

SISTEM PENGURUSAN KUNCI KESELAMATAN (KMS)

**Memperkasa Kedaulatan Digital Sektor Awam Malaysia Menerusi
Tadbir Urus Kriptografi yang Komprehensif dan Berdaya Tahan**

JABATAN DIGITAL NEGARA
KEMENTERIAN DIGITAL

Realiti & Cabaran Sektor Awam:

Ekosistem Digital Kerajaan Semakin Kompleks



Perluasan Awan & Aplikasi

Sempadan perimeter keselamatan tradisional (on-premise) kini telah lenyap.



Data sebagai Sasaran Utama

Data dalam transit (bergerak) dan data berehat (disimpan) memerlukan perlindungan mutlak daripada ancaman moden.



Kepercayaan adalah Nadi

Keselamatan bukan lagi sekadar dinding penghalang; ia adalah pemboleh utama untuk penyampaian perkhidmatan kerajaan yang pantas dan selamat.

Setiap Perkhidmatan Kerajaan Memerlukan Kepercayaan

Transformasi digital Malaysia bergantung sepenuhnya kepada keyakinan rakyat. Aplikasi kerajaan, portal data, dan transaksi kewangan semuanya diasaskan oleh satu elemen yang tidak kelihatan: **Rahsia Digital (Digital Secrets)**. Jika kita kehilangan rahsia ini, kita kehilangan kepercayaan.

1



Data Terperingkat

Perlindungan data rakyat di pangkalan data kerajaan.

2



Transaksi Selamat

Pembayaran dalam talian portal rasmi (cth. GovWallet/PayNow).

3



Akses Sistem

Pegawai awam log masuk ke sistem awan (Cloud) kerajaan.

Realiti

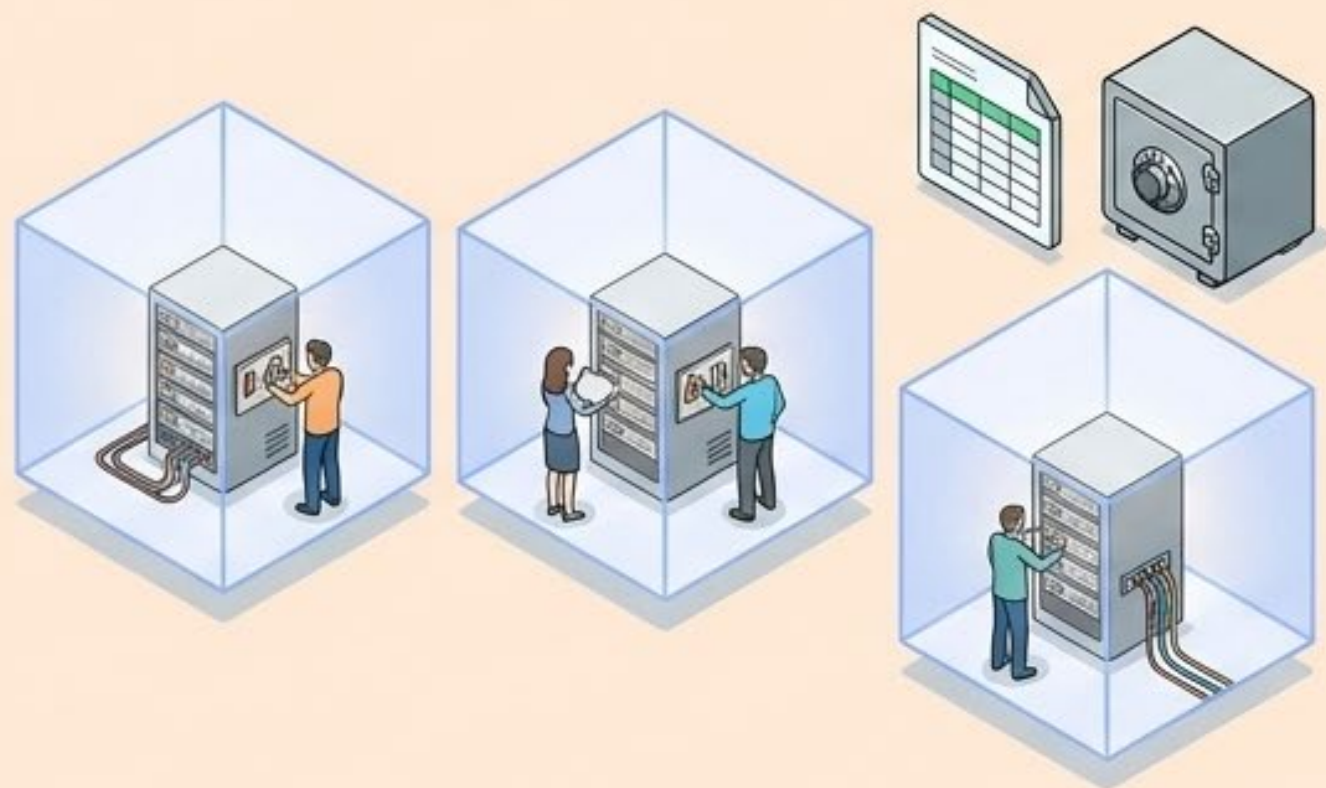
- Enkripsi tidak bermakna jika 'kunci' dibiarkan berseparah.
- Tanpa pengurusan kunci yang sistematik, data berisiko tinggi untuk hilang, dicuri, atau tidak dapat diakses (ransomware/kegagalan sistem).

Rahsia ini adalah Cryptographic Keys dan Digital Certificates. Bagaimana kita menyimpannya menentukan tahap keselamatan negara.

Realiti Semasa Operasi IT Sektor Awam: Risiko Silo & Manual

47.06%

agensi masih **bergantung kepada kaedah manual** untuk menguruskan kunci enkripsi, yang sangat terdedah kepada ralat manusia.



Vendor Lock-In

Kekurangan pakar kriptografi dalaman menyebabkan kebergantungan mutlak kepada kontraktor luar.



Pengurusan **Silo**

Setiap agensi membeli perkakasan mahal (CAPEX tinggi) tanpa piawaian yang seragam.



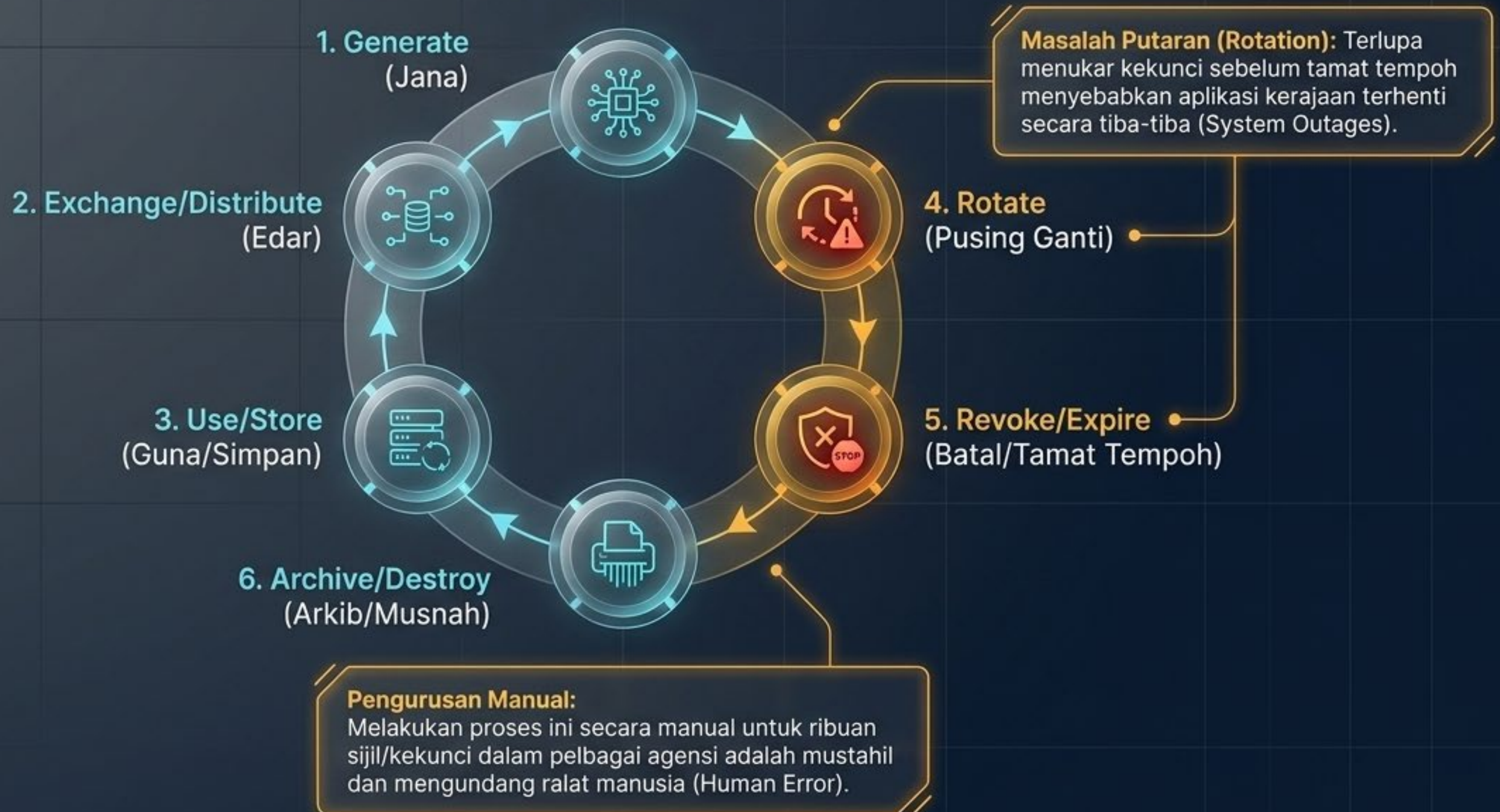
Zero Visibility

Tiada pemantauan berpusat (Whole-of-Government) untuk menjejaki akses data secara masa nyata.

Meleraikan Kekeliruan: KMS vs PKI

	PKI (Public Key Infrastructure)	KMS (Key Management System)
Analogi Utama	Jabatan Pendaftaran Negara (JPN) yang mengeluarkan kad pengenalan. 	Dompot digital pintar / bilik kebal bersulit yang mengawal kad pengenalan tersebut. 
Fungsi Teras	Mengeluarkan, mengesahkan, dan mengikat identiti (Sijil Digital Asimetri). 	Melindungi dan memusatkan kitaran hayat semua jenis kunci (Simetri, Asimetri, Sijil PKI). 
Fokus Perlindungan	Data in Transit dan kepercayaan identiti digital. 	Data at Rest, penyulitan pangkalan data, dan pengurusan akses. 

Kitaran Hayat Kekunci: Di Mana Risiko Sebenarnya Berlaku?



Pusat Kawalan Kriptografi:

Key Management System

Key Management System (KMS) ialah platform berpusat yang melindungi, mengurus, dan mengautomasikan kitaran hayat semua kunci kriptografi dan rahsia digital (secrets) di dalam sesebuah organisasi.



Storan Berpusat:

Satu bilik kebal digital untuk semua aset.



Kawalan Kitaran Hayat:

Mengurus dari penciptaan hingga pemusnahan kunci.



Audit & Pematuhan:

Merekodkan siapa, bila, dan bagaimana kunci digunakan.

Tiga Kelebihan Transformatif KMS



Ketahanan Operasi & Automasi

- Mengurangkan ralat sistem dan masa henti (*outages*) yang berpunca daripada pengurusan manual.

➡ kitaran hayat kunci membebaskan masa pegawai IT untuk fokus kepada tugas strategik.



Tadbir Urus & Akauntabiliti Mutlak

- Memusatkan repositori kunci dan sijil untuk visibiliti 100%.
- Standardisasi proses di seluruh agensi memastikan tiada 'shadow IT' dalam penggunaan kunci.



Keselamatan Kalis Masa Depan

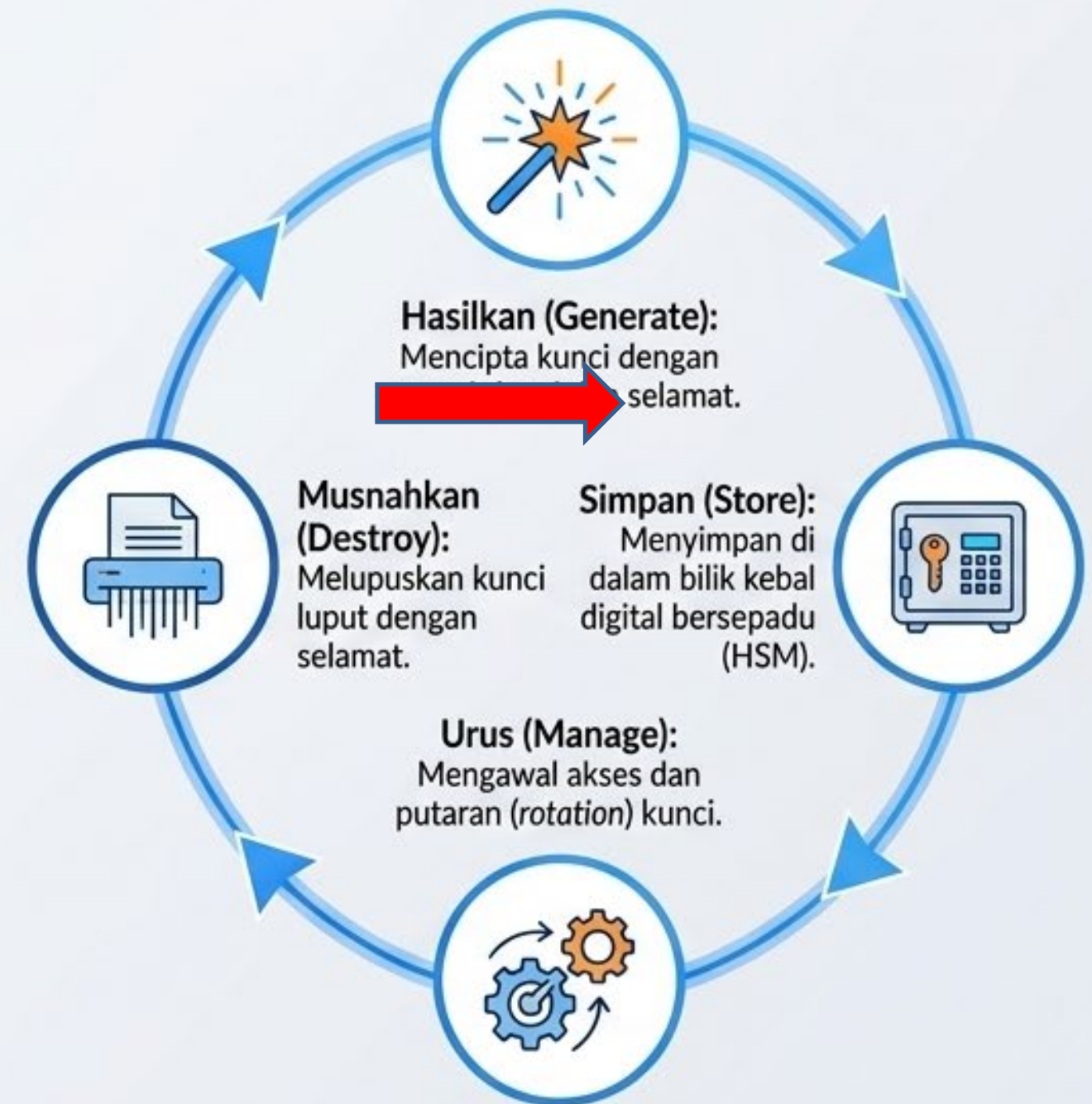
- Menguatkuasakan dasar keselamatan berpusat (*centralized policy enforcement*).
- Pengasingan kunci yang selamat (Root-of-trust) melindungi sektor awam daripada taktik serangan siber yang semakin canggih.

Apakah itu KMSaaS?

Sistem Pengurusan Kunci Berpusat yang disediakan sebagai platform perkongsian (*Service*) untuk seluruh sektor awam.



Kitaran Hayat Berpusat:



Kebenaran Empirikal: Dapatan Kajian Agensi

Berdasarkan kaji selidik lapangan terhadap 42 agensi sektor awam.

Diagnostic Dashboard

Keperluan Urgen KMS Berpusat

4.45 / 5.00

Min Kesedaran



Sangat Tinggi

Penjawat awam amat faham kepentingan kedaulatan data.



Kritikal

Resolusi utama untuk menutup jurang antara kesedaran dan amalan.

Min Amalan Organisasi



Sederhana

Polisi dan alat operasi harian masih terhad atau lemah.

Kajian membuktikan: Penjawat awam mahu mengamalkan keselamatan tinggi, tetapi dihalang oleh kekangan infrastruktur fizikal. KMSaaS adalah jawapan yang dituntut secara kritikal.



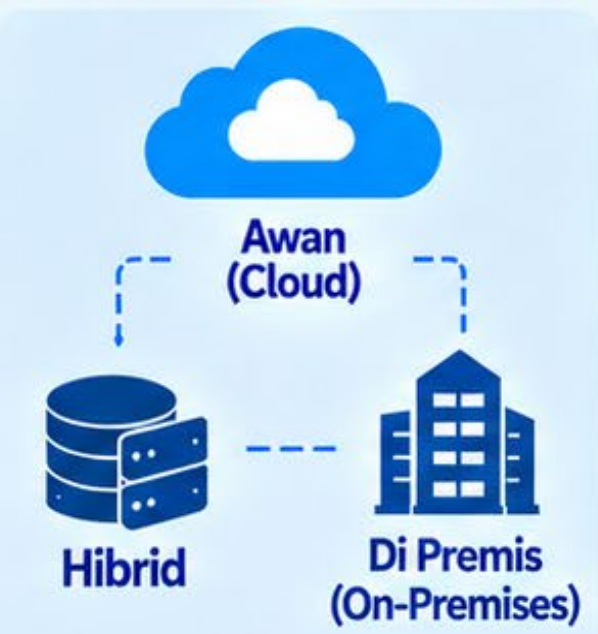
Apakah Asas kepada Prototaip Ini?

Prototaip ini tidak dibina secara sembarangan, sebaliknya mematuhi **5 Pillar Utama** khusus untuk Sektor Awam.

1

Seni Bina & Penempatan

Boleh menyokong persekitaran **Awan (Cloud)**, **Hibrid**, dan **Di Premis (On-Premises)**.



2

Pemilikan Kunci

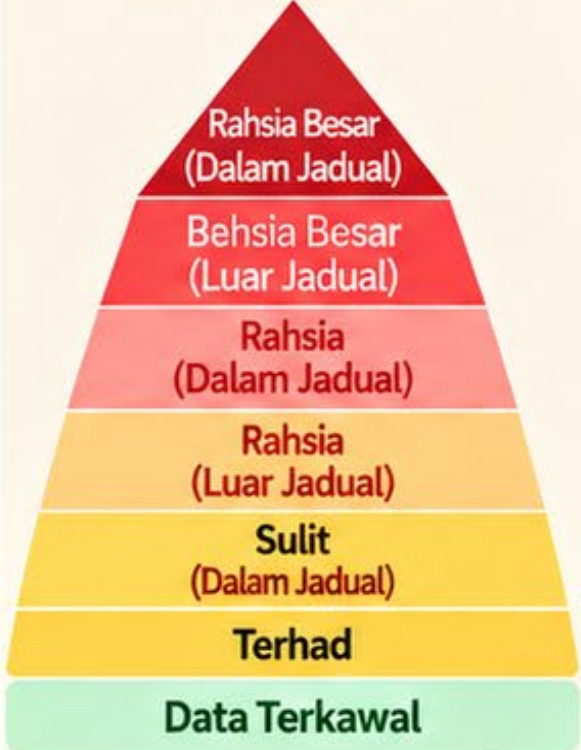
Menyokong fleksibiliti **Service-Generated**, **BYOK (Bring Your Own Key)**, dan **HYOK (Hold Your Own Key)**.



3

Klasifikasi Profil Jaminan

Selari dengan **Akta Rahsia Rasmi 1972** (TERHAD hingga RAHSIA BESAR).



4

Pengasingan Tenant (Tenant Isolation)

Struktur hierarki kunci yang memisahkan data antara agensi secara mutlak.



5

Katalog Perkhidmatan

Menyediakan fungsi kriptografi asas dan lanjutan menerusi API (Layan Diri / Self-Service).



Kesimpulan

Rangka kerja 5 pillar ini memastikan prototaip KMSaaS dibina dengan kukuh, selaras keperluan sektor awam, serta bersedia untuk masa hadapan.

INFORMATION CLASSIFICATION & ASSURANCE PROFILES

Berdasarkan Matrik Klasifikasi Maklumat (Akta Rahsia Rasmi 1972)

Classification	KMS Assurance Zone	HSM Isolation & Community Sharing	Deployment Baseline
Data Terkawal	Zone A (Protected)	- Community sharing dibenarkan - Shared HSM cluster dengan community partition atau tenant partition mengikut risiko	Fully Cloud, Hybrid H1/H2/H3 or Fully On-Premises based on risk
Terhad	Zone B (Classified)	- Community sharing dibenarkan dalam classified boundary - Dedicated community/tenant partition	Fully Cloud (<i>Not a baseline</i>), Hybrid H1/H2/H3 or Fully On-Premises
Sulit (Luar Jadual)	Zone B (Classified Enhanced)	- Community sharing conditional - Dedicated classified community/tenant partition dan admin separation	Hybrid H1/H2/H3 or Fully On-Premises with stronger segmentation
Sulit (Dalam Jadual)	Zone C (High-Assurance Isolated)	- No community sharing - Dedicated physical HSM cluster	Fully On-Premises
Rahsia (Luar Jadual)	Zone C (High-Assurance Isolated)	- No community sharing - Dedicated physical HSM cluster	Fully On-Premises
Rahsia (Dalam Jadual)	Zone C (High-Assurance Isolated)	Dedicated KMS/HSM/network/admin/audit domain	Fully On-Premises

Rahsia Besar (Luar Jadual)	Zone C (High-Assurance Isolated)	- Dedicated physical HSM cluster - Zero Trust - No shared service plane	Fully On-Premises	KC-4 Highest Assurance
Rahsia Besar (Dalam Jadual)	Zone C (High-Assurance Isolated)	- Isolate compute, network, identity, admin, HSM, audit, backup dan DR - Smallest named-user population	Fully On-Premises; individually assessed	KC-4+ Highest Assurance - Scheduled

Komponen Teras Infrastruktur Kriptografi

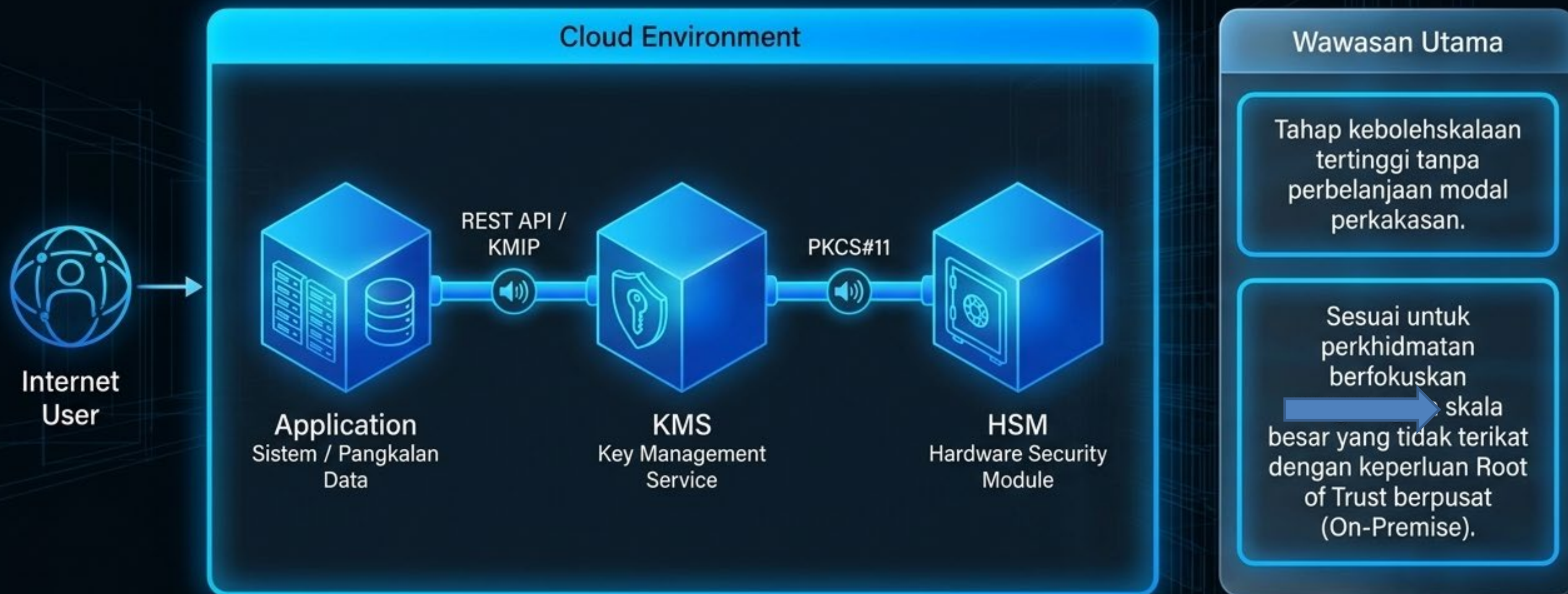


Kedudukan ketiga-tiga entiti ini dalam infrastruktur (Awan, Agensi, atau JDN) akan menentukan postur kedaulatan data anda.

Spektrum Penempatan: Imbangan Antara Kedaulatan dan Ketangkasan



Model 1: Awan Sepenuhnya (Fully Cloud)



Peralihan Ke **Hibrid**: Memisahkan Logik Aplikasi Dari Teras Kriptografi

Pendekatan **hibrid** membenarkan agensi memecahkan **silo**—menjalankan aplikasi di persekitaran berkelajuan tinggi sambil mengekalkan **kunci** (HSM) secara **berpusat** di fasiliti berdaulat.

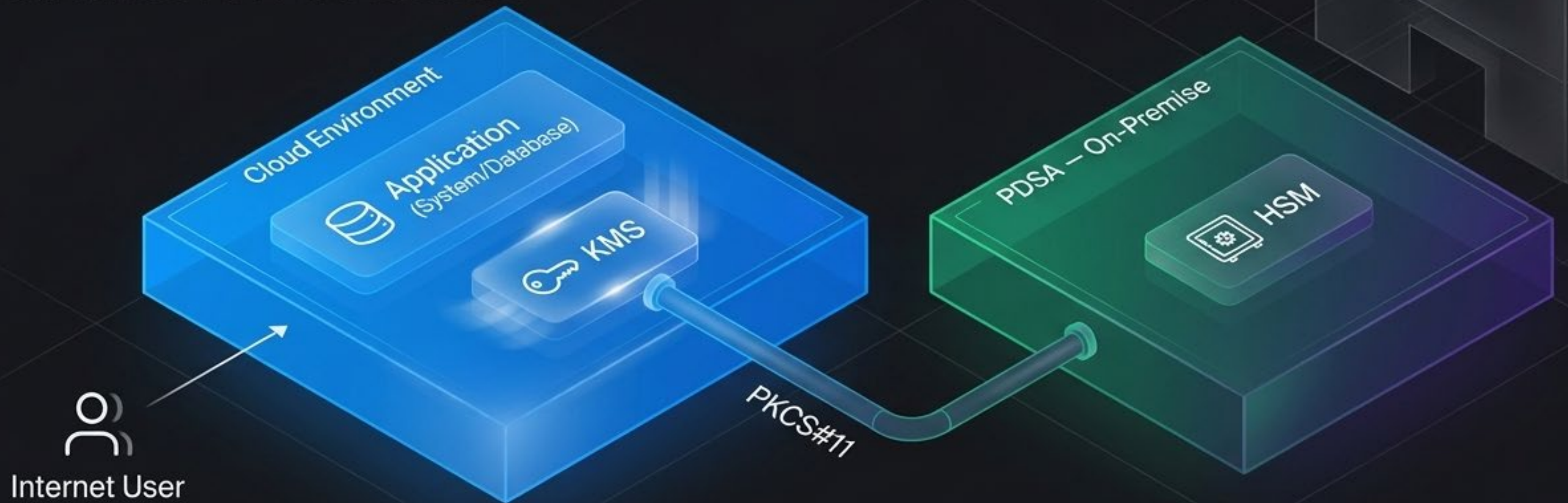
Model 2 (Hibrid H1): Kawalan Agensi Tempatan



KMS ditempatkan di dalam persekitaran agensi (atau premis JDN), manakala HSM ditempatkan di premis JDN.

Agensi memiliki **hak kawalan penuh** terhadap lapisan perkhidmatan KMS, tetapi Jabatan Digital Negara (JDN) memegang hak jagaan Root of Trust secara berpusat.

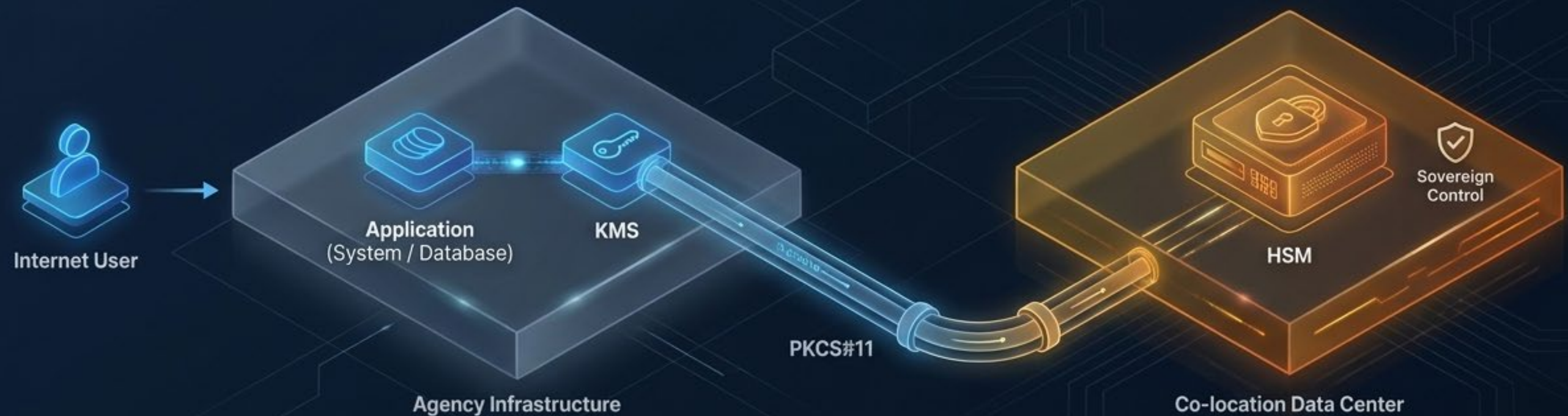
Model 2 (Hibrid H2): Kebolehskalaan Awan Bertemukan Kedaulatan



KMS dihoskan oleh Cloud Service Provider (CSP) untuk kebolehskalaan awan (cloud scalability) manakala HSM kekal berada di premis JDN.

Gabungan ideal: Aplikasi boleh mengembang mendadak di awan, tetapi kunci rumah infrastruktur negara tidak pernah meninggalkan fasiliti kerajaan.

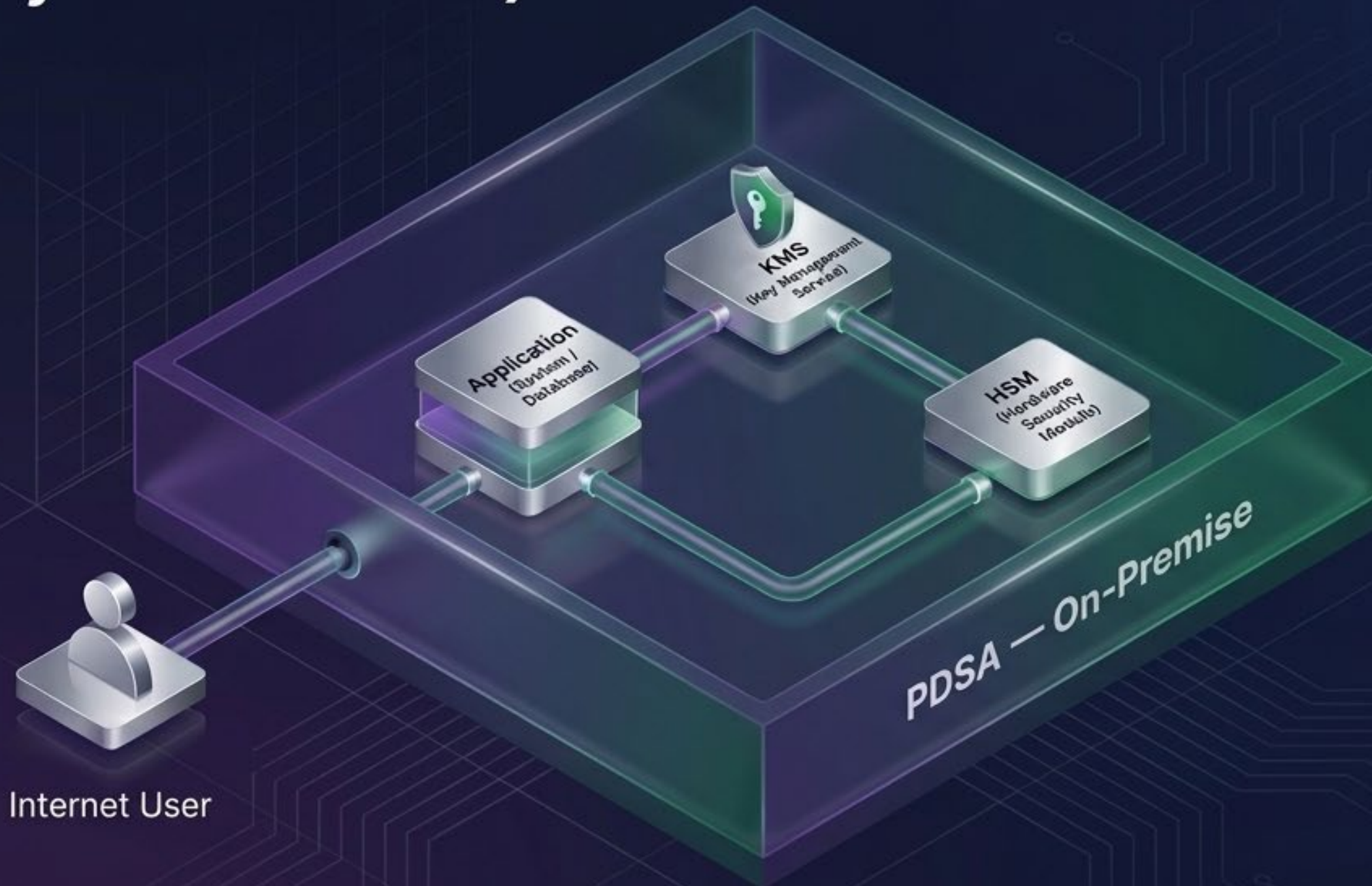
Model 2 (Hibrid H3): Peluasan Kedaulatan Melalui *Co-Location*



KMS berada di persekitaran agensi atau PDSA manakala HSM ditempatkan di fasiliti co-location yang diluluskan.

Sesuai untuk seni bina teragih (*distributed architecture*). Ia kekal tertakluk kepada kawalan kedaulatan (*sovereignty*) dan prosedur hak jagaan yang didokumenkan secara ketat.

Model 3: Di Premis Sepenuhnya (Fully On-Premises)



Wawasan Utama

Postur keselamatan
negara (CNII).
→ kritikal

Risiko luaran paling minimum kerana data dan operasi kriptografi tidak merentasi infrastruktur pihak ketiga. Tiada kebergantungan luar.

Rangka Kerja Keputusan Agensi



3 Manfaat Transformatif KMSaaS



Ketahanan Operasi & Automasi

Menghapuskan ralat manual.  kitaran hayat kunci (*key rotation*) secara automatik membebaskan masa pegawai IT untuk fokus kepada tugas strategik agensi.



Katalog Perkhidmatan Bersatu

Standardisasi di seluruh sektor awam (WOG). Menyatukan panggilan API kriptografi (TDE, Envelope Encryption, Tokenization) ke dalam satu portal layan diri yang mudah diintegrasikan.



Tadbir Urus & Akauntabiliti Mutlak

Visibiliti dan log audit masa nyata 100%. Merekodkan secara tepat siapa, bila, dan sistem mana yang memanggil kunci, menjadikan audit pematuhan semudah satu klik.

Inovasi Keselamatan: Sanitasi Data Kriptografi (CE)



Pematuhan Perundangan: Selaras dengan Garis Panduan Sanitasi Media Elektronik Sektor Awam (SPA Bil. 4/2022) & SPA 2/2021 v2. Ini adalah mekanisma sanitasi data paling pantas dan selamat untuk pelucutan perkhidmatan (*decommissioning*) di awan, tanpa perlu memusnahkan cakera keras fizikal.

Mandat & Ekosistem Perundangan (The Policy Shield)

Akta Rahsia Rasmi 1972 [Akta 88] (OSA)

Penentu hierarki klasifikasi maklumat

Akta Keselamatan Siber 2024 (Akta 854)

Mematuhi keperluan infrastruktur maklumat kritikal negara (NCII).

Arahan Keselamatan 2017 (Para 139)

Mandat perlindungan fizikal dan logikal.

Garis Panduan CFA (SPA Bil. 2/2021 v2)

Pematuhan residensi awan, klasifikasi data rahsia rasmi, dan pengurusan kriptografi.

Arahan Keselamatan 2017

Garis Panduan CFA (SPA Bil. 2/2021 v2)

Peralihan kepada KMSaaS bukan lagi satu opsyen teknikal, sebaliknya instrumen wajib bagi memastikan agensi mematuhi perundangan keselamatan dan kedaulatan data tertinggi negara.

Kalis Masa Depan (Future-Proofing): Menuju 2030



Menuju Kedaulatan Digital Sektor Awam yang Mutlak

Transformasi ke KMSaaS adalah anjakan dari kerumitan manual kepada automasi pintar. Ia memacu pematuhan dasar, melindungi aset strategik, dan membina kepercayaan perkongsian data negara.



Sesi Soal Jawab (Q&A)
Jabatan Digital Negara, Kementerian Digital