THALES

Need for PKI for Data Protection - Addressing Data Breaches & Data Privacy

Ved Prakash
Business Development Leader – Banking & Enterprise
India & SAARC

Ved-v.prakash@thalesgroup.com
+91-9029963079

Discussion Flow :-

1. PKI - Foundation for Digital Trust
2. Top 3 Risk Areas of PKI
3. About Thales – Leadership Journey in PKI Solution & Data Protection
4. Major Problem Areas in Data Protection Today
5. Regulatory & Compliance drivers for PKI Solution & Data level protection
6. Data Breach Protection Strategy
7. Thales Technology Solutions – Use Cases
8. Knowledge Workshop Session – On Request

Disclaimer

- This presentation is for knowledge purposes only. Opinions or points of view expressed in this presentation represent the view of the presenter, and does not necessarily represent the official position or policies of the Thales

Safeguarding Trust – PII Data Privacy & Protection Paramount

- When users share their data with you, they put trust in you and its your responsibility to make sure that you uphold that trust

- PKI is a core component of data confidentiality, information integrity, authentication, and data access control

Top 3 Risks of PKI

Below are Top 3 Risks of PKI the from our Experience

1. Failure to properly protect or store Encryption Keys. Stolen or Irrecoverable encryption keys.
2. Issuing Certificates to an unintended party/multiple parties.
3. Failure to Issue, Renew, or revoke certificates within the environment

Is any of these questions your concern?

- **Where is the Root of Trust for PKI – Is my PKI application really secure? Is it compliant? Can I trust my PKI?**
- **What's your IRM approach? More self inflicted or regulations driven? Where do you think its going?**
  - Are you taking a data centric approach in today's changing threat landscape
- **How many encryption systems do you have in place? How many where there 2 years ago? What's your biggest challenge with them?**
- **Has key, cert and credential management been a growing pain for you?**
- **How are you Securing machine identities of the important internal business application (ex Switch, CRM,) ?**
- **How do you ensure that database admin who has access is not able to see the PII data? – remarks from leading auditors**
- **How are you securing the data in the cloud infrastructure – Office 365, Amazon or Azure with**
- **Have you implemented Centralized Encryption Key Management solution Or Key Management Policy**
  - This helps in complete lifecycle all the encryption keys from creation to distribution, rotation, archival and deletion of keys

About Thales - In India Since 1953, R&D & Regional HQ – Noida

#1 worldwide

Payloads for telecom satellites

Air Traffic Management

Sonars

Security for payment transactions

#2 worldwide

Rail signalling systems

In-flight entertainment

Military tactical radio

#3 worldwide

Avionics

Civil satellites

Surface radars

€21bn+
Revenues (Unaudited 2021)

81,000
Employees

68
Countries

Leadership in Data Security

Thales Cloud Protection & Licensing helps secure more than 80% of the world's payment transactions and most valuable corporate and government information.

We currently protect data for:

- 21 NATO member countries
- 19 of the 20 largest banks in the world
- 3,000 financial institutions worldwide
- 4 out of 5 top energy companies
- 4 out of 5 aerospace companies

Global leader in Data Protection (On premise and cloud) using **Encryption + Key Management Technology**

1 bn €
Self-funded R&D*

* Does not include externally financed R&D

THALES

InOrganic Growth Journey

THALES

Building a future we can all trust

gemalto

security to be free

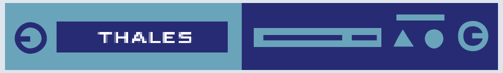
SafeNet

An Unrivalled Data Protection Portfolio for Encrypting Everything

The Market Leading Data Encryption Products

in Support of your Data Security Strategy

SafeNet Luna Network HSM



payShield HSM

SafeNet Cloud HSM On Demand

#1 General Purpose HSMs

#1 Payment HSMs

Thales CipherTrust Data Security Platform

CipherTrust Cloud Key Manager

#1 Data Encryption

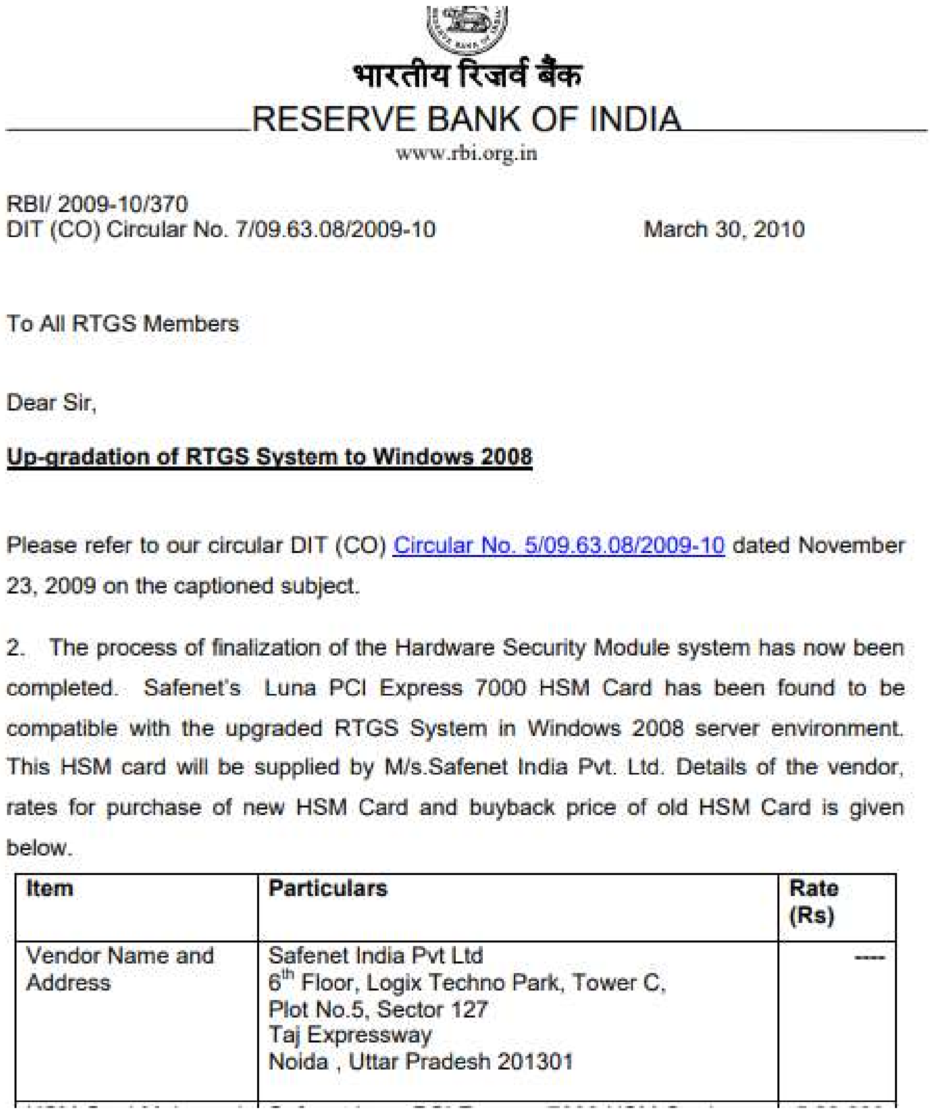
#1 Key Management

SafeNet CN Series High-Speed Network Encryptors

SafeNet CV1000 Virtual Encryptor

#1 Network Encryption

RBI Circular dated 2010…



भारतीय रिजर्व बैंक

RESERVE BANK OF INDIA

www.rbi.org.in

RBI/ 2009-10/370
DIT (CO) Circular No. 7/09.63.08/2009-10 March 30, 2010

To All RTGS Members

Dear Sir,

Up-gradation of RTGS System to Windows 2008

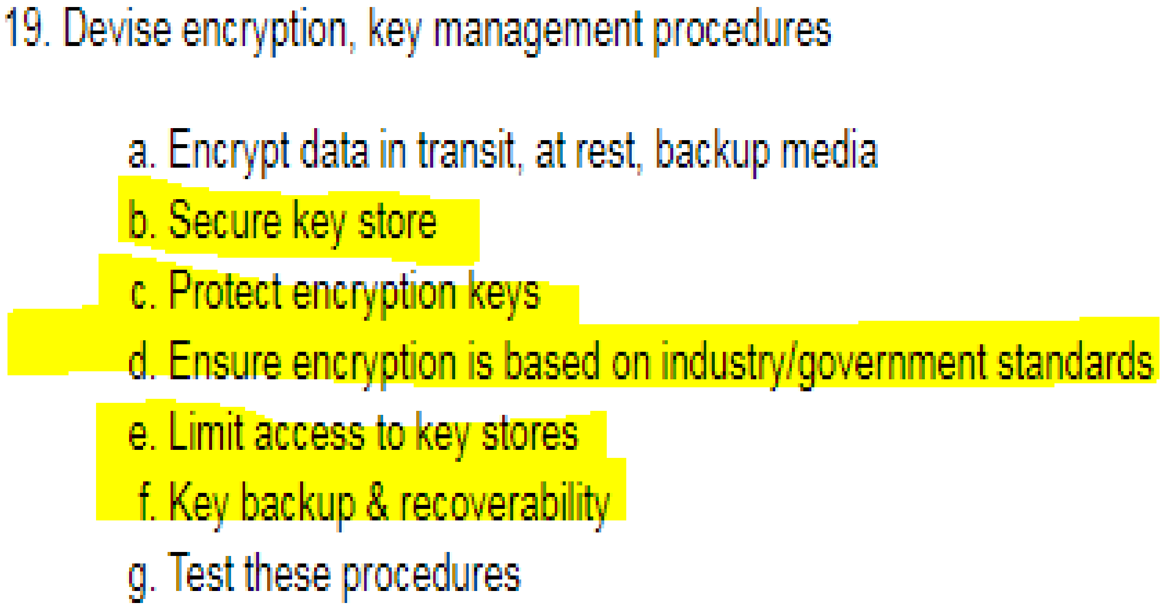
Please refer to our circular DIT (CO) Circular No. 5/09.63.08/2009-10 dated November 23, 2009 on the captioned subject.

2. The process of finalization of the Hardware Security Module system has now been completed. Safenet's Luna PCI Express 7000 HSM Card has been found to be compatible with the upgraded RTGS System in Windows 2008 server environment. This HSM card will be supplied by M/s.Safenet India Pvt. Ltd. Details of the vendor, rates for purchase of new HSM Card and buyback price of old HSM Card is given below.

Item	Particulars	Rate (Rs)
Vendor Name and Address	Safenet India Pvt Ltd 6th Floor, Logix Techno Park, Tower C, Plot No.5, Sector 127 Taj Expressway Noida , Uttar Pradesh 201301	-----

RBI Guideline

- https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=8365&Mode=0



19. Devise encryption, key management procedures

a. Encrypt data in transit, at rest, backup media

b. Secure key store

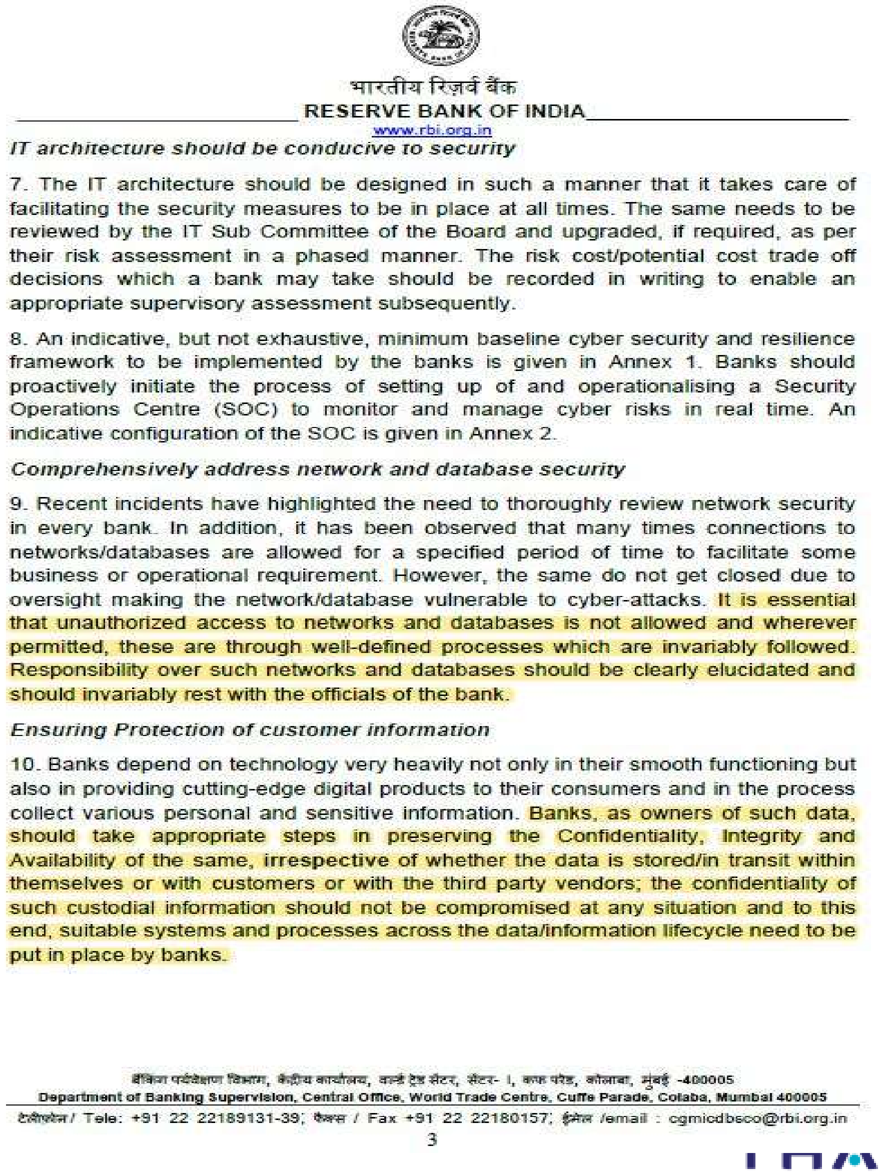
c. Protect encryption keys

d. Ensure encryption is based on industry/government standards

e. Limit access to key stores

f. Key backup & recoverability

g. Test these procedures



भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

www.rbi.org.in

IT architecture should be conducive to security

7. The IT architecture should be designed in such a manner that it takes care of facilitating the security measures to be in place at all times. The same needs to be reviewed by the IT Sub Committee of the Board and upgraded, if required, as per their risk assessment in a phased manner. The risk cost/potential cost trade off decisions which a bank may take should be recorded in writing to enable an appropriate supervisory assessment subsequently.

8. An indicative, but not exhaustive, minimum baseline cyber security and resilience framework to be implemented by the banks is given in Annex 1. Banks should proactively initiate the process of setting up of and operationalising a Security Operations Centre (SOC) to monitor and manage cyber risks in real time. An indicative configuration of the SOC is given in Annex 2.

Comprehensively address network and database security

9. Recent incidents have highlighted the need to thoroughly review network security in every bank. In addition, it has been observed that many times connections to networks/databases are allowed for a specified period of time to facilitate some business or operational requirement. However, the same do not get closed due to oversight making the network/database vulnerable to cyber-attacks. It is essential that unauthorized access to networks and databases is not allowed and wherever permitted, these are through well-defined processes which are invariably followed. Responsibility over such networks and databases should be clearly elucidated and should invariably rest with the officials of the bank.

Ensuring Protection of customer information

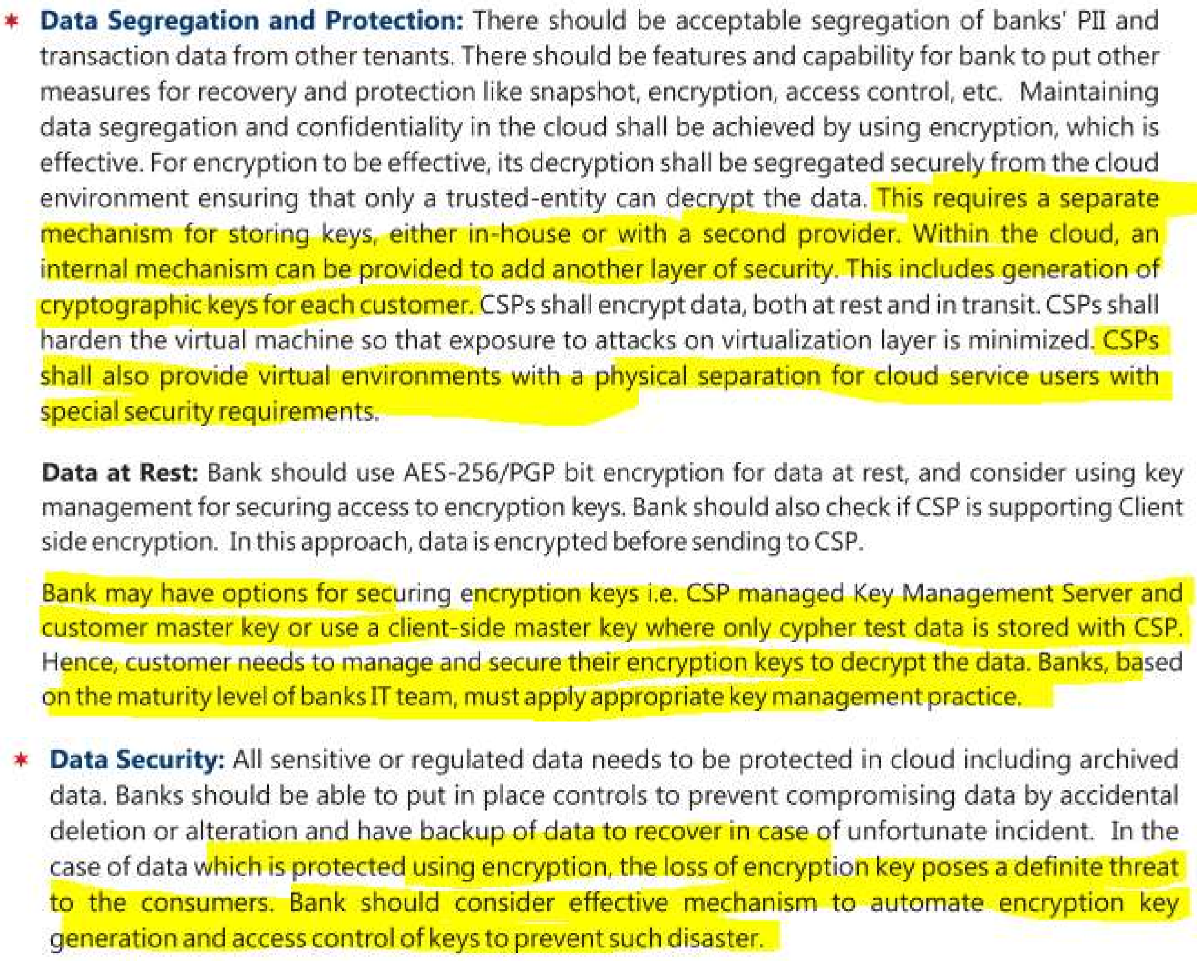
10. Banks depend on technology very heavily not only in their smooth functioning but also in providing cutting-edge digital products to their consumers and in the process collect various personal and sensitive information. Banks, as owners of such data, should take appropriate steps in preserving the Confidentiality, Integrity and Availability of the same, irrespective of whether the data is stored/in transit within themselves or with customers or with the third party vendors; the confidentiality of such custodial information should not be compromised at any situation and to this end, suitable systems and processes across the data/information lifecycle need to be put in place by banks.

बैंकिंग पर्यवेक्षण विभाग, केंद्रीय कार्यालय, वर्ल्ड ट्रेड सेंटर, सेंटर- I, कफ परेड, कोलाबा, मुंबई -400005
Department of Banking Supervision, Central Office, World Trade Centre, Cuffe Parade, Colaba, Mumbai 400005
टेलीफोन / Tele: +91 22 22189131-39; फैक्स / Fax +91 22 22180157; ईमेल /email : cgmicdbsco@rbi.org.in

3

IDRBT Guidelines

https://www.idrbt.ac.in/assets/publications/Best%20Practices/FAQ_Cloud.pdf

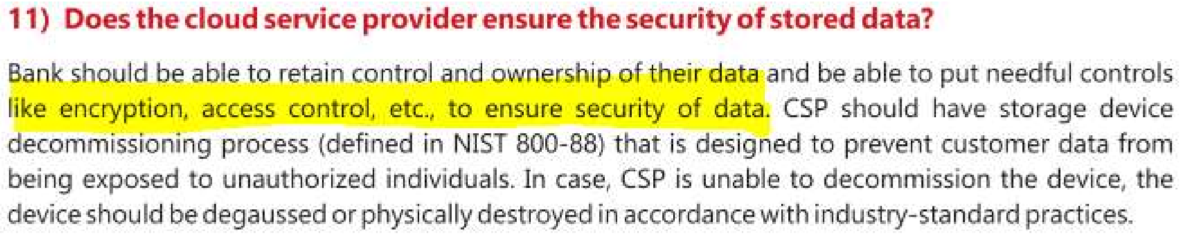


- **Data Segregation and Protection:** There should be acceptable segregation of banks' PII and transaction data from other tenants. There should be features and capability for bank to put other measures for recovery and protection like snapshot, encryption, access control, etc. Maintaining data segregation and confidentiality in the cloud shall be achieved by using encryption, which is effective. For encryption to be effective, its decryption shall be segregated securely from the cloud environment ensuring that only a trusted-entity can decrypt the data. This requires a separate mechanism for storing keys, either in-house or with a second provider. Within the cloud, an internal mechanism can be provided to add another layer of security. This includes generation of cryptographic keys for each customer. CSPs shall encrypt data, both at rest and in transit. CSPs shall harden the virtual machine so that exposure to attacks on virtualization layer is minimized. CSPs shall also provide virtual environments with a physical separation for cloud service users with special security requirements.

Data at Rest: Bank should use AES-256/PGP bit encryption for data at rest, and consider using key management for securing access to encryption keys. Bank should also check if CSP is supporting Client side encryption. In this approach, data is encrypted before sending to CSP.

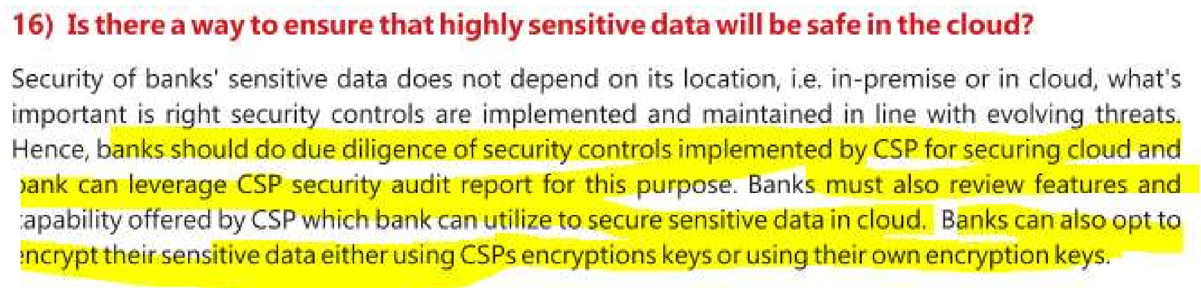
Bank may have options for securing encryption keys i.e. CSP managed Key Management Server and customer master key or use a client-side master key where only cypher test data is stored with CSP. Hence, customer needs to manage and secure their encryption keys to decrypt the data. Banks, based on the maturity level of banks IT team, must apply appropriate key management practice.

- **Data Security:** All sensitive or regulated data needs to be protected in cloud including archived data. Banks should be able to put in place controls to prevent compromising data by accidental deletion or alteration and have backup of data to recover in case of unfortunate incident. In the case of data which is protected using encryption, the loss of encryption key poses a definite threat to the consumers. Bank should consider effective mechanism to automate encryption key generation and access control of keys to prevent such disaster.



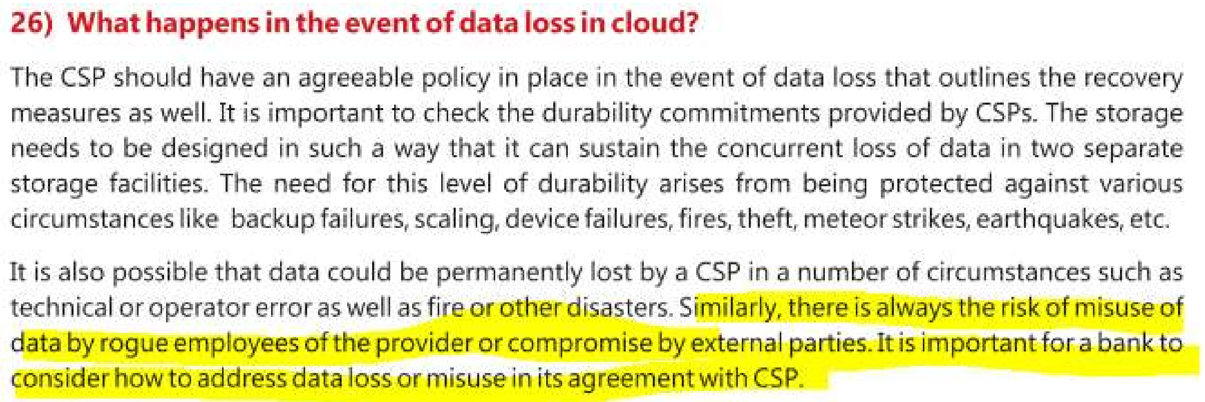
11) Does the cloud service provider ensure the security of stored data?

Bank should be able to retain control and ownership of their data and be able to put needful controls like encryption, access control, etc., to ensure security of data. CSP should have storage device decommissioning process (defined in NIST 800-88) that is designed to prevent customer data from being exposed to unauthorized individuals. In case, CSP is unable to decommission the device, the device should be degaussed or physically destroyed in accordance with industry-standard practices.



16) Is there a way to ensure that highly sensitive data will be safe in the cloud?

Security of banks' sensitive data does not depend on its location, i.e. in-premise or in cloud, what's important is right security controls are implemented and maintained in line with evolving threats. Hence, banks should do due diligence of security controls implemented by CSP for securing cloud and bank can leverage CSP security audit report for this purpose. Banks must also review features and capability offered by CSP which bank can utilize to secure sensitive data in cloud. Banks can also opt to encrypt their sensitive data either using CSPs encryptions keys or using their own encryption keys.

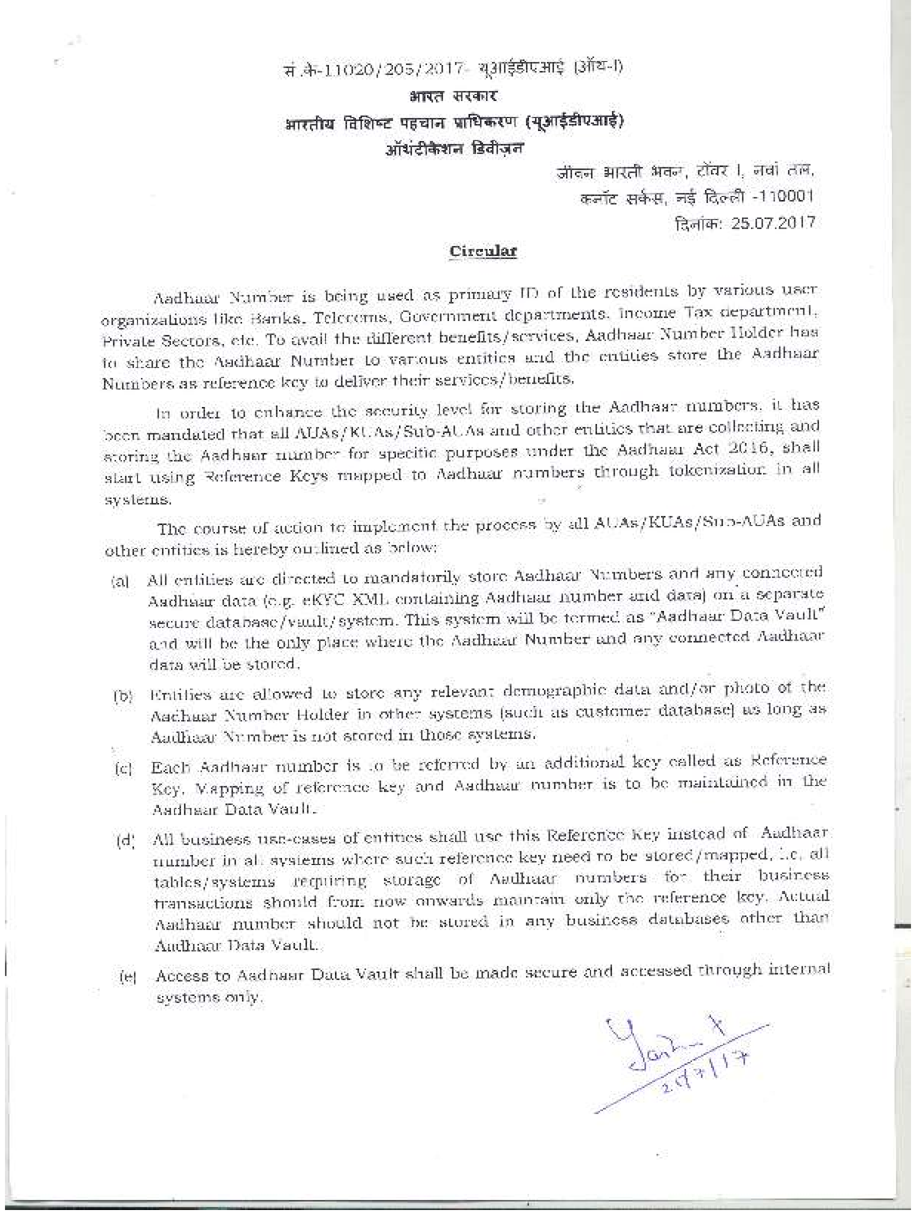


26) What happens in the event of data loss in cloud?

The CSP should have an agreeable policy in place in the event of data loss that outlines the recovery measures as well. It is important to check the durability commitments provided by CSPs. The storage needs to be designed in such a way that it can sustain the concurrent loss of data in two separate storage facilities. The need for this level of durability arises from being protected against various circumstances like backup failures, scaling, device failures, fires, theft, meteor strikes, earthquakes, etc.

It is also possible that data could be permanently lost by a CSP in a number of circumstances such as technical or operator error as well as fire or other disasters. Similarly, there is always the risk of misuse of data by rogue employees of the provider or compromise by external parties. It is important for a bank to consider how to address data loss or misuse in its agreement with CSP.

UIDAI Circular



सं.के-11020/205/2017- यूआईडीएआई (ऑथ-I)

भारत सरकार

भारतीय विशिष्ट पहचान प्राधिकरण (यूआईडीएआई)

ऑथेंटीकेशन डिवीज़न

जीवन भारती भवन, टॉवर I, नवां तल,
कनॉट सर्कस, नई दिल्ली -110001
दिनांक: 25.07.2017

Circular

Aadhaar Number is being used as primary ID of the residents by various user organizations like Banks, Telecoms, Government departments, Income Tax department, Private Sectors, etc. To avail the different benefits/services, Aadhaar Number Holder has to share the Aadhaar Number to various entities and the entities store the Aadhaar Numbers as reference key to deliver their services/benefits.

In order to enhance the security level for storing the Aadhaar numbers, it has been mandated that all AUAs/KUAs/Sub-AUAs and other entities that are collecting and storing the Aadhaar number for specific purposes under the Aadhaar Act 2016, shall start using Reference Keys mapped to Aadhaar numbers through tokenization in all systems.

The course of action to implement the process by all AUAs/KUAs/Sub-AUAs and other entities is hereby outlined as below:

(a) All entities are directed to mandatorily store Aadhaar Numbers and any connected Aadhaar data (e.g. eKYC XML containing Aadhaar number and data) on a separate secure database/vault/system. This system will be termed as "Aadhaar Data Vault" and will be the only place where the Aadhaar Number and any connected Aadhaar data will be stored.

(b) Entities are allowed to store any relevant demographic data and/or photo of the Aadhaar Number Holder in other systems (such as customer database) as long as Aadhaar Number is not stored in those systems.

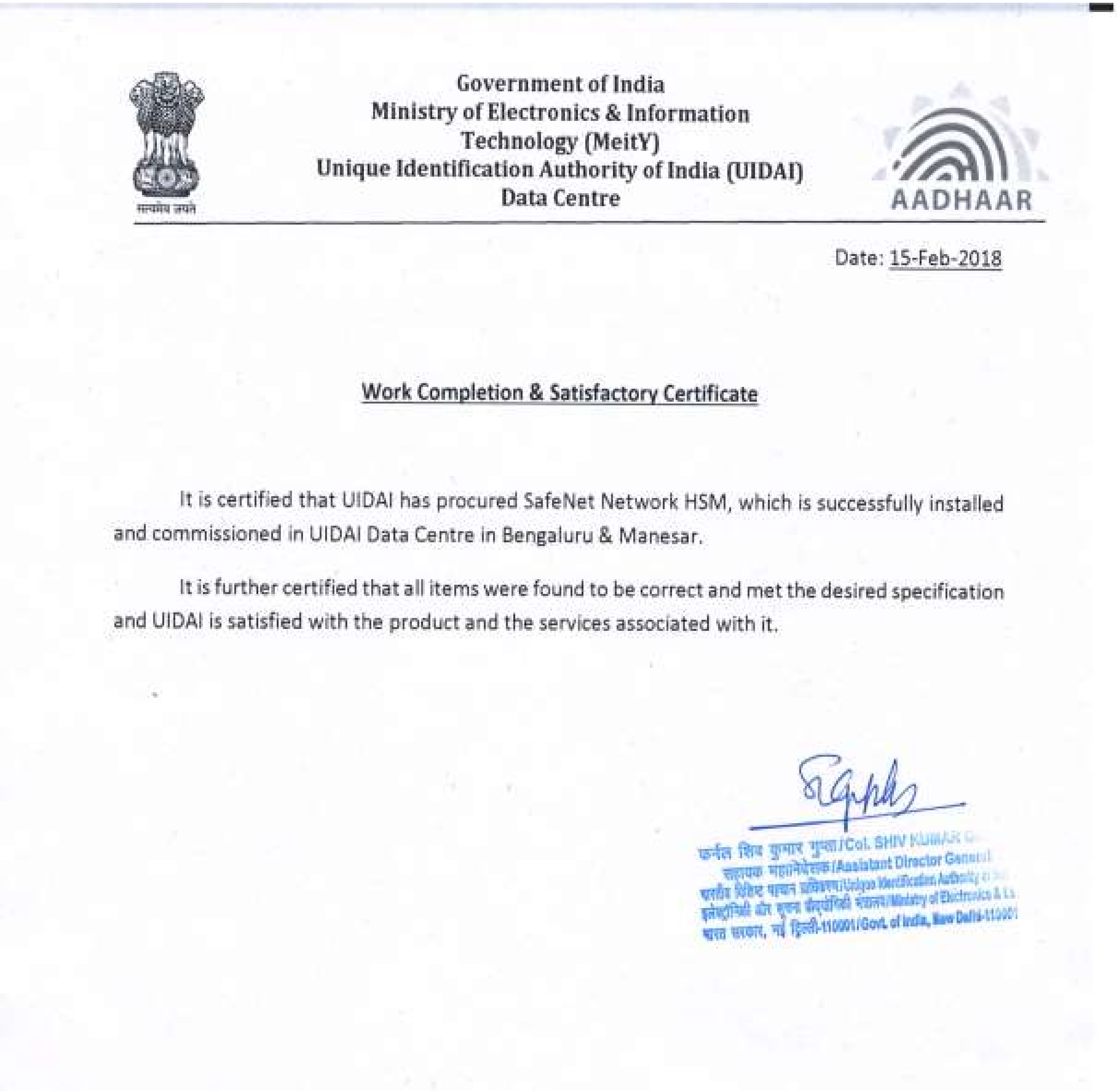
(c) Each Aadhaar number is to be referred by an additional key called as Reference Key. Mapping of reference key and Aadhaar number is to be maintained in the Aadhaar Data Vault.

(d) All business use-cases of entities shall use this Reference Key instead of Aadhaar number in all systems where such reference key need to be stored/mapped, i.e. all tables/systems requiring storage of Aadhaar numbers for their business transactions should from now onwards maintain only the reference key. Actual Aadhaar number should not be stored in any business databases other than Aadhaar Data Vault.

(e) Access to Aadhaar Data Vault shall be made secure and accessed through internal systems only.

24/7/17

UIDAI Satisfactory Letter



सत्यमेव जयते

Government of India
Ministry of Electronics & Information
Technology (MeitY)
Unique Identification Authority of India (UIDAI)
Data Centre

AADHAAR

Date: 15-Feb-2018

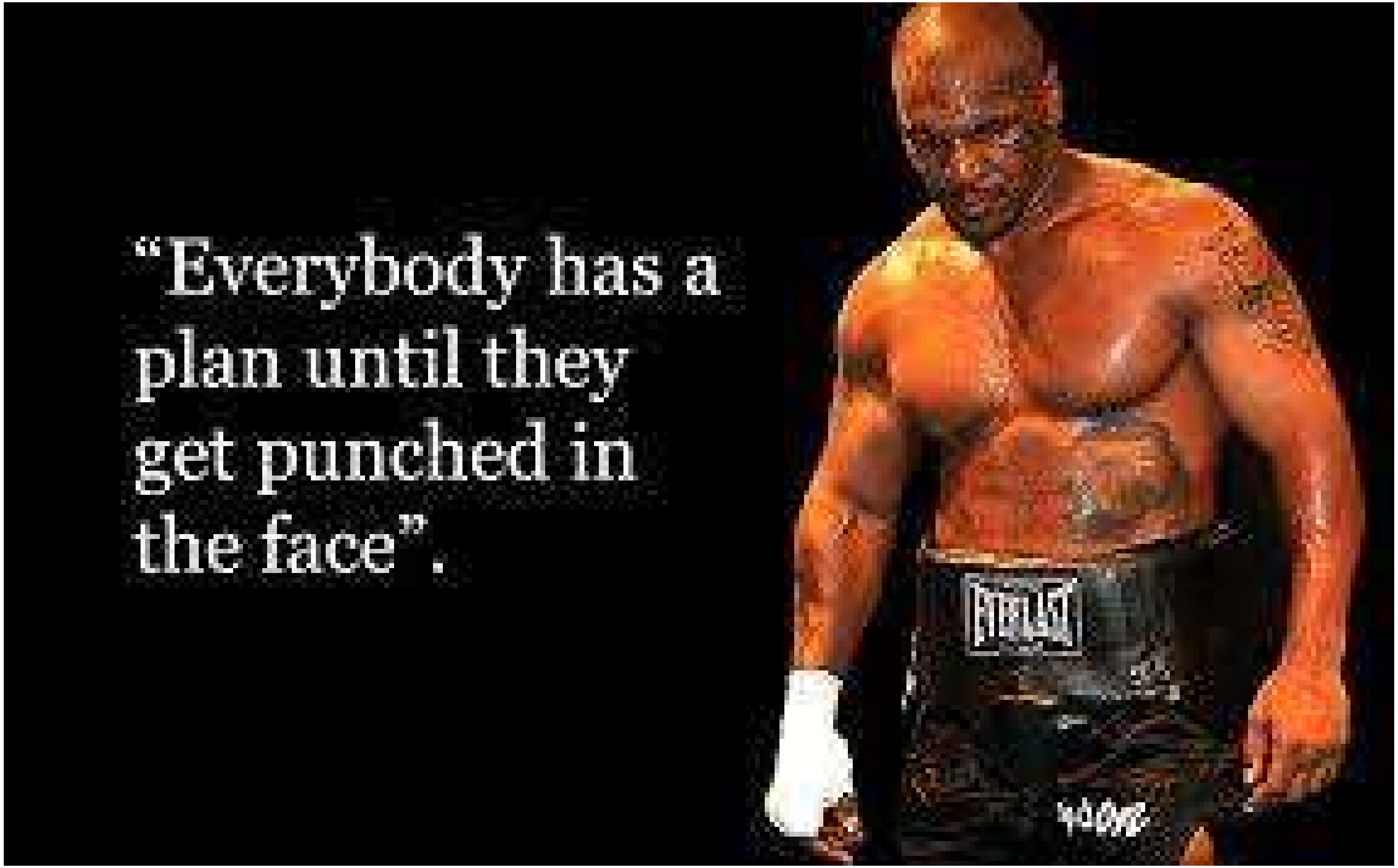
Work Completion & Satisfactory Certificate

It is certified that UIDAI has procured SafeNet Network HSM, which is successfully installed and commissioned in UIDAI Data Centre in Bengaluru & Manesar.

It is further certified that all items were found to be correct and met the desired specification and UIDAI is satisfied with the product and the services associated with it.

कर्नल शिव कुमार गुप्ता/Col. SHIV KUMAR G
सहायक महानिदेशक/Assistant Director General
भारतीय विशिष्ट पहचान प्राधिकरण/Unique Identification Authority of
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय/Ministry of Electronics & I
भारत सरकार, नई दिल्ली-110001/Govt. of India, New Delhi-110001

Are you Ready for the Punch?



Major Punch Areas in Data Protection are:

1) **Data Breaches**
   a) Ransomware Attacks - Rising
   b) Insider Threat (Privilege user misuse/ Prevent DBAs, System Admins, Root users from accessing data (PII)
2) **Meeting Compliance/Regulatory requirements on Data Protection**
   a) RBI/UIDAI/IRDA/UIDAI/PCI/GDPR/SEBI/Meity on Cybersecurity Framework/Upcoming Data Privacy Bill
3) **Customer Data Privacy**
   a) Separation of Duty
   b) Prove & Attest to Data ownership
   c) Access Controls
4) **Lack of Data Visibility** - What Data to secure & where all PII data is residing?

Problem Areas Contd:-

5. **Data Sovereignty for Journey in Cloud** – Rulings like Cloud Act enacted in 2018 allows Federal Agencies to compel US based technology companies via warrants or subpoena to provide requested data stored on servers regardless of whether the data is stored in the US or on the foreign soil

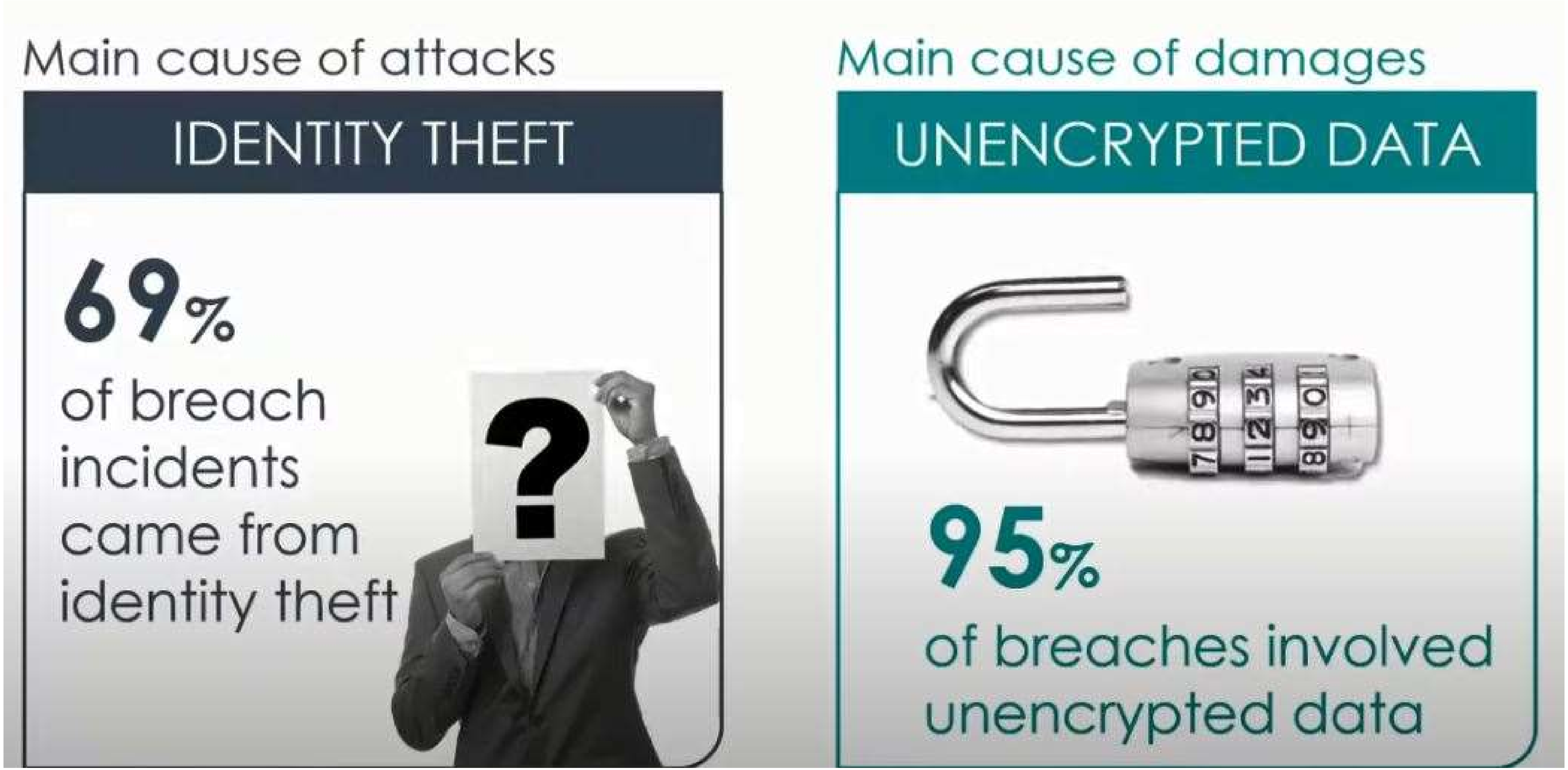
6. **Problem of Data Silos** – Heterogeneous Encryption Environments (Native encryption processes)

Data Breach Targets

The different types of data include the following:

- **Personally Identifiable Information:** includes data such as Aadhar numbers, PAN no, contact information, birth dates, education and other personal information.
- **Financial Information:** includes charge card numbers and expiry dates, bank accounts, investment details and similar data.
- **Health Information:** includes details on health conditions, prescription drugs, treatments and medical records.
- **Intellectual Property:** includes product drawings and manuals, specifications, scientific formulas, marketing texts and symbols, proprietary software and other material that the business has developed.
- **Competition Information:** includes data on competitors, market studies, pricing information and business plans.
- **Legal Information:** includes documentation on court cases the company may be pursuing, legal opinions on business practices, merger and acquisition details and regulatory rulings.
- **IT Security Data:** includes lists of user names and passwords, encryption keys, security strategies and network structure.

The main causes of Data Breaches



Main cause of attacks

IDENTITY THEFT

69%

of breach incidents came from identity theft

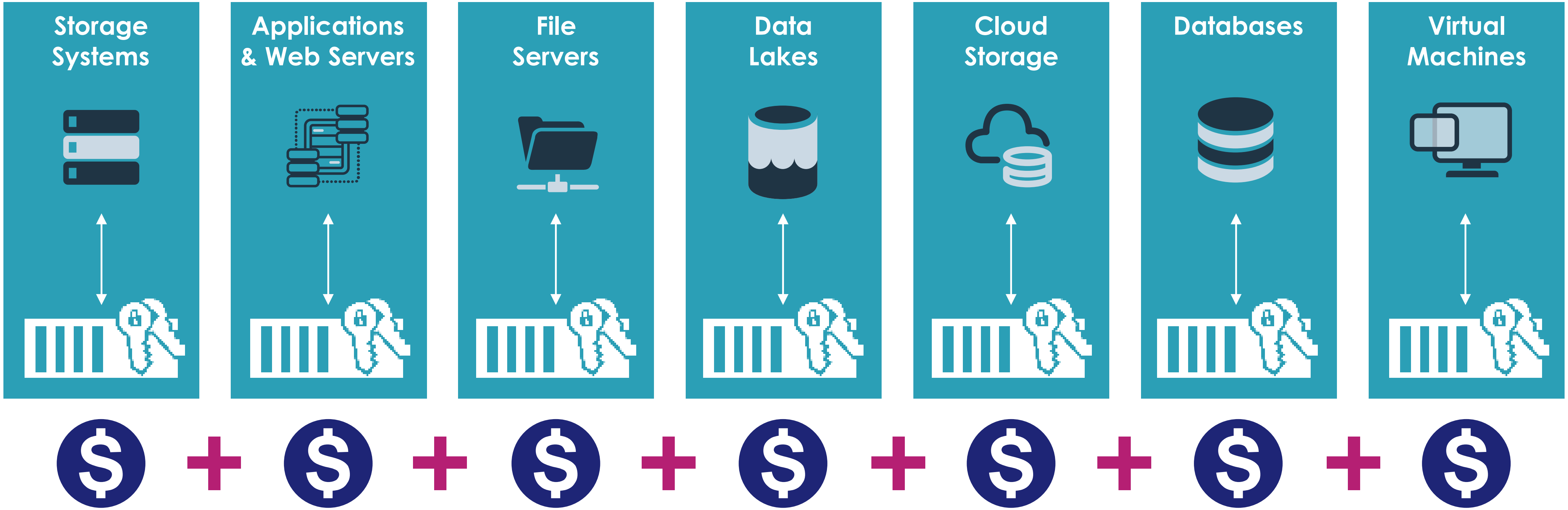
Main cause of damages

UNENCRYPTED DATA

95%

of breaches involved unencrypted data

The Business Problem: Too Many Silos



Storage Systems

Applications & Web Servers

File Servers

Data Lakes

Cloud Storage

Databases

Virtual Machines

Costly & Complex Administration • No Repeatable Process • Audit Challenges
Inconsistent Security Policy Enforcement • Inhibited Data & Business Workflow
•
Fragmented Approach = Higher Risk

The more **data** you possess…

- Who controls the keys?
- Where are the keys located?
- Are the keys trusted?
- Will they pass an audit?
- Do they work with my 3rd party applications?

The more **Encryption Keys** you have to store and manage

Why Centralized Key Management System ?

BROAD RANGE OF ENCRYPTION TOOLS

MILLIONS OF KEYS TO PROTECT, CONTROL, BACKUP AND STORE SECURELY

EASIER TO STEAL KEYS THAN BREAK A CRYPTO ALGORITHM

Best Practices for Cryptographic Key Lifecycle Management

Key Generation

Make sure the key strength matches the sensitivity of the data. The greater the key length, stronger the encryption

Key Access

Ensure the same person creating and managing the key has no access to the protected data

Key Storage

Use FIPS 140-2 compliant appliances for key storage

Key Rotation

Periodically rotate encryption keys and document key lifecycle

Backup & Recovery

Given the magnitude of sensitivity, all keys must be backed up on a periodic basis.

Shared Responsibility Model Illustrates Data Security Roles

🟦 Customer Responsibility

🟪 Provider Responsibility

You're responsible for data security. What do you do?

Infrastructure as a Service (IaaS)	Platform as a Service (PaaS)	Software as a Service (SaaS)
🟦 Data	🟦 Data	🟦 Data
🟦 Application	🟦 Application	🟪 Application
🟦 Runtime	🟪 Runtime	🟪 Runtime
🟦 Middleware	🟪 Middleware	🟪 Middleware
🟦 O/S	🟪 O/S	🟪 O/S
🟪 Virtualization	🟪 Virtualization	🟪 Virtualization
🟪 Servers	🟪 Servers	🟪 Servers
🟪 Storage	🟪 Storage	🟪 Storage
🟪 Networking	🟪 Networking	🟪 Networking
Ex: Virtual machines, EC2 instances	Ex: Storages(S3, Azure blob storage, RDS DBs, Data lake platforms)	Office 365, sales force

Challenge #1: On Cloud - The presumption of losing control

CIO/CTO/CISO/IT.

- ❑ How do I maintain security controls on my cloud infra?
- ❑ What Control am I going to be left with post this migration ?
- ❑ How do I manage my PII Data Risks ?
- ❑ How do I manage my Audits ?
- ❑ How do I meet Compliance Regulations ?

<u>Control the keys & encrypt the data</u>

- *What* keys are created
- *Where* the keys are stored
- *Who* can access the keys
- *When* the keys are revoked

<u>Decoupling of the encryption keys from data sets</u>

✓ Encryption Keys should always be segregated and separately managed from Application Owners in a certified Key management Solution (FIPs 140-2)

Top Cloud Security Risk Areas

Encryption Key Visibility

Data Loss

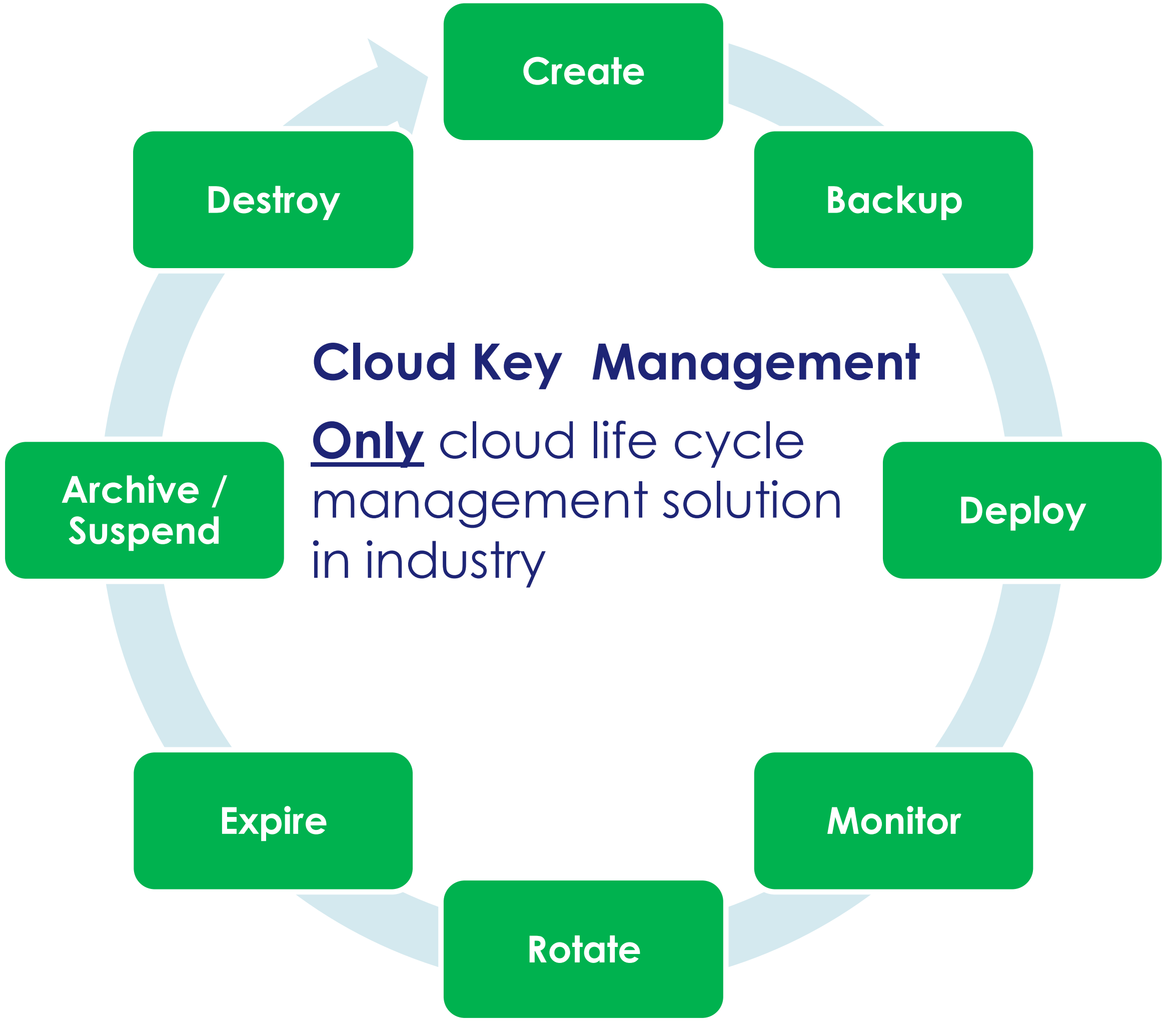
Vendor Lock

Attaining Compliance

Key Lifecycle Mgmt

Cloud Key Lifecycle Management Comparison

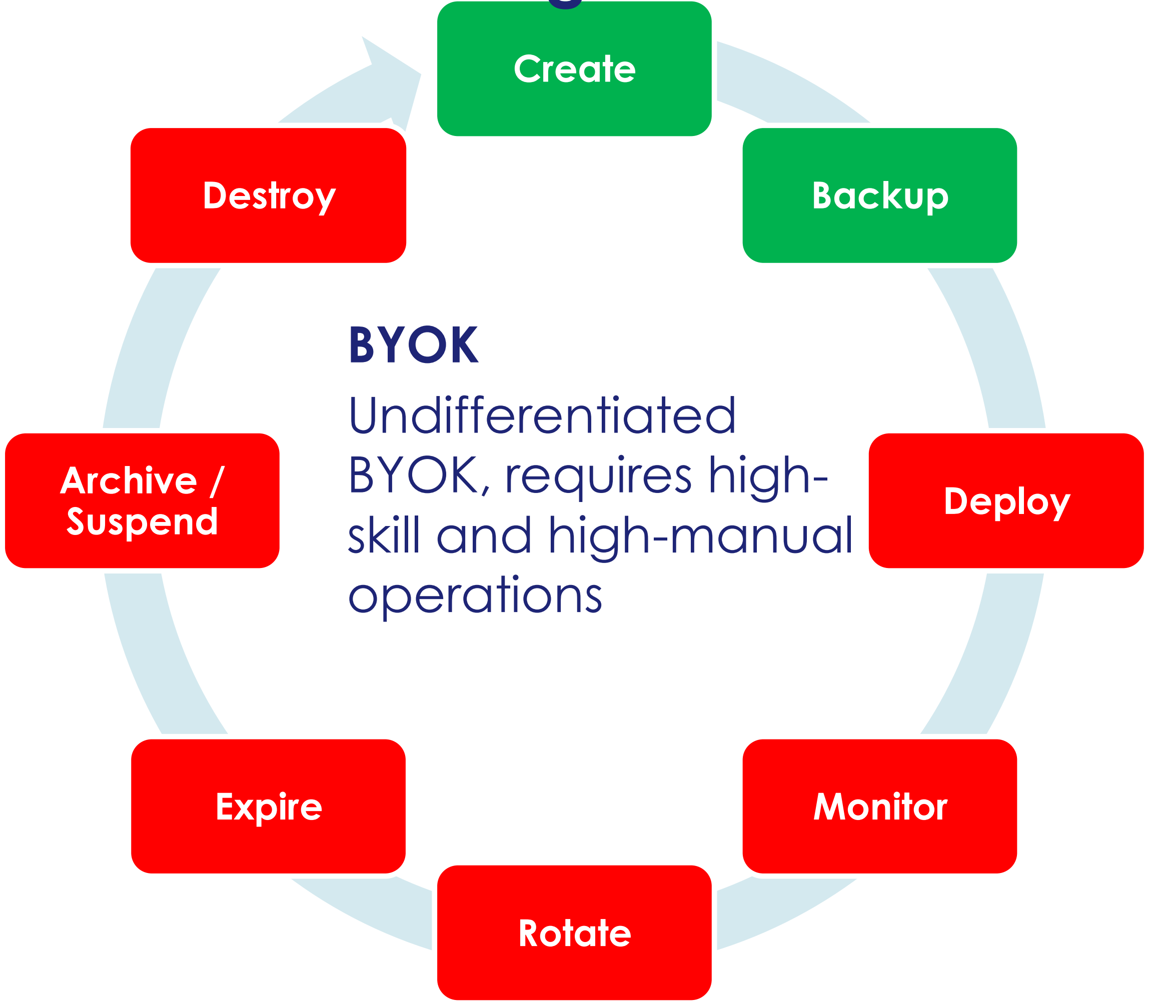
Automated Key Life Cycle Management



Cloud Key Management

Only cloud life cycle management solution in industry

Admin in the Middle Lifecycle Management



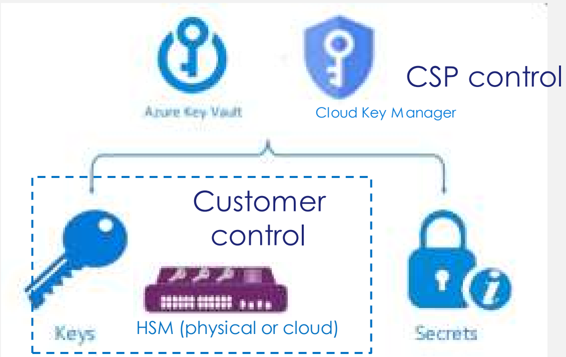
BYOK

Undifferentiated BYOK, requires high-skill and high-manual operations

BYOE & BYOK is way forward to protect your workload in cloud

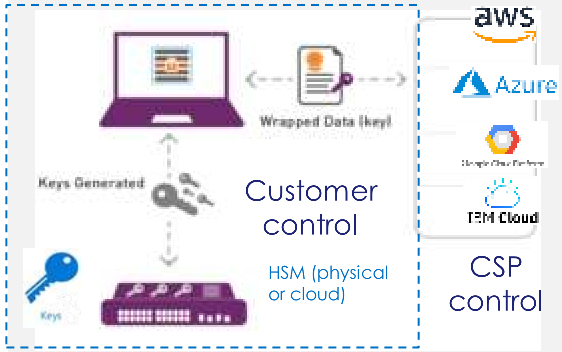
Cloud native encryption

- CSP responsible for both encryption and cryptographic key management
- Can encrypt everything
- No segregation of duty, No protection against **APT / Rogue sys admin / Subpoena**



Bring your own key (BYOK)

- Customers bring their own key and share it with CSP
- Can protect at disk-level and individual file / container
- Manual operation vs **automated operation** with **key life cycle management**



Bring your own encryption (BYOE)

- Customers own and manage their own keys and encrypt workload before uploading to cloud
- Retain full control of cryptographic keys
- Applicable to multiple clouds

Works with all leadig CSP

- Applicable to Office 365
- BYOK for SAAS & PASS
  - (Recently Implemented at Leading Banks in India)
- BYOE for IAAS
  - (Implementation in Progress at Leading Bank In India)

Summary - Key Outcome Areas:-

1. **Customers using native CSP Key Vault would need to enable customer key control functionality using BYOK service & Thales Key Management Solution**
   1. **BYOK – Empower Customer to control own keys**
   2. **Address Data Privacy measures & Compliance (Audit & IT security)**
   - ✓ **Decouple keys from data** - Encryption Keys should always be segregated and separately managed from Application Owners in a certified external Key management Solution (FIPs 140-2 Level)
   - ✓ Example Applications – Office 365, Video eKYC, XpressConnect,, Sprinklr, Wibimo, Signzy, Moneyfront, IECO, Moengage
2. **On Premise/Hybrid Environment – Data at rest encryption : System level control** User/groups for System/ LDAP/AD/Hadoop/Containers
   1. Includes Privileged/Root Users for APT/Malware protection
3. **Centralized Key Management System (Fips 140-2 Level 3)**

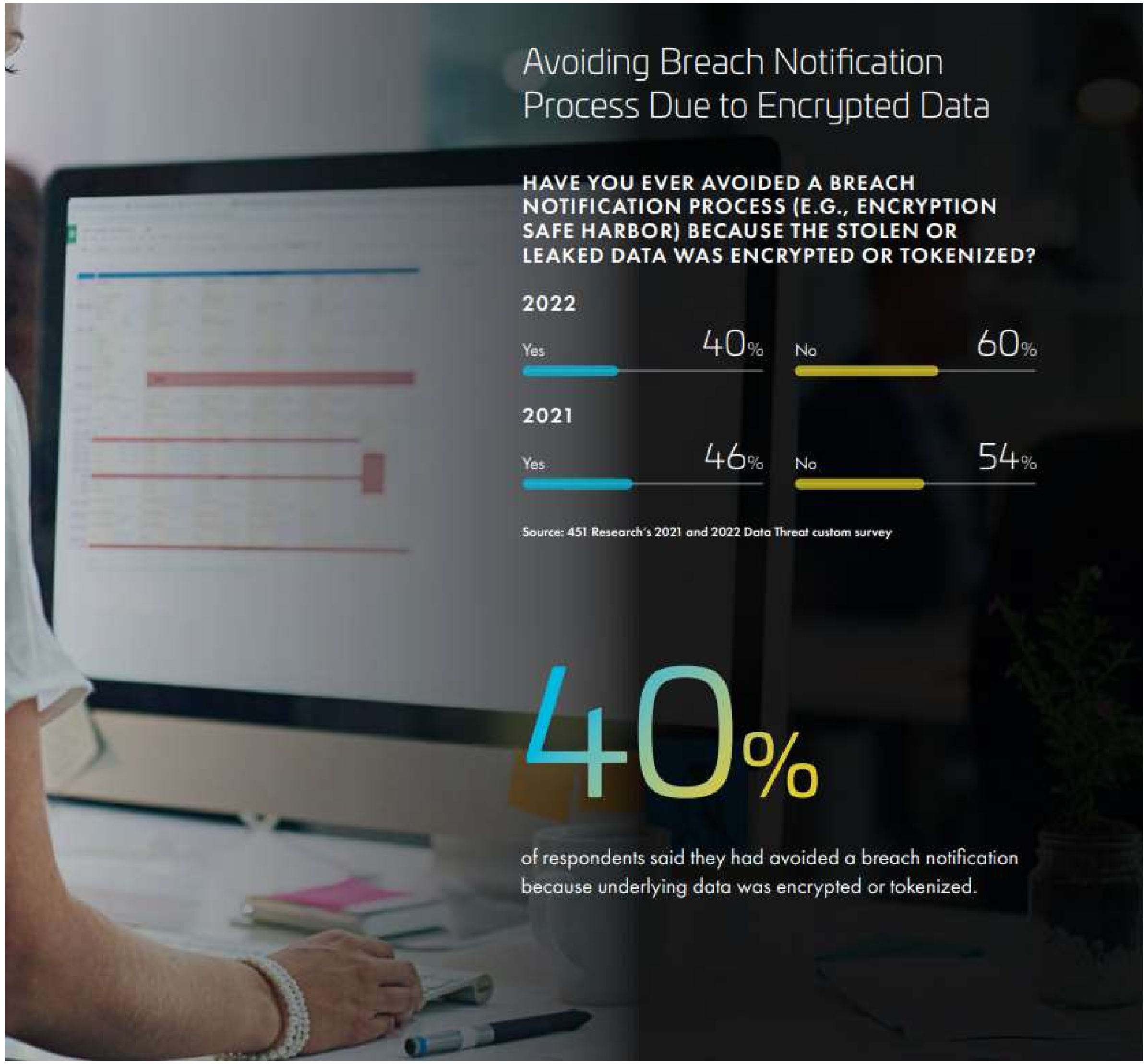
Meeting Regulatory compliances on Data Security & Privacy

Organizations & Financial Institutions are facing more and more compliance and regulatory measures and enforcement to protect the confidential data wherever it is stored or used

- ISO 27001 Requirements: A.12.3 Cryptographic controls & Key Management
- PCIDSS (Payment Card Industry Data Security Standard)
- RBI Guidelines on Information Security/Cybersecurity Framework/SEBI/IRDA
- IDRBT guidelines for Cloud Security
- Cloud Security Alliances Guidelines
- Aadhar AcT 2016 – Aadhar Data Vault
- GDPR (General Data Protection Regulation)
  - enforced from 25 May 2018
- Data Protection Bill (Coming soon)
  - Privacy by design principle to be incorporated

- **Common compliance requirements:**
  - Data **Encryption & Tokenisation**
  - **Access control** against privileged users
  - Secure **Key management**
- **Free resources**
  - https://www.thalesesecurity.com/solutions/compliance

Thales Data Threat Report 2022 Contd..



Avoiding Breach Notification Process Due to Encrypted Data

HAVE YOU EVER AVOIDED A BREACH NOTIFICATION PROCESS (E.G., ENCRYPTION SAFE HARBOR) BECAUSE THE STOLEN OR LEAKED DATA WAS ENCRYPTED OR TOKENIZED?

2022

Yes	40%	No	60%

2021

Yes	46%	No	54%

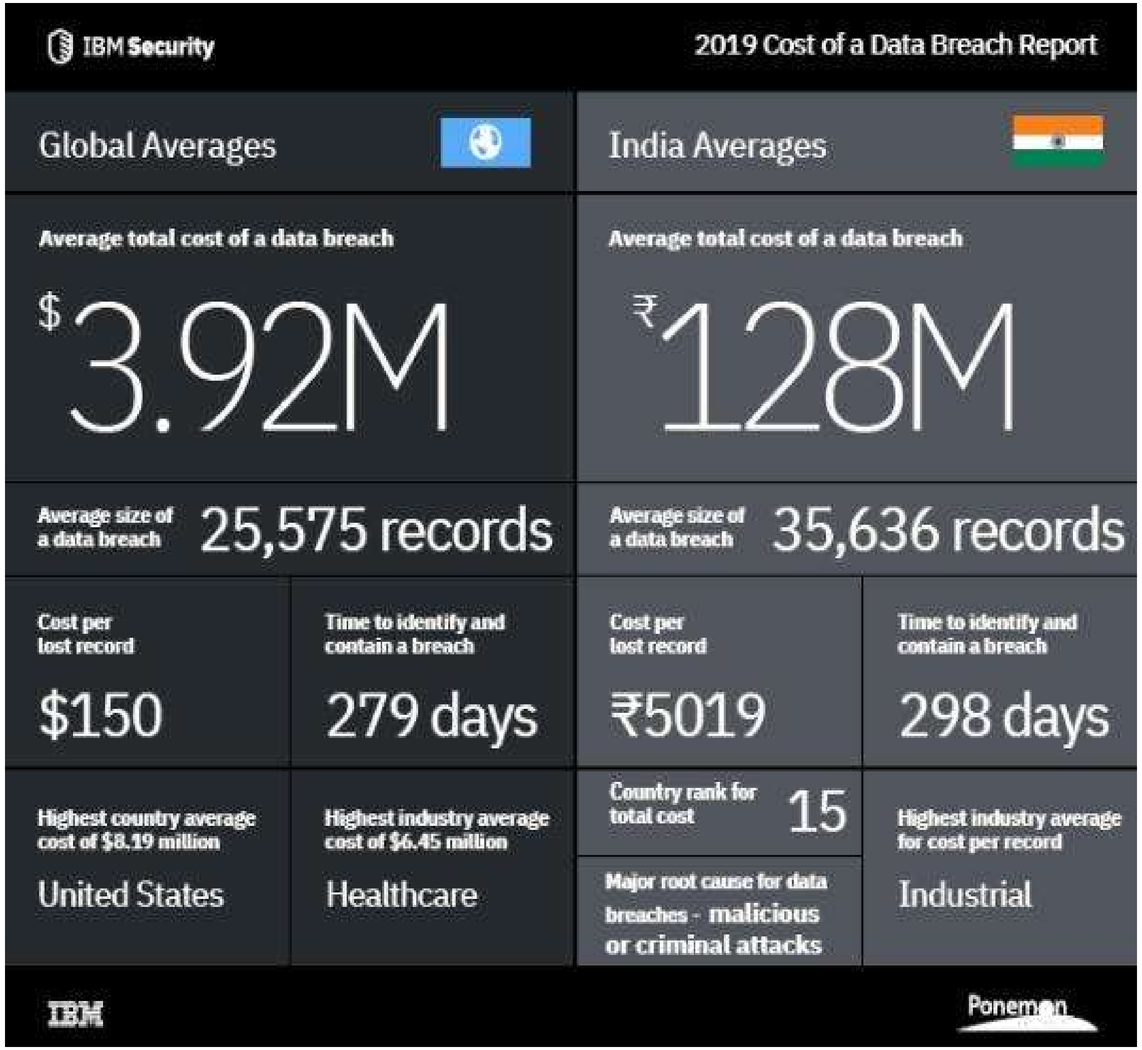
Source: 451 Research's 2021 and 2022 Data Threat custom survey

40%

of respondents said they had avoided a breach notification because underlying data was encrypted or tokenized.

Data Breach News – Recent Study by IBM

- Indian organizations lost Rs. 12.8 crore on average to data breaches
- The cost of a data breach has risen 12% over the past 5 years and now costs $3.92 million on average
- Extensive use of encryption was also a top cost saving factor, reducing the total cost of a breach by $360,000 for those organizations that invested in encryption technologies



IBM Security

2019 Cost of a Data Breach Report

Global Averages

Average total cost of a data breach

$3.92M

Average size of a data breach 25,575 records

Cost per lost record

$150

Time to identify and contain a breach

279 days

Highest country average cost of $8.19 million

United States

Highest industry average cost of $6.45 million

Healthcare

India Averages

Average total cost of a data breach

₹128M

Average size of a data breach 35,636 records

Cost per lost record

₹5019

Time to identify and contain a breach

298 days

Country rank for total cost 15

Major root cause for data breaches - malicious or criminal attacks

Highest industry average for cost per record

Industrial

IBM

Ponemon

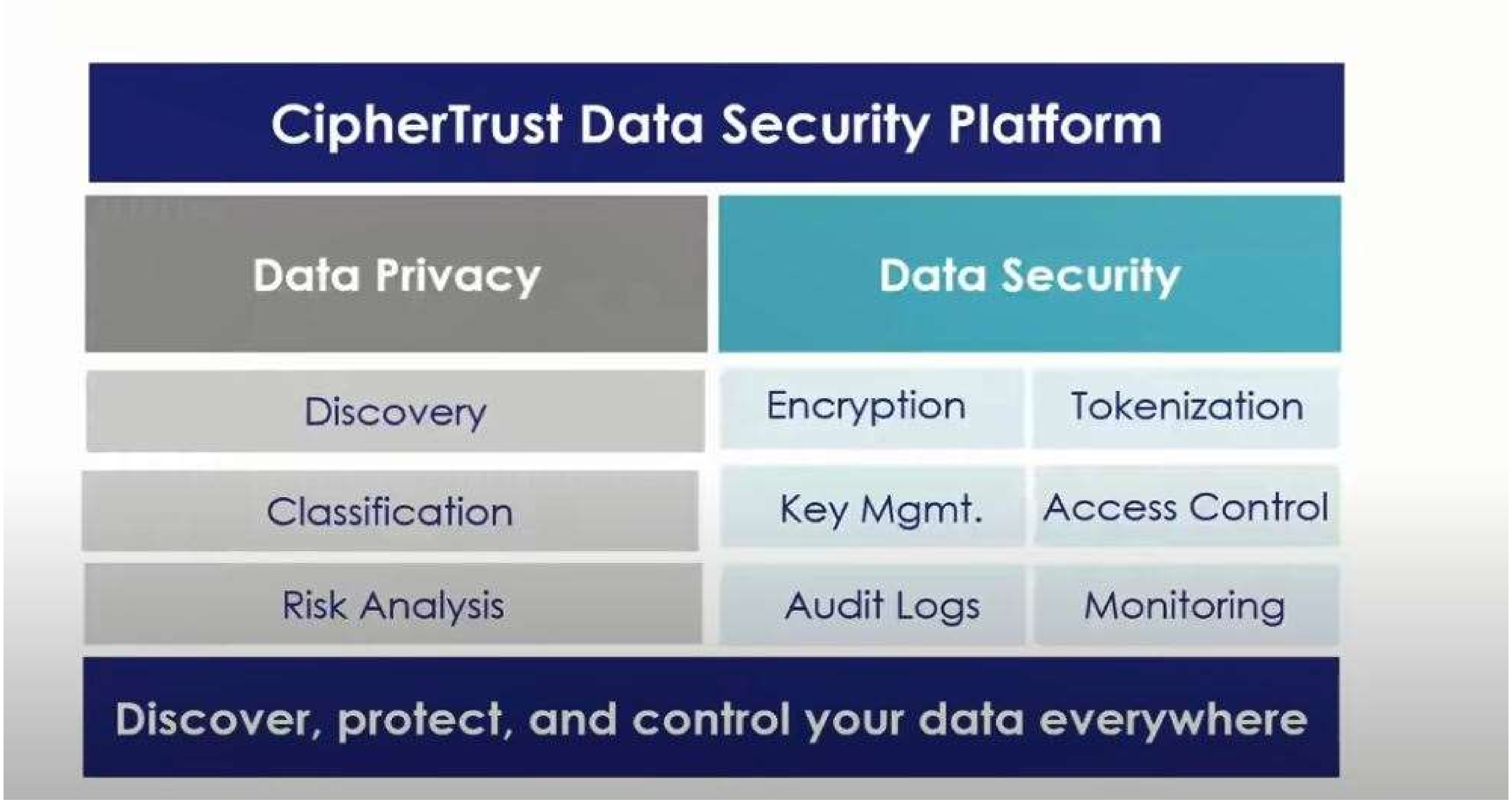
Source: https://www.csoonline.in/media-releases/indian-organizations-lost-rs-128-crore-average-data-breaches-study

Key Measures & our recommendations for Data level security

1. **Finding the sensitive Data & Classify -** (Restricted, Confidential, Public etc as per Compliance & Organization Policy) in the given Data Store
   a) Encrypt the data (PII) - such as aadhar, pan, driving license, ration card, voter id, passport numbers, bank account routing information, etc.
2. **Encrypted data & encryption keys** need to be kept in separate environment and managed separately – **Ensure Key Management system in place**
3. **For securing data in cloud** – Encryption Keys shall not be in the custody of the cloud provider but maintained by the cloud consumer as per security guidelines
4. **File Level Encryption** solution address 90% of our customers' needs alone for encryption (structured or un-structured data)
   a) prevents you against rising ransomware attacks
   b) Offers Protection from insider threats
      ✓ Prevent DBAs, System Admins, Root users from accessing data (PII)

THALES

CipherTrust Data Security Platform

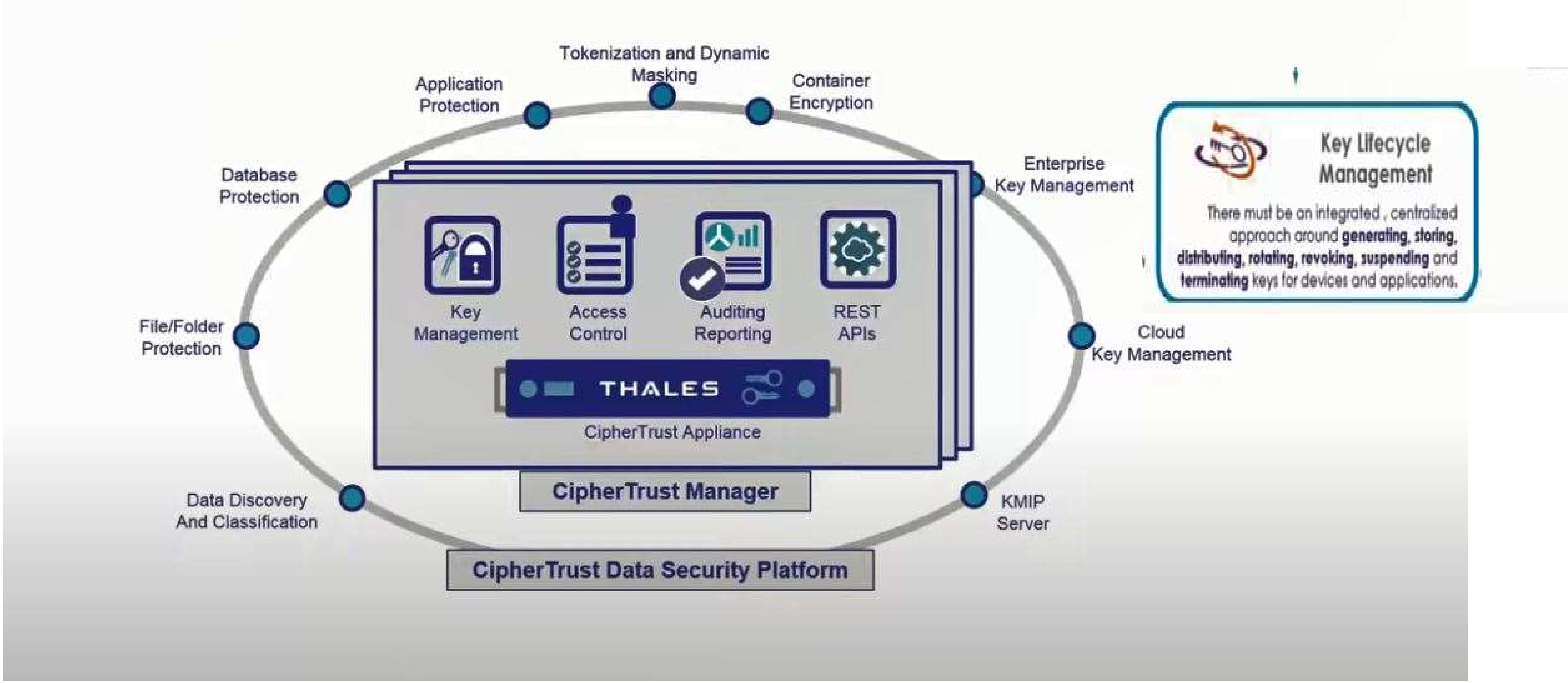


CipherTrust Data Security Platform

Data Privacy	Data Security	
Discovery	Encryption	Tokenization
Classification	Key Mgmt.	Access Control
Risk Analysis	Audit Logs	Monitoring

Discover, protect, and control your data everywhere

Thales New Data Protection & Key Management – Single window of Operation



There must be an integrated , centralized approach around **generating, storing, distributing, rotating, revoking, suspending** and **terminating** keys for devices and applications.

Thales Live Data Transformation – Patented Technology

WHEN DOWNTIME ISN'T AN OPTION,
THERE'S ONLY ONE ENCRYPTION OPTION LEFT.

Vormetric's revolutionary, newly patented technology streamlines the deployment and operation of encryption – deploy protection without business disruption.

Zero Downtime Deployments

- Transparently transform clear data to encrypted data
  - Business continuity
  - No disruption to the users, applications or business
  - Regardless of number of files or size of the database

Zero Downtime Key Rotation

- Transparently implement and schedule key rotations
  - as a best practice
  - Maintain compliance without business disruption

Patent Technology

US Patent #9203619 B2
Demo available on http://enterprise-encryption.vormetric.com/Vormetric-Live-Data-Transformation-Demo.html

Data Breach Mitigation Strategy

1. **Accept the Breach** — **Perimeter security** alone **is no longer enough**.
2. **Protect What Matters, Where It Matters** — **Data** is the **new perimeter**.
3. **Secure the Breach** — **Attach security** to the **data** and **applications**. Insider threat is greater than ever.

Breaches will happen – we must prepare!

How to Secure the Breach – The Breach Protection Strategy

SECURE THE BREACH

ENCRYPT SENSITIVE DATA

- Secure data at rest and in motion
- Secure data across environments

ESTABLISH IDENTITIES OF SENSITIVE APPLICATIONS

OWN & SECURE ENCRYPTION KEYS & APPLICATION IDENTITIES

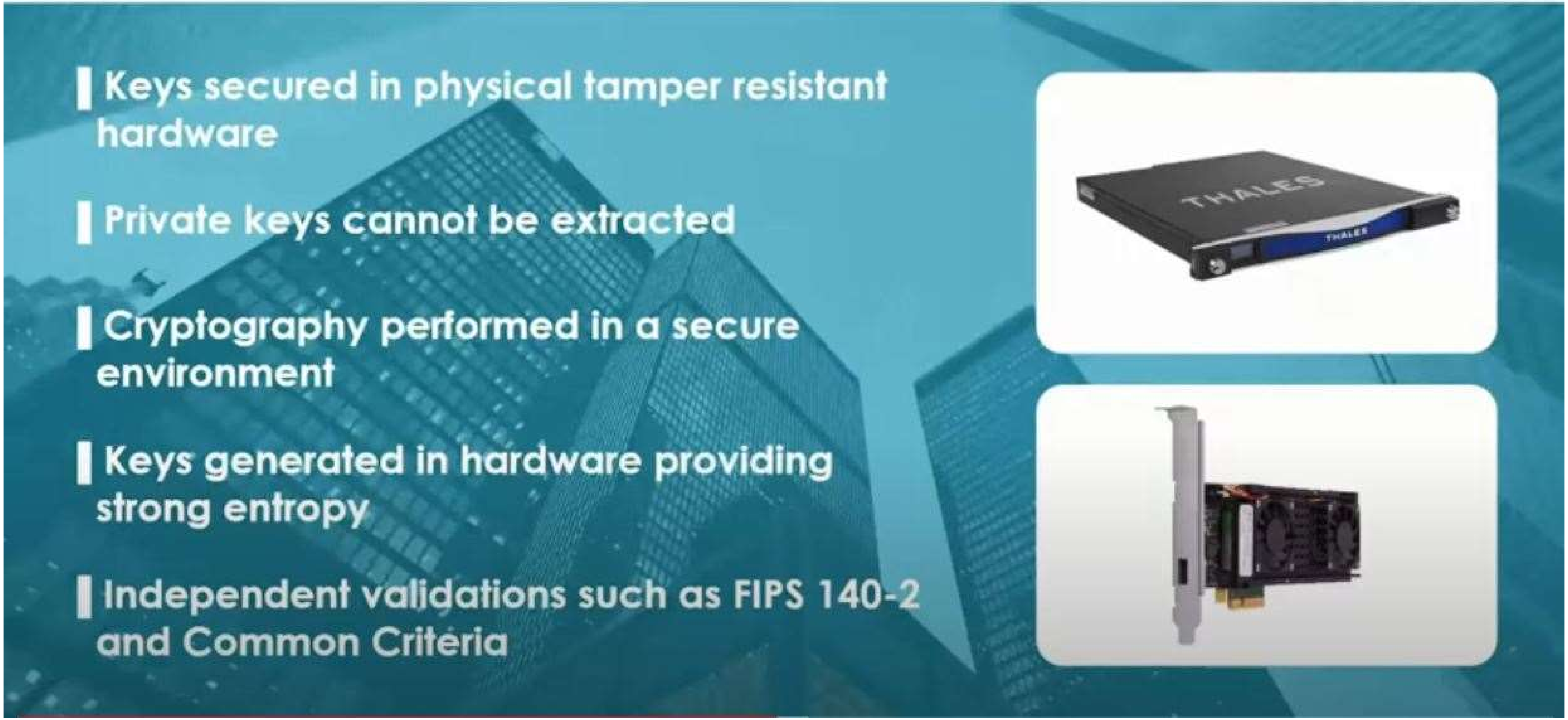
- Manage key lifecycle
- Store keys securely
- Manage cryptographic resources

MANAGE & CONTROL ACCESS

- Verify a user's identity, assess and apply the right access policy and enforce the appropriate access controls using single sign-on

THALES

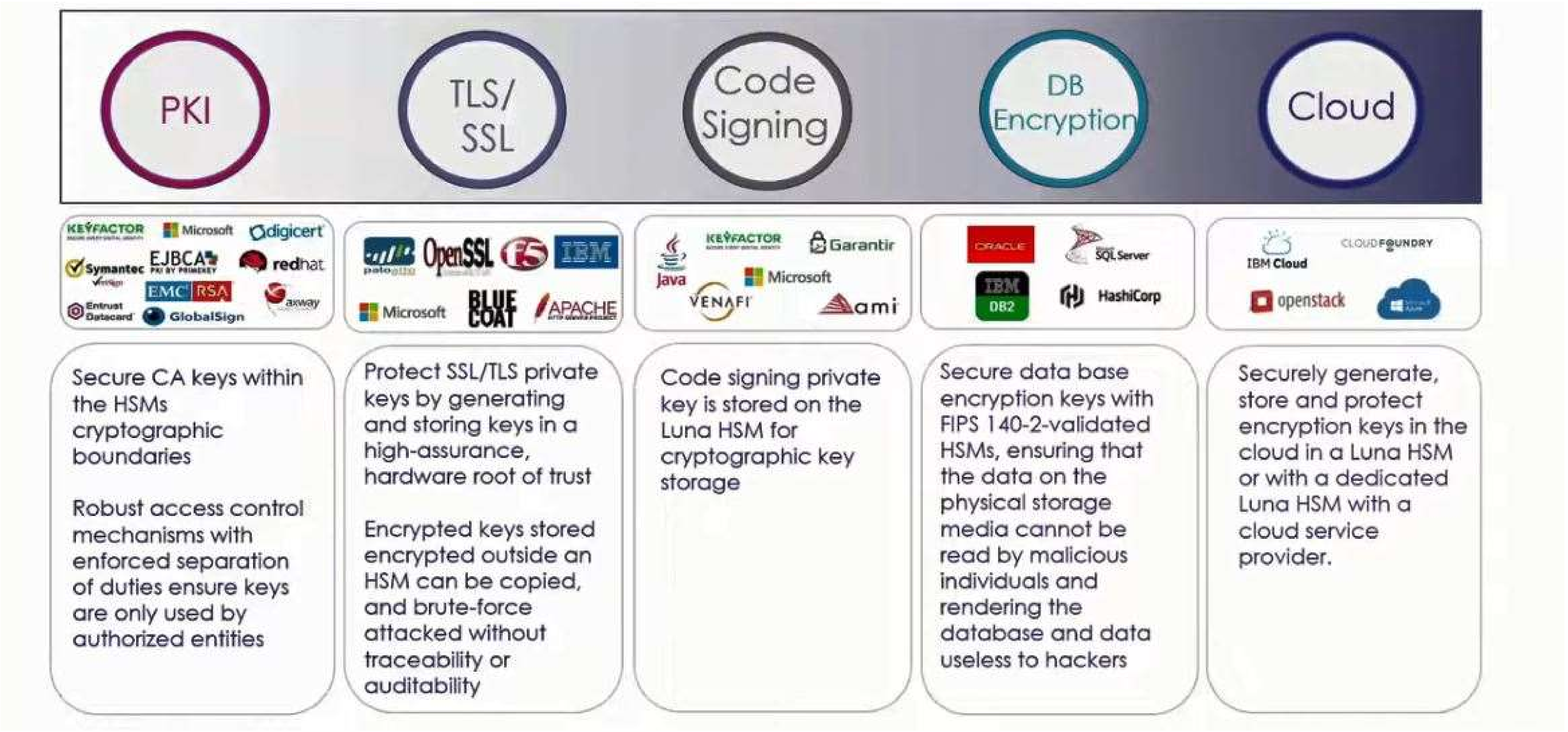
Why HSM is critical component for PKI ?



- Keys secured in physical tamper resistant hardware
- Private keys cannot be extracted
- Cryptography performed in a secure environment
- Keys generated in hardware providing strong entropy
- Independent validations such as FIPS 140-2 and Common Criteria

THALES
THALES

What for HSM to be used ? – Key Use Cases



PKI

Secure CA keys within the HSMs cryptographic boundaries

Robust access control mechanisms with enforced separation of duties ensure keys are only used by authorized entities

TLS/ SSL

Protect SSL/TLS private keys by generating and storing keys in a high-assurance, hardware root of trust

Encrypted keys stored encrypted outside an HSM can be copied, and brute-force attacked without traceability or auditability

Code Signing

Code signing private key is stored on the Luna HSM for cryptographic key storage

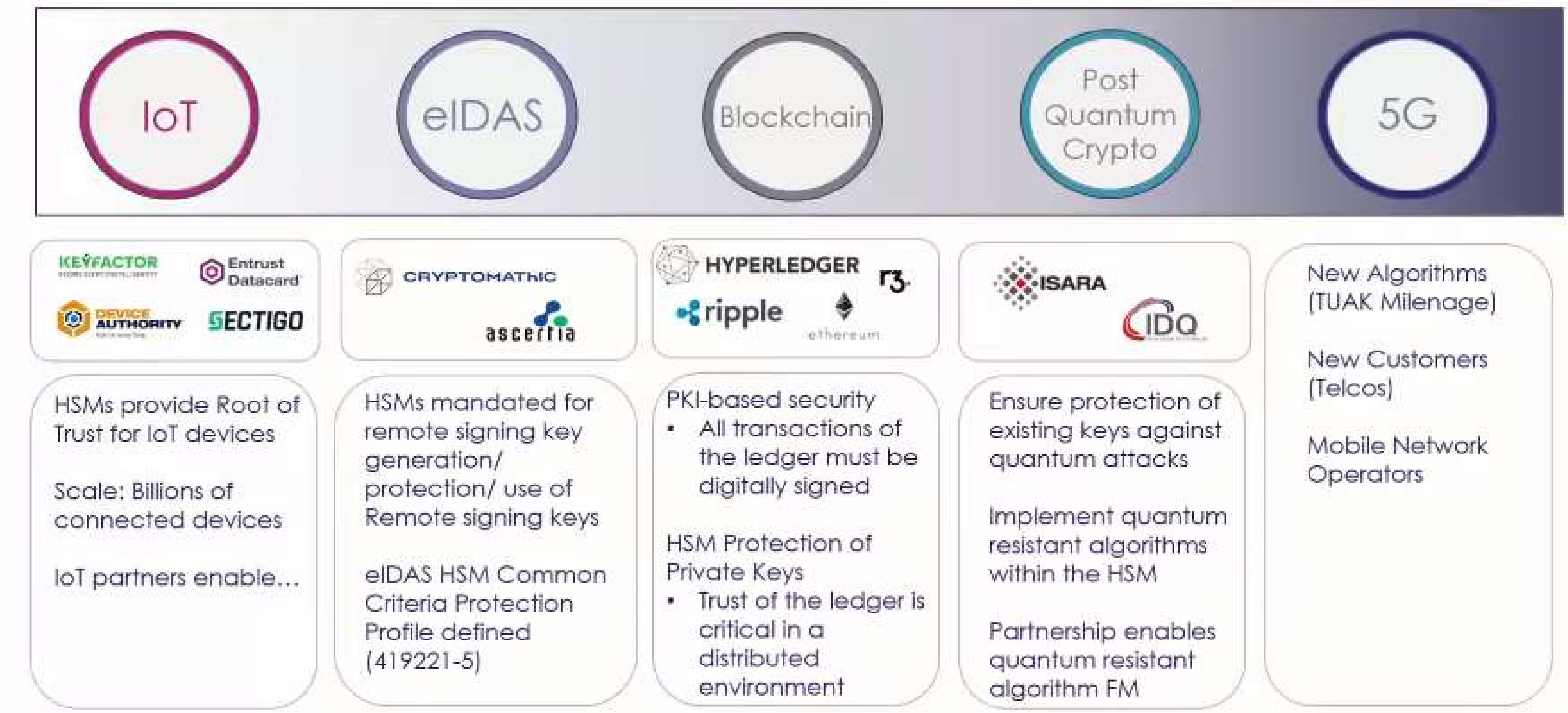
DB Encryption

Secure data base encryption keys with FIPS 140-2-validated HSMs, ensuring that the data on the physical storage media cannot be read by malicious individuals and rendering the database and data useless to hackers

Cloud

Securely generate, store and protect encryption keys in the cloud in a Luna HSM or with a dedicated Luna HSM with a cloud service provider.

Modern Technology Use Case



IoT

KEYFACTOR
Entrust Datacard
DEVICE AUTHORITY
SECTIGO

HSMs provide Root of Trust for IoT devices

Scale: Billions of connected devices

IoT partners enable…

eIDAS

CRYPTOMATHIC
ascertia

HSMs mandated for remote signing key generation/ protection/ use of Remote signing keys

eIDAS HSM Common Criteria Protection Profile defined (419221-5)

Blockchain

HYPERLEDGER
r3
ripple
ethereum

PKI-based security

- All transactions of the ledger must be digitally signed

HSM Protection of Private Keys

- Trust of the ledger is critical in a distributed environment

Post Quantum Crypto

ISARA
IDQ

Ensure protection of existing keys against quantum attacks

Implement quantum resistant algorithms within the HSM

Partnership enables quantum resistant algorithm FM

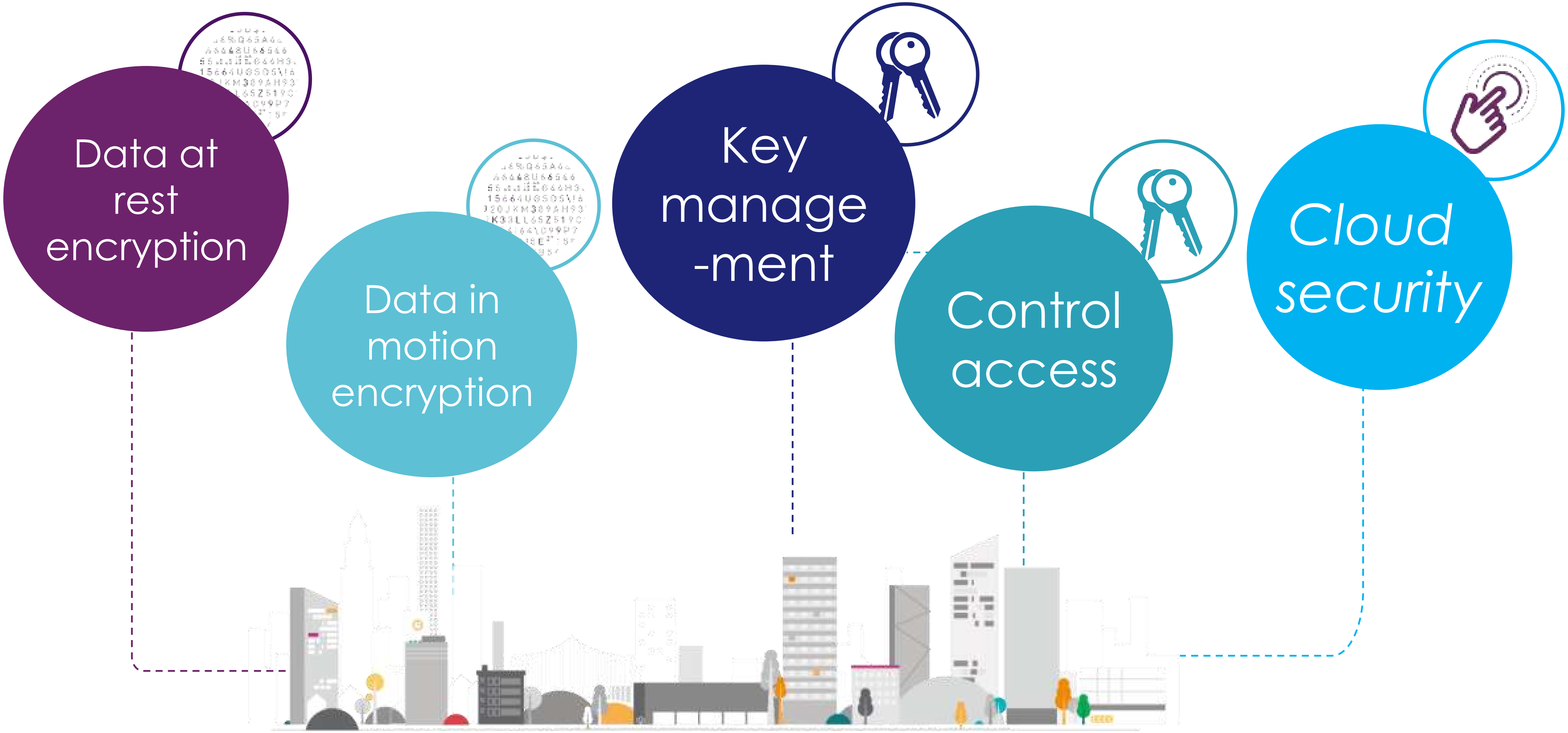
5G

New Algorithms (TUAK Milenage)

New Customers (Telcos)

Mobile Network Operators

What Organizations are looking for today…



Data at rest encryption

Data in motion encryption

Key manage -ment

Control access

Cloud security

Knowledge workshop – 2 hr

At What Level do we need to encrypt data

- Protecting data in transit
- Database level encryption
- Application Level Encryption

Encryption Operation Lifecycle

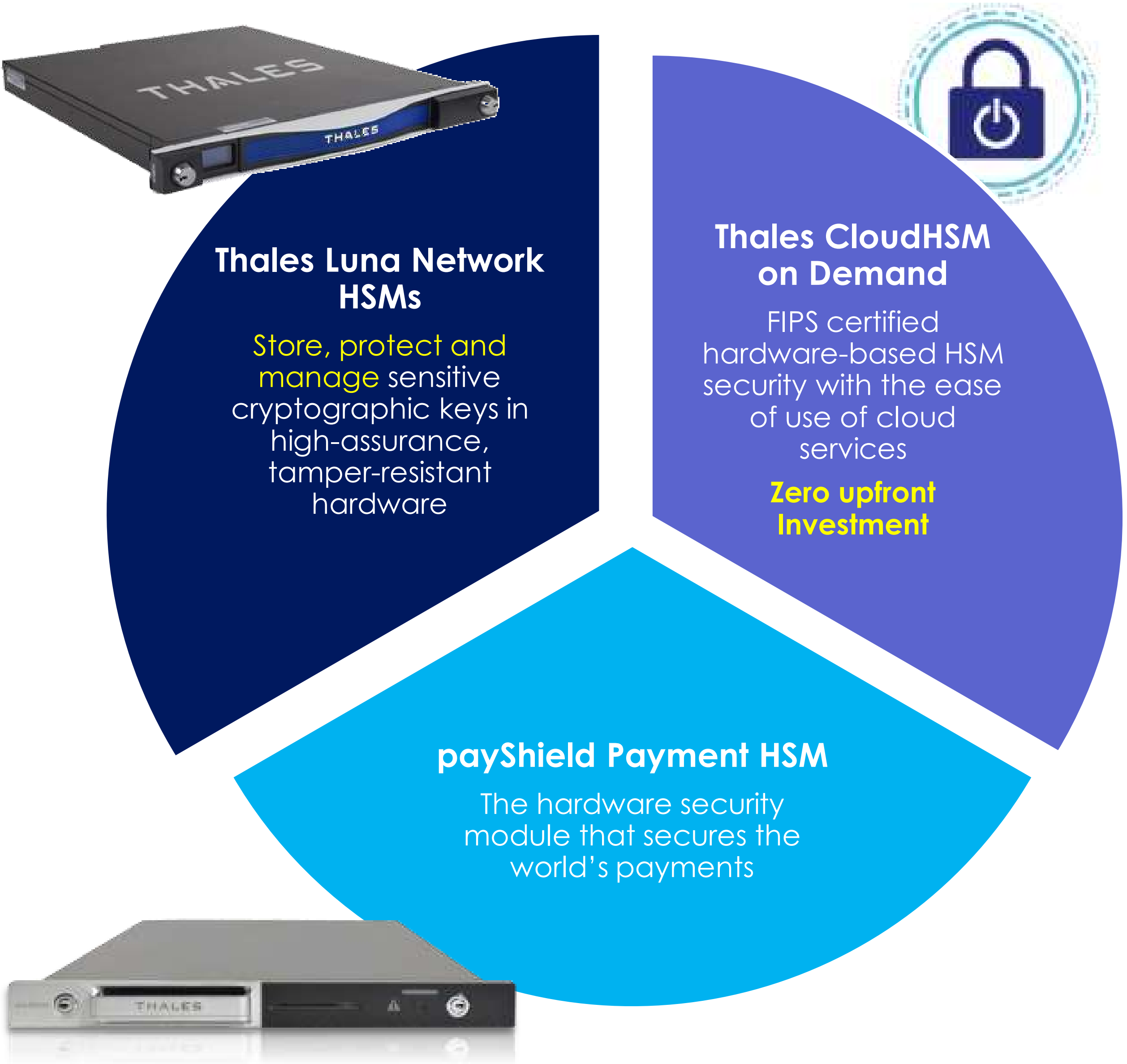
- Authorized encryption Approaches & Mechanism
- Mapping of Encryption scheme based on data classification and security association
- Key Management Lifecycle
- Monitoring & Exception Handling

How CipherTrust will integrate in your IT Environment

THALES

Thanks.
Email – ved-v.Prakash@thalesgroup.com
Mobile No : +91 - 9029963079

Data Protection and Privacy
Thales Hardware Security Modules (HSMs)



Thales Luna Network HSMs

Store, protect and manage sensitive cryptographic keys in high-assurance, tamper-resistant hardware

Thales CloudHSM on Demand

FIPS certified hardware-based HSM security with the ease of use of cloud services

Zero upfront Investment

payShield Payment HSM

The hardware security module that secures the world's payments

General Purpose HSM

(Luna)

- IoT
- 5G
- Blockchain
- PKI
- Code Signing
- Quantum
- Remote Signing
- Aadhar Data Vault
- SSL /TLS
- Smart Card Issuance

✓ Secure CA keys within HSM

✓ Protect SSL/TLS Pvt keys

PayShield Payment HSM

- Payment credential issuing – cards, mobile secure elements, wearables, connected devices and host card emulation (HCE) applications
- Point to point encryption (P2PE)
- Security tokenization (for PCI DSS compliance)
- EMV payment tokenization
- Card and mobile payment authorization
- POS, mPOS and SPoC key management
- PIN and EMV cryptogram validation
- Remote key loading

Engagement Use cases

- Encrypt PIII Data at servers, files, within databases
- Encrypting KYC images files that contain Aadhar
  - Video eKYC data, Voice biometrics stored for voice banking
- Centralized Key Management - achieve separation of duties in encryption process implemented in applications
  - Make sure all keys at diff apps can be managed without fail automatically and keys are rotated periodically
  - If someone accidentally delete the cryptographic key(s) there are the measures to recover
- Sys admin should not able to see the PII data
- Encryption of password in configuration files.
- Encryption of critical data fields in storage and transit – Data at rest encryption
  - TDE services on SQL server database, oracle etc for safeguarding against unauthorised access, insider threat
  - The Master keys applied for the TDE will be securely transferred and stored in Thales KMS
- Sharing sensitive data with outside vendor – Tokenization & Data Masking
- Securing data on cloud - Office 365, Amazon or Azure with BYOK (bring your own keys)
- **Non Compliance -** As per RBI /IDRBT not having the appropriate mechanism would get notified during audit
  - If the key operation goes wrong, and the procedure clearly violates the regulatory guideline, who will be responsible

The more **data** you possess…

- Who controls the keys?
- Where are the keys located?
- Are the keys trusted?
- Will they pass an audit?
- Do they work with my 3rd party applications?

The more **Encryption Keys** you have to store and manage

RBI Cybersecurity Framework & Thales Solution Mapping

Requirements	Clauses
Data Discovery & Classification Base line controls, page 7 sec 1.2 Classify data/information	based on information classification/sensitivity criteria of the bank
Data Security	
• Banks need to ensure the integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives.	Chapter II, Information Security – Data Security (i), (v), (ix)
Encryption of Data at the Core	
• Structured Data: Applications' Data, Databases	Chapter II, Information Security –Application Control and Security (3,5,6,7,11,14,15,16,23) Encryption (ii, iii a-f, v)
• Unstructured Data: File Servers, Archives	
Centralized Key Management for Effective Encryption Implementation	
• Mistaken or intended modification of data, eve by bypassing applications is controlled	Chapter II, Information Security – Encryption (iv a-k)

DDC

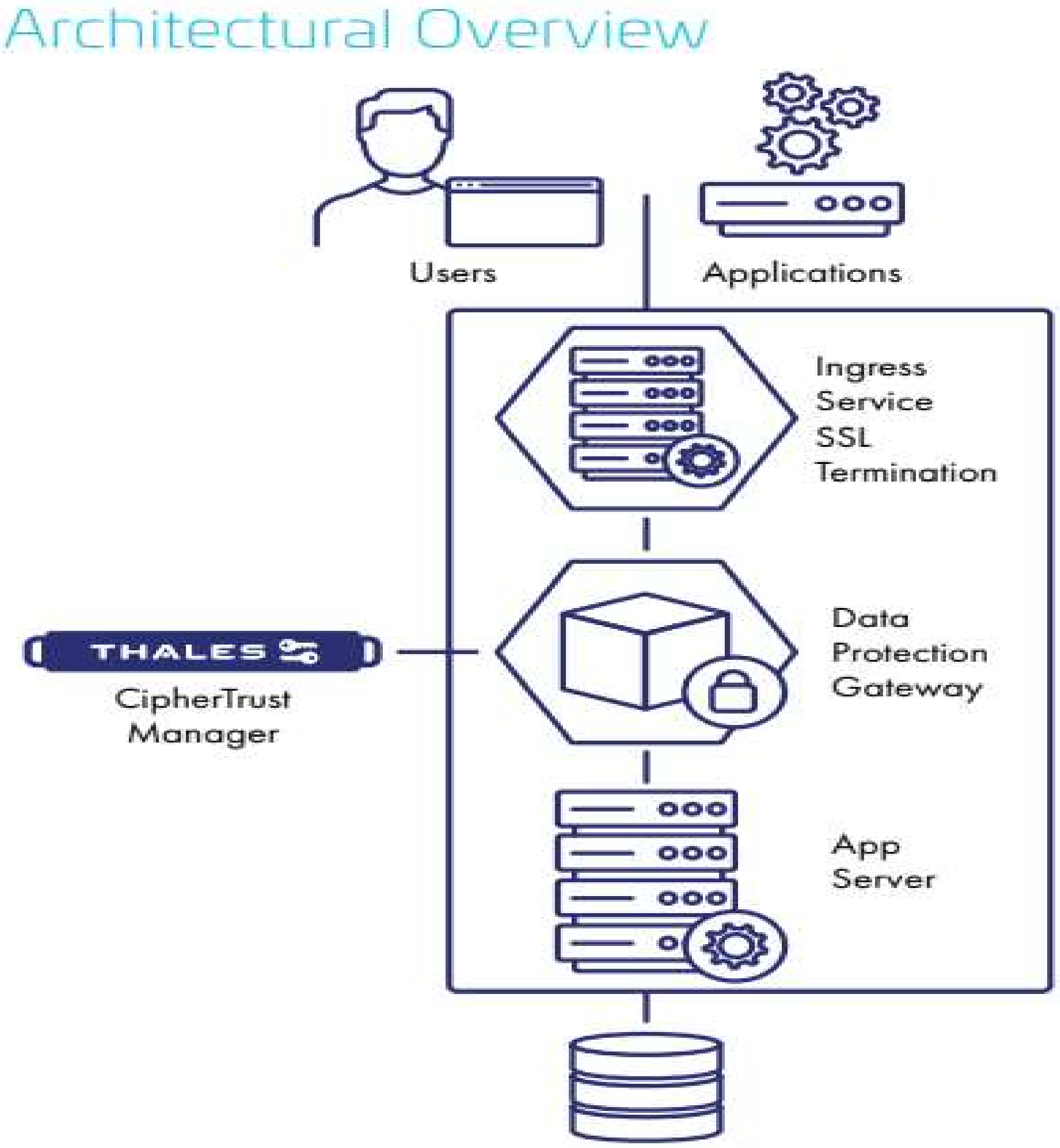
Confidentiality (Encryption + Centralized Key Management)
Authentication, Non Repudiation
HSM: DigSig Verification

Thales Crypto Suite:
Application Encryption
Database Encryption
Transparent Encryption:
File Server Encryption
VM machine encryption

Centralized Key Management

THALES

Architectural Overview



Key Technologies

1. **Data Discovery & Classification** - Know where is your sensitive data, classify its sensitivity level
2. **Data Encryption** - is the process of scrambling plain data into an unreadable format through the use of an algorithm that creates a unique “key” known as an “encryption key” or “crypto key”
   - ✓ BYOK - Empower Customer to control own keys
   - ✓ BYOE – Empower customer to control complete encryption process
3. **Tokenization** - is the process of assigning a random surrogate value (also known as a “Token”) to the original data to avoid it’s easy identification. The original data is first received at its initial entry point by the Tokenization Manager and then encrypted.
4. **Data Masking - Also known as “Data Obfuscation”**, data masking is the process of hiding (or obscuring) the original data with random characters or other data.
   1. Masked sensitive data before sharing with third-party
   2. Initial encryption or tokenization of PII data in production databases to meet privacy mandates/regulations
   3. Enabling DevOps team to utilize actually represented data without any sensitive information available in clear
5. **Centralized Key Management** - Since encryption keys pass through multiple phases during their lifetime – like generation, distribution, rotation, archival, storage, backup and destruction, key management plays a pivotal role in optimal data protection.

Understanding Key Management

KEY MANAGEMENT

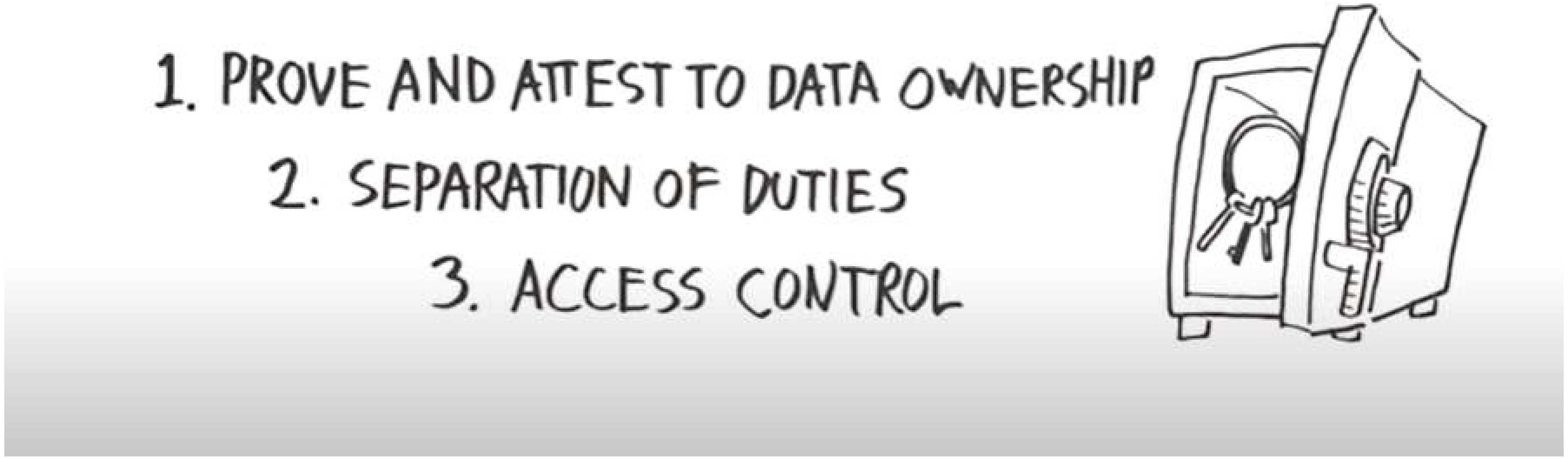
PROTECTING, STORING, BACKING UP AND ORGANIZING ENCRYPTION KEYS

Two Main reason for

SENSITIVE DATA BREACH
COMPLIANCE & GOVERNANCE

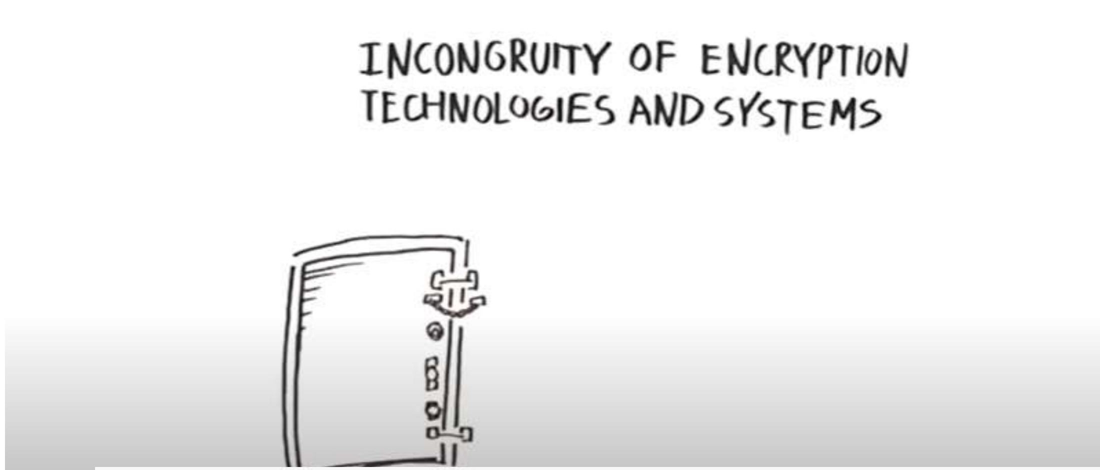
1. BREACHES, SENSITIVE DATA LOSS

2. COMPLIANCE AND GOVERNANCE OF SENSITIVE DATA

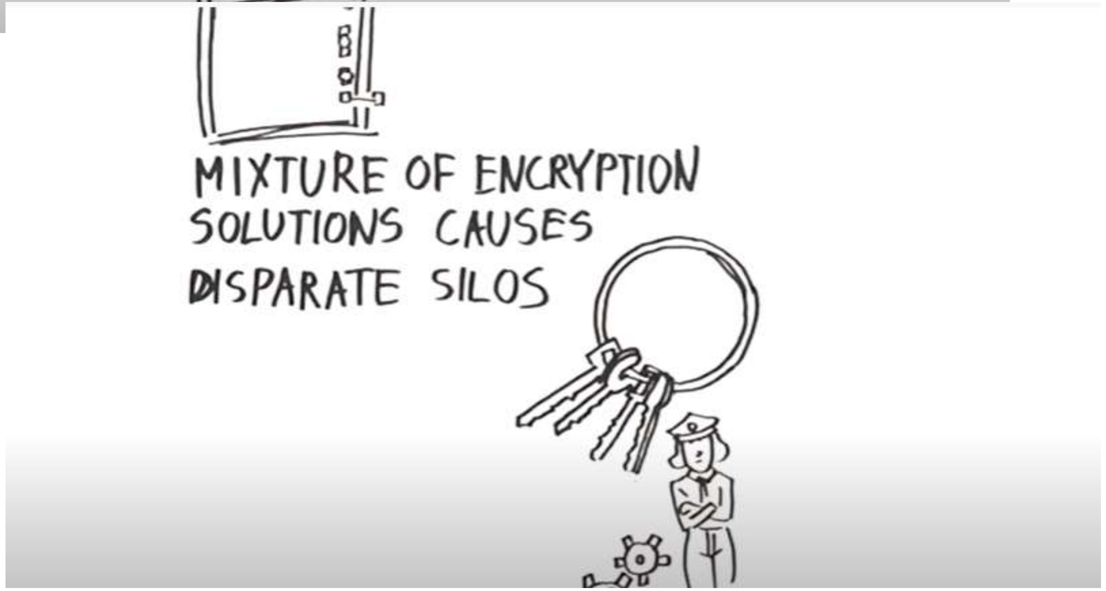


1. PROVE AND ATTEST TO DATA OWNERSHIP
2. SEPARATION OF DUTIES
3. ACCESS CONTROL

Challenges Organizations having with encryption keys:



INCONGRUITY OF ENCRYPTION TECHNOLOGIES AND SYSTEMS



MIXTURE OF ENCRYPTION SOLUTIONS CAUSES DISPARATE SILOS

Pain Point – Siloed Approaches cause Security blind spots

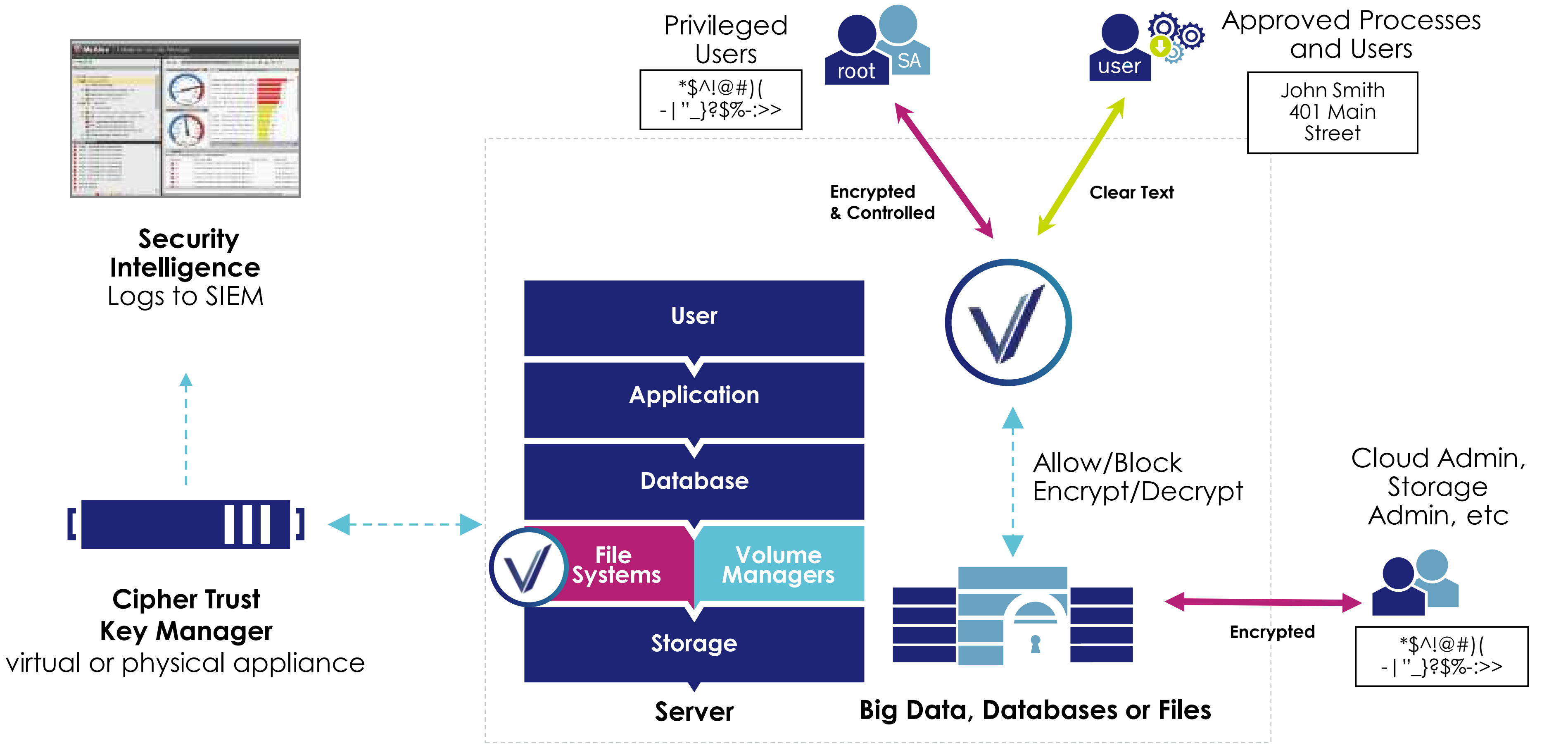
Database Encryption	Full Disk Encryption	Data Masking	Token-ization	Cloud Encryption	File Encryption	Access Policies	
Customer Records	Physical Security	PHI	PCI	Cloud Migration	Big Data	Privileged User Control	…

$ + $ + $ + $ + $ + $ + $

Each use case requires individual infrastructure, management consoles and training

Complex • Inefficient • Expensive

How Thales Transparent Encryption Works



Security Intelligence
Logs to SIEM

Cipher Trust Key Manager
virtual or physical appliance

Privileged Users

*$^!@#)(
-|"_}?$%-:>>

root

SA

Encrypted & Controlled

user

Approved Processes and Users

John Smith
401 Main
Street

Clear Text

User

Application

Database

File Systems

Volume Managers

Storage

Server

Allow/Block
Encrypt/Decrypt

Big Data, Databases or Files

Encrypted

Cloud Admin, Storage Admin, etc

*$^!@#)(
-|"_}?$%-:>>

Some of the current problem areas? Here we contribute:

1. **Discovering & classifying sensitive data (PII)? –** How are you doing data discovery and
2. **How are you managing /mitigating the risks with PII /sensitive data**
   a) What will be the best or consistent encryption strategy helpful in safeguarding the sensitivedata
   b) Are you considering -Application level encryption of data , file/folder level encryption
   c) Data at rest/in use/I transit, Techniques like - Tokenization & Data masking
3. **How are we achieving separation of duties in encryption process implemented in applications?**
   a) Decouple keys from data - Encryption Keys should always be segregated and separately managed from Application Owners in a certified Key management Solution (FIPs 140-2 Level 3 & Above)
   b) How do you ensure that the Sys admin is not able to see the PII data from the data base?
4. **Do you have a Key Management Policy? Or Centralized & Automated Key Management System**
   a) How do you protect, store & manage the encryption keys? How many encryption keys are involved?
   b) Silo encryption processes running with no centralized visibility to encryption key management
      ✓ *What* keys are created, *Where* the keys are stored, *Who* can access the keys, *When* the keys are revoked
   c) Just confined to using of Native TDE functionality for SQL/MS SQL/Oracle and not storing & managing Master keys separately
   d) How to make sure all keys at diff apps and can be managed without fail automatically
   e) How to manage key rotation ? If someone accidentally delete the cryptographic key(s) what are the measures to recover (if any).
   f) What's the consequence of non-compliance. If the key operation goes wrong, and the procedure clearly violates the Bank's Cyber Policy, who will be responsible?
5. **How are you moving workloads on multi cloud environment? –** Are you considering the bring your own key (BYOK) and Bring your own encryption (BYOE) approaches?
6. **How is privacy by design principle being incorporated in current IT System landscape?**

Thales Live Data Transformation – Patented Technology

WHEN DOWNTIME ISN'T AN OPTION,
THERE'S ONLY ONE ENCRYPTION OPTION LEFT.

Vormetric's revolutionary, newly patented technology streamlines the deployment and operation of encryption – deploy protection without business disruption.

Zero Downtime Deployments

- Transparently transform clear data to encrypted data
  - Business continuity
  - No disruption to the users, applications or business
  - Regardless of number of files or size of the database

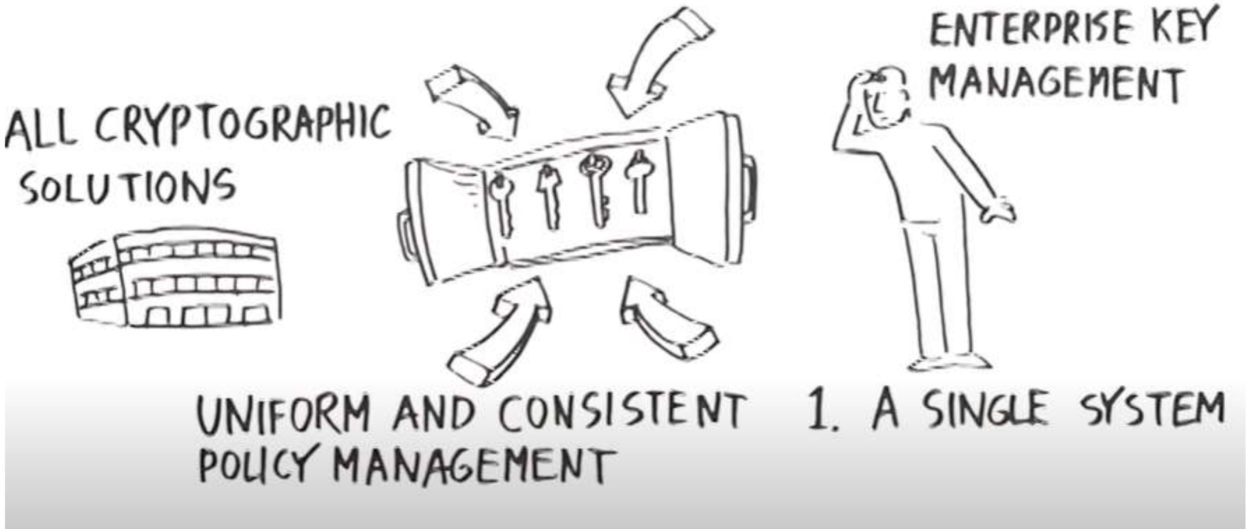
Zero Downtime Key Rotation

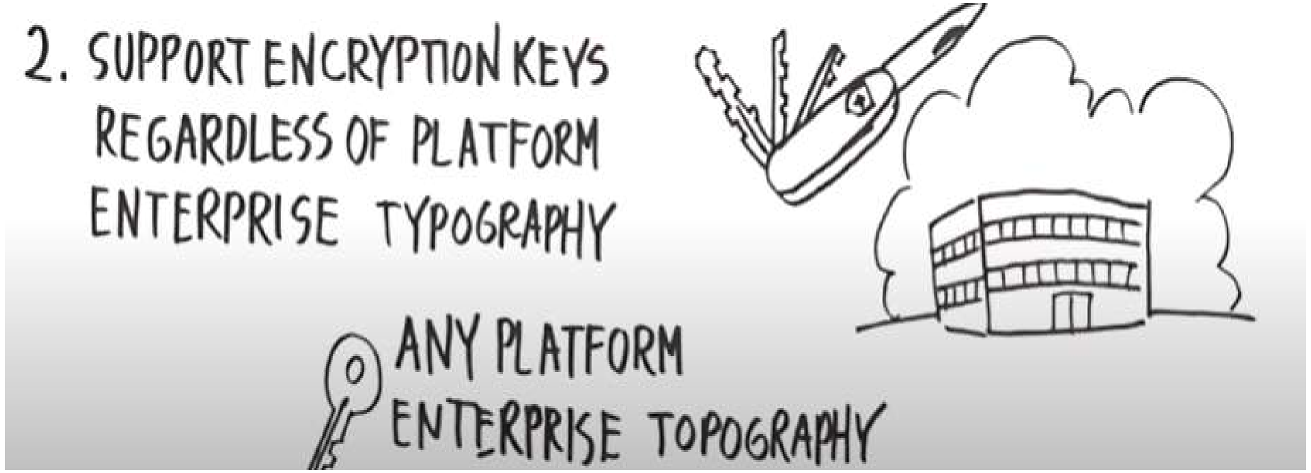
- Transparently implement and schedule key rotations
  - as a best practice
  - Maintain compliance without business disruption

Patent Technology

US Patent #9203619 B2
Demo available on http://enterprise-encryption.vormetric.com/Vormetric-Live-Data-Transformation-Demo.html

What to look for – when implementing KMS Solution


ALL CRYPTOGRAPHIC SOLUTIONS
ENTERPRISE KEY MANAGEMENT
UNIFORM AND CONSISTENT POLICY MANAGEMENT
1. A SINGLE SYSTEM


2. SUPPORT ENCRYPTION KEYS REGARDLESS OF PLATFORM ENTERPRISE TYPOGRAPHY
ANY PLATFORM ENTERPRISE TOPOGRAPHY

Support Multi Cloud /On Premise or Hybrid Environment

Problems of Silo based encryption – Inefficiency + complexity

INEFFICIENT AND A WASTE OF TIME AND RESOURCES

WHERE IS IT!

ORGANIZATIONS

- EXPERIENCE KEY LOSS OR PERMANENT DATALOSS

New -CipherTrust Data Protection Gateway - What does it do?

- Customers understand the benefits of app-layer protection, but sometimes find it painful to deploy our products and retro fit their applications
- DPG aims to solve this problem by protecting sensitive data without needing any code changes! We are starting off with protecting JSON data in REST API's. So, for instance you might specify that you want to protect a JSON field called "Credit_card" by using the FF1 algorithm.
- The CipherTrust Data Protection Gateway from Thales offers transparent data protection to any RESTful web service or microservice leveraging REST APIs
- The Gateway interprets RESTful data and performs protection operations based on profiles defined centrally in the Thales CipherTrust Manager and operates seamlessly with other components such as ingress services used to terminate SSL