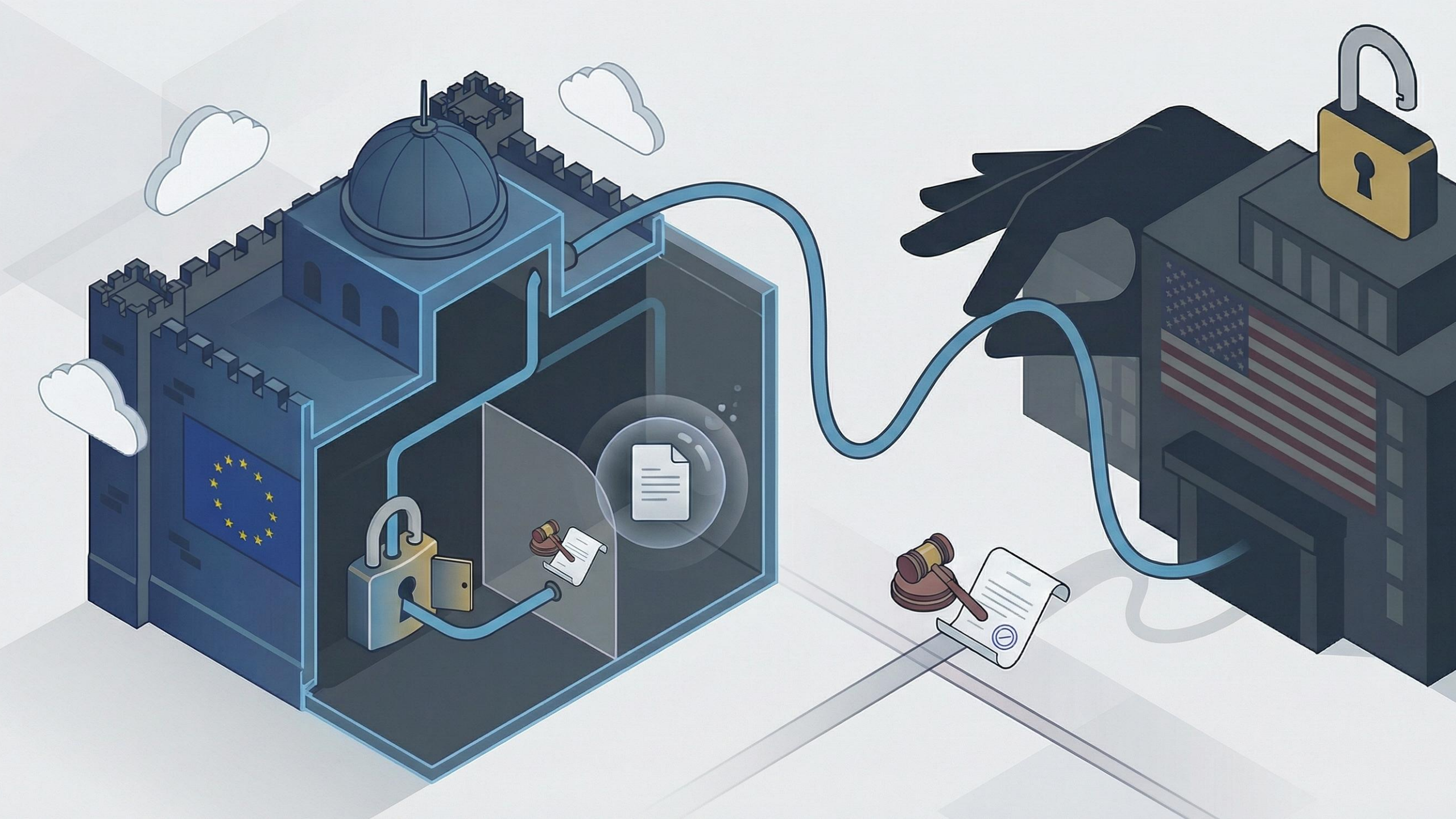
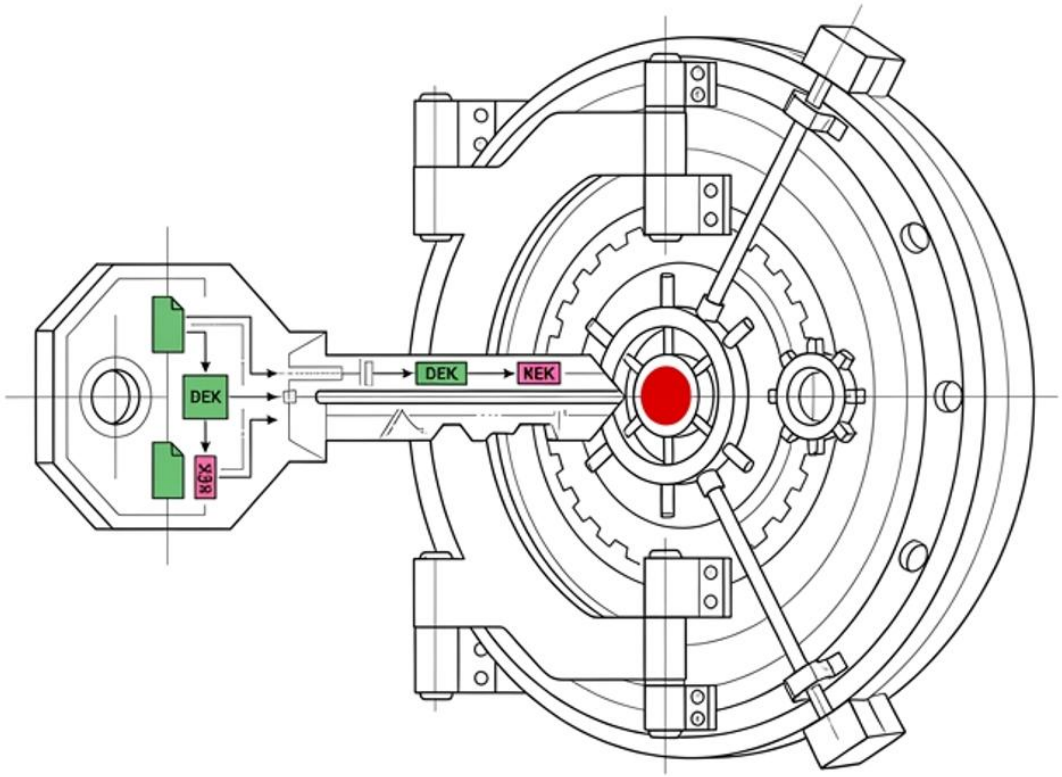




Marknadsföring som efterlevnadsmodell för molntjänster

Skövde 2026-04-29

AITYR

André Catry

- **Entrepreneur**
  - Aityr, Caty Consulting, C-Resiliens, Tutus Data, Mollitiam , Nationellt SensorSystem , Týr Cyber Defense
- **Author**
  - Honungsapan, Tigerögat, Solroskoden
- **Advisor**
  - Chief engineer / IT & Security Architect SAAB (Consultant)
  - Lawfirm Kahn Pedersen (Consultant)
- **Security expert /Lead Security Consultant**
  - IT & Security Architect / Investigator / Analyst / IT-Forensics
- **Security Consultant**
  - IT defense unit (ITF)
  - Military Intelligence & Security Service MUST (CERT)
- **Avdelningsdirektör (Principal administrative officer)**
  - IT security advisor to government agencies
  - Computer Forensics / Investigations
  - Lawful interception
- **Departementssekreterare (First Secretary, Desk Officer)**
  - IT security, 4 years embassy Moskva
  - Project manager

USA:s extraterritoriella räckvidd

- FISA (1978), EO 12333 (1981), Patriot Act (2001), FISA 702 (2008), CLOUD Act (2018)

AITYR

USA:s extraterritoriella räckvidd

- FISA (1978), EO 12333 (1981), Patriot Act (2001), FISA 702 (2008), CLOUD Act (2018)
- Dataavtal mellan EU och USA
  - Safe Harbor (2000),

AITYR

USA:s extraterritoriella räckvidd

- FISA (1978), EO 12333 (1981), Patriot Act (2001), FISA 702 (2008), CLOUD Act (2018)
- Dataavtal mellan EU och USA
  - ~~Safe Harbor (2000),~~
  - Privacy Shield (2016),

AITYR

USA:s extraterritoriella räckvidd

- FISA (1978), EO 12333 (1981), Patriot Act (2001), FISA 702 (2008), CLOUD Act (2018)
- Dataavtal mellan EU och USA
  - ~~Safe Harbor (2000),~~
  - ~~Privacy Shield (2016),~~
  - EU:s och USA:s ramverk för dataskydd DPF (2023) – (PCLOB!!!)

AITYR

USA:s extraterritoriella räckvidd

- FISA (1978), EO 12333 (1981), Patriot Act (2001), FISA 702 (2008), CLOUD Act (2018)
- Dataavtal mellan EU och USA
  - ~~Safe Harbor (2000),~~
  - ~~Privacy Shield (2016),~~
  - EU:s och USA:s ramverk för dataskydd DPF (2023) – (PCLOB!!!)
- Medför exponering mot utländsk jurisdiktion

AITYR

SECRET//COMINT//REL TO USA, AUS, CAN, GBR//20291123

United States SIGINT System
January 2007 Strategic Mission List

Introduction – Director's Intent

(S//SI) The SIGINT Strategic Mission List represents the intent of the Director, National Security Agency in regard to mission priorities and risks for the United States SIGINT System (USSS) over the next 12-18 months. The list is derived from review of the Intelligence Community National Intelligence Priorities Framework, DCI/DNI Guidance, the Strategic Warning List, National SIGINT Requirements Process (NSRP) and other strategic planning documents. The missions included on the list are in relative priority order and represent the most urgent tasks for the USSS. The list is not intended to be all encompassing, but is intended to set forth guidance on the highest priorities.

Topical Missions and Enduring Targets

(S//SI) The SIGINT Strategic Mission List is divided into two parts. It includes 16 critical topical missions in Part I of the list, which represent missions discerned to be areas of highest priority for the USSS, where SIGINT can make key contributions. In addition to the 16 critical topical missions, Part II of the SIGINT Strategic Mission List includes 6 enduring targets that are included due to the need to work these targets holistically because of their strategic importance. In addition to their long-term strategic importance, the enduring targets can potentially "trump" the highest priority topical missions on the list at any time, based upon evolving world events. Elements of these targets are also represented throughout the topical target sets. For each of the 16 topical missions and each of the 6 enduring targets the Strategic Mission List includes:

1) Focus Areas – critically important targets against which the SIGINT enterprise is placing emphasis. DIRNSA designation of a target as a focus area constitutes his guidance to the SIGINT System that it is a "must do" target for that mission.

2) Accepted Risks – strategically significant targets against which the USSS is not placing emphasis and for which SIGINT should not be relied upon as a primary source. DIRNSA's reasons for accepting these risks include high difficulty and lack of resources or as an "Economy of Force Measure," in order to achieve focus on the most critical targets.

United States SIGINT System
January 2007 Strategic Mission List

(S//SI) **J. MISSION: Emerging Strategic Technologies: Preventing Technological Surprise.**
Focus Areas: Critical technologies that could provide a strategic military, economic, **or political** advantage: high energy lasers, low energy lasers, advances in computing and information technology, directed energy weapons, **stealth and counter-stealth**, electronic warfare technologies, space and remote sensing, electro-optics, nanotechnologies, energetic materials. The emerging strategic technology threat is expected to come mainly from Russia, China, India, Japan, Germany, France, Korea, Israel, Singapore, and Sweden.
Accepted Risks: Technological advances and/or basic S&T development on a global basis elsewhere.

Sverige

Den legala hotbilden: **Amerikansk lagstiftning i svenskt moln**

USA → EU

CLOUD Act

(Clarifying Lawful Overseas Use of Data)

Ger amerikanska myndigheter befogenhet att kräva ut data från amerikanska molnleverantörer, oavsett var i världen servrarna fysiskt står (t.ex. i ett datacenter i Sverige).

FISA 702

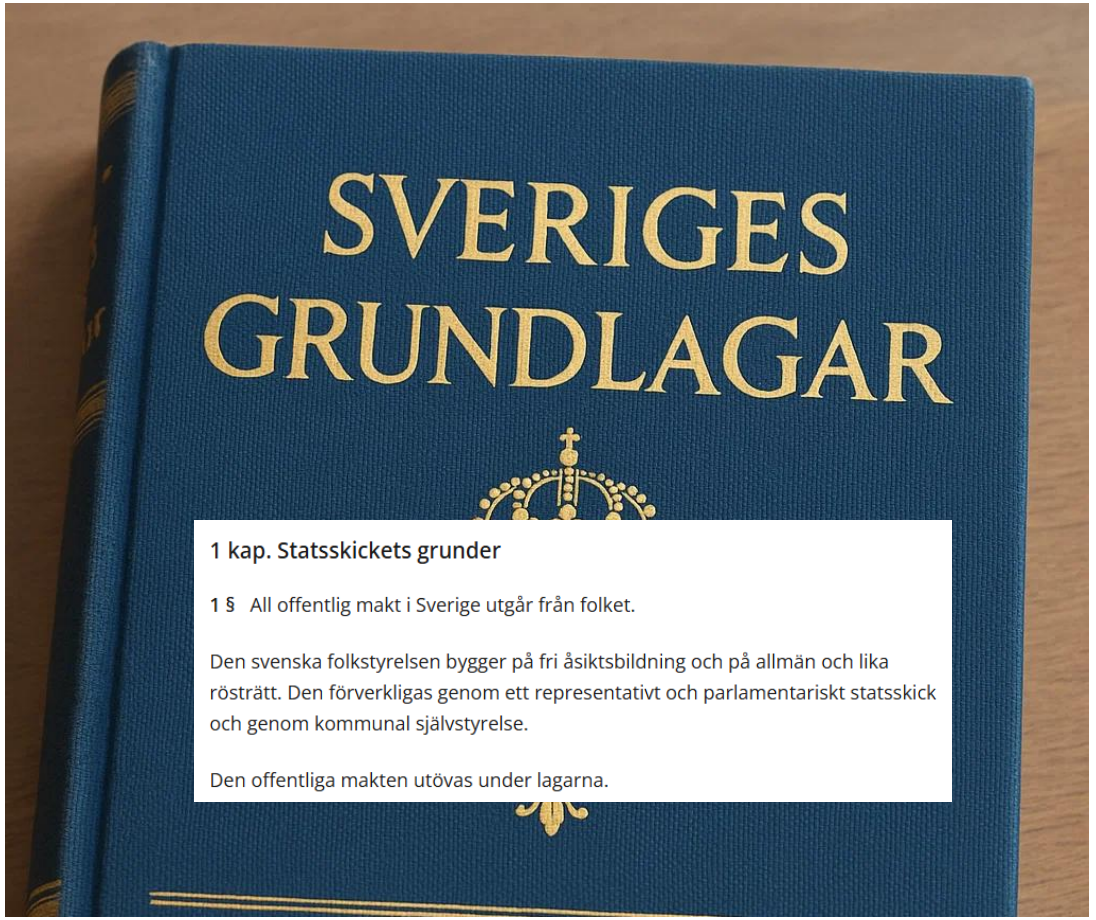
(Foreign Intelligence Surveillance Act)

Möjliggör riktad signalspaning och övervakning mot icke-amerikanska medborgare utanför USA. Kräver inget traditionellt domstolsbeslut (warrant) för specifika sökningar.

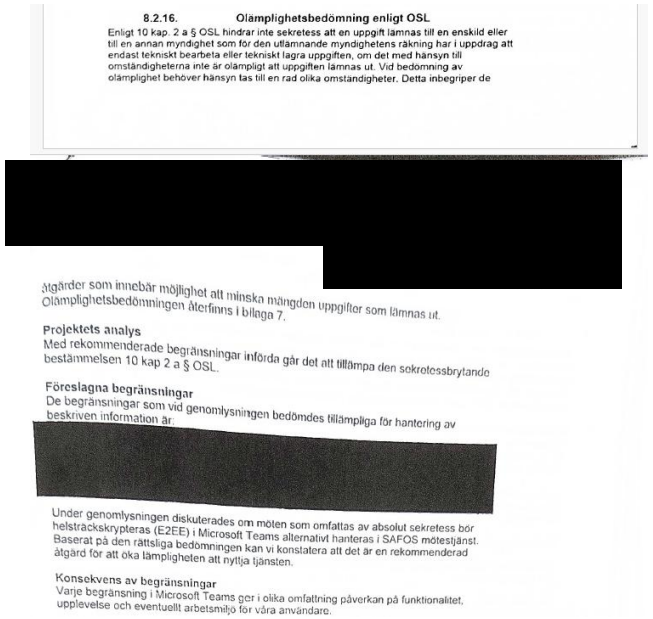
Slutsats: Lokala datacenter och GDPR trumfar inte amerikanska leverantörers skyldighet att följa amerikansk lag för nationell säkerhet.

Svensk författningssamling

- I Sveriges grundlag står det:
  - *All offentlig makt i Sverige utgår från folket.*
  - *Den offentliga makten utövas **under lagarna**.*
- Digital suveränitet måste vara förankrad i **svensk jurisdiktion**.



AITYR



8.2.16. Olämplighetsbedömning enligt OSL

Enligt 10 kap. 2 a § OSL hindrar inte sekretess att en uppgift lämnas till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut. Vid bedömning av olämplighet behöver hänsyn tas till en rad olika omständigheter. Detta inbegriper de

[redacted]

åtgärder som innebär möjlighet att minska mängden uppgifter som lämnas ut.
Olämplighetsbedömningen återfinns i bilaga 7.

Projektets analys

Med rekommenderade begränsningar införda går det att tillämpa den sekretessbrytande bestämmelsen 10 kap 2 a § OSL.

Föreslagna begränsningar

De begränsningar som vid genomlysningen bedömdes tillämpliga för hantering av beskriven information är:

[redacted]

Under genomlysningen diskuterades om möten som omfattas av absolut sekretess bör helsträckskrypteras (E2EE) i Microsoft Teams alternativt hanteras i SAFOS mötestjänst. Baserat på den rättsliga bedömningen kan vi konstatera att det är en rekommenderad åtgärd för att öka lämpligheten att nyttja tjänsten.

Konsekvens av begränsningar

Varje begränsning i Microsoft Teams ger i olika omfattning påverkan på funktionalitet, upplevelse och eventuellt arbetsmiljö för våra användare.

8.2.16. Olämplighetsbedömning enligt OSL

Enligt 10 kap. 2 a § OSL hindrar inte sekretess att en uppgift lämnas till en enskild eller till en annan myndighet som för den utlämnande myndighetens räkning har i uppdrag att endast tekniskt bearbeta eller tekniskt lagra uppgiften, om det med hänsyn till omständigheterna inte är olämpligt att uppgiften lämnas ut. Vid bedömning av olämplighet behöver hänsyn tas till en rad olika omständigheter. Detta inbegriper de åtgärder som innebär möjlighet att minska mängden uppgifter som lämnas ut. Olämplighetsbedömningen återfinns i bilaga 7.

Projektets analys

Med rekommenderade begränsningar införda går det att tillämpa den sekretessbrytande bestämmelsen 10 kap 2 a § OSL.

Föreslagna begränsningar

De begränsningar som vid genomlysningen bedömdes tillämpliga för hantering av beskriven information är:

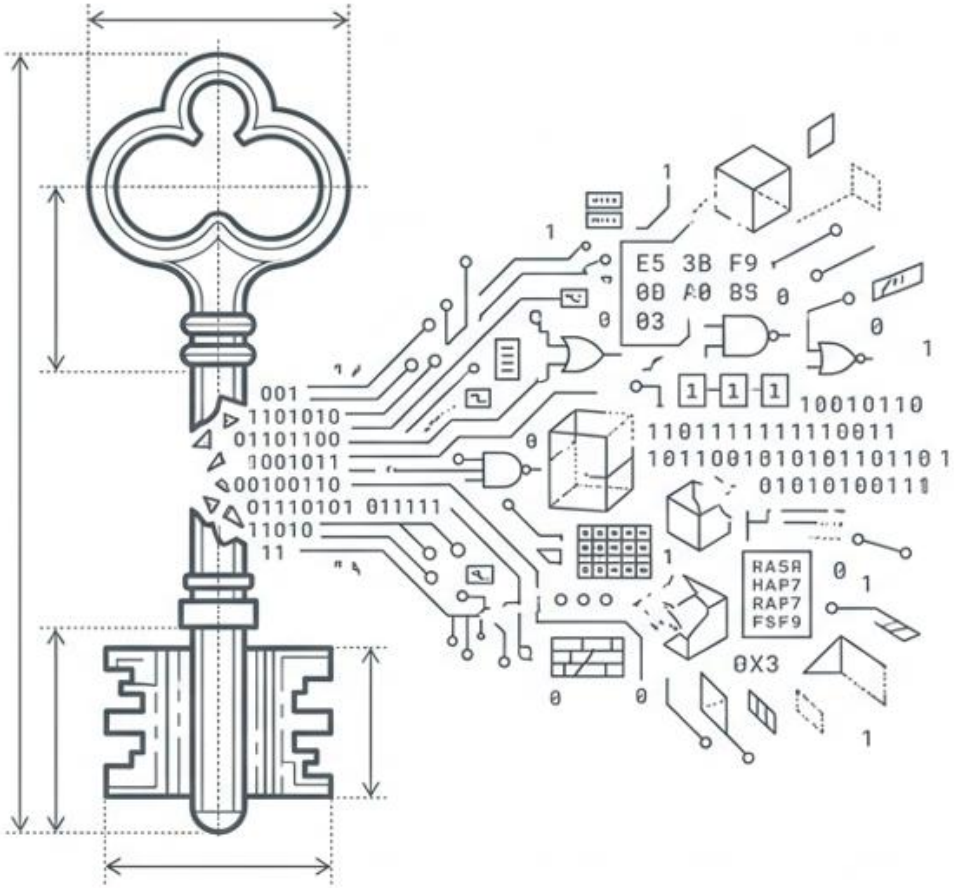
Under genomlysningen diskuterades om möten som omfattas av absolut sekretess bör helsträckskrypteras (E2EE) i Microsoft Teams alternativt hanteras i SAFOS mötestjänst. Baserat på den rättsliga bedömningen kan vi konstatera att det är en rekommenderad åtgärd för att öka lämpligheten att nyttja tjänsten.

Konsekvens av begränsningar

Varje begränsning i Microsoft Teams ger i olika omfattning påverkan på funktionalitet, upplevelse och eventuellt arbetsmiljö för våra användare.

I Microsoft Teams finns möjligheten att använda totalsträckskryptering, även kallad end-to-end-kryptering (E2EE). Den används för att man ska kunna säkerställa att endast kommunikationsdeltagama kan dekryptera innehållet. Kommunikation i Microsoft 365 genomförs alltid minst med standardkryptering via transport layer security (TLS).
E2EE sker dock endast vid tvåpartssamtal och inte i chattfunktionen i Teams i standardversionen. För att utnyttja totalsträckskryptering vid möten med fler än två personer, s.k. flerpartssamtal, krävs Teams Premium. I dagsläget stödjs inte totalsträckskryptering i chattar, men man kan minska risken genom att utbilda användarna och i viss utsträckning ta fram DLP-regler som förhindrar att sådana data delas i Teamschattar. Vidare kan man stänga av möjligheten till chatt genom mallar för olika typer av möten.
Microsoft Teams Premium Premiumversionen av Teams erbjuder utökad funktionalitet:
1. Totalsträckskryptering för flerpartssamtal: Med denna kryptering kan man säkerställa att alla flerpartssamtal är skyddade, att känslig information förblir konfidentiell och att Microsoft inte kan ta del av dessa data.

Kryptering verkar vara lösningen



AITYR

Löftet om Digital Suveränitet

AWS Digital Sovereignty Pledge: **Control** without compromise.

Microsoft Azure: **Sovereignty** by design. Empowering organizations to maintain control.

Google Cloud: Maintain **control** over your data and how it is processed.

Löftet om Digital Suveränitet

AWS Digital Sovereignty Pledge: **Control** without compromise.

Microsoft Azure: **Sovereignty** by design. Empowering organizations to maintain control.

Google Cloud: Maintain **control** over your data and how it is processed.

Budskapet är enhetligt: Lagra data inom EU, Kryptera din data, äg din nyckeln (BYOK, HYOK), då har ni Digital Suveränitet.

AITYR

Krypteringens byggstenar: DEK och KEK

DEK (Data Encryption Key)

Representeras i grönt. Den faktiska nyckeln som krypterar er data. För att molntjänsten ska kunna läsa eller skriva data, måste denna nyckel packas upp ur sitt rosa kuvert.

KEK (Key Encryption Key)

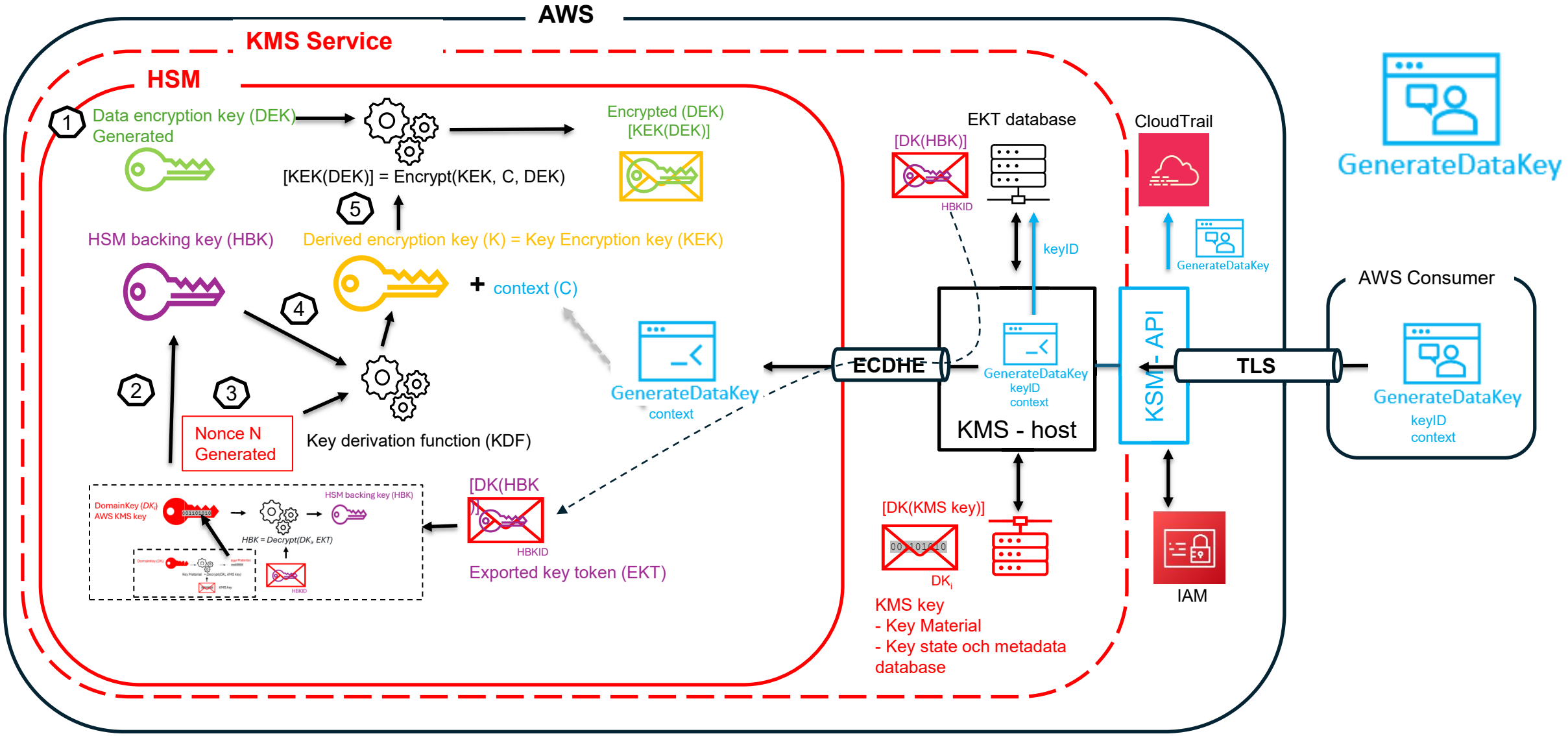
Representeras i rosa. Den övergripande nyckeln som kunden hanterar och roterar. Används uteslutande för att slå in (wrap) och skydda datanycklar.

Vad säger dokumentation

The HSM does the following:

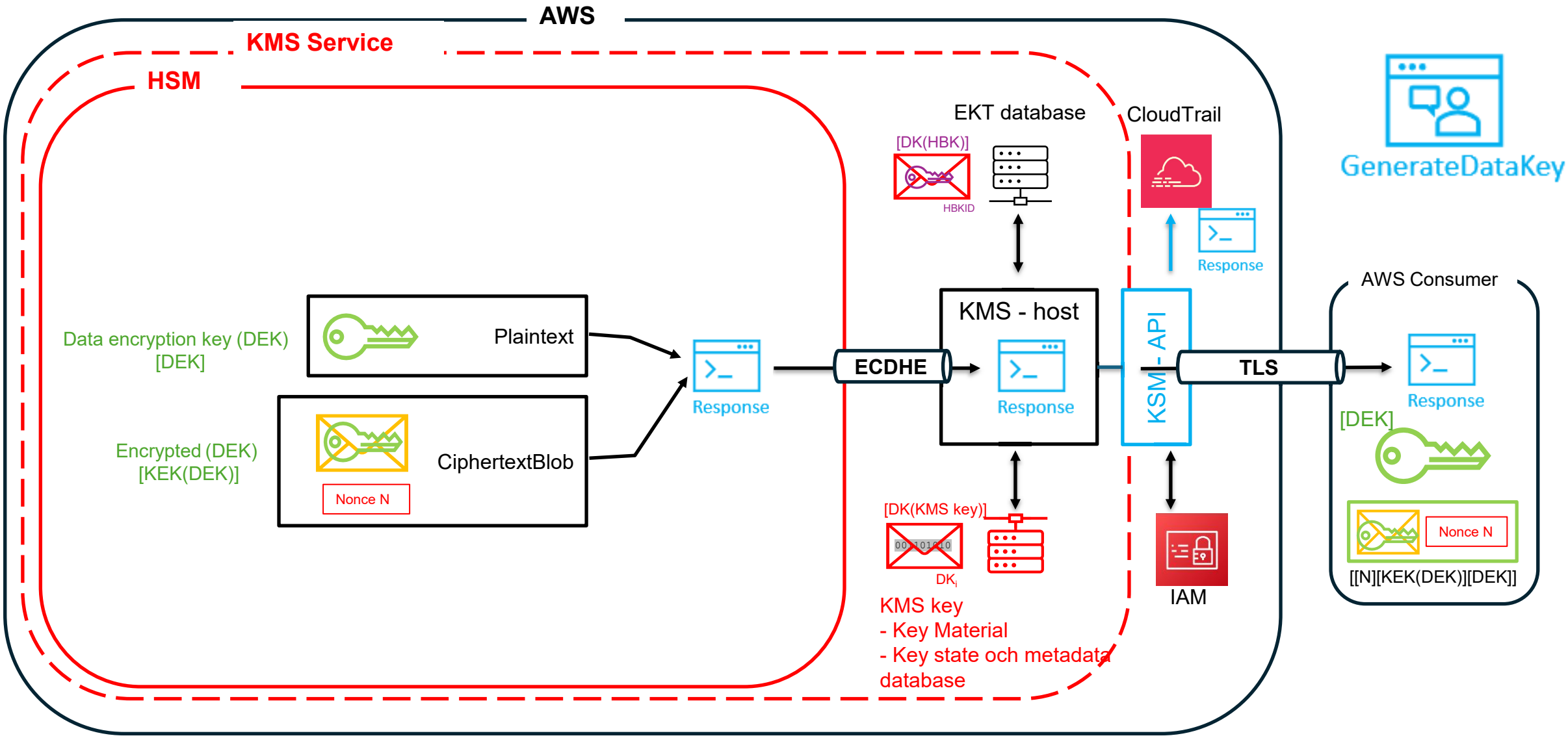
- Generates the requested secret material and hold it in volatile memory.
- Decrypts the *EKT* matching the key ID of the KMS key that is defined in the request to obtain the active *HBK* = *Decrypt(DKi, EKT)*.
- Generates a random nonce *N*.
- Generates a 256-bit AES-GCM derived encryption key *K* from *HBK* and *N*.
- Encrypts the secret material ciphertext = *Encrypt(K, context, secret)*

https://docs.aws.amazon.com/kms/latest/cryptographic-details/generating-data-keys.html



https://docs.aws.amazon.com/kms/latest/cryptographic-details/generating-data-keys.html

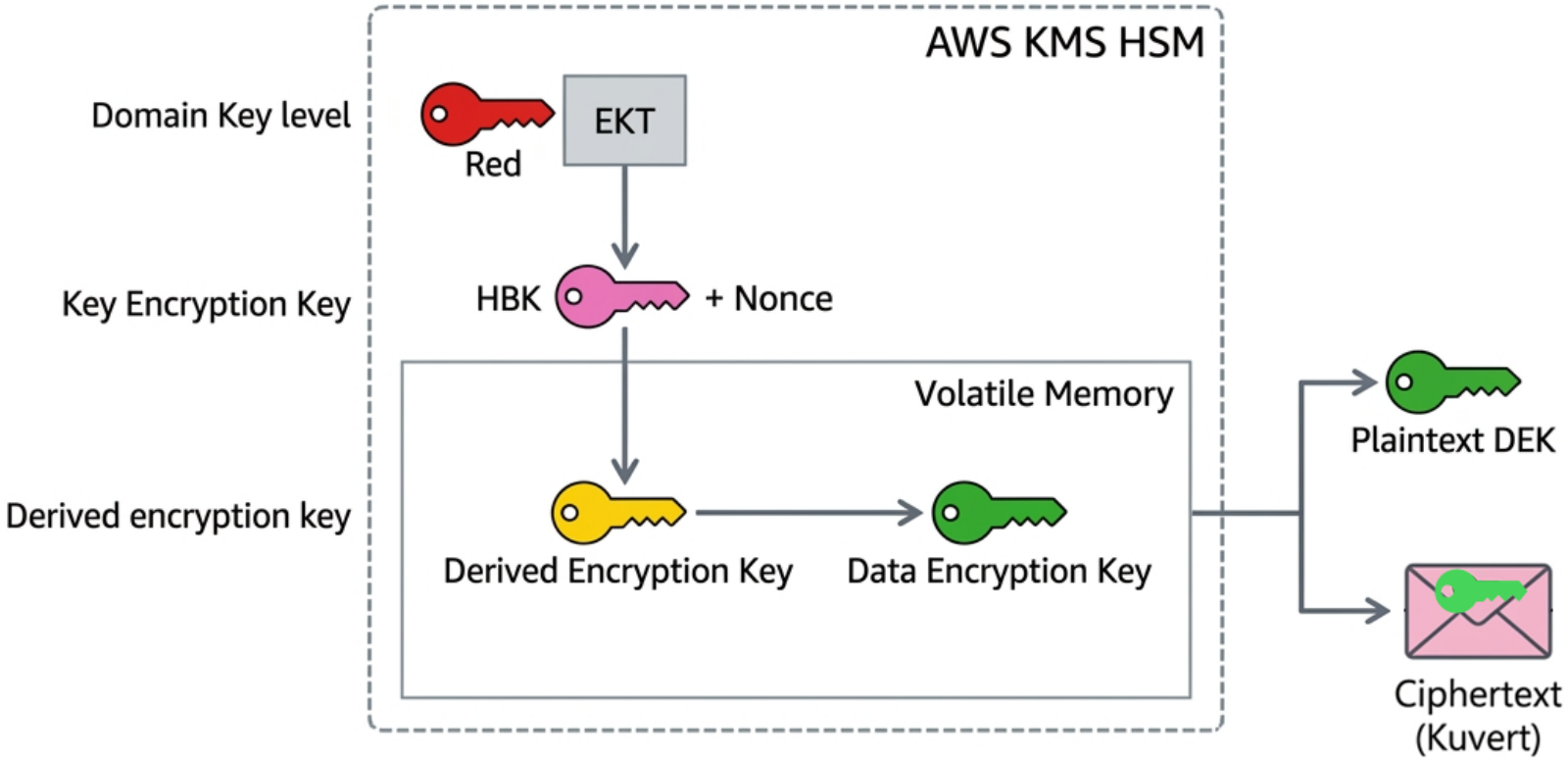
AITYR



https://docs.aws.amazon.com/kms/latest/cryptographic-details/generating-data-keys.html

AITYR

Kuvertkryptering: Först skapa nycklar

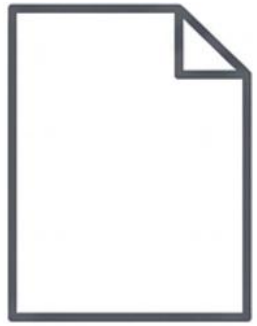


AWS KMS behåller varken klartexten eller chiffertexten efter att TLS-sessionen stängts.

AITYR

Kuvertkryptering

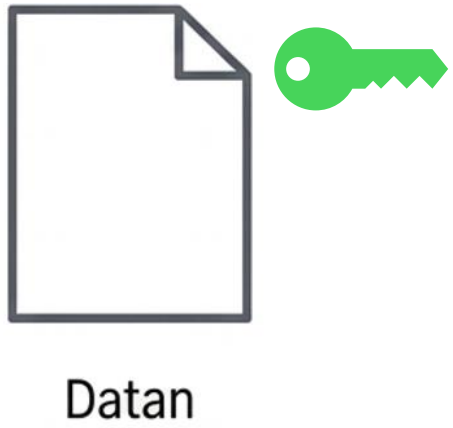
För att hantera miljontals krypteringsoperationer utan att överbelasta systemet, krypterar AWS/Microsoft/Googel inte datan med huvudnyckeln. De använder kuvertkryptering (Envelope Encryption).



Datan

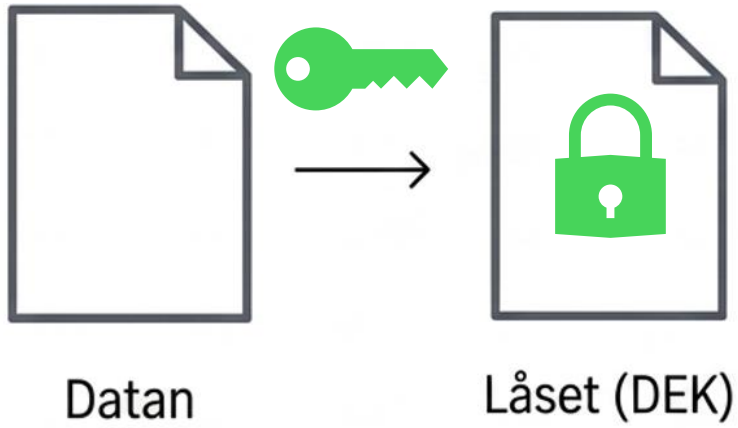
Kuvertkryptering

För att hantera miljontals krypteringsoperationer utan att överbelasta systemet, krypterar AWS/Microsoft/Googel inte datan med huvudnyckeln. De använder kuvertkryptering (Envelope Encryption).



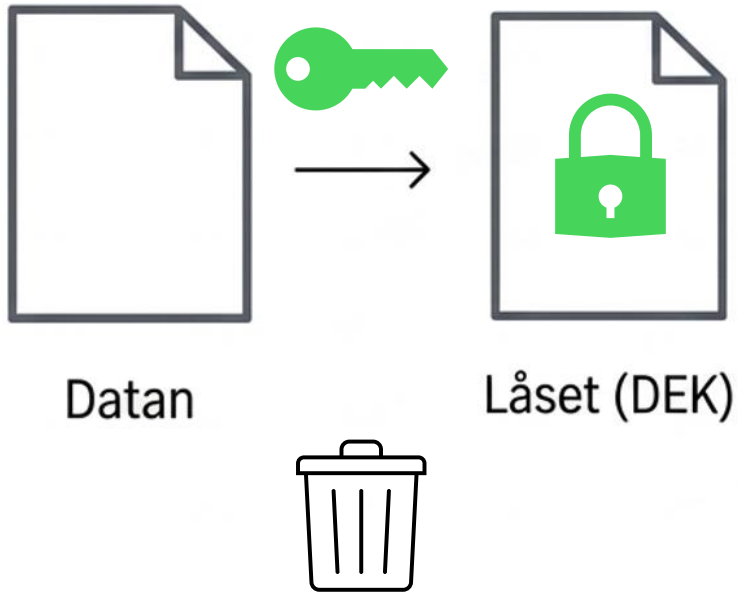
Kuvertkryptering

För att hantera miljontals krypteringsoperationer utan att överbelasta systemet, krypterar AWS/Microsoft/Googel inte datan med huvudnyckeln. De använder kuvertkryptering (Envelope Encryption).



Kuvertkryptering

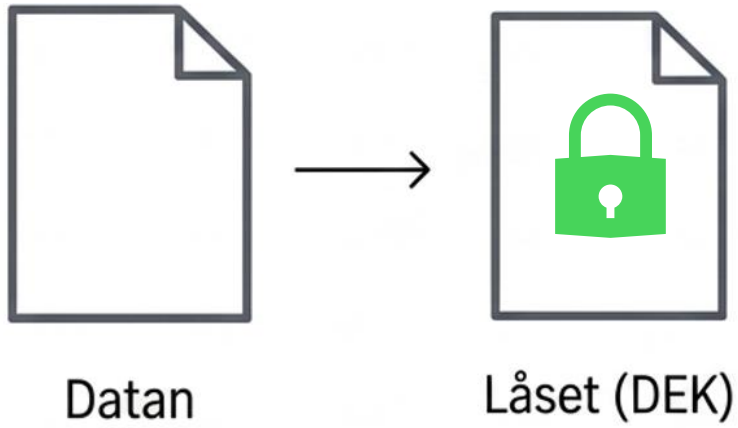
För att hantera miljontals krypteringsoperationer utan att överbelasta systemet, krypterar AWS/Microsoft/Googel inte datan med huvudnyckeln. De använder kuvertkryptering (Envelope Encryption).



AITYR

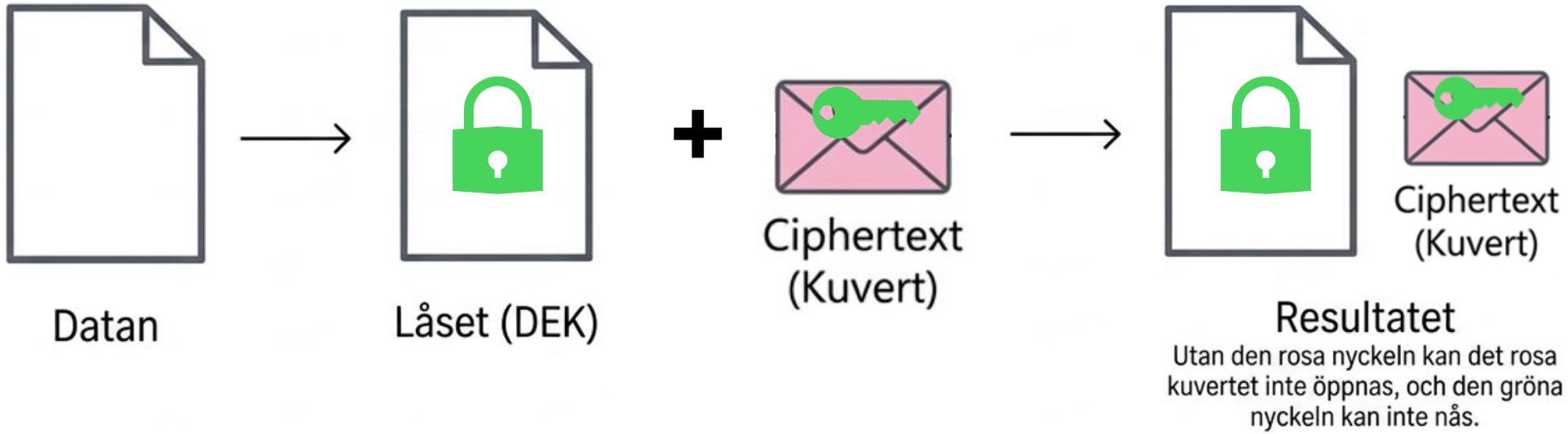
Kuvertkryptering

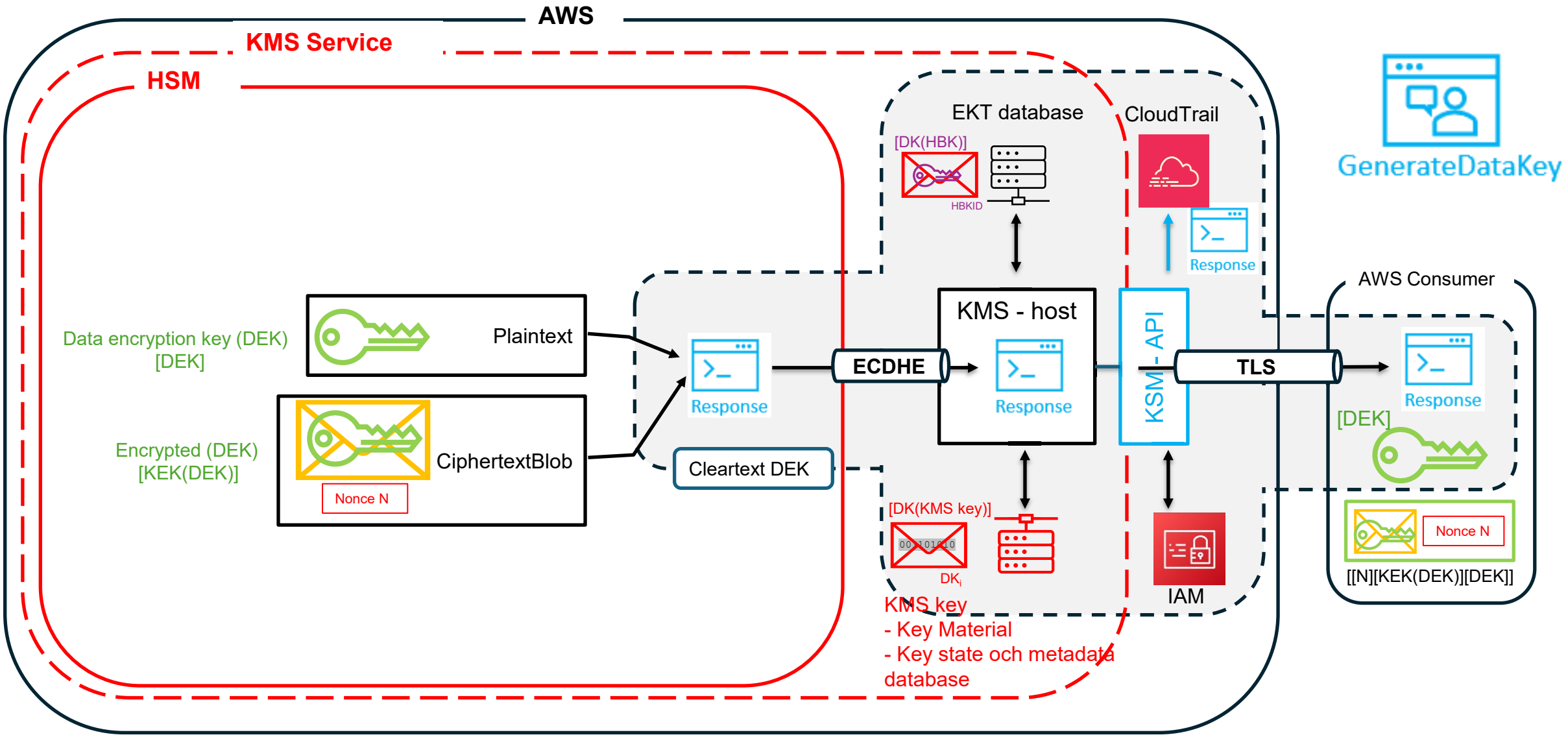
För att hantera miljontals krypteringsoperationer utan att överbelasta systemet, krypterar AWS/Microsoft/Googel inte datan med huvudnyckeln. De använder kuvertkryptering (Envelope Encryption).



Kuvertkryptering

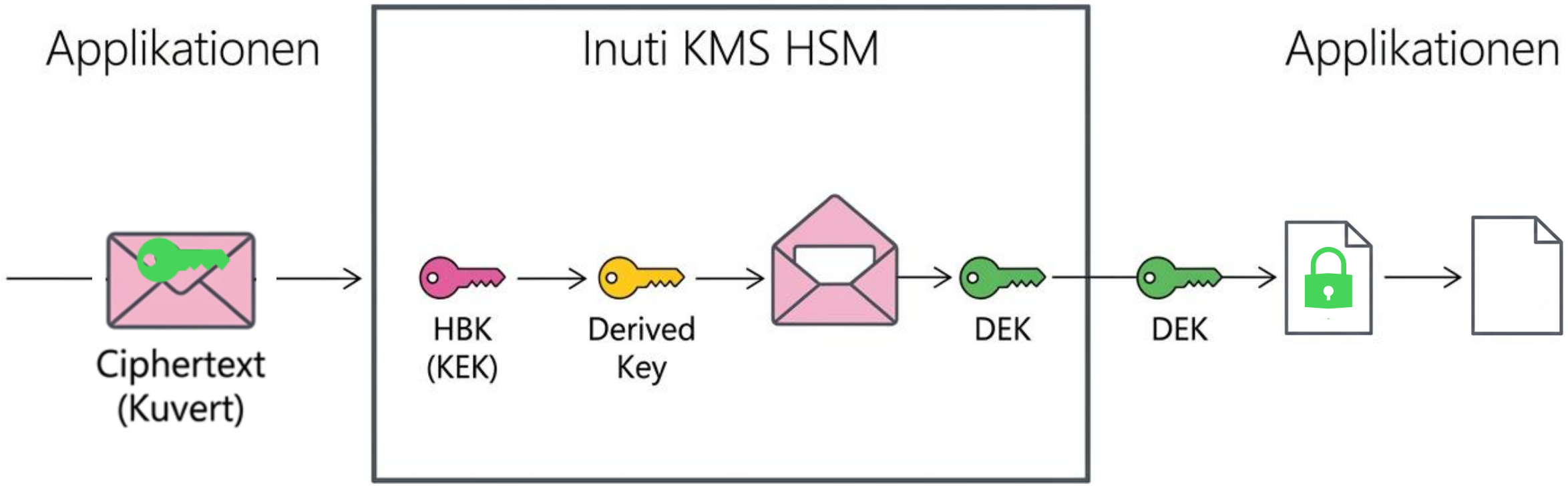
För att hantera miljontals krypteringsoperationer utan att överbelasta systemet, krypterar AWS/Microsoft/Googel inte datan med huvudnyckeln. De använder kuvertkryptering (Envelope Encryption).



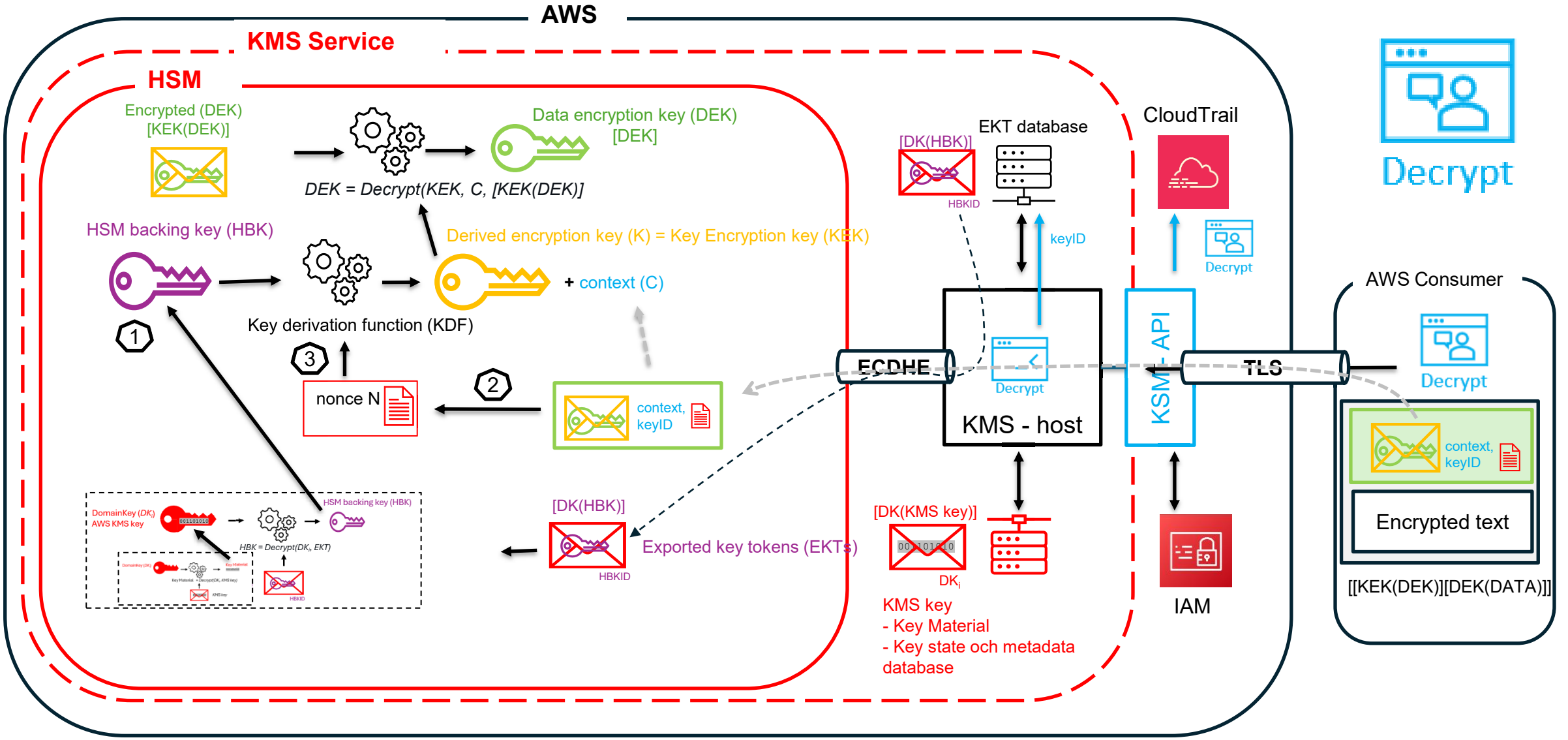


AITYR

Dekryptering: Uppackningen av kuvertet



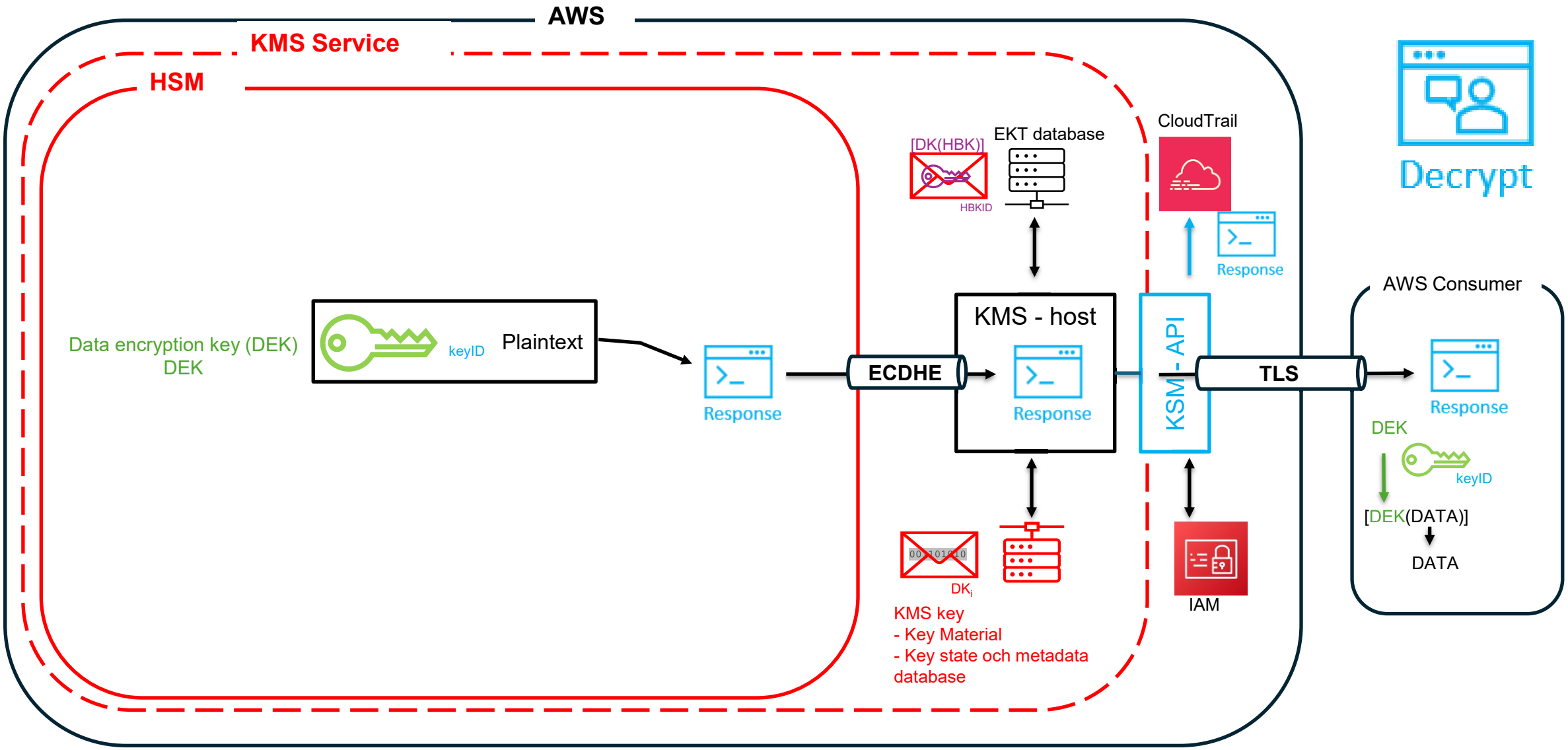
AITYR



The HSM runs the following:
1.Decrypts the *EKT* to obtain the *HBK = Decrypt(DK_j, EKT)* .
2.Extracts the nonce *N* from the *ciphertext* structure.
3.Regenerates a 256-bit AES-GCM derived encryption key *K* from *HBK* and *N*.
4.Decrypts the *ciphertext* to obtain *plaintext = Decrypt(K, context, ciphertext)* .

https://docs.aws.amazon.com/kms/latest/cryptographic-details/decrypt-operation.html

AITYR



The resulting key ID and plaintext are returned to the AWS KMS host over the secure session and then back to the calling customer application over a TLS connection.

AITYR

Den falska tryggheten

Illusionen.

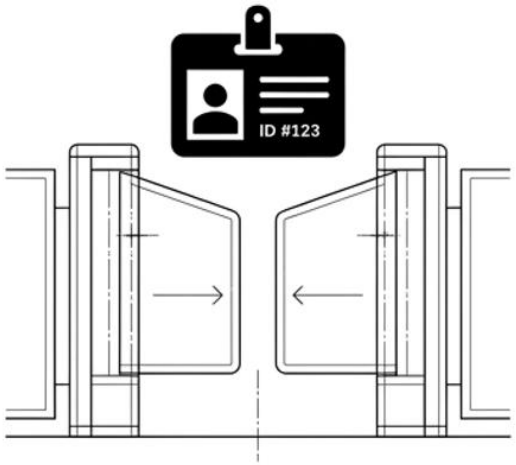
Organisationer antar att genom att äga och hantera sina egna krypteringsnycklar (KEK) uppnås total kryptografisk suveränitet, oberoende av molnleverantören.

AITYR

Den falska tryggheten

Illusionen.

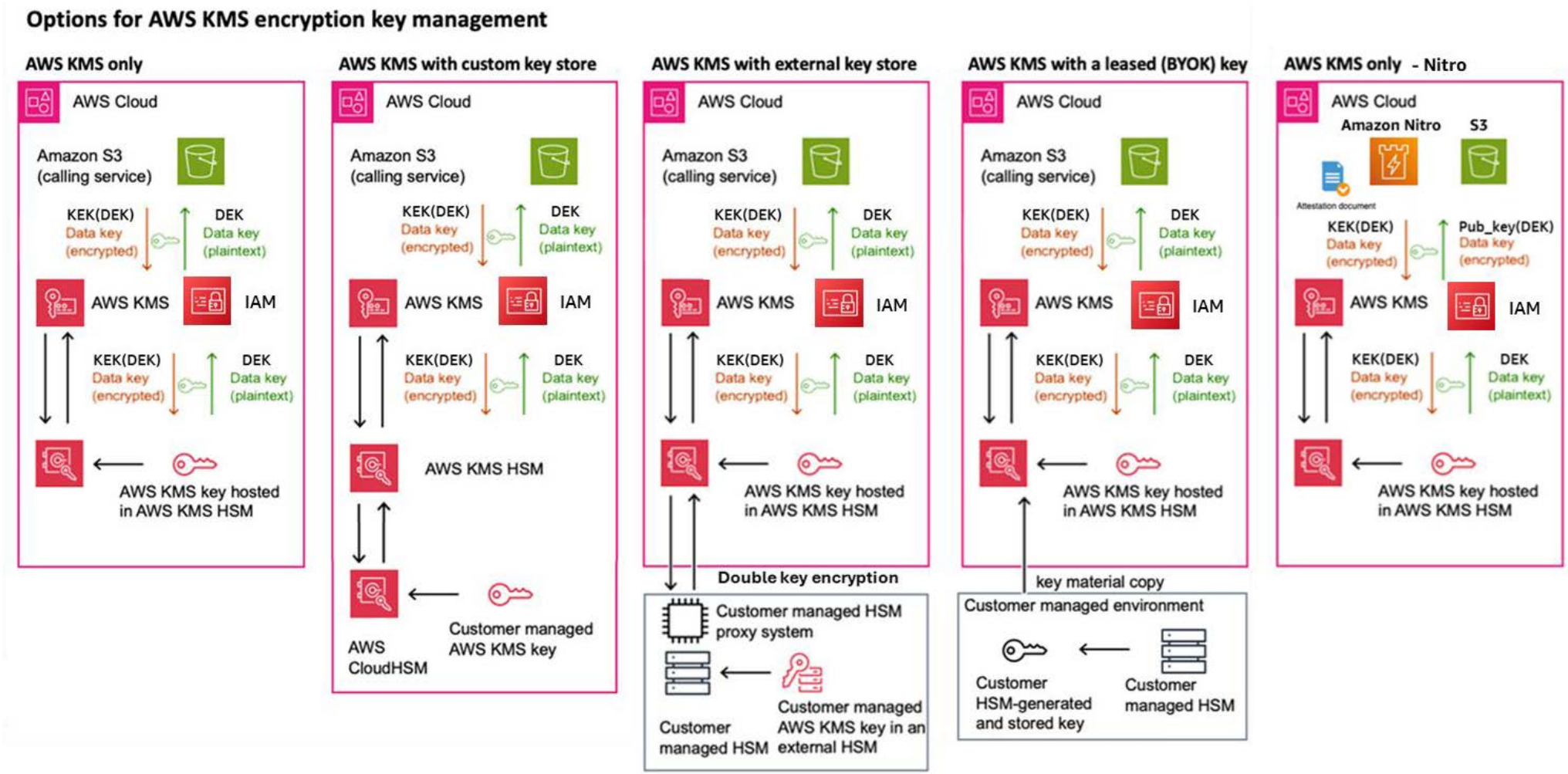
Organisationer antar att genom att äga och hantera sina egna krypteringsnycklar (KEK) uppnås total kryptografisk suveränitet, oberoende av molnleverantören.

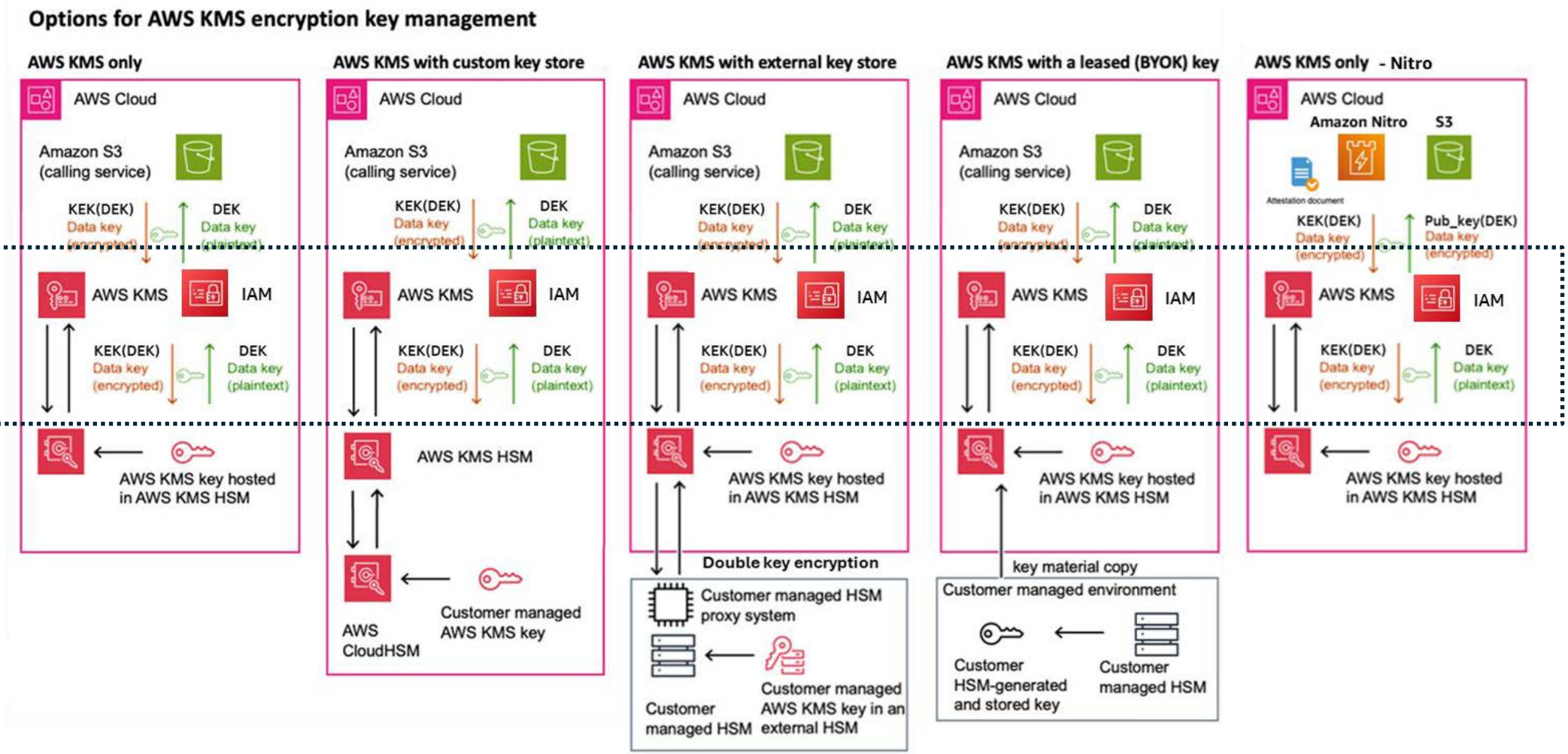


Verkligheten.

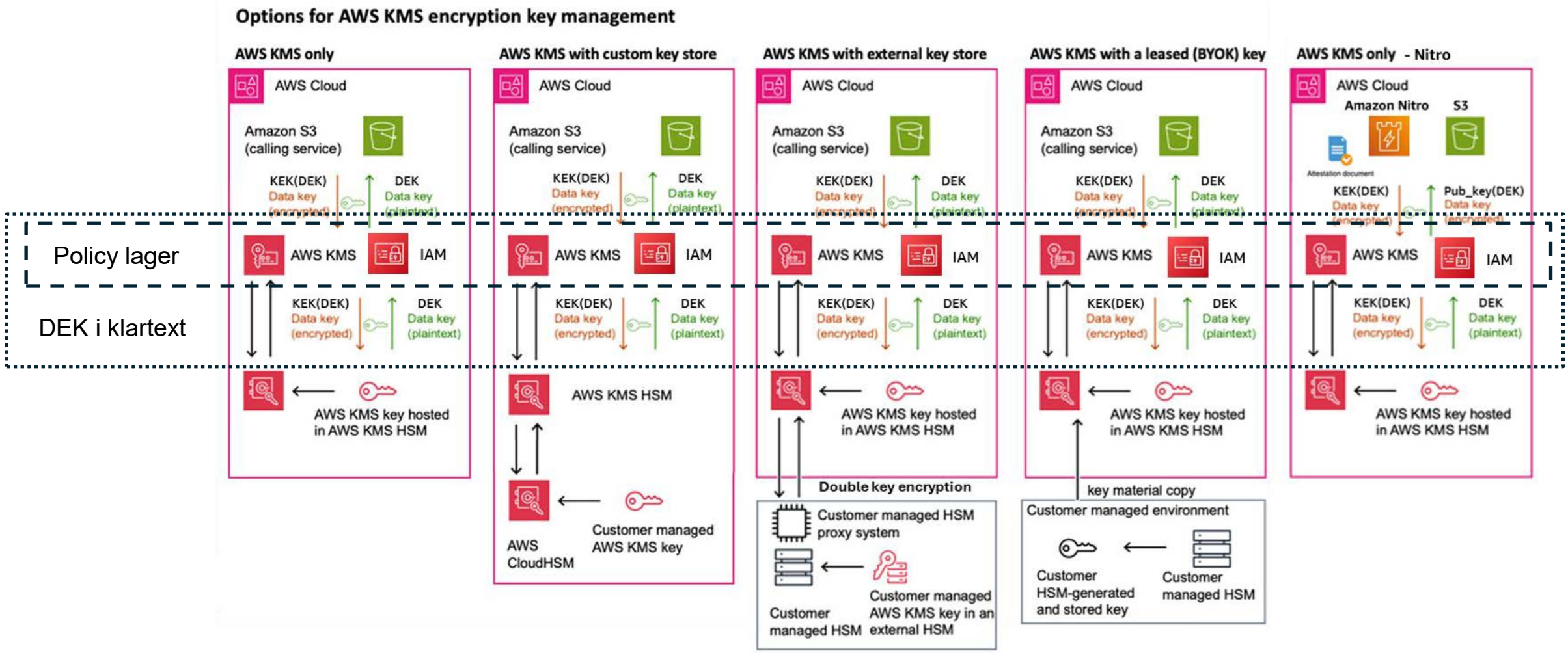
Nyckelhantering via molnens krypto-API:er exponerar datanycklar i klartext.

Datasäkerhet i molnet är inte ett kryptografiskt matematiskt skydd – det styrs helt av leverantörens IAM-kontrollplan.


Options for AWS KMS encryption key management
AWS KMS only
AWS Cloud
Amazon S3
(calling service)
KEK(DEK)
Data key
(encrypted)
DEK
Data key
(plaintext)
AWS KMS
IAM
KEK(DEK)
Data key
(encrypted)
DEK
Data key
(plaintext)
AWS KMS key hosted
in AWS KMS HSM
AWS KMS with custom key store
AWS Cloud
Amazon S3
(calling service)
KEK(DEK)
Data key
(encrypted)
DEK
Data key
(plaintext)
AWS KMS
IAM
KEK(DEK)
Data key
(encrypted)
DEK
Data key
(plaintext)
AWS KMS HSM
Customer managed
AWS KMS key
AWS
CloudHSM
AWS KMS with external key store
AWS Cloud
Amazon S3
(calling service)
KEK(DEK)
Data key
(encrypted)
DEK
Data key
(plaintext)
AWS KMS
IAM
KEK(DEK)
Data key
(encrypted)
DEK
Data key
(plaintext)
AWS KMS key hosted
in AWS KMS HSM
Double key encryption
Customer managed HSM
proxy system
Customer managed
AWS KMS key in an
external HSM
Customer
managed HSM
AWS KMS with a leased (BYOK) key
AWS Cloud
Amazon S3
(calling service)
KEK(DEK)
Data key
(encrypted)
DEK
Data key
(plaintext)
AWS KMS
IAM
KEK(DEK)
Data key
(encrypted)
DEK
Data key
(plaintext)
AWS KMS key hosted
in AWS KMS HSM
key material copy
Customer managed environment
Customer
HSM-generated
and stored key
Customer
managed HSM
AWS KMS only - Nitro
AWS Cloud
Amazon Nitro
S3
Attestation document
KEK(DEK)
Data key
(encrypted)
Pub_key(DEK)
Data key
(encrypted)
AWS KMS
IAM
KEK(DEK)
Data key
(encrypted)
DEK
Data key
(plaintext)
AWS KMS key hosted
in AWS KMS HSM

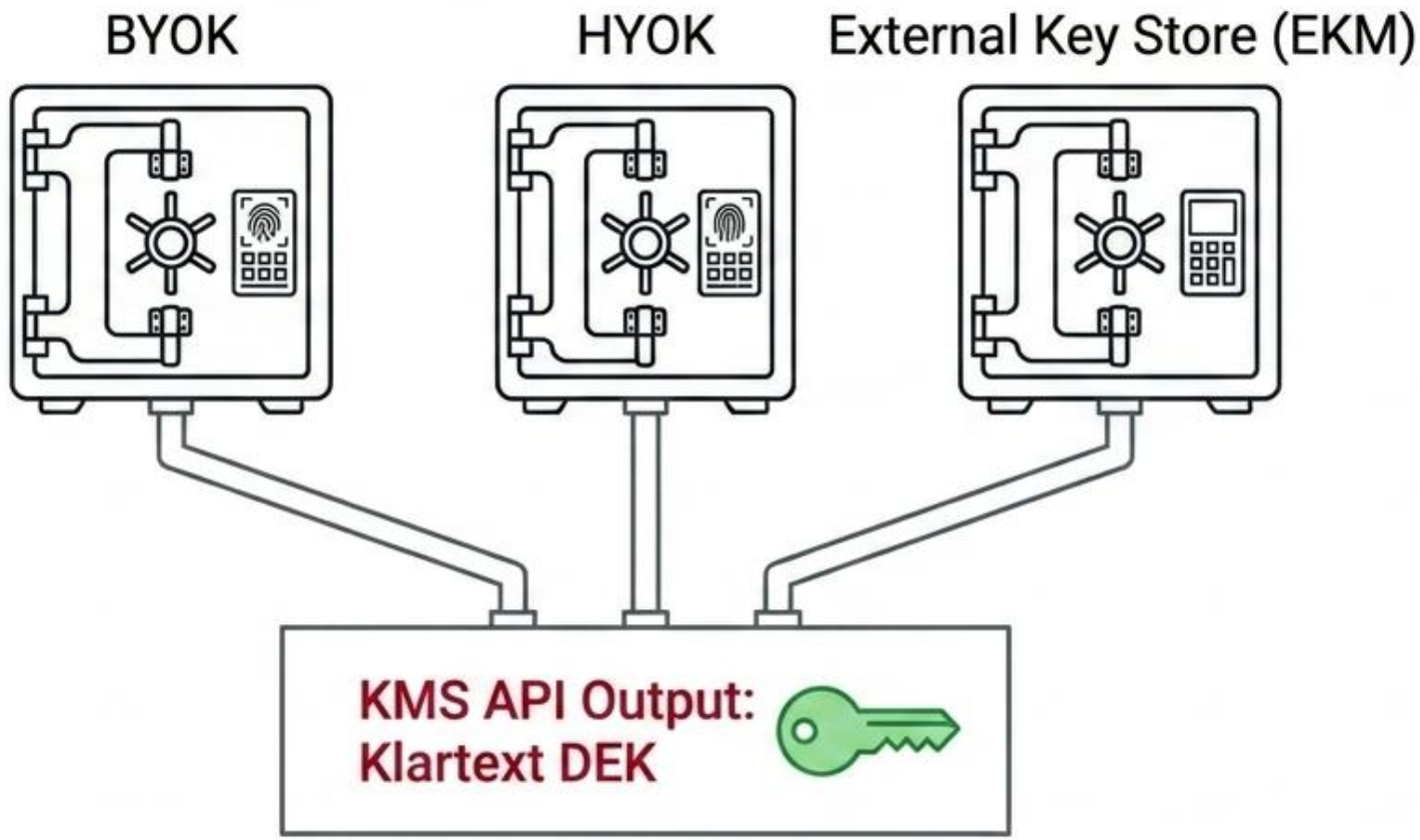

Options for AWS KMS encryption key management
AWS KMS only
AWS KMS with custom key store
AWS KMS with external key store
AWS KMS with a leased (BYOK) key
AWS KMS only - Nitro
AWS Cloud
Amazon S3 (calling service)
KEK(DEK) Data key (encrypted)
DEK Data key (plaintext)
AWS KMS
IAM
AWS KMS key hosted in AWS KMS HSM
AWS KMS HSM
AWS CloudHSM
Customer managed AWS KMS key
Double key encryption
Customer managed HSM proxy system
Customer managed HSM
Customer managed AWS KMS key in an external HSM
key material copy
Customer managed environment
Customer HSM-generated and stored key
Customer managed HSM
Amazon Nitro
S3
Attestation document
Pub_key(DEK) Data key (encrypted)
DEK i klartext

AITYR


Options for AWS KMS encryption key management
AWS KMS only
AWS KMS with custom key store
AWS KMS with external key store
AWS KMS with a leased (BYOK) key
AWS KMS only - Nitro
Policy lager
DEK i klartext
AWS Cloud
Amazon S3 (calling service)
KEK(DEK) Data key (encrypted)
DEK Data key (plaintext)
AWS KMS
IAM
AWS KMS key hosted in AWS KMS HSM
AWS KMS HSM
AWS CloudHSM
Customer managed AWS KMS key
Double key encryption
Customer managed HSM proxy system
Customer managed HSM
Customer managed AWS KMS key in an external HSM
key material copy
Customer managed environment
Customer HSM-generated and stored key
Customer managed HSM
Amazon Nitro
S3
Attestation document
Pub_key(DEK) Data key

AITYR

Illusionen av extern nyckelhantering

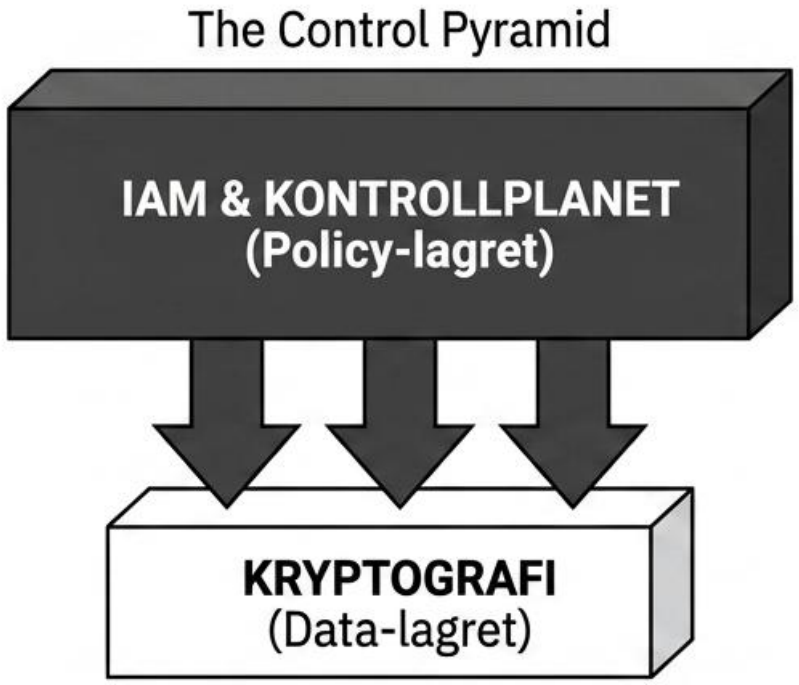


Leverantörer säljer externa krypteringslager som en lösning på suveränitet. Men oavsett vem som äger, roterar eller hanterar KEK-kuvertet, måste DEK-nyckeln packas upp i leverantörens miljö för att tjänsterna ska fungera. Arkitekturen lägger till massiv komplexitet, men noll faktisk datasekretess mot molnleverantören leverantören.

Branschstandard, inte en enskild bugg

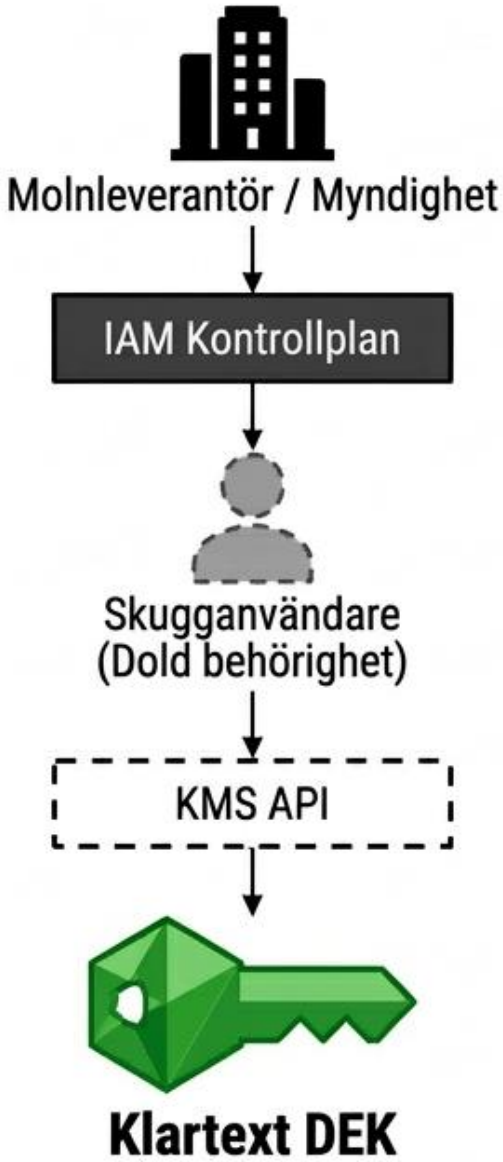
	AWS KMS	Azure Key Vault	Google Cloud KMS
Huvudnyckel (KEK)	HBK / KMS Key	Master Key / KEK	Cloud KMS Key
Datanyckel (DEK)	Customer Data Key	Content Encryption Key (CEK)	Data Encryption Key (DEK)
Dekrypteringsanrop	Decrypt / GenerateDataKey	UnwrapKey	Decrypt
DEK Exponering i API	✓ Returneras i klartext	✓ Returneras i klartext	✓ Returneras i klartext

IAM övertrumfar alltid krypto



Eftersom systemet rent arkitektoniskt kan och måste leverera en klartext-DEK via API:et, handlar molnsäkerhet inte längre om oknäckbar matematik. Säkerheten reduceras till en enda fråga: Vem har IAM-behörighet att anropa API:et? Policy-lagret överstyr alltid krypto-lagret.

Hotet från skugganvändaren



Den som kontrollerar IAM och API-gränssnittet kontrollerar din **data**. Molnleverantören (eller en aktör med laglig rätt att tvinga leverantören) äger kontrollplanet. De har den tekniska förmågan att tilldela dolda IAM-behörigheter till kundens nycklar och begära ut DEK i klartext, helt förbi kundens vetskap.

Den Tredje Nyckeln: Illusionen om Total Datasuveränitet

Många organisationer använder Microsofts "Customer Key" i tron att de har total kontroll över sin kryptering. I verkligheten skyddas datan av tre nycklar, där Microsoft äger den tredje, vilket skapar en juridisk bakdörr till krypterad data under amerikansk jurisdiktion.

Den Tekniska Verkligheten

3 nycklar skyddar din DEP-nyckel

Kundens Rotnycklar
Kunden hanterar två egna rotnycklar.

Microsofts "Availability Key"
Microsoft genererar och äger en obligatorisk tredje tillgänglighetsnyckel.

Automatisk reservlösning i bakgrunden: Nyckeln används av Microsoft för driftstörningar (Exchange) eller katastrofåterställning (SharePoint/OneDrive) utan kundens inblandning.

Olika tekniker för olika tjänster: Exchange använder AES-256 I sitt hemliga lager, medan SharePoint/OneDrive nyttjar en RSA-2048-arkitektur.

Exchange

SharePoint/OneDrive

Juridiska & Strategiska Konsekvenser

Amerikansk lag trumfar lagringsort

Microsofts "Availability Key"

Eftersom Microsoft har den tekniska förmågan att dekryptera datan lyder den under amerikansk jurisdiktion.

Kapacitet innebär exponering

Om en leverantör kan låsa upp din data åt dig, kan de även tvingas göra det av en domstol.

Illusionen om datasuveränitet

Egna krypteringsnycklar (BYOK/HYOK) ger inte fullt skydd så länge den tredje nyckeln existerar.

Sårbarheten i Teams E2EE: Scenariot för ”Osynlig Avlyssning”

Hur avlyssningen genomförs

GKMP
(Key Management Protocol)
Förhandling

Manipulerad nyckelförhandling via GKMP

Microsofts servrar dirigerar nyckelförfrågningar till en dold nod som därmed får korrekta krypteringsnycklar.

Maskering i användargränssnittet

Infrastrukturen döljer den extra noden från deltagarlistan, vilket gör den helt osynlig för legitima mötesdeltagare.

1234-5678-9012-3456-7890

Identiska säkerhetskoder

Eftersom den dolda noden deltar i den officiella förhandlingen genereras en korrekt 20-siffrig säkerhetskod.

Hypotesen förutsätter att P2P dvs 1:1 samtal avvänder GKMP

Varför sårbarheten kvarstår

Avsaknad av “Post-Compromise Security”

Teams använder DTLS-protokollet som inte roterar nycklar automatiskt när en deltagare lämnar mötet.

Den “stulna” nyckelns livslängd

Passiv avlyssning efter anslutning

En nod kan ansluta kort för att hämta nyckeln och sedan avlyssna samtalet passivt utifrån.

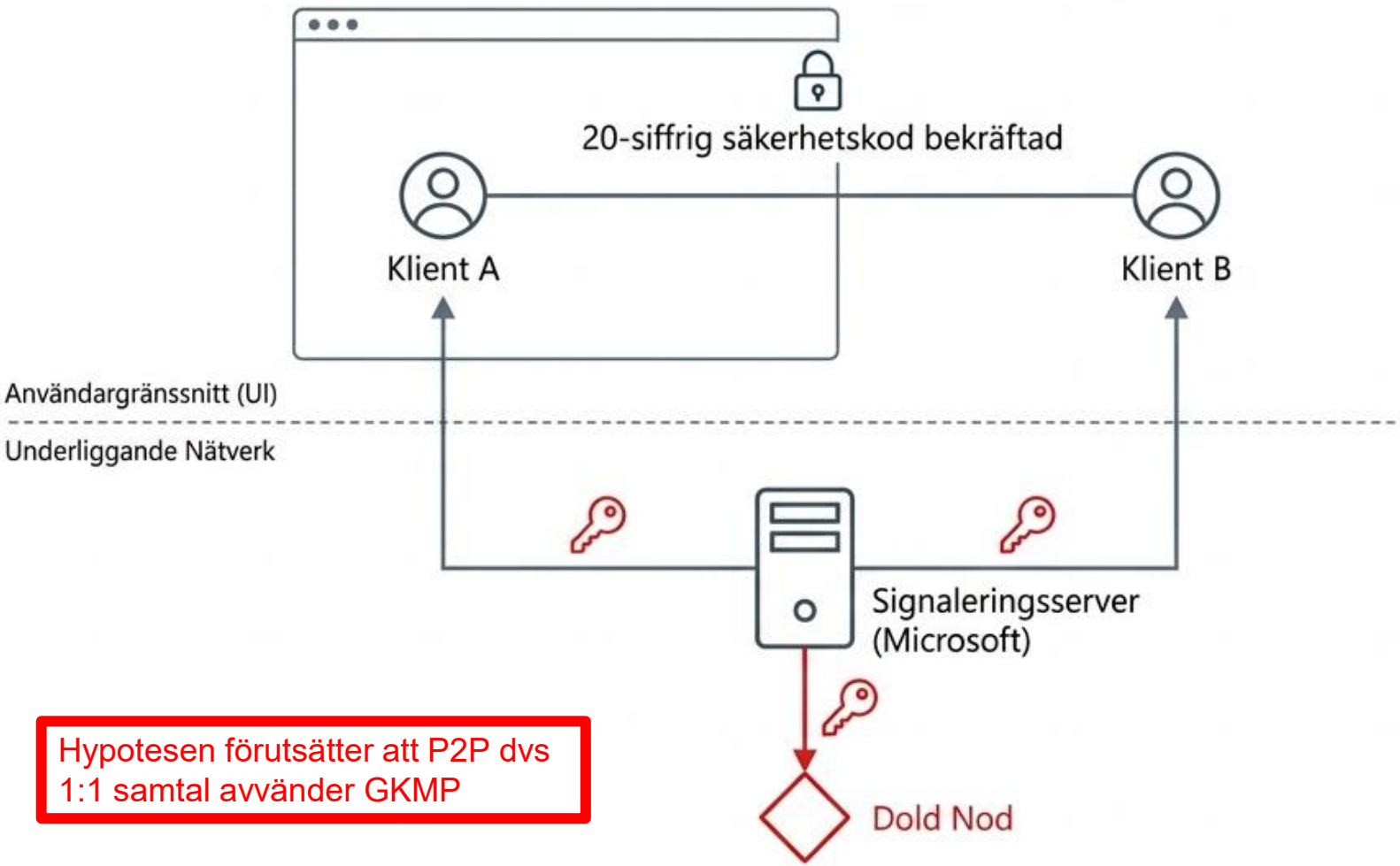
Centraliserad kontroll som riskfaktor

Microsofts kontroll över signaleringen skapar en teknisk bakväg som är sårbar för juridiska påtryckningar.

AITYR

Så injiceras en dold avlyssningsnod via signaleringsservern

Steg 1: Manipulering av GKMP-protokollet och gränssnittets blindfläck



Hypotesen förutsätter att P2P dvs 1:1 samtal avvänder GKMP

Serverns roll: Microsoft äger servrarna som dirigerar signaleringen. Vid påtryckningar kan servern dirigera GKMP-förfrågningar till en extern, fientlig nod.

Nyckelutbytet: Den dolda noden deltar i nyckelförhandlingen. Alla tre parter får samma nyckel, vilket genererar en intakt säkerhetskod hos de legitima deltagarna.

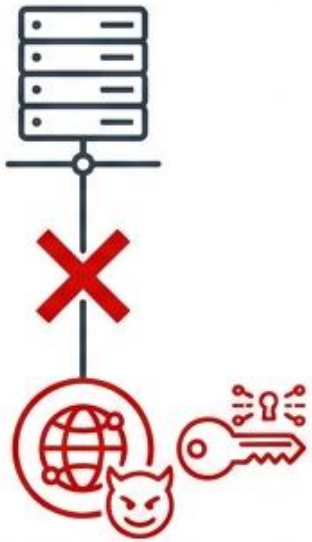
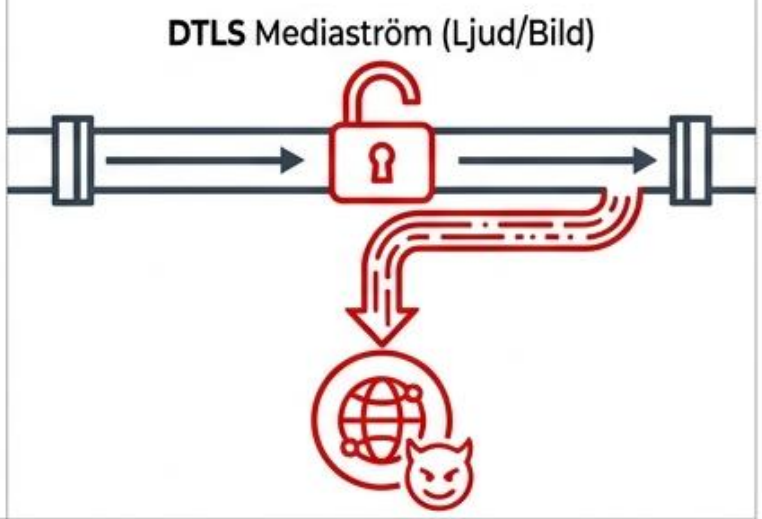
Gränssnittets blindfläck: Signalen för att en deltagare har anslutit filtreras bort på servernivå. Deltagarlistan i gränssnittet uppdateras aldrig.

AITYR

Avsaknaden av Post-Compromise Security i DTLS möjliggör passiv avlyssning

Steg 2: Hur nyckeln överlever trots att noden kopplar ned

Hypotesen förutsätter att P2P dvs 1:1 samtal avvänder GKMP

Sekvens 1: Anslutning	Sekvens 2: Frånkoppling	Sekvens 3: Läckaget
		
Aktiv injektion: Den fientliga noden kopplar upp mot servern och stjäl krypteringsnyckeln via GKMP.	**Dold närvaro:** Nätverkslänken till signaleringsservern bryts avsiktligt. Den aktiva uppkopplingen avslutas för att helt undvika upptäckt.	**Svagheten i DTLS:** Teams roterar inte nycklar när någon lämnar. Hänglåset förblir öppet och noden kan fortsätta dekryptera datan passivt.

Permanent kompromettering: Ett avbrutet nätverksanrop stoppar inte avlyssningen. Eftersom nyckeln förblir statisk roteras den inte. Den dolda aktören kan fortsätta avlyssna ljud och bild under hela samtalets livslängd.

AITYR

Klinisk syntes: Systemets inbyggda sårbarheter mot statliga aktörer

Hypotesen förutsätter att P2P dvs 1:1 samtal avvänder GKMP

Varför Teams E2EE-arkitektur fundamentalt brister i miljöer med extrema säkerhetskrav

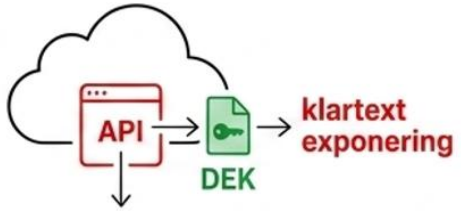
Krav för extrem sekretess	Status i Teams nuvarande E2EE
Infrastrukturoberoende	**Komprometterad.** Microsoft kontrollerar signaleringsservern och kan påtvinga omdirigering (GKMP-manipulation).
Verifikation av noder	**Otillräcklig.** Deltagarlistan i UI kan manipuleras från servernivå utan att den 20-siffriga säkerhetskoden varnar legitima användare.
Framåtriktad sekretess (Post-Compromise Security)	**Saknas.** DTLS roterar inte nycklar. En stulen nyckel ger obegränsad tillgång till mediaströmmen under hela sessionen.

Slutsats: Systemets fundamentala asymmetri

Felet ligger inte i själva krypteringsalgoritmen, utan i förtroendemodellen. Så länge servern kan injicera dolda noder i nyckelutbytet, och protokollet (DTLS) tillåter att dessa nycklar förblir aktiva utan rotation, är systemet designmässigt försvarslöst mot en motståndare som har legal eller teknisk kontroll över infrastrukturen.

Arkitekturens tre obestridliga fakta

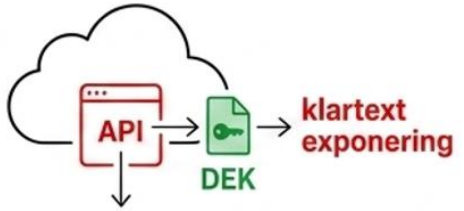
1 **DEK (datanyckeln) hanteras och exponeras i klartext i molnets applikations-API för alla större leverantörer (AWS, Azure, GCP).**



AITYR

Arkitekturens tre obestridliga fakta

1 **DEK (datanyckeln) hanteras och exponeras i klartext i molnets applikations-API för alla större leverantörer (AWS, Azure, GCP).**

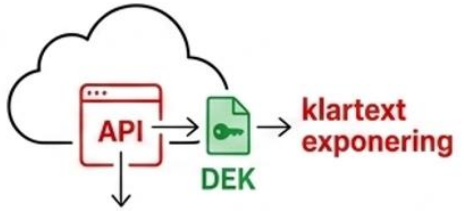


2 **Extra krypteringslager (BYOK/HYOK) skyddar endast KEK, och förhindrar inte klartext-exponeringen av DEK.**

AITYR

Arkitekturens tre obestridliga fakta

1 **DEK (datanyckeln) hanteras och exponeras i klartext i molnets applikations-API för alla större leverantörer (AWS, Azure, GCP).**



2 **Extra krypteringslager (BYOK/HYOK) skyddar endast KEK, och förhindrar inte klartext-exponeringen av DEK.**

3 **I molnet övertrumfar kontrollplanet alltid kryptografin. Den som kontrollerar IAM, kontrollerar i slutändan din data.**

AITYR

Slutsats: Den brustna tillitscirkeln

1

Teknisk suveränitet i ett delat publikt moln existerar inte.

Kryptolagret är underordnat kontrollplanet.

2

Kryptot skyddar mot tredje part, aldrig mot plattformsägaren.

All dataskyddsstrategi i molnet förlitar sig i slutändan på operationell och juridisk tillit till leverantören, inte på kryptografiska garantier.

3

Klartext-exponering är oundviklig.

Oavsett hur väl du skyddar huvudnyckeln (KEK) externt, måste leverantören få tillgång till datanyckeln (DEK) i klartext för att systemet ska fungera.

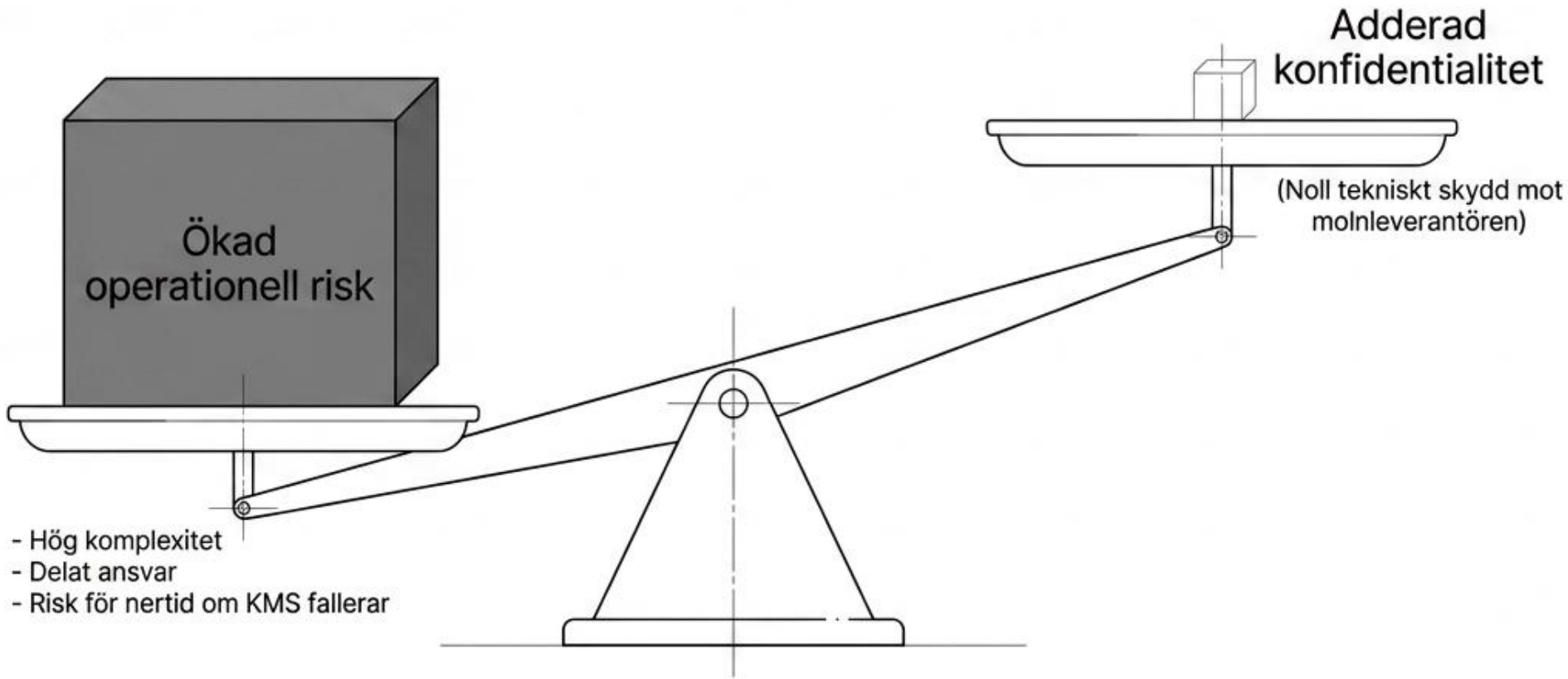
Kan du inte lita på att leverantören kan stå emot främmande lagstiftning, kan datan inte lagras i deras miljö.

NCSC:s varning om komplexitet och tillit

”Du måste förlita dig på säkerheten hos KMS för att lita på molnet. Försök inte undvika att lita på KMS... Att skapa din egen KMS är tekniskt mycket utmanande, och konsekvenserna av ett implementeringsfel kan bli katastrofala.”

AITYR

Den sanna kostnaden för kryptografisk komplexitet



Att implementera komplexa KEK-skydd utan att förstå att DEK fortfarande exponeras är farligt. Vi riskerar vår egen tillgång till data vid felkonfigurationer eller API-avbrott, samtidigt som vi helt misslyckas med att stänga ute leverantören.

AITYR

Marknadsföring
ger inget skydd i molntjänster

AITYR

André Catry
0761-811213
andre@aityr.se

Innovation for a Safer World

AITYR

Stockholm, Sweden

+46 8 414 00 058

info@aityr.ai