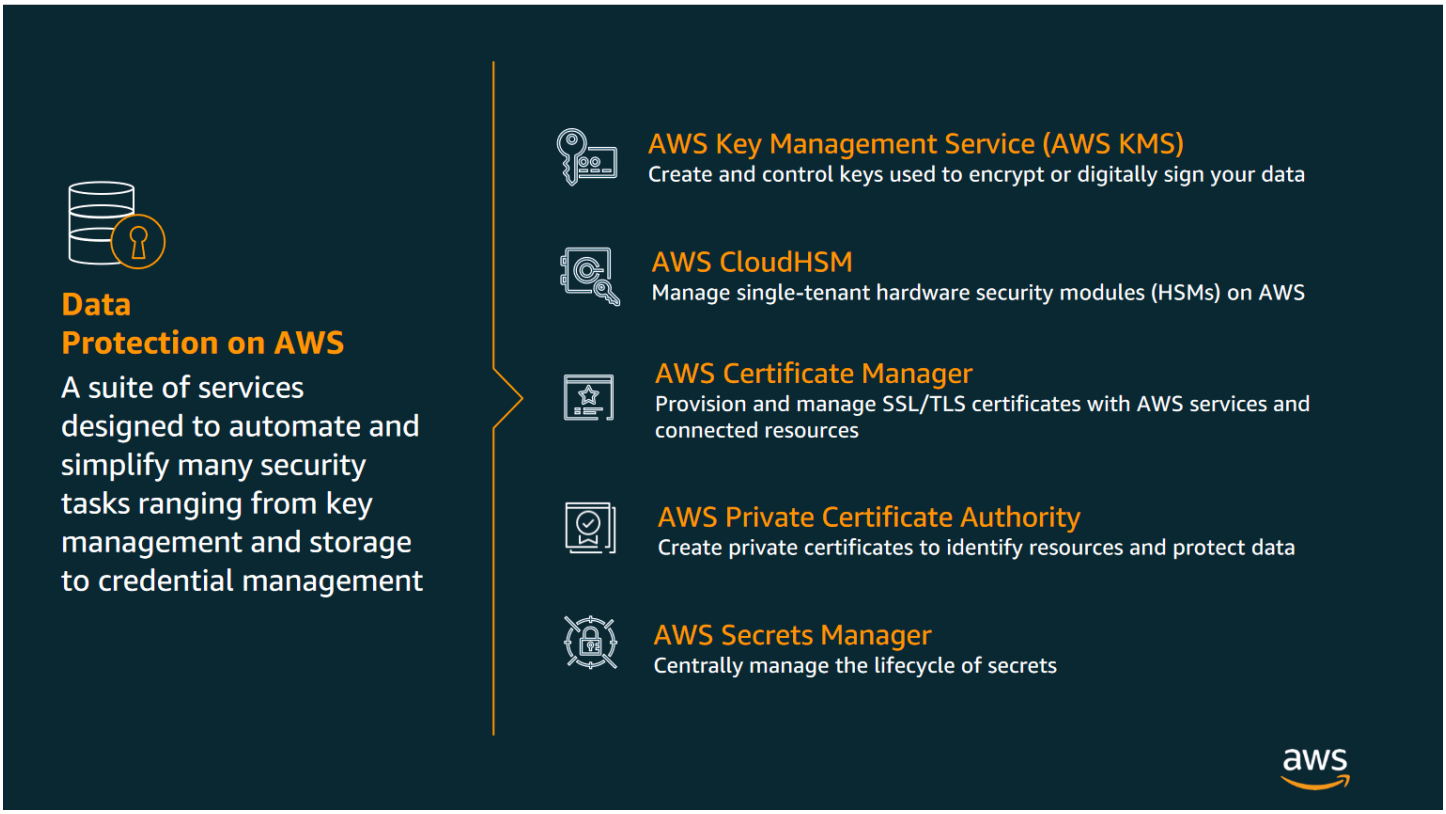
AWS menawarkan berbagai layanan kriptografi yang komprehensif untuk mengamankan data, mengelola kunci enkripsi, dan melindungi informasi sensitif. Ini termasuk AWS Key Management Service (KMS) untuk manajemen kunci terpusat, AWS CloudHSM untuk PKCS11 aplikasi dan modul keamanan perangkat keras khusus, dan AWS Encryption SDK untuk enkripsi sisi klien. AWS Secrets Manager adalah layanan yang memungkinkan Anda menyimpan, mengelola, dan mengambil informasi sensitif dengan aman seperti kredensyal basis data, kunci API, dan rahasia lainnya sepanjang siklus hidupnya. AWS Certificate Manager (ACM) menyederhanakan proses penyediaan, pengelolaan, dan penerapan sertifikat transport layer security (TLS) tepercaya publik

untuk digunakan. Layanan AWS AWS Private Certificate Authority (PCA) memungkinkan Anda untuk menghasilkan dan mendistribusikan sertifikat x509 untuk sumber daya internal Anda.

Panduan ini dirancang untuk membantu Anda memilih layanan dan alat AWS kriptografi yang paling sesuai dengan kebutuhan dan organisasi Anda.

Video berikut adalah segmen dua menit dari presentasi yang memperkenalkan praktik terbaik untuk kriptografi.

# Memahami




Memilih layanan AWS kriptografi yang tepat tergantung pada kasus penggunaan spesifik Anda, persyaratan keamanan data, kewajiban kepatuhan, dan preferensi operasional sebagaimana diuraikan dalam tabel berikut.

Key management

Jika Anda perlu mengelola kunci enkripsi dengan aman, pertimbangkan Layanan Manajemen AWS Kunci (KMS). Ini memungkinkan Anda untuk membuat, memutar, dan mengelola kunci kriptografi yang terintegrasi dengan yang lain Layanan AWS. KMS menggunakan FIPS yang divalidasi HSMs untuk membantu Anda memenuhi persyaratan kepatuhan dan untuk memberikan

jaminan tentang kebenaran implementasi primitif kriptografi yang diekspos oleh KMS. Beberapa aplikasi memerlukan fungsi kriptografi tertentu atau antarmuka aplikasi yang hanya tersedia dengan HSM tradisional dan AWS CloudHSM menyediakan modul keamanan perangkat keras khusus (HSMs) di cloud yang memberi Anda kontrol penuh atas kunci dan operasi kriptografi Anda.

Data encryption

Untuk mengenkripsi data sensitif seperti detail pelanggan atau kekayaan intelektual, terintegrasi erat dengan AWS penyimpanan, AWS KMS database, dan layanan pesan (misalnya S3, RDS, atau EBS). Jika Anda memerlukan enkripsi sisi klien, AWS Encryption SDK ini adalah pustaka sumber terbuka yang memudahkan untuk mengenkripsi data dalam aplikasi Anda sebelum mengirimnya ke cloud.

Secure communications

Untuk melindungi data dalam perjalanan, AWS Certificate Manager (ACM) menyederhanakan pengelolaan sertifikat TLS yang dipercaya publik. Gunakan untuk menegaskan identitas aplikasi Anda yang menghadap ke internet dan memfasilitasi komunikasi enkripsi antara aplikasi, pengguna, dan layanan cloud Anda tanpa khawatir tentang perpanjangan sertifikat. Untuk aplikasi internal, Anda dapat menggunakan AWS Private Certificate Authority (PCA) untuk menghasilkan dan mendistribusikan sertifikat x509 untuk sumber daya internal Anda, termasuk klien dan server.

Secrets and credentials management

Untuk menyimpan dan mengambil rahasia aplikasi dengan aman seperti kredensyal basis data, kunci API, atau sertifikat, pertimbangkan. AWS Secrets Manager Ini menyediakan rotasi rahasia otomatis dan kontrol akses berbutir halus. Atau, AWS Systems Manager Parameter Store adalah opsi berbiaya lebih rendah untuk mengelola konfigurasi yang tidak sensitif dan dapat diintegrasikan dengannya. AWS Secrets Manager

Compliance and auditing

Untuk pekerjaan kepatuhan terhadap peraturan, pertimbangkan AWS KMS dan AWS CloudHSM untuk membantu memastikan standar enkripsi terpenuhi. AWS Artifact adalah portal swalayan yang menyediakan akses sesuai permintaan ke AWS laporan keamanan dan kepatuhan, seperti sertifikasi ISO dan laporan SOC, serta kemampuan untuk meninjau dan menerima perjanjian seperti Business Associate Addendum (BAA). Anda juga dapat menggunakan layanan seperti AWS Config AWS Security Hub CSPM, dan AWS Audit Manager untuk memantau kepatuhan dan menghasilkan artefak yang sesuai untuk penggunaan Anda sendiri atau untuk konsumsi oleh pemangku kepentingan Anda.

Saat memilih antara layanan AWS kriptografi, pertimbangkan persyaratan berikut.

| Persyaratan | Layanan |
| --- | --- |
| Usaha rendah, dikelola sepenuhnya | AWS KMS atau AWS Secrets Manager |
| Memerlukan antarmuka aplikasi tertentu atau algoritma kriptografi yang tidak didukung oleh KMS | AWS CloudHSM |
| Encrypting/decrypting data dalam aplikasi Anda | AWS Encryption SDK |
| Manajemen Sertifikat TLS publik yang disederhanakan | AWS Certificate Manager |
| Manajemen rahasia | AWS Secrets Manager |

Dengan menyelaraskan kebutuhan Anda dengan opsi ini, Anda dapat menerapkan solusi kriptografi yang disesuaikan dengan kebutuhan keamanan dan operasional Anda.

# Pertimbangkan

Memilih layanan AWS kriptografi yang tepat melibatkan pemahaman kebutuhan keamanan, operasional, dan kepatuhan spesifik Anda. AWS menawarkan berbagai layanan kriptografi, masing-masing dirancang untuk mengatasi kasus penggunaan yang berbeda, dari manajemen kunci hingga enkripsi data dan komunikasi yang aman. Untuk membuat keputusan berdasarkan informasi, Anda harus mengevaluasi persyaratan Anda berdasarkan beberapa kriteria penting, termasuk kasus penggunaan, kebutuhan kontrol dan fleksibilitas, kewajiban kepatuhan, pertimbangan biaya, dan integrasi dengan Layanan AWS. Kriteria ini akan membantu Anda menyelaraskan pilihan Anda dengan tujuan keamanan organisasi dan alur kerja operasional Anda.

Use case

> Pertimbangkan apa yang Anda butuhkan untuk layanan kriptografi: enkripsi data, manajemen kunci, komunikasi aman, atau manajemen rahasia. Misalnya, AWS KMS sangat ideal untuk enkripsi yang terintegrasi ke dalam Layanan AWS, sementara AWS CloudHSM sesuai dengan organisasi yang membutuhkan kemampuan kriptografi tertentu, antarmuka aplikasi, atau HSM penyewa tunggal, seringkali karena kepatuhan yang ketat atau kebutuhan aplikasi tertentu.

Mengklarifikasi tujuan memastikan Anda memilih layanan yang sesuai dengan kebutuhan Anda, mengoptimalkan fungsionalitas dan biaya.

Control and flexibility

Evaluasi tingkat kontrol yang Anda butuhkan atas operasi kriptografi Anda. Layanan terkelola seperti AWS KMS memberikan kemudahan penggunaan dengan overhead manajemen minimal dengan HSM multi-tenant sambil mempertahankan kontrol penuh atas materi utama Anda. Sebaliknya, AWS CloudHSM menawarkan model penyewa tunggal untuk kebutuhan aplikasi, kriptografi, atau kepatuhan tertentu.

Compliance requirements

Jika Anda beroperasi di industri yang diatur, pastikan layanan sesuai dengan standar seperti GDPR, PCI DSS, atau HIPAA. AWS KMS dan keduanya AWS CloudHSM bersertifikat FIPS 140-2 Level 3. Memilih layanan yang memenuhi persyaratan non-fungsional Anda membantu menjaga kepercayaan dan dapat menghindari potensi hukuman hukum atau keuangan.

Cost considerations

Nilai anggaran Anda terhadap model penetapan harga layanan. AWS KMS hemat biaya untuk kebutuhan enkripsi umum, sementara AWS CloudHSM menimbulkan biaya lebih tinggi karena perangkat keras khusus. Memahami implikasi biaya membantu Anda mengoptimalkan pengeluaran keamanan Anda.

Integration with AWS ecosystem

Jika Anda banyak menggunakan Layanan AWS, prioritaskan solusi kriptografi seperti AWS KMS atau ACM yang terintegrasi mulus dengan S3, RDS, atau Lambda. Ini memastikan alur kerja yang lebih lancar dan mengurangi upaya pengembangan. Kemampuan integrasi dapat secara signifikan meningkatkan efisiensi operasional.

# Pilih

Memilih layanan AWS kriptografi yang tepat melibatkan pemahaman kebutuhan keamanan, operasional, dan kepatuhan spesifik Anda. AWS menawarkan berbagai layanan kriptografi, masing-masing dirancang untuk mengatasi kasus penggunaan yang berbeda, dari manajemen kunci hingga enkripsi data dan komunikasi yang aman. Untuk membuat keputusan berdasarkan informasi, Anda harus mengevaluasi persyaratan Anda berdasarkan beberapa kriteria penting, termasuk kasus penggunaan, kebutuhan kontrol dan fleksibilitas, kewajiban kepatuhan, pertimbangan biaya, dan

integrasi dengan Layanan AWS. Kriteria ini akan membantu Anda menyelaraskan pilihan Anda dengan tujuan keamanan organisasi dan alur kerja operasional Anda.

| Kasus penggunaan target | Kapan Anda akan menggunakannya? | Layanan yang direkomendasikan |
|---|---|---|
| Manajemen kunci | Untuk membuat, memutar, dan mengelola kunci kriptografi yang terintegrasi dengan aman Layanan AWS | AWS KMS |
| Manajemen kunci | Untuk integrasi aplikasi tertentu atau primitif kriptografi | AWS CloudHSM |
| Enkripsi data | Untuk menerapkan enkripsi sisi klien untuk melindungi data sensitif seperti detail pelanggan atau kekayaan intelektual. | AWS Encryption SDK<br>AWS SDK Enkripsi Basis Data |
| Komunikasi yang aman | Untuk melindungi data dalam perjalanan dan menyederhanakan pengelolaan SSL/TLS sertifikat. | AWS Certificate Manager<br>AWS Private CA |
| Rahasia dan manajemen kredensyal | Untuk menyimpan dan mengambil rahasia aplikasi dengan aman seperti kredensyal basis data, kunci API, atau sertifikat. | AWS Secrets Manager<br>AWS Toko Parameter |

# Gunakan

Anda sekarang harus memiliki pemahaman yang jelas tentang apa yang dilakukan setiap layanan AWS kriptografi, dan mana yang mungkin tepat untuk Anda.

Untuk mengeksplorasi cara menggunakan dan mempelajari lebih lanjut tentang masing-masing layanan AWS kriptografi yang tersedia, kami telah menyediakan jalur untuk mengeksplorasi cara

kerja masing-masing. Bagian berikut menyediakan tautan ke dokumentasi mendalam, tutorial langsung, dan sumber daya lainnya untuk membantu Anda memulai.

AWS Certificate Manager

- Memulai dengan AWS Certificate Manager

  Mulai gunakan AWS Certificate Manager, termasuk bekerja dengan sertifikat publik dan swasta.

  Jelajahi panduan
- Praktik terbaik untuk AWS Certificate Manager

  Tinjau rekomendasi yang dapat membantu Anda menggunakan AWS Certificate Manager lebih efektif.

  Jelajahi panduan
- AWS Certificate Manager FAQ

  Tinjau halaman FAQ AWS Certificate Manager (ACM) untuk jawaban rinci atas pertanyaan umum tentang fitur, kemampuan, dan penggunaan ACM. Ini mencakup topik-topik seperti jenis sertifikat yang dikelola ACM, integrasi dengan yang lain Layanan AWS, dan panduan tentang penyediaan dan pengelolaan sertifikat. SSL/TLS

  Jelajahi FAQs

AWS CloudHSM

- Memulai dengan AWS CloudHSM

  Pelajari cara membuat, menginisialisasi, dan mengaktifkan cluster di AWS CloudHSM. Setelah menyelesaikan prosedur ini, Anda akan siap mengelola pengguna, mengelola klaster, dan menggunakan pustaka perangkat lunak yang disertakan untuk melakukan operasi kriptografi.

  Jelajahi panduan
- Praktik terbaik untuk AWS CloudHSM

  Jelajahi praktik terbaik untuk mengelola dan memantau AWS CloudHSM klaster Anda.

  Jelajahi panduan
- AWS CloudHSM harga

Tinjau halaman harga untuk mempelajari tentang AWS CloudHSM harga. Tidak ada biaya dimuka untuk digunakan AWS CloudHSM. Dengan AWS CloudHSM, Anda membayar biaya per jam untuk setiap HSM yang Anda luncurkan sampai Anda mengakhiri HSM. Panduan ini memberikan tarif per jam untuk setiap AWS wilayah.

Jelajahi halaman harga

- AWS CloudHSM FAQ

  Tinjau halaman AWS CloudHSM FAQ untuk jawaban terperinci atas pertanyaan umum tentang AWS CloudHSM, termasuk fitur-fiturnya, harga, penyediaan, keamanan, kepatuhan, kinerja, dan integrasi dengan aplikasi pihak ketiga.

  Jelajahi FAQs

AWS Encryption SDK

- Memulai dengan AWS Encryption SDK

  Pelajari cara menggunakan AWS Encryption SDK dengan AWS KMS.

  Jelajahi panduan

- Praktik terbaik untuk AWS Encryption SDK

  Tinjau halaman Praktik AWS Encryption SDK Terbaik untuk panduan tentang pemanfaatan efektif AWS Encryption SDK untuk mengamankan data Anda. Mengikuti praktik terbaik ini membantu memastikan kerahasiaan dan integritas data terenkripsi Anda.

  Jelajahi panduan

- AWS Encryption SDK FAQ

  Tinjau halaman AWS Encryption SDK FAQ untuk jawaban atas pertanyaan umum tentang AWS Encryption SDK, termasuk fitur-fiturnya, bahasa pemrograman yang didukung, dan praktik terbaik untuk implementasi.

  Jelajahi FAQ

AWS Database Encryption SDK

- Memulai dengan AWS Database Encryption SDK

  Pelajari cara menggunakan SDK Enkripsi AWS Database dengan AWS KMS.

  Jelajahi panduan
- Konfigurasikan SDK Enkripsi AWS Database

  Pelajari cara mengonfigurasi SDK Enkripsi AWS Database, termasuk memilih bahasa pemrograman dan memilih kunci pembungkus.

  Jelajahi panduan

AWS KMS

- Memulai dengan AWS KMS

  Pelajari cara membuat kunci KMS, termasuk kunci enkripsi simetris dan asimetris.

  Jelajahi panduan
- Praktik terbaik untuk AWS KMS

  Pelajari praktik terbaik enkripsi untuk AWS KMS.

  Jelajahi panduan
- AWS KMS harga

  Tinjau halaman Harga AWS Key Management Service (KMS) untuk mempelajari tentang biaya yang terkait dengan penggunaan AWS KMS, termasuk biaya untuk penyimpanan kunci, permintaan API, dan fitur opsional seperti toko kunci khusus.

  Jelajahi halaman harga
- AWS KMS FAQ

  Halaman FAQ AWS Key Management Service (KMS) memberikan jawaban terperinci atas pertanyaan umum tentang AWS KMS, termasuk fitur-fiturnya, langkah-langkah keamanan, praktik penagihan, opsi manajemen kunci, dan integrasi dengan lainnya. Layanan AWS

  Jelajahi FAQs

### AWS Private CA

- Praktik terbaik untuk AWS Private CA

  Tinjau rekomendasi yang dapat membantu Anda menggunakannya AWS Private CA secara efektif.

  Jelajahi panduan
- Memulai dengan AWS Private CA

  Pelajari cara membuat dan mengaktifkan root CA secara terprogram.

  Jelajahi panduan
- AWS Private CA harga

  Tinjau biaya yang terkait dengan pengoperasian sertifikat pribadi CAs dan penerbitan sertifikat pribadi.

  Jelajahi halaman harga
- AWS Private CA FAQ

  Dapatkan jawaban terperinci atas pertanyaan umum tentang AWS Private CA, termasuk fitur-fiturnya, harga, penyediaan, keamanan, kepatuhan, kinerja, dan integrasi dengan lainnya. Layanan AWS

  Jelajahi FAQs

### AWS Secrets Manager

- Memulai dengan AWS Secrets Manager

  Pelajari cara membuat AWS Secrets Manager rahasia.

  Jelajahi panduan
- Praktik terbaik untuk AWS Secrets Manager

  Pelajari tentang praktik terbaik yang harus Anda pertimbangkan saat menggunakan AWS Secrets Manager.

  Jelajahi panduan

- AWS Secrets Manager harga

  Tinjau halaman AWS Secrets Manager harga untuk mempelajari biaya yang terkait dengan penyimpanan, pengelolaan, dan pengambilan rahasia dengan aman seperti kredensyal basis data dan kunci API.

  Jelajahi halaman harga
- AWS Secrets Manager FAQ

  Tinjau halaman AWS Secrets Manager FAQ untuk jawaban terperinci atas pertanyaan umum tentang AWS Secrets Manager, termasuk fitur-fiturnya, langkah-langkah keamanan, harga, dan kemampuan integrasi.

  Jelajahi FAQs

## Jelajahi

- Penelitian dan sumber daya

  Jelajahi AWS blog, video, dan alat tentang kriptografi.

  Tinjau sumber daya
- Video

  Tonton video ini dari saluran AWS Pengembang YouTube untuk mengembangkan dan menyempurnakan strategi kriptografi Anda lebih lanjut.

  Jelajahi video kriptografi

# Riwayat dokumen

Tabel berikut menjelaskan perubahan penting pada panduan keputusan ini. Untuk pemberitahuan tentang pembaruan panduan ini, Anda dapat berlangganan umpan RSS.

| Perubahan | Deskripsi | Tanggal |
| --- | --- | --- |
| Publikasi awal | Panduan pertama kali diterbitkan. | Januari 31, 2025 |

Terjemahan disediakan oleh mesin penerjemah. Jika konten terjemahan yang diberikan bertentangan dengan versi bahasa Inggris aslinya, utamakan versi bahasa Inggris.